Ransomware Diaries: Volume 1 | Analyst1

By Jon DiMaggio

Published: 2023-01-16 · Archived: 2026-04-05 18:58:42 UTC

I gotta story to tell…

The LockBit ransomware gang is one of the most notorious organized cybercrime syndicates that exists today. The gang is behind attacks targeting private-sector corporations and other high-profile industries worldwide. News and media outlets have documented many LockBit attacks, while security vendors offer technical assessments explaining how each occurred. Although these provide insight into the attacks, I wanted to know more about the human side of the operation to learn about the insights, motivations, and behaviors of the individuals on the other side of the keyboard. To prepare for this project, I spent months developing several online personas and established their credibility over time to gain access to the gang's operation.

The LockBit ransomware gang is one of the most notorious organized cybercrime syndicates that exists today.

Over the months, I spent my time on criminal forums and private chat groups used by ransomware criminals and gained inside knowledge about the LockBit gang itself. I identified the accounts and infrastructure used by the gang and the criminals they interacted with. I could see the tools and resources used to manage and conduct attacks from the adversary's perspective. More importantly, I learned about the opinions, personal habits, motivations, and insecurities of the human criminals behind the operation. Then, I took many of the public events and high-profile attacks to include theories previously made about the LockBit gang and tried to capture the side of this very interesting story.

Next, I will walk through the entire lifecycle of LockBit activity from September 2019 until January 2022. I will detail the gang's criminal operation and add LockBit's version of events to tell the story, as it has not been detailed before. In conducting this research and analysis, I found several mistakes made in attributing the early activities of the LockBit gang, which I will discuss. Finally, I will provide a complete intelligence assessment focused on my findings, open-source information, technical data, and human intelligence gained while profiling LockBit itself.

If you are not interested in the larger story, you may want to skip to the "Unmasking Lockbit" section near the end of this report for a summary of unique findings derived from the human intelligence I gained from my interactions with Lockbit. However, the screenshots and details surrounding each conversation are included throughout the body of the report itself in the order in which they took place.

Before I begin, here are a few things I learned about LockBit and its operation over the course of my research:

The Prequel

Little information exists about the LockBit gang before September 2019, when their operation began. As with any skill or trade, becoming proficient in what you do requires practice and experience. For example, I know ransomware groups like DarkSide and REvil began as affiliates supporting more mature Ransomware as a Service (RaaS) programs before branching out independently. Similarly, the criminals behind the LockBit gang likely started their illicit careers before the LockBit operation began.

Today, an information gap exists, making it difficult to clarify what led these criminals to begin the LockBit operation. Still, one theory exists. Some security vendors believe LockBit is associated with now defunct ransomware known as Gogalocker and Megacortex.[4,5,6] These ransomware operations began in January 2019,[7,8] six months before we first saw LockBit ransomware in the wild. The security vendor based the attribution on the following evidence:

- ***Targeting:*** Similar victims
- ***Tool-use:*** The use of PowerShell to execute commands and run scripts
- ***Self-spreading mechanism:*** The use of Address Resolution Protocol (ARP) tables to identify victim hosts and the use of the Server Message Block (SMB) protocol to identify and spread the ransomware across shared resources/networked devices throughout victim environments.[9]

As an analyst, I have issues with the supporting evidence used to make this attribution.

Previous Attribution?

You don't always need to conduct attribution, but when you do, it needs to be unbiased and developed from solid evidence. When done incorrectly, it creates a snowball effect, misleading future analysis built on false attribution. I was intrigued when I first read the attribution linking LockBit to Gogalocker and Megacortex because I have done extensive research on all three and previously presented on Gogalocker at the 2020 RSA Conference.[10,11] I witnessed firsthand the targeting, tools, and ransomware behaviors that other security vendors would eventually use to associate the activity with one another. Before we continue, let's vet the attribution used to associate LockBit with other ransomware variants since it's essential to understand where LockBit may have originated.

First, let's discuss the attribution based on how the ransomware spreads. Today, many ransomware variants use ARP tables to discover victim hosts and SMB to spread across shared network resources within the environment. In 2019, however, human attackers usually conducted ransomware propagation, manually working within the compromised victim environment. At that time, it was less common to use self-propagation techniques. This is likely why the security vendor made the attribution, but in reality, even then, this technique was not unique.

Worms and viruses had used this same technique to self-propagate long before these ransomware variants existed. Further, older ransomware like Wannacry took advantage of similar protocols for host discovery and self-spreading. In contrast, it is not a one-for-one comparison, but the protocols, methods, and development ideas behind it have existed for a long time. The use of PowerShell, also used as attribution evidence, is seen in every ransomware attack I have investigated. It's a tool present on every Windows operating system. These methods and resources are common, making them weak for attribution purposes.

Last, the vendors stated that the targeting seen in the attacks supported their attribution. When I first read this, I thought the security vendors intended to communicate the similarities in targeting originated from the specific

code or methods used within the ransomware binary itself to target operating system files. This could be a more substantial technical point for attribution if novel. However, it seems the attribution stems from a more general sense describing the broader overlap in victim targeting.

In terms of ransomware attacks, victims are almost always targets of opportunity, not design. Remember, the attacker wants to get paid and seeks access to any victim they deem profitable enough to pay the ransom. Further, many Russian-based ransomware gangs, like LockBit, have strong relationships with other gangs, who sometimes share resources and even victim data.[12] So, using targets and industries seen across multiple ransomware operations is generally not convincing enough to support strong attribution. Additionally, in November 2021, Europol arrested twelve men for supporting the Gogalocker ransomware operation.[13] Not one of the men arrested claimed to have any association with LockBit. If they had, they likely would have used the information as a bargaining chip to minimize the sentence they were facing. For these reasons, I believe the attribution made between LockBit, Gogalocker, and Megacortex was made in error.

PART I: All Your Important Files Are Encrypted!

The LockBit gang began its operation in September 2019 and was first known as “ABCD ransomware.” The security community dubbed it “.abcd” because the ransomware payload appended the characters “.abcd” to each file it encrypted. However, the ABCD ransomware was far less sophisticated than later-developed LockBit variants. Nevertheless, while slow, simple, and less advanced, the attacker succeeded at compromising and infecting victims. At the time, the operation did not have the infrastructure to host chat-based negotiations as it does today. Instead, the ransom note instructed victims to contact them by email, as seen in **Figure 1** below.[15]

Figure 1: Early ransom note delivered with .abcd ransomware

Over the first six months of activity, LockBit primarily extorted victims in the United States, Germany, France, and China.[16] However, since they did not use a victim data leak or name and shame site at the time, we only know of victims who publicly reported an incident, leaving us with a limited view of the attack volume. To learn more about the early operation, I identified victims who posted to support forums seeking help after being infected with “.abcd” ransomware in late 2019. The first was a small firm with 17 computer systems within its enterprise, and the second with just four systems.

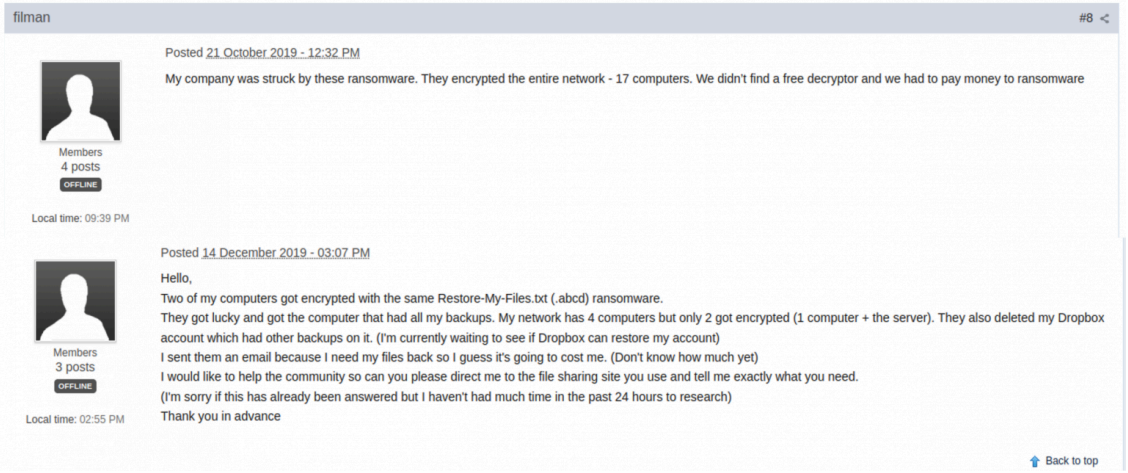


Figure 2: LockBit victims seeking help after their systems were encrypted by ABCD ransomware[17]

Both victims confirmed that the attacker used the known .abcd-related email addresses seen in Figure 1 to negotiate the ransom payment. During the negotiation, the adversary demanded three bitcoin (BTC) for the key necessary to decrypt victim files. After several days of not paying the ransom, the criminal dropped the price to .5 BTC, which one of the two victims paid. After payment, LockBit provided the decryptor, and the victim recovered all of their data. With only four systems in total, the second victim decided to rebuild their environment. While the victim used only four systems to run their business, they stated, the attacker also encrypted their backups and their Dropbox account, resulting in a loss of customer data.

While this is only two victims, based on available information, the attacker asked most victims for a payment of between one and three bitcoin. At that time (June-December 2019), the cost of one bitcoin fluctuated between $7,000 and $11,000 USD,[18] making the maximum demand around $30,000. This was far less than the multimillion-dollar ransom LockBit demands today.

> After several days of not paying the ransom, the criminal dropped the price to .5 BTC, which one of the two victims paid.

RaaS Program

Several months after the ransomware operation began, the adversary behind the attacks made changes to their name and branding. Personally, I don't like the name ".abcd ransomware." Apparently, LockBit did not either because, after only several months of activity, the adversary behind the attacks decided to change its name. Ultimately, they updated their code, altering its behavior to now append ".lockbit" to each file, and began to reference the name "LockBit" within the ransom note, completely doing away with the .abcd reference. Additionally, the adversary began using their own infrastructure to support victim negotiation. This is how the name LockBit came to exist and is the branding the crime syndicate behind the operation still goes by today. Figure 3 displays the original ransom note (left) from November 2019 depicting the ".abcd" ransomware and the updated LockBit updated ransom note (right) from February 2020 showing the change using the LockBit name and infrastructure.

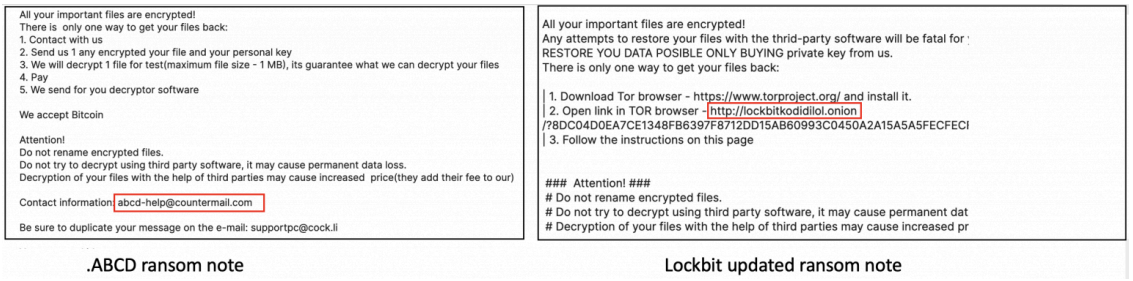


Figure 3: Ransom notes depicting changes incorporating the name LockBit

Note that during the first five months of the operation, LockBit conducted attacks themselves without the support of hacker affiliates. While the adversary keeps 100% of profits made in a closed program, there are fewer attacks than in a RaaS program in which many affiliates take part in the operation for a share of the ransom profit. However, LockBit revamped its business model to grow and scale and began its RaaS program in **January 2020.**[19]

The new RaaS campaign had several attractive features to tempt affiliates to join the operation. The LockBit gang claimed their ransomware payload had fast encryption capabilities and could self-propagate within a victim environment. As mentioned, at the time, most RaaS operations required the affiliate to manually enumerate and spread ransomware, which often took days to weeks to complete. Evidence to support the claim came in **April 2020**, when LockBit compromised a victim organization through its web server.[20,21] LockBit gained access by exploiting unpatched, vulnerable VPN software.

Now, with access to the internal network, LockBit brute-forced an administrative account to acquire the credentials necessary to deploy ransomware and infect the first host, patient zero. Next, to identify other hosts in the target environment, patient zero performs an ARP request to obtain the Mac addresses of connected hosts and their associated IP addresses listed in the ARP table, allowing patient zero to connect to each system. To connect with other known systems beyond those in its local subnet, patient zero uses the SMB protocol to identify networked devices and shared network resources, such as file servers, domain controllers, and other high-value target systems. This should sound familiar because it is the technique I discussed earlier, which security vendors used for attribution.

With the knowledge and connectivity to reach most hosts throughout the environment, patient zero tells all systems to execute a single command. The command instructs the hosts to connect to an external attacker-controlled website. Then based on the victim's browser and operating system values, it downloads one of two .png image files from the site, delivering the ransom payload throughout the victim's environment. From start to finish, the attack took only several hours to gain privileged access, enumerate the network, and deploy the ransom payload. At the time, it was one of the fastest ransomware infections observed.

Ironically, this dated tactic used to propagate the ransomware gave LockBit the upper hand over many of its competitors. When it worked, this feature provided the attacker with two advantages. First, they do not have to spend the time and resources working to discover and infect systems with the ransom payload. Second, the adversary can increase their attack volume. Now, they can conduct several attacks over the time it took to implement a single attack. However, for the attack to work at this speed, the adversary needs to gain access and admin rights quickly, and is only effective if the target's defenses cannot detect the activity or the ransom payload.

This was just one attack, and while most breaches don't run this smoothly, it showed us what was coming. LockBit's end goal was to create fast, efficient automated ransomware attacks that require little technical hacking experience.

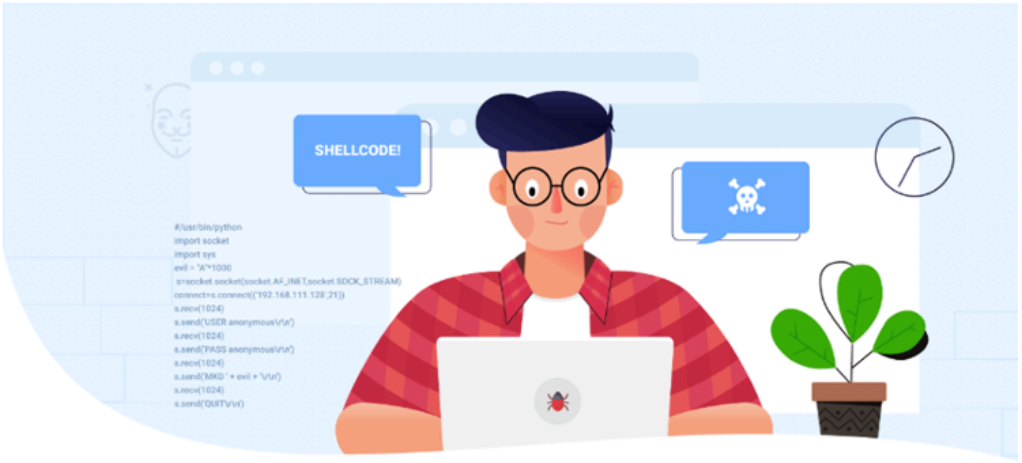
During the first year of RaaS activity, other victims and security researchers posted details about similar attacks. While all relied on the same ransomware payload, some attacks included other tools and resources. For example, in at least one incident, LockBit used a publicly available keylogger to capture the keystrokes of the target users.[22] The gang also used a custom screensaver, which locked out the legitimate user and required an attacker-specified password to regain access to the desktop.

The Summer Paper Contest!

In the early days, LockBit was not well known. They were one of many ransomware gangs attempting to gain recognition in a community of organized criminals. The individual leading LockBit needed a way to communicate and market the LockBit brand. The problem was LockBit could not post ransomware ads using traditional marketing and social media platforms. Even if it could, that would not reach the criminal demographic relevant to a ransomware gang. However, underground criminal forums and markets are full of criminals LockBit wished to attract to support its operation and generate revenue for the gang. For these reasons, senior members of the gang created the LockBitSupp persona. LockBitSupp, short for LockBit Support, began interacting and posting on the forums, participating in conversations, and socializing with other criminals. Still, the persona was unknown and had little criminal credibility at that time.

To change this, LockBit ventured beyond the borders of the traditional ransomware community and donated money to sponsor a "Summer Paper Contest" on a Russian hacking forum in June 2020. To win the contest, applicants would conduct research and write a paper on various hacking topics, shown in Figure 4.

We're kicking off the ?summer PAPER CONTEST #4! With a prize fund - 15.000$



LOCKBIT

Летний конкурс статей

$15000 призовой фонд

Напиши статью - заработай на отдых

The winner of the competition (1st place) receives a prize - **$5,000**

2nd place - **$4,000**

3rd place - **$3,000**

4th place - **$2,000**

5th place - **$1,000**

Total prize pool **$15,000**

If a LockBIt likes your article, it will be rewarded additionally. Topics of interest to the sponsor: cryptolockers, networks.

Contest

Sponsor Sponsored by LockBIt,locker team LockBit. Thanks for the financial sponsorship!

Accepted article topics:

- Hacks (web, *nix). Any. Methods for pouring shells, fixing, elevating rights. Your stories and tricks. Interesting hack stories.
- Malware and Malware coding. Bots-botnets, viruses, trojans. Bot development. Exploitation and monetization.
- Hacking programming: writing bruters, parsers, checkers, spammers, flooders, etc.
- SI and phishing in practice (phishing systems, point infections).
- "Wireless" hack. Hacking wi-fi, bluetooth, intercepting and sniffing traffic.
- Search for 0day and 1day vulnerabilities. Development of exploits for them.
- Spot infections and attacks.
- ART attack. LAN hacks, privilege escalation, domain controller capture, attack development
- Hidden internet. Alternative DNS. Cryptodomains. All about TOR. I2P.
- Traffic: mining methods, working with traffic.
- Non-standard methods of extracting material: admin, shells, roots, bases, socks, ssh, dedics, etc.
- Antidetects and Fingerprints. Work with antidetect systems. hiding methods. Working with collected fingerprints.
- Cryptography. Interesting combinations, algorithms. Writing your own cryptoalgorithm and hacking someone else's.
- Digital forensics. Up-to-date software, information collection, investigation methodology.

Figure 4: LockBit sponsors hacking article contest

Members of the forum community could then read and vote for the paper they liked most. Authors of the top five papers received a monetary prize ranging from $1,000 to $5,000. Then, from the top five, LockBit selected the paper they liked best for an additional prize. This is one of several examples demonstrating how LockBit differs from most ransomware attackers we have seen to date.

While atypical, this helped LockBit grow its reputation within the criminal underground. Threat detection and response are insufficient for an effective response. The abundance of intelligence gathered from diverse sources and applications makes it difficult to establish connections and make informed decisions.

Ransom Cartel: I'm gonna make him an offer he can't refuse

Also in June 2020, LockBit and four other ransomware gangs began to announce a new partnership to form the world's first ransomware cartel. Forming a cartel would benefit its associated gangs, who would have greater resources, funding/revenue, and present an increased threat to targeted organizations than a single ransomware gang, making this a scary scenario. The five gangs that formed the cartel can be seen in Figure 5 below:

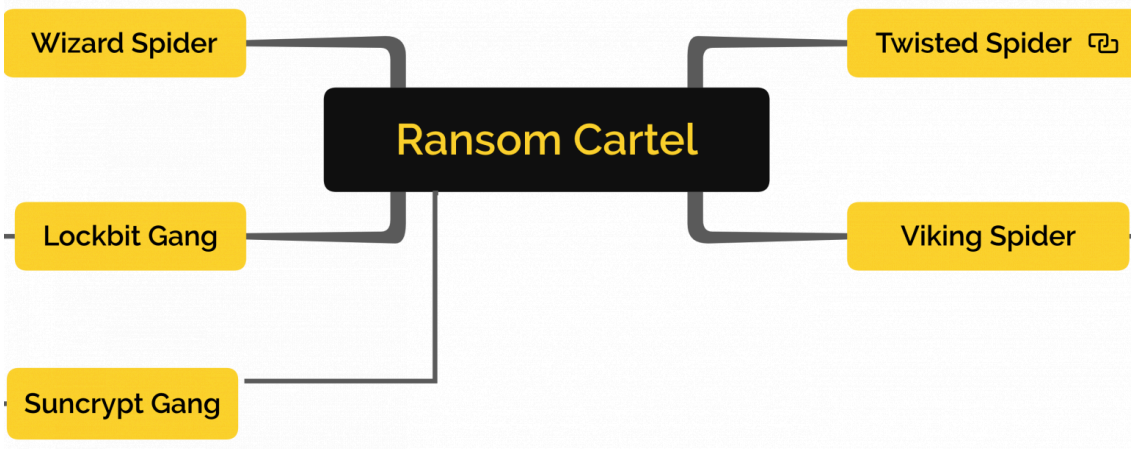


Figure 5: Ransom Cartel from 2021 (Spider names from CrowdStrike)

Cartel Analysis

After I initially heard the claim, I analyzed all the relevant data at the time. I found the groups did share resources, such as victim data and infrastructure, and collaborated with one another. For example, the LockBit gang, among others, shared stolen victim data with Twisted Spider, who ran Maze & Egregor ransomware operations.[23] Twisted Spider posted LockBit's victim data to their leak site to further pressure and extort the victim. Data and infrastructure were not the only things the gangs shared with each other. They also shared their tactics. For example, Twisted Spider is the first ransomware gang to steal sensitive data and use it for a second extortion demand. LockBit was one of the early adopters of this tactic and incorporated it into their own attacks. LockBit also is one of the first gangs to encrypt the master boot record, in addition to system data, which several other cartel gangs incorporated into their attacks. LockBit even took design aspects from code development originally seen in Twisted Spider's Egregor ransomware, such as unique anti-analysis techniques integrated into their payload.[24]

Despite claims of forming a cartel, things are not always as they appear. After conducting extensive analysis, I found that the five ransomware gangs invented the cartel as propaganda to boost their criminal credibility and gain name recognition. You see, to be an actual cartel, there must be two primary components: leadership and money. The pretend cartel had neither. While the cartel gangs made a lot of money, there was no revenue-sharing model between them. Instead, each kept the money they extorted and shared only the revenue within their operation.

Twisted Spider was the cartel's voice giving the image that it was the central leader directing the gangs within. They frequently made statements, published press releases, and talked to outlets, such as *Bleeping Computer*, about the cartel. However, despite their mafioso dreams, it was not the "Pablo Escobar" of ransomware. Instead, they were in between a clown and a cheerleader, desperately seeking the media's attention. Despite all their claims, I found no evidence to support that any other gangs took direction from Twisted Spider or anyone else.

In short, there was no cartel. However, the fact that these criminal organizations worked and collaborated is significant. This was when I first realized how small the ransomware community really is. Many ransomware criminals operate and work with one another.[25] You can read the full story and my analysis on the ransom cartel in Analyst1's white paper "Ransom Mafia," which you can find here.[26]

Consumer Reviews Matter — The Wexford Complaint

You can see that reputation was important to the LockBit gang based on their participation in criminal forums and the cartel. However, as a new RaaS provider, LockBit struggled to gain the momentum and popularity it sought over its first year of operation. To be a successful RaaS provider, LockBit needed to attract the top affiliates who would conduct attacks leading to ransom payouts. However, several other more established ransomware gangs, such as REvil and Twisted Spider, existed at the time that also ran RaaS operations. LockBit marketed their RaaS across criminal forums to establish themselves and strived to be one of the most respected and known criminal gangs.

Affiliates rely on criminal forums and markets to obtain reviews of other criminals and their service offerings. They use the information the same way you would a consumer reviews site, such as Yelp or Google reviews, to determine the reputation of a business. Also similar, it only takes a few bad reviews to tarnish your reputation. LockBit certainly understood the importance of having a solid reputation, but it should have judged the significance of addressing criticism and complaints on the forums. You see, in the Russian criminal ecosystem, criminals use an organized arbitration process to address issues and grievances between one another.[27]

In September 2020, an individual using the alias "Wexford" filed an arbitration claim against LockBit on an underground Russian forum.[28] In the claim, seen in Figure 6, Wexford stated that he had been working as an affiliate for the LockBit operation for several months, and none of his victims paid the ransom.

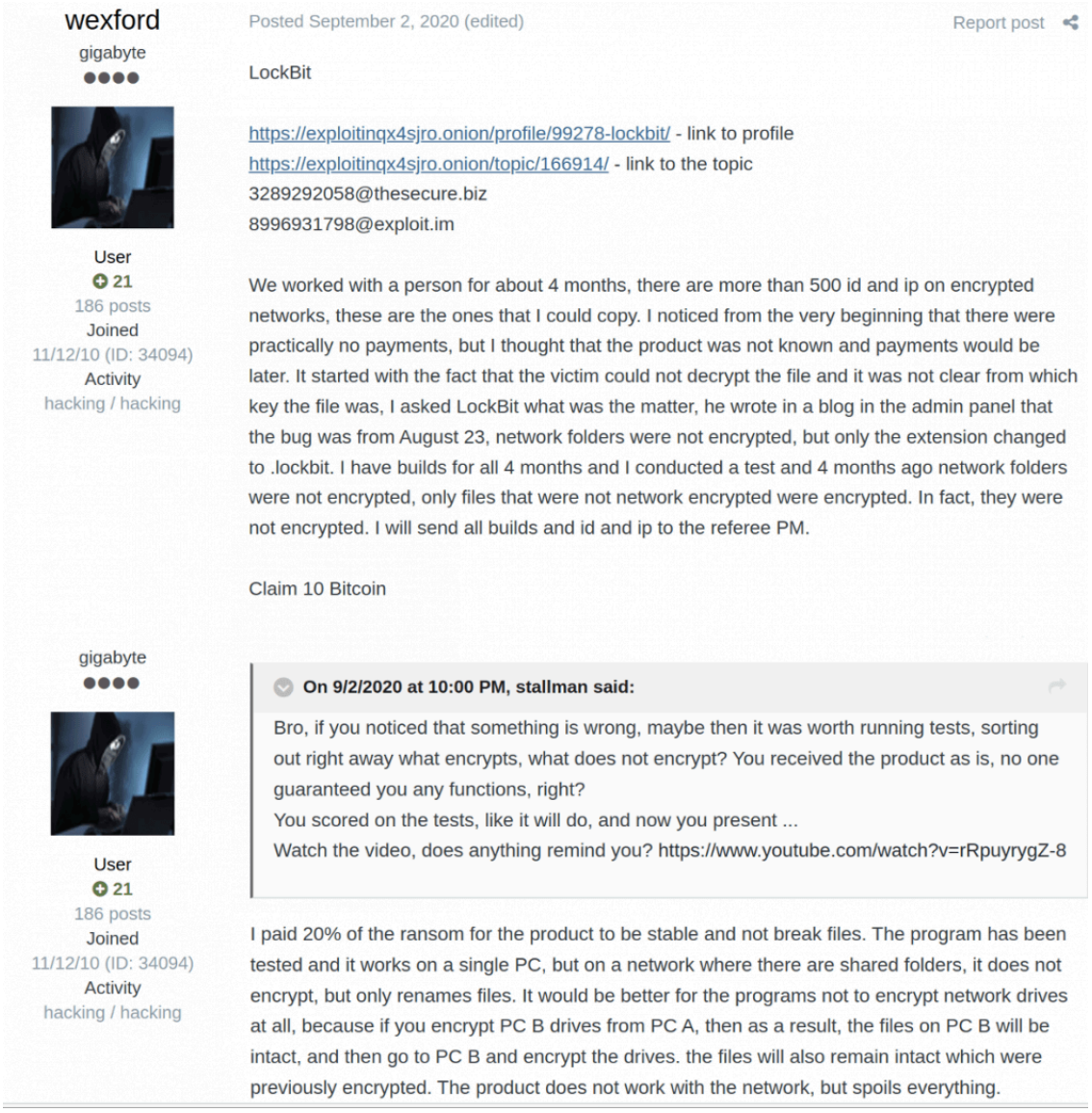


Figure 6: Wexford complaint posted on an underground criminal forum

Wexford claimed that due to the development error, the ransomware failed to encrypt the files on networked hosts but instead appended the ".lockbit" extension to the filename, leaving the data untouched. Now, the victim could simply rename the files on networked systems and remove the .lockbit extension, allowing the victim to restore their data without paying the ransom.

> *I renamed the file, removed the LockBit extension, and the file opened." — Wexford*

Wexford spent four months breaking into victim environments, deploying faulty ransomware that failed to encrypt the victim's data. As a direct result, none of the victims paid the ransom, leaving him with nothing to show for his work. Making matters worse, LockBit refused to accept responsibility and told Wexford he should have tested the payload and notified them about the issue sooner. Other affiliates responded that their victims also often disappeared without paying and now understood why. LockBit eventually fixed the bug, but the fact that it existed and its refusal to accept responsibility certainly tarnished its reputation within the criminal community.

PART II: Extreme Makeover — LockBit Edition!

After the arbitration case with Wexford, LockBit knew it needed to do better if it wanted to become one of the top ransomware syndicates. Over the next six months, LockBit worked on a new project, internally referred to as "**LockBit Red**," and publicly known as "**LockBit 2.0**."

In September 2020, I saw a forum post (Figure 7) created by LockBit to hire someone who could help automate tasks using the Active Directory Group Policy. At the time, I thought LockBit was looking for someone to help compromise a specific organization by exploiting some aspect of Group Policy to deliver ransomware within their environment. However, I later realized LockBit needed development help to add functionality to its ransomware. Using group policy to terminate security services and deploy ransomware was one of the new capabilities found in LockBit Red.

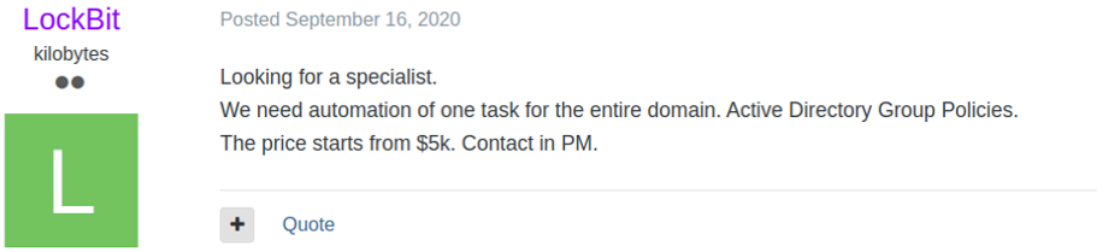


Figure 7: LockBit post to hire support for the LockBit Red project

While the project would not be launched publicly until June 2021, the gang began beta-testing with select affiliates in April 2021. The new ransomware update included the addition of many capabilities and features. LockBit claimed its ransomware had an updated encryption capability, making it faster than the previous version, which allowed it to encrypt victim data quicker than its competitors. To simplify operations, LockBit also designed an updated admin panel, accessed via Tor, allowing affiliate partners to conduct and control their attacks from one easy-to-use graphical interface. LockBit Red included many attractive hack tools and attack resources, such as port and vulnerability scanners, the ability to clear and delete logs, terminate security services, remove shadow copies that could allow users to restore data, and much more. The gang also introduced chat functionality into its interface, with the ability to send the attacker push notifications when a victim responds to negotiate the ransom demand. Figure 8 displays an ad posted by LockBit to market both its updated ransomware and affiliate program:

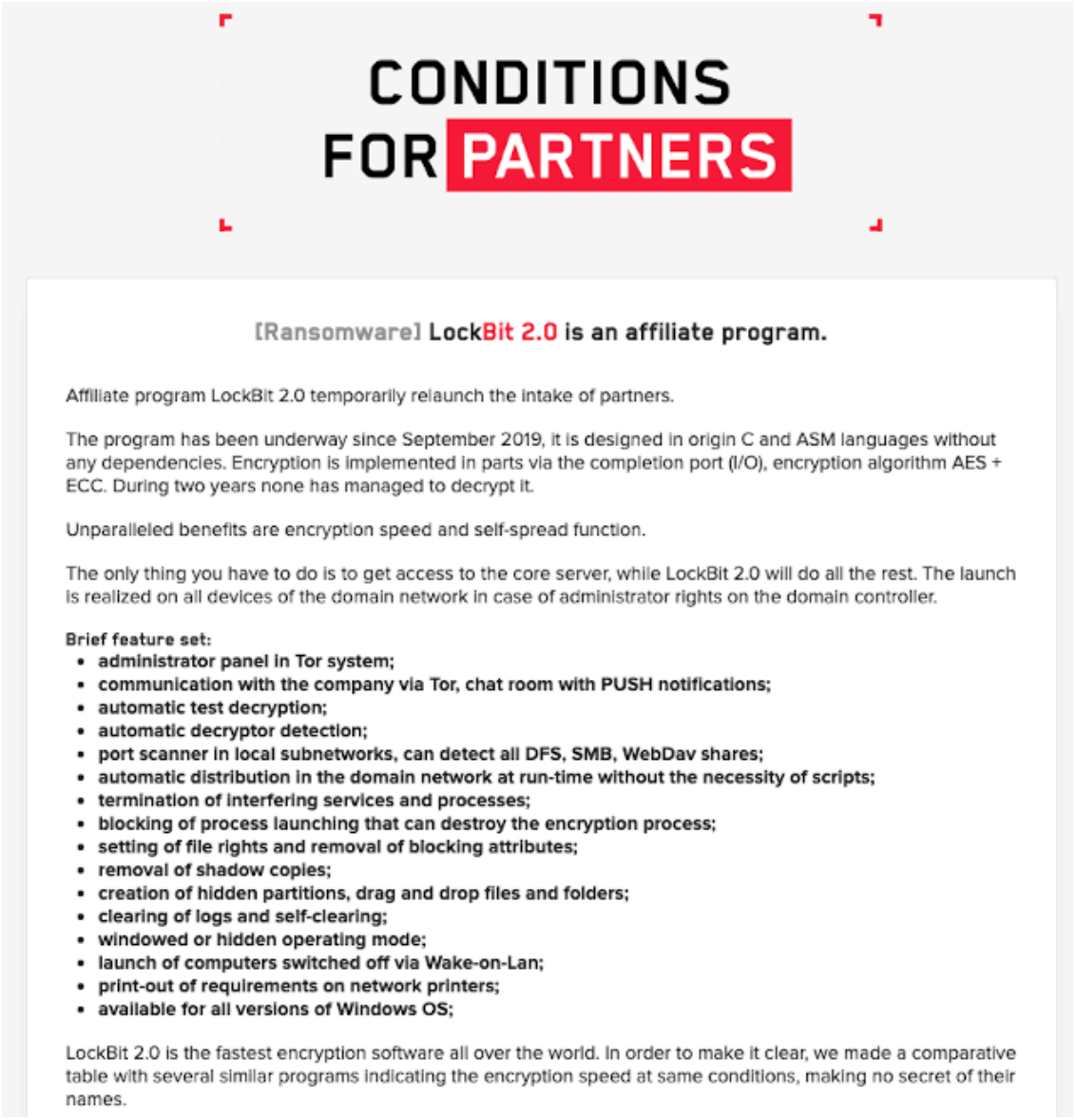


Figure 8: LockBit affiliate recruitment ad

LockBit also included a feature, first seen used by Wizard Spider (Conti & Ryuk ransomware), a few months earlier, that leveraged a Wake-on-Lan feature that allowed attackers to boot systems powered off at the time of the attack. I know LockBit is associated with Wizard Spider as part of the cartel. Still, I don't know if they copied the technique or had help integrating the feature into LockBit Red. Regardless, this feature is essential to the attacker, as it ensures that any systems in the victim environment that was not in an "on" state could be infected and encrypted. For example, before this feature existed, if a victim had servers storing backup data and was powered down at the time of infection, the attacker could not deploy the ransom payload to the offline server. Then, after the attack, the victim could boot the server and use it to restore data without paying a ransom. Now, with this feature, the adversary can ensure it infects all available systems in the target environment.

LockBit Red included many features attractive to affiliates. However, LockBit's payment model was the most significant benefit to its partner affiliates. In most RaaS operations, the core gang controls the money and receives the victims' payments directly. Then, after receiving the ransom payment, the core gang pays a percentage to the affiliate. Some RaaS providers, such as REvil, took advantage of the situation and did not always pay the

affiliates, leaving them with nothing to show for their time and work. LockBit is one of the first to offer an alternative payment model in which the affiliate controls the money. This model elevates the issue of not being paid and likely drew many affiliates to work with LockBit. Additionally, LockBit has to launder only its own money, making it a cleaner process with less overhead and risk involved.

Steal this report!

Stealing and threatening to sell or release a victim organization's sensitive data is often more damaging than encrypting their systems with ransomware. The data theft extortion tactic is lucrative for criminals but requires additional work and resources. For example, criminals must either know which data is most sensitive or steal a lot of it to ensure they have the most critical information. Transferring large amounts of data is noisy and often detected; this can be a problem for an adversary who wants to execute the attack quickly and efficiently while remaining undetected in the victim's environment. While LockBit's ransomware payload is one of the fastest data encryptors, it initially relied on legitimate publicly available tools, such as Rclone, to steal and exfiltrate data which was cumbersome and added time to the attack.[29]

To address the issue, LockBit developed its own data exfiltration tool called "StealBit," which is available to all affiliates supporting their program and is faster than Rclone. StealBit also includes built-in defense evasion techniques and can delete itself after use.[30] LockBit made StealBit available to affiliates directly from the admin panel used to manage their ransomware attacks. This minor detail is important because it provides the attacker with a central management console that incorporates many attack features within a single graphical interface. This reduces the overhead and complexity of conducting ransomware attacks. Later, in April 2022, while conducting research for this paper, I received screenshots directly from LockBit showing the attacker's view of the StealBit management console. While some of the features in this screenshot were not available in 2021, it provides context into how easy LockBit has made it to steal data from its victims.

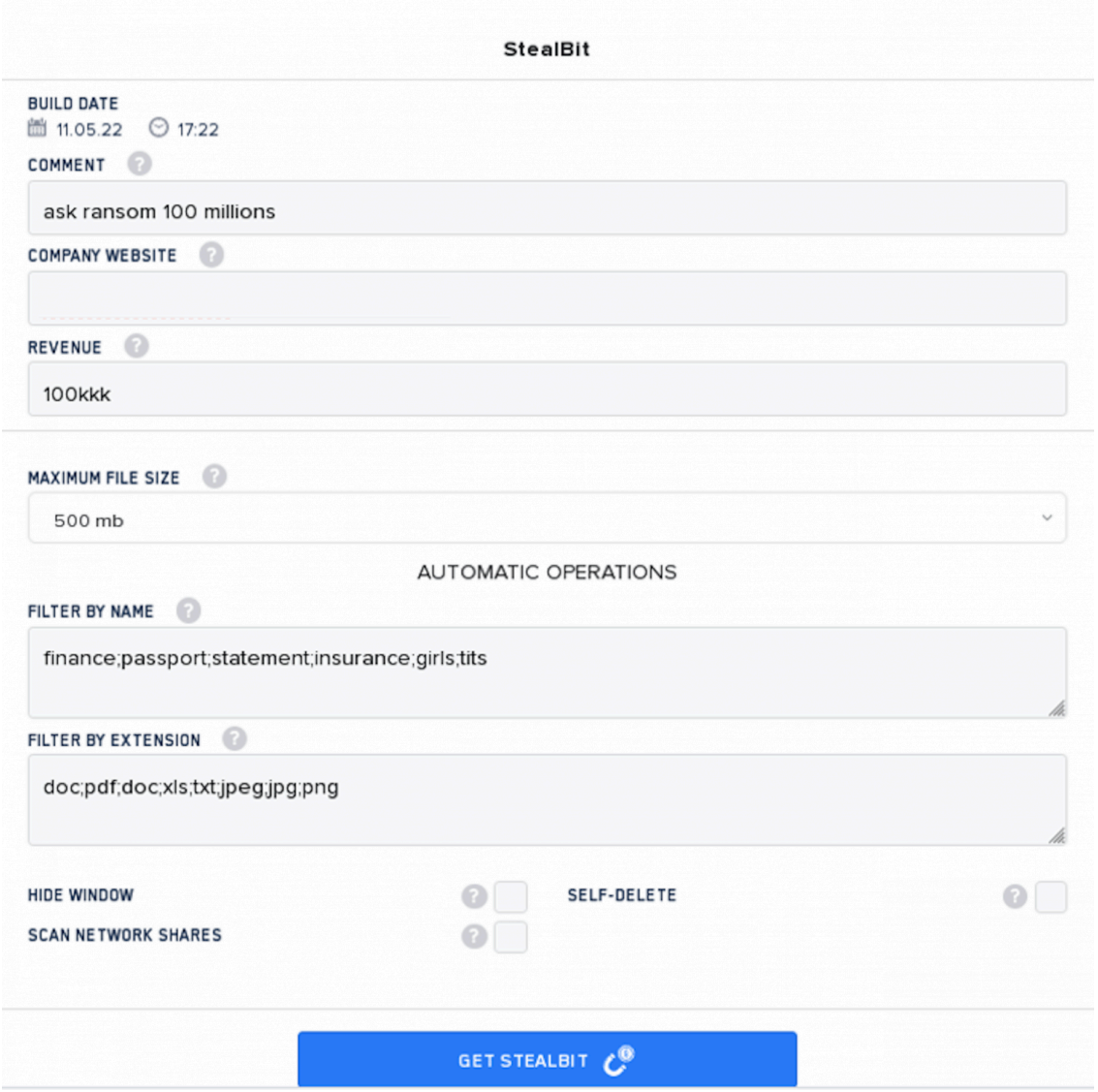


Figure 9: StealBit attacker management console

Now, the LockBit affiliate can simply point and click to deploy its ransom payload and manage StealBit to identify and exfiltrate victim data throughout their environment. Further, LockBit designed StealBit with many easy-to-use features, such as targeting and copying specific file types and applications.[31] If the affiliate does not know what data they should steal, StealBit can copy entire folders and directories, regardless of the type of data within it. Once copied, the attacker still needs to exfiltrate the data outside the victim's environment. Previously, this was a problem for LockBit since it had to rely on legitimate online data storage and distribution services and websites. Often, the victim or law enforcement would contact the data storage service provider, and LockBit would lose access to the data they worked so hard to steal. To alleviate the issue, LockBit began uploading data to its own data leak site, eliminating the need to rely on third-party services.

"Help Wanted, Apply Within"

Despite all its features and user-friendly integrations, the significant aspect of LockBit's makeover was its effort to market and build its brand. In reality, LockBit Red was simply an update to the ransomware services offered through the RaaS. However, with its release, the LockBit gang conducted a strong marketing campaign to get people talking about them. With the new update and associated propaganda, criminals, security researchers, and

the news media posted content about the gang and its operation. When it was all said and done, the gang significantly increased its criminal credibility and attracted new experienced affiliate hackers to help drive their criminal enterprise.

Access Brokers

One problem all ransomware attackers must address is gaining access to a target's environment. Historically, ransomware gangs needed to conduct the initial breach themselves or rely on affiliate hackers. Additionally, the initial access phase of the attack is one of the most cumbersome and time-consuming phases. Criminals saw this as an opportunity to make money and began a new criminal business model acting as "access brokers," who would obtain and sell access directly into victim environments.

Access brokers spend their time conducting stealthy attacks to bypass an organization's security defenses and gain access to their internal network and systems. The hard part of this type of attack is not the initial breach. You see, many tools and resources exist, making this task easier than you might think. However, gaining admission without anyone noticing and maintaining entry is far more difficult. Due to this, access brokers can charge a hefty fee for their services.

Insider Threat

While purchasing access saved time, the cost came directly from LockBit's bottom line, eating into profit. As part of their LockBit Red campaign, LockBit devised a new tactic to reduce cost. Rather than pay access brokers, LockBit attempted to directly recruit employees of the potential target organization to provide inside access to their environments for a monetary reward.32 If successful, LockBit could reduce costs while bypassing much of the time and effort necessary to compromise targets. Additionally, by using an insider, LockBit could decrease the chance of identification since an insider could provide legitimate credentials and entry to the organization's infrastructure.

How to NOT handle a ransomware attack

LockBit's insider threat campaign appeared to pay off in **July 2021**. With the new software, infrastructure, and supporting staff, LockBit conducted an attack against one of the largest global IT consulting companies, **Accenture**.[33,34] To facilitate the operation, LockBit claimed to gain access to Accenture's environment with the help of an insider,[35] resulting in the theft of 6TB of data.[36] Shortly after, news of the attack began to circulate. Initially, Accenture was slow to acknowledge the breach, and when it did, the firm said it was an isolated incident and did not expose customer data. There was one problem, however. LockBit posted the stolen data, which Accenture claimed did not exist, to their auction site, threatening to sell it to other criminals or leak it online if the consulting firm did not pay a $50 million ransom. Making the situation worse, in an interview with *Bleeping Computer*, LockBit claimed the stolen data included information it could use to gain access to other Accenture customers.[37]. The gang also claimed they had already used information taken from the stolen data to breach an airport that utilized Accenture's software.[38] LockBit and Accenture had very different stories.

Someone was not telling the truth.

One month later, in **August**, **two airlines**, one in Egypt and another in Bangkok, fell to ransomware attacks conducted by the LockBit gang. Both were customers of Accenture. Nothing is **worse than lying about a breach leading to the theft of your customer's data**. In reality, LockBit likely oversold the magnitude of the attack, and Accenture significantly downplayed what took place. Months later, Accenture would despairingly provide additional details submerged within their Annual 10-K report required by the US Securities and Exchange Commission (SEC).[39] In the report, buried under financial performance data, Accenture admitted the breach took place, and that data was stolen and leaked, which could impact their customer base moving forward.

"To date, these incidents have not had a material impact on our or our clients' operations; however, there is no assurance that such impacts will not be material in the future, and such incidents have in the past and may in the future have the impacts discussed below."[40] — Accenture

Falling victim to a ransomware attack is not something an organization should be ashamed of. With today's advanced and creative attackers, almost anyone can become a victim. However, how you handle the incident says a lot about your organization and its culture. Nothing is worse than denying an incident only to have the attacker post contradicting evidence publicly. In this incident, Accenture walks a fine line where they don't tell the complete truth, but they also don't outright lie about what happened. Instead, they provide vague details about the incident and then launch a PR campaign to control the story to make the loss appear less significant. In these situations, the stockholders and the victim organizations' customers lose the most.

In **October 2021**, LockBit introduced a new variant of their ransomware. Previously, ransomware could encrypt only data on Microsoft Windows-based systems. This posed a problem for attackers in large corporate environments running other systems, such as Linux-based platforms that run virtual systems. The new variant was the first version of LockBit ransomware developed as a Linux encryptor purposed to compromise VMware ESXi virtualization platforms. LockBit officially named the release "**LockBit Linux-ESXi Locker version 1.0**."[41,42]

The following month, **November 2021**, **BlackMatter**, another prominent RaaS provider linked to the former DarkSide ransomware gang, announced it was **shutting down its operation**. At that time, BlackMatter had a strong working relationship with LockBit and pushed its affiliates to transition to LockBit's operation in preparation for BlackMatter's closure. Further, BlackMatter directed its most recent victims to LockBit's chat portal to continue the negotiation process.[43] With victim data and seasoned affiliates transitioning over to LockBit's operation, the gang certainly benefited from BlackMatter's downfall. Additionally, while unknown at the time, LockBit recruited one of BlackMatter's most vital resources: its developer.[44]

The Smear Campaign

In addition to BlackMatter's exit, the notorious ransomware gang REvil also briefly ceased operations in the latter half of 2021 and then returned at a limited capacity, leaving many affiliates looking for employment. REvil had been the top ransomware gang within the RaaS community for some time before its downfall. When REvil's issues began, LockBit strategically launched a smear campaign across one of the most popular criminal forums. LockBit directly challenged REvil on several issues. LockBit could have presented these comments and questions to REvil directly in a private conversation but instead chose to challenge REvil in front of the entire criminal community. I believe LockBit engaged REvil to tarnish its reputation in front of other ransomware criminals. This

is an important part of this story because it shows the strategic steps LockBit took to climb to the top. LockBit took a move straight out of the Russian government's playbook and spun its false narrative around legitimate information to discredit its competition. Next, let's take a closer look at LockBit's slander campaign against some of its competing criminal gangs between August 2021 and January 2022.

The Baby Killer Incident

I think it's fair to say most criminals are not known for their ethics. Still, even for criminals, certain crimes are viewed poorly, such as crimes that harm children. LockBit especially understood this, and when a ransomware attack on a US hospital resulted in the death of a baby,[45] it seized the opportunity to discredit its competitors. On a popular criminal forum, a user posted a link to a legitimate news article detailing the infant's death, which can be seen in Figure 10.

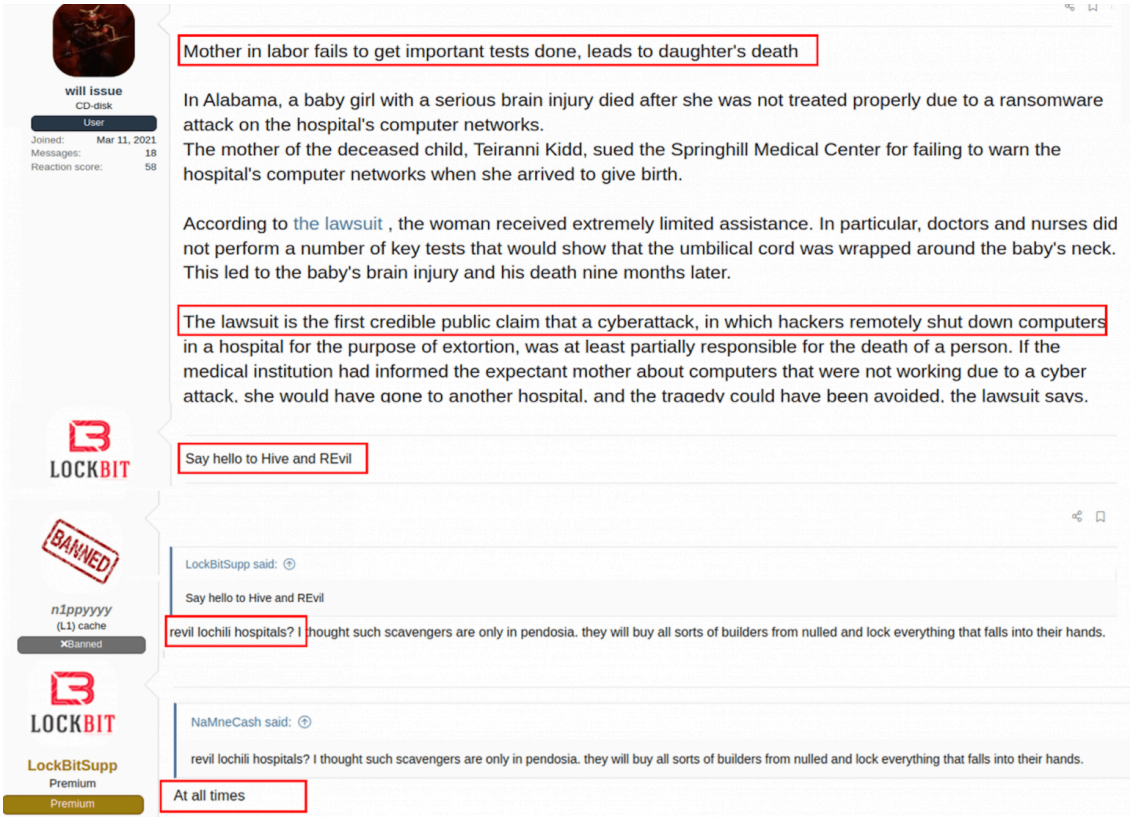


Figure 10: LockBit claiming REvil is associated with a ransomware attack that resulted in the death of a baby

In the post, LockBit insinuated REvil or Hive was behind the ransomware attack. It is a good story and easy to point the finger since both REvil and Hive have previously attacked hospitals, making the accusation plausible. However, there is no evidence or claim that either gang had anything to do with the attack. Neither the news reports nor the official court documents mention REvil or Hive ransomware.

However, they do state that the attack took place using Ryuk ransomware, which Wizard Spider controls. Further, despite LockBit's claims, it also targets healthcare organizations, but LockBit left that part out. It annoys me that LockBit frequently tells the media and criminal community that it does not target healthcare-related organizations like hospitals. Their data auction site has many examples which contradict its claims.

LockBit, no one likes a hypocrite.

Has anyone seen my keys?

The baby killer posts were just one part of a larger smear campaign. Another occurred after the major attack against Kaseya, an MSP software provider, which resulted in over 1,500 companies becoming infected with REvil ransomware.[46] Many of the victims involved in the attack avoided ransom payments and decrypted their data for free after allegedly receiving the decryption key directly from the FBI.[47] LockBit asked REvil how the FBI obtained decryption keys related to the Kaseya MSP incident. REvil responded that someone hacked their server and stole the keys necessary to decrypt victim data. LockBit then provided its scenario, insinuating that REvil, who used the alias 0_neday on the criminal forum, was not only lying but that they were compromised and cooperating with the FBI and referred to REvil as "snitches."

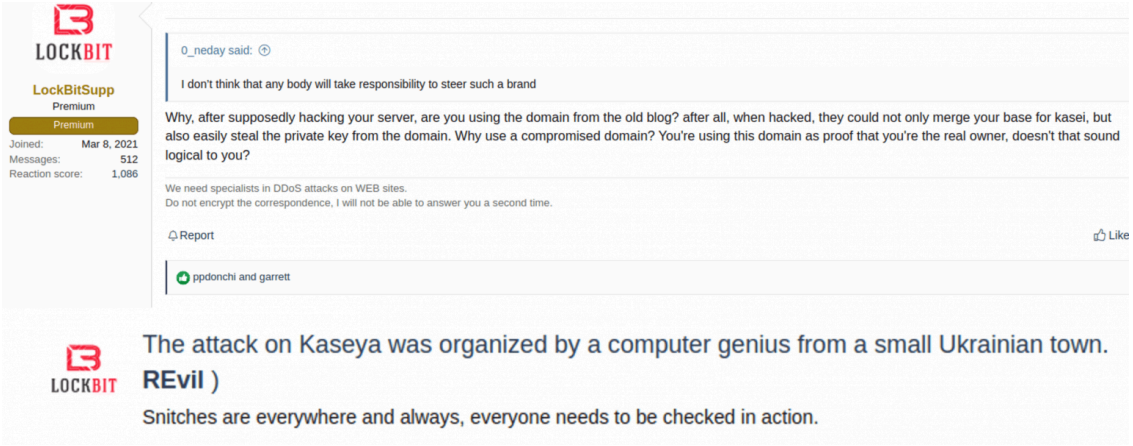


Figure 11: One of several posts challenging REvil and questioning their decisions and loyalties

While I believe the US government did hack REvil to obtain the decryption keys, I do not believe REvil cooperated or had any association with the FBI. Why would they? REvil had nothing to gain by doing so and, at the time, had little to fear in regard to arrest.

Slide into Your DMs

In another post, which took place shortly after several REvil members were arrested in Russia, LockBit posted a private conversation between themselves and a senior leader of REvil. The conversation included details of concerns about the United States and its campaign to bring down REvil members. LockBit tried to use this as evidence that REvil worked and cooperated with the FBI. Figure 12 is the introduction LockBit posted to the forum, which accompanied the leaked private conversation.

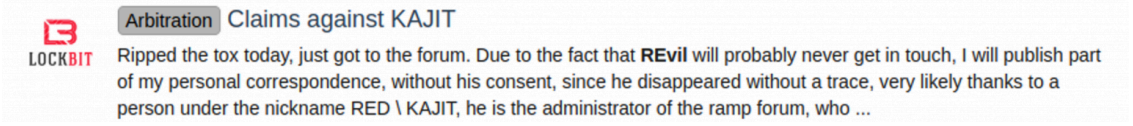


Figure 12: LockBit post of a private conversation between them and REvil

The private conversation LockBit posted is too long to show here, but it did not prove Lockbit's claim. Again, this is another example in which LockBit released sensitive information and added its own self-supporting narrative.

There is no way to validate how much of what LockBit claims is accurate; however, the continued propaganda released over 2021 and in the beginning of 2022 certainly worked in LockBit's favor. I chose to focus on REvil and Hive in these examples, but LockBit uses the "smear campaign" tactic often against any ransomware gang they feel threatens its dominance in the criminal community. **This type of betrayal is rarely done among other ransomware criminals and highlights Lockbits insecurities.** For this reason, I believe LockBit's motivation is not only financial but also personal. LockBit had already acquired great financial wealth but still felt the need to spend the time and energy posting misinformation and complaining about their competition.

PART III: Nothing can stop me now!

With new malware, resources, and infrastructure, LockBit's RaaS was one of the more attractive options to affiliates than many of its peer ransomware gangs. Still, one gang, who operated the Conti ransomware RaaS, seemed untouchable, even to LockBit. With their new branding and ransomware resources, LockBit grew its operation, yet the top-tier affiliates at the time supported the Conti ransomware operation responsible for many high-profile attacks.

As 2022 began, the REvil gang's demise continued, resulting in the arrests of many of its members.[48] Still, despite all LockBit's efforts, Conti continued to rise to the top, becoming the most dominant gang in the underground ransomware ecosystem. However, in February 2022, an opportunity unexpectedly presented itself. Russia began military operations to invade Ukraine and overthrow its government. The war posed a problem for ransomware gangs, which relied heavily on their affiliate partners. Many top affiliates lived and worked in Ukraine, executing ransomware attacks in which they partnered with Russian-based ransomware gangs. Conti must have forgotten this because shortly after the war began, the gang posted the following pro-Russia message to their website:

"The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructure of an enemy." — Conti Ransomware Gang

Posting this message was idiotic. I still have difficulty believing Conti did not realize the backlash this would cause. Surely, if I knew many of the world's best cyber hackers who support ransomware were Ukrainian, Conti also had to know. I'm not sure if they were really that stupid or were more concerned about the Russian government's perception of Conti's cooperation with Ukrainian nationals. Whatever the reason, affiliates, cybersecurity researchers, and even LockBit took notice. LockBit quickly leveraged Conti's mistake and posted the following message to its own site's "press release" section, announcing they had no political agenda and were all about the money.

"For us, it is just business, and we are all apolitical. We are only interested in money for our harmless and useful work." — LockBit Ransomware Gang[49]

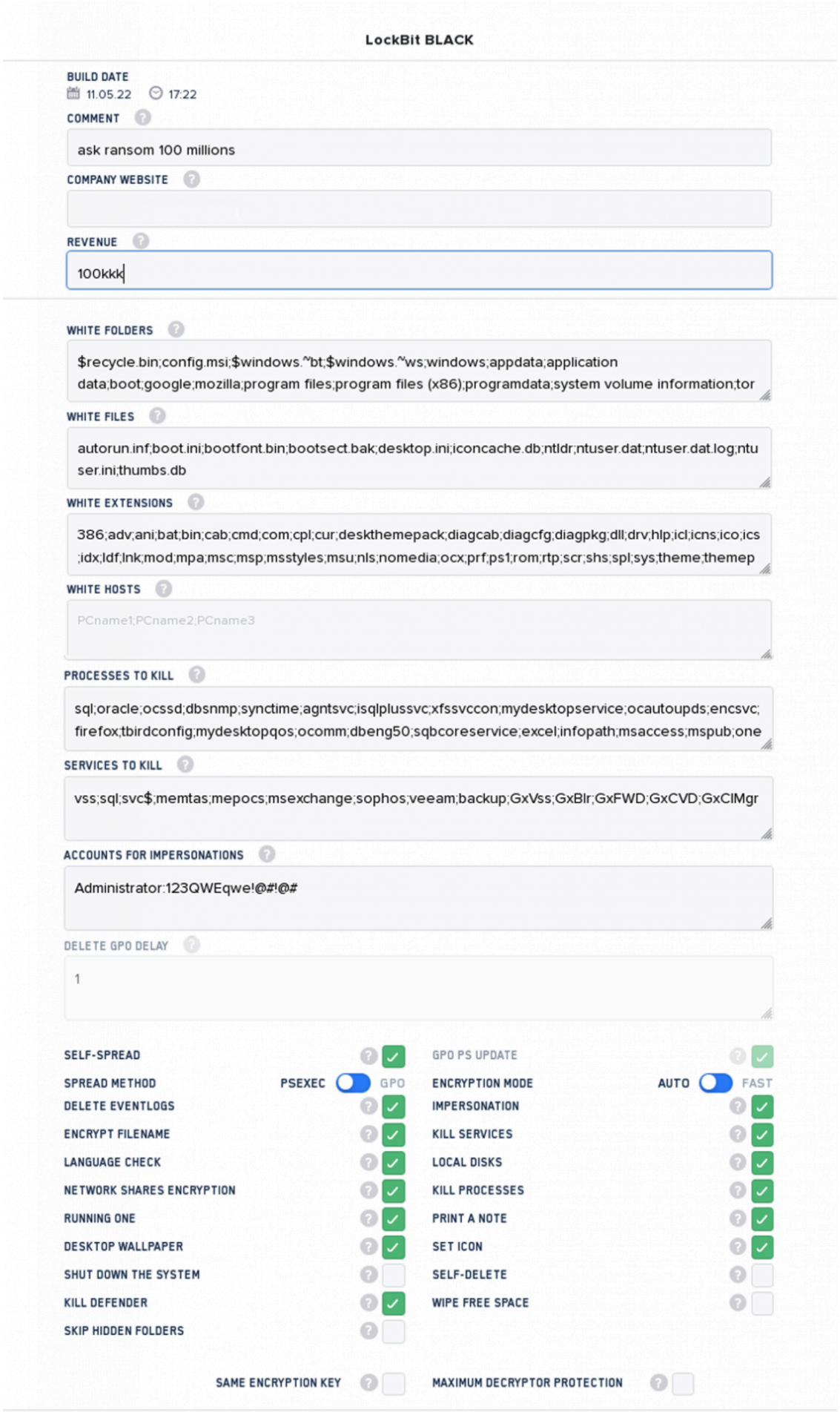
Taking a neutral stance was smart. The Conti gang alienated itself from many of its partners by making a divisive political statement and putting itself in the crosshairs of every pro-Ukraine hacker on the planet. It did not take long to see the effects of the backlash. On February 27, 2022, a security researcher from Ukraine leaked Conti's internal data surrounding its operation. The researcher obtained the data from Conti's internal servers.[50] The

impact of the leaks certainly affected Conti's operation.[51] The leaked data included chat logs between Conti's criminal employees, operational documents, and source code for their ransomware builder, encryptor, and decryptor.[52] All of this contributed to their operation ending in mid-May 2022.

The Black Album

Conti may have felt pressure to close its operation due to these circumstances. Additionally, it received much attention after it took down most of Costa Rica's government with a massive ransomware attack in 2022 just before their exit. When Conti left, it went out on top, with years of attacks and an enormous operation that employed many criminals who partnered or worked with the gang. LockBit's time had come, and the gang needed to find a way to rise to the top or find itself surpassed by one of its many criminal competitors. How would LockBit accomplish this?

The answer came the following month, in **June 2022**, when LockBit officially announced another major release of their ransomware, which they referred to internally as **LockBit Black** (publicly known as LockBit 3.0). I originally heard about LockBit Black in April 2022 when the gang first began to beta-test it with a small number of affiliates. At the time, the leader of LockBit and I were taking part in "Trafficked," an investigative TV show that focused on cybercrime (can't make this stuff up!). The episode will air in early 2023, but surprisingly, during the interview, LockBit shared screenshots of the updated management console. Additionally, he discussed many of LockBit Black's new features. Figure 13 displays the LockBit Black management console as the attacker would see it when managing a LockBit ransomware attack.


LockBit BLACK
BUILD DATE
11.05.22
17:22
COMMENT
ask ransom 100 millions
COMPANY WEBSITE
REVENUE
100kkk
WHITE FOLDERS
$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;appdata;application data;boot;google;mozilla;program files;program files (x86);programdata;system volume information;tor
WHITE FILES
autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db
WHITE EXTENSIONS
386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;dll;drv;hlp;icl;icns;ico;ics;idx;ldf;lnk;mod;mpa;msc;msp;msstyles;msu;nls;nomedia;ocx;prf;ps1;rom;rtp;scr;shs;spl;sys;theme;themep
WHITE HOSTS
PCname1;PCname2;PCname3
PROCESSES TO KILL
sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;tbirdconfig;mydesktopqos;ocomm;dbeng50;sqbcoreservice;excel;infopath;msaccess;mspub;one
SERVICES TO KILL
vss;sql;svc$;memtas;mepocs;msexchange;sophos;veeam;backup;GxVss;GxBlr;GxFWD;GxCVD;GxCIMgr
ACCOUNTS FOR IMPERSONATIONS
Administrator:123QWEqwe!@#!@#
DELETE GPO DELAY
1
SELF-SPREAD
SPREAD METHOD
PSEXEC
GPO
DELETE EVENTLOGS
ENCRYPT FILENAME
LANGUAGE CHECK
NETWORK SHARES ENCRYPTION
RUNNING ONE
DESKTOP WALLPAPER
SHUT DOWN THE SYSTEM
KILL DEFENDER
SKIP HIDDEN FOLDERS
GPO PS UPDATE
ENCRYPTION MODE
AUTO
FAST
IMPERSONATION
KILL SERVICES
LOCAL DISKS
KILL PROCESSES
PRINT A NOTE
SET ICON
SELF-DELETE
WIPE FREE SPACE
SAME ENCRYPTION KEY
MAXIMUM DECRYPTOR PROTECTION

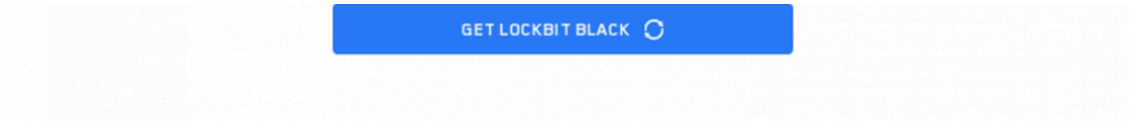


Figure 13: LockBit Black management console

Often, criminal gangs use their ransomware and resources to conduct attacks and provide small updates as necessary to stay ahead of security vendors. However, LockBit is not one of them. Unfortunately, ransomware and resource development are areas in which LockBit excels. As shown in Figure 13, LockBit Black improved on LockBit Red and added several new features, making it even easier for criminals to conduct attacks.

Additionally, LockBit added several other components to its program, such as additional mirror sites to enhance its infrastructure, making it harder for law enforcement or government agencies to interrupt its operation. LockBit also started a "bug bounty program," offering researchers a monetary reward if we could identify vulnerabilities or development errors in its ransomware. This was especially important after Microsoft's DART team identified a flaw in LockBit ransomware, which they referred to as "buggy code." The bug allowed Microsoft to restore encrypted data associated with MSSQL database files.[53] LockBit's bug bounty program description, as seen on its website, is shown in Figure 14.

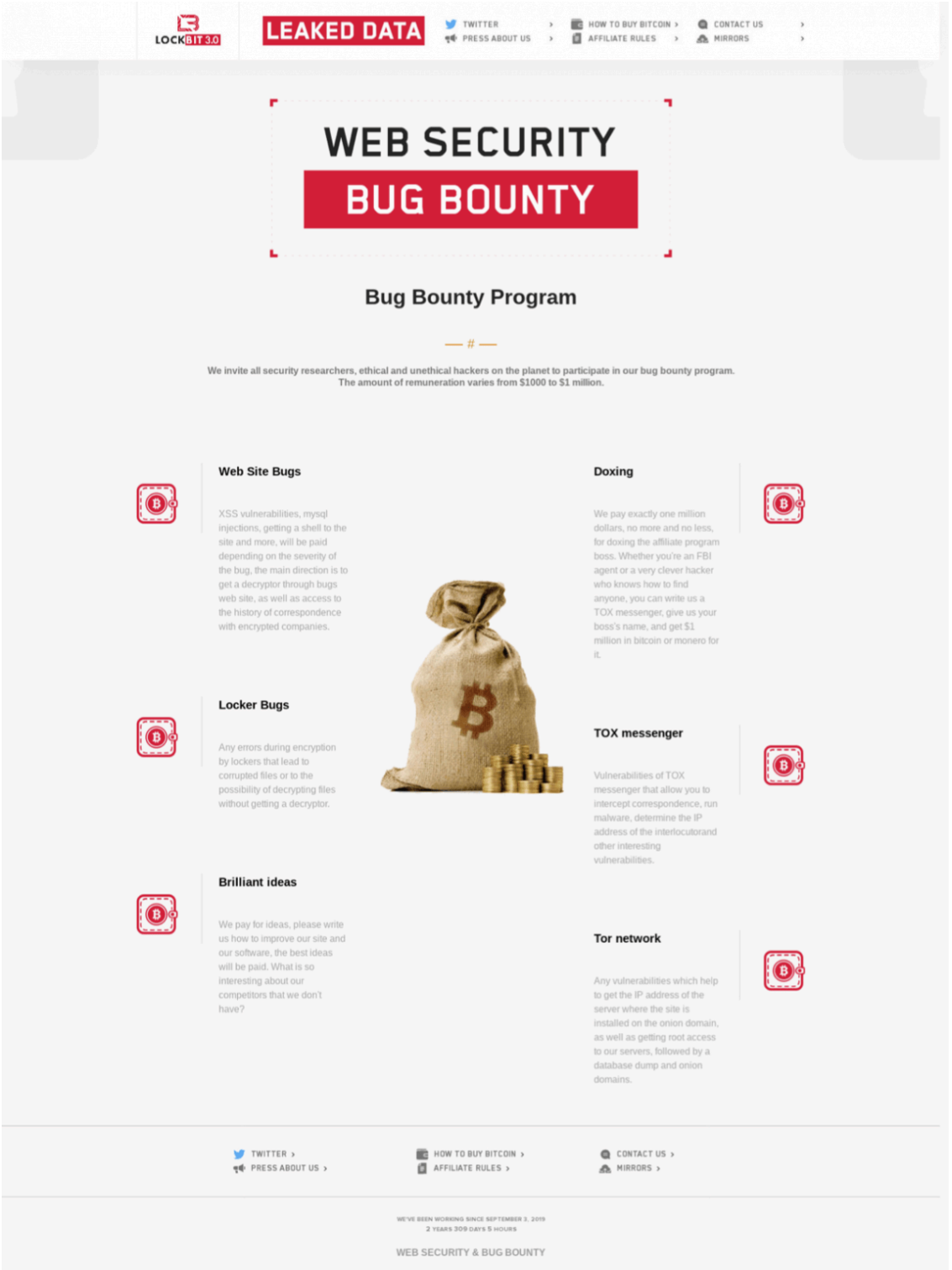


Figure 14: Bug bounty program details posted to LockBit's website

Like LockBit Red, LockBit Black opened with a new recruitment effort, which conveniently began near the time Conti shut down its operation. The affiliate recruitment campaign was a success. Within a month of opening its newly updated ransomware program, LockBit had conducted its highest volume of attacks, far surpassing its competition, making it the most active ransomware operation in the world, finally.

LockBit did not just take first place, statistically; it dominated the ransomware scene. One month after the new program began in July, LockBit conducted 61 attacks.[54] That's nearly two attacks a day. I don't have metrics on

the ransom amounts paid that month, but with such a high volume of activity, LockBit likely had the most lucrative operation. The next closest group, BlackBasta, which is believed to be an evolution of the Conti gang, conducted 35 attacks.[55] In my opinion, LockBit's payment model, putting the affiliate in control of collecting and distributing ransom payments in addition to their "easy to use" feature-rich ransomware management panel, was the key to its success. Other additions to its program included an updated ransom note, wallpaper, and infrastructure. Additionally, LockBit added Zcash as a payment option for its victims.

A Behind-the-Scenes Look into the Making of "The Black Album"

This is where things got interesting. To tell this part of LockBit's story, I need to explain the background of several other ransomware gangs. In August 2020,[56] the REvil ransomware gang helped one of their affiliates, at the time, stand up their own ransomware operation, known as DarkSide. The DarkSide ransomware gang is famous for committing one of the dumbest attacks of all time against the Colonial Pipeline.[57] After the attack, when gas stopped flowing across the east coast of the United States, the US government engaged many of its cyber resources to address the attack and the criminals behind it. As a result, in May 2021, DarkSide closed its operation, leaving some of its criminal partners unpaid for their work.

DarkSide was the target of both the US government and now criminal hackers to whom it owed money. Both are reasons DarkSide tried to go unnoticed when they began new ransomware operations only two months after retirement in July 2021. To go unnoticed, the gang rebranded itself as "BlackMatter" and used a new ransomware payload to conduct attacks.

For this reason, when BlackMatter began operations in July 2021, the individuals behind it hid that they were originally the Darkside gang. However, researchers quickly identified the use of the same code routines seen in both DarkSide and BlackMatter ransomware, indicating a link existed between the two.[58] As news traveled criminals posted to forums and markets discussing the connection and their distrust of the gang. Finally, in early November, things became too hot to handle for BlackMatter who posted a cryptic message on its site stating that authorities were closing in and some members were no longer available.

***"Due to certain unsolvable circumstances associated with pressure from the authorities (part of the team is no longer available after the latest news) — project is closed." — BlackMatter*[59]**

Still, DarkSide/BlackMatter was not done yet. Once again, just two weeks after retiring the BlackMatter operation, the gang developed new ransomware and started another RaaS program, called BlackCat (aka Alphv).[60] Later, in an interview, a member of BlackCat would confirm the association, though it downplayed how many members of the original DarkSide gang remained.[61]

The point is that all three gangs, DarkSide, BlackMatter, and BlackCat, are the same individuals who rebranded their operations under new names and ransomware. For a group of hackers behind such large-scale attacks, they are not very creative in coming up with new names that are intended to fool the security community. Personally, I am waiting to see what name they use next. If anyone from the gang is reading this, I would like to nominate the name "DarkMatter". No one will ever guess the association!

While the Darkside backstory is interesting, you are probably wondering what this has to do with LockBit. Remember from earlier, when BlackMatter shut down operations, it pushed its affiliates to work with LockBit, demonstrating the two gangs had a good relationship up to this point. However, all good things must come to an end, and in mid-November 2021, LockBit successfully recruited one of the primary developers who supported ransomware development for both DarkSide and BlackMatter ransomware operations.

The leadership within BlackMatter felt LockBit poached their developer, which it did, causing bad blood between the gangs. This became apparent in conversations between the two within the criminal forum seen in Figure 15.

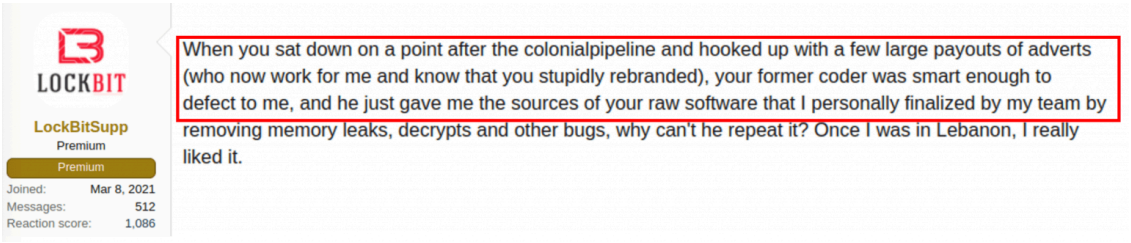


Figure 15: Conversation with BlackCat/Alphv (BlackMatter/DarkSide) about LockBit's relationship with their former developer

Over the next six months, the former BlackMatter developer worked for LockBit to create its new ransomware variant, LockBit Black (3.0). As discussed, the gang officially released LockBit Black in June 2022, and researchers and security organizations quickly began to dissect and analyze its payload. The initial analysis showed several overlaps and similarities between it and BlackMatter ransomware.[62] Keep in mind that the developer's defection to LockBit was publicly unknown at the time. Due to this, many other researchers and I believed that LockBit purchased BlackMatter's source code and used it in the development of LockBit Black.

However, according to LockBit, that is not correct. For reasons I don't really understand, LockBit became upset over the claim that it purchased BlackMatter source code to develop its own ransomware. LockBit went on a rant, threatening the developer and insulting BlackMatter/DarkSide/BlackCat on a criminal forum. In the argument, LockBit threatened the developer indirectly, insinuating he could release information about the developer's past, his current location, and even information about his wife. LockBit also accused the developer of being lazy and an abuser of alcohol and drugs:

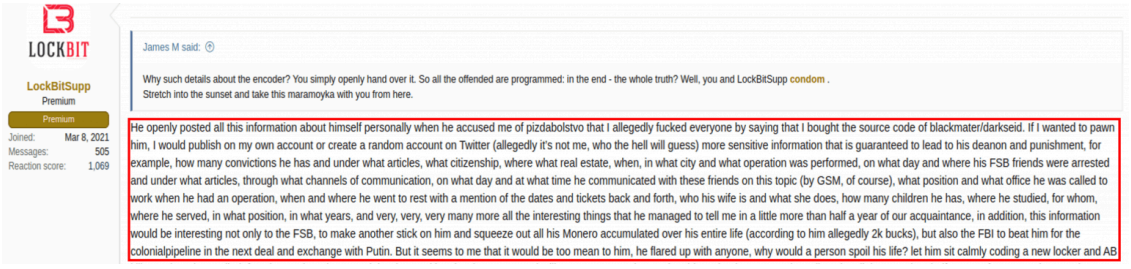


Figure 16: LockBit threatens BlackMatter developer

However, LockBit screwed up. The problem with lying is that you must keep your story straight. In an interview several months before this conversation took place, the cybersecurity outlet Red Hot Cyber (RHC) asked about the LockBit 3.0 project. LockBit responded:

> ***"The source codes of DarkSide/BlackMatter windows locker were bought and significantly improved."***

So, which is it, LockBit? Did you buy the code or did you get it for free? What's more interesting to me is that LockBit feels the need to lie about the topic. At the end of the day, who cares? There are a few possible explanations. First, LockBit lies so often it can't keep its story straight. Second, there are several individuals behind the LockBitSupp persona. Or third, LockBitSupp does not think what it says on the dark web will be known or leaked in the public domain.

In reality, the BlackMatter developer became tired of his original ransomware gang's constant cycle of starting and stopping operations, as well as running from the US government, and wanted to work under a more stable, consistent brand: LockBit ransomware.[63] If only he had known the amount of drama he would have to deal with from LockBit. He would have thought twice about joining the gang if he knew LockBit would post information and harass him and his previous employer all over the criminal forums. Compared to listening to LockBitSupp all day, I bet that quiet prison cell is looking pretty good at this point!

LockBit made one other comment, which is important to disclose. It claimed the developer formerly worked for the cybercrime group known as Fin7, which is a group behind many high-profile banking and financial-crime-related attacks.[64] More importantly, if true, this also provides a common link between LockBit, DarkSide, BlackMatter, BlackCat and Fin7. Further, while outside the scope of this report, Fin7 has also been linked to the BlackBasta ransomware gang, which, if you recall, what I mentioned, has a strong context to the former Conti gang.[65] Again, the ransomware community is much smaller than most people think.

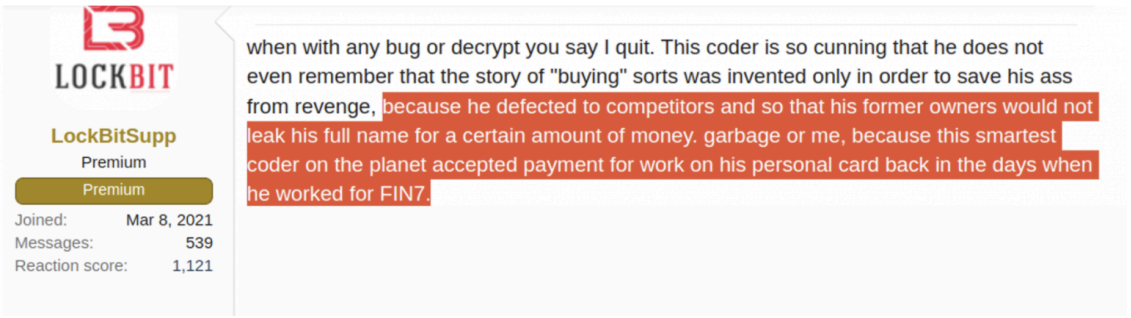


Figure 17: LockBit post linking its developer to Fin7

LockBit also claimed the developer used his personal banking information to receive payment for work he did while working under Fin7. This is vague but would indicate that a financial trail exists which could be used to reveal the developer's actual identity and provide evidence of his involvement in the attacks. However, finding that needle in the haystack would be quite difficult.

Below is a high-level association diagram showing the basic connections between various criminal gangs discussed in this section in relation to LockBit:

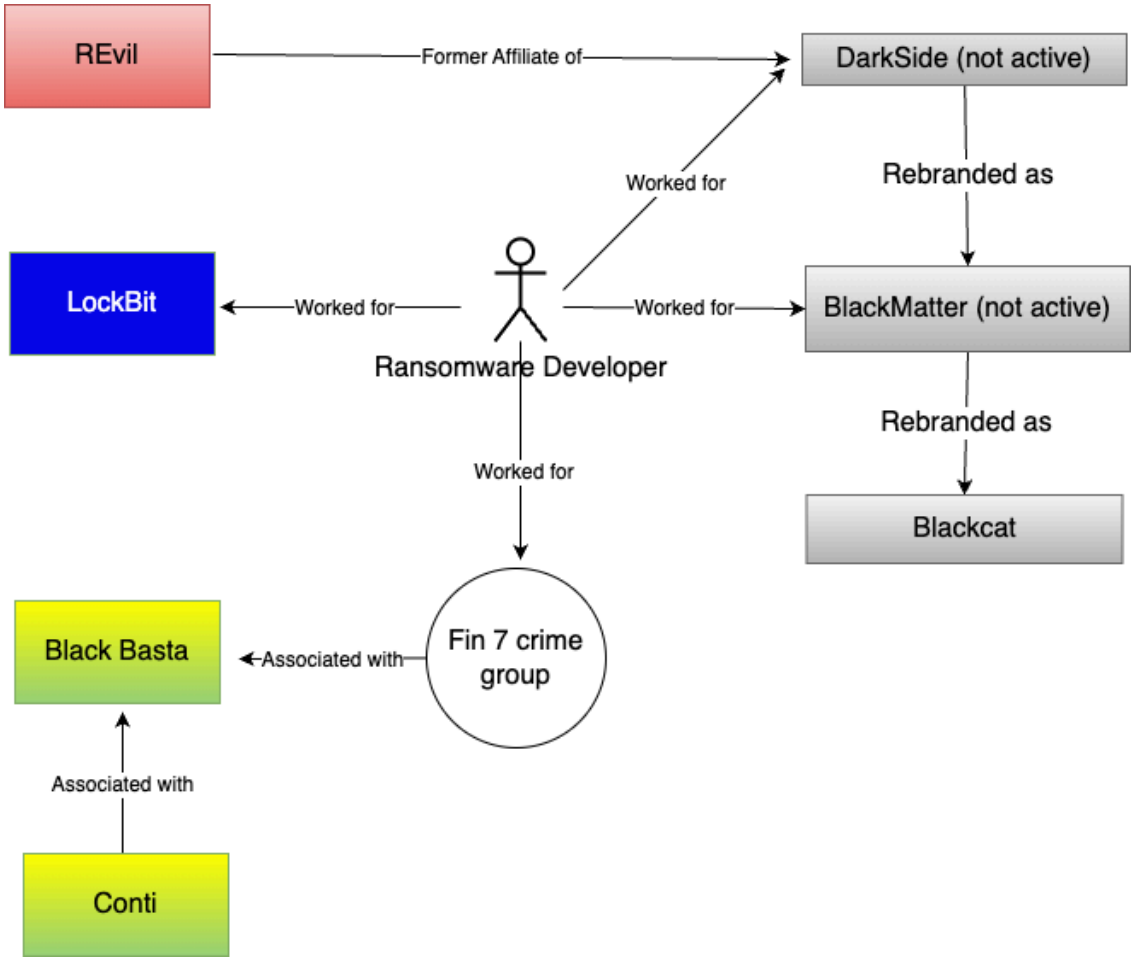


Figure 18: High-level relationships between criminal gangs (do not use for attribution!)

It's important to note that the links and associations I have discussed in this section were to show the behind-the-scenes activity that went into the making of LockBit Black. The associations and activities involving these gangs originate from claims made directly by senior members who run these criminal operations. Many of the claims made can be backed with technical evidence found in each ransomware variant's code or functionality.

Please do not make attribution based on LockBit or other security vendors' findings.

Make attribution based on your own research backed by data and evidence to support your findings. My intent is to tell you the story, originally told by the criminals themselves, from their point of view. Solid attribution with evidence should be used if you choose to repurpose this information for your official attribution.

The Mandiant PR Stunt

In June 2022, the global cybersecurity company Mandiant really, really pissed off LockBit. In a strange turn of events, LockBit named Mandiant as a victim on their data auction site. However, soon, it became clear the breach was not authentic. LockBit had not actually compromised or stolen any of Mandiant's data. As a researcher who follows the gang closely, I felt this tactic seemed out of character for LockBit. You see, at the time of this writing, LockBit has 1,243 victims listed on their website. Remember, this is not even close to a representation of total victims since LockBit removed previous victim data from their site when they shut down LockBit Red and began Lockbit Black. Still, since launching LockBit Black in June 2022, the crime syndicate has compromised over

1,200 victims. In all these attacks, I have not seen another example where LockBit lied about a victim. Usually, the gang is concerned with its image and reputation. So, why would LockBit lie about Mandiant? The answer is *complicated*.

You see, before LockBit's post, Mandiant released a public blog detailing ransomware activity it calls UNC2165.[66] The group UNC2165 is a cluster of ransomware activity they associate with the ransomware gang EvilCorp. Apparently, Mandiant identified EvilCorp conducting ransomware attacks in which they used Lockbit's ransomware to encrypt their victim's data.

Let me explain why this is an issue. In August 2021, I wrote a research paper titled "Nation-State Ransomware."[67] In that report, I mention various links between Russian-based ransomware gangs and the Russian government. One of the links involves an attack against a US defense contractor, which was initially discovered by Prodaft, a cybersecurity company.[68] Prodaft detailed the overlap between the EvilCorp ransomware gang and Silverfish, a Russian government-associated espionage group, which I expand on in my research.[69] This is part of the reason LockBit was concerned about the association Mandiant made. EvilCorp's association with the Russian government attracts greater attention than a lone criminal group.

Making matters worse, in 2018, the US Treasury imposed financial sanctions against EvilCorp, including any individual or entity associated with the gang. The sanctions made it difficult, if not impossible, for a US company to legally pay a ransom demand when the attack is associated with EvilCorp. This was LockBit's largest concern, as their entire operation could be jeopardized if the United States categorized them as an EvilCorp partner. The irony in this story, based on statements made directly from LockBit on a criminal forum, is that the gang did not willingly partner with EvilCorp. Instead, EvilCorp gained access to LockBit's ransomware payload and began to use it without LockBit's consent. LockBit did not willingly agree to the partnership, nor did they want to do business with EvilCorp. Personally, I believe LockBit on this topic, mainly because they have previously tried to distance themselves from political and government-affiliated organizations. Second, this is not the first time EvilCorp has posed as another ransomware gang to avoid sanctions placed against them.[70] Third, LockBit has little to gain and a lot to lose by partnering with EvilCorp. It turned out the entire thing was a PR stunt to make a point that things are not always as they appear. Mandiant was not a LockBit victim, and LockBit was not an EvilCorp partner.

The 0-Day

I have researched a lot of ransomware attacks over the years, and it is extremely rare that I see a cybercriminal use a true, non-disclosed 0-day. However, LockBit is a unique adversary and executed an attack in July, where they exploited a previously unknown vulnerability found on some versions of Microsoft Exchange servers. In the attack, LockBit gained access to two exchange servers running Windows Server 2016 Standard.[71] The exploit allowed LockBit attackers to gain remote access into the victim's environment with escalated privileges, where they stole data and encrypted systems.[72] Using a 0-day demonstrates the capability and access to resources unavailable to most attackers. However, LockBit generates a lot of revenue from extorting its victims and certainly has the capital to buy or pay others to discover unknown software flaws that it can repurpose for its criminal operations.

DELETE_ENTRUSTCOM_MOTHERFUCKERS

Over the summer of 2022, LockBit continued its attacks and listed several other high-profile organizations as victims. Unfortunately, unlike Mandiant, the other companies LockBit named as victims were not part of a PR stunt. LockBit conducted attacks against one of the world's largest technology manufacturers, **Foxconn**, and the security technology company **Entrust**, among many others. Figure 19 shows a portion of the companies on LockBit's data auction site, as seen in mid-August 2022.

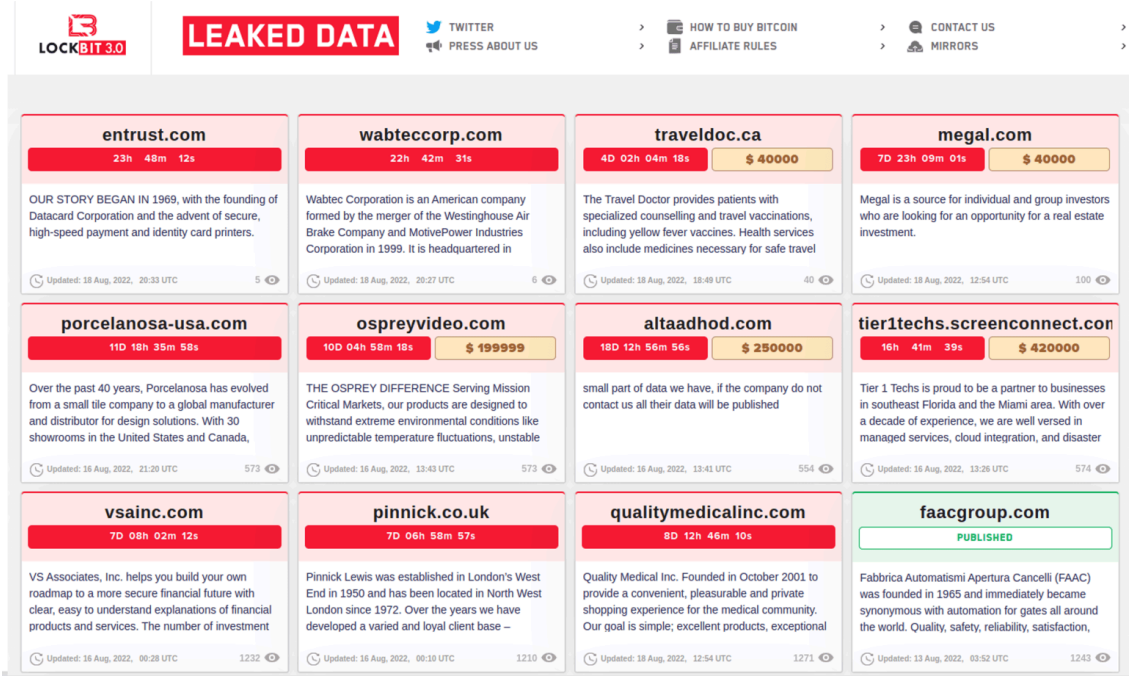


Figure 19: LockBit data auction leak site — August 2022

After LockBit breached Entrust, it claimed to steal over 300 GB of its internal data.[73] However, unlike most companies, Entrust aggressively responded when LockBit threatened to leak their data. Remember, LockBit prefers to leak victim data from its own infrastructure, which they control. So, when it threatened to post the Entrust data it stole, Entrust responded with a denial of service attack, crippling LockBit's infrastructure. For several days, LockBit's data auction site could not be reached. The victim chat portal, hosted on the same server, was also down. Now, LockBit looked foolish and was losing money. They finally got a taste of their own medicine. Well played, Entrust!

Entrust's response clearly frustrated LockBit. on August 23, 2022, LockBit made the below statement about the situation:

LOCKBIT

LockBitSupp
Premium
Premium
Joined: Mar 8, 2021
Messages: 539
Reaction score: 1,120

Aug 23, 2022 #5

1. What doesn't kill makes you stronger. We strengthen the infrastructure, increase the number of mirrors, duplicate servers, new methods of protection against DDoS.
2. Advise a site where you can order the services of dudosers on these greedy people (or maybe from local who are involved, the site entrust.com), who lit up 5kk and were ready to give only 1kk.
3. No one bought access to them, but was broken by a zero.
4. I upload all their 300GB information in archives to the torrent tracker, soon I will distribute it privately in tox to everyone who wants it, and then I will post the links publicly.
5. The function of randomization of links in the notes of the locker has already been implemented, each build of the locker will have a unique link that the dudoser will not be able to recognize.
6. A system of bulletproof data storage of all companies in the clearnet is being developed, in addition to the torus.
7. I am looking for dudosers in the team, most likely now we will attack targets and provide triple extortion, encryption + date leak + dudos, because I have felt the power of dudos and how it invigorates and makes life more interesting.

Entrust, thanks for the motivation, you make us stronger, and you will remain as a holey and greedy office, in a couple of days the whole world will know all your secrets, if I were you, I would pay before it's too late and destroy your information, because for now no one could download it thanks to dudos.

Figure 20: LockBit response to Entrust DDoS attack as seen on a Russian forum used by cybercriminals

Still, I applaud Entrust's effort and response. Publicly, Entrust acknowledged and notified its customers of the breach.[74] Unlike Accenture, Entrust was transparent about the attack. Many people will likely disagree, but I think the DDoS attack was a brilliant response. For one, it's almost impossible to prove who is behind it from a legal perspective. More importantly, Entrust accomplished something no other victim has achieved. For several days, they brought LockBit's operation to a halt and delayed the exposure of their data. The DDoS attack cost LockBit time and money necessary to stabilize its infrastructure. Further, they refused to pay the ransom, leaving LockBit and its partners unpaid for their time and work. While there are no winners in a ransomware attack, Entrust sent a strong message to LockBit that day, which can be seen in the DDoS attack data itself, shown in Figure 21.

```
127.0.0.1 - - [20/Aug/2022:19:47:49 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
```

Figure 21: Entrust/LockBit DDoS attack data[75]

The lesson here is if you target Entrust, Entrust will target you!

While the response was admirable and certainly sent a message to LockBit, there was a downside. LockBit saw the impact of the attack on their own operation and decided to add DDoS attacks to their attack playbook. Despite LockBit's threats, it has used DDoS as a third form of extortion very sparingly. Remember, LockBit is not conducting the attacks; their affiliate partners are. Affiliates are not going to conduct a DDoS unless they need to. LockBit wants the tactic used to make a point, but affiliates simply want to get paid.

While LockBit credited Entrust for giving them the idea, this was simply a ploy to blame them for the attack technique. You see, SunCrypt, another ransomware gang, used the DDoS tactic as a form of extortion back in 2020, when the two criminal organizations played nice with one another as part of the pretend cartel.[76]

Still, I learned something about LockBit when it fell victim to Entrust's DDoS attack. Apparently, they are not very good at distributing data outside of their own infrastructure. You see, when LockBit realized they were now the victim of a DDoS attack and its infrastructure was down, it threw the equivalent of an online tantrum, threatening Entrust, and then began to post links where it publicly posted its data.

Here is a **timeline of events**:

- **June 18, 2022 —** Entrust attack first reported publicly77
- **June 19, 2022 —** LockBit posts the negotiation chat log to their data leak site, making the private conversation public to pressure Entrust into paying the ransom. This is the first time LockBit published victim negotiations.78 While it was speculated at the time that this was a new tactic that LockBit would continue to use, this appears to be an isolated incident.
- **~August 20, 2022 —** LockBit begins to leak Entrust data on its data leak site
- **~August 21, 22 2022 —** DDoS attack shuts down LockBit infrastructure79
- **August 24, 2022 —** Entrust data is posted to a popular criminal forum known as "Breached" (breached[.]vc / breached[.]to) by a user named "LockBit." The filenames and directory structure were uploaded to match the data previously seen in the original leak posted to LockBit's infrastructure. Strangely, the contents of the files could not be validated since many of the file archives were corrupt. I initially assumed the post was from the authentic LockBit ransomware gang. However, after thinking the data was not from the Entrust breach, it seemed the upload may have been from someone else claiming to be LockBit. But why? What would anyone gain from posting irrelevant data with the same filenames and directory structure as the real thing? This did not make sense.
- **August 25, 2022** — LockBit claims the leak on the Breached forum was fake
- **August 27, 2022** — LockBit posts Entrust data across three publicly available data-sharing websites. Each link directs the user to a torrent allegedly comprised of Entrust data. However, once again, the data is corrupt.
- **~August 28, 2022** —LockBit's infrastructure is back online, signaling the end of the DDoS attack. Entrust data is once again available for download directly from LockBit's infrastructure.
- **August 29, 2022** —LockBit claims they identified and fixed the issue causing data corruption within the file archives

Once the data became available on LockBit's infrastructure, both researchers and cybercriminals compared the data from the initial release on the Breached forum, the torrent release on public infrastructure, and the data posted to LockBit's website. While much of the data from the earlier attempts was corrupt, a limited sampling of the data could be validated against the final release of authentic Entrust data stolen. It was, in fact, the same. Since the data was the same, and LockBit claimed the breached release was fake, I first questioned if LockBit could have an insider releasing data on their own. I was not the only person who thought something was wrong. You can see in the below thread LockBit claiming the data was fake and discussing how it may have ended up on the Breached forum:

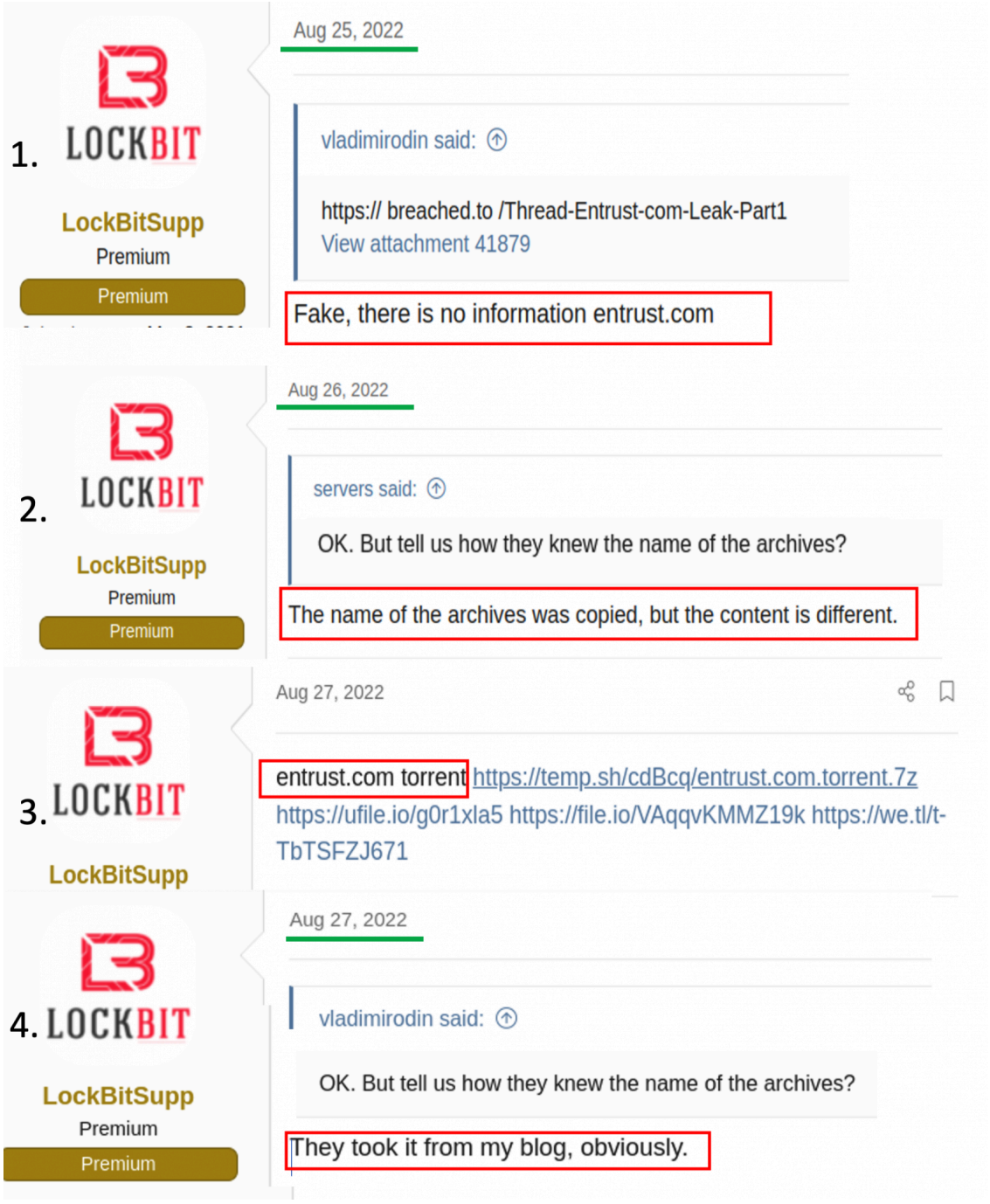


Figure 22: LockBit claims Breached forum post of Entrust data is fake

I know it was you, Fredo.

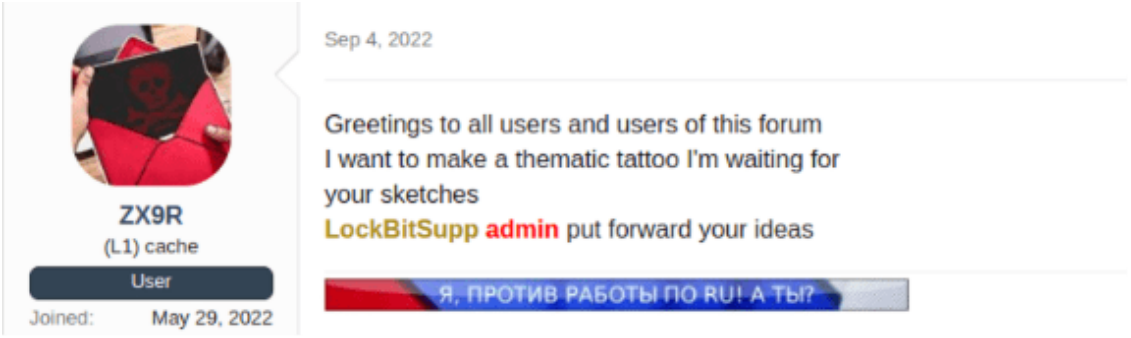
LockBit claimed someone took the data from its initial post on the data leak site. However, I could never access the data until after the DDoS attack and could not validate if it was previously accessible. If so, this would explain how the data was posted to Breached. Other criminals also questioned LockBit and claimed the data was never available before the DDoS attack. In my opinion, there is no insider threat. LockBit themselves posted the data to Breached and then realized it was corrupt and struggled to correct the issue. Apparently, even LockBit has tech problems sometimes! After failing several times to correct the compression issue, LockBit knew it would look foolish after making such a spectacle about its revenge for the DDoS attack. So, to avoid looking incompetent, it

claimed the data was fake and had been uploaded by a fraudulent third party. I don't think so. **I know it was you, LockBit!**

Do you like my tattoo?

You might think after the very public Entrust debacle, LockBit would give its PR campaign a break and just focus on its operation, but you would be wrong. In early September 2022, a member of the Russian forum LockBit frequents began a thread asking for suggestions for a "thematic tattoo" and tagged LockBit in the post. LockBit replied, offering to pay anyone who tattooed the LockBit name and logo on their body. The tattooed individual simply needed to post proof of the tattoo to collect payment. No one would tattoo a ransomware gang's name on themselves, would they? Apparently, there are lots of stupid people in the world who will do anything for money. The LockBit circus was in full effect.

Soon, posts on social media began to appear, and a list of BTC wallets with images of tattoos and videos was shared on GitHub, as well as the underground forum where LockBit initially posted.[80,81] Below is part of the conversation and a sampling of images submitted as evidence for payment from LockBit groupies:



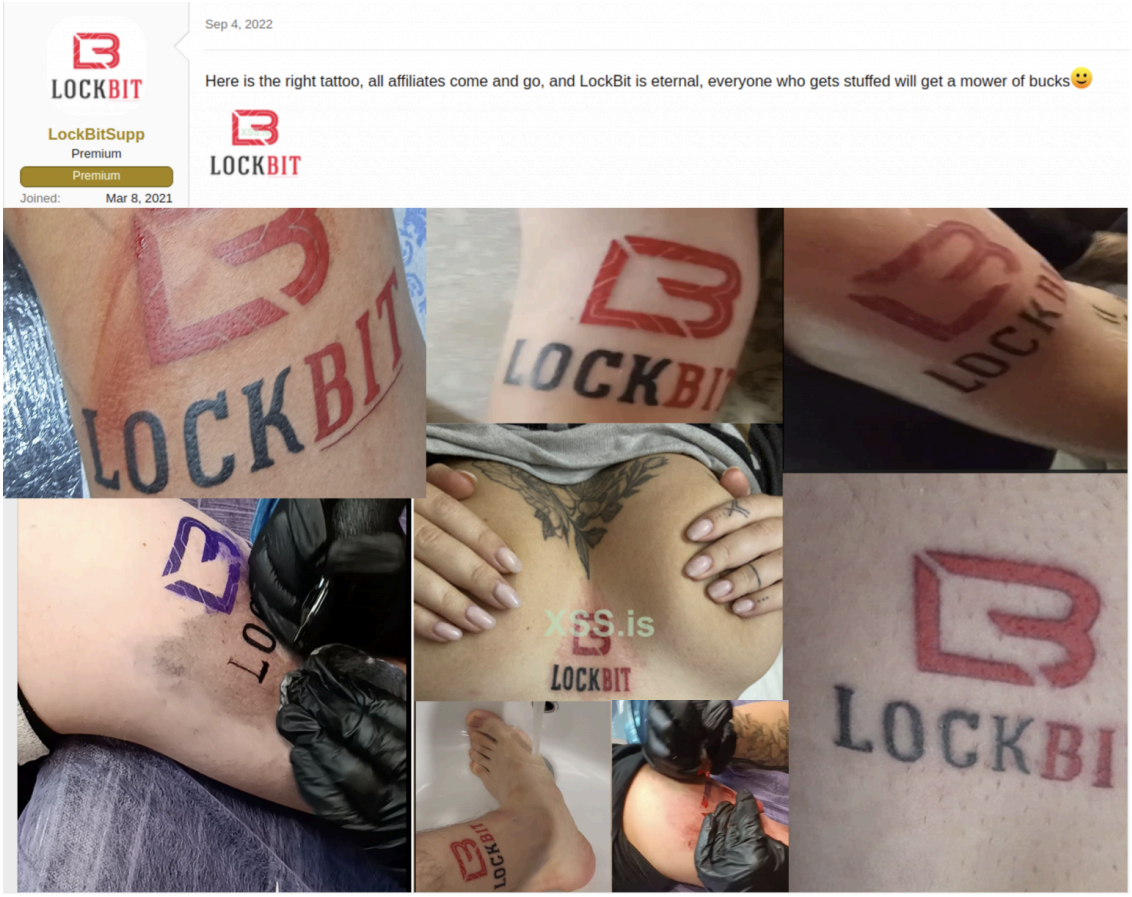


Figure 23: LockBit tattoo convo and groupie tattoos

I don't think LockBit initially planned this as a PR stunt, because they did not start the forum thread but instead responded as a joke to the person who made the initial post. However, once people posted images and videos to social media, showing themselves getting the LockBit tattoo, the press began to publish articles about the event. Soon, what started as a simple comment on a forum was a major public spectacle reported by news organizations worldwide. Suddenly, LockBit needed to pay up, which they did for the most part.

The Drunken Developer

To say the least, September was an interesting month for LockBit. On September 21, 2022, as the buzz from the tattoo contest began to subside, an unknown persona with the alias "Ali Qushji Crew" made a bold claim on both Telegram and Twitter:[82]

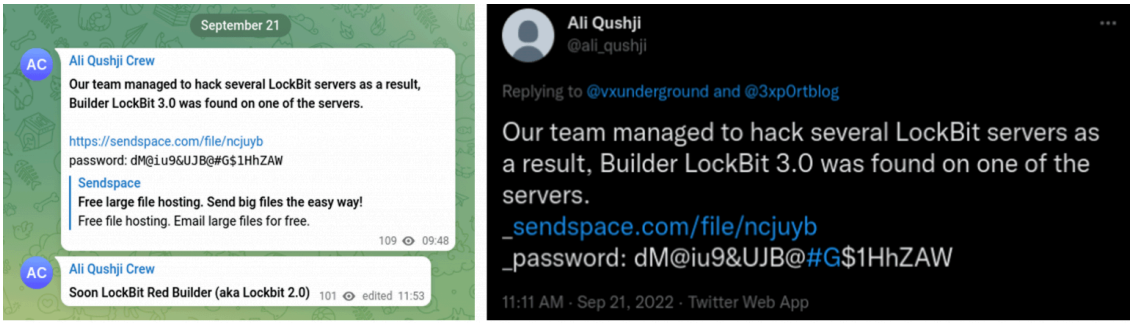


Figure 24: Telegram post and tweet from someone claiming they hacked LockBit

According to the persona, they had hacked LockBit's infrastructure and stole its ransomware builder source code, which they made available to download using the supplied password. This is significant since the builder creates the LockBit ransomware payload used in attacks. Once made public, anyone can use it as they see fit. Shortly after the tweet, a cybersecurity researcher based in Ukraine, @3xp0rt, uploaded the files to GitHub, making them available for anyone to analyze.

The strangest part of the incident is not the leak but the story surrounding it. You see, Ali Qushji and its associated team did not hack LockBit infrastructure or steal the builder as claimed. Instead, Ali Qushji and the hacking tale were created to provide plausible deniability to the real perpetrator behind the leak. However, while the story and persona were fictitious, the ransomware builder source code leaked was authentic! The obvious question is, if LockBit was not hacked, how did the person behind the leak gain access to the ransomware builder? The answer came from vx-underground:[83]

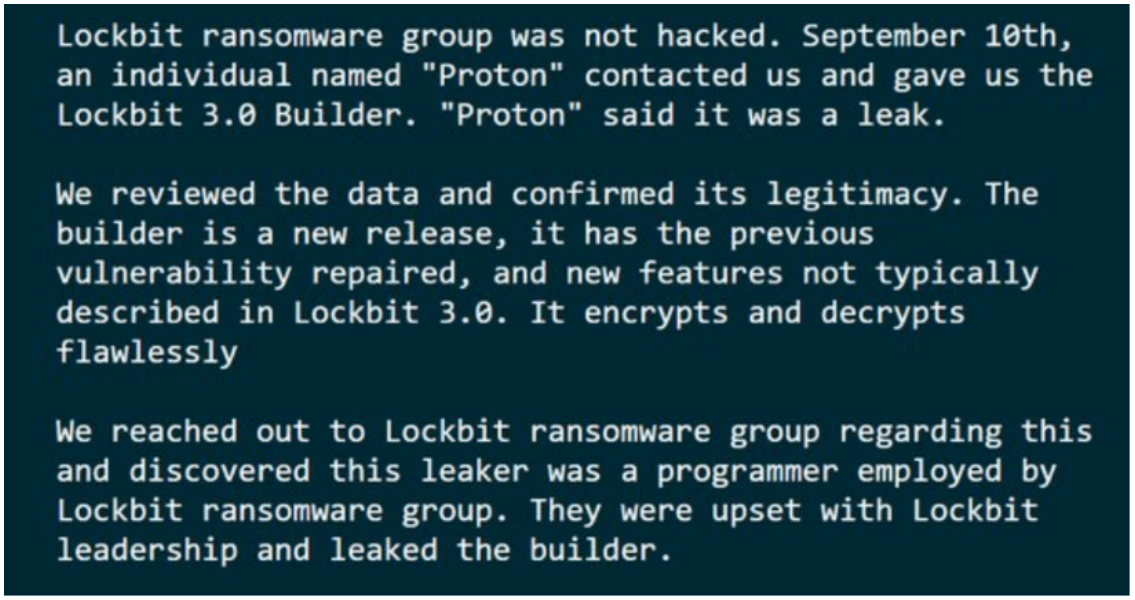


Figure 25: Explanation posted to Twitter explaining the ransomware builder was leaked by an insider and not hacked by Ali Qushji[84]

When the news of the leak became public knowledge, the dark web blew up with chatter across hacking forums and markets. Now we have "Proton," (Figure 25)"Ali Qushji," (figure 24), and a mystery developer/programmer attributed to the ransomware builder's leak. I could not wait to see what LockBit would say. Have you ever watched a good TV show that ends with a cliffhanger leaving you to wait in anticipation for the next episode? That was what this felt like. Further, I found the Proton account also had a telegram channel and posted the exact message, word for word, as the Ali Qushji post.

LockBitSupp was not responding to questions on the forum, but it showed he was available online in Tox, a secure chat platform it uses to communicate. I guess LockBit was busy investigating what and how the builder leaked and did not want to comment until it understood how the leak transpired. Several hours passed. Then, finally, LockBit responded, addressing the situation. LockBit claimed a disgruntled employee with an on-the-job drinking problem was behind the leak. Here is LockBit's explanation:

LockBit is a criminal, so I must question the validity and motivation behind anything it claims. No matter which of the explanations is accurate, it reflects poorly on LockBit. However, in this case, LockBit's explanation makes the most sense. For one, if someone did, in fact, compromise one of LockBit's servers, why would they only release a single builder? It's plausible a developer may only have access to the code (builder) he is developing and not the entire arsenal of ransomware, explaining why only it was released. Second, if the scenario in which a hacking team was behind the attack were true, why did they only create their online persona just prior to the leak? This is a huge red flag. Only an amateur or someone with little experience developing online personas would present the leak in this manner. Yet, something else LockBit said convinced me to believe their version of the events. If an outside group did breach LockBit's server and gain access to their most sensitive data, — their source code — then why did they:

"Just forget to deface it [LockBit's website] when they broke it, and also merge the builder of the world's fastest stealer, locker 2.0, Linux locker with 14 types of architectures, a database with correspondence, wallets for payment, advert logins and web sources panels, and history of visits to the server with my IP address from Starlink." — LockBitSupp

This is a rare occasion where every point LockBit made rings true. Unfortunately, LockBit runs a very secure operation. Someone would have exposed them a long time ago if it didn't. Anyone who put the time and effort into breaching LockBit would not stop with a single builder. For example, look at all the information and data gained from the infamous Conti leak compared to this event.[85] Chat logs, tools, operational playbooks, wallets, and source code were all leaked in that event. In comparison, it's not even close. This was the act of a disgruntled employee making a point to his boss and not an elite team of hackers trying to expose LockBit's whole operation.

The more important part of the story, according to LockBitSupp, is the disgruntled developer — the same developer discussed earlier who defected from BlackMatter to develop LockBitBlack.

"This coder is so cunning that he does not even remember that the story of 'buying' sorts was invented only in order to save his ass from revenge, because he defected to competitors" — LockBitSupp

The "story" LockBitSupp is referencing is that it purchased BlackMatter ransomware source code as opposed to stealing it by recruiting its developer as I discussed earlier. The "defected to competitors" comment references the developer leaving BlackMatter to support LockBit. However, if true, I would consider the developer central to LockBit Black and expect him to have access to far more information and resources than he released in the leak.

There was another point made while discussing the breach with LockBit, which may explain the motivation behind the leak. A few months earlier, in July 2022, LockBit paid out $50,000 to an individual who found a flaw in the code present in LockBit Black, which allowed files to be decrypted without the decryption key.[86] Apparently, the code was originally present in BlackMatter, and since LockBit used that to develop LockBit Black, the same vulnerability also existed in it. The theory is that LockBit took the $50K out of the developer's salary since he did not correct the flaw before using it to develop LockBit Black. LockBit acknowledged the flaw and stated it did pay the $50K payment as part of its bug bounty program but denied the funds were taken from the developer. Instead, LockBit claims it paid the bounty from its own funds, which had nothing to do with the

disgruntled developer. However, this theory fits perfectly into the events leading up to the leak and would provide a motive for why the developer betrayed LockBit.

You Have the Right to Remain Silent

In late September and October 2022, LockBit continued to break records with high-volume attacks. One victim, Pendragon, was a United Kingdom-based automotive company that LockBit attacked and demanded a $60 million ransom! LockBit operated as usual, encrypting systems and stealing internal data from the organization. Pendragon, however, refused to negotiate with LockBit. The company stated, "We refuse to be held hostage by this group, and we will not be paying a ransom demand."[87] There were also several European-based healthcare-related organizations breached in October 2022 that also refused to pay. Unfortunately, the breach resulted in patient data being exposed on the dark web.[88] Despite several non-paying victims, LockBit had many other victims who did pay. With so many attacks taking place involving LockBit ransomware, things were going well for the gang, but that was about to change.

On November 9, 2022, a dual Russian-Canadian national, Mikhail Vasiliev, was accused of participating in the "LockBit global ransomware campaign" and arrested at his home in Canada. The next day, the US Department of Justice (DOJ) issued a criminal complaint also charging him with a series of ransomware-related charges.[89] The arrest was reported by news outlets globally. The DOJ released the following statement pertaining to the arrest:

"Yesterday's successful arrest demonstrates our ability to maintain and apply relentless pressure against our adversaries," said FBI Deputy Director Paul Abbate. "The FBI's persistent investigative efforts, in close collaboration with our federal and international partners, illustrates our commitment to using all of our resources to ensure we protect the American public from these global cyber threat actors."[90]

Adding to the buzz, many news outlets published headlines similar to the one below:

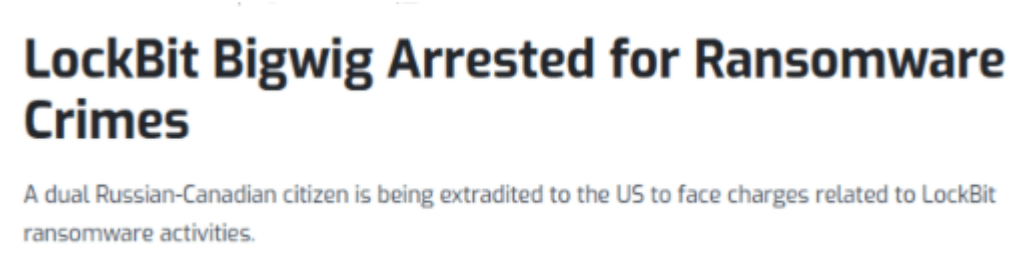


Figure 26: DarkReading news article about the LockBit arrest

When I heard a core member of LockBit was arrested, I was immediately skeptical. You see, LockBit is extremely careful in running their operation, and I would be shocked if any core gang member would reside in a US-friendly nation where they could be arrested and extradited. Most ransomware-related arrests involve affiliates who often live outside of Russia. Did they actually arrest one of the key leaders of LockBit? I found the answer buried within the details of the court documents.

In the criminal complaint, the DOJ stated Vasiliev was caught off guard as he sat at a table in his garage while using his laptop. Fortunately, Vasiliev did not have time to log out of his laptop before being subdued, making its

contents available to law enforcement. The confiscated laptop was the same system Vasiliev used to communicate with LockBit and to conduct attacks. According to the criminal complaint:

Unfortunately, since Vasiliev was not actively logged into the attack management console, law enforcement could not access LockBit's administrative infrastructure. However, they gained some additional information from analyzing the laptop's memory.

The information in this section of the criminal complaint was especially informative. Having firsthand knowledge of the admin console and infrastructure, I recognized the platform based on the pages found in the memory of Vasiliev's computer. Specifically, the reference to *"/page#builder/builder_red"* told me Vasiliev was not a core member of the gang. You see, "*builder_red"* represents the admin page used for *"LockBit Red,"* which I discussed earlier is the internal name used for LockBit 2.0, the previous version of LockBit ransomware. LockBit Red was replaced with LockBit Black in June 2022. This indicated Vasiliev worked with the gang prior to June and had not accessed the new LockBit Black operation used in current operations. A core member would have certainly accessed the LockBit Black admin console. While it's possible Vasiliev accessed LockBit Black from another system, I think that detail would be included in the criminal complaint.

To be clear, if Vasiliev is not a core member, as I believe, the arrest is still significant. It just means the arrest will have a smaller impact than what the media portrayed. Further, regardless of Vasiliev's role with the gang, his maximum penalty is five years in prison.[92] The punishment does not fit the crime when you consider the damage LockBit causes to its victims. I don't think this will send the "warning to ransomware actors" that the DOJ is publicizing. While outside the scope of this paper, the penalties for supporting ransomware attacks must be much tougher.

Unmasking LockBit

There is a lot of information discussed in this report! If you have read my previous research, you know I pride myself on supporting my assessments and analysis with technical evidence. I like to break down each finding and show exactly how I came to my conclusion. However, this report is based primarily on human intelligence gathering, which makes it much harder to lay out in an analytical, evidence-driven format.

In place of technical evidence, I have provided human intelligence supported by screenshots and quotes throughout this report to convey the analysis and findings I will give next. Remember, since my research is based on human correspondence, underground forum posts, and statements made directly by the individuals behind and associated with the LockBit operation, there is a higher margin for error. Still, I wanted to tell this story in a way not previously reported and show the operation from the eyes of the adversary. I also wanted to demonstrate the value of human intelligence in a cyber context because I believe it is extremely valuable for understanding ransomware adversaries. After months of investigating, this is what I learned about the humans hiding behind the LockBit persona and its ransomware operation.

Two members of the LockBit gang, the leader and another core member, likely operate the LockBitSupp persona.

- Throughout this report, we discuss interactions and behaviors observed by the LockBitSupp persona. One of the frequent points discussed by criminals is whether the individual behind the persona is the gang's

leader, as it claims, or if there are multiple individuals. Some criminals speculate that the persona is nothing more than a PR tool; however, I don't agree with that assessment. There could be multiple individuals behind the account, but if so, they are key members of the gang. The persona has a high level of knowledge about the gang's operation and access to sensitive materials that only a senior member would have.

- I believe the gang's leader is behind the LockBitSupp persona and, on occasion, has another member fill in to keep the profile active and engaged with the criminal community. I believe this because there are only a few occasions in which the persona contradicts itself and makes mistakes. On other occasions, I believe the contradictions are intentional to throw off law enforcement and researchers like myself.
- For example, remember the incident I discussed earlier, where the LockBitSupp persona stated they purchased BlackMatter source code and then, several months later, claimed they obtained it for free from a ransomware developer. I believe another gang member operated the persona to conduct the interview through the LockBitSupp persona and not the gang's leader. That individual did not expect the question about how it obtained the source code and answered incorrectly. This triggered a series of events that eventually led the developer to defect and leak LockBit's source code to its ransomware builder.

LockBit did NOT operate the Gogalocker and Magacortex ransomware operations as attributed in previous security vendor reporting. The attribution was derived from weak evidence too common to use for attribution. Further, after a series of arrests of members associated with Gogalocker, no evidence or accusations exist to connect the operations with one another.

LockBit is associated with several high-profile ransomware gangs:

- LockBit personally knows the identity of the key members of DarkSide, BlackMatter, and BlackCat ransomware gangs. He also had close ties to the key leaders who previously ran the REvil ransomware gang. Additionally, LockBit claims another popular criminal persona known well in the criminal community is associated with the leadership behind the former Conti gang, now BlackBasta. Lockbit also claims this individual and the other core members of the former Conti gang are working for the FSB [93].

LockBit interacted and frequently communicated with the REvil persona "Unknown", amongst others, who is believed to have been the leader of the gang. LockBit does not believe the individual currently running REvil, is the authentic REvil leader.

LockBit confirmed that the core members of DarkSide were the same individuals behind BlackMatter and BlackCat ransomware. LockBit also confirmed the leadership of BlackBasta are the same individuals who ran the former Conti ransomware operation. While the security community already made these connections through technical means, LockBit's interpretation is derived from human relationships with the members who make up these gangs, making it a more significant association.

LockBit did not purchase BlackMatter source code as believed but instead obtained access to it from its developer in November 2021.

The developer of DarkSide ransomware is the same individual who developed BlackMatter and LockBit Black ransomware and previously developed malware for Fin7, another cybercrime group.

The developer who recently leaked LockBit ransomware should be a high-value target for law enforcement and government operations.

- The developer is highly connected within the Russian ransomware and organized cybercrime community.
- The individual previously developed malware for Fin7 and then created DarkSide ransomware, which was used in the Colonial Pipeline attack, and then developed ransomware for BlackMatter ransomware operations before joining LockBit to create LockBit Black.
- The individual (developer) has defected from BlackMatter and LockBit and may now be in hiding.

- **This person would provide the best chance to turn into a major player with inside knowledge of human and technical operations spanning major cybercrime syndicates.** Both BlackMatter and LockBit have previously threatened the developer.
- The developer has information related to the identity of both LockBit and DarkSide leadership and possibly Fin7. Leadership in these gangs also likely knows the identity of the developer. The fact that neither LockBit nor BlackMatter have attempted to Dox, or worse, physically harm the developer is an indication that he likely has information that could be used against these gangs if something were to happen to him. (I don't know this for a fact, but it makes sense and has been insinuated by sources close to the involved parties.)

- Additionally, LockBit has made threats against the developer but never followed through even after the developer leaked its source code.

Another party, who is well known and connected to cyber criminals and has close ties to the developer, shared inside details stating the developer told him directly that he did, in fact, leak the LockBit ransomware builder source code after LockBit refused to pay him the amount they agreed upon.

Developer attributes:

- Male, likely in his mid-30s, living in Russia or in a former CIS state in Eastern Europe
- Served in a military unit where he performed a job that required a high level of technical knowledge
- Previously convicted of crimes and may have served a short sentence in prison
- Married and has children
- Allegedly operates his own site on the dark web to solicit work, indicating he likely works for other criminals in addition to LockBit
- The developer provided his side of the story and details the timeline and sequence of operational events from when he defected from BlackMatter to when he and LockBit began their altercation resulting in his quitting the operation. **A transcript of his statement can be found in the appendix of this report.**

According to LockBit's former developer, since he left the operation, LockBit has had no support for LockBit 3.0.

- If true, this could be leveraged against LockBit.

While LockBit's operation continues to dominate the ransomware ecosystem, many criminals are growing tired of the gang's leadership and public antics.

The leader of LockBitSupp claims he keeps his PGP secret key and a multi-signature wallet on a hidden flash drive. The wallet requires passwords, which in a previous conversation, he stated were 50 characters in length and randomly generated. It also requires a key file, which he states is on another flash drive that he keeps around his neck made from red wool. He uses wool so he can quickly rip off and swallow the flash drive upon his arrest. Who knows if any of this is true, but he certainly put much thought into the story. You can see his claims in Figure 27 below.

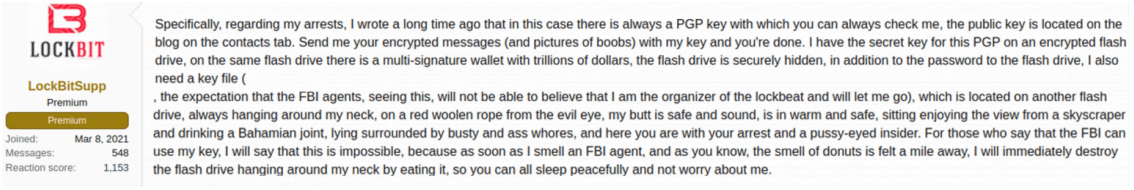


Figure 27: LocBitSupp discusses how he will evade being identified as the leader of the gang if arrested

On several occasions, LockBitSupp claimed he uses Starlink, the satellite internet provider owned by Elon Musk.

> *"I have already said more than once that I use Starlink, because it increases the radius of my search."*
> *— LockBitSupp*

LockBitSupp claims he believes the area of accuracy for an IP address assigned to a satellite network is much broader than traditional methods, which would make it harder to track him down should his network access be identified. Once again, I don't know if he is telling the truth or if this is for show.

Final Entry

LockBit is not going away anytime soon. Despite the recent negativity expressed by members within the criminal community, LockBit runs a lucrative operation that is attractive to cybercriminals. The easy-to-use, point-and-click graphical interface built into the attack management console makes it fast and efficient for criminals to conduct enterprise ransomware attacks with far less technical expertise required than ever before. Additionally, the affiliate-controlled payment model builds trust with cybercriminals and ensures they are paid for their work. However, if any of these services or components of the RaaS program change, such as not updating ransomware, tools, or infrastructure, LockBit activity would significantly decrease. Further, there is a lot of competition waiting to move in if LockBit were to fall out of favor with cybercriminals.

The previous gangs that once held first place, such as Maze, REvil, and Conti, all eventually fell. The common theme across each is that their egos grew out of control, and their greed drove them to push things too far. Eventually, they overstep and gain attention from entire governments with greater resources than traditional law enforcement. Regardless, it's unlikely LockBit will ever face arrest or spend time in a prison cell. In reality, its greatest concern is that its own government will find them, confiscate their finances, and force them to support its military or government cyber operations.

This may be one reason LockBit claims it no longer resides in Russia, though I believe that is more likely a story intended to throw off investigators. For example. over the course of my investigation, LockBitSupp discussed living in China, the Netherlands, Hongkong, and even the US. At one point, the gang's leader even claimed he

owned a stake in two restaurants based in New York City! However, the one place he discussed the least, Russia, is most likely where he resides today.

Another problem is we approach ransomware criminals similarly to traditional criminals. Ransomware criminals are protected and out of the reach of law enforcement unless they leave Russia and are caught in a nation that allows extradition to the United States. However, we address the problem by issuing warrants and working to arrest Russian ransomware criminals like LockBit with tactics that continue to fail. I don't fault law enforcement, but it's time we change the way we approach the ransomware problem.

In my opinion, we need to conduct information warfare operations intended to inject propaganda and misinformation across dark web forums used by ransomware criminals. If criminals lose trust in the RaaS provider, they will not work for them. Paranoia, distrust, and concerns about losing revenue are common among ransomware affiliates. We need to play on this fear. This, in conjunction with attacks against ransomware services and infrastructure, would deny the resources that ransomware gangs provide to their affiliates. Driving distrust and causing intermittent service outages would frustrate criminals and affect the RaaS provider negatively. Regardless of how we address the issue, one thing is for sure, what we are doing now is not working, and it's time for a change.

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.

Apendix

Statement from LockBit Black Developer

"LockBitSupp is being disingenuous when it portrays its "fired" coder as a deranged psycho who is on anti-anxiety medication.

It benefits him, given that he does not disclose the "quotes" about the details of what happened.

The coder who worked with him is me. I'll make it clear right away, no one fired me, in fact. I left on my own.

The decision to leave was made after I finally got an understanding of the situation that I was simply thrown.

At the moment, LockBit has no technical support for either the current 3.0 draft or the old 2.0 without any support for almost a year now. I don't know how LockBitSupp parted ways with the coder who wrote 2.0.

According to LockBitSupp, the type encoder became afraid of something and decided to leave. I think about the true state of affairs, regarding the 2.0 developer, we will never know.

Now to what happened to me.

At the end of 2021…

By that time, on the LockBitSupp forum, if my memory serves me, I wrote that I was considering proposals for cooperation.

I wrote to him. He was very happy, as I understood, especially after he found out who I was.

I said that I was ready to write a new locker from scratch. And showed him my source. To which he said that there was no need to write a new locker, it was enough to modify the metter code. I warned him that the metter had already fired at that moment with all possible ABs, to which he replied that it didn't matter, because adverts still cut down AB before setting up the network.

We agreed with him on such terms of cooperation.

1. Before the release of the locker, at the stage of finalizing the code of the metter, he pays me 20K per month.

2. After the release, I get 10% of the money he receives from adverts for further support of the 3.0 project. The payment of these interests will occur every first day of the month, after the release.

3. LockBitSupp will remove its 2.0 from the panel so that adverts use only 3.0.

These are all agreements on which mutual agreement has been reached. I specifically draw your attention to this.

Further, within 6 months (before the release), I added 2 functions to the current metter code:

1. PsExec distribution over the network.

2. Distribution over the network using GPO (group policies), plus automatic self-removal of group policy after a specified time.

Additionally, uninstallation of MS defender, overwriting of free space on the hard disk after encryption, and secure deletion of files (multiple overwriting of the contents of the file before deletion, including the filename, to prevent the recovery of deleted files) was added.

I note that with the next check for AVcheck (even before the release), my locker started to fire like LockBit 3.0! I asked a question about this LockBitSupp, what's going on? To which he replied that most likely the tester who tested the new locker had a "leak," he forgot to turn off the AV. Here I had the first bad feeling that the locker was being used even before the release. Later it turned out that LockBitSupp gave it to some advert for a 'test' so that he would check it 'in combat' conditions. True, he kept silent about whether the payment was as a result of this 'test.'

The release took place at the end of June 2022.

After the release, LockBitSupp announced a bug bounty, which I found out later, i.e., he didn't ask for my consent.

Literally a couple of weeks later after that, LockBitSupp tells me that some kind of researcher from some cantor's recovery got in touch with him, which states that there is a bug in the encryption of my locker and that larger files, such as virtual disk images, can be decrypted. But only such files. Because they contain large areas filled with

zeros, the blocks on which the data is encrypted are repeated. Salsa encryption algorithm20. This was my joint, I admit it. And the jamb was, as it turned out, even when the metter was. I don't want to justify myself. I just wanted the best, it turned out as always, I in pursuit of encryption speed, decided to rewrite the salsa algo from 32 registers to SSE myself and missed one significant moment. Vobshem, I quickly fixed it. Replacing the standard algorithm. After that, LockBitSupp billed me 50K, which he promised to the researcher, as a reward. To which I said that if the profit is divided 90% by 10%, then the costs should be shared in the same ratio. I transferred him 5K in Monero, as my share in the reward of the researcher. By the way, another lie of LockBitSupp is that he paid all 50K from 'his own pocket.'

Then came August 1. And, accordingly, the payment of my interest. To which he told me that his wallet was being synchronized. As a result, the wallet was synchronized with him only after 9 days. At the end, he sends me a screenshot of a wallet with bitcoins, on which there are approximately 120K in dollars.

The fact is that I'm 'in the know' and I understand perfectly well that for the promoted software it's not just a penny, but tears … To my question LockBitSupp, why is that? He replied that most of the adverts were on vacation. And the fact that you can't compare 2020 and 2022, that everything is complicated, etc. LockBitSupp went on to say that out of the 120K received, it takes back the 50K paid to the researcher for the bug bounty. As a result, 70K remained, of which only 5K are mine (interesting math) 10% of 70K turns out to be not 7K but 5. As a result, he transferred 10K to me — this is 5K that I gave to pay the researcher and 5K — my interest for the month.

At that time, the current locker 3.0 was supported by me, plus, I wrote a new metamorphic locker on SysCall to bypass the AB proactivation (to be fair, I note that the new locker was invisible at least to sophos) and utilities for 'killing' AB. LockBitSupp knew about these developments, but we had not yet stipulated the conditions for their use on the PP.

Naturally, I suspended development. I decided to wait another month, leaving only support for 3.0.

Literally after this, LockBitSupp turns to me, like the files of the 'clients' of adverts are not decrypted. I asked for samples of these files.

And found out that the files are encrypted twice. At the beginning with my locker, then 2.0. Naturally I ask LockBitSupp a question about our deal that he had to take his 2.0 away. To which he replied that 'everything is for the convenience of adverts,' that adverts have a choice whether to work with 2.0 or 3.0. Naturally, wallets 2.0 and 3.0 are different. In fact, it turns out that he takes everything from 2.0 to himself, and from 3.0, I can only get 10% (and I didn't receive those, judging by August 1). He never removed 2.0 from the panel, even after everything was revealed.

Then came September 1. Instead of his interest, he sent me a screenshot of wallet 3.0 with ~42 bitcoins, announcing with pathos that there would be something else and that I didn't trust him in vain, the amount would only grow, because. adverts began to return from holidays.

I asked him to give me my 4 bitcoins, since 10% is mine. To which he replied that I didn't work for 2 months (probably forgot about support for 3.0) and I will receive this money ONLY when I give him a new metamorphic locker and killers for defender and sophos, at least. At the same time, I remind you that the conditions for new

developments have not been discussed. I told him about it. To which LockBitSupp stated that 10% is for EVERYTHING, i.e., for support 3.0 and for ALL new developments!!!

And then I went nuts. Immediately he tells me that for 10%, I should generally work 24/7 without a breeze. He began to offer ‘guarantors’ through which I can get money if I fulfill his conditions.

I thought carefully and announced my leaving.

In general, I told everything as it is. PS I don’t remember exactly, but, LockBitSupp somewhere stated that he ‘bought’ metter sources for 1KK. So, he did not buy anything, he got everything from me.”

IOCs

Type	Indicator Value
URL	hxxps://lockbitsupp[.]uz
URL	hxxps://lockbitapt[.]uz
URL	hxxps://decoding.at/
URL	hxxps://decoding.at
URL	hxxps://bigblog.at
URL	hxxp://ppaauuaa11232.cc/dlx5rc.dotm
URL	hxxp://ppaauuaa11232.cc/aaa.exe
URL	hxxp://lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd[.]onion
URL	hxxp://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd[.]onion
URL	hxxp://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd[.]onion
URL	hxxp://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd[.]onion
URL	hxxp://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd[.]onion
URL	hxxp://lockbitsupp[.]uz
URL	hxxp://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad[.]onion
URL	hxxp://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd[.]onion
URL	hxxp://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd[.]onion
URL	hxxp://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd[.]onion
URL	hxxp://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid[.]onion

URL	hxxp://lockbitsapzxzkpf33daeacsarqdtjjlkouxd7emxaqk7f3svavbmmad[.]onion
URL	hxxp://lockbitsapu34zkhnafamvkegbmdfh5yvqjbth6g376z2tgvef34jnqd[.]onion
URL	hxxp://lockbitsapliyedzmz5yjcoj27yfgeix6rzrhj7ss4kvfmdv6iyvxlad[.]onion
URL	hxxp://lockbitsapfq6mp7djlmbtk4uj53vnueldrjsgfjew3ccridkufmmmyd[.]onion
URL	hxxp://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did[.]onion/or
URL	hxxp://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did[.]onion
URL	hxxp://lockbitks2tvnmwk[.]onion/?f51e3d94fa5d7445ac6ccf46aaf94046
URL	hxxp://lockbitks2tvnmwk[.]onion/?f51e3d94fa5d7445a8696d94832c0475
URL	hxxp://lockbitks2tvnmwk[.]onion/?eca510985c0f395fc68355f78c72eb7e
URL	hxxp://lockbitks2tvnmwk[.]onion/?eca510985c0f395fc4baa509e1da3bcf
URL	hxxp://lockbitks2tvnmwk[.]onion/?d0407ac9d97c78cbe1bab382e265a7d9
URL	hxxp://lockbitks2tvnmwk[.]onion/?d0407ac9d97c78cbde67fd2060343ad5
URL	hxxp://lockbitks2tvnmwk[.]onion/?d0407ac9d97c78cbb88e6c4b00b8a89a
URL	hxxp://lockbitks2tvnmwk[.]onion/?d0407ac9d97c78cbb6f307818bf431f2
URL	hxxp://lockbitks2tvnmwk[.]onion/?d0407ac9d97c78cbaf286670236c136f
URL	hxxp://lockbitks2tvnmwk[.]onion/?d0407ac9d97c78cb888c818dbe3e5451
URL	hxxp://lockbitks2tvnmwk[.]onion/?cb814bf5252f2b2ea736bae86cbcf628
URL	hxxp://lockbitks2tvnmwk[.]onion/?cb814bf5252f2b2ea3fe8107302e50ff
URL	hxxp://lockbitks2tvnmwk[.]onion/?addd79899d34fb74c43f52b0a95da6a7
URL	hxxp://lockbitks2tvnmwk[.]onion/?addd79899d34fb7491c6ff7476ce466dthis
URL	hxxp://lockbitks2tvnmwk[.]onion/?addd79899d34fb7491c6ff7476ce466d
URL	hxxp://lockbitks2tvnmwk[.]onion/?A51C1D5E9695AD10E3E5D3142E83715D
URL	hxxp://lockbitks2tvnmwk[.]onion/?A51C1D5E9695AD10B1522FE6DF4E9208
URL	hxxp://lockbitks2tvnmwk[.]onion/?a51c1d5e9695ad108fab064cdbdb6ae1
URL	hxxp://lockbitks2tvnmwk[.]onion/?a51c1d5e9695ad10816fa0b6cc7c88d9
URL	hxxp://lockbitks2tvnmwk[.]onion/?a2232793f05765b5c9ac68b9fad2a1ff
URL	hxxp://lockbitks2tvnmwk[.]onion/?a2232793f05765b5c28d50f847219aa9

URL	hxxp://lockbitks2tvnmwk[.]onion/?a2232793f05765b5b85bb84c8da9db4d
URL	hxxp://lockbitks2tvnmwk[.]onion/?a2232793f05765b5aa8bd0bc79613991
URL	hxxp://lockbitks2tvnmwk[.]onion/?9b7fda8d33fec3f997360f45c651cd80
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4ce514760e6c76dd19
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cd8f82cd385f7b7d4
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cbf37248ab20916dd
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cba28204b9ace04d7
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cb4866f7e3736dc38
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cb0221ee5b5d41430
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4caff60ac8c075e649
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cafa3a6a68e5a0970
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cad70668439891476
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4cac43816fe754becc
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4ca9a01f7006c0a55e
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4c9f9a1cc242625249
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4c9ea6d36aad088c6a
URL	hxxp://lockbitks2tvnmwk[.]onion/?96b283ef5b7acd4c956975d05400de35
URL	hxxp://lockbitks2tvnmwk[.]onion/?962823c4ebe6623dda54cba73ca3f6d9
URL	hxxp://lockbitks2tvnmwk[.]onion/?962823c4ebe6623d8d7f97d1626ba803
URL	hxxp://lockbitks2tvnmwk[.]onion/?92727ee520aebc7ddb0b8513298c5f9f
URL	hxxp://lockbitks2tvnmwk[.]onion/?92727ee520aebc7db018651dbcf6a903
URL	hxxp://lockbitks2tvnmwk[.]onion/?8cf3e3c381b4e3e2dd6218830eab1937
URL	hxxp://lockbitks2tvnmwk[.]onion/?8cf3e3c381b4e3e2c3e99c5cab5b114f
URL	hxxp://lockbitks2tvnmwk[.]onion/?8b28321abd4e73ffa3972c962701b1c6
URL	hxxp://lockbitks2tvnmwk[.]onion/?8b28321abd4e73ff947ffdb0830a9bbd
URL	hxxp://lockbitks2tvnmwk[.]onion/?8841dd9b0ac925ffea072c230e6c6e86
URL	hxxp://lockbitks2tvnmwk[.]onion/?8841dd9b0ac925ffcb8a22ce2d1f7a6a

URL	hxxp://lockbitks2tvnmwk[.]onion/?8841dd9b0ac925ff8cdb45fa32c58795
URL	hxxp://lockbitks2tvnmwk[.]onion/?85c01e35fd24495cd7f75dbe06dd8a8e
URL	hxxp://lockbitks2tvnmwk[.]onion/?85c01e35fd24495cabd967551f73c273
URL	hxxp://lockbitks2tvnmwk[.]onion/?828c57864cbb23b6f00d7365444267c2
URL	hxxp://lockbitks2tvnmwk[.]onion/?828c57864cbb23b6e1fda4efbb92a2c4
URL	hxxp://lockbitks2tvnmwk[.]onion/?828c57864cbb23b6c0372f2c9dfc478e
URL	hxxp://lockbitks2tvnmwk[.]onion/?828c57864cbb23b694906f88baef18c7
URL	hxxp://lockbitks2tvnmwk[.]onion
URL	hxxp://lockbitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd[.]onion
URL	hxxp://lockbitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad[.]onion
URL	hxxp://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevoa3eqdfcntxad5lmyd[.]onion
URL	hxxp://lockbitaptjpikdqjynvgozhgc6bgetgucdk5xjacozeaawihmoio6yd[.]onion
URL	hxxp://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd[.]onion
URL	hxxp://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd[.]onion
URL	hxxp://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid[.]onion
URL	hxxp://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd[.]onion
URL	hxxp://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion
URL	hxxp://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd[.]onion
URL	hxxp://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd[.]onion
URL	hxxp://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd[.]onion
URL	hxxp://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead[.]onion
URL	hxxp://lockbitapt[.]uz
URL	hxxp://lockbit-decryptor[.]top/?cb814bf5252f2b2ea736bae86cbcf628
URL	hxxp://lockbit-decryptor[.]top/?cb814bf5252f2b2ea3fe8107302e50ff
URL	hxxp://lockbit-decryptor[.]top/?a2232793f05765b5c9ac68b9fad2a1ff
URL	hxxp://lockbit-decryptor[.]top/?a2232793f05765b5c28d50f847219aa9
URL	hxxp://lockbit-decryptor[.]top/?a2232793f05765b5b85bb84c8da9db4d

URL	hxxp://lockbit-decryptor[.]top/?a2232793f05765b5aa8bd0bc79613991
URL	hxxp://lockbit-decryptor[.]top/?9b7fda8d33fec3f997360f45c651cd80
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4ce514760e6c76dd19
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cd8f82cd385f7b7d4
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cbf37248ab20916dd
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cba28204b9ace04d7
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cb4866f7e3736dc38
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cb0221ee5b5d41430
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4caff60ac8c075e649
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cafa3a6a68e5a0970
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cad70668439891476
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4cac43816fe754becc
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4ca9a01f7006c0a55e
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4c9f9a1cc242625249
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4c9ea6d36aad088c6a
URL	hxxp://lockbit-decryptor[.]top/?96b283ef5b7acd4c956975d05400de35
URL	hxxp://lockbit-decryptor[.]top/?8cf3e3c381b4e3e2dd6218830eab1937
URL	hxxp://lockbit-decryptor[.]top/?8cf3e3c381b4e3e2c3e99c5cab5b114f
URL	hxxp://lockbit-decryptor[.]top/?8b28321abd4e73ffa3972c962701b1c6
URL	hxxp://lockbit-decryptor[.]top/?8b28321abd4e73ff947ffdb0830a9bbd
URL	hxxp://lockbit-decryptor[.]top/?8841dd9b0ac925ffea072c230e6c6e86
URL	hxxp://lockbit-decryptor[.]top/?8841dd9b0ac925ffcb8a22ce2d1f7a6a
URL	hxxp://lockbit-decryptor[.]top/?8841dd9b0ac925ff8cdb45fa32c58795
URL	hxxp://lockbit-decryptor[.]top/?85c01e35fd24495cd7f75dbe06dd8a8e
URL	hxxp://lockbit-decryptor[.]top/?85c01e35fd24495cabd967551f73c273
URL	hxxp://lockbit-decryptor[.]top
URL	hxxp://lockbit-decryptor[.]com/?addd79899d34fb74c43f52b0a95da6a7

URL	hxxp://lockbit-decryptor[.]com/?addd79899d34fb7491c6ff7476ce466dfollow
URL	hxxp://lockbit-decryptor[.]com/?addd79899d34fb7491c6ff7476ce466d
URL	hxxp://lockbit-decryptor[.]com/?
URL	hxxp://dtutgqjuzv7sktgl[.]onion/

Citations

1. https://twitter.com/3xp0rtblog/status/1569230420314554372

2. https://github.com/3xp0rt/LockBit-Tattoo

3. https://www.redhotcyber.com/en/post/rhc-interviews-lockbit-3-0-the-main-thing-is-not-to-start-a-nuclear-war/

4. https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

5. https://cyware.com/research-and-analysis/lets-talk-about-lockbit-an-in-depth-analysis-7cf0

6. https://arstechnica.com/information-technology/2020/05/lockbit-the-new-ransomware-for-hire-a-sad-and-cautionary-tale/]

7. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/targeted-ransomware-threat

8. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks

9. https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

10. https://www.youtube.com/watch?v=FbZyADzEez4

11. https://symantec.broadcom.com/hubfs/Symantec-Targeted-Ransomware-White-Paper.pdf

12. https://analyst1.com/whitepaper/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

13. https://techcrunch.com/2021/10/29/europol-hackers-norsk-hydro/

14. https://nostarch.com/art-cyberwarfare

15. https://tria.ge/220824-x5m6ysaahk/behavioral1#report

16. https://id-ransomware.blogspot.com/2019/10/abcd-ransomware.html

17. https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register

18. https://finance.yahoo.com/quote/BTC-USD/history?period1=1410739200&period2=1593302400&interval=1wk&filter=history&frequency=1wk

19. https://www.hhs.gov/sites/default/files/lockbit-ransomware.pdf

20. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/

21. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-self-spreads-to-quickly-encrypt-225-systems/

22. https://thedfirreport.com/2020/06/10/lockbit-ransomware-why-you-no-spread/

23. https://www.bleepingcomputer.com/news/security/ransomware-gangs-team-up-to-form-extortion-cartel/

24. https://thehackernews.com/2022/07/experts-find-similarities-between.html

25. https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/

26. https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

27. https://analyst1.com/blog/dark-web-justice-league

28. https://geminiadvisory.io/lockbit-launches-ransomware-blog/

29. https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

30. https://www.cybereason.com/blog/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool

31. https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/

32. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

33. https://www.bleepingcomputer.com/news/security/accenture-confirms-hack-after-lockbit-ransomware-data-leak-threats/

34. https://www.crn.com/news/security/accenture-s-lack-of-transparency-in-ransomware-attack-sets-bad-example-partners

35. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

36. https://twitter.com/AuCyble/status/1425422006690881541

37. https://www.bleepingcomputer.com/news/security/lockbit-gang-leaks-bangkok-airways-data-hits-accenture-customers/

38. https://www.bleepingcomputer.com/news/security/lockbit-gang-leaks-bangkok-airways-data-hits-accenture-customers/

39. https://www.techtarget.com/searchsecurity/news/252508243/Accenture-sheds-more-light-on-August-data-breach

40. https://www.sec.gov/ix?doc=/Archives/edgar/data/1467373/000146737321000229/acn-20210831.htm

41. https://duo.com/decipher/lockbit-ransomware-variant-targets-vmware-esxi

42. https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

43. https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

44. https://cyware.com/news/connecting-the-dots-between-lockbit-30-and-blackmatter-a33ce68f

45. https://www.theregister.com/2021/10/04/in_brief_security/

46. https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

47. https://gizmodo.com/report-fbi-had-ransomware-decryption-key-for-weeks-bef-1847715916

48. https://analyst1.com/file-assets/History-of-REvil.pdf

49. https://twitter.com/ddd1ms/status/1498012695035011079

50. https://analyst1.com/blog/a-behind-the-scenes-look-into-investigating-contileaks-1

51. https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/conti-ransomware-group-announces-shutdown-proliferation-continues-via-affiliates

52. https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/

53. https://techcommunity.microsoft.com/t5/microsoft-security-experts/part-2-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254421

54. https://www.malwarebytes.com/blog/threat-intelligence/2022/08/ransomware-review-july-2022

55. https://www.malwarebytes.com/blog/threat-intelligence/2022/08/ransomware-review-july-2022

56. state.gov/darkside-ransomware-as-a-service-raas/

57. https://analyst1.com/file-assets/History-of-REvil.pdf

58. https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/

59. https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-claims-to-be-shutting-down-due-to-police-pressure/

60. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

61. https://www.scmagazine.com/analysis/ransomware/blackcat-confirms-blackmatter-roots-but-makes-an-ask-of-the-researcher-community

62. https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant–lockbit-3-.html

63. https://www.redhotcyber.com/en/post/rhc-interviews-lockbit-3-0-the-main-thing-is-not-to-start-a-nuclear-war/

64. https://www.justice.gov/opa/press-release/file/1084361/download

65. https://therecord.media/fin7-cybercrime-cartel-tied-to-black-basta-ransomware-operation-report/

66. https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions

67. https://analyst1.com/whitepaper/nation-state-and-ransomware

68. https://www.prodaft.com/resource/detail/silverfish-global-cyber-espionage-campaign-case-report

69. https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf

70. https://www.speartip.com/resources/evil-corp-poses-as-babuk-to-avoid-sanctions-and-secure-payment/

71. https://borncity.com/win/2022/10/11/exchange-server-neue-0-day-nicht-notproxyshell-cve-2022-41040-cve-2022-41082/

72. https://therecord.media/microsoft-investigating-alleged-exchange-zero-day/

73. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/

74. https://techcrunch.com/2022/07/27/entrust-data-stolen-june-cyberattack/

75. https://breached.vc/Thread-Entrust-com-Leak-Part1

76. https://analyst1.com/whitepaper/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

77. https://techcrunch.com/2022/07/27/entrust-data-stolen-june-cyberattack/

78. https://angle.ankura.com/post/102htog/lockbit-implements-new-technique-by-leaking-victim-negotiations

79. https://twitter.com/vxunderground/status/1562839055158558720?lang=e

80. https://github.com/3xp0rt/LockBit-Tattoo

81. https://twitter.com/vxunderground/status/1568273779050127363?lang=en

82. https://twitter.com/3xp0rtblog/status/1572510793861836802

83. https://twitter.com/_JohnHammond/status/1572570711155417089?

84. https://twitter.com/_JohnHammond/status/1572570711155417089?

85. https://analyst1.com/blog/a-behind-the-scenes-look-into-investigating-contileaks-1

86. https://twitter.com/ido_cohen2/status/1571039567666638848

87. https://techmonitor.ai/technology/pendragon-posted-on-lockbit-3-0-blog

88. https://www.bankinfosecurity.com/lockbit-publishes-stolen-data-as-hospital-rejects-extortion-a-20155

89. https://www.justice.gov/usao-nj/pr/russian-and-canadian-national-charged-participation-lockbit-global-ransomware-campaign

90. https://www.justice.gov/opa/pr/man-charged-participation-lockbit-global-ransomware-campaign

91. https://www.justice.gov/usao-nj/press-release/file/1551116/download

92. https://therecord.media/alleged-lockbit-operator-to-be-extradited-from-canada-to-u-s/

93. https://the-key.tk/2022/12/17/interview-lockbit/

Source: https://analyst1.com/ransomware-diaries-volume-1/