Black Basta exposed: A look at a cybercrime data leak

intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak

On Feb. 11, 2025, a mysterious leaker going by the Telegram username **ExploitWhispers** released one year's worth of internal communications between members of the **Black Basta** ransomware group on a Telegram channel. **Black Basta** is still active in a reduced capacity, but in 2022, it was the third most impactful ransomware group. Its members appeared to be experienced Russian-speaking ransomware and cybercrime veterans, some of whom worked with the infamous **Conti**ransomware-as-a-service (RaaS) group. The 197,000 chat messages are drawn from 80 different chatrooms on Matrix servers hosting on six domains. The leak rivals the chat leak that affected **Conti** ransomware gangin late February 2022. **Black Basta's** leak provides similar insight as **Conti's**: **Black Basta** is a polished ransomware group that carefully studied potential victims, ran sophisticated phishing and malware campaigns and employed a range of people for support, including call services, malware development, initial access, crypters and penetration testing. The messages reveal a range of technical data that formed **Black Basta's** operations, including cryptocurrency wallets, domain names, indicators of compromise (IoCs), tools and techniques. But the chats also reveal discord in the group, petty quarrels and tangible worries of getting caught by international law enforcement. One key member of Black Basta contended they had been able to elude law enforcement in mid-2024 with help from influential people, a situation that is explored further in this piece.

This blog post will explore high-level insights drawn from the messages. Intel 471 plans to release a series of reports looking at this gang's tactics, techniques and procedures (TTPs), including phishing, social engineering, vulnerabilities exploited and lateral movement, as well as a look at identified victims, cryptocurrency payment flows and possible real-world identities of threat actors.

Why were the chats released?

@ExploitWhispers is the username for someone who was the administrator of a Telegram chat group called "Шепот Басты" (Eng. Basta Whisper). The informant claimed gang members were "crossing the line," which referred to their alleged attacks on Russian financial institutions, as a reason for the leak. These attacks have yet to be verified.

Who is in the chats?

The chat logs reveal most group members used a consistent format for Matrix aliases, which included a "username" and a two-letter alias such as the "tt" suffix, while some others had custom handles. It is possible core team members, in-house developers and system

administrators used standard handles, and the **Black Basta** group's affiliates and partners used custom handles. However, this is a working hypothesis at the time of this report.

Theexposed internal communications also reveal several actors with managerial roles in the gang's operations. For example, **usernamegg** aka **GG** was a senior manager and team leader. The conversations indicate **usernamegg** coordinated the group's daily operations, hired new members, interacted with affiliates and partners, and supervised budgeting and finance activity. We believe this actor also goes by **tramp**.

Another leading member of the **Black Basta** group, the actor **tinker**, negotiated with victims, managed call centers and supervised other activities. The actor allegedly had the same role in the **Conti** group previously. The actor **tinker** revealed an affiliation with the **BlackSuit** aka **Royal** ransomware group, a spinoff of **Conti's Team 2** subgroup, and admitted to be working as a **Royal** negotiator.

Where is Black Basta based?

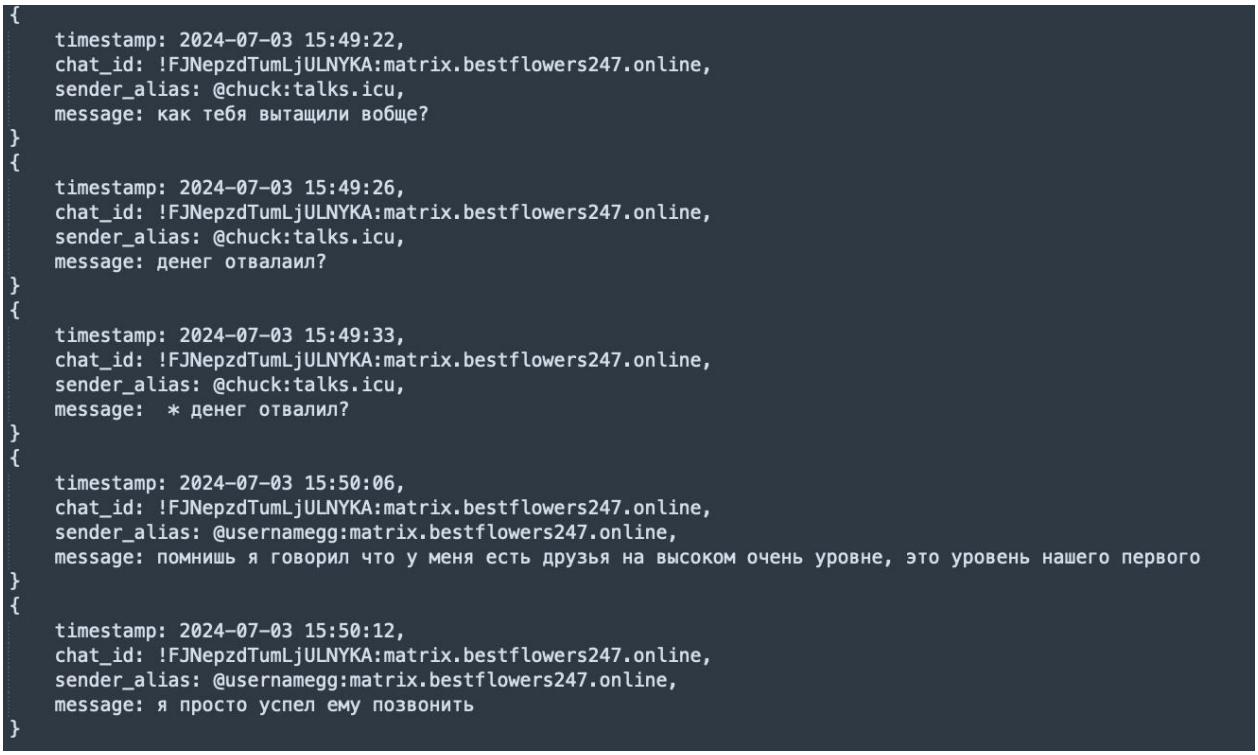
Our preliminary research indicated **usernamegg** rented at least two offices in Moscow, Russia, where developers, malware operators and network intruders were based. The actor also mentioned "an influential ally" who was a high-ranking employee at a large company and provided protection against possible law enforcement action.

Operational security

The gang's key members frequently expressed operational security (OPSEC) concerns, were afraid their infrastructure and systems could be compromised and worried that personal data might be exposed in response to **Black Basta** gang members' attacks oncritical infrastructure.

For example, the actor **w** used a conversation with **usernamegg** to claim the OPSEC measures included using a remote desktop, multiple layers of the onion router (Tor) and virtual private network (VPN) connections and disk encryption.

The chat leak contains no messages from **usernamegg** between June 21, 2024, and July 3, 2024. On that day the actor reappeared, making the comment: "I am here. I'll tell you all about it when you get here." In a private conversation with **chuck, usernamegg** disclosed that they were apprehended once by law enforcement officers, but high-level officials helped **usernamegg** escape:



The image depicts a screenshot of **Black Basta** group members' leaked conversations from July 3, 2024, where the actor **usernamegg** talked about their alleged arrest.

The chat reads:

(translated from Russian):

@chuck:talks.icu, message: how did they get you out?

@chuck:talks.icu, message: did you pay a lot? }

@usernamegg:matrix.bestflowers247.online, message: remember when I said I had friends at a really high level; this is the level of our first

@usernamegg:matrix.bestflowers247.online, message: I've just managed to call him.

usernamegg's absence in the chats overlaps with a report in an Armenian news outlet of a man who was arrested and purportedly wanted by the U.S. On June 24, 2024, an Armenian news outlet,168.am, reported that a 34-year-old identified as Oleg N. had been arrested on June 21, 2024, related to charges filed in the U.S. state of Washington.

This arrest surfaced again in the same news outlet on Sept. 20, 2024. The story identifies the man as **Oleg Nefedov** and claims he was wanted by the U.S. on an Interpol notice but was no longer in custody. The story claims after Nefedov's arrest, a judge found the prosecutor did not present a translation of the Interpol notice to **Nefedov**. The prosecutor argued it was not required. The article says **Nefedov** was released within 72 hours of his arrest, which appears to be the period in which a court must make a decision on whether to continue to detain someone, and that **Nefedov's** "whereabouts are unknown."

The story continued to evolve. On Sept. 30, 2024, 168.am reported that disciplinary action was being considered against the judge in Nefedov's case, Artush Gabrielyan, for allegedly waiting too long to hold **Nefedov**'s detection hearing. **Nefedov**, the story contends, is a Russian man wanted by the U.S. in connection with fraud "worth several billion." After the detention period expired at 4 PM on June 24, 2024, Nefedov's attorney petitioned for the hearing to be adjourned for 15 minutes, and Nefedov left the court, the publication reported. On Oct. 10, 2024, the Armenian publication CivilNet published a story contending that disciplinary action had been undertaken against Gabrielyan.

The **Oleg Nefedov** persona ties together with claims in the **Black Basta** chats made by the leaker, **ExploitWhispers**. **ExploitWhispers** suggested the actor **Bio** had identified the actor **GG** aka **usernamegg** as **tramp** and speculated **AA**, **GG** and **tramp** might be aliases for the same individual who possibly used the **Oleg Nefedov** persona.

Intel 471 continues to investigate the news stories and the claims around the **Oleg Nefedov** and **usernamegg** personas. Chat leaks can illuminate much about a group, but also can present ambiguous information that can be difficult to verify.

Who helped usernamegg?

The identity of the person **@usernamegg** refers to as "level of our first" and "him" in Figure 1 is unclear but suggests someone in a position of influence and authority. In the chats, **@usernamegg** claims the person runs "big corporations" and could provide trouble-free passage through immigration thanks to another high official — referred to as the "number one" — who was aware of **@usernamegg's** predicament."

This type of connection with the state would not be unheard of for a high-ranking cybercrime player. Russia's intelligence services and the cybercriminal underground have long maintained relationships, with the former leaning on the latter for operational support under a quid pro quo arrangement: Underground actors can continue their activity without repercussions as long as they cooperate with the state. The foundation for these relationships is institutionalized corruption, where the state — which has the power to conduct raids, audits and other forms of harassment — can coerce cybercriminal actors into paying protection money, participating in state-directed cyber operations such as espionage or data theft and supporting state narratives through hacktivist or misinformation campaigns. These relationships have been described in public documents, such as the FSB tasking of cybercriminal actors to breach Yahoo email accounts in 2014; in U.S. sanctions levied against the Trickbot actors, who were related to **Conti**; and the use of the GameOver Zeus botnet to search for sensitive data on Ukrainian computers.

Other potentially identifying information emerged in the chats. Both **chuck**, who apparently developed and operatedQbotakaQakbotmalware, and **usernamegg** allegedly purchased property in Dubai, United Arab Emirates (UAE). The actor **chuck** also claimed in messages

around July 2024 to have communicated with criminal defense attorney Arkady Bukh about the legal risks of residing in the UAE. The actor **chuck** subsequently expressed the view that the risks of being arrested as a result of an Interpol notice were low.

Conclusion

The **Black Basta** gang attacked at least 165 organizations in 2022 but is off to a slower start this year — Intel 471 has recorded only eight victims so far. The chat messages broadly reveal discord within the group, suggesting this could be a reason for the low number of successful attacks. Chat leaks contributed to the decline of the **Conti** ransomware group, as the security lapse that led to it drove waning confidence among affiliates. Nonetheless, these threat actors are veteran ransomware attackers, and it is likely that if **Black Basta** completely dissolves, group members will re-integrate themselves into other ransomware operations, which makes this intelligence valuable. Intel 471 will continue to analyze the messages.