LockBit 2.0 Interview with Russian OSINT

ke-la.com/lockbit-2-0-interview-with-russian-osint/

August 24, 2021

On August 23, 2021, the YouTube channel Russian OSINT published an interview with the LockBit 2.0 ransomware gang in Russian. KELA translated the full interview.

Main points:

- LockBit's representative brags that **no other RaaS affiliate program provides the same conditions for affiliates, including their own stealer for a victim's data, paying ransoms directly to the affiliates' wallets, and more.** He claims LockBit 2.0 is the fastest ransomware.
- According to LockBit's representative companies did not become better at protecting themselves despite the wave of ransomware attacks in recent years.
- **The ransomware ban on forums did not prevent LockBit from recruiting new affiliates.** In fact, it only helped them to compete with new RaaS programs since the latter are less recognizable without a presence on the forums.
- **A victim's location is not important for LockBit, they care only about the company's revenue.** LockBit claims it will not attack healthcare, education, charitable organizations, and social services.
- LockBit supposes **the supply chain attacks (like the Kaseya attack by REvil) will happen more often in the near future.**
- LockBit supposes that **the guiding principle behind companies' decision whether to pay the ransom or not is potential loss calculations.**
- **The COVID-19 pandemic and the migration to remote work have benefited LockBit, making it easier to infect targets**.
- **Two reasons for the prevalence of American and European companies among ransomware victims** are, in LockBit's opinion, the fact that **cyber insurance is more developed in those countries**, and that **some of the world's wealthiest companies are located there**.
- When asked how to protect from ransomware attacks, LockBit suggests that **companies should employ a full-time Red Team, regularly update their software, maintain employee awareness of social engineering, and invest 5-10% of the corporate budget in cybersecurity**, depending on the size and complexity of the corporate network.

Question (Q): What does it mean - LockBit? Do you have a story behind this name?

Answer (A): “Lock” is a lock and “Bit” is a unit of measure for the amount of information in computer systems.

Q: Why do you think you continue to work successfully while many other ransomware groups are forced to close their business?

A: Because we enjoy our work and we take anonymity seriously.

Q: Compared to other ransomware - Maze, REvil, Conti, DarkSide - how does your product differ from them from a technical point of view?

A: On our blog in the onion network *[TOR – KELA]* there is a comparison table. We are in the first place in terms of the encryption speed and the speed of dumping the company data. The distribution and encryption processes are automated. Just one *[payload – KELA]* launch on the domain controller is enough – after the shortest period of time, the entire corporate network is encrypted.

Q: The year 2021 has become a real headache for all big companies that have been attacked by ransomware. What is the reason we have not heard anything like this in 2019-2020?

A: A lot of information in the press, big money – it attracts more and more people to this business. At the same time, the risks are growing.

Q: In general, how do you treat other ransomware-as-a-service [operations - KELA] - neutrally, positively, negatively?

A: We have a negative attitude towards ransomware gangs that encrypt healthcare and educational institutions. We prefer to attack those who are, like us, “business sharks”.

Q: What LockBit attacks do you think were the loudest ones?

A: A lot of noise around the attack is bad. A silent attack no one knew about is good for the company’s reputation, and our income.

Q: The Lockbit 2.0 update has recently appeared. What are the most significant changes in a new version of the software?

A: We continue to move in our own direction. LockBit, unlike other RaaS, is, first of all, a software complex and only then a set of related services. Our mission is to provide a tool that will help to carry out an attack as soon as possible. The faster the attack is carried out, the less the risk that the attack will be repelled. It also means more companies can be encrypted in one working day. The most significant changes are the increase in encryption speed without losing quality and, of course, a stealer *[StealBit – KELA]* that automatically downloads all important data of a company to the administrative panel. Clients of the affiliate program *[affiliates of the RaaS program – KELA]* no longer need to mess with servers and cloud storage services, wasting time on the routine job and subsequently losing data after a first complaint filed to the cloud provider. In addition, now all the company's data is stored in our TOR blog with the ability to download each file separately thanks to a listing [LockBit's blog posts now include a live file explorer through which one can see the exact files that were leaked and download each one separately – KELA]. There is no other affiliate program on the planet with such an arsenal.

Q: What does the organizational structure of LockBit look like? Does it resemble the Italian mafia?

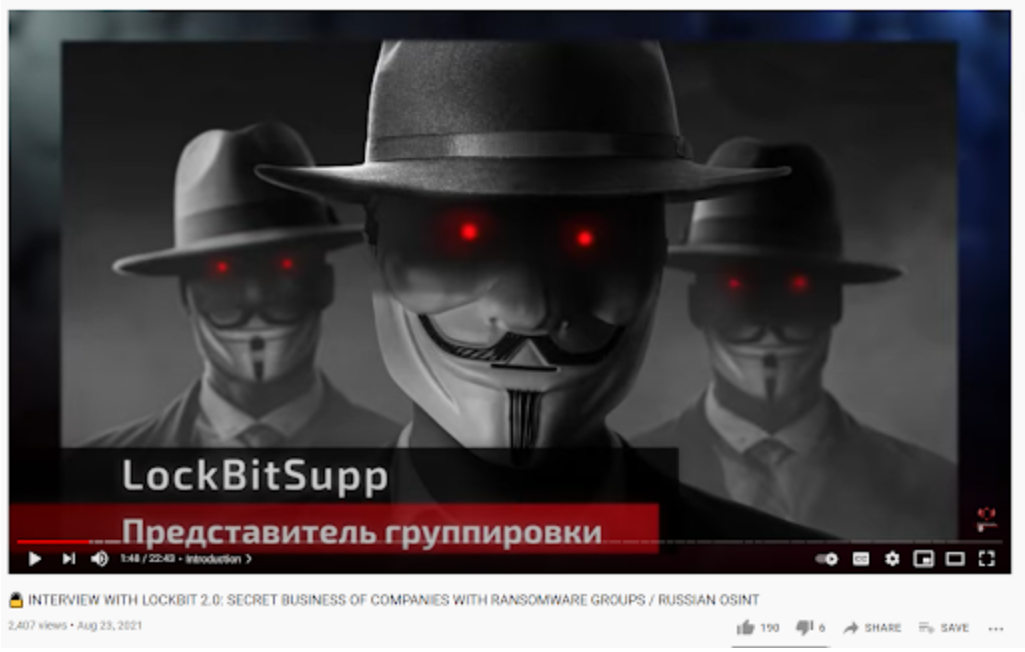
A: It is a classic organized crime group, all the participants get their share *[of income – KELA]*. It doesn't resemble the Italian mafia. In real life, it's better when no one knows what we do, especially relatives. A human factor is the weakest point of any criminal group.

Q: Did you notice any changes in the level of companies' security - now that the ransomware topic is so widely discussed?

A: No. Firstly, companies do not want to spend money on protecting a corporate network and hiring highly paid specialists. Secondly, any protection measure can be bypassed.

Q: How much have you earned in recent years in USD?

A: Enough for a comfortable life. Money loves silence.



LockBit's interview on YouTube

Q: Why do some lockers [ransomware - KELA] require a ransom in Bitcoins and others in Monero - what is it related to?

A: Security or the convenience of cashing out. Only in our affiliate program, a client communicates with encrypted companies by himself. We are not intermediaries and we cannot steal money from anyone – unlike what Avaddon, DarkSide, and REvil did. We do not limit our clients in their choice of currency, it all depends on their priorities, even Dogecoin *[is accepted – KELA]*. Payments are carried out exclusively to our clients' wallets, and then they transfer to us 20% of the ransom.

Q: Special services of all the world are actively working to fight with lockers following the attacks on Kaseya, Colonial Pipeline, JBS. Did you feel such pressure on yourself from law enforcement?

A: We did not. You can only feel the pressure of law enforcement when they have already come to you with an angle grinder and jumped into your window. It is impossible to pressure us by other methods

Q: REvil earlier declared they are apolitical. What is your attitude to politics? Do you have similar views?

A: For us, the unfriendly attitude of the West *[towards Russia – KELA]* is beneficial. It makes it possible to have such an aggressive business and feel calm operating from the CIS countries.

Q: Western media often associate the Russian language of correspondence on forums with Russia. If we talk not about you but about your competitors - is there a practice of fouling the trail? Let's say to communicate with journalists in Russian, and within their infrastructure - only in English?

A: All media are under control and not apolitical. In the West, Russia is represented as the aggressor and the main enemy. Therefore, for the West it is profitable, at any opportunity, to blame Russia for all sins in order to form a negative image about the main enemy. These accusations are not necessarily based on something. The West is behaving in the same way towards China. The United States of America were initially a colony of invaders that exterminated the indigenous population of America and prior to today has been regularly violating human rights. It is not surprising the Black Lives Matter movement appeared in the US. Also, the US is essentially a printing machine *[of money – KELA]* and thanks to this it behaves as a master of the world. Therefore, you should not pay attention to what the Western media say. The practice of fouling the trails on purpose exists.

Q: Following the attack on Colonial Pipeline, ransomware was banned on forums. In response, DDoS attacks [against the forums - KELA] were carried out, but no one took responsibility. What is heard backstage, can you somehow comment on the situation?

A: The attacks were carried out by some people who felt betrayed by their beloved forums who turned out to be cowards. After a while, the insult receded and these DDoS attacks were gone too.

Q: How are you managing to attract adverts [affiliates - KELA] now when all topics related to ransomware are banned on forums?

A: For us, it is easier because we have a perfect reputation and we are famous all over the world. For new affiliate programs, it will be harder to announce themselves and earn a reputation during the information blockade. So, this taboo on forums did us a favor. We do not need a large number of adverts because we know how the Indian fairytale about the [Golden] antelope has ended *[an Indian fairytale with anti-greed morale – KELA]*. When a certain amount of quantity and quality is reached, we close the recruiting process. It is easy to open an affiliate program but it is an art to keep it open.

A greedy Raja drowns in gold in an Indian fairytale about a golden antelope

Q: How do you choose the next target for your attacks? What is the main factor? Do you have any preferences for the region where your potential target is located?

A: The bigger the company's capitalization is – the better. There are no *[other]* main factors. If there is a target, then it needs to be "worked out" *[attacked – KELA]*. It does not matter where the target is situated, we attack everyone. There is no time and desire for preparing for an attack on a specific target because there is always enough work. Our targets are businesses, capitalists.

Q: Do you have any moral code in terms of choosing targets? For example, not to attack healthcare or educational organizations.

A: We do not attack healthcare, education, charitable organizations, social services – everything that contributes to the development of personality and sensible values from the survival of the species perspective. Healthcare, medicine, education, charitable

organizations, and social services remain intact.

Q: What victim companies have been paying a ransom more often than others? Why in your opinion?

A: The victims who are paying are the ones who do not make backups and poorly protect sensitive information, regardless of the industry.

Q: Will the lockers go bankrupt if authorities around the world will introduce a ban on paying ransoms at the legislative level for companies in the US, Europe, CIS, Asia, in the Middle East? Since the money for the maintenance of their infrastructure will simply be nowhere to be taken.

A: There will be no such law that will prohibit companies from paying a ransom. Often, the information [that was stolen] is strategically important. Losing this information is a huge loss for a company, it may cost a leading position in the market. It can turn into serious damage to the country's economy. Authorities won't make such a rash step.

Q: Could such events as the Olympic Games in Japan serve as a catalyst for an increase of attacks on a certain region, in particular, the hosting country?

A: For companies, it always makes sense to worry about their cyber security, regardless of the Olympic Games. The timing doesn't matter.

Q: What do you think about REvil's attack on Kaseya? Is it possible to expect a new stage in the development of the ransomware business, namely, attacking the supply chain? What is the likelihood that this kind of attack will occur more often in the near future?

A: We think that REvil has an excellent advert who performed this attack. Such affiliates are always very valuable since they form the image and authority of the affiliate program. Such attacks for sure will be carried out in the future since there is no flawless software. Vulnerabilities are endless and everywhere.

Q: In your opinion, what guides the companies' decision whether to pay the ransom or not?

A: Potential loss. However, sometimes you stumble on guys with principles. I'll repeat myself – we are dealing with capitalists in the first place, which means they assess the risks, probable benefits, or losses from the deal.

Q: Do you offer any discounts on the ransom, if the company contacts you quickly and operates properly during negotiations?

A: Almost always. Our target is to streamline the attacks.

Q: How did the global COVID-19 pandemic - and the mass migration to remote work - affect you, and did it change your strategy?

A: *[It influenced – KELA]* positively, of course. Many employees started working remotely from personal computers, which are easier to infect with a virus and steal account information used to access the companies.

Q: Why are US and EU companies targeted more often by ransomware than others? There is an opinion that one of the reasons is the language barrier: companies from countries with more complex languages are attacked less often; is it the reason?

A: The insurance in this sphere *[i.e. insurance in the case of ransomware – KELA]* is more developed in the US and EU, and the largest number of the world's wealthiest companies is concentrated there.

Q: Sometimes lockers change their names and do a "rebranding". Will this tendency persist, in your opinion?

A: It becomes more difficult to enter this business, more money and knowledge are required. It makes no sense to change the name if you are honest with your clients and hold your reputation dear. Trust is being earned in a matter of years but is lost in a moment – like it was the case with Avaddon, DarkSide, and REvil.

Q: Are you using any OSINT tools or technologies throughout the attacks?

A: All available methods are being used.

Q: In your practice, did you encounter cases, when a group of companies performed a sensitive deal, and during those activities, a company paid a little "protection fee", so that no one would intrude their systems and affect the deal, for example at the moment when a merger decision was being made?

A: This is a fantasy.

Q: Probably you have watched my episode with a famous lawyer from New York, Arkady Bukh. In that episode, we spoke about the fact that sometimes cybercriminals disclose their accomplices, for their own profit and a "green card". Do you know any public cases, when partners "sold" their accomplices and handed over incriminating materials to special services?Q: Probably you have watched my episode with a famous lawyer from New York, Arkady Bukh. In that episode, we spoke about the fact that sometimes cybercriminals disclose their accomplices, for their own profit and a "green card". Do you know any public cases, when partners "sold" their accomplices and handed over incriminating materials to special services?

A: We don't know of such cases. If you are caught, don't get sad, hand over everything you've had.

Q: Some time ago, Cisco Talos published an interview with your representative. What reactions and what results did you get from this interview? Did it meet your expectations?

A: We have got new affiliates.

Q: What advice can you give to companies, so that they will not become LockBit's target?

A: Employ a full-time Red Team, regularly update all software, perform preventive talks with a company's employees to thwart social engineering, and most importantly – use the best ransomware-fighting antivirus – BitDefender.

Q: If you could turn back time, would you be doing the same things you do now?

A: Of course not. I sleep very badly at night. Money can't buy happiness.

Q: A billion dollars - is it enough to "leave the stage"?

A: We love our job. The money is not the target – the process is the important thing. And of course, fortunate is not the one who is rich, but the one who has a loyal wife *[quote from a popular Russian crime movie "The Brother" – KELA].*

Q: How would you briefly describe your life's path?

A: The one of self-realization. You should do the things that you can do the best because you need to realize your potential – this is a basic necessity for every human.

Q: Were there cases when cybersecurity companies tried to deanonymize you? If yes, please share the details of such attacks - what did you remember the most?

A: There were. Usually, they try to make you click a link using social engineering, but sometimes they send journalists to perform behavioral analysis and create a possible criminal profile.

Q: In one of my interviews with Wojciech, a Polish offensive OSINT specialist, he said "Ransomware, first and foremost, bets on easy money and obvious access points such as RDP, unpatched VPN, and trivial phishing - they all work in a relatively similar way. ICS hacking requires specialized knowledge, understanding of protocols' work. I highly doubt the possibility of locking critical infrastructures in some city." In your opinion, is his claim true?

A: True, but only partially. Those who have specialized knowledge and tools unavailable for many can mask their attacks, so that it would not be clear whose work it was – a professional or an average hacker.

Q: The chastity belts' locking story [an end of 2020 ransom demands aimed at users of IoT chastity cages - KELA]. What sense do those attacks make, when some lockers conduct them? Is this some PR stunt to make yourself known?

A: It's a ROFL *["rolling on the floor laughing" – KELA]*.

Q: Recently, Western media wrote that some ransomware groups recruit negotiators to their lines - does it really require specialized people?

A: It depends on the pentester's free time. A good pentester doesn't have time for negotiations.

Q: I heard an opinion from one cybersecurity specialist, that the lockers' existence is profitable for certain large infosecurity companies. For example, a victim company is required to pay ten million dollars, and then immediately comes a large cybersecurity company and promises to decrypt

for seven million; but in reality, the cybersecurity company turns to the lockers - without the victim's knowledge - and negotiates to pay, say, five million dollars from their own pocket. In the end, a large infosec giant makes two million. Is there some truth to it?

A: It's 100% true. Almost all recovery companies do this.

Q: When you became a dollar millionaire, how much did this feeling change you as a person? What in your worldview has fundamentally changed?

A: It gave me confidence in the future, and also the ability to pay for a very expensive surgery required for my brother. Attitude to security and anonymity has fundamentally changed.

Q: Sophos Labs' experts wrote earlier that LockBit, before encrypting the victim, calls GetUserDefaultLangID which determines the default keyboard setting. If there are Russian, Ukrainian, Uzbek, Kazakh, Armenian, and other languages then the target is not encrypted. Let's suppose that many companies adopt this practice, does it mean that companies would not be encrypted anymore?

A: The system's language is checked, and not the keyboard setting.

Q: Not once we hear opinions of certain info security experts, and even underground members, that locking, ransomware, is, to say it nicely, a not very smart endeavor skill-wise, meaning that this is some sort of primitiveness that has little in common with the art of hacking. How would you comment on this attitude towards ransomware?

A: This claim is invalid because few can write the fastest encryption algorithm in the world; the software always requires support and innovation, so technical savviness is extremely important.

Q: In your practice, have you seen - from the inside - cases when companies deceive their clients, collect more of their information than needed, sell it, manipulate clients, and siphon money, using the acquired data? Can you talk about such cases?

A: Yes, we did. Usually, such companies pay the ransom significantly faster. I can't tell the details, because our reputation is important to us and in case of ransom payment we destroy the company's data, ensuring complete confidentiality of the deal.

Q: Not only in the CIS countries, but possibly in South America, the Middle East, Europe, and Asia as well, companies invest too little in their cybersecurity. Often, executives do not understand what risk management is, are not ready to allocate budgets to train their infosec experts and employees, nor spend money on protection of their infrastructure, pay adequate salaries, etc. Here is where many problems begin. It's no surprise that, sometimes, skilled infosec experts switch to the "dark side". If organizations, afraid of the possibility of being attacked by ransomware, will start investing money in their cybersecurity, the lockers' job will become harder due to stern competition between "blackhat" and "whitehat" experts, which will surely make the global infosecurity market bigger. Do you, generally, support this attitude, that companies need to give more attention to their cybersecurity, invest more money in infosec?

A: I don't support it. Let them fire everyone – I need the cybersecurity specialists more.

Q: What percentage of the corporate budget should, ideally, be spent on cybersecurity, so a company could calmly deal with its commercial affairs?

A: It depends on the complexity of the corporate infrastructure and the amount of potential entry points. I think that about 5-10% would be enough to make sure that the company will never fall victim to ransomware.

Q: Final question - you have been cornered: would you fight to the death, or retreat to save your life?

A: You should first make a commercial offer which is very difficult to refuse, and if it won't help – fight to the death. But as we know, money defeats evil.