TAR X

Lockbit

OP. Chronos Report

MAY 2024

XG3 UNIT

xMDR powered by Cipher

LockBit 3.0

Last Seen 15/05/2024

Type Ransomware

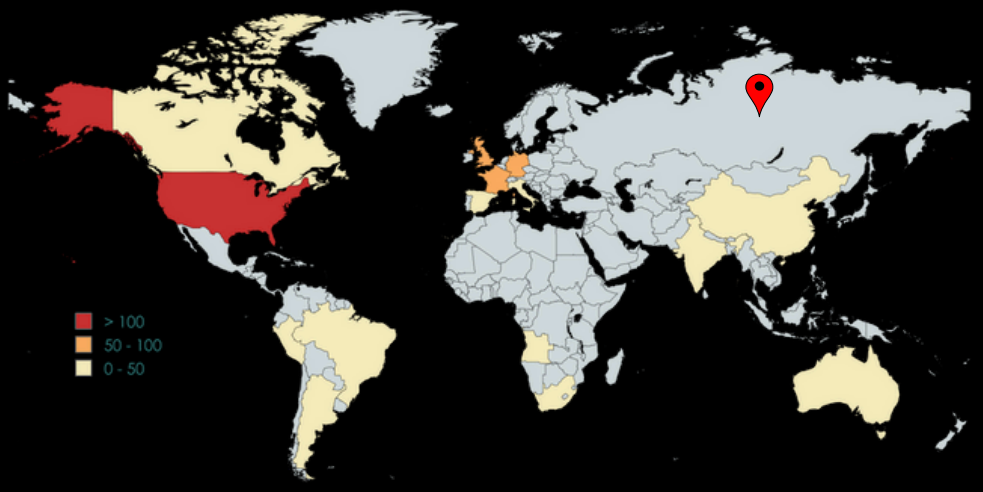
Risk **Very High**

Sectors All sectors can be afected

Sofistication High

Motivation Financial gain

Last Update 14/05/2024



Origin

Cipher xMDR Platform

- TTP: +50
- Rules: +60

MITRE Arsenal Used by Actor: 95%

LockBit is a ransomware family developed by the group known as Bitwise Spider and its first attacks were carried out in September 2019. Its most important targets include organizations in the United States, China, India, Indonesia and Ukraine, in addition to several European countries such as France or Germany. It is one of the leading ransomware groups on the global scene and operates through an affiliate system. The group behind LockBit offers its affiliates a tool known as StealBit to exfiltrate information from compromised companies before launching the ransomware attack. companies before launching the ransomware attack. Through their blog on the TOR network they show their victims and also recruit their affiliates, although they warn that they only cooperate with experienced pentesters who know how to professionally handle tools such as Metasploit Framework and Cobalt Strike.

Background

Lockbit emerged in 2019, and although not many people remember it, it called itself "ABCD Ransomware". It was set up as RaaS, "ransomware as a service", which means that it is a central team that develops its malware and gives permissions to people who are part of its affiliate team to launch attacks with this malware and share the profits.

In the particular case of Lockbit, it has had specific features to enter its affiliate system, including, for example, the payment of 1 BTC as a deposit. It has also proved to be an innovative group in terms of how affiliate models work, as in this case, the operators themselves charge their victims directly and then pay a proportional share to the group, which increases the trust of their workers. Also, the profit rate is higher than in other affiliate programmes, as the % that the group keeps as profit is slightly lower. Their extortion methods evolved to incorporate the threat of a distributed denial of service (DDoS) attack as an additional layer of pressure.

In addition, it has always positioned itself as one of the groups that invests the most in technical innovations to continue improving its line of business. In this case, the leader of the gang, better known as LockbitSupp or PutinCrab, has proven to be a very entrepreneurial and talented businessman. Updates to the malware have been constant, with updates being released periodically, more or less on an annual basis, and constantly improving.

In addition, since the launch of version 3.0, the number of members has multiplied and the group has grown considerably and become even more effective.

Currently, it was, and still is, one of the most active groups with the most ransomware attacks behind it, with victims all over the world, but with a special predilection for targeting the US.

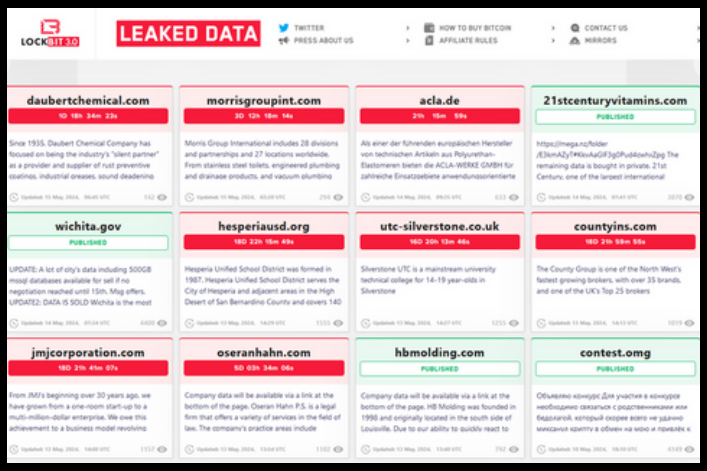
"It is the most notorious ransomware group, because of its sheer volume of attacks. And the reason for their success is that the leader is a good businessman," says Jon DiMaggio, chief security strategist at Analyst1, who has studied LockBit's operations in depth. "It's not that he has great leadership skills, but they created malware that anyone could use, where you just point to a target and click. They update their software, constantly look at user feedback and care about the user experience. They also poach people from rival gangs. In itself, it runs it like a business and, as such, it is extremely attractive to criminals".

OP. CRONOS

By becoming one of the most sought-after groups of cybercriminals, Lockbit put a target on his back, so it was logical that sooner or later intelligence agencies would try to catch him. Actions they have taken in the past, such as the papper writing contest, with prizes for the winners, or the $1,000 reward for getting a tattoo of the gang's logo, added to that wake-up call. In addition, major operations such as REvil and CONTI had been carried out previously. The result was expected by some.

The NCA, in collaboration with the FBI, Interpol, and other agencies from different countries, began what became known as Operation Cronos at the beginning of the year. On 20 February 2024, the NCA took control of Lockbit's blog, where he advertised his victims, to publicise a series of announcements promulgating actions that had been taken against the group.

In this operation they seized the servers' infrastructure, froze cryptocurrency wallets where they collect their payments, launched tools to decrypt victims, imposed international sanctions and arrested two members.
In private chats and a post on a hacking forum, "LockbitSupp", the site's main administrator, explained that law enforcement exploited a critical vulnerability to hack into its servers.



Lockbit "wall of shame" blog

However, they still left a clue in this part of the operation that would be resolved later. The unknown about the identity of the user LockbitSupp. One of the posts that hosted the domain taken over by the NCA talked about this issue, giving clues about his possible identity, such as that he drove a Mercedes or that he did not live in the US as the user had said, but they did not reveal much more details about the possible real identity. It was therefore suggested that the operation was not yet complete.

Blog sized by law enforcement

OP. CRONOS II

Seven days after the operation, messages and information about the leaks were posted on a new LockBit page. The site lists pre- and post-removal victims, suggesting that LockBit may not have lost access to its entire dataset or infrastructure.

A few days later, the administrator himself posted a whole message stating how the infrastructure had been accessed, arguing that they had become too lazy in applying protections and the NCA and FBI took advantage of this, and also appealed that the people they had arrested were innocent people who had nothing to do with the gang. They claimed that they were going to become active again and that nothing could stop the group, because their main goal was no longer solely for financial gain, but was focused on carrying out a million attacks, and that they would not withdraw from the gang.

In fact, just a few days later, the gang seemed to be back to its usual routine of operations. Websites were up again and new attacks began to be published, although they were also mixed with companies that had been attacked prior to the operation.

In fact, it quickly became clear that they had not only returned to their usual activity, but that it had increased, and that they had adopted more aggressive positions in negotiations and had somehow grown in the face of adversity.

After a few months of continuing with the usual march, a new domain suddenly appeared that had been retaken by the forces of law and order. And on it appeared a promising advertisement: The coveted identity of the user LockbitSupp. This time, it was revealed that the real person behind this user was 31-year-old Dmitry Yuryevich Khoroshev. He was identified as the mastermind of the ransomware group, one of the most active and dangerous in the world.

This has been followed by measures such as asset freezes and travel bans issued by various foreign affairs offices. Therefore, he becomes one of the most wanted people on the planet.

In view of this fact, a multitude of threads from different researchers emerged on RRSS, using OSINT techniques, trying to verify if this was really the much coveted identity of Lockbitsupp. Users managed to obtain all kinds of data, from emails and cell phones to the area where he lived.

OP. CRONOS II

However, LockbitSupp, the leader, spoke out again, denying that this was his real identity, that the NCA had got the wrong person and showed real concern for Dmitry, even offering a reward if anyone could provide information on his whereabouts because he feared he was in grave danger.

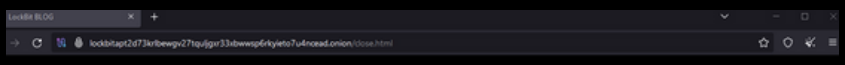
Serious doubts have arisen in the intelligence analyst community about the identity of LockbitSupp, as no definitive evidence has yet been thrown on the table.

In addition, among other data released by the NCA was a list of users who were part of the gang's affiliate group, which, while only pseudonyms, showed an increase of almost 50 people over February. Therefore, the gang had grown after the first incident.

In addition, the group's response was violent and in those post-operation days posted more daily attacks than ever before, posting more than 60 in a single day, although not all were actual attacks, there was a bit of a fog in that mind game.

Currently, the NCA has taken control of some of the group's websites and their logo is displayed with a shutdown message if access is attempted.

At the moment we don't know if this will be the final one, if there will be more parts of the cronos operation, or what will be the real end, but the group, as of today, is still operating.



NCA
National Crime Agency

Blog closed by law enforcement

LockBit Ransomware

Total Victims

1800

Some data

Top Countries

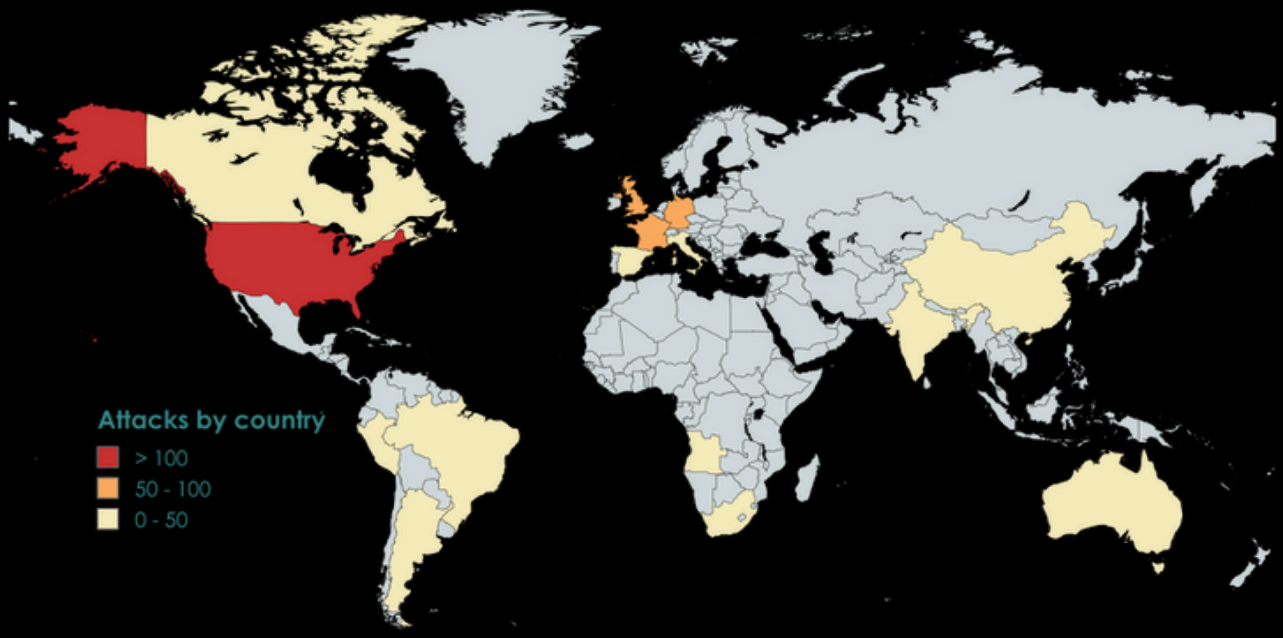
- USA - **562**
- FRA - **91**
- GBR - **86**

Top Sectors

- Manufacturing - **37%**
- Construction - **33%**
- Retail - **30%**

Top Victims

- UK Royal Mail
- Taiwan Semiconductor Manufacturing
- Boeing



Recent Victims

- **Ransom Victim:** morrisgroupint.com || Group: lockbit3 || Country: USA
- **Ransom Victim:** acla.de || Group: lockbit3 || Country: Germany
- **Ransom Victim:** hesperiausd.org || Group: lockbit3 || Country: USA
- **Ransom Victim:** utc-silverstone.co.uk || Group: lockbit3 || Country: UK
- **Ransom Victim:** countyins.com || Group: lockbit3 || Country: UK
- **Ransom Victim:** jmjcorporation.com || Group: lockbit3 || Country: USA
- **Ransom Victim:** oseranhahn.com || Group: lockbit3 || Country: USA
- **Ransom Victim:** 21stcenturyvitamins.com || Group: lockbit3 || Country: USA
- **Ransom Victim:** colonialsd.org|| Group: lockbit3 || Country: USA

Conclusion

Key Points:

- **Did the operation really work?** To this day the group is still operating and it seems that all the actions taken by FBI, NCA and other participants, have not had the effect of dismantling the gang that we all expected.
- **Does LockbitSupp's identity really correspond to the one disclosed by the NCA?** No concrete evidence has yet been shown that Dmitry Koroshev is the administrator and creator of the famous group.

Upcoming:

- **Is there really a chance that the group can be definitively dismantled?** The target currently being sought is to stop the operation and interrupt the execution of new attacks, however, for the moment, it seems that the Cronos operation has been more aimed at creating chaos and uncertainty than at dismantling the gang completely.

Overall:

Lockbit continues to position itself as the number 1 RaaS band top currently, despite the hard blow suffered with the Cronos operation, therefore, we have to keep improving and researching to find the right keys to finish the band's business.

Threat actor data available in xMDR Platform

TTP's 54

Top 3 Most Relevant

- Exploit Public-Facing Application
- Remote Services: Remote Desktop Protocol
- Data Encrypted for Impact

Tools Used 40

Top 3 Most Used By Actor

- LockBit Ransomware
- PsExec
- FileZilla

CVE's 40

Top 3 Most Used By Actor

- CVE-2021-22986
- CVE-2023-0669
- CVE-2023-27350

xMDR

ADVERSARIALLY

Threat Actor Report

APR 2024

cipher

a Prosegur company