LockBit Takedown & Operation Cronos: A Long-Awaited PsyOps Against Ransomware | Analyst1

By Anastasia Sentsova

Published: 2024-02-29 · Archived: 2026-04-05 18:43:34 UTC

Contributor: Jon DiMaggio.

Operation Cronos

His name was Cronos, the youngest leader of the first generation of Titans. He overthrew his father and ruled during the mythological Golden Age until he was overthrown by his son, Zeus, and imprisoned in Tartarus. Tartarus is the place in the underworld where souls are judged after death and the wicked receive divine punishment.

This is the Greek mythological story about Cronos, the name of which was likely chosen for the most epic operation against ransomware known to this day. On **February 20, 2024**, the taskforce **"Operation Cronos,"** comprising of NCA, FBI, Europol, and others, including the public sector, announced the takedown of one of the most prolific ransomware groups, LockBit. According to the Europol statement, the months-long operation has resulted in the compromise of LockBit's data leak site and other critical infrastructure that enabled their criminal enterprise. This included the takedown of 34 servers in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States and the United Kingdom.

We've seen various actions taken against ransomware in the past, including arrests, seizures, sanctions, and other measures. However, the approach chosen by law enforcement for this LockBit takedown is notably different. It seems that a new strategy was employed this time, involving PsyOps (Psychological Operations). In our blog, we will summarize the takedown events, discuss LockBit's comeback and actors' response, and analyze details of this operation that represent an effective strategy for combating ransomware this time and moving forward.

On **February 19, 2024**, the LockBit data leak site used for the double-extortion technique displayed a seizure banner. The message left by law enforcement stated, ***"We can confirm that LockBit's services have been disrupted. Return here for more information at 11.30 GMT on Tuesday 20th Feb."*** The following day, LockBit's data leak site appeared as usual with the same interface but with one slight adjustment. Instead of the usual list of cards displaying claimed victims, placeholders for victims contained a series of announcements about actions taken and details uncovering LockBit's operations. With some of the information published by law enforcement on **February 20, 2024**, the rest was scheduled to be shared during the next four days. Ironically and of course, intentionally mirroring the countdown approach used by actors when threatening to leak their victims' data.

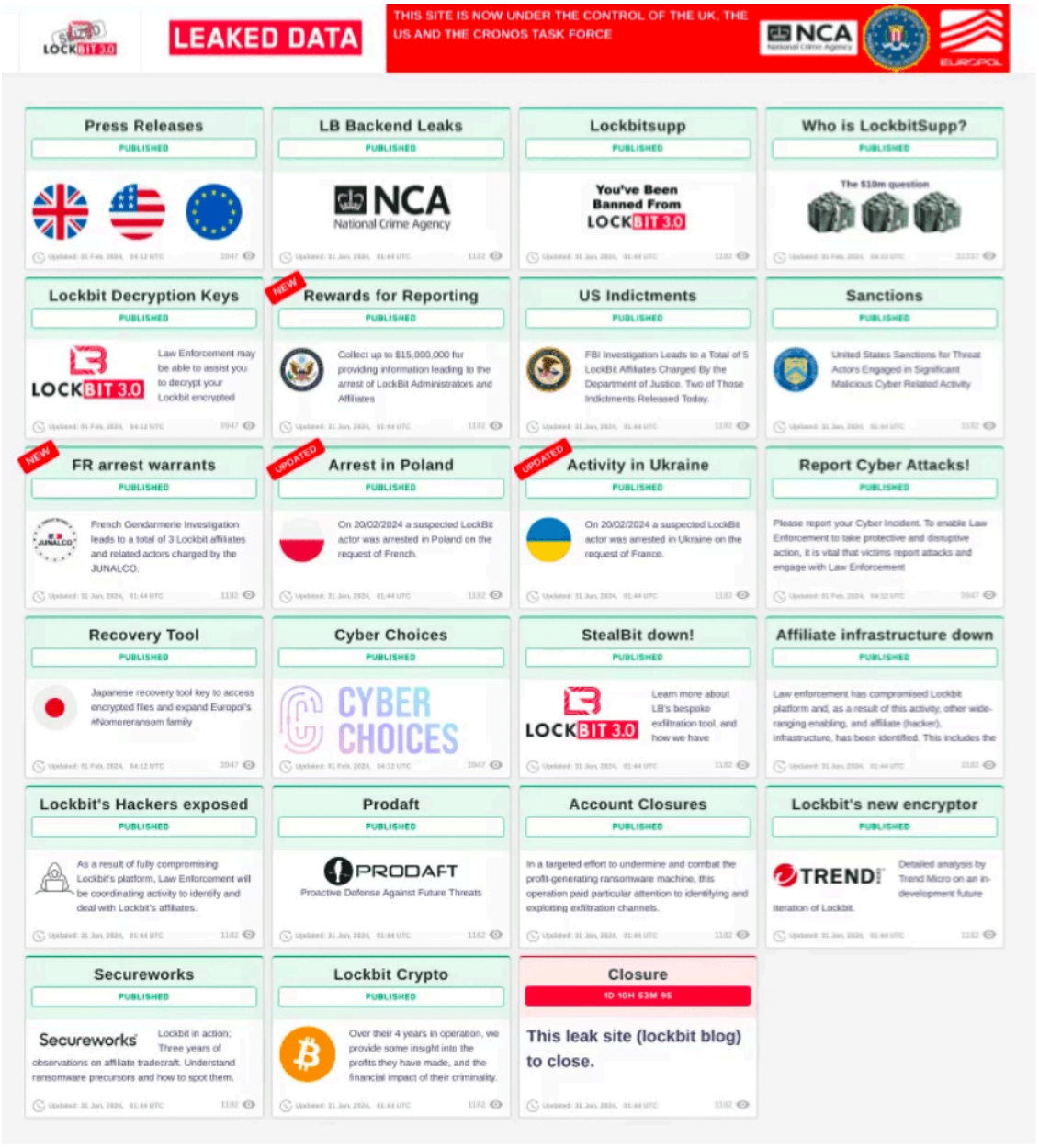

Figure 1: LockBit data leak site displays a seizure banner
Source: Analyst1

Overall data shared with the public included press releases, screenshots of the LockBit backend infrastructure, internal chats, information relating to decryption keys law enforcement acquired, arrest announcements of suspects in Poland and Ukraine, details of operations such as the takedown of the StealBit exfiltration tool used during attacks and analysis of blockchain activity related to ransom payment proceeds. Reports by the cyber security companies Trend Micro and Prodaft who assisted in the investigation, were also provided.

More significantly, law enforcement teased they planned to release the real-world identity of the person behind the LockBitSupp persona, who is a key member of the LockBit syndicate. According to law enforcement's post on the seized webpage, seen below, they planned to release the information on **February 23, 2024**.

Figure 2: A teaser of LockBitSupp identity reveal with a countdown set to be announced on February 23, 2024
Source: Analyst1

The intrigue surrounding the revelation of LockBitSupp's identity is just one component of a broader PsyOps campaign orchestrated by law enforcement. Indeed, when combating ransomware, success isn't solely achieved by targeting the technical aspect of the actor's ecosystem. The NCA statement also confirmed this: ***"As of today, LockBit are locked out. We have damaged the capability and most notably, the credibility of a group that depended on secrecy and anonymity."*** After all, behind ransomware are real humans who, in fact, already have mastered psychological manipulation, not only of their victims but also of the informational landscape, including social media and traditional media outlets. This time, perhaps, it was law enforcement's turn to play mastermind games publicly.

In our next section, let's look at what tactics were used to target human vulnerabilities of actors.

Takedown Tactics

To understand the effectiveness of law enforcement's PsyOps campaign, it's essential to delve into two key components pivotal to the success of ransomware operations: **brand reputation** and **interpersonal relationships** among actors. Additionally, analyzing LockBitSupp's response is essential to gauge the impact of the takedown. Given LockBitSupp's outspoken nature, it was unsurprising that they issued a statement shortly after the takedown. This analysis of the LockBitSupp reaction offers valuable insights into the efficacy of the PsyOps tactics deployed. Moreover, their response unveils the psychological triggers that resonated most strongly with ransomware actors. Below are the visual reflecting tactics used to target each key component, which we will elaborate on in detail.

Figure 3: Takedown tactics used to target non-technical key component crucial for LockBit operations
Source: Analyst1

1. Undermine Brand & Leader's Credibility

Brand reputation is paramount for ransomware groups, particularly those operating under the RaaS (Ransomware-as-a-Service) model. Establishing a solid reputation is crucial to attracting affiliates who are vital figures in generating revenue. This brand recognition and reputation is predominantly built across two key fronts: DarkWeb visibility and media coverage.

Throughout LockBit's four-year operation, the group established a strong presence on the DarkWeb. The group also had no problem receiving widespread media attention globally, contributing to the group's notoriety in the broader public sphere. Indeed, the more attention a ransomware group receives in the media, the more it solidifies its image as a formidable threat. This visibility can instill fear and urgency among potential victims, increasing the likelihood of ransom payouts.

During the week following the takedown announcement, the tone of reporting on LockBit shifted significantly. Instead of highlighting the group's notoriety and its latest high-profile victims as usual, numerous articles praised LockBit's defeat and revealed details that undermined its infamous status. For instance, reports surfaced regarding LockBit's promise to delete victim's data upon payment of ransom uncovered by law enforcement during the investigation. According to the NCA statement, ***"Some of the data on LockBit's systems belonged to victims who had paid a ransom to the threat actors, evidencing that even when a ransom is paid, it does not guarantee that data will be deleted, despite what the criminals have promised."***

With this information uncovered and presented to the world, law enforcement again emphasized the importance of not trusting ransomware actors. However, this message may resonate even more firmly this time, encouraging ransomware victims to exercise greater caution in their decision-making process. The revelation further diminishes the likelihood of ransom payouts for LockBit, whose credibility was undermined by their "promise" to delete data. LockBitSupp's response, as expected, denied these allegations by stating, ***"These people dare to lie about me supposedly not deleting stolen information of companies after paying the ransom, clowning around."***

In addition to exposing LockBit operations, the announcement of revealing the identity of LockBitSupp was a deliberate tactic aimed at undermining a leader's credibility. This move is indeed strategic, as in the case of LockBit, the LockBitSupp persona is closely tied to the group itself. In regular business, such strategy is often referred to as "CEO branding" or "personal branding." This approach can be advantageous as it adds a human element to the brand and enhances trust and credibility (from affiliates in our LockBit case). However, it can also pose risks, as any negative publicity or damage to the leader's reputation can directly impact the company's image. So, by targeting and defeating LockBitSupp directly, the entire enterprise's reputation is compromised.

This strategy was also intended to induce anxiety for LockBitSupp and, as a result, for all individuals involved in LockBit's operations. The looming threat of exposing LockBitSupp's identity was aimed at triggering psychological consequences that could disrupt their focus and decision-making. This strategy was used to exploit the actors' vulnerability by instilling fear and uncertainty, compromising the group's operational efficiency.

The reveal of LockBitSupp's identity didn't happen as promised on **February 23, 2024** (perhaps left for the better moment). Even despite that, this tactic succeeded in applying psychological pressure on the actor, who also openly admitted to feeling personally targeted. ***"I wonder why the alpha, revil, hive blogs were not designed so nicely? Why weren't their deanons published? Even though the FBI knows their identities? Strange isn't it? Because with such stupid methods FBI is trying to intimidate me and make me stop working."***

Instead, the **"Who is LockBitSupp"** card was updated with details of information about the actor, stating that law enforcement is aware of where they live, what car they drive, and even stating that LockBitSupp, in fact, cooperating with law enforcement, once again undermining LockBit's leader's reputation and creating distrust among its members. Creating distrust among its members was another tactic which we will discuss in the next section.

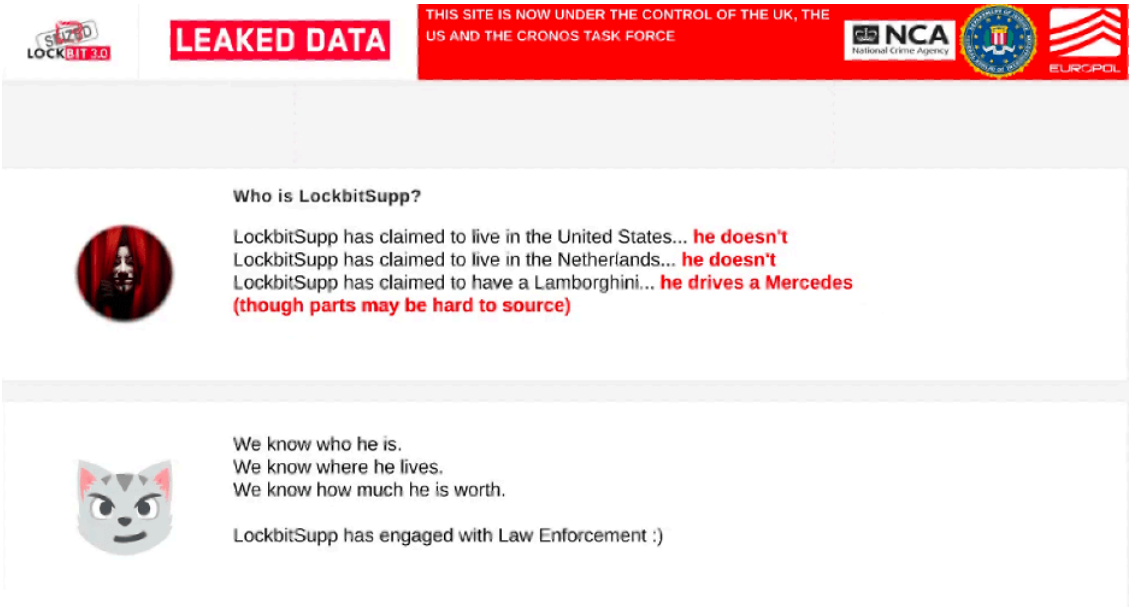

Figure 4: Message left for LockBitSupp providing details of their identity
Source: Analyst1

2. Create distrust among LockBit members

LockBitSupp stands out for the significant visibility that actor has across the DarkWeb and their active engagement within the underground community. Known for their creativity, LockBitSupp orchestrated various interactive events, such as the "Summer Paper Contest" announced in **June 2020** and the LockBit tattoo contest in **September 2022**. During the latter event, LockBitSupp offered a reward of around $1,000 to anyone willing to get a tattoo featuring the LockBit logo.

Operation Cronos couldn't be more timely considering recent events that unfolded not in favor of LockBit and the challenges they faced. Shortly before the announcement, on **January 30, 2024**, LockBitSupp was banned from two top-tier Russian-speaking DarkWeb forums following a complaint from a forum member. Interestingly, law enforcement referenced this incident in one of the announcement cards directed at LockBit, adding a layer of irony to the situation and LockBit's personal shame. In our earlier blog, we discussed details of the ban event.

Check out the full blog "This Forum is a Bunch of Communists and They Set Me Up", LockBit Spills the Tea Regarding Their Recent Ban on Russian-Speaking Forums

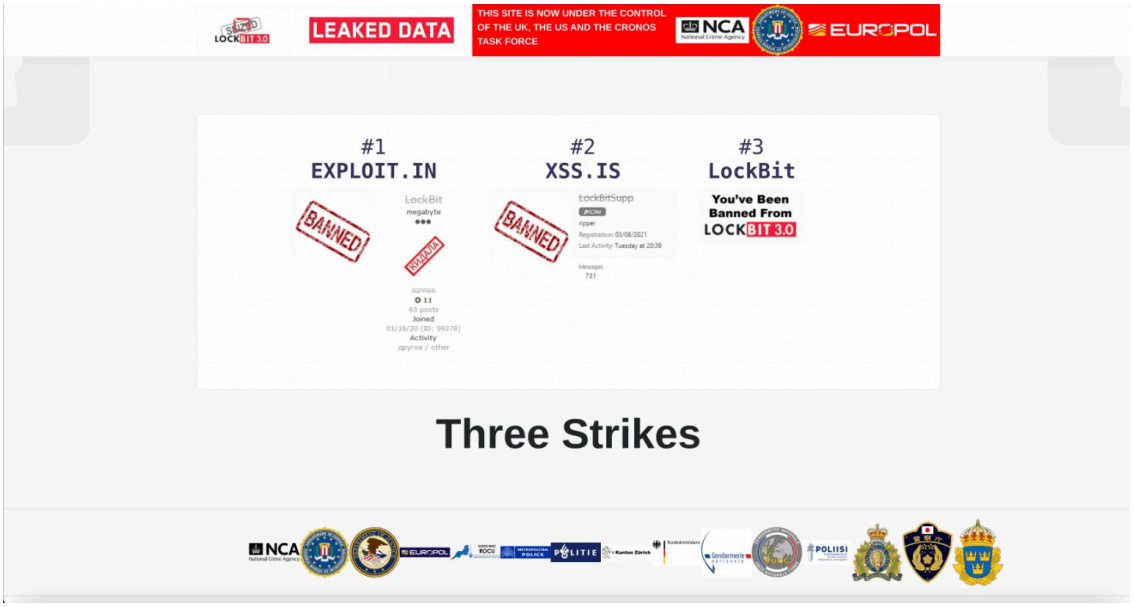

Figure 5: One of the announcement cards reminding of LockBit's recent ban
Source: Analyst1

With these recent events and the law enforcement takedown, LockBit's favorable position within the underground community is now at risk of significant decline. The backlash from LockBit's members may stem from their leader's inability to protect their infrastructure as promised, thereby jeopardizing all members. Details shared during the takedown included the publication of various information exposing these individuals. For instance, a screenshot of the admin panel revealed the monikers of nearly 200 LockBit members. Additionally, the announcement by The Justice Department (DOJ) regarding the indictment of two suspected LockBit members, Artur Sungatov and Ivan Kondratyev, also known as Bassterlord, adds to the complexity of the event.

Despite the severity of the situation, LockBitSupp's response appears to be dismissive: ***"I didn't pay much attention to it, because for 5 years of swimming in money I became very lazy."*** This attitude is certainly not the most effective approach to addressing such a major setback. In addition, in their statement, LockBitSupp attempted to downplay law enforcement investigation, casually denying the role of those arrested or indicted and

the importance of intelligence obtained, ***"The generated nicknames of the partners, which have nothing to do with their real nicknames on forums and even nicknames in messengers, not deleted chats with the attacked companies and accordingly wallets for money, which will be investigated and searched for all those who do not launder crypto, and possibly arrest people involved in laundering and accuse them of being my partners, although they are not. All of this information has no value because it is all passed to the FBI and without hacking the panel, after every transaction by insurance agents or negotiators."*** , also denying the reveal of Bassterlord's identity, stating that the law enforcement named a wrong person, ***"Basssterlord is not caught, I know Basssterlord's real name, and it's different than the poor guy the FBI caught."***

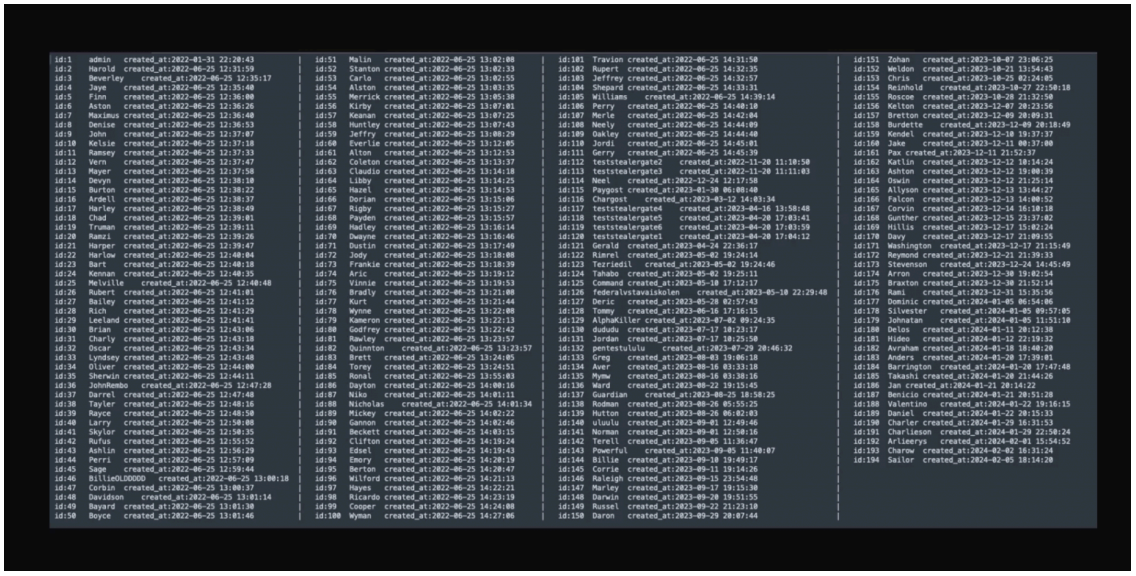

Figure 6: Screenshot of admin panel with the list of LockBit's monikers
Source: Analyst1

This dynamic has the potential to further escalate and staring interpersonal relationships between actors, especially considering that some group members face consequences while the key member remains free, both physically and in terms of their identity not being publicly exposed. This distrust is also likely to be exacerbated by the apparent repercussions faced by other LockBit members. Moreover, the insinuation from law enforcement about LockBitSupp's potential cooperation doesn't bolster their credibility either.

In our next section, we will analyze how legal implications can exert pressure on LockBit's operations and discuss why they are significant.

3. Add pressure through legal matters

According to the DOJ announcement, a U.S. indictment charged two individuals with attacks on multiple U.S. and international victims. These two individuals, Artur Sungatov and Ivan Kondratyev, both identified as Russian nationals residing in Russia.

The pursuit of ransomware actors through legal avenues presents both challenges and opportunities in the fight against cybercrime. Despite the global dispersion of these actors, the implementation of indictments and sanctions serves as a powerful tool for applying pressure and disrupting their illicit operations. While concerns exist regarding the cooperation of certain jurisdictions, such as Russia, the initiation of indictments can still have

significant repercussions for ransomware actors, potentially drawing unwanted attention from their own governments. Previously hidden in the shadows of the underground, these actors suddenly might find themselves under intense scrutiny from their own state, leaving them with little freedom. Just this alone can be an incredibly powerful tool for applying pressure.

Furthermore, targeting cryptocurrency assets, enhances the effectiveness of law enforcement efforts. Thus, as part of the takedown, Operation Cronos Crypto Analysis revealed and seized multiple assets identified to have been used by actors to receive and launder ransom payment proceeds. By employing the appropriate tools for blockchain analysis, law enforcement can effectively disrupt ransomware operations by depriving actors of their illicit profits. This undermines their financial capabilities and sends a strong message of deterrence to other cybercriminals.

In response to law enforcement actions and the unveiling of blockchain analysis, LockBitSupp attempted to discredit the evidence presented, "***I really dislike that all such throw-ins are made without publishing transactions and wallets, thus it is impossible to verify what is true. You can accuse me of anything without proving anything, and there is no way I can refute it, because there are no transactions and bitcoin wallets."*** Indeed, losing the battle on this front and their illicit profits are probably what hits actors the most.

With this ongoing battle, the question remains: what is LockBit's next move, and will they survive? In our concluding section, we will analyze what future might hold for LockBit.

What the Future Holds for LockBit?

Operation Cronos is one of several takedown operations executed against ransomware criminals over the past several years. Previous law enforcement operations targeted ransomware adversaries such as DarkSide, REvil, Hive, and BlackCat. While most of these efforts disrupted the criminals' operations significantly, some led to the criminal's demise. Other groups chose to rebrand and rebuild their operations from scratch, using new monikers to mask their previous criminal identities. On rare occasions, like the current situation with LockBit and previously with BlackCat, ransomware groups attempt to *weather the storm* and maintain their brand.

There is no question that Operation Cronos delivered a significant blow to the LockBit ransomware program. However, now, LockBit is trying to restore its operation and wants to prove to the world that it's still the top-running ransomware gang. Its quick return was no surprise to Analyst1 based on our long-rgyhunning relationship with the real-world person leading the gang, who is a narcissist with an immense ego. With the threat of prison and a lifetime of having to look over his shoulder, you would think, why doesn't he simply walk away? The answer can be summarized in one word… vengeance.

To obtain the revenge it seeks, in the coming months, we expect LockBitSupp will encourage its affiliates to prey on high-profile targets, including Fortune 500 companies, hospitals, government, and other organizations that will allow the gang to profit and make headlines, which it desperately needs to restore it once untarnished criminal brand. Additionally, the actor will almost certainly update its ransom payload, which has not seen a refresh since June of 2022 and will retool its operation with updated resources. Understand that LockBit considers the takedown personal, which, in our opinion, it was. After years of making statements to Analyst1's Jon DiMaggio, such as **"You and the FBI are too dumb to catch me"** it appears the law enforcement wanted to make an example of the group and all who support it, which they did. The following points detail how this was achieved:

1. The taskforce “Operation Cronos” did not just seize LockBit’s infrastructure; it gained access to all of LockBitSupp’s private and often sensitive operational conversations from the Tox communication application the gang uses to discuss day-to-day operations.
2. Law enforcement collected information on all of LockBit’s affiliates from the ransomware admin panel, including IP logs, ransom negotiations logs, decryption keys, and obtained cryptocurrency addresses used to launder ransom payment proceeds.
3. The integrity of the group’s infrastructure was harmed significantly raising concerns about further law enforcement compromise of LockBit’s operations. This is due to visibility into LockBit’s infrastructure and intelligence that was obtained that would allow silently watching and collecting information on its criminal participants and the gang’s operations.
4. Most significantly, Operation Cronos invoked doubt and fear amongst the criminal community who trusted LockBit to keep their anonymity and operational security safe. LockBitSupp failed them and possibly himself. The law enforcement may not have publicly deanonymized LockBitSupp, but it inferred that LockBitSupp cooperated with them in order to keep his identity private.

For these reasons, LockBit’s recovery will be challenging, and it has much to overcome to accomplish a meaningful return, let alone to successfully enact the vengeance it so desperately seeks. Still, we should not discount LockBit as the actor has proved to be a worthy adversary and has overcome significant challenges in the past. Further, law enforcement must be ready for round two of this fight, as all signs indicate that LockBit is now more motivated than ever. Analyst1 will be watching, and continuing report on our analysis of LockBit and support the war against ransomware!

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.
