LockBit Attempts to Stay Afloat with a New Version

By By: Trend Micro Research Feb 22, 2024 Read time: 12 min (3194 words)

Published: 2024-02-22 · Archived: 2026-04-05 13:43:22 UTC

This research is the result of our collaboration with the National Crime Agency in the United Kingdom, who recently took action against LockBit as part of an international effort resulting in the disruption of the group's infrastructure and undermining of its operations. More details can be found on their website herenews article.

Introduction

LockBitnews article is a Ransomware-as-a-Service operation (RaaS) that has been involved in numerous security incidents for organizations globally over the years. By offering LockBit as a RaaS, its developers can provide it to other criminals for their own operations. In a typical RaaS setup, earnings are split between both the developers and their affiliates after the ransom has been negotiated and paid. LockBit normally charges a 20% share of the ransom per paying victim, with the remaining 80% going to the affiliate. However, if LockBit itself is the one carrying out the negotiations, this fee goes up to 30 to 50%. In November 2023, the group introduced new recommendations for ransom values based on the revenue of the victim, forbidding discounts above 50%.

From a purely technical side, what made LockBit special compared to other competing ransomware packages was that it used to have self-spreading capabilities. Once a host in the network becomes infected, LockBit is able to search for other nearby targets and to try and infect them as well, a technique that was not common in this kind of malware.

From a criminal group perspective, LockBit was known to be innovative and willing to try new things (though less so in recent times, as we will see in this entry). For instance, they came up with a public contest — a “bug bounty” — to find new ideas from the cybercriminal community to improve their ransomwarenews article. This group also developed and maintained a simple point-and-click interface that allowed a cybercriminal to choose various options before compiling the final binary for the attack, therefore lowering the technical barrier of entry for their criminal affiliates.

The group also promoted themselves through stunts in the cybercriminal community, such as paying people to get LockBit tattoos and even offering a US$1 million bounty for anyone who could find out the real-world identity of LockBit’s gang leader (an individual or group known by the online nickname “LockBitSupp”).

As part of this innovative streak, LockBit has published several versions of their ransomware, from the initial v1 (January 2020) to LockBit 2.0 (nicknamed “Red”, from June 2021), then to LockBit 3.0 (nicknamed “Black”, from March 2022). In October 2021, the threat actor introduced LockBit Linux to accommodate attacks on Linux and VMWare ESXi systems. Finally, an intermediate version, nicknamed “Green,” that incorporated code apparently inherited from the defunct Conti ransomware, emerged in January 2023. However, this version was not identified as a new 4.0 versionnews article.

In recent times, the group has experienced issues, both internally and externally, that have threatened its position and reputation as one of the top RaaS providers. This blog entry touches on these issues and provides a look into our data, which shows the group's seeming decline over the past couple of years.

Furthermore, we will examine an in-development version of the ransomware we track as LockBit-NG-Dev (NG for Next Generation), which could be an upcoming version the group might consider as a true 4.0 version once complete. We will examine its capabilities in relation to other LockBit versions, such as the "Green" version from 2023.

A detailed technical analysis of LockBit-NG-Dev can be accessed in the **appendix**.

Recent LockBit issues and difficulties

The LockBit group has had internal security incidents, due to the distributed semi-anonymous structure of the group itself and the interactions between the affiliate program members and the LockBit operators.

Information leaks by disgruntled developers or group members have occurred in the past. In September 2022, the builder for the ransomware was leakednews article by a developer associated with the group This leaked build had significant impact on the cybercriminal scene by lowering the threshold for criminals to start their own RaaS enterprise via clones of the LockBit operation.

When builds are leaked, it can also muddy the waters with regards to attribution. For example, in August 2023, we observed a group that called itself the Flamingo group using a leaked LockBit payload bundled with the Rhadamanthys stealer. In November 2023, we found another group, going by the moniker Spacecolon, impersonating LockBit. The group used email addresses and URLs that gave victims the impression that they were dealing with LockBit.

This LockBit knock-off group even used a leak site similar to LockBit (Figure 2). This further demonstrates how the leaked build has diluted the skill needed to operate a RaaS. Events like these might even cause doubt for legitimate LockBit victims as to whether they are dealing with LockBit or an impostor.

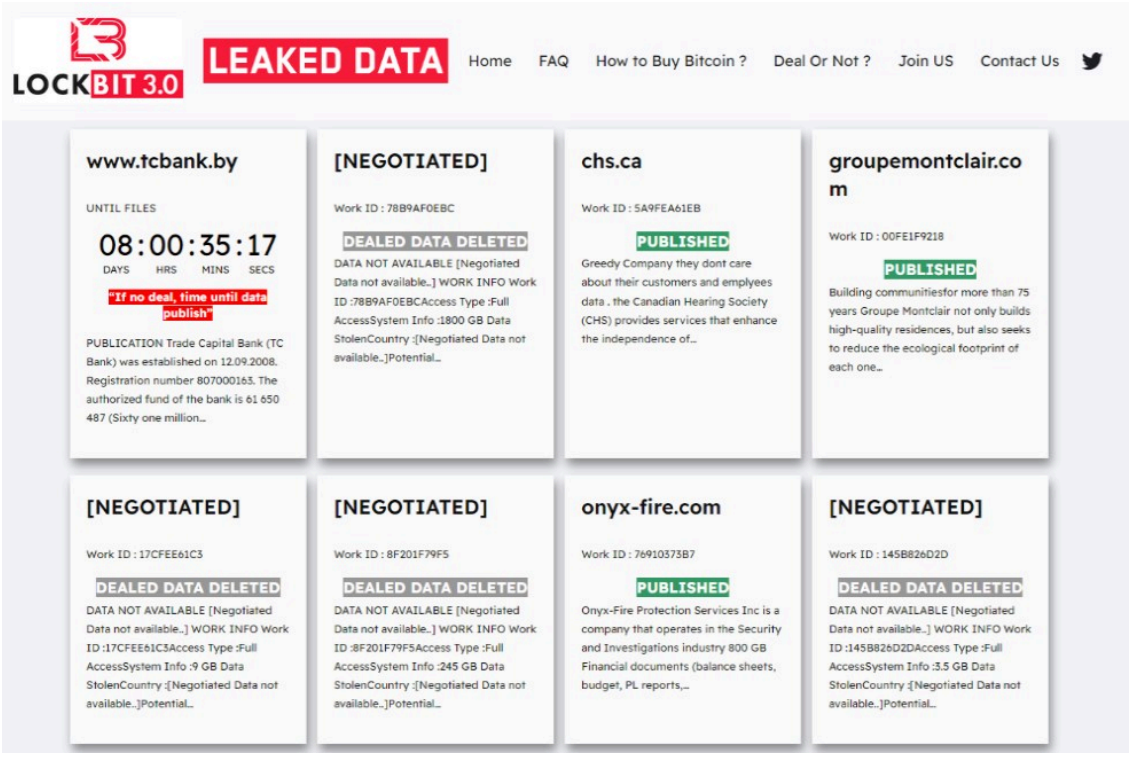


Figure 2. A false LockBit leak site made by another threat actor

The leaked build was a serious blow to the LockBit operation for several reasons:

1. The fact that it was leaked in the first place by a disgruntled developer shows that it's not all smooth sailing for the LockBit operation. Anything that signals internal discontent will undoubtedly be concerning for current or prospective affiliates.
2. A leak like this should be called out for what it is — a security failure. If their core build can be leaked, then affiliates might wonder if there are other security concerns. An incident like this in a software company would be seen as a complete failure of internal processes and controls, or worse, the absence of them.
3. Any technical advantage that LockBit may have had in the past is severely diluted due to the leaked build. Other groups that want to start up their own RaaS now have a level playing field without having to go through months of development and costs associated with building up an operation from scratch.
4. The LockBit "brand" has likely suffered a blow, even though the operators would like to let on that everything is running smoothly. It would have been expected that following the leak, LockBit would have tried to change their build and add something innovative to strengthen their position as a leading RaaS provider. However, the development of LockBit seems to have stagnated. This possibly leads back to the source of the leak: Was the disgruntled employee one of the core developers who they have struggled to replace?

The ransomware affiliate model is essentially a partnership, and just like any business relationship, any partner should be questioning the long-term viability of an organization with such questionable internal security.

Over the past few months, we've seen a downshift in confidence towards LockBit. There have been several factors causing concern for affiliates. In April 2023, the group began to add several posts to the leak site, which contained fake victims with made-up leaked data. It's possible that this was part of internal testing. However, it's

highly likely that this could have been an attempt to artificially inflate the number of victims to give the impression that the threat actor was maintaining their success.

One of the most notable concerns is the apparent instability of the threat actor's infrastructure. During a ransomware operation, the negotiation phase is highly dependent on the threat of data being released. If the leaked data is not available, then it becomes more difficult for affiliates to apply the pressure required for a successful negotiation. Back in August 2023, we observed unusual behavior in LockBit's leak site, with victims being added and removed within minutes, resulting in an error message.

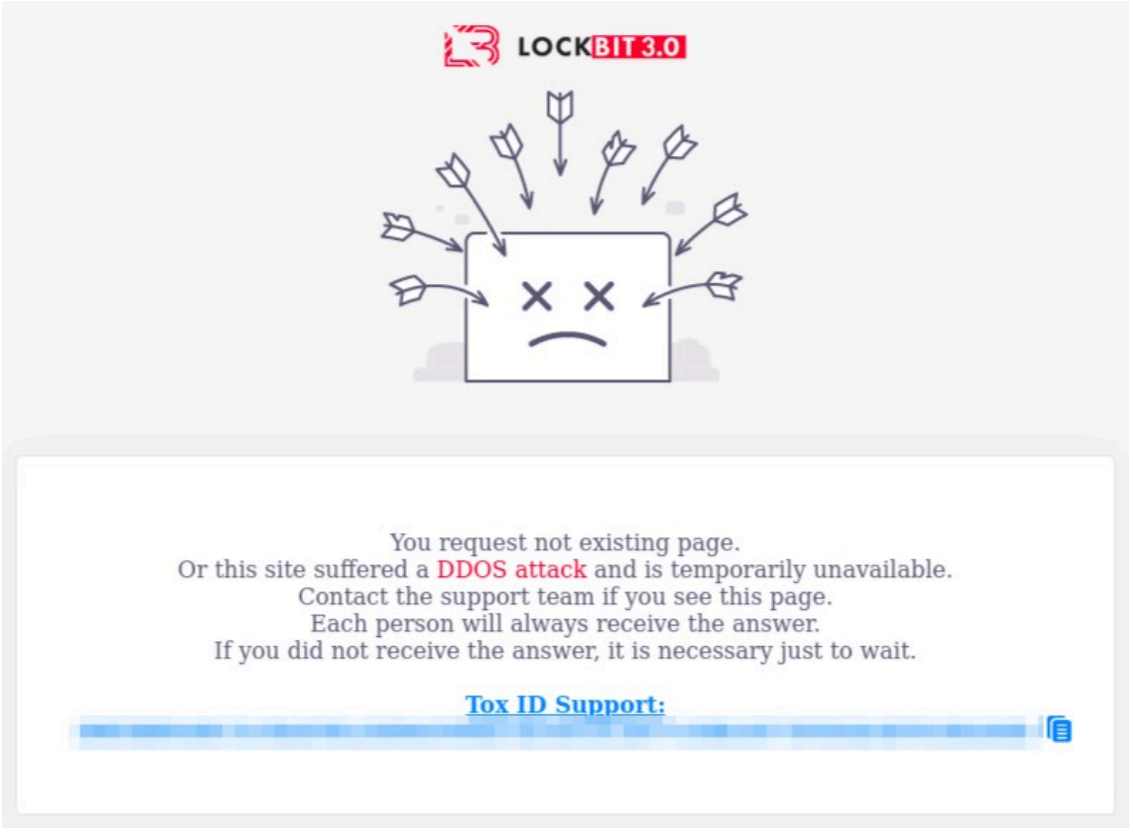


Figure 3. LockBit leak site error message

Throughout the first half of 2023, there were also numerous claims by the group that they had released data following an organization's failure to pay a ransom demand. What's interesting is that there was no way to download the data that was "published" — there was simply a post saying the files were published. This topic is thoroughly covered in the *Ransomware Diaries Volume 3* series by Jon DiMaggio.

In September 2023, LockBitSupp issued a proposal via a Tox message to implement new rules for affiliates in an effort to improve negotiations. The decline in successful negotiations and increased frustration with negotiators could signal that the quality of affiliates that the operation attracts has been impacted by the lack of innovation and continued technical issues. The proposal included a minimum payment along with a fixed discount of 50%. It also proposed that payment should not be less than that of the amount covered by the victim's insurance policy. Shortly after, the actor Bassterlord (an affiliate of LockBit and the leader of a group called the National Hazard Agency) published a tweet suggesting that these rules were being applied.


LockBit
Those working on the blog

LockBit

A very important social survey, please read very carefully and vote.

Since the rank of the partners and the rank of the attacked companies are very different, the redemption prices and the size of discounts are not regulated in any way, one partner can take 10% of the annual turnover of the company, for example, there are cases where the amount of payment is $ 2 million, and the annual turnover of the company is $ 10 million, and other similar cases with similar figures, and another less experienced partner does not negotiate very competently, needs money very much and takes 0.00005% of the annual turnover of the company, for example, there are cases where a company with an annual turnover of $ 2 billion, a partner agrees to buy 100 thousand dollars, recovery companies keep statistics of payments and, in accordance with the ongoing results of negotiations, may try

to repeat the success of "talented" negotiation, and in fact just luck and lack of discipline and regulation of the amount of payments in the partner program, in my opinion, this is very harmful in future negotiations to all partners and those who have a lot of money and experience, and those who recently took a small payment, and now they will hope for a large one, when the money for food appeared.

Beginners and those who currently have little money often agree to make discounts as much as 90% of the initially announced fair price, because of such discounts, other partners who have a lot of money and strong nerves suffer, recovery companies thinking that any partner can make a 90% discount are trying to push this discount in negotiations with experienced partners where there will never be such a discount, because of this, the deal either breaks down as experienced the partner publishes information after insignificant offers, or negotiations are delayed for a long time in anticipation of a large discount

The purpose of the survey is to develop new rules of negotiation tactics and pricing policy for the size of the buyout and the allowable sizes , the opiniondiscounts. Will be of each partner is taken into account. The new rules will help improve the situation and stabilize the amount of payments at a high level.
You can offer your options, you can vote for several items:
1. Do not change anything and leave everything as it is, each partner does whatever he wants and has no restrictions, as it has always been.

2. Limiting the size of the minimum allowable requested amount at the beginning of negotiations, depending on the annual turnover of the company, for example, 3% and prohibit making a discount of more than 50%, for example, if the company's revue is $ 100 million, you start negotiations with $ 3 million and do not have the right to take a ransom of less than $ 1.5 million.

3. Do not impose any restrictions on the minimum allowable requested amount, since it is not always possible to qualitatively inflict maximum damage to the attacked company, but limit the maximum possible discount from the amount of the ransom you originally announced to 50%, for example, if you say because the redemption price is 1 million dollars, you have no right to take less than 500 thousand dollars.
4. Prohibit taking an amount less than the figure indicated in the cyber insurance, provided that you have found a cyber insurance.
5. Prohibit taking an amount less than 50% of the figure indicated in the cyber insurance, provided that you have found cyber insurance.
6. Another option suggested by you.

It is very important for me to hear your opinion if I am wrong about something or missed something or you have your own brilliant idea how to maximize our income and become richer.

[open on a new tab]

Figure 4. Translated version of the proposed rules from LockBitSupp

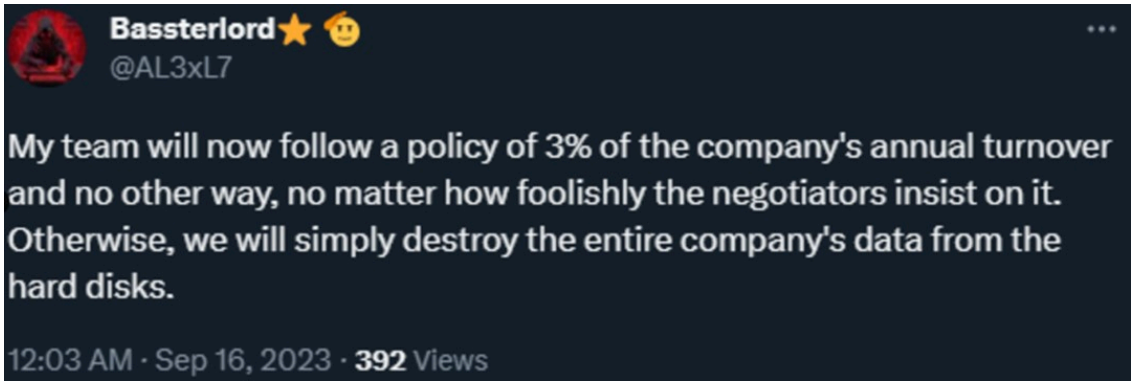


Figure 5. Tweet by Bassterlord endorsing LockBit's new rules

In early November, we also observed some unusual behavior in the leak site mirrors. For several days, there were inconsistencies when trying to access them, and a lot of the site mirrors would redirect to the victim chat page. This is yet another example of the litany of technical issues the group seems to be suffering from while trying to maintain a stable operational infrastructure.

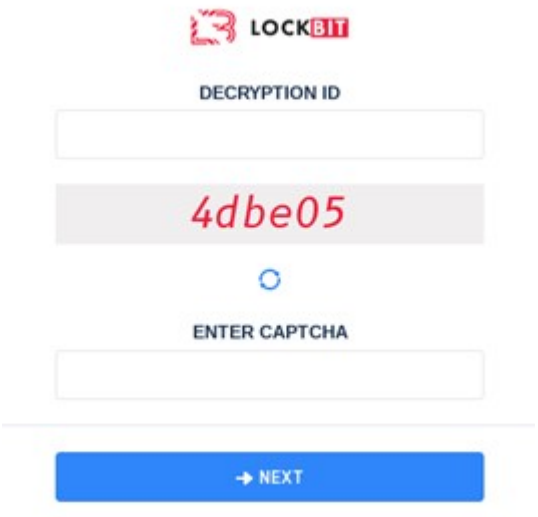


Figure 6. What users see when they are redirected from the leak site to the victim chat site

It's clear that LockBit has been having issues throughout 2023, and it stands to reason that this is having a negative impact on their ability to attract or retain affiliates. There are several factors at play that may dissuade a potential affiliate from joining the group:

1. Affiliates seem to be losing faith in the program. To compound LockBit's technical issues, there also seems to be a shortage of staff for the operators. They're not as responsive as they used to be, sometimes taking days or even weeks to reply to inquiries.
2. The new affiliate rules standardize ransom demands and constrain the amount an affiliate can earn may not go down well and could result in further migration of affiliates.
3. The delay in an updated release of LockBit, combined with the attempts to attain rival builds suggest there's a brain drain in the operation and their core developer(s) may have privately moved on (as opposed to the very public departure of the person who leaked the LockBit build).
4. The recent public call to ALPHV (BlackCat) and NoEscape affiliates to join the LockBit group has an air of desperation around it. In the past, threat actors were clamoring to join the group. In more recent times, however, it looks like the LockBit operators are desperate for fresh affiliates and actively looking for opportunities to capitalize on the misfortunes of rival groups.

At the end of January 2024, a malicious actor using the moniker "michon" on the XSS forum opened a thread for arbitration against LockBitSupp. The malicious actor claimed that LockBitSupp refused to pay for access they provided that led to a ransomware payout. In the beginning of the thread, it appears that this malicious actor was somewhat inexperienced and did not outline conditions for the sale at the time. However, as the thread progressed and private chat logs were provided, there was a clear shift in sentiment from observers. There emerged a negative reaction to LockBitSupp's attitude towards the malicious actor and the nature of the transaction, with a number of observers giving LockBitSupp's responses a thumbs down. As the thread ended, LockBitSupp was directed to pay 10% of the ransom payment to the claimant within 24 hours.

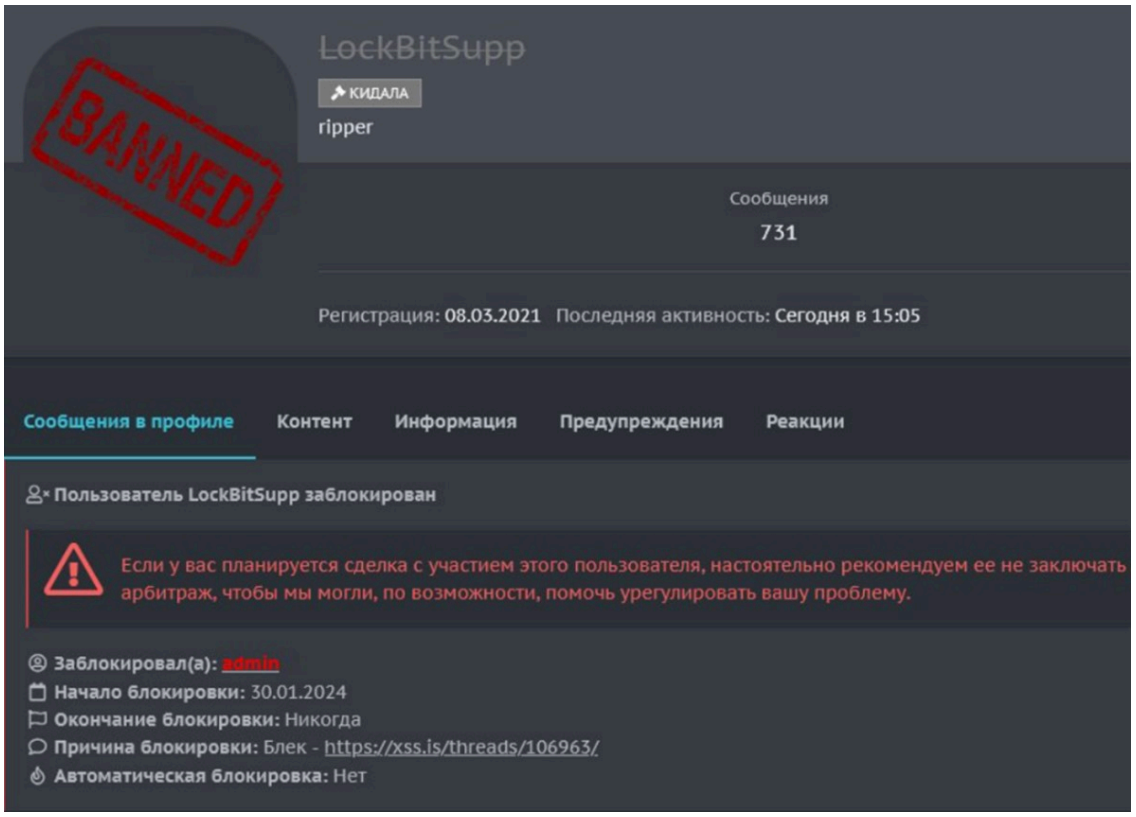
There are a couple of key observations to be made after examining the contents of the forum thread;

1. LockBitSupp displayed a degree of arrogance when responding to both the claimant and other supporters who weighed in on the topic. The actor came across as someone who was "too big to fail" and even

showed disdain to the arbitrator who would make the decision on the outcome of the claim.

2. This discourse demonstrated that LockBitSupp is likely using their reputation to carry more weight when negotiating payment for access or the share of ransom payouts with affiliates. This is probably not the first time that someone has tried to begin a working relationship with LockBitSupp and has been dealt unfavourable terms. The fact that this was played out in public may also dissuade others from dealing with LockBitSupp in the future.
3. The type of behavior exhibited by LockBitSupp is similar to those observed with other operators of RaaS groups that have overstepped the line and inevitably ended up disbanding. There are no positives for LockBitSupp with regards to this arbitration. The malicious actor has quite likely alienated their peers, potential access suppliers, and affiliates.

On January 30, 2024, LockBitSupp was banned from the XSS forum and assigned the status ripper/scammer. The actor was also subsequently banned from the Exploit forum.



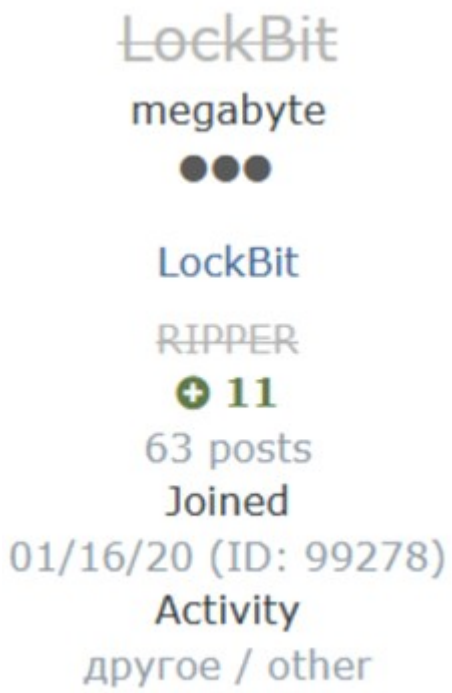


Figure 7. LockBitSupp banned from the XSS and Exploit forums

LockBit's Decline

According to our confirmed breach data, there are some indications that although LockBit has maintained its position as the intrusion set with the largest number of attacks, it's overall share of ransomware impact has seen a steady decline over the last two years. There is a clear decline in numbers when we look at the figures for LockBit 2.0 and the shift to LockBit 3.0, although there was a slight rise during the fourth quarter of 2023, which may be attributed to the increased law enforcement activity against rival groups. LockBit offered affiliates the chance to migrate to their operation during this period.

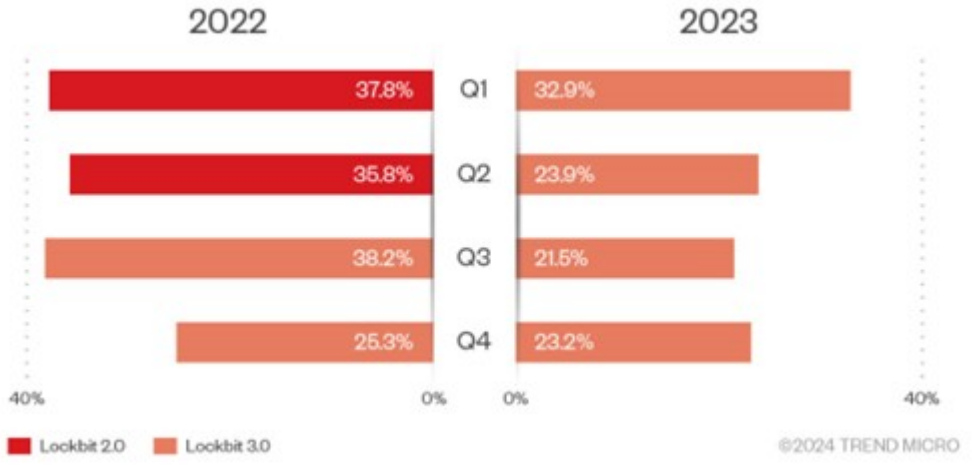


Figure 8. Breach data from Q1 2022 to Q4 2023 shows that LockBit's market share (among the major groups we track) as the RaaS with the highest number of attacks suffered a decline in late 2022 and throughout most of 2023 (click the image to enlarge)

Threat actors associated with LockBit

This section will examine the people behind the LockBit group. There are several nicknames and online personas that are frequently associated with LockBit, including LockBit (forum user) and LockBitSupp (forum user).

The official online presence from the group was through "LockBitSupp" — the username used by the user/s offering LockBit support, and "LockBit," a more generic account that, through multiple conversations, has shown a direct involvement with the LockBit affiliate program. Notably, the LockBit user ran a publicity stunt on the XSS forum, where they offered to pay US$1,000 to anyone getting LockBit tattoos. Public information shows that LockBit spent US$20,000 to pay people who got tattoos done. However, some forum members complained about being scammed by LockBit after they got the tattoo but were not paid for it.

Another prominent member of the criminal underground, Bassterlord, is believed to be associated with the LockBit group. Bassterlord is a criminal who claims to be from Ukraine (LDNR, according to their response in a public interview) and has previously worked with the REvilnews article RaaS group. Bassterlord is famous within the cybercrime community for selling the second edition of their manual for attacking corporate networks. Bassterlord's handle on the XSS forum was renamed to "National Hazard Agency," which is believed to be a sub-group within the LockBit operation. This group has claimed responsibility for high-profile attacks such as the one launched against the Taiwan Semiconductor Manufacturing Company (TSMC) in June 2023. A known handle used by Bassterlord on Twitter ("AL3xL7") has openly mentioned their affiliation to the LockBit group.

Yet another prominent member of the cybercrime underground who has previous ties to LockBit is the malicious actor "wazawaka" (identified by the FBI as Mikhail Matveev), who was known to be an affiliate throughout 2020 and 2021. Matveev was indicted by the US Department of Justice in May 2023. It should be noted that this malicious actor communicates regularly with Bassterlord and has made references to rejoining the LockBit affiliate program.

An unknown actor, "Ali_qushji" claimed to have compromised the LockBit server infrastructure. However, LockBitSupp contradicted this information, mentioning that the leak actually originated from a disgruntled developer. This person uses the handle "protonleaks" and is thought to be a former employee of the groupnews article and the individual who leaked the build.

Figure 9. A user claiming to have leaked the LockBit build

The new LockBit-NG-Dev version

Recently, we came into possession of a sample that we believe represents a new evolution of LockBit: an in-development version of a platform-agnostic malware-in-testing that is different from previous versions. The sample appends a "locked_for_LockBit" suffix to encrypted files which, being part of the configuration and therefore still subject to change, leads us to conclude that this is an undeployed upcoming version from the group.

Based on its current developmental state, we are tracking this variant as LockBit-NG-Dev, which we further believe could form the basis of a LockBit 4.0 that the group is almost certainly working on.

A detailed analysis follows in the technical appendix, but some key changes include:

- LockBit-NG-Dev is now written in .NET and compiled using CoreRT. When deployed alongside the .NET environment, this allows the code to be more platform-agnostic.
- The code base is completely new in relation to the move to this new language, which means that new security patterns will likely need to be created to detect it.
- While it has fewer capabilities compared to v2 (Red) and v3 (Black), these additional features are likely to be added as development continues. As it is, it is still a functional and powerful ransomware.
- It removed the self-propagating capabilities and the ability to print ransom notes via the user's printers.
- The execution now has a validity period by checking the current date, likely to help the operators assert control over affiliate use and make it harder for automated analysis systems by security companies.
- Similar to v3 (Black), this version still has a configuration that contains flags for routines, a list of processes and service names to terminate, and files and directories to avoid.
- It also still has the ability to rename the filenames of encrypted files to a random one.

As mentioned in the introduction, those looking for a detailed analysis of LockBit-NG-Dev can refer to the **technical appendix**.

Conclusion

The criminal group behind the LockBit ransomware has proven to be successful in the past, having consistently been among the top impactful ransomware groups during their whole operation. In the last couple years, however, they seem to have had a number of logistical, technical, and reputational problems.

This has forced LockBit to take action by working on a new much-awaited version of their malware. However, with the seeming delay in the ability to get a robust version of LockBit to the market, compounded with continued technical issues — it remains to be seen how long this group will retain their ability to attract top affiliates and hold its position. In the meantime, it is our hope that LockBit is the next major group to disprove the notion of an organization being too big to fail.

More information on LockBit can be found in this link.
