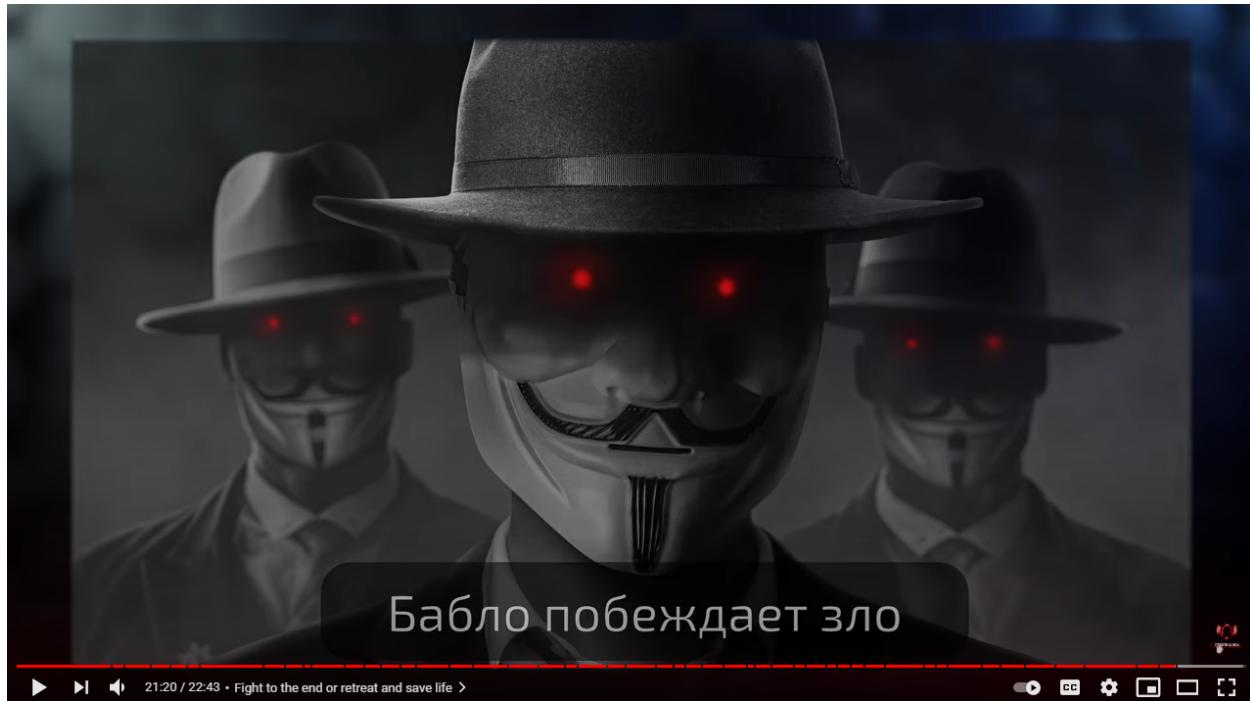


**LockBit Interview - 08/23/2021**  
**English Version - Translation by AdvIntel**



*Source: Russian OSINT YouTube Channel LockBit Interview*

**Q:** What LockBit stands for and what is the history of its origin?

**A:** Lock is a lock, bit is a binary digit.

**Q:** Why do you think you continue to operate successfully while many other ransomware syndicates were forced to close their businesses?

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

**Q:** How different are you from Maze, REvil, Conti, Darkside in terms of the technical features of your products?

**A:** There is a comparison table on our onion data leak website. Nobody can beat us when it comes to the speed of encryption and data exfiltration, plus the level of automation with the distribution and encryption are processed. All it takes is one run on a domain controller and the entire corporate network is encrypted in the shortest amount of time.

**Q:** 2021 is a real headache for all major companies that have been attacked by ransomware. Why is there such an increase in attacks compared to 2019 and 2020?

**A:** A lot of publicity and a lot of money are two factors that attract people into this business, but the risks grow along with it.

**Q:** How do you generally feel about other Ransomware-as-a-Service - neutral, positively, negative?

**A:** I feel negative towards RaaS, which encrypts medical and educational institutions. We only attack business sharks just like us.

**Q:** What is the most “loud” and high-profile LockBit's attack?

**A:** A “loud” attack is bad for the company because it causes reputational losses for the company. A quiet attack is good for both - the company and for our profit.

**Q:** What are the most significant changes to the newly released version of LockBit 2.0?

**A:** Unlike other RaaS, LockBit 2.0 first of all is a complex software itself and then a set of related services. Our mission is to provide a tool that can help launch an attack in the shortest amount of time. The faster the attack is performed, the lower the risk that the attack can be repelled and the more companies can be encrypted within a business day.

The most significant changes are the increase in encryption speed without loss of quality and, of course, Stiller, which automatically downloads all-important company data into the administration panel. Affiliate program partners no longer need to fiddle with servers and cloud storage and waste time on routine work, subsequently losing data after the first complaint to the cloud provider. Besides, thanks to the listing all company's data are stored in our torrential blog with the ability to download each file separately. No other affiliate program on the planet has such an arsenal.

**Q:** What does LockBit's organizational structure look like, does it resemble the Italian mafia?

**A:** It is a classic organized crime group - all the participants are in on the take. It does not resemble the Italian mafia, as we prefer no one to know what we are doing in real life, especially the relatives. The human factor is the weakest aspect in any criminal group.

**Q:** Do you notice any changes in the security practices of companies as ransomware attacks became very common and widely discussed?

**A:** No. First, companies don't want to spend money and hire qualified and costly specialists to protect corporate networks and. Second, any protection can be bypassed.

**Q:** How much money did you make over the last few years?

**A:** Enough for a comfortable life. Money likes silence.

**Q:** Why do some lockers require redemption in Bitcoins, while others prefer Monero? What is the reason for that?

**A:** Safety and convenience of cashing out. Our program lets affiliates handle negotiation processes with encrypted companies. Thus, we are not cheating anyone for money like Avaddon, DarkSide and REvil did. Our partners can choose whichever crypto they want, even DogeCoin. Ransom payment is made exclusively to the partner's wallets, after which they transfer us 20% of the redemption.

**Q:** The intelligence services around the world are actively working to combat ransomware following the attacks on Kaseya, Colonial Pipeline, and JBS. Did you feel any kind of pressure from law enforcement?

**A:** We didn't. The only way you can feel the pressure from the security apparatus is when they are already at your doorstep physically breaching your door or your window. It is impossible to put pressure or intimidate us by any other means.

**Q:** REvil has previously stated that they are apolitical. What is your attitude towards politics? Do you share a similar view?

**A:** We benefit from the hostile attitude of the West. It allows us to do conduct such an aggressive business and operate freely within the borders of CIS countries.

**Q:** The Western media often associates Russian language correspondence on forums with Russia. Is there a practice of misleading the trail, not you but your competitors? Let's say you communicate with journalists in Russian, but within your own infrastructure in English?

**A:** All media are controlled and not apolitical. The West presents Russia as an invader and as the common enemy. Therefore, it is essential for the West, to use any opportunity, to accuse Russia of any mortal sins in order to form a negative opinion

about this main enemy. As a result, there is absolutely no need (for the West) to ground or back up these accusations. The West behaves in the same way with China as well. The United States of America was founded by foreign invaders who exterminated the native population of the continent and regularly violates human rights to this day. There is a reason why the BLM movement exists in the U.S. Moreover, the United States is essentially a (money) printing press and as a result, they behave as if they were the masters of the world. Therefore, we should not pay attention to what the Western media is saying. The practice of purposefully misleading the trial exists.

**Q:** Ransomware topics were banned from DarkWeb forums after the attack on Colonial Pipeline. Right after forums were heavily DDoS attacked, but nobody claimed responsibility. What really happened behind the scenes?

**A:** The attacks were carried out by some people who felt that they were betrayed by their beloved forums. After a while, the resentment went away, so DDoS attacks.

**Q:** How did you manage to attract affiliates while forums completely banned ransomware activity?

**A:** It was actually easy as our impeccable reputation works well for us and we are famous across the community. But it definitely made it harder for new affiliate programs to promote and earn a reputation in the time of information blockade. The banning of topics related to ransomware played well for us and benefited our business. We do not need a large number of affiliates, we all know this Indian fairytale that didn't end well. When we reach a certain number of quality partners, we close enrollment. It is not hard to open an affiliate program, the hardest part is to stay afloat.

**Advintel Comment:** *Indian fairytale is a story about a greedy raja who met a magical antelope that produced gold by banging its hooves. Driven by greed, the rajah kept asking for more until he eventually drowned in a mountain of gold which then turned into rubble.*



*Screenshot illustrates a scene from a cartoon based on Indian fairytale "Gold Antelope"*

*Source: Russian OSINT YouTube Channel LockBit Interview*

**Q:** What is the deciding factor for you to choose the next target? Do you have any preferences in terms of the geographical region?

**A:** The main deciding factor is the capitalization of the company, the bigger the better. It doesn't matter what the geographical location of the target, we attack everyone who comes to hand. There is no time for a planned attack on a particular target as we have enough work to take care of. Our target is business capitalists.

**Q:** Are you driven by any moral code when choosing the next target to exclude medical or educational institutions for example?

**A:** We do not attack medical and educational institutions, as well as social services and charities. Anything that contributes to the development of the human beings and their safety remains untouched.



*Source: Russian OSINT YouTube Channel LockBit Interview*

**Q:** What companies pay ransom more often and easier to negotiate with and why?

**A:** Those companies that don't do backups and don't protect sensitive information pay well, regardless of industry.

**Q:** How are you going to handle the business if the U.S., Europe, CIS, Asia, and the Middle East will penalize companies for paying the ransom?

**A:** These countries won't pass such a law. There is too much strategically important information that might cause the companies to go out of business and seriously damage counties' economies. The authorities won't take such a hasty step.

**Q:** Is there any correlation between major world events such as the Olympic Games in Japan and the increase of cyberattacks in that particular geographical region?

**A:** Companies should worry about their cybersecurity practices all the time, regardless of any events such as the Olympics.

**Q:** What do you think about the REvil's attack on Kaseya? Are we going to see an increase in supply chain attacks such as Kaseya?

**A:** We think that REvil has really great pentesters who performed this attack. Such people are extremely valuable because they are the ones who form a positive image and credibility of an affiliate program. Similar cyberattacks will happen for sure, there is always vulnerability to exploit.

**Q:** What are the factors for companies to decide whether to pay or not to pay a ransom?

**A:** Mostly profit, but sometimes we deal with some principled ones. Again, our targets are capitalists first and foremost and they always carefully weigh an assessment of risks and possible benefits or losses of the deal.

**Q:** Do you make any discounts on ransom if the company responds and negotiates quickly?

**A:** Very often. Our goal is to put the process on stream.

**Q:** How have you been affected by the global Covid-19 pandemic? Has the mass shift to telecommuting changed your strategy?

**A:** We saw a positive impact on our business. Many employees are working remotely on personal computers, making it easier for us to infect them with a virus and steal credentials to access the company.

**Q:** Why are US and EU companies the most being attacked by ransomware? Some people say that this is due to relatively simple language. Other countries with more complex languages create a language barrier which makes it harder to communicate with targets. Is this true?

**A:** The United States and European entities are the most insured companies across the globe plus these regions have the biggest concentration of the richest companies.

**Q:** Sometimes RaaS rebrand themselves and change their names. Do you think this trend will continue to grow?

**A:** It's getting harder to get into this business as it takes more money and more experience. There is no point in changing the name if you are honest with your partners and value your reputation. It is very hard to earn trust and very easy to lose it, like Avaddon, DarkSide, and REvil did.

**Q:** Do you use any OSINT tools and techniques in support of attack?

**A:** All available methods are being used.

**Q:** Did you have any cases when you intruded into the company's network in the middle of an important deal, for example during the acquisition with another company? If yes, were there attempts from the company to pay you for your silence just to close the deal?

**A:** That's nonsense.

**Q:** You might have seen my interview with the famous lawyer from New York, Vitaly Buch where he was talking about the fact that sometimes gang members betray other members and give up all of the information to secret services in exchange for the Green Card. Are you aware of any public cases like this?

**A:** We know of no such cases. If you have been caught, do not be offended, part with your money quickly.

**Q:** Earlier, Cisco Talos published an interview with your representative. What kind of reaction and what kind of result did you get after that interview? Did it meet your expectations?

**A:** Gained new affiliates.

**Q:** What advice do you have for companies to avoid being targeted by LockBit?

**A:** Hire a full-time Red Team, update all software regularly, have due diligence talks with employees to counter social engineering. And most importantly, use the best ransomware antivirus - BitDefender.

**Q:** If you could turn back time, would you still do what you are doing now?

**A:** Of course not, I don't sleep very well at night, it's not about money.

**Q:** Is a billion dollars enough to go off-stage?

**A:** We love our work and money is not the goal. We enjoy the process and stability and fortune is more important for us.

**Q:** Could you briefly describe your life path?

**A:** My path is self-realization. People need to do what they do best because it's important to use the potential to the maximum. This is a basic necessity for every person.

**Q:** Did someone try to de-anon you? If yes, please share the details of such attempts. What is the most memorable?

**A:** There have been attempts. Usually, they send phishing links and use social engineering. Sometimes they send journalists to perform behavioral analysis to build a supposed profile of the attacker.

**Q:** In one of my interviews with Wojciech, an offensive OSINT specialist from Poland, he said the following. Ransomware primarily relies on easy money and exploits clear entry points, like RDP, unpatched VPN, and banal phishing. ICS hacking requires specialized knowledge and understanding of how protocols work. I highly doubt the possibility of locking down the critical infrastructure of the whole city. Is his statement correct?

**A:** Correct, but only in part. Those who have advanced skills and tools available for such an attack are able to hide their potential by mimicking an average hacker. It makes it hard to distinguish whose work it was - an average hacker or highly professional one.

**Q:** What is the story with the encryption of chastity belts? Is it some sort of PR move to get fame?

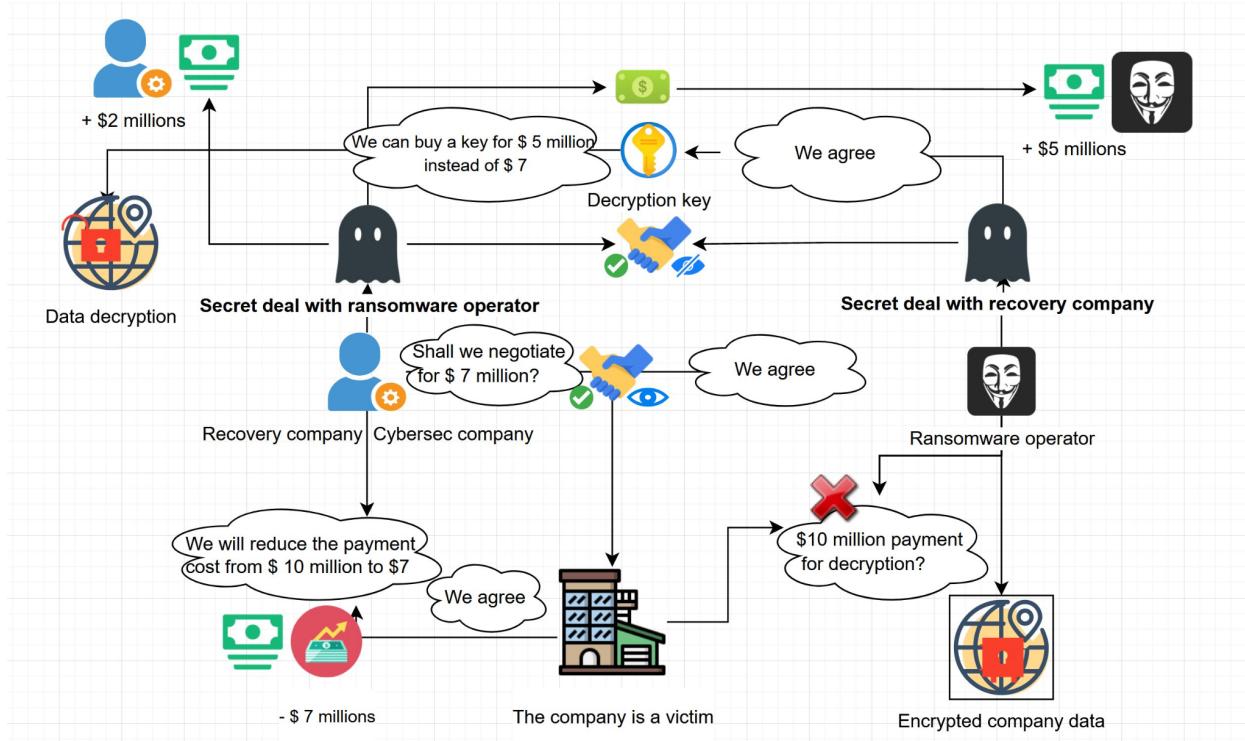
**A:** It's ROFL.

**Q:** The Western media recently wrote that some ransomware groups are recruiting negotiators in support of their operations? Do they really need special people for that?

**A:** It all depends on the pentester's free time. A good pentester has no time to negotiate.

**Q:** I've heard that some big infosec companies benefit from ransomware attacks. In some cases, when a company is asked for a 10 million ransom, a big cybersec company comes into play and promises to decrypt the network for 7 million. In reality, they negotiate with ransomware operators without the knowledge of the victim company and offer, let's say 5 million dollars. In the end, they end up with 2 million in profit. Is there any truth in it?

**A:** It's 100% true, almost all companies do it that way.



*Infographic reflects a scheme which, according to the cybercriminals is used by incident response companies and was mentioned by LockBit 2.0 representative*

*Source: Russian OSINT YouTube Channel LockBit Interview*

**Q:** Did a million dollars change you as a person and make you look at the world differently?

**A:** It gave me confidence in the future, and I was able to pay for a very expensive surgery for my brother. It also drastically changed my attitude towards security and anonymity.

**Q:** Sophos Labs experts previously wrote that LockBit accesses GetUserDefaultLangID, which determines the keyboard layout, before encrypting the victim. It does not encrypt the machine if there are Russian, Ukrainian, Uzbek, Kazakh, Armenian, or other CIS languages. Can it be used by companies to avoid an attack and encryption?

**A:** The system language is checked, not the keyboard layout.

**Q:** I often hear an opinion from the underground community that ransomware does not require advanced technical skills. That is a kind of primitivism, which has little in common with the concept of the art of hacking. How would you comment on this attitude towards ransomware?

**A:** This statement is wrong because there are only a few people in the world able to write the fastest encryption algorithms. Software constantly requires support and innovation, so being technically savvy is extremely important.

**Q:** Have you seen cases where companies cheat on their customers by collecting more data than necessary and then trading this data and taking advantage of people? Could you share such cases?

**A:** Yes, we have and usually such companies pay the ransom much faster. I won't give you any details. We value our reputation and destroy all of the victim's data if the ransom is paid, guaranteeing full confidentiality of the deal.

**Q:** Former Soviet Union countries, as well as South America, the Middle East, Europe, and Asia, invest little if not at all in cybersecurity. Management does not understand what risk management is and does not allocate budgets to address security practices including training of their it-specialists and paying decent wages, staff as well as spending money for effective solutions to protect their infrastructure. Hence, many problems arise. No wonder why very competent professionals sometimes go to the dark side. If organizations would invest in their cybersecurity for fear of being attacked by lockers, it will become harder for lockers to work. It will also create competition between Black & White specialists, which will undoubtedly lead to the growth of the Infobase market worldwide. Do you support the approach for companies to pay more attention to their cybersecurity and invest more money?

**A:** I don't support it. I'd be happy for the companies to lay off all of the cybersecurity specialists, so I would be able to hire them.



*Source: Russian OSINT YouTube Channel LockBit Interview*

**Q:** What percentage of a company's budget should ideally be spent on cybersecurity to make sure safe development of its commercial products?

**A:** It depends on how complex the company's infrastructure is and how many potential entry points there are. I think around 5-10% would be enough to ensure that the company would never be hit by ransomware.

**Q:** Final question. You are backed into a corner - are you going to fight to the death or retreat for your life?

**A:** First make a commercial offer which is very hard to refuse. And if it does not help, then fight to the death, but as you know money always beats evil.

**LockBit Interview - 08/23/2021**  
**Russian Version - Transcript by AdvIntel**

**В:** Что означает LockBit и есть ли история происхождения этого названия?

**О:** Лок - замок, бит - единица измерения количества информации в компьютерных системах.

**В:** Как вы думаете почему вы продолжаете успешно работать когда многие другие группы шифровальщики вынуждены закрывать свой бизнес?

**О:** Потому что мы получаем удовольствие от нашей работы и серьезно относимся к анонимности.

**В:** Если сравнивать вас с другими шифровальщиками Maze, REvil, Conti, Darkside чем вы отличаетесь от них с технической точки зрения ваших продуктов.

**О:** В нашем блоге луковой сети есть сводная таблица. Мы на первом месте по скорости шифрования и скорости выкачивания данных компаний, процесс распространения и шифрования автоматизированы. Достаточно одного запуска на контроллере домена и через кратчайший промежуток времени вся корпоративная сеть зашифрована.

**В:** 2021 год по настоящей головной болью для всех крупных компаний, которые подверглись атаке шифровальщиков. С чем это связано и почему мы не слышали ничего подобного в 2019 и 2020 годах.

**О:** Много информации в прессе, большие деньги - это привлекает всё больше и больше людей в этот бизнес, но вместе с этим растут риски.

**В:** Как в целом относитесь к другим Ransomware-as-a-Service - нейтрально, положительно или отрицательно?

**О:** Отрицательно относимся к RaaS, который шифрует медицинские и учебные заведения. Мы предпочитаем атаковать акул бизнеса, таких же как и мы.

**В:** Какие атаки LockBit считаете самыми громкими?

**О:** Громкая атака это плохо и тихая атака, о которой не узнала общественность это хорошо, как для репутации компании так и для нас деньги.

**В:** Недавно вышло обновление LockBit 2.0. Какие наиболее значимые изменения появились в новой версии софта?

**О:** Мы продолжаем двигаться своим направлением. LockBit в отличие от других RaaS это это в первую очередь программный комплекс, а уже потом набор сопутствующих услуг. Наша миссия предоставить инструмент, который в максимально короткие сроки поможет провести атаку. Чем быстрее проводится атака, тем меньше риск что атаку смогут отразить, а также больше компаний можно зашифровать за рабочий день. Самые значимые изменения это увеличение скорости шифрования без потери качества и конечно же Стиллер, который автоматически скачивает все важные данные компаний в административную панель. Клиентам партнёрской программы больше не нужно возиться с серверами и облачными хранилищами. Тратя время на рутинную работу, в последствии теряя данные после первой жалобы по облачному провайдеру. Кроме того теперь все данные компаний хранятся в нашем торг блоге с возможностью скачивать каждый файл отдельно благодаря листингу, такого арсенала нет ни в одной партнёрской программы на планете.

**В:** На что похожа организационная структура LockBit, напоминает ли она допустим итальянскую мафию?

**О:** Классическая организованная преступная группа - все участники в доле. Итальянскую мафию не напоминает, лучше чтобы в реальной жизни никто не знал чем мы занимаемся, а тем более родственники. Человеческий фактор самое слабое место в любой преступной группе.

**В:** Замечаете ли вы какие-либо изменения в уровне защищенности компаний сейчас, когда тема шифровальщика стала широко обсуждаться.

**О:** Нет. Во-первых компании не хотят тратить деньги на защиту корпоративной сети и найм высокооплачиваемых специалистов. Во-вторых любую защиту можно обойти.

**В:** Сколько вы заработали за последние годы в долларах?

**О:** Достаточно для комфортной жизни. Деньги любят тишину.

**В:** Почему некоторые локеры требуют выкуп биткоинах, а другие в монеро? С чем это связано?

**О:** Безопасность и удобства обналичивания. Только в нашей партнерской программе клиент сам общается с зашифрованными компаниями. Мы не являемся посредниками и не можем никого кинуть на деньги как это сделали Avaddon, DarkSide и REvil. Мы не ограничиваем своих клиентов в выборе, любая удобная валюта хоть DogeCoin, в зависимости от приоритетов. Выплата осуществляется исключительно на кошельки клиента после чего он переводит нам 20% от выкупа.

**В:** Спецслужбы всего мира ведут активную работу по противодействию локеров после атак на Kaseya, Colonial Pipeline и JBS. Почувствовали ли вы на себе подобное давление?

**О:** Не почувствовали. Давления массы силовика можно почувствовать только когда к тебе уже пришли с болгаркой или запрыгнули в окно. Другими методами невозможно оказать давление на нас.

**В:** REvil ранее заявляли о своей аполитичности. А какое у вас отношение к политике, у вас схожее мировоззрение?

**О:** Для нас выгодны недружественное отношение Запада. Это дает возможность вести столь агрессивный бизнес и спокойно чувствовать себя, находясь в странах бывшего СНГ.

**В:** Западные СМИ часто ассоциируют русский язык переписки на форумах с Россией. Если говорить не о вас, а о ваших конкурентах, существует ли практика запутывания следов? Допустим общение с журналистами на русском языке, а внутри своей структуры и друг с другом на английском?

**О:** Все СМИ подконтрольны и не аполитичны. Россия представляется на Западе как агрессор и главный враг, поэтому Западу выгодно при любом удобном случае обвинить во всех грехах Россию, с целью формирования негативного мнения о главном враге и совершенно необязательно, чтобы эти обвинения были обоснованы. В сторону Китая Запад ведет себя точно также. Соединенные Штаты Америки же изначально являлась колонией захватчиков, которая истребила коренное население Америки и до сегодняшнего дня регулярно нарушает права человека. Не зря же в Соединенных Штатах Америки существует общественное движение Black Lives Matter. Также Соединённые Штаты Америки являются по своей сути печатным станком и благодаря этому ведет себя как хозяин в мире. Поэтому не стоит обращать внимание на то что говорят западные СМИ. Практика целенаправленного запутывания следов существует.

**В:** После атаки на Colonial Pipeline шифровальщикам запретили работу на форумах и в ответ прилетели DDoS атаки, но никто не взял на себя ответственность. Что слышно в кулуарах можете как-то прокомментировать ситуацию?

**О:** Атаки были осуществлены некоторыми людьми, которые почувствовали предательство и трусость от родных и горячо любимых форумов. Через какое-то время обида прошла как и DDoS атаки.

**В:** Как в последнее время вам удавалось привлекать адвертов, когда все темы связанные с локерами на формах блокируются?

**О:** Нам в этом плане проще, так как у нас есть безупречная репутация и о нас известно всему миру. Новым партнерским программам будет тяжелее заявить о себе и заработать репутацию в информационной блокаде. Поэтому табу на форумах пошло нам на пользу. Мы не нуждаемся в большом количестве адвертов, так как знаем чем закончилась индийская сказка про антилопу. При достижении определенного количества и качества мы закрываем набор. Открыть партнёрскую программу легко, а вот не дать ей закрыться это уже искусство.

**В:** Как выбираете следующая цель для своей атаки? Что является решающим фактором? Есть ли у вас какие-то предпочтения по региону, где расположена ваша потенциальная цель?.

**О:** Чем больше капитализация компании, тем лучше, решающих факторов нет. Если есть цель то её нужно отработать, где расположен на цель неважно. Мы атакуем всех подряд, кто попадется под руку. Готовится к атаке на конкретную цель нет времени и желания, так как работы всегда хватает и без этого. Наш сектор это бизнес капиталисты.

**В:** Придерживайтесь ли вы какого-либо морального кодекса при выборе целей для, как например не проводите атаки на медицинские и образовательные учреждения?

**О:** Медицина, образование, благотворительные фонды социальной службы, всё что способствует развитию человеческой личности, здравых ценностей с точки зрения выживания вида мы не атакуем. Медицина, образование благотворительные фонды, социальные службы остаются нетронутыми.

**В:** Какие компании жертвы платили выкуп чаще других и почему на ваш взгляд?

**О:** Платят те, кто не делает бэкапы и плохо защищает чувствительную информацию, независимо от отрасли.

**В:** Если власти по всему миру сделают на законодательном уровне запрет на оплату выкупов Ransomware для компаний в США, Европе, СНГ, Азии и на Ближнем Востоке. Не обанкротятся ли локеры, так как деньги на содержание инфраструктуры просто неоткуда будет взять?

**О:** Не будет такого закона, который запретит компаниям платить выкуп. Информация часто бывает стратегически важной, потеряв её это потеря компании или как минимум лидирующих позиций на рынке. Это серьезный урон экономике страны, на такое опрометчивый шаг власти не пойдут.

**В:** Является и такие события как Олимпийские игры в Японии своеобразным катализатором увеличения на определенный регион, в частности на страну организатора?

**О:** Компаниям всегда имеет смысл беспокоиться о своей кибербезопасности, независимо от Олимпийских игр, мораториев нет.

**В:** Что вы думаете об атаке REvil на Kaseya? Можно ли ожидать новый этап развития бизнеса шифровальщиков, а именно комбинацию атак на цепочку поставок? Какова вероятность что атаки, подобные kaseya будут совершаться чаще в ближайшем будущем?

**О:** Думаем, что у REvil есть великолепные адверты, выполнивший эту атаку. Такие кадры всегда очень ценные, так как именно они формируют имидж и авторитет партнерской программы. Подобные атаки будут совершаться в будущем, так как не бывает безупречного программного обеспечения, везде и всегда будут находиться уязвимости.

**В:** По вашему мнению чем руководствуются компании, когда решают платить или не платить выкуп.

**О:** Выгодой, но порой попадаются принципиальные. Повторюсь, мы имеем дело с капиталистами в первую очередь, а это оценка рисков, возможной выгоды или убытков от сделки.

**В:** Делаете ли вы какие-либо скидки на выкуп, если компания быстро идёт на контакт и оперативно взаимодействует в переговорах.

**О:** Практически всегда. Наша цель поставить атаки на поток.

**В:** Как на вас повлияла мировая пандемия Covid-19? Массовый переход на удаленную работу изменил ли вашу стратегию?

**О:** Конечно же положительно. Много сотрудников стали работать удаленно с личных компьютерам, которые проще заразить вирусом и украдь учетные данные для доступа в компанию.

**В:** Почему компании США и Европейского Союза чаще других подвергаются атакам шифровальщиков? Есть мнение, что одна из причин этой языковой барьера. Компании стран с более сложными языками атакуются реже, является ли это причиной?

**О:** В Соединенных Штатах Америки и ЕС развито страхование в этой сфере. Именно тут сосредоточено больше всего богатейших мировых компаний.

**В:** Иногда локеры меняют свои названия и делают ребрендинг. Как вы считаете, сохранится ли эта тенденция на ваш взгляд?

**О:** Войти в этот бизнес становится сложнее, требуется больше денег и знаний. Менять название нет смысла если ты честен с клиентами и дорожишь своей репутацией. Доверие зарабатывается годами, а теряется в одно мгновение, как это произошло с Avaddon, DarkSide и REvil.

**В:** Используете ли вы во время атаки какие-либо ОСИНТ инструменты и технологии?

**О:** Используются все доступные методы.

**В:** Встречались ли на практике случаи, когда группа компаний проводила ответственную сделку и во время этих мероприятий компания давала небольшие откупные только за то чтобы никто не вторгся в их систему и не повлиял на сделку, допустим на момент принятия решений по слиянию компаний.

**О:** Это фантастика.

**В:** Возможно вы смотрели мой выпуск с известным адвокатом из Нью-Йорка, Виталием Бухом. Там речь шла о том, что иногда представители cybercrime отдают своих подельников ради своей выгоды и Green Card. Известны ли вам публичные

случаи, когда партнеры закладывали подельников и отдавали компромат в руки спецслужб.

**О:** Подобные случаи нам неизвестны. Если ты попался, то не обижайся, давай побыстрее с деньгами расставайся.

**В:** Ранее Cisco Talos публиковали интервью с вашим представителем. Какую реакцию и какой результат вы получили после этого интервью? Совпало ли это с вашими ожиданиями?

**О:** Получили новых адвертов.

**В:** Какой советы вы можете дать компаниям, чтобы они не стали мишенью LockBit?

**О:** Нанимать на full-time red team, регулярно обновлять все ПО, проводить профилактические беседы с сотрудниками компаний для противодействия социальной инженерии. И самое главное использовать лучший антивирус по борьбе с программами вымогателями и BitDefender.

**В:** Если бы вы могли повернуть время вспять, стали ли бы заниматься тем чем занимаетесь сейчас?

**О:** Конечно нет, я очень плохо сплю по ночам не в деньгах счастье.

**В:** Миллиард долларов достаточно ли чтобы уйти со сцены?

**О:** Мы любим свою работу, деньги не являются целью, важен процесс и конечно же не тот счастлив у кого много добра, а тот у кого жена верна.

**В:** Как бы вы кратко описали свой жизненный путь?

**О:** Путь самореализации. Нужно делать то, что получается лучше всего, ведь свой потенциал важно реализовать. Это базовая необходимость для каждого человека.

**В:** Бывали ли случаи когда вас пытались деанонитить cybersec компаний? Если да, то поделитесь подробностями таких атак. Что больше всего запомнилось?

**О:** Бывали. Обычно пытаются заставить перейти по ссылке с помощью социальной инженерии, но иногда подсылают журналистов, чтобы провести поведенческий анализ и составить предполагаемый портрет преступника.

**В:** В одном из моих интервью с Войцехом, специалистом из Польши по jffensive OSINT, он говорил следующее. Ransomware прежде всего делают ставку на легкие деньги и понятные точки входа такие как RDP, не пропатченные VPN и банальный Fishing, они работают примерно все одинаково. Хакинг ICS требует специальных знаний, понимание работы протоколов, я ставлю под большое сомнение идеи локинга критической инфраструктуры в каком-нибудь городе. На ваш взгляд, верно ли его утверждение?

**О:** Верно, но лишь отчасти. Те, кто обладает специальными знаниями и недоступным для многих инструментарием, способны замаскировать свои атаки таким образом, чтобы не было понятно кто работал профессионал или среднестатистический хакер.

**В:** История с шифрованием поясов целомудрия, в чём смысл подобной акции у некоторых локеров? Это некий пиар ход, чтобы заявить о себе?

**О:** Это ROFL.

**В:** Недавно в западных СМИ писали, что некоторые Ransomware группы набирают в свои ряды переговорщиков? Неужели для этого требуются специальные люди?

**О:** Это зависит от свободного времени пентестера. У хорошего пентестера нет времени на переговоры.

**В:** Я слышал от одного из cybersec специалистов мнение, что некоторым большим инфосек компаниям выгодно существование локеров. Например от компании жертвы требует 10 млн долларов, тут же приходит большая cybersec компания и обещает дешифровать за 7 млн, но на деле cybersec компания обращается к локерам без ведома компании жертвы, договаривается выплатить из своего кармана допустим 5 млн долларов. По итогу крупный infosec гигант зарабатывает профит 2 миллиона. Есть ли в этом доля правды?

**О:** Это 100% правда, так делают практически все Recovery компаний. Когда вы стали долларовым миллионером, как сильно это ощущение поменяло вас как личность? Что кардинально изменилось в мировоззрении,

**В:** Это дало мне уверенность в завтрашнем дне, а также возможность провести очень дорогую операцию, необходимую моему родному брату. Кардинально изменилось отношение к безопасности и анонимности.

**О:** Специалисты Sophos Labs ранее писали, что LockBit перед шифрованием жертвой обращается к GetUserDefaultLangID, которая определяет раскладку клавиатуры. Если там есть русский, украинский, узбекский, казахский, армянский и другие языки, то цель не шифруется. Допустим эту практику внедрят во многих компаниях, получается компании больше не смогут быть зашифрованы?

**О:** Проверяются язык системы, а не раскладка клавиатуры.

**В:** Не в первый раз слышал мнение отдельных ИБ-специалистов и даже представителей андеграунда, что локинг шифровальщики это мягко говоря не умное занятие с точки зрения скила и навыков. То есть это некая примитивщина, которая мало что имеет общего с понятием искусства хакинга. Как бы вы прокомментировали такое отношение к Ransomware?

**О:** Это утверждение неверно, потому что мало кто способен написать самые быстрые алгоритмы шифрования в мире. Программное обеспечение постоянно требует поддержки и нововведений, поэтому техническая подкованность крайне важна.

**В:** Из своей практики, видели ли вы случаи, когда компании обманывают своих клиентов, собирают о них больше данных, чем нужно, торгуют ими манипулируют клиентами и выкачивают деньги, пользуясь полученной датой? Можете ли вы рассказать о таких случаях?

**О:** Да, видели. Обычно такие компании гораздо быстрее платят выкуп, подробностей рассказать не могу, так как мы дорожим своей репутацией и в случае уплаты выкупа уничтожаем данные компаний, при этом гарантируя полную конфиденциальность сделки.

**В:** Не только в СНГ, но возможно Южной Америке, на Ближнем Востоке, Европе, Азии, компании мало вкладывают свою кибербезопасности. Зачастую, руководство не понимает что такое риск-менеджмент, не готовы выделять бюджеты на обучение своих it-специалистов, персонала, а также тратить деньги на закупку эффективных решений по защите своей инфраструктуры, платить достойную заработную плату и многое другое. Отсюда и вытекают многие проблемы. Неудивительно почему иногда очень грамотные специалисты переходят на темную сторону. Если организации начнут из-за опасений быть атакованными локерами вкладывать деньги в своих кибербезопасность, локерам станет сложнее работать, появится жесткая конкуренция между Black & White специалистами, что приведет несомненно к росту рынка инфобиза во всём мире. Поддерживаете ли

вы в целом такой подход по компании должны уделять больше внимания своей кибербезопасности и вкладывать больше средств?

**О:** Не поддерживаю. Лучше пусть всех уволят, мне нужнее специалисты по кибербезопасности.

**В:** Какой процент бюджета компании в идеале должен тратиться на кибербезопасность, чтобы компания могла спокойно заниматься развитием своих коммерческих продуктов?

**О:** Зависит от того насколько сложная инфраструктура компании и насколько много потенциальных точек входа. Я думаю около 5-10% будет вполне достаточно чтобы компания никогда не пострадала от вымогателей.

**В:** Финальный вопрос. Вас загнали в угол - драться насмерть или отступить, сохранив жизнь?

**О:** Сначала сделать коммерческое предложение, от которого очень трудно отказаться. А если не поможет, то драться насмерть, но как известно бабло побеждает зло.