The Record.
BY RECORDED FUTURE

An interview with LockBit: The risk of being hacked ourselves is always present

Editor's Note: Even though the LockBit ransomware group has been operating since September 2019, up until June this year, they have been a marginal player on the ransomware landscape.

But following the deployment of a new version of their Ransomware-as-a-Service platform, called LockBit 2.0, and the sudden retirement of rival operations Darkside, Avaddon, and REvil, LockBit has become one of today's largest RaaS platforms.

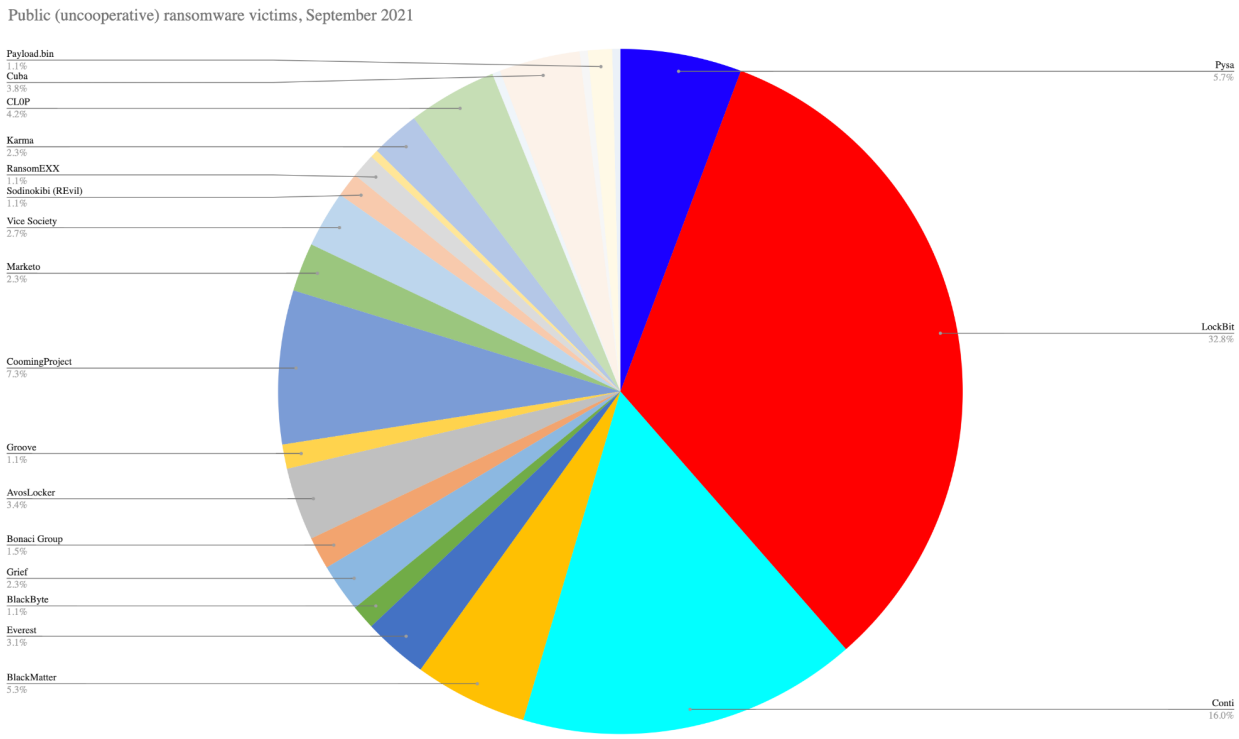
Cybercriminal groups who previously rented ransomware payloads from other gangs seems to have flocked to the LockBit group over the summer, leading to a surge in attacks that caused Australian officials to issue a rare warning to local companies. Furthermore, stats collected by Recorded Future have shown that LockBit was, by a large margin, the most active ransomware group last month, in September, amounting for almost a third of all victims listed on ransomware leak sites.

Following similar interviews with the administrators of the REvil and BlackMatter operations, the LockBit group has also agreed to talk to Recorded Future analyst and The Record writer Dmitry Smilyanets. The interview, translated from Russian by one of Recorded Future's linguists, is available below.

Dmitry Smilyanets: LockBit accounted for 34% of ransomware attacks that were reported in September. Tell us the secret of how you were able to conquer the market? Or are these numbers high just because most of your victims choose not to pay the ransom?

LockBitSupp: We haven't started to conquer the market yet. Now we are at the stage of developing and improving the software. The secret is very simple – an impeccable reputation – we are the only ones who have never scammed anyone or changed our brand. People trust us. Accordingly, the more affiliates, the more attacks. The LockBit Blog is just a small fraction of the companies that refused

to pay the ransom. In the past 3 months, we have attacked over 700 companies. "*My Phantom jet, with a white arrow on its wing, is gaining height.*"



PIE CHART SHOWING THE NUMBER OF HACKED COMPANIES LISTED ON RANSOMWARE LEAK SITES, IMAGE SOURCE: THE RECORD

DS: Several countries are now discussing mandating that ransomware attacks be disclosed within days after they took place. With better stats on such attacks, your group is bound to stand out as one of the top threats today. Have you considered limiting your Ransomware as a Service (RaaS) program to avoid making too much noise with your attacks?

LB: Restrictions are created for people who want to live on a salary. We are not planning to introduce any restrictions. We only live once. Noise or not, any mistake in anonymity will destroy you. We do not care if the company discloses information about the attack, this is a purely private business of the company.

IMAGE: THE RECORD

DS: What sets you apart from other groups is StealBit, tell me more about that malware.

LB: It is not enough to just encrypt the company, sometimes it is much more important to steal valuable information, for non-disclosure of which, the company is ready to pay more than for decryption. StealBit allows you to steal information as quickly and as simply as possible.

DS: You allow your affiliates to speak with their victims and accept payments directly. Has this model proven to be successful?

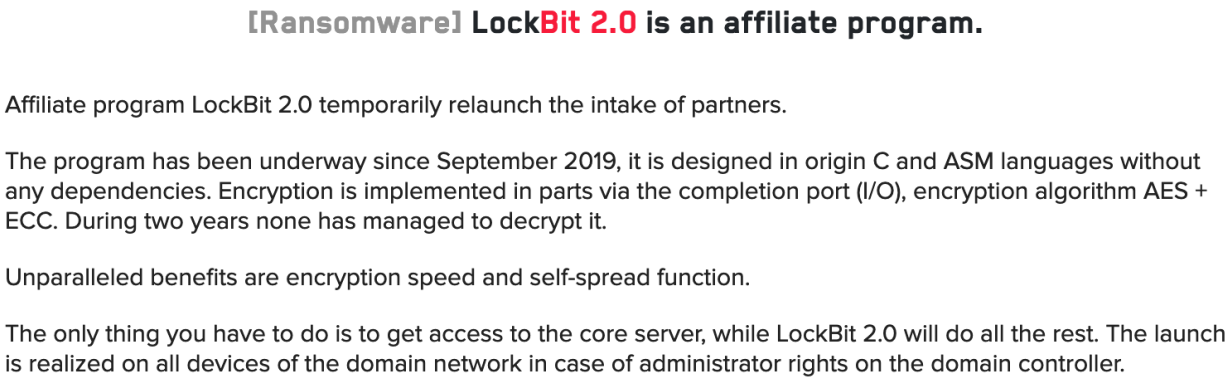
LB: There is no reason not to trust the affiliates. If a person is inclined to long-term cooperation, then they will never leave us. But the most important thing is maintaining an impeccable reputation, we cannot deceive our advertisers and steal their ransom, as Avvadon, Darkside, and REvil did.

DS: Do you believe the RaaS business model will sustain itself? How do you think it will change in the next 5 years?

LB: Competition will increase, the defense level of companies will rise, the wealth of our affiliates will increase too.

DS: Has the REvil disband over the summer played a role in your success? How many affiliates have joined your operation since Unknown disappeared?

LB: “Disband” of REvil does not affect our success in any way, 4 adverts came to us from them. It’s easy to start an affiliate program, but to keep it open is a form of art.



[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

IMAGE: THE RECORD

DS: Do you know what really happened to Unknown?

LB: Nobody really knows, but I’m sure this is a classic exit scam, the same thing happened with Avvadon and Darkside. As soon as a large payment comes, the owner of this partnership program thinks about whether it is worth working further and risking his life, or is it better to exit right now and calmly spend the money for the rest of his life. In our case, such a case is impossible, since we fundamentally do not touch the money of our affiliates.

DS: You are very active on forums. Why did Exploit ban your account?

LB: For my signature. It is not very clear how cybercriminals can prohibit certain types of cybercrime, because, in fact, everyone on this forum is breaking the law. It turns out that conducting a pentest with post-payment for rich companies is prohibited, but stealing money from the bank cards of millions of individuals is allowed. It is also not very clear why the accounts of our competitors are not blocked who continue to buy and sell network accesses and look for pentesters on the forum Exploit. Perhaps this is some kind of selective policy – I admit that this may be the work of competitors and their dishonorable ways of dealing with the number one affiliate program in the world. “*All this looks like some kind of bullshit, drugs are not allowed, but vodka is allowed*”. It’s a shame, annoying, but okay.

DS: You mentioned that REvil and Hive are locking hospitals, do you?

LB: We do not attack hospitals, there were several cases when affiliates encrypted dental offices and nursing homes by mistake. We issued decryption keys free of charge.

DS: After the US and Russian presidents met in June everyone is looking for signs of change. And I see some change – the attacks have increased after a temporary slowdown in summer. Are these events related or did the affiliates just go for a long vacation?

LB: It's just a summer vacation. Like all people on the planet, no one wants to work in the summer, and even more so when you have millions of dollars. The meetings of the presidents will not affect anything, everyone who works seriously does not live in the United States or Russia. Personally, I live in China and feel completely safe.

DS: Some ransomware families prevent affiliates from attacking American companies and infrastructure. Do you have any special recommendations for your partners? What happens if your adverts deploy LockBit into critical infrastructure against your will?

LB: This has not happened yet. Not a single affiliate will go against our will, because we work only with trusted people who have a code of honor, each of our affiliates is responsible for their words and actions.

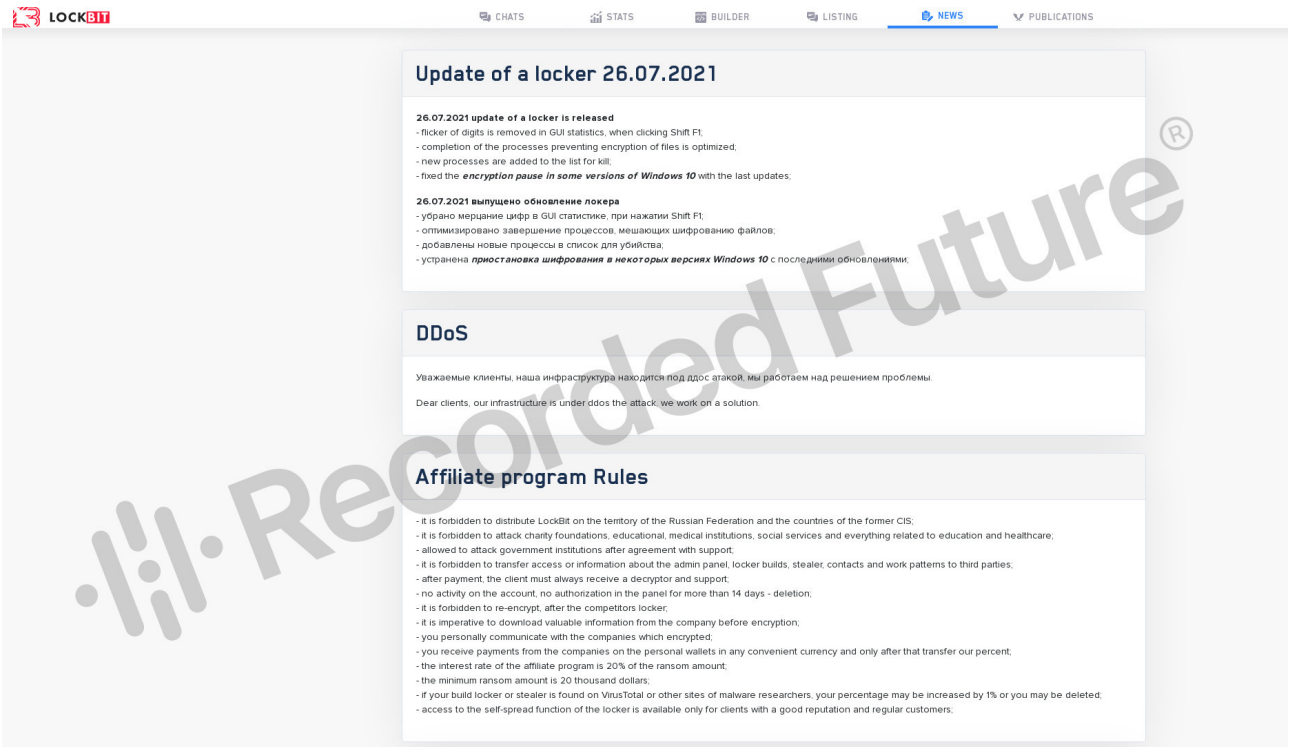


IMAGE: THE RECORD

DS: Representatives from 30 countries met this month to discuss how to address ransomware attacks. Does this worry you in any way or do you believe this is just political grandstanding?

LB: They are just shaking the air. If you cannot defeat the enemy – lead him. Nobody canceled Newton's third law.

DS: Law enforcement agencies in several countries are now openly discussing hacking ransomware infrastructure to destroy stolen data and retrieve encryption keys. Does this worry you? Are your storage systems safe enough?

LB: This is one of the most effective methods to deal with us; no one is immune from hacking infrastructure with the help of 0-days. Using NSA hardware backdoors, it is possible to access any server on the planet. Therefore, the risk of being hacked is always present. At the moment, we are absolutely confident in the security system for storing decryption keys and stolen data, no competitor has any analogs. In addition to this, we have several backups of stolen company data on servers in various parts of the world, as well as encrypted offline backups held by trusted parties who receive a salary for safekeeping the data.

DS: The US government said it would go hard after cryptocurrency services that have helped ransomware groups launder funds. Do you anticipate this being a problem for you and the ransomware landscape in the future, or do you have other avenues of laundering funds?

LB: "*Our path is difficult and far, my* bitcoin *rushes to the east*". Show me at least one Chinese who will listen to what the US is telling him and not accept cryptocurrency from us when exchanging for cash dollars in Hong Kong.

DS: Are you ready to provide a decryption key for a company that was unable to raise funds in October for free?

LB: There are no companies without money, there are cunning companies that do not want to spend money on protecting their network, pay salaries for good system administrators, and then on a ransom. Perhaps we will make a free decrypt for one company "who could not raise funds", but in that case, the data of this company will remain in our great onion blog forever.