Deciphering Black Basta's Infrastructure from the Chat Leak

flare.io/learn/resources/blog/deciphering-black-bastas-infrastructure-from-the-chat-le

March 6, 2025

This article has originally appeared on Cybercrime Diaries

On February 20, 2025, the cybersecurity community received an unexpected stroke of luck as internal strife seemingly spread within the infamous Black Basta ransomware group. On that day, an unknown individual using the alias ExploitWhispers released a file on Telegram, allegedly containing the group's internal chat logs. The file was a JSON dataset comprising of 196,045 messages from a Matrix/Element chat, primarily in Russian, spanning from September 18, 2023, to September 28, 2024.

While the true identity of the leaker and their actual motives remain unknown, ExploitWhispers accused Black Basta of crossing a red line by targeting Russian banks. A preliminary analysis suggests that most, if not all, of the leaked data appears legitimate. However, the possibility of data manipulation cannot be entirely ruled out.

Black Basta is a ransomware-as-a-service (RaaS) group that emerged in April 2022 and has since attacked over 500 organizations worldwide across various sectors, including healthcare, manufacturing, and utilities. Notable victims include Ascension, Dish Network, Maple Leaf Foods, BT Group, and Rheinmetall. According to estimates published by The

Record in November 2023 the group received over 100 million dollars in ransom payments to that date. However, since January 2025 no new victims have been reported and the group's leak site is presently down, suggesting that an internal conflict could have shaken up the group.

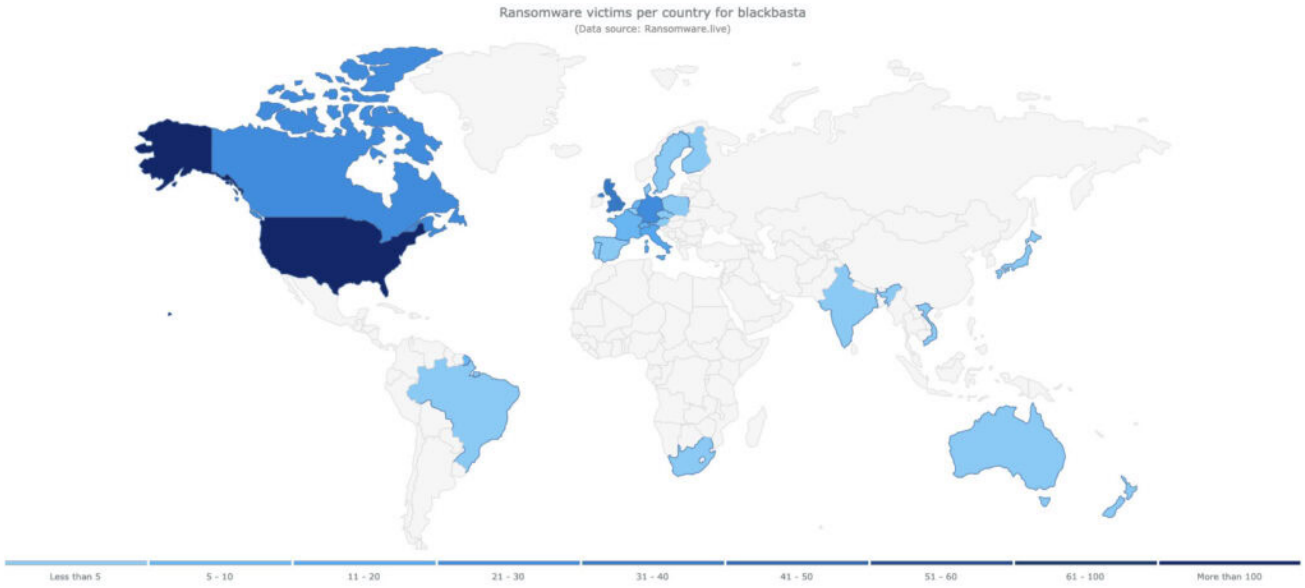

Figure 1: Ransomware victims per country for Black Basta (Source: Ransmware.live)

Back in 2022, this RaaS was founded by Conti Team 3, also known as Tramp's team, which remained in control of the group during the period covered by the leak. In the leaked chat, Tramp appears under the aliases gg and aa. An investigation by LeMagIT, supported by external sources, confirmed that the likely real identity of this threat actor is Oleg Nefedov, a Russian citizen originally from Yoshkar-Ola.

While extensive research has already been published, providing insights into who Nefedov is and which vulnerabilities the group exploited, this short blog focuses on Black Basta's internal organization. Additionally, this will offer a glimpse into how and where the group hosted and obfuscated its leak site and C2 servers.

Back in 2022, this RaaS was founded by Conti Team 3, also known as Tramp's team, which remained in control of the group during the period covered by the leak. In the leaked chat, Tramp appears under the aliases gg and aa. An investigation by LeMagIT, supported by external sources, confirmed that the likely real identity of this threat actor is Oleg Nefedov, a Russian citizen originally from Yoshkar-Ola.

While extensive research has already been published, providing insights into who Nefedov is and which vulnerabilities the group exploited, this blog will primarily focus on Black Basta's internal organization. This offers a look into how and where the group hosted and obfuscated its leak site and C2 servers.

Key Observations from the Leak and Available Information

- The true identity of the group's leader, Tramp (aka gg), is possibly Oleg Nefedov, a 35-year-old Russian citizen from Yoshkar-Ola, who is officially known as a successful entrepreneur, but claims to be protected by powerful friends allowing him to pursue his malicious endeavors.
- Black Basta operates as a highly structured and hierarchical organization, with at least two offices, likely located in Moscow or its outskirts.
    - Group members have several different specializations focusing on areas such as infrastructure management, initial access, malware and C2 obfuscation, development, and negotiations.
    - A key distinction existed between threat actors who were employees of the group—working under Tramp's direct and strict supervision in office settings—and more independent operatives, known as pentesters or affiliates, working online.
    - These independent affiliates were often Tramp's former associates from other illicit operations, such as Conti RaaS or banking trojans. They operate within their own teams, using distinct tools, methods, and internal hierarchies. This division sometimes leads to tensions between them and Black Basta's core management.
    - The group periodically changes Matrix servers for OSPEC reasons. In September 2024, Tramp decided to migrate to a new server. This can also be explained by Tramp's brief arrest that almost resulted in an extradition from Armenia during a vacation trip in June 2024.
- Black Basta members are active on major Russian-language cybercrime forums such as XSS, Exploit, and RAMP, where they purchase services from other threat actors. These services include crypting (payload obfuscation), hosting, spam campaigns, exploits, and initial access to compromised networks.
- The group's leak site, admin panel, and C2 servers were primarily hosted on legitimate providers such as Hetzner, but these were acquired through third-party resellers that specialized in server rentals and accepted cryptocurrency payments.

    Infrastructure obfuscation appeared to be a more viable strategy than relying on bulletproof hosting. However, bulletproof hosting services, such as Gerry, were used for deploying abuse-resistant C2 servers for Cobalt Strike and for fast-flux capabilities, which helped conceal the real IP addresses of domains.
- Overall, the leak of this chat underscored once again that a substantial part of cybercriminal activity takes place outside forums or public chats, with the latter being just the tip of the iceberg.

Black Basta's Organization and Internal Hierarchy

A statistical analysis of the leaked data provided valuable insight into the group's hierarchy. The most active user—by far—was the leader, Tramp, also known as "gg" (@usernamegg in the Figure 2 below). He was responsible for coordinating other members, developing new

methods for obtaining initial access, participating in attacks, handling negotiations, and maintaining strict control over his employees. He enforced this control by personally visiting both offices where they operated.

Lapa is the second most active user, he can be described as a senior “pentester” who seemingly knew Tramp before joining the chat in September 2023. The majority of messages from this user were related to access to corporate networks of victims. There are also active external pentesters such as “w.”

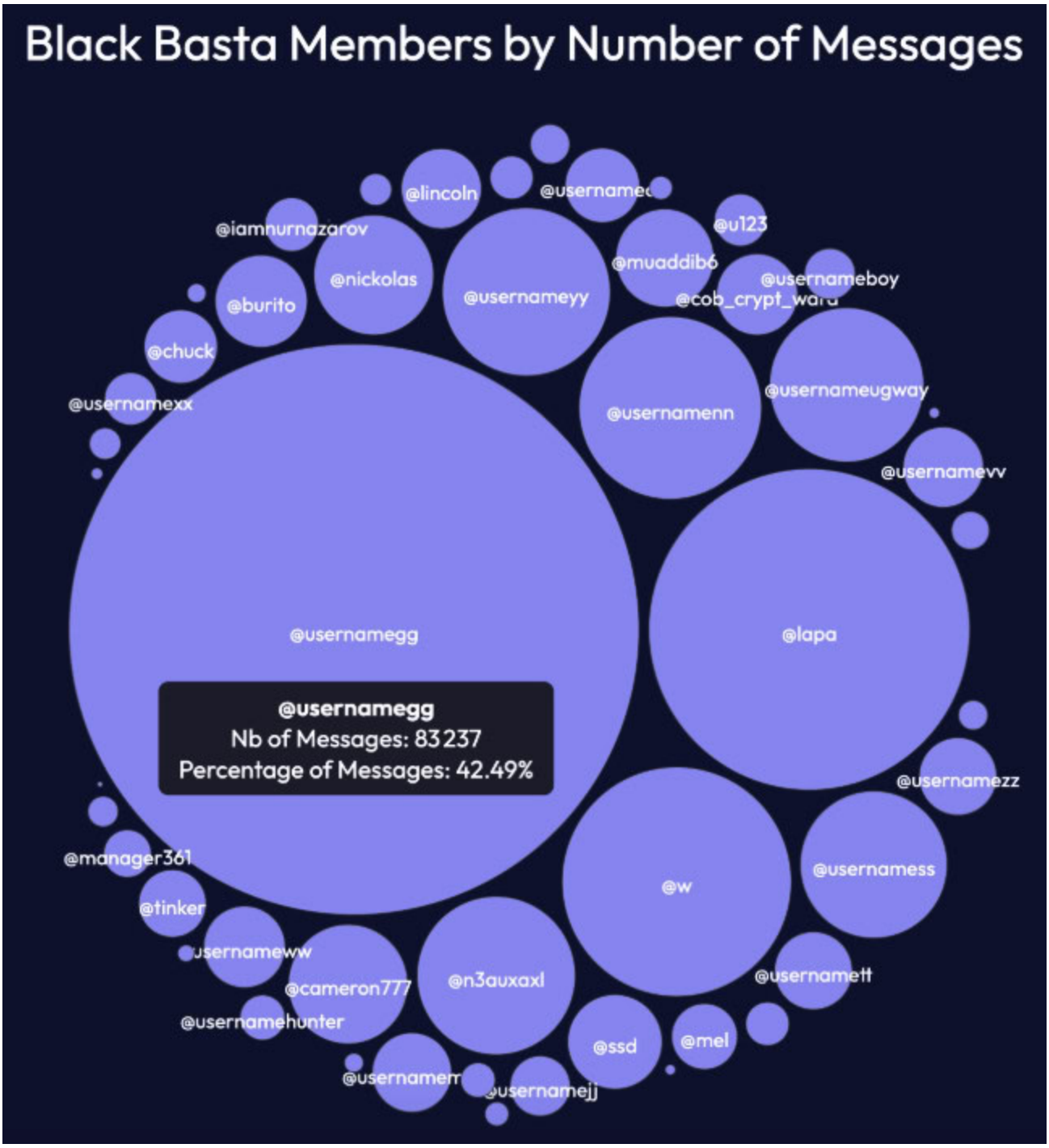

Figure 2: Black Basta members by number of messages (Source: Flare)

The periods of activity and the nature of messages itself indicate that the group had specifically defined and organized vacations periods, like in January or June 2024 when almost all activity stopped.

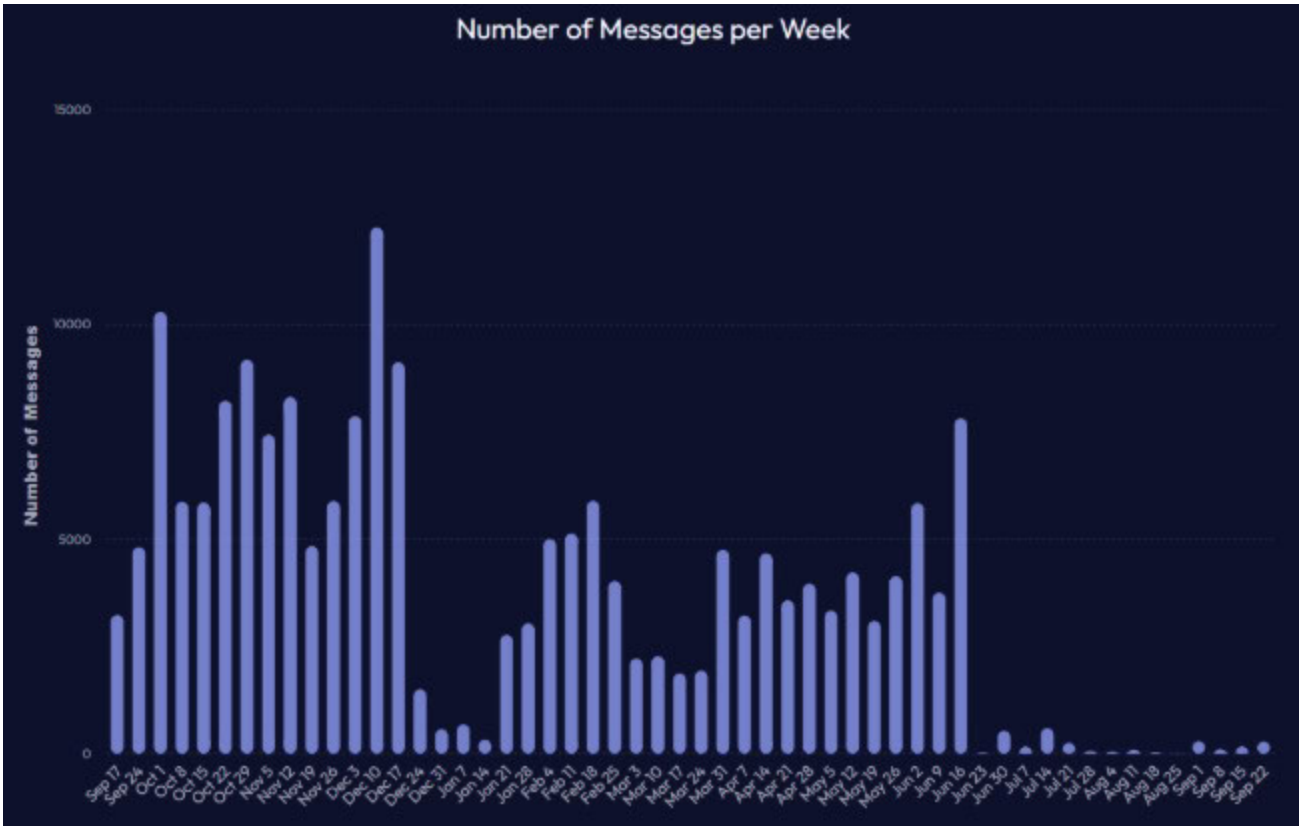

Figure 3: Messages per Week on Black Basta (Source: Flare)

Another notable observation was the distinct structure of the usernames present in the chat. Usernames composed of the word “username” followed by two letters—such as “gg” (aka Tramp), “ww”, “tt”, or “ss”—and hosted on the bestflowers247.online Matrix server appeared to belong to Black Basta’s core members (example: @usernamegg:bestflowers247.online). These threat actors were directly managed by Tramp, who also provided them with their Matrix accounts.

This structure clearly distinguished them from other members of the chat, who used their own Matrix servers, had different username formats, and operated more independently. These independent actors, that can be in fact considered as affiliates, often referred to their own teams and other threat actors who were not part of the chat.

This differentiation is also highlighted in the graph below, where it can be seen that core members remained active for a much longer period than external ones. However, some noticeable discrepancies suggest that the data might be incomplete or that certain core members were simply dismissed in June 2024.

For instance, no disputes or conflicts were recorded for core members such as “ww”, “mm”, “zz”, or “cc”, yet the chat abruptly stopped in June 2024. This indicated the following possibilities: that the dataset is likely incomplete or that these members moved to another communication channel.

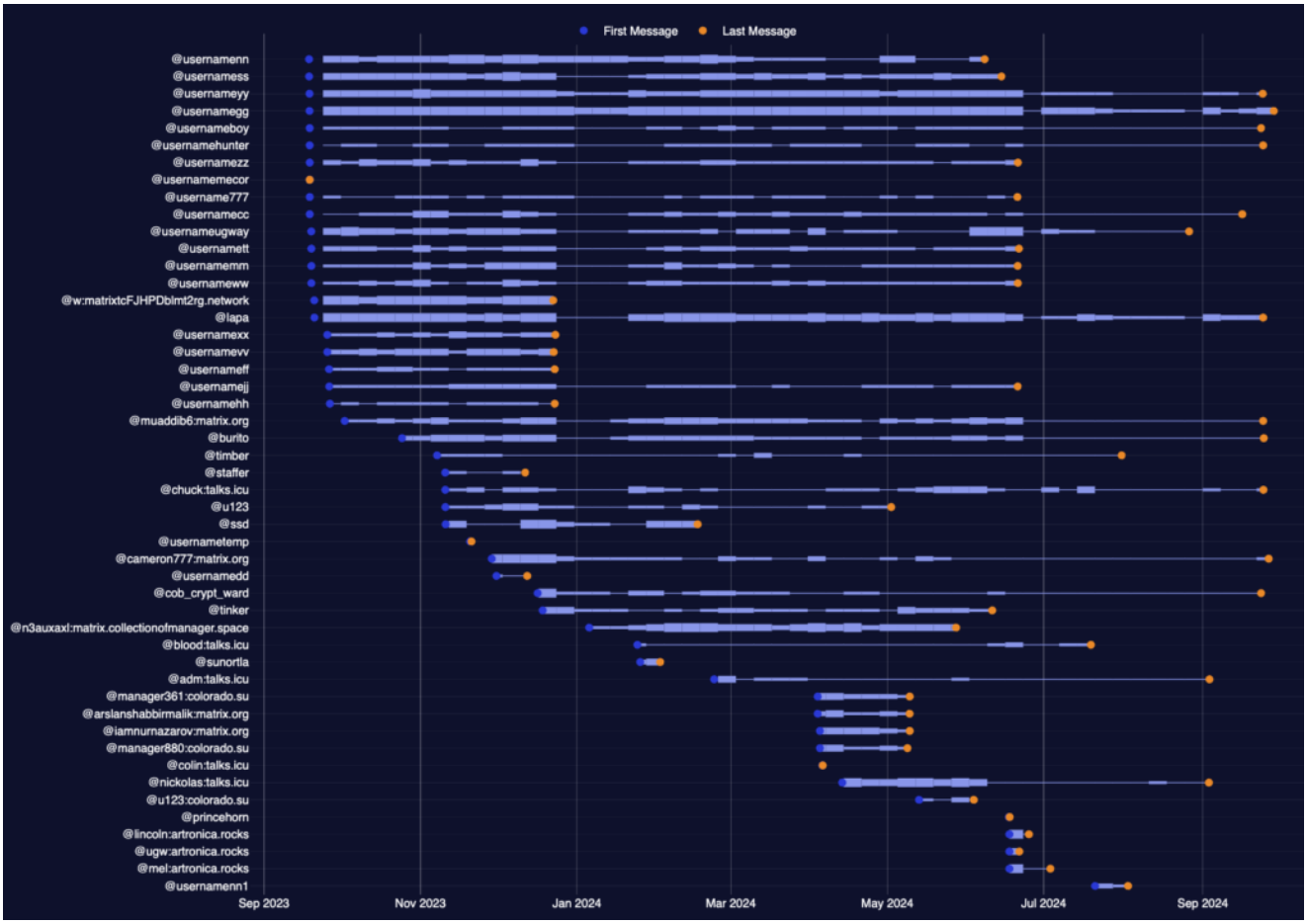

Figure 4. Black Basta members and their first and last messages (Source: Flare)

Analysis of the various exchanges between members in the chat led to deciphering their main roles and specializations within Black Basta. As shown in the graph below—and accessible through the provided link—the group could be divided into the following specialties:

- Leadership and management: Led by gg, also known as Tramp.
- Infrastructure management, servers, and hosting payments: Handled by yy, also known as bio.
- Internal pentesters and support: A group working directly under Tramp’s command from two offices. These members were strictly monitored, often asking for his permission even to step away from their computers for a few minutes. Notable members included nn, ww, zz, and others.

- External affiliates: More independent and experienced, often operating with their own teams. They were particularly active in obtaining initial access and conducting social engineering attacks. For instance, Kortez was frequently mentioned as the leader of another malicious group working alongside blood, adm, nickolas, and u123.
- Coders and programmers: Mostly seasoned malware developers such as n3auxaxl, also known as mekor, and chuk. They were responsible for developing new malware, including the group's Pikabot, which consisted of a downloader/installer, a loader, and a core backdoor component. Black Basta occasionally hired additional coders, though this appeared to be one of the hardest roles to fill.
- Crypting and obfuscation specialists: Primarily a small group of two individuals. One notable figure was muaddib6, also known as Bentley, who may have been the infamous Russian threat actor Vitaly Kovalev.
- Social engineering experts: Specialized in gaining initial access by targeting high-value companies. They used tactics such as impersonating IT support personnel, calling employees, and convincing them to install AnyDesk to deploy malware.
- Brute-force and password de-hashing specialists: At least two threat actors focused specifically on these techniques.

Black Basta's Internal Structure

Figure 5: Black Basta's Internal Structure (Source: Flare)

Black Basta's Infrastructure: Hosted in Germany and Obfuscated

Thanks to this preliminary work, which helped identify the main specialization of each threat actor active in the chat, it became easier to determine where to look for specific information, such as details about the group's infrastructure.

According to the previous paragraphs and Figure 5, the threat actor yy, also known as bio, was responsible for Black Basta's hosting, websites, and penetration testing servers.

As illustrated in Figure 6 below and in the graph available here, the group's most critical servers were likely purchased from VPSKot, a company accepting cryptocurrency payments and reselling servers from legitimate hosting providers unaware of their real customers. One such provider was the German company Hetzner, where Black Basta hosted its Onion websites like the administrative panel, blog, and Element/Matrix chat service in September 2023.

Black Basta's Key Servers in September 2023

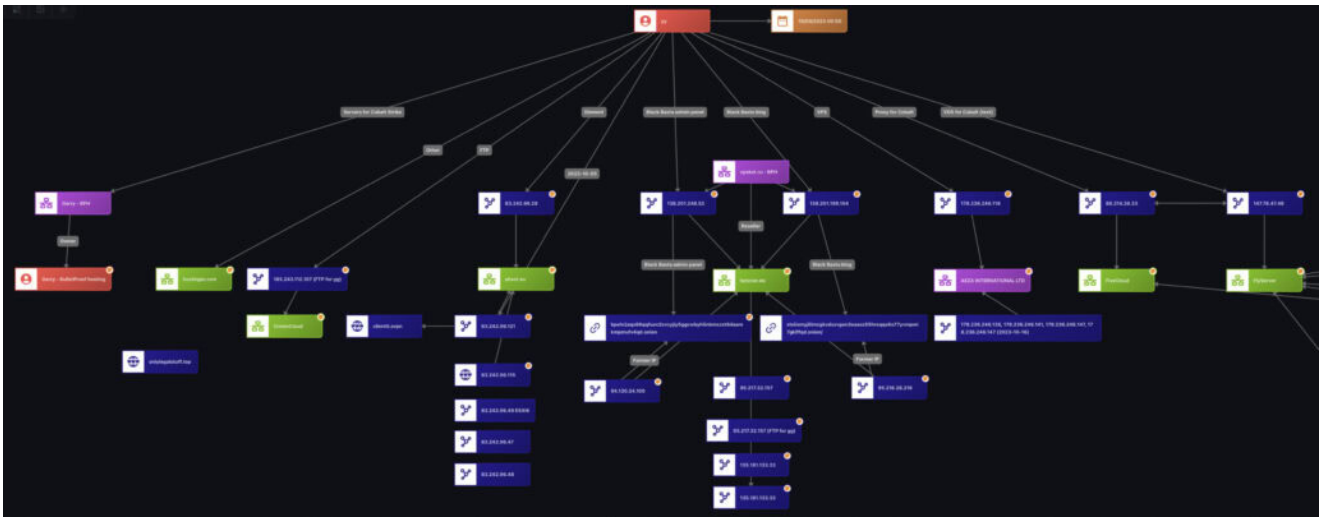

Figure 6: Black Basta's Key Servers (Source: Flare)

The examination of yy's messages from November 2023 also gives an interesting glimpse into how Black Basta deployed Cobalt Strike on servers and obfuscated them behind proxies. Cobalt Strike is a post-exploitation framework commonly used by red teams and cybercriminals to establish command and control, move laterally within networks, and execute malicious payloads.

The group seemingly used bulletproof hosting (BPH) but rather marginally, mainly preferring to acquire many servers from « grey » and offshore hosting companies to rotate their servers and obfuscate their sensitive infrastructure. One BPH that was still mentioned multiple times in the leak, referred to as « the Abkhaz hosting », was a service advertised by the threat actors « gerry », one of the most prominent illicit hosting presently active on Russian-language cybercrime forums.

Black Basta's Cobalt Strike Servers and Proxies in November 2023

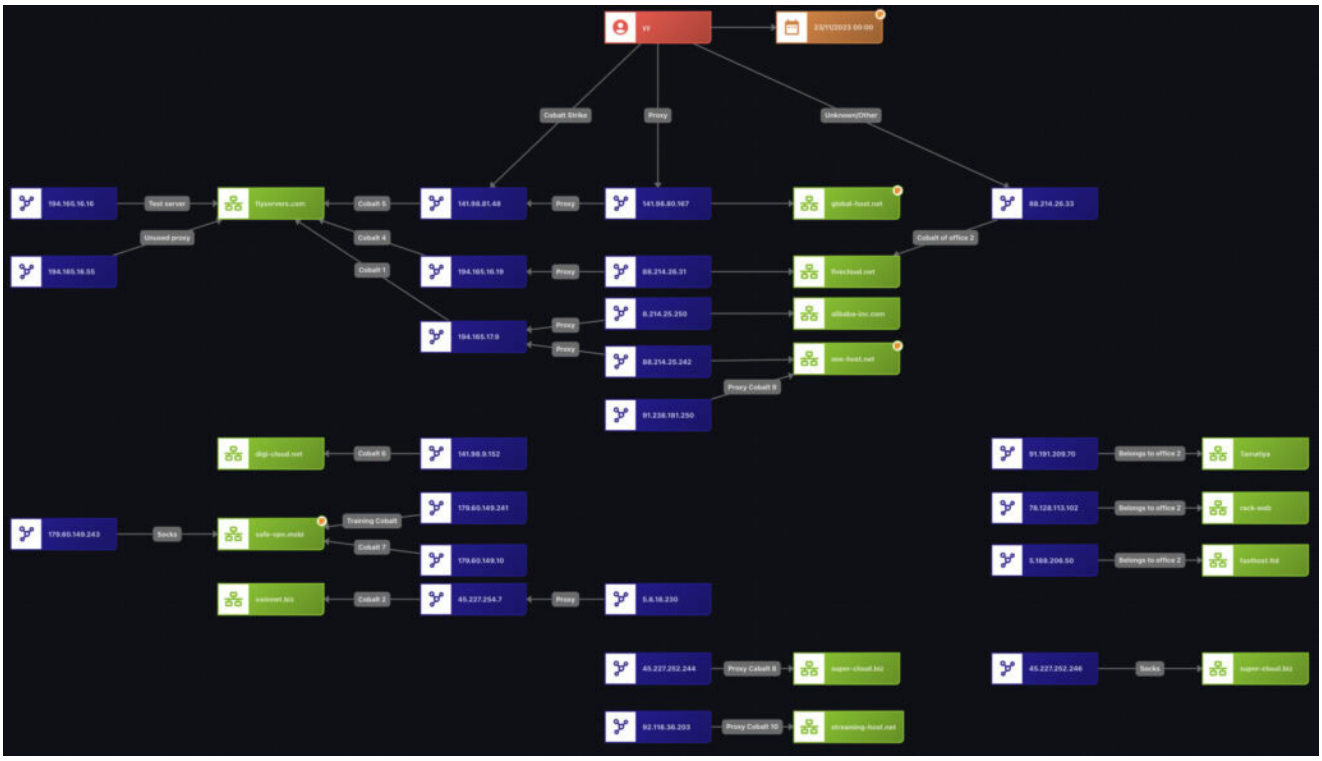

Figure 7: Black Basta's Cobalt Strike servers and proxies (Source: Flare)

Final Thoughts on the Black Basta Leak: A Treasure Trove to Explore

This blog offers just a glimpse into the valuable information that can be extracted and analyzed from this leak. It contains numerous threat actor handles, illicit services from cybercrime forums, contact details, cryptocurrency addresses, and identified vulnerabilities. One particularly interesting investigative approach could be leveraging these indicators to track threat actor accounts across forums, potentially uncovering their real identities. For example, this allowed the identification of several accounts on cybercrime forums of mentioned threat actors by a search in the Flare platform with their TOX IDs.

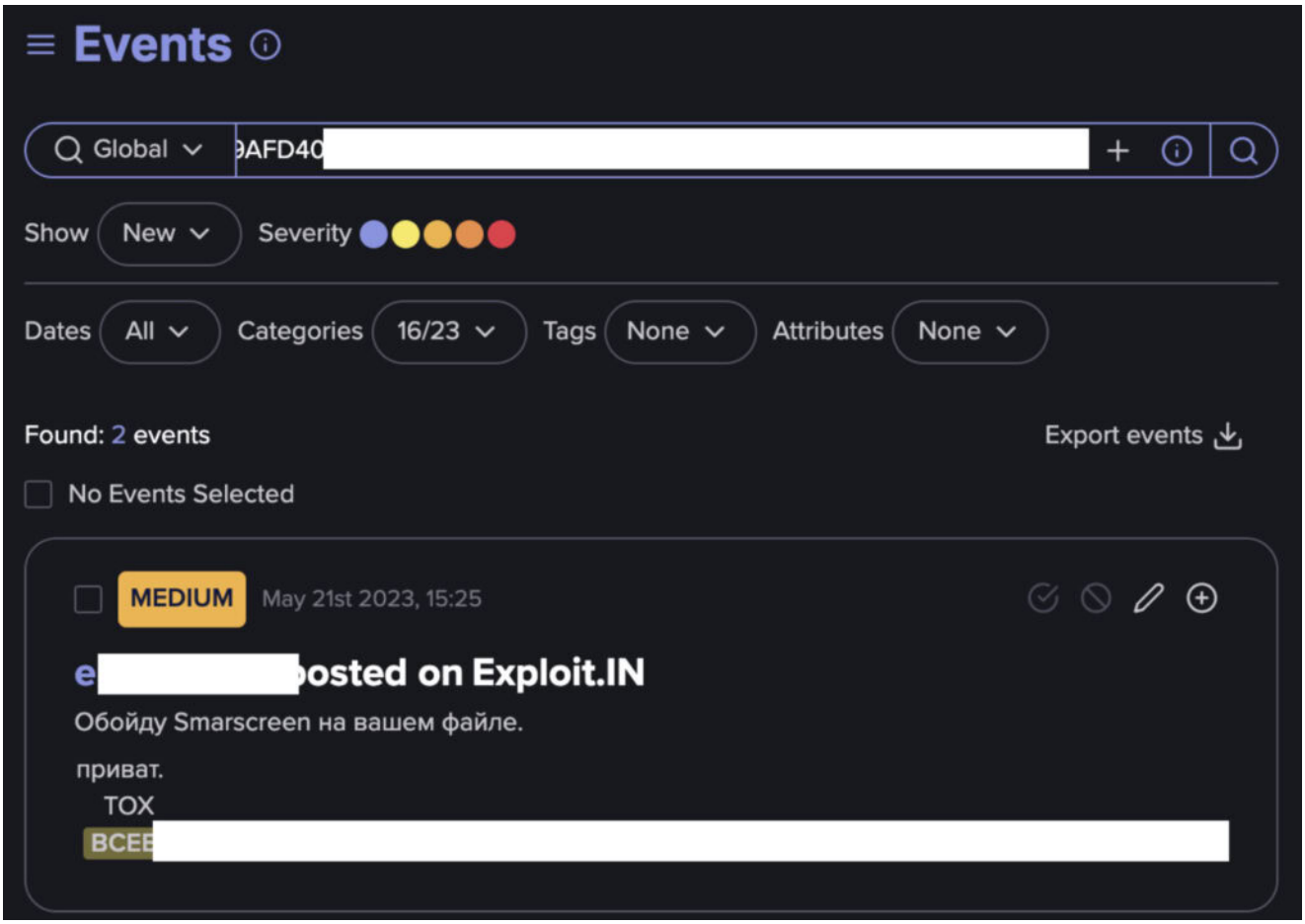

Figure 8: Black Basta threat actors found in Flare (Source: Flare)

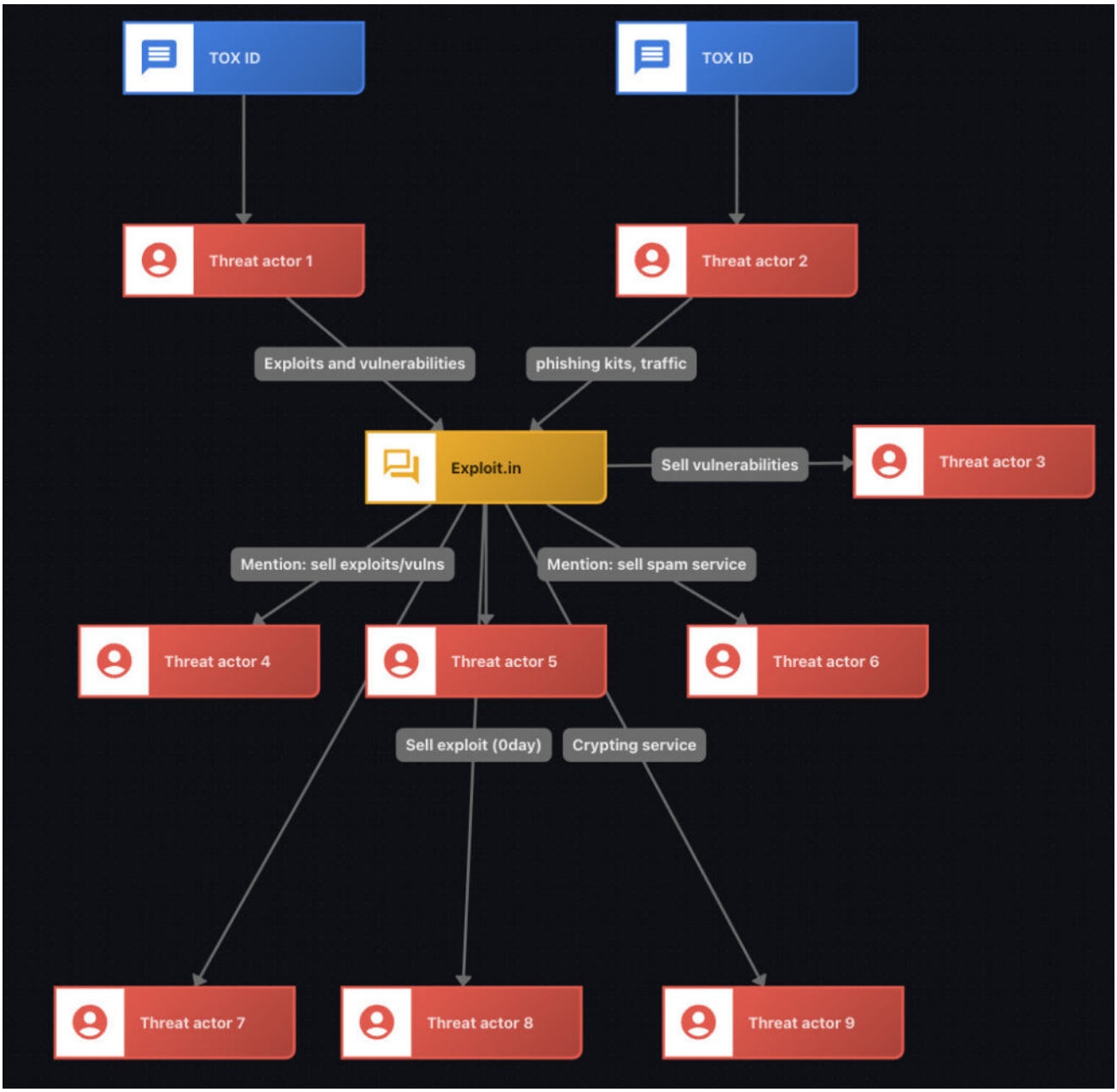

Figure 9. Examples of threat actors selling various services on Exploit that were mentioned in the leak

Dig Further into Cybercrime with Flare Academy

Interested in following more cybercrime research? Check out Flare Academy's training sessions, which are led by cybersecurity researchers. Check out the upcoming sessions here.

We also offer the Flare Academy Discord Community, where you can connect with peers and access training resources from the Flare Academy training.

Can't wait to see you there!

Sources

“Black Basta – Chat Viewer,” February 2025. https://ransomware-leaks.com/.

Garrity, Patrick. “Exposing CVEs from Black Bastas’ Chats.” VulnCheck, February 24, 2025. https://vulncheck.com/blog/black-basta-chats.

Ransomwarelive. “Balck Basta – Ransomware.Live 👀,” March 5, 2025. https://www.ransomware.live.

Rieß-Marchive, Valéry. “Ransomware : de REvil à Black Basta, que sait-on de Tramp ?” LeMagIT, March 1, 2025. https://www.lemagit.fr/actualites/366619807/Ransomware-de-REvil-a-Black-Basta-que-sait-on-de-Tramp.

Townsend, Kevin. “Black Basta Leak Offers Glimpse Into Group’s Inner Workings.” SecurityWeek, March 3, 2025. https://www.securityweek.com/black-basta-leak-offers-glimpse-into-groups-inner-workings/.