



The Ransomware Diaries:
Volume 3

LOCKBIT'S SECRETS

All Available Data Published!

REVIL
2019 - 2022

LOCKBIT
2019 - 202?

HIVE
2021 - 2023

By Jon DiMaggio

Date: 15 August 2023

WARNING:

PLEASE DO NOT TRY THIS AT HOME.

**ENGAGING WITH RANSOMWARE
CRIMINALS SHOULD ONLY BE CARRIED OUT
BY TRAINED PROFESSIONALS.**

**WHILE IT SEEMS “COOL” TO INTERACT
WITH BAD GUYS, DOING SO PUTS YOU AND
YOUR EMPLOYER AT GREAT RISK.**

**PLEASE DO NOT ATTEMPT TO EMULATE
WHAT YOU SEE IN THIS REPORT UNLESS
YOU HAVE THE KNOWLEDGE, EXPERIENCE,
AND SKILL SET TO PERFORM
SUCH ACTIONS.**

THANK YOU!

Contents

Intro	4
Key Findings	5
Previously on the Ransomware Diaries	7
LockBit Gets Handsome	8
The Royal Ransomware Drama	12
Gotta Make That Green!	15
LockBit's American Dream	16
The Baddie Dox	19
A Royal Mess	23
Behind the Scenes of the Royal Mail Attack	28
LockBit Goes to Space Camp	30
An Apple a Day Keeps LockBit away	33
Dark Who?	35
The Tox Oday	37
You're Under Arrest for Being Stupid	43
Reflecting on the arrest	44
LockBit's Secrets	47
Secret #1: LockBit Sucks at Publishing Victim Data ..	47
Secret #2: Extended Support Wait Times	55
Secret #3: There Is No Ransomware Update	56
Secret #4: LockBit Must Tely on Leaked, Poorly Coded, or Stolen Ransomware	58
Closing Time	60

Intro

In this volume of the Ransomware Diaries, I will share interesting, previously unknown details of the LockBit ransomware operation that LockBit has tried very hard to cover up. Until now, you have been lied to about LockBit's true capability. Today, I will show you the actual current state of its criminal program and demonstrate with evidence-backed analysis that LockBit has several critical operational problems, which have gone unnoticed.

This time, besides using fake personas, I have spoken directly with the gang and many of its affiliate partners. I also reached out to victims. I learned what happens behind the scenes during the ransom negotiations and the relationships LockBit has with its affiliate partners and competing rival gangs. LockBit has secrets it does not want either party to know. Now, I look forward to sharing them with you!

Before I begin, I need to share a significant event that took place as I finalized this report. Since August 2023, LockBit's leadership has vanished and is now unreachable to fellow gang members, including its affiliate partners. Several of LockBit's close associates have shared concern that the gang's leadership may be on the run or dead. While LockBit's data leak site and infrastructure is up, no one appears to be actively managing LockBit's RaaS program.

Before I begin, I need to share a significant event that took place as I finalized this report. In August 2023, LockBit's leadership has vanished and was unreachable to fellow gang members, including its affiliate partners, for the first two weeks of August 2023. During that time, several of LockBit's close associates shared concerns that the gang's leadership was on the run or dead. Then, on August 13, LockBit reappeared on private channels as if it never happened. Still, during the time LockBit was gone, LockBit's data leak site and infrastructure were up, but no one was actively managing it. The question is: why? Fortunately, I have some answers.

Key Findings

Before I begin, I want to share the following key findings identified over the course of my research:

- **LockBit may currently be compromised.** After sharing my findings in this report with the LockBit, gang, it disappeared and went dark on Tox, which it uses to communicate and run its operation. At the same time, I received a message from affiliates who thought I hacked the gang. Then, I received another message from a third party who indicated they may have hacked the gang's infrastructure. At the time, it was unclear if the humans behind the LockBit gang had gone into hiding, or were just taking a break, but their lack of activity was significant, I believe the gang went dark to clean up the intrusion into its infrastructure.
- Lockbit has an issue publishing and leaking victim data. It has used propaganda on its leak site and a strong narrative across criminal forums to hide the fact it often cannot consistently publish stolen data. Instead, it relies on empty threats and its public reputation to convince victims to pay. Somehow, no one but affiliate partners noticed. This problem is due to limitations in its backend infrastructure and available bandwidth.
- **LockBit recently updated its infrastructure to address these deficiencies.** However, this is a gimmick to make it appear that it corrected the previously mentioned problem with posting victim data. It claims victims' "FILES ARE PUBLISHED". Often, this is a lie and a ploy to cover up the fact that LockBit cannot consistently host and publish large amounts of victim data through its admin panel, as promised to its affiliate partners. Further, over the past six months LockBit has presented empty threats it failed to act upon after many victims refused to pay. Yet, somehow, no one has noticed.
- **Affiliates are leaving LockBit's program for its competitors.** They know that LockBit is unable to publish large amounts of victim data, despite its claims. Additionally, it takes them days to weeks to review the correspondence and reply to their affiliate partners. Some requests simply go unaddressed by the LockBit gang.
- **LockBit missed its most recent release date to produce an updated ransomware variant to support its partner affiliates.** Instead, it relies on outdated, publicly available ransomware, leaked from its competitors.
- **LockBit wants to steal ransomware from its rival ransomware gangs to use in its own operation and offer through its admin panel.** It wants to provide an al-a-carte-style ransomware offering and become a one-stop shop for hacker affiliates.

PART I:
OUR
STORY

Previously on the Ransomware Diaries

In the first volume of the *Ransomware Diaries*, I detailed my account of the LockBit ransomware gang, which I wrote after spending months working undercover using fake personas to monitor conversations and build relationships with cyber criminals.

The [Ransomware Diaries Volume 1](#) demonstrated how human intelligence can add value when applied to the technical analysis of cyber threats. Hopefully, this volume will build upon that work.

The most significant difference between my initial research and this report is that I have been able to establish a direct line of communication with the leader of LockBit, and many of its affiliate partners, directly as myself. While risky, talking directly with the gang made for a greater personal interaction, allowing me to obtain more information than I could with fake personas alone.

Still, I used personas while investigating criminal activity discussed in this report and monitored conversations across dark web forums. Additionally, I scrutinized LockBit's leak site, examining each new victim post to observe how LockBit published data and negotiated with its victims.

I contacted victims, asking questions about their incident, and seeking details to better understand the human interaction they experienced dealing directly with ransomware criminals. Now, I will share details of my ongoing investigation as it took place.

Finally, I have significant, previously unknown findings, which LockBit has tried to hide from both the public and its partners, which I will expose to provide an inside look into the LockBit ransomware gang.

This is our story.

LockBit Gets Handsome

After publishing my research, I was concerned about how the LockBit gang would react once they saw I had posted details of their internal operation. Pissing off the world's most notorious cybercriminal, who has deep pockets and strong ties within Russian organized crime, is not the smartest thing I have done, so I was curious about their reaction.

Subsequently, in January, after the Ransomware Diaries went live, I logged onto both Exploit and XSS – two forums often used by Russian cybercriminals. The first comment I saw from LockBit was made on XSS and was not what I expected. A security researcher asked LockBit what it thought of the report. You can see LockBit's response in Figure 1.

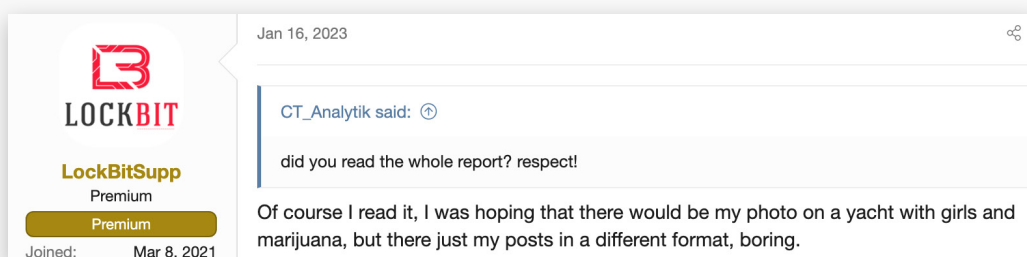


Figure 1: A comment from LockBit on the underground forum, XSS, about my Ransomware Diaries Volume 1 report.

I laughed when I read the comment. Later in a direct conversation, I asked LockBit to send me pictures of it on its yacht to include in this report; however, it declined to send them!

Next, I checked the Exploit forum. There were no comments about my report, but LockBit definitely sent a message. When I viewed Lockbit's account, I saw my own face staring back at me! Apparently, LockBit decided to update its avatar and use my face to represent its persona.

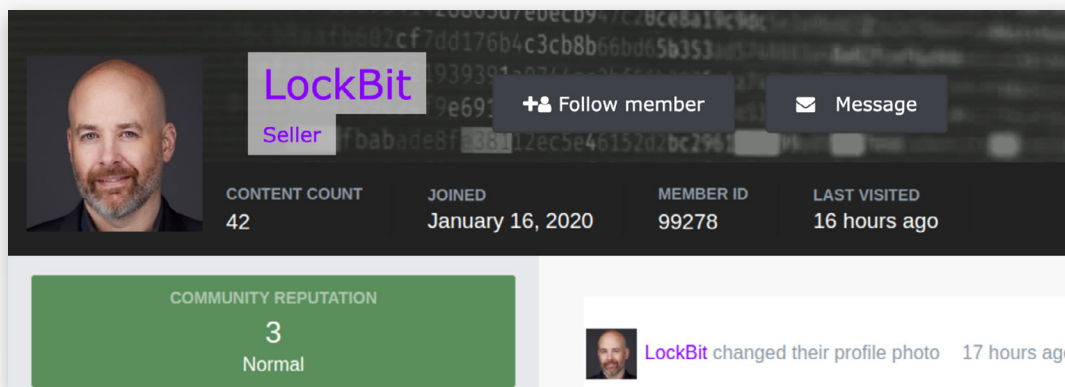


Figure 2: My Oh Sh!t moment – LockBit updating their profile with my picture. At least it's a good pic.

At first, I was unsure if this was an authentic account associated with the same criminals I interacted with previously. In those interactions, I engaged with the gang through an account they used, named “LockBitSupp,” on the XSS forum. This other account present on the Exploit forum, with my face as the avatar, was titled “LockBit.”

Still, I wanted to see if there was a “LockBitSupp” account on the Exploit forum, so I conducted a query for the username. I found it had previously existed, but had been dormant since May of 2021, when the forum admins banned ransomware content after the fallout of the Colonial Pipeline incident. Since then, the “rules” have been relaxed a bit, though recruiting for ransomware operations is still banned.

The criminal behind the “LockBit” account created it in January 2020, over a year before registering the “LockbitSupp” persona. The LockBit account had also been dormant for some time and only recently became active. Shortly after, in March 2023, the person behind the “LockBit” account made a new post that provided additional evidence, proving this was one of the gang’s personas.

You see, LockBit uses Tox, an encrypted communication application, to communicate with other criminals, journalists, and researchers. Similar to how a phone number is assigned to a phone, Tox has its own unique value used to identify and connect each account, which LockBit lists on the “contact us” section of their data leak site.



Figure 3: Lockbit Tox ID seen on their website and in a post by the “LockBit” account.

You can see in Figure 3 that LockBit's Tox ID documented on the "Contact Us" page is the same Tox ID provided in a post by the "LockBit" account that uses my face. It is also the Tox ID used by the LockBitSupp persona on the other forum (XSS) discussed in my previous research. Now, I was confident the account was authentic and used by core members of the LockBit gang.

The Tox ID convinced me, but the human traits behind the account were even more convincing. After spending so much time studying, observing, and profiling the LockBitSupp persona over the last year, I have become especially familiar with the human characteristics of the individuals behind LockBit's mask. As detailed in my previous research, at that time, at least two people operated the "LockBitSupp" account. One is the gang's leader himself.

Now, to be fair, it has always been professional with me. However, while engaging with other criminals, I have observed characteristics indicating it is closed-minded, sexist, racist, and sometimes quite dramatic when engaged. If the gang's leader were a celebrity instead of a criminal, it would have been canceled long ago.

At least two people operated the "LockBitSupp" account. One is the gang's leader himself.

Further, while I know this will anger it, its personality reminds me of "UNKN," the former leader and voice of the REvil ransomware gang. Ironically, the two hated one another and constantly argued in front of other criminals on underground forums.

The second person facilitating the LockBitSupp account is friendlier and more pleasant to deal with. It is also much younger than the leader, based on his mannerisms and communication style. It is nice to talk to in comparison to Mr. Grumpy pants!

So now that you know there are multiple people behind the persona, understand that when I talk about LockBit as an individual, I am referring to the first personality I describe. I am referring to the gang leader and not one of the other LockBit members operating the account.

Since I began my research, additional people may now respond from this account. Still, the two I described have historically worked the persona since the early days of its operation.

I also noticed that the gang's leader frequently posts on the criminal forums today, compared to the Tox account, which has a tiered structure to facilitate its operation. That account is where I have communicated with the younger member more frequently. I mentioned that there may be additional gang members responding from the account today, because LockBit's Tox account is almost always online. All of this and the stark differences in personalities and mannerisms make me confident in this assessment.

Now, let me explain Lockbit's workflow to operate Tox. With a 24/7 operation, the gang has a structure to successfully manage and handle the volume of communication requests and questions that come in daily. LockBit's leadership assigns rotating responsibilities to the gang's lower-ranking members, who keep the queue moving and answer requests. They respond to messages from "online" accounts first and then filter out remaining requests as time permits.

However, it takes longer to get a response whenever I ask for anything significant where a decision is needed. The lower-ranking members handling the account must push the request to the leader and await his response. I know this because I have talked with the younger guys more often on Tox, but when I have something significant to ask, it takes them much longer to respond to me. Then when I do get the response, the mannerisms, feel, and tone are entirely different.

Additionally, several very bright researchers with expertise in the Russian language have told me that one of LockBit's close partners within the gang, who often operate the Tox chat and occasionally posts on criminal forums, is of Ukrainian descent.

I am not an expert and cannot attest to this myself, but I have been told there is a difference in the grammar and verbiage used by someone who learned to speak Russian in Ukraine vs. someone who is a native Russian speaker. This would also explain why LockBit distanced itself from Russia and publicly posted a message after the war began, stating that the gang was a-political and would not take sides.

Note: *You should take the information regarding the LockBit partner and his link to the Ukraine with low confidence, because I personally have no evidence to support the finding. However, in the interest of encouraging further research by more qualified personnel, I decided to share it anyway. If you have evidence to further this discussion, please contact me.*

Now, let's get back to the forums and the new, more handsome Lockbit account that started this story! In true LockBit fashion, it was about to unleash a dramatic plot to deceive and steal from another notorious criminal organization, the Royal Ransomware gang.

In walks Baddie.

The Royal Ransomware Drama

In late January 2023, Lockbit responded to a forum thread titled “LockBit 3.0 Black Builder.” In the thread, an affiliate ransomware hacker asked about the leaked LockBit ransomware builder, which I discussed in the [Ransomware Diaries Volume I](#).

LockBit tells the affiliate:

“The builds from the merged builder differ in size from the builds from my panel, hence the conclusion that the offended encoder somehow modified the builder, there are no guarantees that there is no universal master key.” – LockBit

In other words, LockBit is saying that since the file size of the builder had changed, someone may have altered the source code. LockBit warns that the developer could have altered the builder to allow for a universal decryption key, which, if true, would allow victims to decrypt their data without paying a ransom.

I suppose this is possible, but in reality, the variance in the file size could be anything from an altered feature to a universal key or even a backdoor. I have looked at the leaked builder, and the changes appear insignificant. It likely would have been discovered if there were an issue, since the disgruntled developer leaked the builder [in September 2022](#).

Several days after LockBit made the statement, another persona who goes by the moniker “Baddie” joined the conversation. Let’s pause and establish Baddie’s relevance before continuing with our story. You see, Baddie is a persona I follow, and I bet many of you reading this will recognize it as well. If not, as pointed out by security researcher Azim Khodjinaev, Baddie claims to be a senior member or possibly the leader of the Royal ransomware gang.

More notably, if truly the leader of Royal ransomware, Baddie is likely part of the former Conti gang. Various [researchers](#), myself included, as well as [cyber security vendors](#) have attributed Royal ransomware as a spin-off group that evolved after the Conti gang [ceased operation](#) in May 2022.

While outside the scope of this report, one of my favorite bad guy chasers, [@BushidoToken](#) (AKA Will Thomas, CTI Researcher at Equinix) wrote a great blog detailing exactly how Royal aligns with the Former Conti gang.

You can read more about the Conti/Royal ransomware link here: <https://blog.bushidotoken.net/2022/11/the-continuity-of-conti.html>



Figure 4: Azim's post showing a post from Baddie on a Russian forum [looking for affiliate hackers to join Royal ransomware](#).

Back to our story...

The Lockbit persona had just posted a comment on the underground forum, Exploit, addressing a hacker who wanted to use the leaked LockBit ransomware builder in extortion attacks. LockBit told the hacker it could make much more money using Lockbit's admin panel as a partner in their operation, as opposed to working alone with the leaked ransomware variant.

This is where Baddie comes into the conversation. Apparently, Baddie is upset with LockBit. While it does not translate well, Baddie is asking LockBit if partnering with their gang is immensely profitable and successful, then why is LockBit trying to convince Royal Ransomware affiliates to give LockBit access to the Royal ransomware builder? You can see part of the conversation in Figure 5.

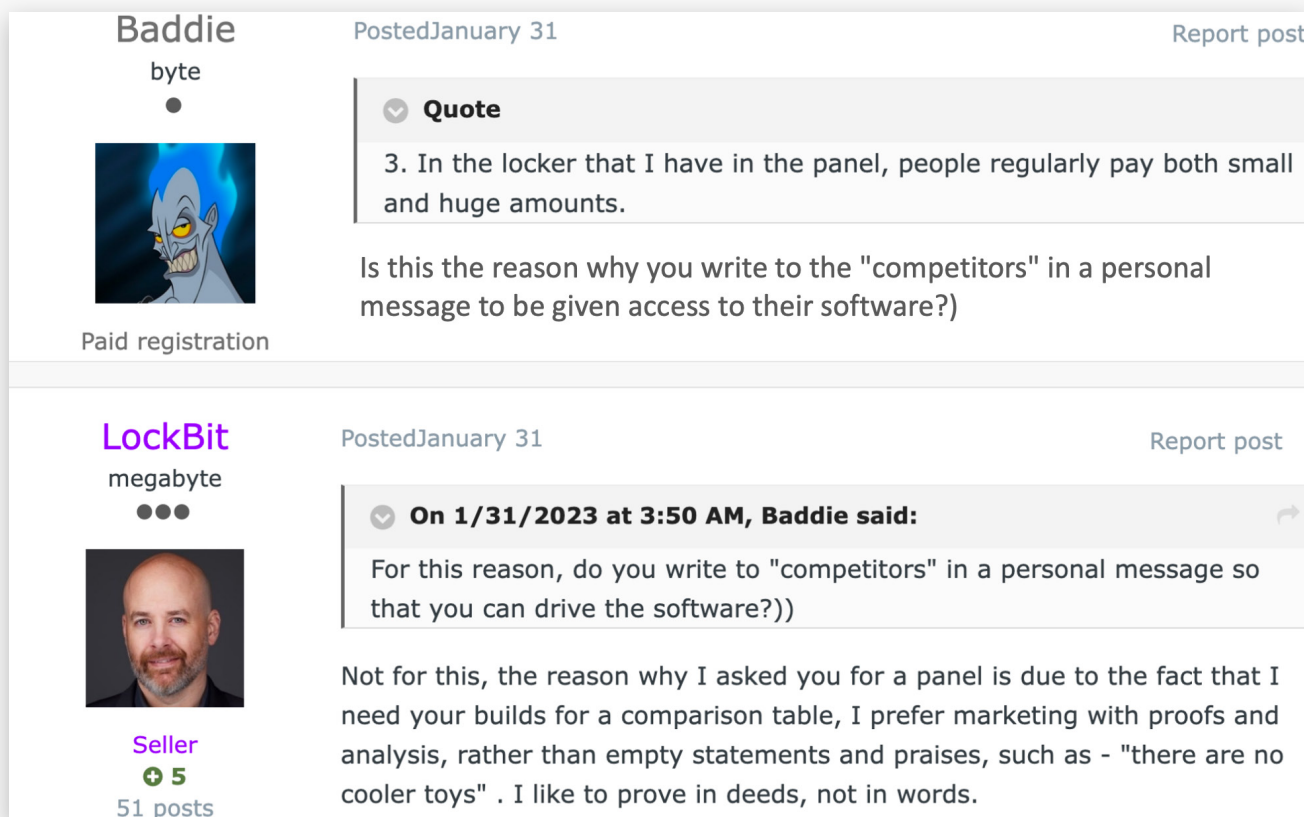


Figure 5: Baddie challenging LockBit about its inquiries into Royal Ransomware

In response, LockBit quickly denies any wrongdoing and states that it wants access to Royal's builder to create a ransomware comparison table. LockBit claims it wants to demonstrate that LockBit Black is the most efficient ransomware offering on the criminal market. Like Baddie, I immediately questioned this. LockBit, you are a criminal, and while I appreciate the business-like effort, you are not taking part in a Gartner vendor assessment. No one is buying this.

Baddie, of course, is reluctant to give LockBit access, and the two men begin to argue. Baddie accuses LockBit of attempting to gain access for other reasons, such as stealing from competitors. Further support of this claim came from VX-underground on January 27, 2023, when it shared interesting news about a new LockBit variant titled "Lockbit Green."

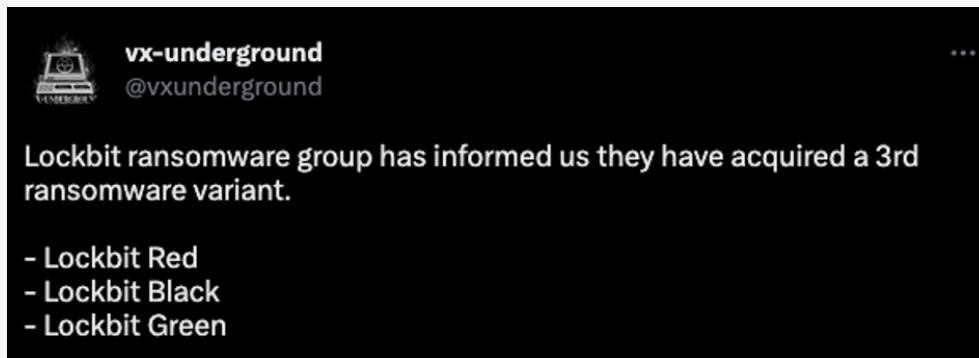


Figure 6: [VX-Underground](#) tweet announcing the release of LockBit Green

This was strange. Usually, LockBit would discuss and beta test a new ransomware variant amongst affiliates before its release. Additionally, LockBit released both Red and Black variants in June each year, not January. Looking at this closer, it became apparent why this release is less significant than previous LockBit updates, which we will discuss next.

Gotta Make That Green!

Before I saw the conversation between LockBit and Baddie, a message appeared from the LockBitSupp persona on the other prominent criminal forum, XSS, in December 2022. The message stated that LockBit planned to release an updated payload based on the leaked Conti ransomware in the coming weeks. Strangely LockBit deleted the post shortly after.

I did not know how I felt about the short-lived post, and I considered that LockBit might be trying to mislead researchers, so I did nothing with the information. I did not think LockBit would use someone else's ransomware because it is focused on building its brand and has a massive ego. Using a competitor's ransomware payload when you have your own would be like working for Apple and owning an Android phone. You just don't do it.

Now, let me explain why LockBit deleted its comment. Remember, I said many of the forum posts today are made by the leader of LockBit. However, the younger member occasionally makes posts from the same account. This was one of those occasions.

You see, the junior LockBit member should only have announced their plans to use a competitor's ransomware once they were ready to add it to their admin panel. The senior member saw the post and deleted it a few hours later.

So, in January 2023, when I read VX-underground's tweet, I wanted to verify if this was, in fact, a revised version of Conti's ransom payload. Fortunately, I did not have to wait long

to validate the claim. Shortly after the release, Bleeping Computer [published an article](#) detailing the similarities and differences between this new release, renamed LockBit Green, and previous Conti variants.

As you likely know by now, LockBit Green is a modified version of Conti ransomware. The two obvious changes were, first, the ransom note, which now directs victims to LockBit negotiation infrastructure, and second, it no longer appends “.lockbit” to encrypted files. Instead, it uses random characters, which are added to each file.

Bleeping Computer and Prodaft, a cyber intelligence company, had an interesting theory explaining why LockBit is using one of its competitor’s payloads. The company believes LockBit wants to attract Conti’s former affiliates, who prefer using the Conti payload. This makes sense since many affiliates have moved on from LockBit’s program to support other competing ransomware operations.

Sadly, the information I found leads to a far worse scenario for defenders and incident responders. To explain, I need to share information and details on other behind-the-scenes events leading up to this, before I present my findings surrounding the use of LockBit Green and other ransomware LockBit is trying to obtain. For those who can’t wait, you can jump ahead to the section titled “LockBits Secrets,” where I will explain everything in greater detail. For the rest of you, please read on.

LockBit’s American Dream

Over the next week, In February 2023, LockBit and Baddie continued their argument. LockBit continued to deny it was trying to steal Royal’s builder, and Baddie continued to call out LockBit’s true intentions. This is where the conversation took a strange turn.

I am unsure if LockBit believes what it says or is trying to deflect and steer the conversation away from itself, but he calls Baddie a gangster and accuses it of working for the FSB. Based on the information I read in the Conti leaks, I think it is highly probable Baddie once did and may still have an association with the FSB, if it genuinely was a former member of the Conti gang, as suggested.

The comment itself is not significant to my research, but LockBit’s negative sentiment towards the intelligence agency is meaningful. In the conversation, LockBit claims that Maksim Yakubets, a wanted criminal the United States [indicted](#) in 2019 for leading the EvilCorp ransomware gang and currently [supporting](#) the FSB, is working with Baddie and Royal ransomware.

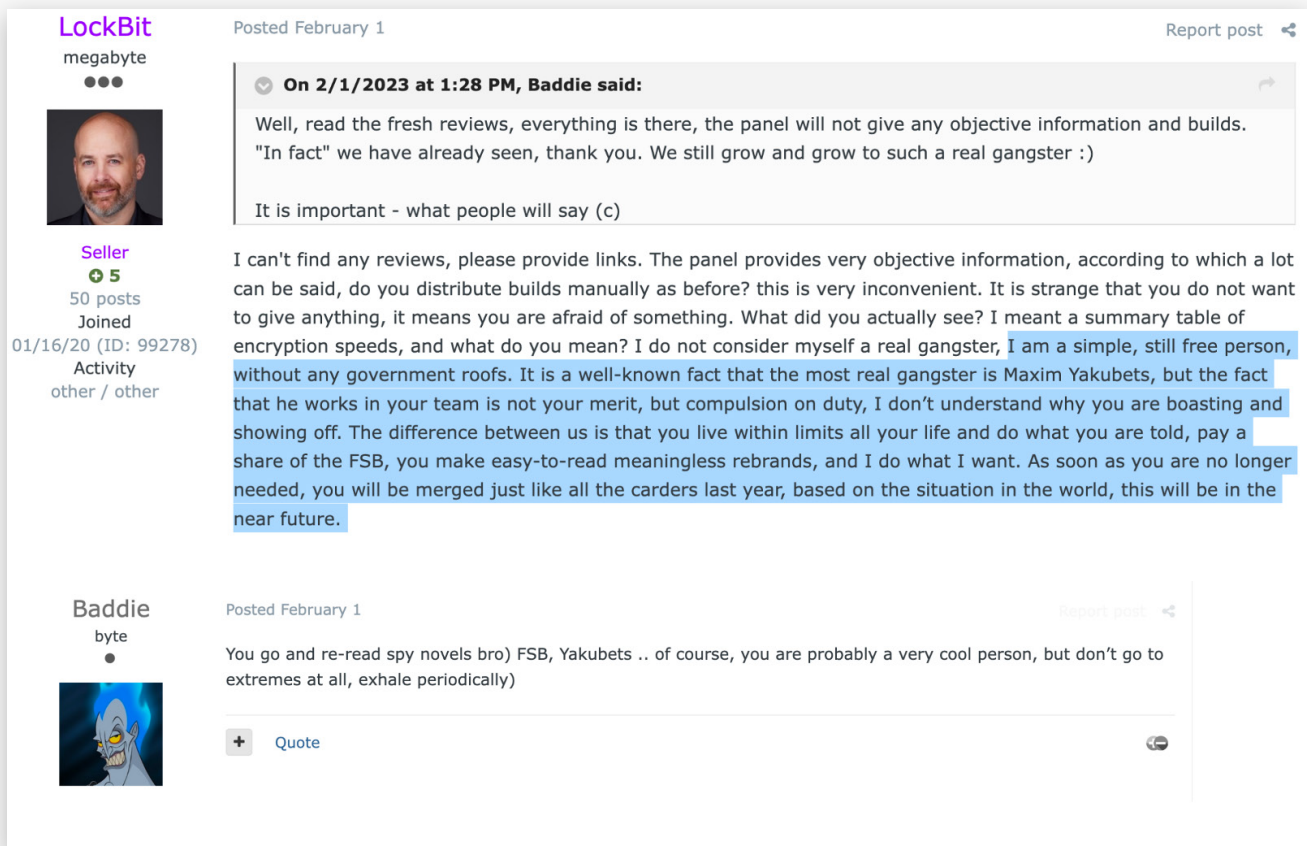


Figure 7: LockBit accuses Baddie and Royal Ransomware of working with Yakubets and the FSB.

The irony in the accusation is that EvilCorp used LockBit ransomware in attacks [last year](#), but LockBit must have forgotten about that. Figure 7 above displays the correspondence between the two gang leaders.

It's important to understand that LockBit does not believe he will ever be arrested, let alone imprisoned. It believes it is too intelligent to be caught. It thinks the only organization that could find him is the FSB, since they have deep connections in the Russian ransomware scene.

This is why the leader of LockBit hides from the FSB as much as it hides from the FBI. It is afraid of having his assets frozen and being forced to support the Russian government. Can you imagine if you went from making hundreds of millions a year to having to take a mediocre salary as a government employee? If that happened, LockBit might have to sell his yacht. That would be true punishment for LockBit.

For these reasons, I began questioning whether LockBit moved to another region outside of Russia. I don't think it would go far and is likely in a former CIS country, but I also noticed it was previously far more careful with his words when discussing the FSB. The fact that it speaks freely and with negative sentiment toward the organization may signify it has

moved outside of their reach. Of course, if you ask LockBit, which I have, it will tell you it is chilling out, enjoying life in the US!

I have spent time trying to determine who the leader of LockBit is and where it lives. Making this determination is not easy, so I have gone down many rabbit holes to explore and assess each of the theories and claims.

LockBit intentionally puts out misinformation. For example, if you recall from Volume 1, LockBit has claimed it lived in China, the Netherlands, Hongkong, and now the US. It even claims it is a partial owner of several restaurants in New York City and owns a Tesla! None of this is likely true, but it makes me laugh and wonder how it comes up with this stuff.

Figure 8 below shows LockBit stating that it now resides in the US. *It wouldn't lie, would it?*

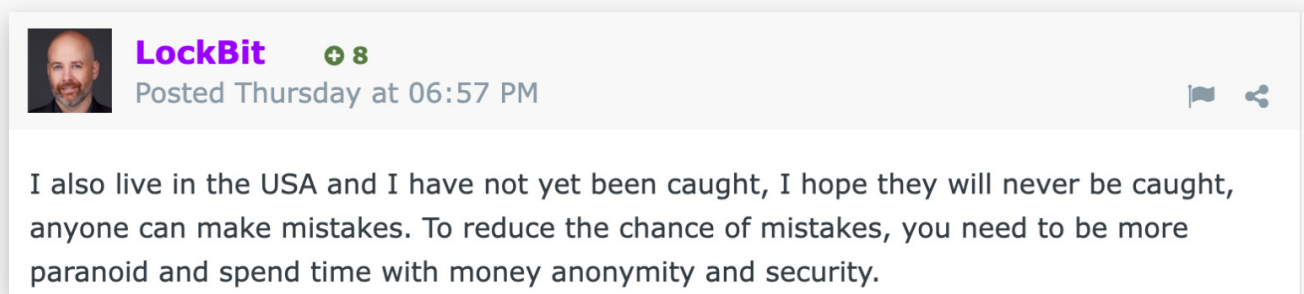


Figure 8: LockBit claims it is in the USA

Again, we should not discount the claims made by a criminal, but we certainly should not take their word for it either. I think it is highly unlikely that LockBit is in the US, but anything is possible. I think it's important to explore all possibilities from a government and law enforcement perspective.

I wrote this section of the report to share my belief that LockBit has fled Russia and is now living in another CIS country. If I am wrong, and it is still in the region, it clearly feels comfortable that Russian intelligence is unaware or incapable of discovering its true identity.

The Baddie Dox

Keeping your identity private is important when you are the leader of a ransomware gang, which is why it's ironic that LockBit would be associated with outing another ransomware figurehead.

Based on the correspondence I have discussed between January and March 2023, Baddie and LockBit do not like one another. Even so, while stealing from each other may be tolerated, there are rules you don't break in the criminal world, such as doxing.

If you are not aware, doxing is when you reveal the human identity of the person behind an anonymous online persona. It's like ratting someone out, which can have serious repercussions when the person identified is a wanted criminal. It is a rule that can get you banned from many forums where criminals conduct business.

For these reasons, I was surprised to see an exchange between LockBit and other criminals, revealing the alleged identity of the man behind the Baddie persona. It started when a member of the forum posted a link to a US Treasury press release that named several members of the TrickBot malware operation. Several of the men listed in the sanctions were also [associated](#) with the Conti ransomware gang. The Treasury issued sanctions against the men for their role in cybercrime operations and money laundering schemes.


It may sound odd that criminals would post and discuss a Treasury press release on an underground hacking forum, but conversing on articles related to ransomware operations is a fairly common practice.

LockBit saw the post and asked about Stern and Baddie, whom the US treasury did not list. We have already discussed Baddie, but if you are not aware, Stern is one of the senior managers of the Conti operation whose correspondence and role were [observed](#) in the chat logs found in the Conti leaks earlier last year.

Shortly after LockBit asked the question, another persona responded, sharing details about Baddie's identity. The information included Baddie's real name, birthdate, passport number, address, education, and social media accounts.

I honestly have no idea if the man listed is really Baddie. This certainly could be misinformation, and I found no incriminating information about the person. Yet, if it were Baddie, I would not expect to easily find evidence linking its identity. I decided not to post the information and photo in case it belonged to an innocent person.

You can see relevant parts of the conversation in Figure 9 below.



eILurko
RAID array


User

Joined: Oct 25, 2021
Messages: 59
Reaction score: 10
Deposit: 0.0025 ₿

Feb 9, 2023

Article: <https://home.treasury.gov/news/press-releases/jy1256>

Vitaly Kovalev | Bentley, Ben
Maksim Mikhailov | Baget
Valentin Karyagin | Globus
Mikhail Iskritskiy | Tropa
Dmitry Pleshevskiy | Iseldor
Ivan Vakhromeyev | Mushroom
Valery Sedletski | Strix



LockBit

LockBitSupp
Premium

Premium

Joined: Mar 8, 2021
Messages: 637

Feb 9, 2023 #3

This is all interesting, but where are stern and Baddie?

When you write to me in a personal message, do not check the "Encrypt correspondence (AES256 + SHA256)" box, if you are afraid that someone else will read your private messages, then write via secure PRIVATE NOTE and you can send a picture or file via [secure FILE SHARE](#)

Report Like + Quote Reply

floppy disk

XBanned

Joined: Oct 27, 2022
Messages: 1
Reaction score: 1

LockBitSupp

And here comes Baddie.

[redacted] | Baddie

[redacted]

date of birth 09/12/1986 (36 years old)
passport number - 27 00 194273
He was originally from Moldova,
lived in Kaliningrad,
telephone in the Russian Federation - [redacted]
currently lives in Germany (has a criminal record in the Russian Federation), hiding from persecution in Germany.
telephone number in Germany - [redacted]
Education: graduated in 2003
Kant (former Kant Russian State University, KSU)
Skype: [redacted]

[redacted]

Social VK networks - [https://vk.com/\[redacted\]](https://vk.com/[redacted])
classmates - [https://m.ok.ru/dk?st.cmd=\[redacted\]](https://m.ok.ru/dk?st.cmd=[redacted])
twitter - [https://twitter.com/\[redacted\]](https://twitter.com/[redacted])

Photo

Figure 9: The conversation about the Treasury sanctions and the dox of Baddie, a senior member of Royal ransomware.

It is strange that the dox was the only post made by the account used to release the information, despite being created in October 2022. Shortly after leaking Baddie's alleged identity, the account was banned by administrators on the forum for attempting to dox someone, though LockBit's role was overlooked.

Many criminals have complained that LockBit gets special treatment on these forums and is rarely held accountable for its actions. I wondered if LockBit is behind the dox against Baddie for challenging its operation. It would not be the first time LockBit has released information on someone it does not like. Time will tell.

PART II:
THE VICTIMS'S
STORY

Now that you know what the leadership of the LockBit gang has been up to behind the scenes, let's discuss the high-profile public attacks that have taken place since January 2023. The public attacks I will discuss have been reported and discussed heavily by the media and other researchers. So, to add value, I will share behind-the-scenes aspects involving the gang itself.

A Royal Mess

Despite LockBit's drama and antics with other ransomware criminals, the gang and its partner hacker affiliates have been busy in the first half of 2023. LockBit kicked off the year by breaching, encrypting, and stealing sensitive data from [Royal Mail](#), the largest postal service provider in the United Kingdom.

On January 12, 2023, Royal Mail followed the instructions left in the ransom note presented on their encrypted systems and logged into LockBit's chat negotiation portal. The conversation began rather cordially.

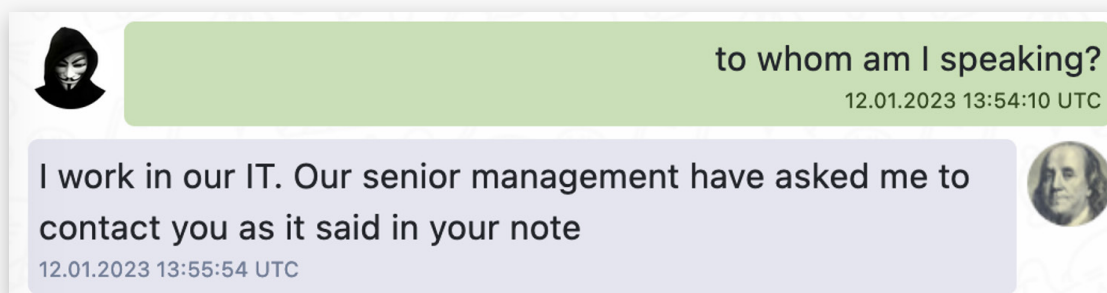


Figure 10: Beginning of Royal Mail ransom negotiations

Now, you may be asking yourself why an employee in the IT department would negotiate such a critical transaction. Well, if you believe what the employee said, it's because his manager asked him to!

I find it highly unlikely that someone in IT was the best option Royal Mail could come up with to manage this crisis. Further, I would have expected LockBit to immediately realize that the "IT guy" was a professional negotiator, not just an employee from Royal Mail's help desk.

Understand that ransomware gangs do not like dealing with negotiators and often terminate discussions once identified. Many will state this upfront because negotiators often drag out the negotiation process to buy the company time, then try to lowball the ransom payment.

Basically, they are an annoyance to ransomware gangs that want the victim to quickly pay for their “post pentest services,” AKA the Ransomware attack.

To my surprise, LockBit did not flag the employee as a hired negotiator and instead continued the conversation.

Let me tell you, for an “IT guy” it did a fantastic job delaying and getting LockBit to decrypt files as “proof” of their decryption capability. It also stalled the gang from posting Royal data on their leak site.

The IT guy had such a nonchalant approach, as though this was just another day at the office. At one point, in the middle of LockBit’s demands, The IT guy told the Lockbit extortionist that it was “time for bed” and that it would talk to him Monday!

Anyways, time for bed. The board has meetings this weekend and we will not have anything new to speak about until Monday while they make their decision.



Figure 11: The “IT guy” goes to bed.

Now at this point, you would expect the LockBit negotiator to realize that the company was stalling for time. Instead, it continued to ask if Royal Mail was ready to pay.

The funniest part of all of this is the extortion demand LockBit requested. The gang wanted Royal Mail to pay \$80 million! That would be the highest ransom paid by any company to date. Further, LockBit had the audacity to tell Royal Mail, “You are very greedy and don’t want to pay for my service.”

One of the negotiator’s stall tactics was to ask LockBit how it came up with the \$80 million figure. Lockbit told him that \$80 million was 0.5% of their revenue and should be easy for Royal Mail to pay. LockBit actually told Royal Mail that it was in their best interest to pay because once it posted Royal Mail’s data publicly, the government would fine them 4% of their annual revenue, amounting to \$640 million. This was how LockBit justified its ransom demand, which is comical.

From January 26 through February 2, the “IT guy” continued to masterfully stall the LockBit negotiator. It told LockBit that the \$80 million ransom was not plausible and that the “Board” would not approve it. To further delay progress, the IT guy argued that they were not the Royal Mail that Lockbit thought they were but instead a much smaller subsidiary of the bigger organization.

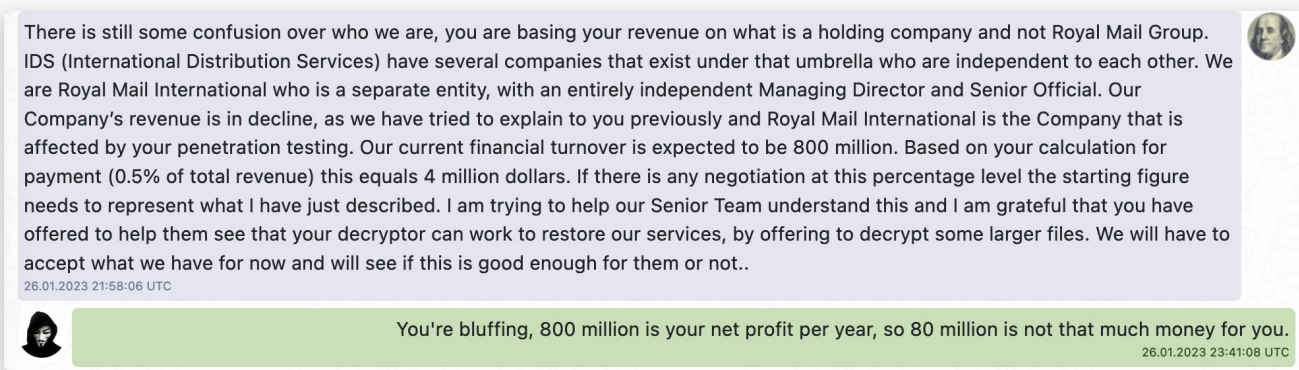


Figure 12: Segment of the chat negotiation log between LockBit and Royal Mail

For every answer LockBit had, the Royal Mail negotiator would restate his argument that they were just a small company owned by Royal Mail. The stonewalling frustrated LockBit, who then began sending various links to websites and wikis that showed information about the Royal Mail corporate structure and financial earnings.

I am not sure why LockBit kept arguing or felt the need to justify its ransom demand, but it was clear to me that the “IT guy” was playing with LockBit at this point.

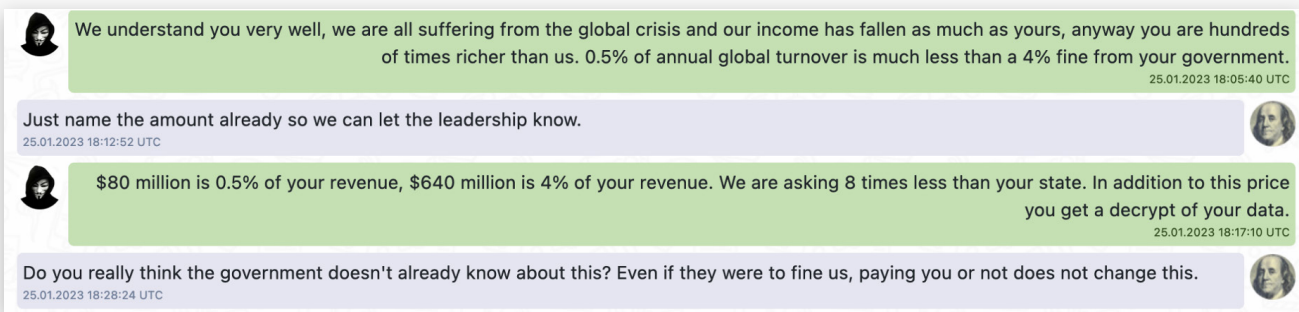


Figure 13: Segment of the chat negotiation log between LockBit and Royal Mail

There was another interesting moment in the negotiation exchange. Royal Mail told LockBit that they needed specific files, totaling 6GB of data, decrypted to send life-saving medical equipment that hospitals needed to be delivered. Royal Mail claimed that without this equipment, patients would die.

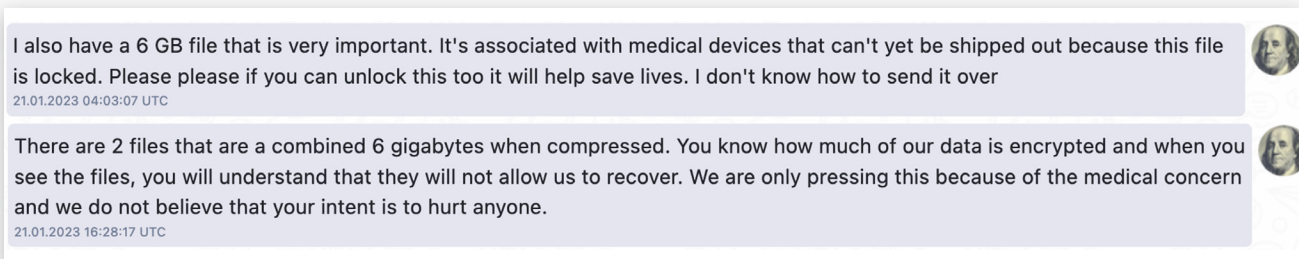


Figure 14: Royall Mail requesting LockBit decrypt files necessary to “save lives”.

It was no surprise that Lockbit did not care. LockBit claimed the files were not related to transporting medical supplies. Instead, they were critical files Royal Mail could use to help restore their data. LockBit was correct, but I don't blame Royal Mail for trying! Either way, it was a good tactic, since LockBit [has given](#) decryption keys to hospitals in the past after its partner affiliates shut down emergency systems.

Royal Mail's attempt to regain access to their data by lying about its purpose upset LockBit. In response, on February 6, 2023, LockBit publicly posted some of Royal Mail's data and told them they had 50 hours to pay. Royal Mail and the "IT guy" never responded to LockBit again.

On February 9, LockBit announced it had released all of Royal Mail's stolen data, making it available to download from LockBit's data leak site.

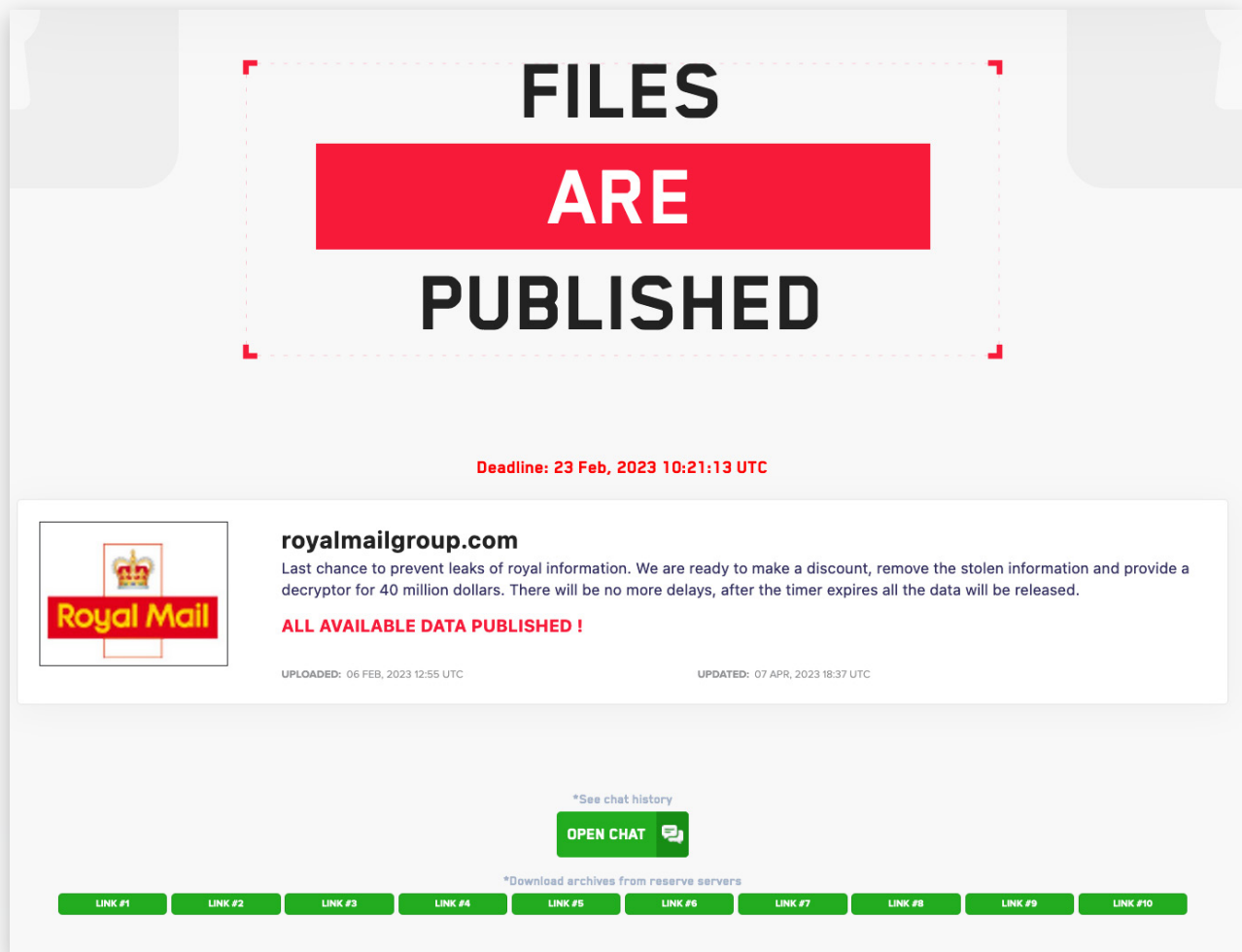


Figure 15: Royal Mail post on LockBit's data leak site stating it had published all available data.

As I was researching this report, something odd occurred regarding the Royal Mail data post. Previously, you could download the stolen data by clicking the "link" button on the

Royal Mail leak post shown in Figure 16. However, several months later, in June 2023, I checked again and could not access the stolen data. Instead, I was presented with this message:

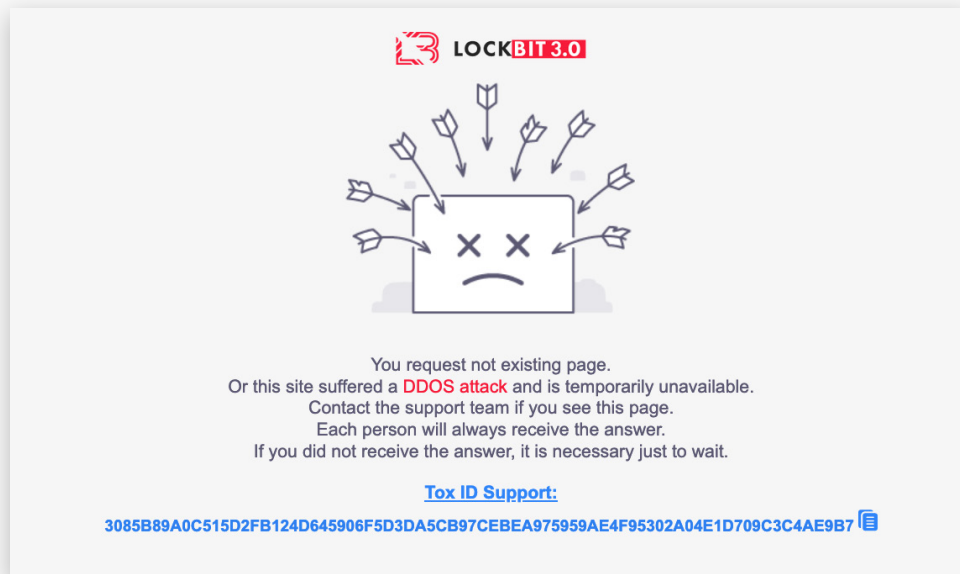


Figure 16: Message presented when clicking the link to download Royal Mail data.

This was strange because the LockBit data leak site claimed the data was present and available to download. If you recall from the first volume of the Ransomware Diaries, someone conducted a denial-of-service attack against LockBit when it tried to leak data from the cyber security company Entrust.

In the event, LockBit's entire infrastructure was down – not just the data download infrastructure associated with that site. I am not an expert on DDoS attacks, but it seems odd that LockBit has not reposted or leaked the data elsewhere. Perhaps LockBit is unaware, since the denial only affects the data download links themselves.

I am a fan of DDoS attacks against ransomware infrastructure when possible. It's effective and frustrates the ransomware gang and its partners. More importantly, it costs them time, resources, and money.

Despite its effectiveness, I do not believe Royal Mail has the expertise or legal authorities to conduct an offensive operation against anyone, let alone the LockBit ransomware gang. However, the UK Government does and would have the legal authority to strike back against a criminal operation. Perhaps that is who is behind the DDoS attack or perhaps LockBit is simply struggling to host the massive amount of stolen Royal Mail data. Regardless, I would love to see more victims follow suit when a ransomware gang leaks their sensitive data.

Behind the Scenes of the Royal Mail Attack

Despite the public reports and ongoing negotiations throughout January, LockBit officially claimed responsibility in February 2023. For several weeks in January, the media and researchers, including myself, attributed the attack to LockBit. Researchers and media initially blamed LockBit for the attack due to the ransom note left by the Royal Mail attacker.

Fellow cyber security researcher Danial Card, AKA “mRr3b00t,” posted an image of the note left for Royal Mail which you can see in Figure 17 below.

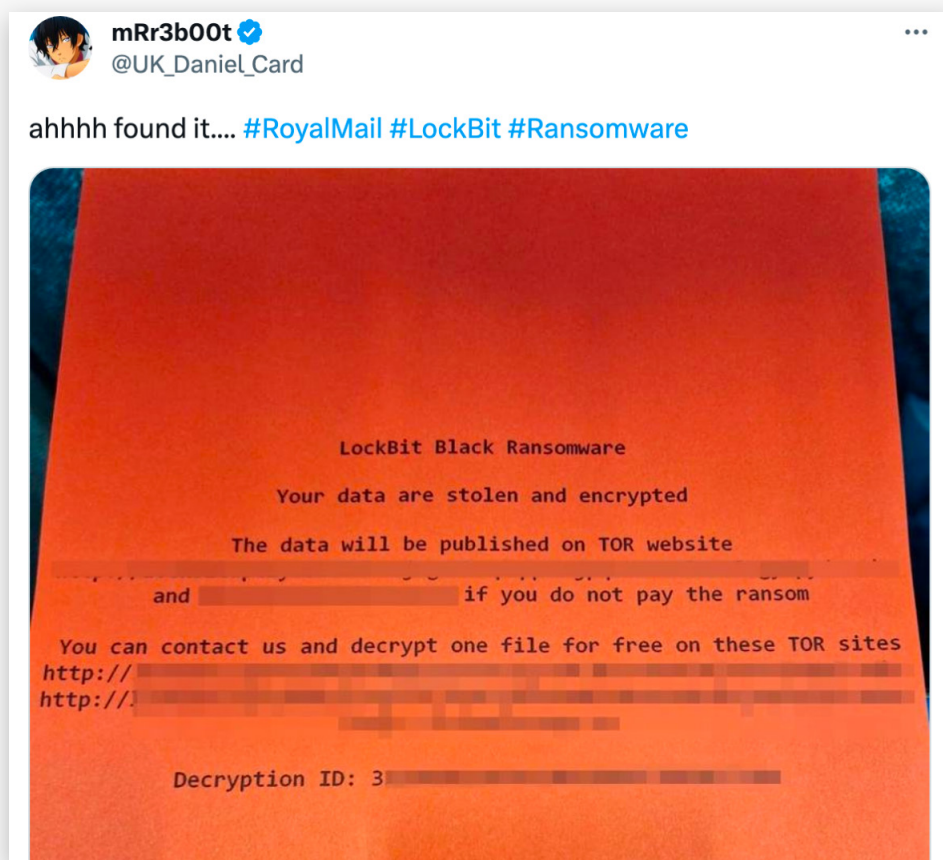


Figure 17: [Ransom note](#) associated with the Royal Mail attack [#]

The title “LockBit Black Ransomware” is listed at the top of the note and includes instructions to the victim directing them to go to LockBit’s victim negotiation website.

Despite the evidence, LockBit claimed it was not responsible. As seen in Figure 18 LockBit discusses the accusations with other criminals, claiming someone else used its ransomware to conduct the attack, but the gang did not authorize it. Instead,

on January 12, LockBit claimed the mystery attacker used the leaked version of its ransomware we discussed earlier.

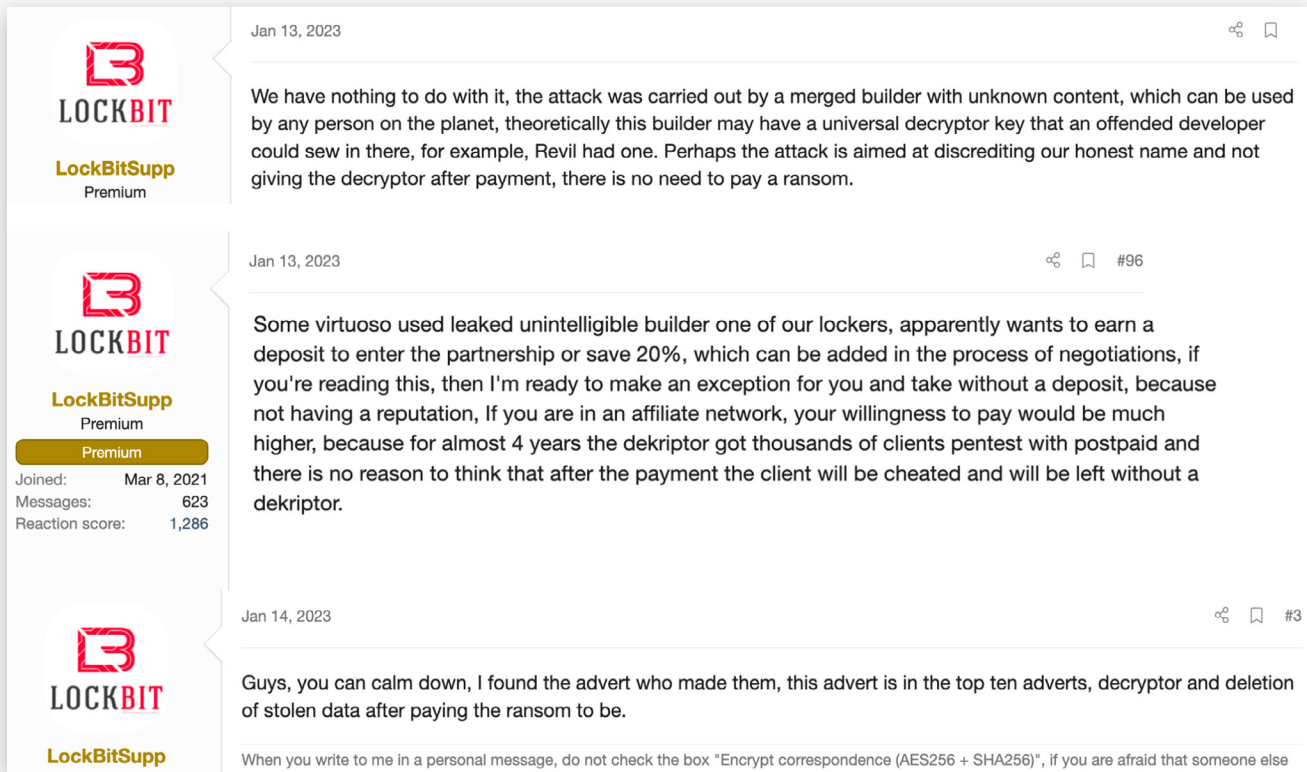


Figure 18: LockBit's response to initial accusations that it was behind the Royal Mail attack

The next day, on January 14, LockBit announced it had identified who was behind the attack. LockBit claimed it was one of its' affiliate partners but still took no responsibility.

Later in the conversation, LockBit stated, **"If you were me, with thousands of targets and hundreds of adverts (hacker partners), with an endless stream of targets, why would I follow them when I can just read the news?"**

This is a significant statement. Essentially, LockBit says it does not monitor or control the companies its partners attack. As we have seen with DarkSide and REvil ransomware gangs, attacking the wrong organization can have significant consequences. However, none of these reasons are why LockBit denied responsibility. You can see the real reason in Figure 19, from the LockBit Gang themselves.

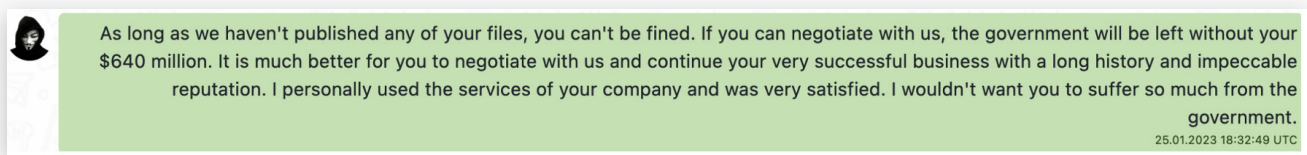


Figure 19: Message from LockBit top Royal Mail during negotiations

I laughed when I read this. I don't know many people who are happy with the postal service! LockBit also believes the government will fine Royal Mail, and the fee will be greater than the ransom. Lockbit uses this as leverage during the negotiation process, claiming the victim will save money and their reputation by making the extortion payment.

Lockbit believes the government won't fine Royal Mail unless someone claims responsibility and publishes leaked data. This is the real reason the gang denied responsibility for the attack, until they realized Royal Mail would not pay. It had nothing to do with the leaked builder and rouge partner excuse. I have noticed that LockBit uses this excuse whenever it's convenient, and it needs to deny responsibility.

For example, just a few weeks before the Royal Mail attack, LockBit [took down SickKids](#), a children's cancer hospital in Canada. In that attack, LockBit claimed the same excuse: that it had nothing to do with the attack, but instead was a rogue affiliate.

Once the media began to publish articles about suffering children who could not get medical attention, LockBit provided the decryption key and allegedly broke ties with the affiliate partner.

Royal Mail was not as lucky, and no decryption key was provided. In addition to leveraging the government fines during the negotiation process, there was one other reason LockBit denied responsibility. Initially, LockBit was concerned about the impact and response from the British government, since Royal Mail is [considered a critical national infrastructure](#). As time went on, and nothing happened, it became less likely that an official government response or sanctions were coming. Eventually, with mounting evidence and no apparent backlash, LockBit felt comfortable taking ownership of the attack.

LockBit Goes to Space Camp

In March, LockBit attacked Maximum Industries, an aerospace manufacturing company. While Maximum is just one of many victims who fell to LockBit attacks in March, it is a high-profile victim due to its partnership with the Space Exploration Technologies Corporation, AKA SpaceX.

As most of you likely know, Elon Musk owns SpaceX, and is one of the wealthiest people in the world. This is likely why Maximum Industries was such an important target to the LockBit gang. LockBit believed they could leverage the relationship between Maximum Industries and SpaceX for a big payday.

Shortly after the attack, LockBit posted a message on its data leak site, claiming to have obtained over 3,000 engineering diagrams. LockBit announced that SpaceX engineers certified the diagrams that Maximum Industries used to develop the parts and equipment used in SpaceX rockets. If SpaceX refused to pay the ransom, it would publish the data.

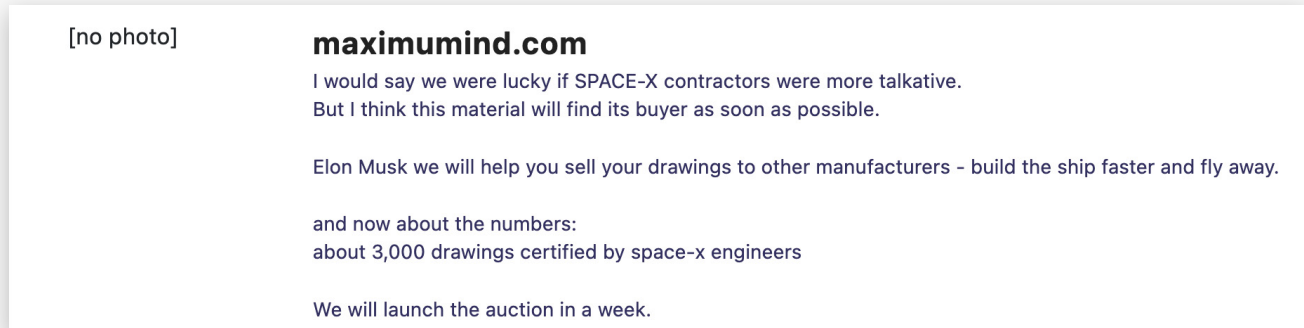


Figure 20: Maximum Industries post on LockBit data leak site

As I researched the incident, I found the most interesting aspect of the breach was not the SpaceX relationship. Instead, it was the method used to compromise and exploit Maximum Industries.

If you recall, I engaged with Bassterlord, one of LockBit's top affiliates featured in the [Ransomware Diaries Volume 2](#). I discussed the breach with Bassterlord, who shared details and later posted screenshots supporting his claims to social media.

Bassterlord told me he was not associated with the attacks, but is friendly with the hackers behind it. Bassterlord shared that the LockBit hacker breached Maximum Industries by exploiting a public-facing VPN infrastructure that had easy-to-guess usernames and passwords such as "test," "password" and "test_1234."

You can see a screenshot of the dumped creds and conversation between Bassterlord and the affiliate hacker behind the attack in Figure 21 on the next page.

According to Bassterlord, his former crew, the National Hazard Agency, is the affiliate behind the attack. They are now responsible for several high-profile breaches conducted over the past six months. They are on the rise within the ransomware affiliate hacker ecosystem.

In the end, neither SpaceX nor Maximum Industries paid the ransom. As time on the auction grew short, LockBit posted the following message on an underground forum.

On March 30, 2023, LockBit updated its website, stating that all of the stolen data was now published. But there was one problem: the data was not there. I will explain why later in the report.

host	origin	service	public	private	realm	private_type	JtR Format
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test123		Password	
2		443/tcp (Cisco SSL VPN)	test	test		Password	
2		443/tcp (Cisco SSL VPN)	test	test		Password	
4		443/tcp (Cisco SSL VPN)	test	test		Password	
4		443/tcp (Cisco SSL VPN)	test	test		Password	
5		443/tcp (Cisco SSL VPN)	test	test		Password	
5		443/tcp (Cisco SSL VPN)	test	password		Password	
3		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test123		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	thomas	password	Password	
1		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	thomas	password	Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test123		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	password		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test@123		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test@123		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test		Password	
1		443/tcp (Cisco SSL VPN)	test	test123		Password	
2		443/tcp (Cisco SSL VPN)	test	test		Password	
2		443/tcp (Cisco SSL VPN)	test	test		Password	
2		443/tcp (Cisco SSL VPN)	test	test		Password	
2		443/tcp (Cisco SSL VPN)	test	test		Password	
2		443/tcp (Cisco SSL VPN)	test	password		Password	
2		443/tcp (Cisco SSL VPN)	test	password		Password	

FishEye (Bas...)

=D

[Redacted]

there was a small office there and rhubarb was about nothing, I just looked at the files and hello there xD

FishEye (Bas...)

[Redacted]

do they even pay? [Redacted] and even all employees' personal numbers were turned off so that they would not call

FishEye (Bas...)

Understood;

[Redacted]

Well, I'm still negotiating

by the way, the spaceix contractors had a password test 12345678 if anything xD That's why I'm telling you that I've eaten up the campaign for you, you apparently just skipped them))

Figure 21: Screenshot from Maximum Industries [breach](#) and [Tox conversation](#) with LockBit Affiliate

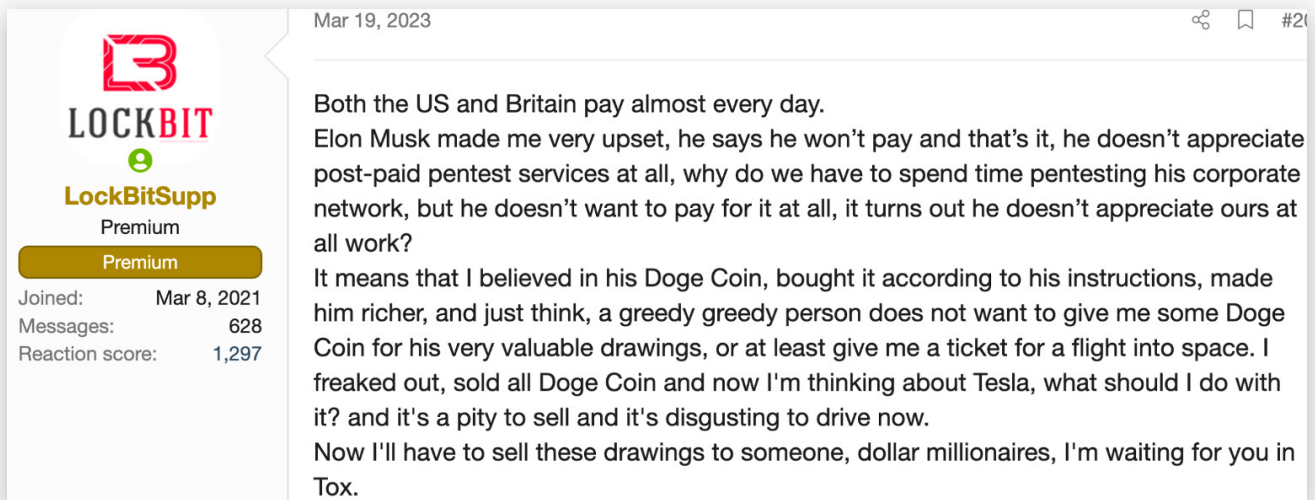


Figure 22: LockBit message to Elon

An Apple a Day Keeps LockBit away

On Saturday, April 15, 2023, MalwareHunterTeam [tweeted](#) a message stating they discovered the first instance of LockBit ransomware designed to infect Apple OS X operating systems, which VX-Underground made [available for download](#).

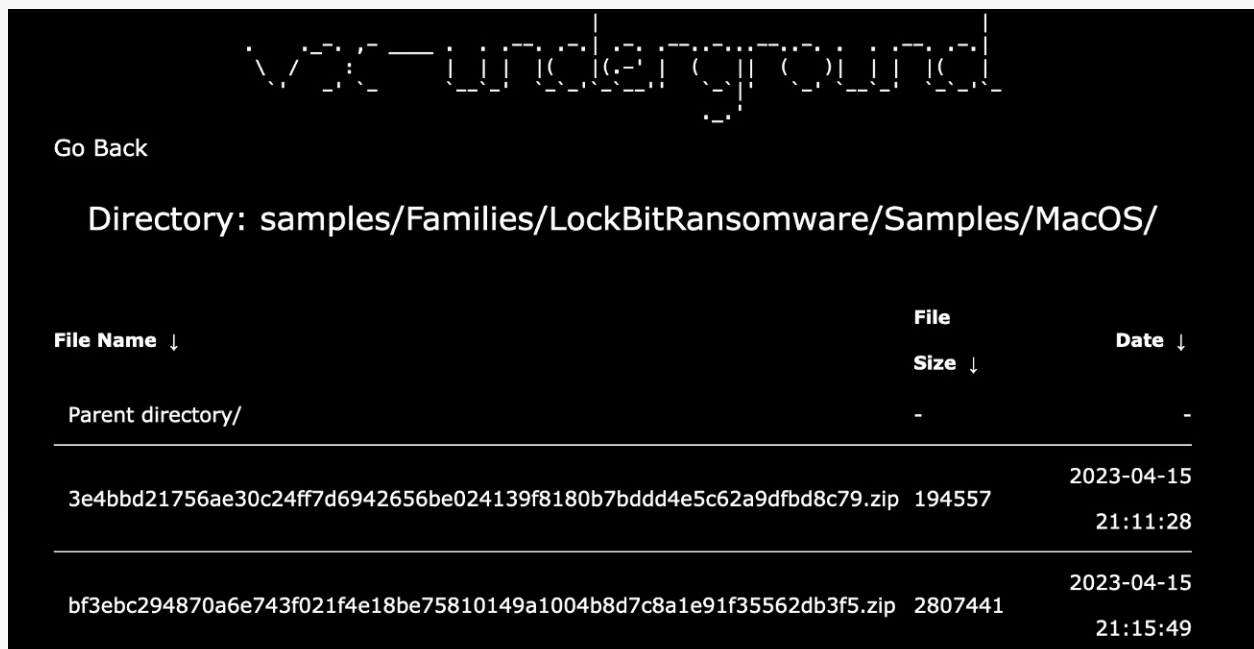


Figure 23: LockBit OS X samples

The weekend of the discovery, I communicated with several researchers who began analyzing the samples. While some had more details than others, there was a common theme

across all conversations. Something was drastically wrong with this ransomware build. There were so many issues that some of the first reports stated the build was an inoperable version of LockBit ransomware, which technically [was not true](#). It did, however, require a lot of *finessing* for the payload to execute and successfully encrypt data.

For example, you would have to bypass Apple's built-in security measures, which do not allow an application to run if it has an invalid signature. Instead, OS X [prevents](#) the ransomware from executing and provides a message directing the user to "move it to the Trash." This also explains why no one has ever reported an attack involving the Apple-based LockBit variant.

Additionally, the analysis of the binary provided clues about its intended use. The ransomware binary [had a hard-coded password](#) "test," which the operator had to provide for it to execute. The binary also had reference to Linux, Windows, and VMware files, which is strange, since this is meant to encrypt files on an Apple operating system.

Now, presenting the information after the fact makes it obvious this payload was not ready for use in attacks, but remember, when it was happening in real-time, information was all over the place.

So shortly after hearing this, I decided just to ask LockBit what was going on. Was this a development build, or was it intended for affiliates to use? Figure 24 shows his response.

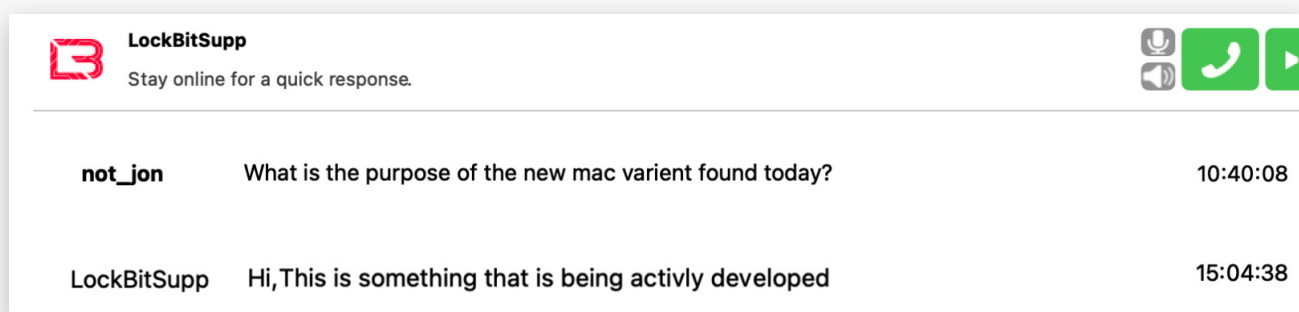


Figure 24: LockBit's response to the Apple variant's purpose

The payload MalwareHunterTeam found was not ready to be used in attacks. The fact that it ended up in a public malware repository before it was operationally ready shows that LockBit is having further issues with his developers and testers. Clearly, this was an OPSEC mistake.

Still, there is valuable insight we can gain from this discovery. The ransomware's existence demonstrates the effort and direction LockBit is moving. Clearly, LockBit is actively pursuing a ransomware payload that will encrypt Apple computer systems running OS X. We were fortunate enough to get an early warning sign of what is to come, and it is only a matter of time before a more polished version appears in LockBit attacks.

Dark Who?

In addition to the leaked Apple ransomware build found in April, another interesting and dramatic LockBit event occurred. The cyber security company DarkTracer noticed that Lockbit made several erroneous posts to its data leak site. The posts were not actual organizations but were fictitious company names and websites like “1.com” and “123.com.”

Even stranger, LockBit made a deadline for the made-up company to pay a \$60,000 ransom or have its imaginary data published. If the victim’s name did not give away that something was off, the \$60,000 ransom should be an indicator because the greedy LockBit gang would ask for a much larger ransom if this was a legitimate victim.

The other clue that this was not real was that LockBit populated the victim description with filler data. Figure 25 shows the tweet made by DarkTracer.



Figure 25: DarkTracer tweet about LockBit data leak site

DarkTracer called out LockBit, stating that its reliability had declined and that LockBit was negligent in managing its services. DarkTracer was correct; these were not actual victims. DarkTracer's only mistake was holding LockBit to the same standard you would a legitimate company.

For example, to test its functionality, you would not expect Bleeping Computer to create news posts filled with erroneous data on its public website to test its ability to publish stories. Instead, you would expect them to conduct testing and development efforts offline.

Apparently, you can't hold criminals to the same standard. You see, LockBit claimed it was simply [updating and testing its backend](#) service's functionality to upload victim data to its site.

This is where things should have ended, but in true LockBit fashion, nothing can end without drama. So, LockBit made a new post on its data leak site, shown in Figure 26.



Figure 26: DarkTrace post on LockBit's data leak site

Notice anything wrong? LockBit called out the wrong company. The tweet that started all of this was made by the company DarkTracer, not DarkTrace.

Making things worse, Lockbit posted a message asking to take DarkTrace CEO, [Poppy Gustafsson](#), out to dinner, and called her sexy. LockBit needs to learn to treat women with respect and have better manners. It should also pay attention to the details and get the right company if it's going to make a dramatic spectacle of an event caused by its own mistakes.

The funny part is that DarkTrace had nothing to do with this. Further, all DarkTracer did was tweet about a mistake LockBit made. LockBit intended to make the post about DarkTracer but got the company and its CEO wrong.

In reality, neither company was breached by LockBit. Instead, LockBit made an ass out of itself and harassed an innocent bystander that had nothing to do with any of this.

The leader of LockBit frequently criticizes its employees and partners who make mistakes. I think it's fair to say, posting erroneous victims and data and then making a spectacle out

of it and threatening the wrong company that had nothing to do with this would warrant enough evidence to propose that maybe LockBit's leadership is the one with the issues. These are not small mistakes. Get it together over there!

The Tox 0-day

In May 2023, a 0-day exploit affecting qTox, a secure messaging platform, [was sold](#) for \$500,000 on a Russian hacking forum. As discussed earlier, LockBit relies on Tox to communicate with the rest of the world outside of the forums. So, as you can imagine, it was not happy about the news about the new vulnerability.

According to a tweet from VX-Underground, Tox users could be exploited simply by accepting a friend request. For LockBit, this meant it would have to stop accepting requests to connect and communicate over Tox. LockBit's approach was to only communicate with established contacts until it came up with a solution or found another means to communicate.

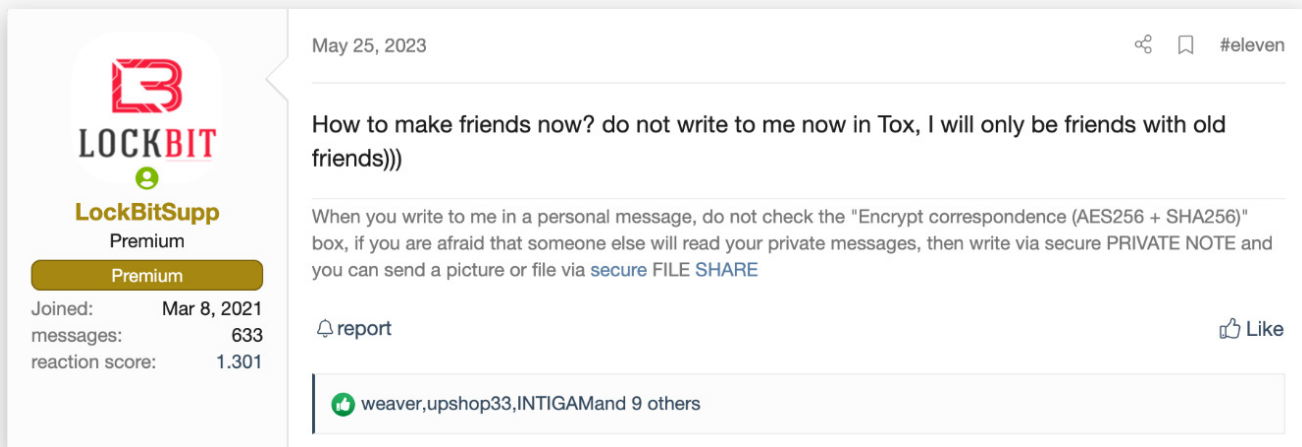


Figure 27: Lockbit's response to the Tox 0day

Lockbit wanted to identify the bug and patch it itself to re-establish the full use of Tox for his communications. You can see in Figure 28 that LockBit is interested in [software called "Reven,"](#) which is used to reverse engineer and identify vulnerabilities in binary applications. LockBit wanted to use Reven to identify the bug in Tox, then create a patch preventing anyone from exploiting it.

Hopefully, LockBit's comment about sending his "friends" to the software owner's house was just a joke. Regardless, the Tox 0day caused issues for LockBit, as communication is essential to running its ransomware operation.

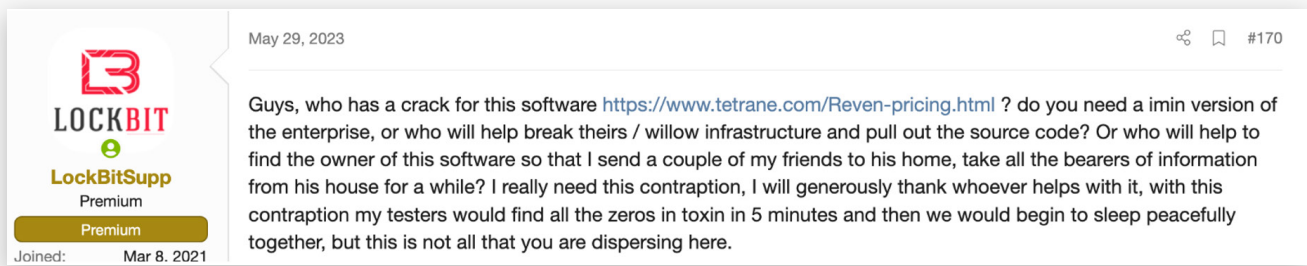


Figure 28: Lockbit posts about obtaining Reven software to find the vulnerability in Tox

This is an excellent example of why law enforcement and government intelligence agencies should continue to try to identify and assess the software that threat actors like LockBit use. They could exploit the operation and potentially infiltrate the gang's systems and accounts.

I know LockBit planned to address the Tox vulnerability, but I do not know if it was successful. Since LockBit is still heavily reliant in Tox and has not discussed the topic lately, I think it's probable that a solution was found.

PART III:
THE COPS'
STORY

The “Borris” Indictment

On May 16, 2023, the US Department of Justice (DoJ) released an indictment for Mikhail Pavlovich Matveev, a Russian national who operated with or [partnered with](#) several ransomware gangs, including the LockBit crime syndicate. Matveev [used the monikers](#) Wazawaka, m1x, Boriselcin, Uhodiransomwar, @fuck_maze, Orange, and my favorite “arestedbyFbi.”

While the indictment spotlighted Matveev’s activities, Brian Krebs first exposed Matveev’s identity and mapped out his online personas, email addresses, and criminal engagements in an [article published in January 2022](#).

Later, Matveev told me that Azim Khodjibaev, a fellow cyber security researcher, tracked him down almost two years before the Brian Krebs article, but had not released the information publicly.

Azim Khodjibaev, tracked him down almost two years before the article.

In addition to Azim, Matveev has spoken to several of us in the research community over the past few years. As I write this, I find it strange to refer to him as Matveev because I have always known him as Borris. I began communicating with him a few months before the indictment, when looking into hackers who previously worked with LockBit. Beyond Azim, security researchers, such as Dmitry Smilyanets from Recorded Future, have gained Matveev’s trust and established a working relationship with the notorious hacker.

In August 2022, Matveev [agreed to do an interview](#) with Dmitry where he shared details on how he participated in attacks against high-profile organizations, like Capcom and the Washington DC police department.

Matveev also discussed the tools and exploits he used and his relationships with various ransomware gangs. Apparently, Matveev had a negative experience with REvil, but liked working with the LockBit gang and thought highly of the gang’s leader. Matveev [stated](#) he “*communicated very well with the LockBit*” and “*He seemed like a normal guy.*”

Still, their relationship was short-lived and Matveev moved on to eventually start his own ransomware gang, Babuk, which fell apart due to internal conflict.

At the time, there was no way to verify all of Matveev’s claims. However, based on the information released in the US indictment, Matveev did more than participate in the attacks. In reality, Matveev was the figurehead who orchestrated the attacks and led ransom negotiations with the victims whom he extorted for hundreds of millions of dollars. He partnered with several gangs, like LockBit, and led the Babuk gang.

“Matveev and the other members of these three ransomware conspiracies attacked at least as many as 2,800 victims in the United States and around the world and made ransom demands to these victims of at least \$400 million. Actual ransom payments from these victims to these perpetrators amounted to over \$200 million.” – [US Department of Justice](#)

After the DoJ released the indictment, Matveev wanted to tell his side of the story and conducted another interview on my favorite podcast, [“Click Here” with Dina Temple-Raston and Sean Powers](#).

In the interview, Matveev continued to downplay his role in ransomware attacks, claimed he made far less than the \$200 million the DoJ alleged he stole, and asked Dina, “Where did they get those numbers from?” The answer was fairly simple: they added the ransom payments made to wallets that Matveev controlled, which amounted to the \$200 million figure.

To be fair, Ransomware gangs and affiliates share profits, so he did have to share this money with his partners. Matveev does not understand that since he is responsible for the attacks, he is also responsible for the money he extorted, regardless of who it was distributed or paid to afterwards.

However, I am sure the DoJ would be happy to adjust those figures if he wanted to share the names and details of his partners with whom he shared his ransom profits. Until then, he will take the heat for the full amount.

Matveev also [told Dina](#) that LockBit had “lost their way” and compared it to REvil, which is primarily considered the scum of the ransomware community due to their high-profile downfall and betrayal of their own partners.

Matveev stated he favors the former Conti gang’s ransomware program, which he claimed is “best product in that space, and they are still out there. We just don’t see them.” This surprised me when he made the statement because, to my knowledge, Matveev has not worked for Conti.

I last communicated with Matveev in early July 2023 and asked him how life has been since the indictment. He said that he is content with his current lifestyle. He has destroyed his passport and come to terms with the fact that he won’t be able to travel outside of Russia anytime soon. The indictment appears to have given him serious “street credibility” amongst his ransomware peers and unwanted attention.

I asked Matveev if he still conducts ransomware attacks, and he said he was taking a break. When I asked what he is doing with his time, if not ransomware, Matveev replied,

“I wanted to tell you that I have dived deeper into exploit development, specifically.”
I don't have all the details, but Matveev says his current project focuses on exploiting Microsoft SharePoint.

Unfortunately, this is a case where crime may have paid off. You see, despite making the FBI's most wanted list and having a \$10 million dollar reward for information leading to his arrest, Matveev is living freely in Kaliningrad, Russia, where the government protects him from prosecution.

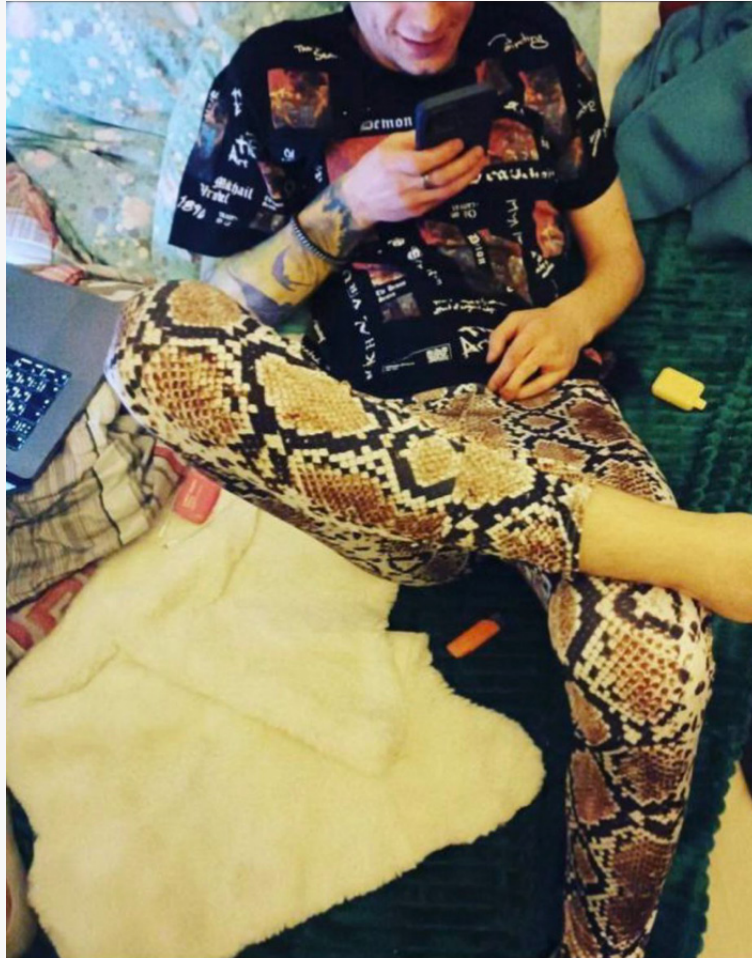


Figure 29: Matveev sharing a photo of himself wearing snakeskin pants a month after he was indicted by the US DoJ

Matveev better hope the protection he receives from the Russian government stands, or similar to REvil, someday he may get a knock at his front door.

You're Under Arrest for Being Stupid

The FBI's Newark, NJ, field office has been busy. Just one month after releasing the indictment against Matveev, the FBI arrested a LockBit affiliate. The [alleged hacker](#) is Ruslan Magomedovich Astamirov, a 20-year-old Russian national from Chechnya who was in the US and [arrested by the FBI](#).

According to the criminal complaint, Astamirov has been conducting ransom and extortion operations for the LockBit gang since August 2020. That means Astamirov began hacking for LockBit at the age of 17! Astamirov should have been at summer camp or playing sports in high school. Instead, he conspired with LockBit to conduct ransomware attacks and extort organizations worldwide. Now, he is facing 20 years in prison.

Lockbit should have an age restriction banning minors from running crimes for its operation because Astamirov was not ready for the very real trouble he has gotten himself into.

Astamirov was smart enough to hack and extort large companies, but based on the criminal complaint, he was way over his head. As much as it pains me to say it, most Ransomware hackers are intelligent people who have skewed ethics and make poor life choices, but Astamirov is not one of them.

Simply put, Astamirov made mistakes as many young people do. He comes from a part of the world where life is very different from the US. For those reasons, I see how he could think cybercrime was appealing, but I hope he turns his life around moving forward. He is young enough that he will have another chance someday. Hopefully, he takes it. Still, he made some really stupid mistakes in his short-lived criminal career, which I will discuss next.

Mistake #1

Astamirov registered accounts with several online gambling platforms, which he attempted to use to launder money he obtained from conducting LockBit ransomware operations. Based on the number of platforms Astamirov registered with, he may have also have a gambling problem. Ask yourself, what could go wrong with using dirty money earned from working with one of the most sought-after criminal gangs to feed your gambling addiction? Most of us would realize this is a recipe for disaster. You see, laundering millions of dollars is not easy when you have no experience cleaning money.

Mistake #2

Astamirov re-used email addresses for both personal and criminal operations. He used the email to register with a crypto exchange and then linked cryptocurrency wallets associated with ransomware payments to the account. The problem is, [he used the same email address](#) to register with social media platforms, like Meta, and online shopping platforms, like Amazon, and then created usernames that included his real name, “astamirov_222” and “astamirov_225”.

Mistake #3

Astamirov set up at least one of two email accounts associated with ransomware operations to sync to his personal-use iPhone and Apple computer. Making things worse, when confronted by the FBI, Astamirov tried to push the blame onto his brother, who likely had nothing to do with this. That’s low. Think about it, how many of you have your sibling’s email accounts synced to your personal devices? Did Astamirov think anyone would believe this?

Mistake #4

Astamirov also used the same email address to register the infrastructure he used in ransomware attacks. I wish all bad guys were this dumb. My job would be much easier. The smartest thing Astamirov did was decide to cooperate with the FBI. This kid had no business engaging in a life of crime. What a dumbass.

While Astamirov may not be a core gang member, and I have highlighted the stupid things he did, the arrest is still a big win for the US and the FBI. The lesson here is just because you know how to hack does not mean you know how to launder cryptocurrency. If you want to be a successful ransomware hacker, you need to be good at both. If either is lacking, you are going to get caught. Kids today...

Reflecting on the arrest

The funny part of this story is that only a few weeks prior to the arrest, LockBit told me criminal affiliates existed in the US. LockBit claimed dozens of affiliates conduct attacks right under our nose. You can see his comment to me in Figure 30 below.

Personally, I hope it is telling the truth. Unlike Russian-based criminals, the FBI can pursue, engage, and apprehend affiliates located on US soil. Over the past 12 months, there have been two arrests, one indictment, and a major takedown of ransomware infrastructure disrupting the [Hive operation](#).

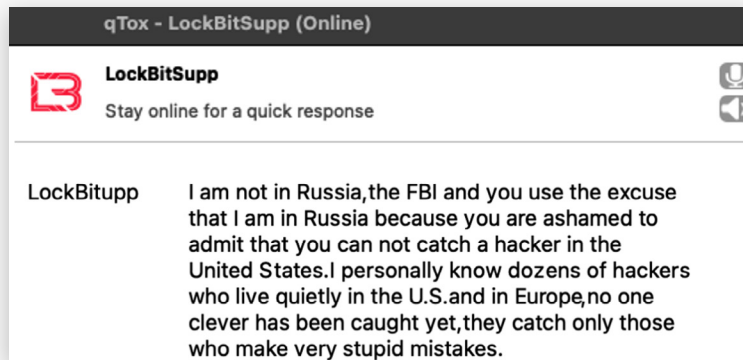


Figure 30: Lockbit claims dozens of affiliates operate within the US.

The problem with being a criminal involved with the most wanted ransomware gang worldwide is that everyone is watching and waiting for you to make a mistake. In addition to researchers, you have government intelligence agencies and law enforcement organizations with both technical and human assets dedicated to finding you. With that kind of heat, it only takes one mistake.

PART IV:
TELLING
SECRETS

LockBit's Secrets

In the first volume of the Ransomware Diaries, I discussed the developer behind LockBit Black and his fallout with the gang's leadership. After departing, the developer gave his side of the story, which I included in the report's appendix. In it, the developer made a comment that stuck with me as I wrote this volume of the Ransomware Diaries. The developer stated:

"At the moment, LockBit has no technical support for either the current 3.0 draft or the old 2.0." – LockBit Black ransomware developer

His claim is significant because, if true, LockBit was left to operate without an experienced ransomware developer. Now, few developers in the world have as much ransomware experience as Lockbit's former developer. After all, he developed DarkSide, BlackMatter, and LockBit Black ransomware, amongst other cybercrime-based malware. For this reason, I wondered how his departure would affect LockBit. I now have enough evidence to pose an answer, which is much more damaging than I initially thought.

**LockBit has
fooled both
victims,
affiliates, and
myself.**

I found problems in LockBit's operation, which are byproducts of the gang's dramatic growth over the past year and a lack of development resources. LockBit has tried to hide these problems and effectively controlled the narrative surrounding its operation. It has fooled both victims, affiliates, and myself.

This is what LockBit does not want you to know.

Secret #1: LockBit Sucks at Publishing Victim Data

LockBit has a significant issue with publishing victim data to its leak site, and the problem is bigger than anyone knew.

Between late February and the end of June 2023, LockBit claimed it released sensitive stolen data from victims who had not given in to its extortion demand. I have learned that most of these were empty threats. For many leak site posts during this timeframe, LockBit did not actually post victim data. It only said it did.

If you are a victim who paid LockBit to prevent it from leaking your data during this timeframe, I am sorry to tell you that you wasted your money. In most instances, LockBit

could not publish your stolen data to its leak site, even if you had not paid, which I will demonstrate to you shortly.

LockBit not only lied to victims, but it also lied to its affiliate partners who shared profit with the gang. For readers who don't know how this works, LockBit automates the process of stealing, hosting, and publishing victim data all through a graphical interface in its admin panel. (You can see screenshots of this panel in my [previous reporting](#)).

The service began to have issues around February 2023 and worsened over time.

Once the affiliate hacker identifies the type of data it wants to steal within the breached environment, they use the admin panel to collect and extract it to LockBit's servers. As far as I know, this part is working as expected. At this stage, the LockBit affiliate and the victim begin negotiations, which they also facilitate through LockBit's admin panel.

Using the panel, the affiliate controls the data it wishes to publish and leak onto LockBit's website. Most affiliates leak data slowly and use a countdown timer as a tactic to encourage the victim to pay. If the timer reaches zero and the victim has not paid the ransom, data is published and released publicly on LockBit's website.

This is how it is supposed to work, but the service began to have issues around February 2023 and worsened over time. As a result, LockBit has not consistently published victim data as it has claimed throughout 2023.

While victims and the media have not noticed, affiliates have. As a result, many affiliates are dissatisfied over their partnership with LockBit. This is LockBit's secret. However, you don't need to take my word for it, I'll show you.

Figure 31 shows three posts of victims who chose not to give in to LockBit's extortion demands. One of these organizations, marked as item 1 in Figure X, is Maximum Industries.

Earlier, I spoke about [this attack which media outlets covered](#) globally due to Maximum's relationship with SpaceX, owned by Elon Musk. That is why it is so ironic that the data has not been released despite the gang's dramatic threats and claims. Notice that in each post (1 - 3) LockBit announces, "ALL AVAILABLE DATA IS PUBLISHED." Yet, at the time of this writing, the data is still not present on LockBit's leak site.

FILES ARE PUBLISHED

Deadline: 30 Mar, 2023 15:46:25 UTC

1

[no photo]

maximumind.com
 I would say we were lucky if SPACE-X contractors were more talkative. But I think this material will find its buyer as soon as possible.

Elon Musk we will help you sell your drawings to other manufacturers - build the ship faster and fly away.

and now about the numbers:
 about 3,000 drawings certified by space-x engineers

We will launch the auction in a week.


ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 13 MAR, 2023 19:26 UTC UPDATED: 30 MAR, 2023 15:04 UTC

FILES ARE PUBLISHED

Deadline: 21 Feb, 2023 10:33:51 UTC

2



ckfinc.com
 At CKF Inc. we are taking current events very seriously. The safety of our customers, our vendors, and our employees is our top priority. We are doing everything we can to provide a safe environment during these difficult times.


ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 06 FEB, 2023 15:33 UTC UPDATED: 07 APR, 2023 18:37 UTC

FILES ARE PUBLISHED

Deadline: 21 Feb, 2023 05:36:33 UTC

3



adamjeeinsurance.com
 Adamjee Insurance Company Limited (AICL) is one of the largest general insurance company adamjee insurance auto insurance quotes and anonymous ballpark estimates to help protect you, your family and your automobile. Insurance and financial products include car insurance, home insurance, personal accident insurance, business insurance, life insurance, IRAs and annuities.

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 06 FEB, 2023 15:36 UTC UPDATED: 07 APR, 2023 18:37 UTC

Figure 31: Three (of many) victims between February and June of which LockBit falsely claims to have leaked their stolen data.

The images in Figure 31 make it clear to me that LockBit has not posted the data because I study victim posts daily. If you don't, it may not be clear what it should look like when data is published. Thus, take a look at Figure 32 below.

In the post, you will see the victim labeled 4, 5, and 6. Notice that each entry includes a download button, exposing the victim's sensitive data. Some have screenshots of stolen data allowing you to browse stolen files in the post itself. Most victim posts made earlier in the year, including examples 1-3, do not. Yet, no one notices because each post includes the message "FILES ARE PUBLISHED."

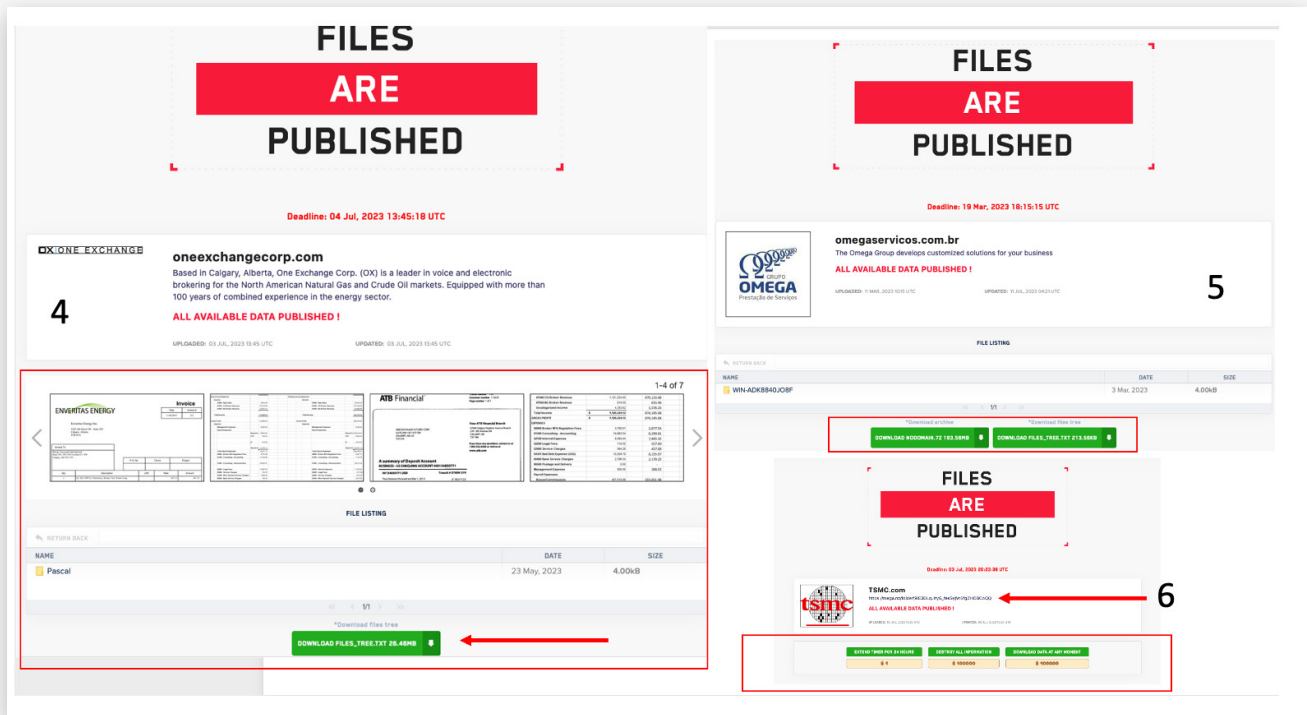


Figure 32: Victim posts on LockBit's leak site in which the data was leaked and available for download.

As stated, the worst part of this situation is that no one noticed. However, while the media and public may not have noticed, I knew that the affiliates it affected would. After all, they share millions of dollars with LockBit to provide these services as their partner. So, to confirm the problem was as bad as I thought, I contacted former and current LockBit affiliates to ask if they were happy with LockBit's operation and why.

Several of the affiliates I spoke with complained that they were unhappy with issues related to publishing stolen data onto LockBit's data leak site, which led them to leave for LockBit's competitors, as seen in the correspondence below.

Lockbit now has huge problems with stealer and the data does not come to the panel for months, so I switched to the merged version of

I have a suspicion that Lockbit has big problems with the panel and I have no desire to work with them

Figure 33: Former LockBit affiliate's explanation of why they LockBit's operation

In addition to my correspondence with affiliates, the former LockBit ransomware hacker Bassterlord commented in a now-deleted public tweet about the situation:

"I have nothing against LockBit, but until the data comes in normally (without delays of 2-4 months), I see no reason to give the affiliate program 20 percent" – [Bassterlord](#)

Affiliates were not the only ones to notice the problem. LockBit did, too.

LockBit knows it has a big problem, which it is trying to rectify. On April 24, 2023, LockBit posted a job ad for a "tester" to help with development updates.

The screenshot shows a job advertisement from LockBit. On the left, there is a profile for 'LockBitSupp Premium' with a 'Premium' badge. The profile information includes: 'Joined: Mar 8, 2021', 'Messages: 607', and 'Reaction score: 1,258'. The main content of the job ad is dated 'Apr 24, 2023' and includes the following text:

A tester is required - a specialist who takes part in testing a component or system. His duty is to search for possible errors and failures in the functioning of the object of testing (product, program). The tester simulates various situations that may arise during the use of the test item so that developers can correct the detected errors.

The necessary qualities of a tester are logical thinking, attentiveness, good memory, the ability to learn and adapt to existing tasks, quickly switch from one type of task to another. Equally important are patience, perseverance and the ability to work in a team.

In addition, the tester acts both as a user and as an expert, and therefore must have a certain mindset: be able to reproduce the behavior of the user of the product and analyze the behavior of the system, the input parameters and the results obtained from the point of view of an engineer.

Basic requirements for the applicant:

- higher education;
- basic skills of administration of operating systems;
- knowledge of English;
- ability to work with the bug tracking system and software versions;
- lack of other work;
- lack of personal life;
- lack of bad habits;
- the ability to keep secrets;
- online 24/7;
- greed;

Salary from 1000 dollars per month.

Write only to Tox

Figure 34: LockBit job ad for a "tester"

I can appreciate LockBit's sense of humor, as requirements for the job include "greed," "the ability to keep secrets," being "online 24/7" and having a "lack of personal life." From what I know of it, that sounds like the leader of LockBit's own job.

Despite the satire, LockBit wanted to hire someone to test and identify “errors” and program “failures” for his product and program. The “program” aspect would cover these testing issues, like the data upload failures I am discussing.

I assume it hired someone, because a few months later, in early July, it made improvements and upgraded its infrastructure. After the update, it posted the following message, which was the first time it addressed or admitted the issue existed.

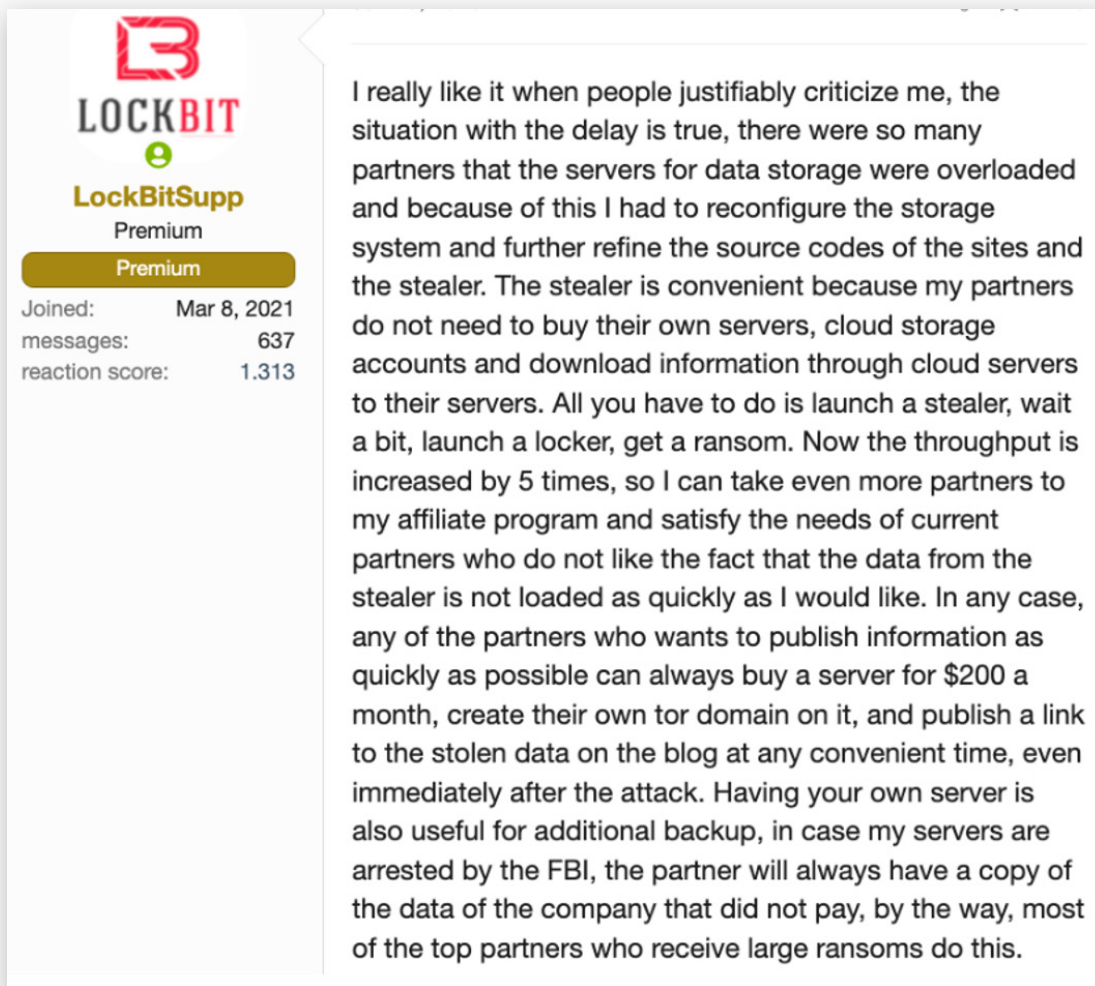


Figure 35: LockBit addresses data posting issue in a conversation on an underground forum

LockBit claims that it corrected the issue and that the problem resulted from the load on its storage servers due to the high volume of use by his affiliate partners. It claims the problem is corrected and that it has increased his throughput to handle five times the load it could facilitate previously.

Now, I can confirm that LockBit did, in fact, make changes and updates to its site. Yet, the update is a Band-Aid and not a long-term solution. It improved the situation but has not corrected it.

There are still many victim posts, like the companies I listed earlier, in which LockBit still claims the data is posted, but it is not. LockBit did improve the situation and more recent posts do include victim data than before the update. **However, many new posts still do not.**

Instead, LockBit made changes to make it appear that you can now download data, but it's nothing more than a gimmick to support its narrative that the problem is fixed.

You see, these links don't make the data directly available to download. Instead, they only allow you to download the file tree, which is a text file listing the directory names and structure of the victim's data, but not the data itself. You can see an example item A, in Figure 36.



Figure 36: File tree accessed by downloading victim data from LockBit's leak site.

In other instances, the posts claim the victim's time to pay has expired and the data is published, but instead of making the data available as it claims, it offers the options to pay to extend time, destroy or download the data, for a fee, as seen in item "B" of Figure 36.

The fee is far less than the ransom demand, so it is unclear to me what the point of this is, besides giving LockBit an excuse not to address the problem, which is preventing it from hosting and publishing the stolen data.

If you're a victim, this is good news. **Unless someone is willing to shell out \$100k, your data is not publicly exposed. Instead, it sits on a server that only LockBit and the affiliate who took it can access.**

Further evidence can be seen in several other posts after LockBit claimed to have corrected the data publishing issue. Item "7" in Figure 37 is one of many new examples where the data is available but not hosted on LockBit's infrastructure. Instead, it is hosted on [legitimate third-party file-sharing platforms](#), hosted on Clearnet.

This may sound trivial since the victim's data is exposed, but it is an issue for LockBit's partners, who pay through revenue sharing for the data to be hosted on LockBit's infrastructure.

Hosting stolen data is one of the benefits LockBit advertised to attract partner affiliates. Prior to this, it was common practice to use third-party file-sharing services. This is a drawback for criminals because law enforcement or the filesharing service provider itself can take down the files, removing access from both the general public and criminals alike.

Now, they have lost control of the data they worked to steal. Further, it damages their reputation making victims less likely to pay the ransom.

7



worldlearning.org


World Learning is international organization that focuses on international development, education, and exchange programs. Based in Brattleboro, Vermont, World Learning "unlocks the potential of people to address critical global issues" through its core program areas: The Experiment in International Living, the School for International Training (including the International Honors Program), and International Development and Exchange Programs.

ALL DATABASES PUBLISHED! CAN BE DOWNLOADED FROM:
<https://www.sendspace.com/file/hbl057> ←
or
https://anonfiles.com/3bl4Q900zb/worlddb_zip ←

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 07 JUL, 2023 22:47 UTC UPDATED: 07 JUL, 2023 22:47 UTC

8



affinityhealthservices.ne

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 12 JUL, 2023 19:31 UTC UPDATED: 12 JUL, 2023 19:31 UTC

Deadline: 12 Jul, 2023 22:31:21 UTC

Figure 37: Updated victim data leak posts

Additionally, despite LockBit's claim, I am still seeing new victims, like the post seen in Item "8" of Figure 37. Here, LockBit states data is posted, yet no link exists. This is the exact problem that I saw earlier that the update allegedly corrected. I guess LockBit really did not fix the issue, nor has he fixed its reputation, which will continue to degrade as more affiliates and victims realize LockBit will struggle to make due to its threat to post victim data.

So, if you are a victim of a new LockBit attack, you may want to roll the dice because it looks to me like LockBit is struggling to support its data hosting infrastructure and letting down its partners.

Secret #2: Extended Support Wait Times

Have you ever needed to address an issue, like your mobile phone service, or needed to speak to a representative about a problem with your itinerary at a major airline? Well, if you have, you likely know how frustrating it can be to wait on hold for long periods to get help with your problem. It may sound funny, but criminals who work with LockBit are facing this exact issue.

You see, LockBit, as I mentioned previously, uses the communication application Tox to converse with its partners. The application makes it difficult if not impossible, for outside organizations like the FBI and government intelligence agencies, to spy on LockBit's conversations.

Often, higher levels of security make applications less user-friendly because you must give up the ease of functionality to harden the application. This is certainly the case for Tox, which is not the most robust or feature-driven platform. Due to this, and the high volume of attacks and increased number of partners working with LockBit, it has a major problem responding to service requests.

There is a growing frustration amongst ransomware criminals due to how long it takes for LockBit to respond.

From an affiliate partner perspective, they work weeks to breach and extort a victim. Then, once they are in and have a foothold on the target network and their data, they run into a problem. It does not matter what the problem is. What matters is that they cannot get a response or resolution promptly, because LockBit is overloaded with message and service requests in its Tox queue.

Personally, I cannot imagine trying to manage hundreds of requests a day. Complaints such as ***"it's impossible to get through to you"*** have grown more common in the LockBit community. Regardless of why, there is a growing frustration amongst ransomware criminals due to how long it takes for LockBit to respond.

According to LockBit, too many people are messaging it daily, making it difficult to keep up with the requests it receives. The other issue is that there is no consistency in responses. LockBit responds to some requests quickly, while others go unread for over a week.

As a solution, LockBit mentioned creating a ticketing system. I like the effort, but it is unlikely it will be able to implement such a system unless LockBit develops something itself. Remember, LockBit can't use a legitimate vendor, and nothing exists to offer the security and confidentiality a criminal organization would need.

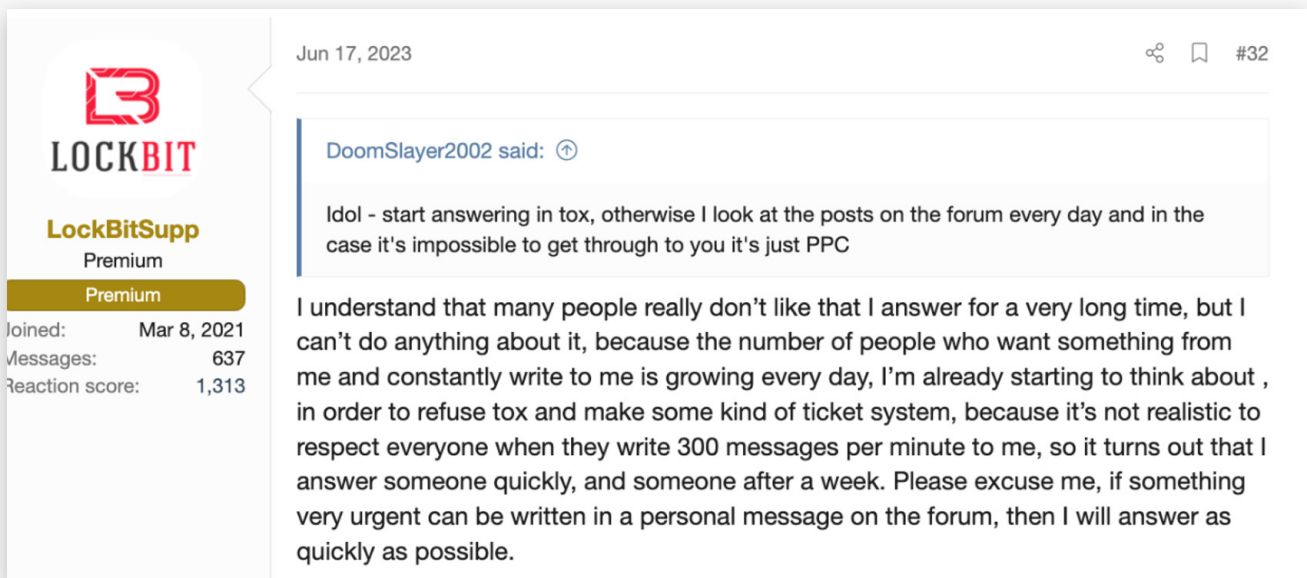


Figure 38: LockBit's response to complaints about the long response time

Since Tox is open source, it would not surprise me if LockBit attempts to implement a ticketing system developed using Tox source code, but that also takes a lot of time and resources to develop and test. If done incorrectly, it would lead to the same frustrations it faces today.

Secret #3: There Is No Ransomware Update

In June 2021, LockBit made its first significant update to its ransomware program, releasing LockBit Red, AKA LockBit 2.0.

In June 2022, LockBit released an even more significant update, named LockBit Black, AKA LockBit 3.0. The same developer behind DarkSide and BlackMatter developed the ransomware and included many new features and services that elevated LockBit to top of the Ransomware food chain.

So, when June 2023 came around, I waited for the next big thing. However, it didn't happen.

Honestly, I knew there would not be an update and have been waiting to write this since last September when LockBit's developer left. The closest update we had this year was LockBit Green, but the only thing it shared with previous LockBit updates was the name and color theme.

That update, as we discussed earlier in this report, was not LockBit's ransomware. Instead, it was ransomware leaked from Conti, a former competitor. I have had that ransomware

build sitting on an external hard drive since February 2022. It's hardly new. LockBit did make some changes to improve the build, but overall, this is lame and not what you expect from the world's most notorious ransomware gang. Do better, LockBit!

There are several reasons that this is bad for LockBit's partners. The most important reason, however, is that most security vendors can identify and prevent LockBit ransomware from executing on their systems.

Looking at recent detections of LockBit Black samples in July 2023, between 50 and 60 out of 71 security vendors can detect LockBit's ransomware, as shown in Figure 39.

	Detections	Size	First seen
<input type="checkbox"/> FE4B2A7C3CB8E0ED22FEB83EDB2CC8514B4F5D5E3DF9283348C02081453DE20C LB3.exe peexe calls-wmi checks-user-input detect-debug-environment self-delete	59 / 71	153.50 KB	2023-07-17 03:54:02
<input type="checkbox"/> CC138C4C961D31D8D8FF5B8C780A0D381B28E1DE7F4F13634617B4D678519058 Gen v2.exe peexe detect-debug-environment calls-wmi checks-user-input	60 / 71	146.00 KB	2023-07-17 00:26:49
<input type="checkbox"/> 8D0692B2B526088470C739767EA0B673D3A785E1DFA60CF3D4E96F8BEEC44124 {93764A20-1D0A-B3AC-3B5F-364004C1DE5D}.xml zip contains-pe	51 / 65	95.52 KB	2023-07-16 06:41:39
<input type="checkbox"/> 641052A26D49D5AFAB2BA53E9FB33BF8B31F917F546A3100A932DE456DD633CA ...93764A20-1D0A-B3AC-3B5F-364004C1DE5D...exe peexe detect-debug-environment calls-wmi self-delete checks-user-input	60 / 71	148.00 KB	2023-07-16 05:24:53
<input type="checkbox"/> 1E1A646B43EBA7B324AE7301A4640DEA1E711017B882FA6369C34B2D5934492D No meaningful names peexe idle calls-wmi detect-debug-environment	52 / 63	146.50 KB	2023-07-13 06:40:09
<input type="checkbox"/> 238D05DF779603163A11BBC75AD50B95F3FAC0A107F1187F43756BCC94F283C5 greenx86.exe peexe idle calls-wmi detect-debug-environment	61 / 71	147.00 KB	2023-07-12 22:45:53
<input type="checkbox"/> 25F9E2BB5312F3BA8D593529546402D91460720239805502C8CE29582C922036 C:\Users\user\Desktop\JtiTVmIh1Cd7.exe peexe calls-wmi detect-debug-environment self-delete	56 / 70	149.00 KB	2023-07-11 04:10:44

Figure 39: VT results for recently submitted LockBit ransomware samples.

This is why LockBit affiliates must find a way to shut down security services prior to executing the payload. Otherwise, it restricts their ability to encrypt systems, reducing the amount of ransom they can demand. Additionally, suppose the affiliate attempts to execute a payload in an environment that uses one of these security solutions. In that case, it will be identified and flagged, likely resulting in a response from defenders.

A year ago, far fewer vendors could detect LockBit Black because it was new and seen for the first time. Updates and feature development are expected when you share your profits with a ransomware provider.

LockBit claims it is working on something new, but I have seen no evidence to support this besides claims made on underground forums. Personally, I like to see results, not empty promises, but perhaps affiliates are content with using outdated ransomware due to LockBit's reputation with the general public.

Honestly, I don't know if an update is a week or a year away, but it's already missed the expected June release date, and all signs indicate that LockBit is having serious development issues. I won't hold my breath.

Secret #4: LockBit Must Rely on Leaked, Poorly Coded, or Stolen Ransomware

If you recall from earlier, Baddie from the Royal ransomware gang confronted LockBit after learning that LockBit had approached Royal affiliates and personnel trying to gain access to their builder. LockBit told Baddie it wanted to build a ransomware comparison table, which was obviously a lie. Lockbit was actually trying to steal ransomware builders from his competitors.

In December 2022, Lockbit began a collection and theft campaign against its competitors. LockBit is willing to buy their ransomware at what it feels is fair market price. If they don't sell, LockBit covertly tries to obtain access and steal it for himself. Let LockBit tell you in his own words:

“Both lockers (LockBit Black and LockBit Green/Conti) present at the moment in the panel, each advert decides which locker it wants to encrypt, fast and small, or a little slower, coders team, I'm not greedy. I take this opportunity to say hello to Revil and Alpha, ready to buy their code too, I want to collect all the top lockers in one panel, plus we are in the process of developing something interesting.” – LockBit

In February 2023, criminals began to discuss a rumor that LockBit had been poking around trying to get access to various competitor ransomware builders. Lockbit was quick to respond (see figure 40).

LockBit wishes to obtain many ransomware variants. It intends to make them available to affiliates directly from the LockBit admin panel. This will provide additional options for its affiliates to leverage during attacks.

By creating a “one-stop-shop,” affiliates can decide what ransom payload they wish to use. We as the security community need to be prepared for this, because it will change how we defend and mitigate ransomware threats.

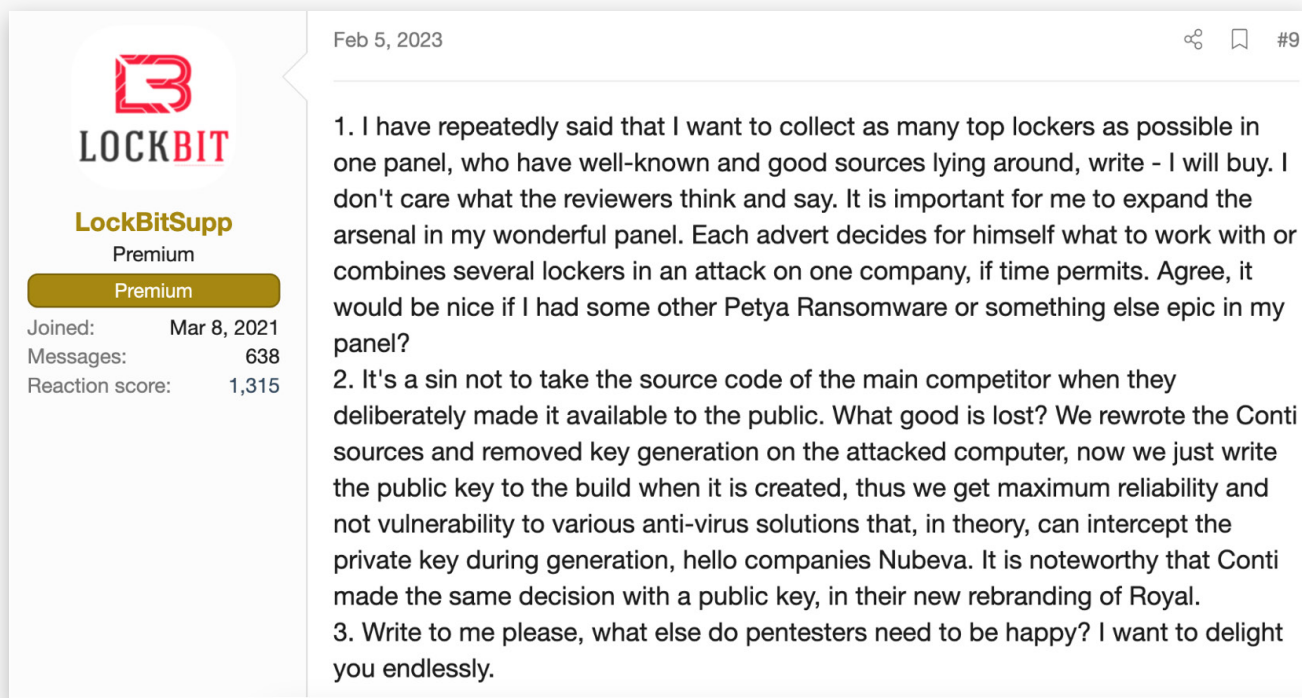


Figure 40: LockBit responding to comments about using/taking his competitor's ransomware

Getting ahead of this will make a big difference in minimizing the impact. First, you must understand precisely how LockBit's new RaaS model will benefit the attacker and further harm the victims. Let me explain.

Consider the situation I discussed earlier where an affiliate tries to deploy LockBit Black ransomware, but defenses within the environment block it. The affiliate would often be out of luck since now they cannot encrypt target systems and data.

Alternatively, in this same situation, well-connected affiliates with access to multiple RaaS programs could simply deploy ransomware from one of LockBit's competitors and extort the victim. Now, LockBit gets none of the profit. Instead, his competitors, like Alphv and Royal, get richer. However, under LockBit's one-stop-shop model, if a ransomware payload is blocked, they have several other options just a few clicks away.

Worse, in this situation, we did our job and detected the payload, but another was deployed moments later because of the ease of use in LockBit's admin panel. The attacker simply selects another option in the graphical interface of the panel and clicks a single button to deploy additional payloads.

Consider a situation where the affiliate intentionally uses multiple, different ransomware payloads within one target environment.

Second, consider a situation like the one LockBit proposed, where the affiliate intentionally uses multiple, different ransomware payloads within one target environment. For example, they deploy LockBit Black, Royal, and Conti ransom payloads. Now, three keys are required to decrypt the data, and the attacker can demand three ransom payments.

An even worse case, do you remember the [Kaseya MSP incident](#) in which over 1,500 downstream companies became infected with ransomware? The FBI obtained the decryption key, and many companies decrypted their data without paying millions in ransom payments. In LockBit's multi-payload model, that would not be possible. If Lockbit can pull this off, it could be disastrous.

Fortunately, this is not only bad for us, but it's bad for all of LockBit's competitors, who had to spend time and money developing their ransomware payloads. You would think they would be more aggressive at deterring it from doing this. Maybe they don't believe it can gain access to their ransomware. If so, they should read Volume 1 of this publication and see what happened to BlackMatter.

Closing Time

The quality of LockBit's operation is degrading. It has been slow to expand its infrastructure and development needs. LockBit has fallen behind in its ransomware and infostealer development schedule. As a result, there is a significant delay in producing new ransomware variants, and LockBit is struggling to publish victim data, causing affiliates to leave and partner with other ransomware gangs.

LockBit has everyone fooled to the point that the gang does not have to leak data because victims blindly pay. No other ransomware gang has obtained a reputation that allows such behavior. If you are a victim and the LockBit ransomware gang is extorting your company, threatening to expose your sensitive data, think hard before you pay.

Below is a list of contributing events that have led to the state of LockBit's program:

- No developer for an extended time
- Data exfiltration and posting issues
- Missed June ransomware development deadline
- Arrests/indictment
- Affiliate loss

- Poorly coded Mac release/leak
- Poor service response time (Tox)
- Need for a ticketing system
- The wacky posts on the leak site with random letters and fictitious companies

LockBit is trying to obtain ransomware from its direct criminal competitors. So far, it has only obtained a leaked version of Conti ransomware. The attempt to gain access to the Royal Ransomware gang's builder and LockBit's own admission claiming it wants to acquire and make it part of its service offering, tells us the direction the gang is moving.

Still, in time, we will see something new from LockBit. The question is, how much damage will it incur in the meantime?

This is a surprising turn of events, since LockBit prides itself in providing its partners with the highest level of customer service and support. It constantly tries to add features and asks its partners what they want to see next in its operation and service offerings. Sometimes, things don't go as planned, and one problem directly causes another, creating a domino effect.

If left unresolved, I believe these issues will lead to the downfall of the infamous LockBit ransomware gang. Still, I know LockBit is resilient, and it will do anything it can not to let that happen. The question is: will it be able to fix this, and if so, how long will it take? Until now, no one knew the truth about the state of LockBit's business.

Today, that changes.

Epilogue

From the beginning, I made it clear to the leader of LockBit that I was conducting an active investigation against the ransomware crime syndicate. So, once I completed my draft of this report, I decided to ask the leader of for an interview to address my findings and give LockBit a chance to present their side of the story.

LockBit agreed, and I sent over my interview questions. The gang's leader never answered after reading my questions. Yet, something I could never predict was about to happen, and I was about to make things much worse.

You see, at the same time this final conversation took place, I jokingly made a post addressed to LockBit on social media:

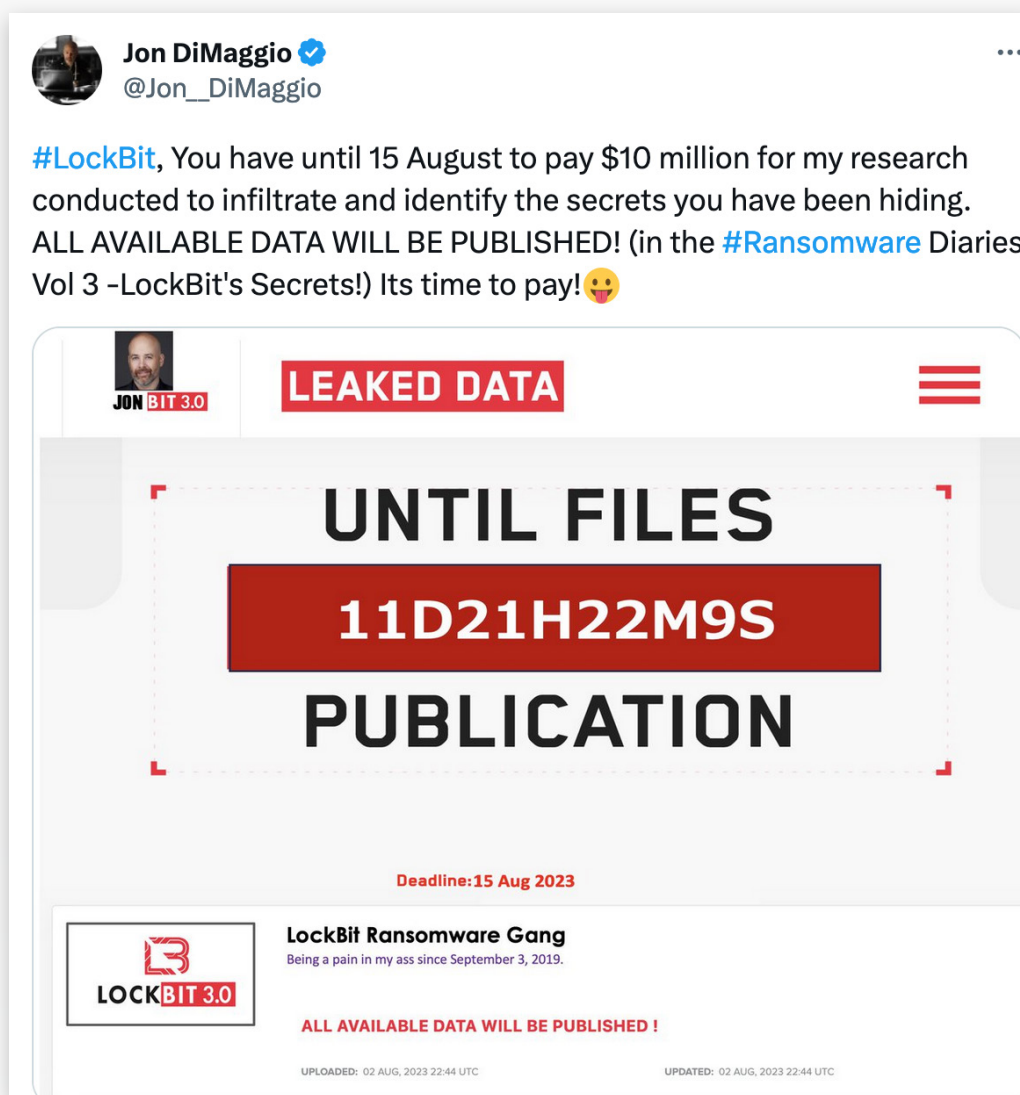


Figure 41: JonBit ransomware gang extorting the LockBit crime syndicate.

I had taken a screenshot of LockBit's leak site and altered it to show "JonBit 3.0" instead of "LockBit 3.0" and added a victim entry for LockBit itself.

Remember, I had grown a relationship and had talked with the gang over the past few months and felt comfortable they would know this was a joke. **To clarify, I am not an extortionist!**

For this reason, I was shocked that the day after my post, the LockBit gang went dormant on its Tox account. This was something that rarely, if ever, happened, and certainly not for an extended time.

Over the next few days, four separate affiliate crews contacted me! This was another clue that something big was happening. Each affiliate wanted to know if I had compromised and hacked LockBit. One directly asked me, "**You actually found a way to de-anonymize everyone from lockbit????**" I told them all I had not hacked anyone. After the fourth affiliate contacted me, I realized more was happening than I initially thought.

It was at this point I realized that I was not the only one who could not reach LockBit – its affiliate partners could not either. That is why they were reaching out. They saw my extortion message, then saw LockBit disappear and thought I was responsible!

It isn't easy to assess the magnitude of these events. In the best-case scenario, something behind the scenes spooked the gang, causing them to step away from its operation. In the worst-case scenario for LockBit, someone has hacked their infrastructure. Regardless, I am telling you that the LockBit gang is in trouble.

The same day I made the extortion tweet seen in Figure 41, another clue presented itself. I received a DM on Twitter from someone I don't know, who may be associated with a cyber security company. In the message, they included the image seen in Figure 42, displaying the login page and Tor address of the LockBit admin panel. On the page, you are presented with a prompt to input your credentials to authenticate and gain access. The person had taken a screenshot and written the message, "But do we really have to, though?"

See below:

The day after my post, the LockBit gang went dormant on its Tox account.

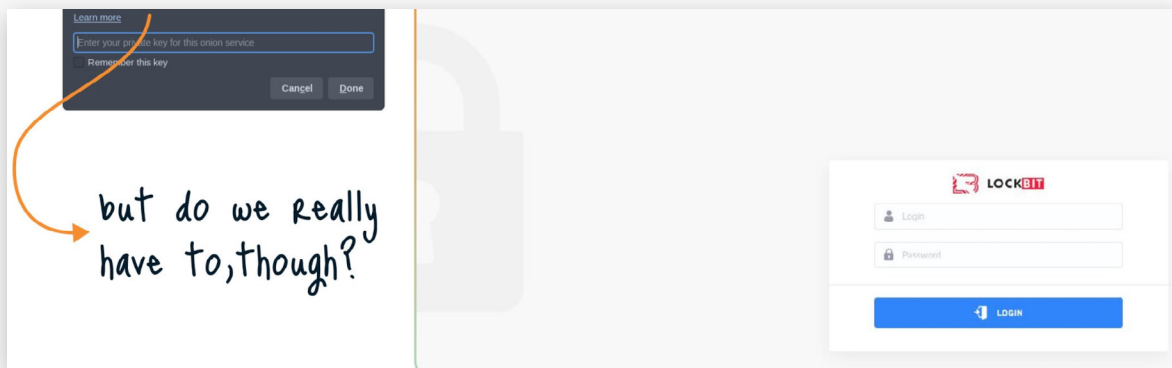


Figure 42: DM I received with a message insinuating LockBit's panel authentication could be bypassed

I don't know if the cyber security company wants this information made public or associated with them, so I am not including their name. However, the post suggested they may have found a way to bypass the login page and gain access to the LockBit admin panel without proper authentication.

Things were beginning to add up. Someone may have hacked LockBit at the same time I did my HUMINT operation against the gang. As a result, now, its partners thought I had hacked and breached the gang and its infrastructure because of my posts! They believed I was about to release their secrets, which, to be fair, was exactly what I had stated.

To clear things up for everyone, **I am an ethical researcher.** I do not hack or dox anyone, let alone the most notorious ransomware gang in the world. Still, **I am not the only one concerned. LockBit is, too.**

I started this story by explaining that LockBit reappeared shortly before I published my research. I believe LockBit's panel and possibly its backend infrastructure may be compromised.

This would explain why LockBit went dark for nearly two weeks, which it has never done before.

When the gang initially disappeared, and I learned of the possible breach, I thought LockBit was on the run. As it turns out, **LockBit does not die easily.** Instead, during this time, LockBit was doing damage control and trying to clean up its infrastructure to restore the integrity of its operation. I cannot state this as fact, but this is my analytical conclusion based on the events and information discovered throughout this research.

Still, the events show that no one, including LockBit, is beyond reach. In conjunction with the problems it has tried to hide from the public and its partners, the gang's hiatus tells me one thing: **LockBit's operation is in trouble.**

ABOUT AUTHOR:

Jon DiMaggio, Chief Security Strategist

Jon DiMaggio is a Senior Threat Intelligence Analyst and has over 14 years of experience. He possesses advanced expertise in identifying, tracking, and analyzing Advanced Persistent Threats (APTs). Additionally, Jon speaks at national level conferences such as RSA and BlackHat. He conducts interviews based on his research with media organizations such as Fox, CNN, Bloomberg, Reuters, Wired magazine, and several others.

ABOUT US:

Analyst1, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With **Analyst1**, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

 @UseAnalyst1

 analyst1.com/blog

Any technical information that is made available by Analyst1 is the copyrighted work of Analyst1 and is owned by Analyst1.

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice.