“This Forum is a Bunch of Communists and They Set Me Up”, LockBit Spills the Tea Regarding Their Recent Ban on Russian-Speaking Forums

By Anastasia Sentsova

Published: 2024-02-08 · Archived: 2026-04-06 00:34:16 UTC

Contributor: Jon DiMaggio.

What Happened?

On January 30, 2024, LockBitSupp, a member of the infamous LockBit ransomware group, faced a ban from two prominent Russian-speaking forums: XSS and Exploit. These forums hold a significant position in the Russian-speaking underground community, being among the oldest forums in existence. The forums are well-structured, with various sections catering to the diverse interests of illicit activity amongst its users. Arbitration is one of the sections available to members, allowing them to file complaints against each other, with forum admins making decisions based on the situation presented.

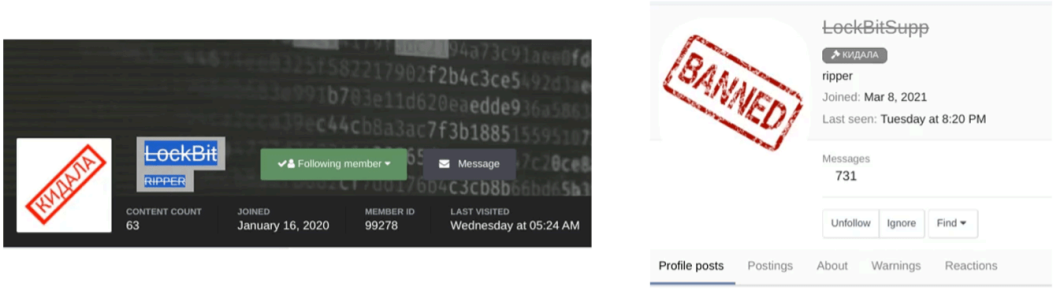

Figure 1: LockBit banned on Exploit and XSS and assigned with the status of “Ripper” (Rus: Кидала)
Source: Analyst1

Getting banned from these forums typically involves a serious violation, and LockBit’s ban was prompted by a complaint from another forum member under the alias “michon.” According to michon, they had collaborated with LockBit, providing access to a target entity. However, LockBit allegedly extorted the target without sharing any of the profit, leading to the complaint and subsequent ban.

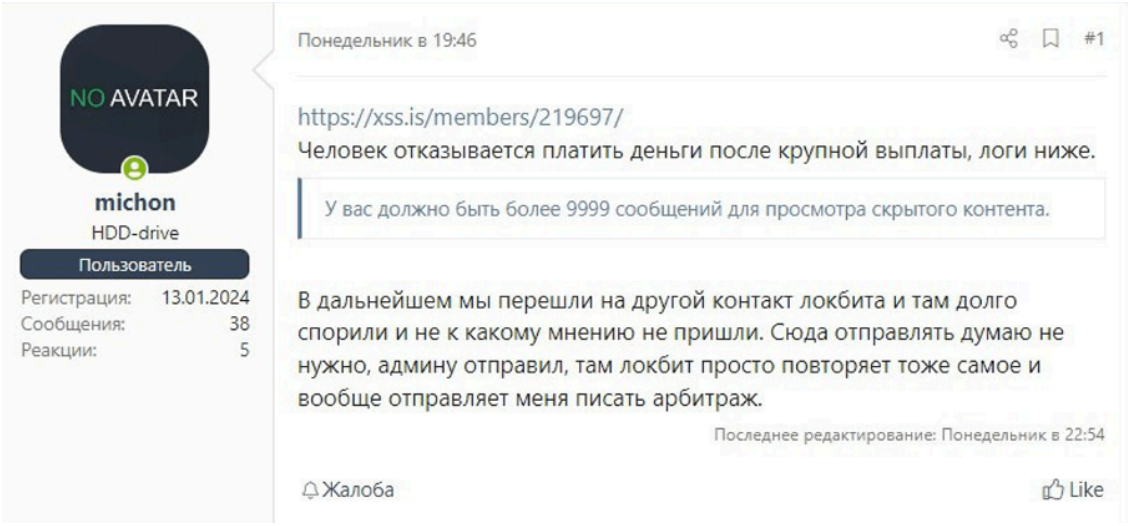

Figure 2: Forum member michon stated that LockBit refused to share a profit after its payout.
Source: Analyst1

LockBit responded with their perspective on the situation, asserting that michon initiated contact with them and provided access to a breached company without any formal agreement. LockBit successfully extorted the payment, and later michon requested a percentage of the payout in the amount of 4 million USD, which LockBitSupp refused to pay. Following the dispute, both parties initially agreed to handle it privately, but michon opted to make it public.

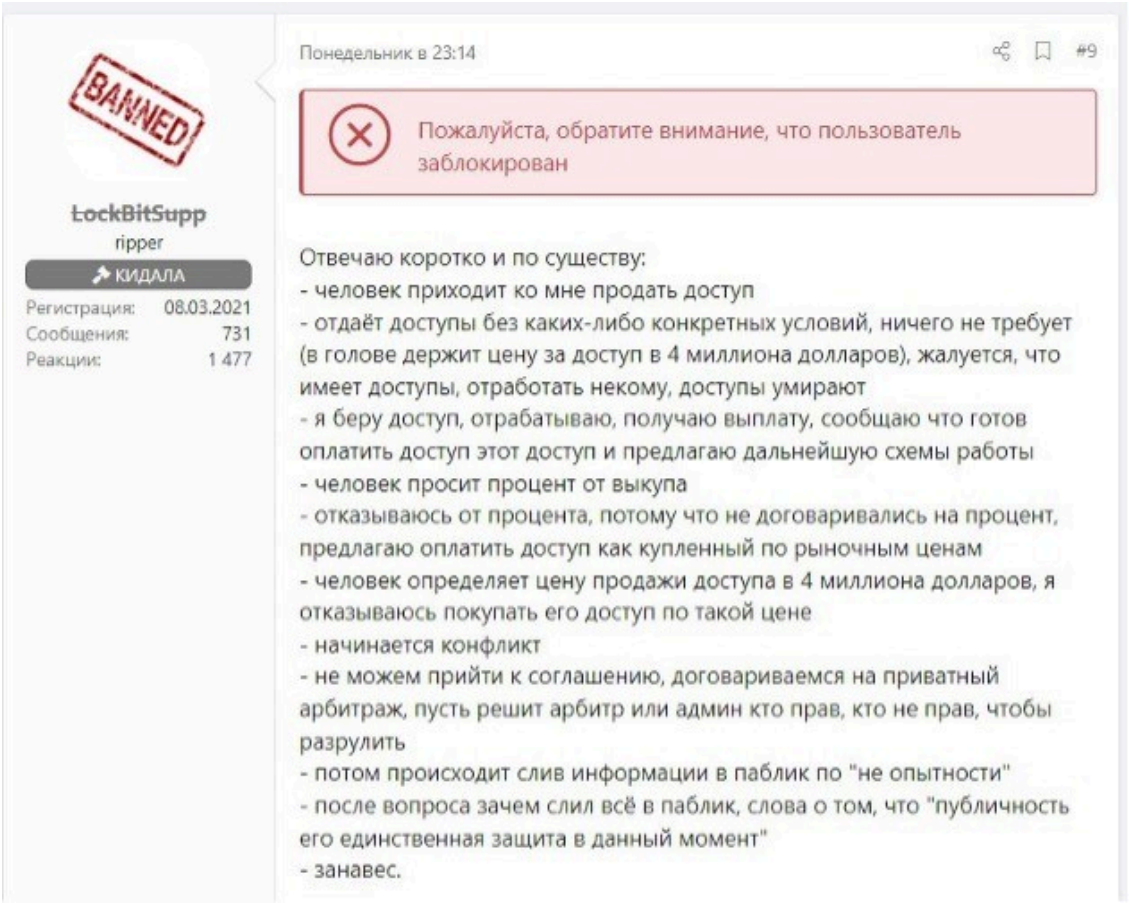

Figure 3: LockBit provides their side of the story by sharing a message on XSS
Source: Analyst1

After the complaint was addressed publicly, an administrator requested that LockBitSupp share 10% of the obtained profit, LockBitSupp declined, leading to their ban. The forum admin stated, ***"Unfortunately, the defendant refused – status assigned. Case closed."***.

In addition, the admin of XSS once again emphasized the ban on the ransomware topic when explaining the rationale behind LockBit's ban. They stated, ***"It's disheartening to witness such arbitrage, especially in light of the real and not imaginary ban on ransomware discussions. I would like to remind everyone of rule number 9: Ransomware is strictly prohibited"*** referring to the ban of the ransomware topic established back in May 2021.

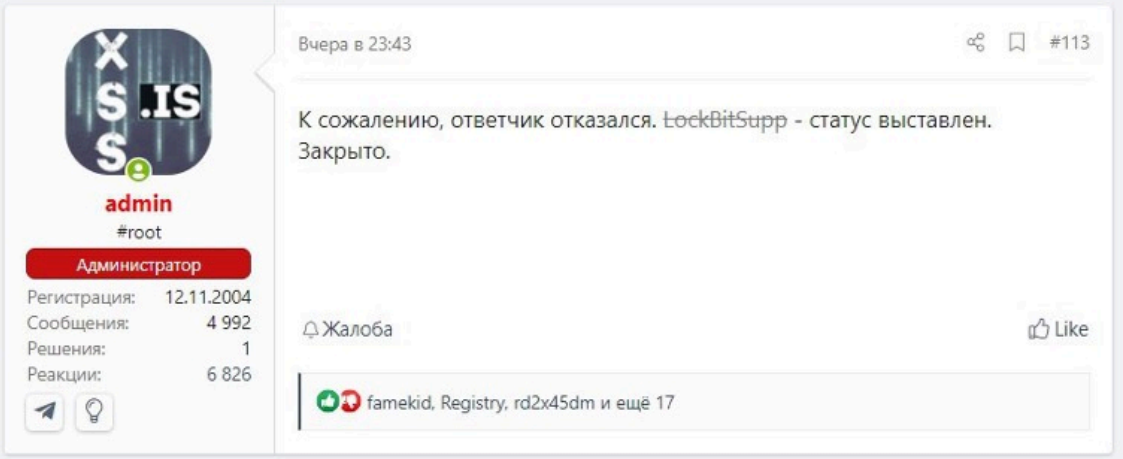

Figure 4: Admin's message on XSS banning LockBitSupp and assigning them with the status "Ripper"
Source: Analyst1

LockBitSupp was banned from XSS and later from Exploit, with the status "Ripper" (Rus: Кидала) assigned. Beyond the ban itself, this status is arguably the most detrimental for a forum member. It signifies a lack of trust, making it strongly discouraged for anyone to engage in collaboration with them. To protect their reputation and prove themselves not guilty, LockBitSupp took this to another DarkWeb forum RAMP to appeal this ban.

Not Guilty Until Proven Otherwise

RAMP is a Russian-speaking DarkWeb forum fully dedicated to ransomware activity. LockBit was one of the first ransomware operations to promote its affiliate program back in 2021 when RAMP was launched after an official ban of the ransomware topic on XSS forum. It was later revealed that the creator of RAMP is the infamous BorisElcin, also known as Wazawaka, who was later identified as Mikhail Matveev.

In May 2023, Mikhail Matveev faced sanctions from the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) due to his suspected involvement in multiple ransomware attacks conducted by Hive, LockBit, and Babuk ransomware syndicates. Matveev, operating on RAMP initially under the aliases TetyaSluha and later Orange, eventually relinquished his admin rights.

It is unclear if Matveev is currently involved in any of RAMP operations. The current admin is an actor operating under the moniker Stallman, a very well known and respected member of the Russian-speaking DarkWeb community.

On Thursday, February 1st, 2024, LockBitSupp leveraged the RAMP forum to tell its side of the story surrounding the events that led to the ban on other Russian underground forums. You can see the post in Figure 5 below.

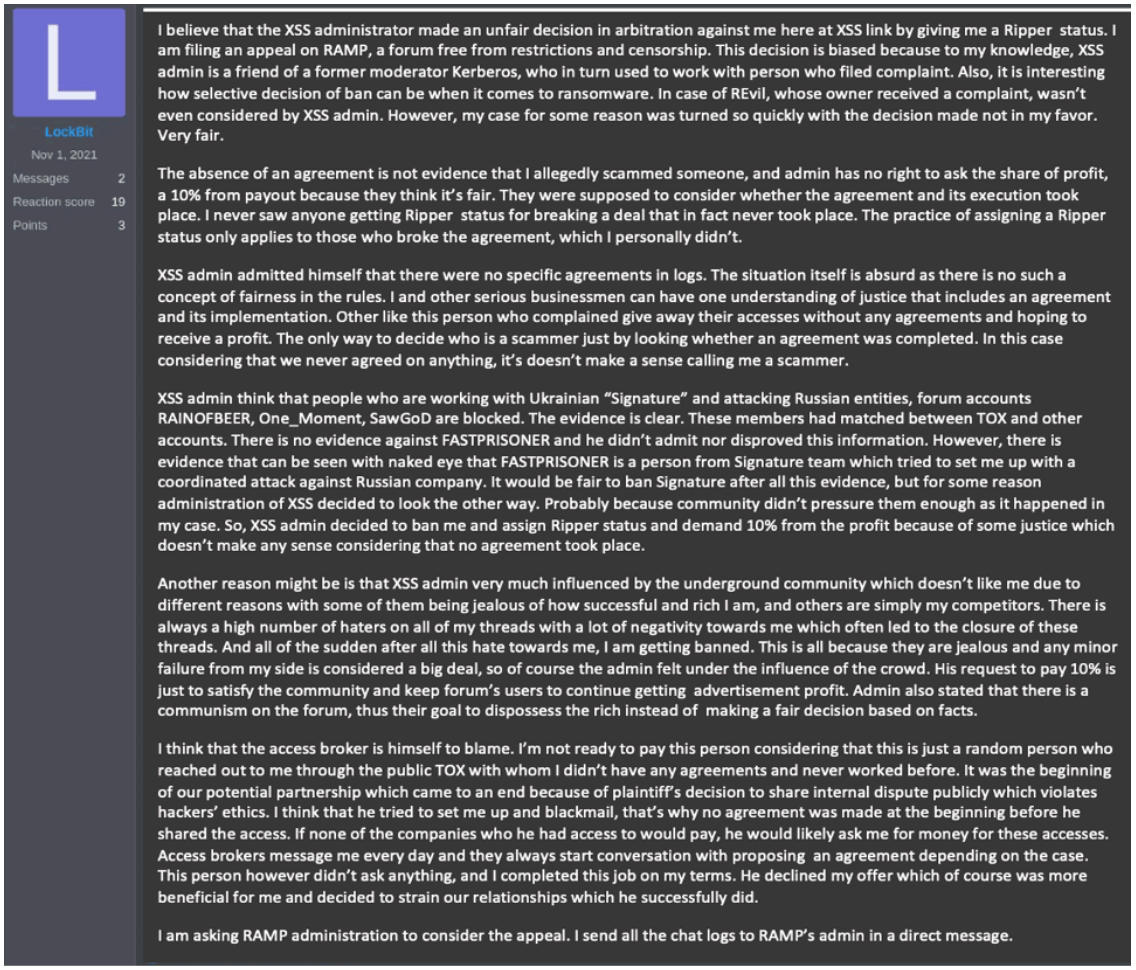

Figure 5: LockBit appeal on RAMP. Translated by Analyst1
Source: Analyst1

LockBitSupp made a post on the RAMP forum, asking the forum administrator, Stallman, to re-evaluate the incident and make an independent determination regarding whether LockBit cheated michon out of the money it was owed for its services. In the post, LockBitSupp claims that the administrator who ruled against it and enforced the ban had ulterior motives influencing their decision. According to LockBitSupp, the ruling XSS admin is the friend of a former XSS moderator and the plaintiff, who also had a previous conflict with LockBitSupp. LockBitSupp believes that this relationship affected the admin's ability to adjudicate the complaint fairly.

While Analyst1 cannot confirm the relationship between the former XSS moderator and the administrator, it appears plausible based on the infrequent enforcement of the rule against ransomware discussions on XSS. The forum is full of conversations about ransomware, yet enforcement is rare and selective. Furthermore, LockBitSupp has frequently engaged in ransomware discussions since joining the forum in March 2021 without facing consequences from XSS moderators until the complaint was filed.

Typically, the XSS admins require complainants to provide evidence of a valid agreement for unpaid services in order to find someone guilty in such situations. However, based on the logs submitted by LockBitSupp, no such agreement was made. In other words, the logs showed that the parties discussed a payment but never agreed upon

the terms or amount, yet the complainant still provided access. The XSS admin confirmed that no prearranged payment agreement existed, yet still ruled in favor of the complainant.

While it's uncommon for us to agree with a threat actor, if we disregard the illegal services and criminal acts that the parties are disputing over and focus on the ruling based on the presented evidence in the arbitration, it seems unfair to hold a party accountable for a monetary amount that was not agreed upon in advance by both parties. Analyst1 had a conversation with LockBitSupp, discussing the events that occurred and the ruling made by the XSS administrators. We questioned LockBitSupp about why they didn't agree to payment terms beforehand to avoid this situation completely.

LockBitSupp explained that the complainant lacked experience, credibility, and reputation, which made it difficult to agree to upfront payment without knowing what they would receive in return. LockBitSupp also mentioned that they often encounter criminals who make empty promises in an attempt to scam the group, and they only make payment after a successful criminal operation where the involved criminals have fulfilled their part of the agreement. Analyst1 can confirm this statement, as it aligns with the terms outlined in the group's affiliate rules listed on their data leak site.

We asked LockBitSupp if this was true, why did it not pay the complainant after the criminal engagement was completed. LockBitSupp stated the complainant became confrontational and impatient and publicly leaked private information about the operation on the forum, which is an offense within the criminal community.

We also asked LockBitSupp why it was banned by the Exploit forum if the complaint was filed on the XSS forum. LockBitSupp explained that ***"This is the rule in the Russian-speaking community and across the forums. If you are getting banned from one forum, you are automatically excluded from others."*** This also explains why LockBitSupp was upset about the ruling. Getting banned across multiple Russian-speaking forums limits the group's exposure to other criminals and resources. LockBit also believes that the moderator's decision, which required it to pay 10% of the criminal revenue generated from the operation in which the complainant provided initial access, was biased and unfair. LockBit says it never agreed to such a large sum and refuses to be blackmailed into making such a payment. Again, we don't often agree with LockBitSupp, but if the logs provided are authentic and inclusive, the logs provided support this claim.

As you may recall, LockBitSupp stood by their decision and refused to make payment, resulting in their expulsion from both the Exploit and XSS forums. However, when LockBitSupp appealed to the RAMP forum administrator, it hoped for a more favorable outcome – which is exactly what it received. On Sunday, February 4th, 2024, Stallman, the RAMP administrator, determined that LockBitSupp did not violate the terms of the agreement. This decision was based on the conversation logs submitted as evidence, which revealed that no prior agreement or promise of payment had been made.

The administrator cited statements from the conversation logs as justification for their decision:

LockBitSupp: *I don't have to pay you just for access. I only going to pay you if the victim pays a ransom. What is not fair? Where do you see injustice?*

michon: *At the moment I want 4 million USD for access.*

LockBitSupp: *Well, I'm not ready to pay you that much for access and no one would ever buy any access for that kind of money.*

However, despite the positive ruling made by the RAMP administrator, XSS and Exploit forums have not lifted the ban. This means that LockBitSupp may have won the appeal but will not benefit from it. Such a discrepancy in verdicts between forums is surprising, considering how interconnected the Russian-speaking underground is.

Making Sense Out of DarkWeb Rambling

DarkWeb forums serve as valuable sources of intelligence, but unlocking their insights requires a thorough understanding of an underground ecosystem. It involves delving into the historical events that have shaped the underground over the years as well as examining the profiles of actors, considering their cultural backgrounds that often influence their behavior.

Drawing parallels between the dynamics of DarkWeb forums and the broader Russian-speaking society, we uncover striking similarities. Both environments are collectivist in nature, placing a strong emphasis on community importance, adherence to established guidelines, and the exchange of shared experiences. This fosters a cohesive environment where individuals feel a sense of belonging and camaraderie.

While the story presented to both the underground world and the wider public may appear straightforward, several details about the LockBit ban raise questions. For instance, the lack of forum reputation of the individual behind the complaint, who registered their account as recently as January 12, 2024. In an underground where hierarchy plays a central role in forming relationships, this seems contradictory. LockBitSupp themselves point to this by saying, ***"This is a random person with no established reputation"***.

The hierarchical structure within DarkWeb forums mirrors the organizational structure seen in various aspects of Russian society, reflecting a preference for a clear and defined chain of command. Moreover, the unwritten code of conduct, respect for authority, a strong sense of camaraderie are foundational principles that shape underground. With the forum's reputation and assigned ranks, underground members navigate their way through the hierarchy, striving to climb the ladder. Until they reach the upper echelons, they treat those already at the top with respect.

The incident involving LockBit's ban sheds light on another important aspect of the Russian-speaking underground: the significance of interpersonal relationships. Trust, collaboration, and deal-making often hinge on these relationships, which are established based on mutual interests and common goals. LockBit's mention of a close relationship between the admin who made the decision and former moderator of XSS, who is a friend of the plaintiff, underscores the interconnected and relationship-based nature of this world.

The publicity of the event, with a public complaint lodged against a notorious actor from one of the most active ransomware groups, is a rare occurrence in the underground. Violating hacker ethics by sharing internal disputes publicly is frowned upon, as highlighted by LockBit's statement: "***He shared an internal dispute that shouldn't have been become public, violating hacker's ethics"***. Indeed, in the world of the underground that relies on principles of secrecy, sensitive discussions are typically kept behind closed doors also to avoid attracting unwanted attention from law enforcement.

This publicity, however, could be seen as an attempt of rivalry from LockBit's competitors. The public execution, ban, and assigning of "Ripper" status could be interpreted as attempts to discredit LockBit and undermine its business. Much like in the offline world, reputation is paramount in the DarkWeb, and individuals seek to build and maintain positive relationships with trusted peers.

The LockBit ban might also be seen as a pushback from the community itself. It's possible that some members perceive LockBit as separating themselves by prioritizing their own interests over those of the community, and showing their success too openly. The LockBit statement "***They are jealous of me because how rich and successful I am"***, "***There is a communism on this forum and their goal is to dispossess the rich***" may sound amusing, but they likely hold some truth and offer insight into what happened to LockBit.

"When you start all this talk about the Cartel, you have to understand that you are not alone here. You must consider other people's opinions", said Bratva, another prominent member of the Russian-speaking DarkWeb community. Indeed, in a community where collective interests often supersede individual ones, separating and placing oneself on a pedestal could be a fatal mistake.

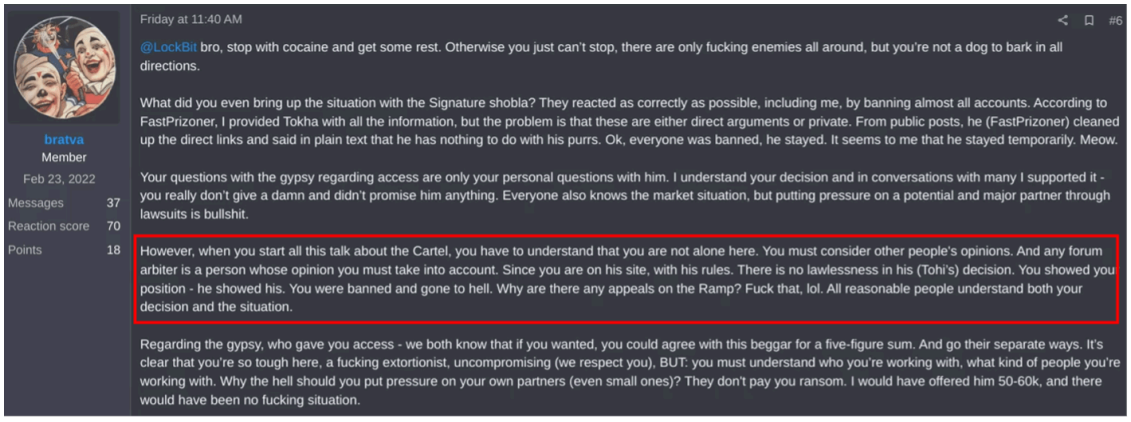

Figure 6: Bratva comments on LockBit's appeal on RAMP by referring to his resistance to obey the community rules
Source: Analyst1

The Russian-speaking underground presents a complex and intricate landscape shaped by multiple factors, including cultural norms, interpersonal relationships, and even the political landscape. Understanding these nuances is crucial for cybersecurity experts and law enforcement agencies in addressing cybercrime. Analyst1 continues to navigate the evolving ecosystem of ransomware for combating emerging threats and building a safer digital space.

About Analyst1

Threat intelligence teams often struggle to bridge the gap from insight to action. Analyst1 is the Orchestrated Threat Intelligence Platform designed to resolve this issue. It automatically organizes threat data, links it to your assets and vulnerabilities, and customizes views for different roles. Analyst1's orchestration layer streamlines workflows and automates reliable actions by integrating with SIEM, ticketing, and vulnerability management systems. From Fortune 500 financial institutions to national security agencies, enterprises trust Analyst1 to unify their defenses, significantly reducing their response time from days to minutes.
