TALOS
Cisco Security Research

Interview with a LockBit ransomware operator

By Azim Khodjibaev,
Dmytro Korzhevin and Kendall McKay

Updated Jan. 4, 2021

CONTENTS

INTRODUCTION

In September 2020, Cisco Talos established contact with a self-described LockBit operator and experienced threat actor. Over the course of several weeks, we conducted multiple interviews that gave us a rare, first-hand account of a ransomware operator's cybercriminal activities. Through these exchanges, we gleaned several valuable takeaways for executives and the broader cybersecurity community.

Companies and security strategists are often most concerned about prolific threats that garner lots of media attention – those involving APTs, sophisticated TTPs and large-scale compromises costing organizations millions of dollars. What is frequently overlooked, though, is a more common and simpler type of threat, which was represented by the LockBit operator we spoke with. The actor is allegedly self-taught and stays up to date on the latest cybersecurity developments, weaponizing new research to use in future attacks. He operates alone, without the support of a large group or state actor. He uses well-known tactics, relying heavily on common tools like Mimikatz, PowerShell, and others rather than exploiting zero-day vulnerabilities or using more sophisticated methods. He looks for targets with well-known security issues that can be easily exploited, and, like many criminals, he says he seeks only modest financial gains to provide for his family.

This actor's TTPs remind us to remain vigilant about these seemingly unsophisticated, common cybercriminals who, despite their straightforward approach to targeting and operations, continue to be highly successful in compromising companies and wreaking havoc on unsuspecting victims. Below are our key takeaways for executives and network defenders from our interview with this LockBit operator:

- **Threat actors continue to view unpatched systems as an easy, if not preferred, method of intrusion.** Routine patching can be difficult, especially for large organizations, and the bad guys know this, too. The most commonly exploited vulnerabilities are those that are well-understood with publicly available exploit code.
- **Many cybercriminals rely almost exclusively on common open-source tools that are readily available on the internet and easy to use.** They are not looking to reinvent the wheel, and tool reuse is a quicker, more effective way for them to carry out their operations than leveraging more sophisticated means. Companies should be most concerned about the tools and tactics that are also likely used by their own red teams.
- **Cybercriminals are avid consumers of security news and remain up to date on the latest research and vulnerabilities, weaponizing that information to use in future attacks.** They are often self-taught and hungry for continual knowledge, a mentality that all but ensures they will always be updating their TTPs and looking for new ways to make their attacks more successful. Organizations should encourage their security teams to continue their own learning – not just by obtaining industry-respected security certificates, but by remaining familiar with the latest open-source information, conducting their own research, and closely following trends in the threat landscape.
- **While threat actors may state publicly that their personal ethics influence their target selection, many adversaries go after the easiest victims regardless of any moral obligation, based on our experience.** We assess that schools, health care providers, and COVID-19 response-affiliated entities remain high-value targets – despite contrary claims by threat actors – given their generally under-funded cybersecurity teams and low downtime tolerance.

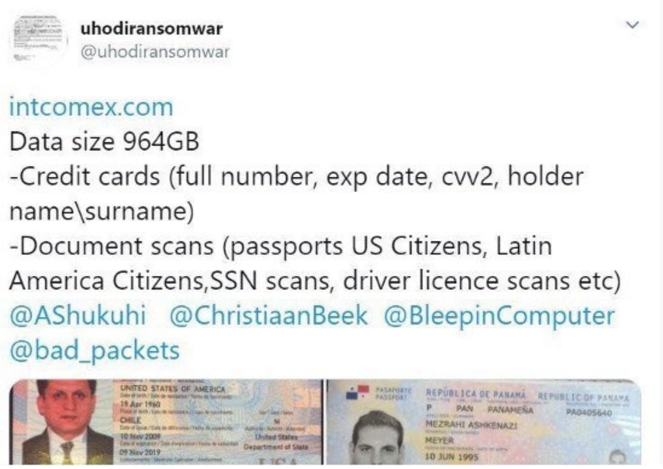
This report also has a human-interest component, as it explores the actor's professed motivations for transitioning from legitimate IT work to illicit cyber activity, his insights on the current threat landscape, and his thoughts on other major ransomware groups. Below are some of the most interesting claims this LockBit operator made, which, if true, provide valuable insight into the current ransomware scene.

- The actor appears to have a contradictory code of ethics, portraying a strong disdain for those who attack health care entities while displaying conflicting evidence about whether he targets them himself. This is probably representative of many adversaries engaged in illicit cyber activity.
- Hospitals are considered easy targets, making ransom payments 80 to 90 percent of the time during a ransomware attack.
- Maze formerly kept up to 35 percent of ransom profits earned by its affiliates, an extremely high amount compared to other ransomware groups that likely deterred some actors from working with them.
- The EU's General Data Protection Regulation (GDPR) law plays to adversaries' favor, with victims in Europe being more likely to pay ransoms to avoid the legal consequences of the compromise if it became public knowledge.
- The U.S. also has lucrative targets, but with data privacy laws requiring victim companies to report all breaches – regardless of whether an attack is mitigated via cooperation with the adversary – the incentive for such entities to pay the ransom is likely somewhat reduced.

INITIAL CONTACT AND ACTOR CREDIBILITY

This operator has several usernames and handles on various social media platforms. As explained below, he made initial contact with us on Twitter using his @ uhodiransomwar account (transliterated from Russian as "go away, ransomware"). The first mention of this actor in open-source reporting was in June 2020, when he published access to a major VPN provider's SSH keys. That same month, security researchers at KELA mentioned uhodiransomwar as being active since 2009 and associated with LockBit ransomware.

Our contact with the actor, who we will refer to throughout this report as the fictitious name "Aleks," began in early September, when he used his uhodiransomwar account to Tweet that he had compromised a Latin American financial institution. Shortly thereafter, the actor tweeted at the victim organization, this time tagging several cybersecurity contacts, likely to compel the victim to respond by drawing public attention to the attack. One of the tagged accounts belonged to Bleeping Computer, a technology news website that has previously communicated with other ransomware operators, and one of the authors of this paper, who focuses on cybercrime in Eastern Europe and Asia. We believe Azim was tagged because he initially followed @uhodiransomwar's account for research purposes.



uhodiransomwar
@uhodiransomwar

intcomex.com
Data size 964GB
-Credit cards (full number, exp date, cvv2, holder name\surname)
-Document scans (passports US Citizens, Latin America Citizens,SSN scans, driver licence scans etc)
@AShukuhi @ChristiaanBeek @BleepinComputer @bad_packets

Figure 1: Screenshot of uhodiransomwar's tweet.

We used this initial indirect contact as an inroad to establish communication with uhodiransomwar. We directly messaged Aleks with questions that were specific to the conditions he set for the victim. During our initial conversations, we shared what we believed to be Aleks' identity and location based on our own research, which he confirmed. The threat actor was familiar with Talos' work based on the information available on their Twitter account. Notably, this did not discourage Aleks from engaging with us. Rather, it sparked a lot of curiosity about the "white hat" side of the business, as he referred to it. Our initial chats, which focused mostly on the victim, occurred over Twitter's direct messaging platform. It was during this time that Aleks offered to conduct an interview for what he referred to as "my interests and research purposes." Talos accepted the offer, interviewing the subject over the course of several days during late September and early October 2020.

Before the interview began, Aleks established some preconditions and guidelines. First, he requested that we refer to him specifically as a "LockBit operator."

Additionally, while he agreed to let us publish our summary and analysis of the interview, he asked us not to share the evidence he provided as proof of his access to LockBit operations. One of the pieces of evidence was a screenshot of a conversation between himself and the victim. Aleks also shared information about a victim organization being compromised two days before the breach was made public, highlighting his inside knowledge of LockBit threat activity. Lastly, Aleks provided some evidence of victims that had paid their ransom on time, but he did not want their names disclosed since they had "honored" their part of the transaction. As always, Talos provided any relevant information to our law enforcement partners at the conclusion of our research.

We found Aleks to be credible during our conversations. As outlined above and throughout other parts of this report, he provided ample evidence of his standing within the LockBit community, including advance knowledge of LockBit operations and changes to the group's ransomware, which we were able to corroborate. His seemingly strong moral convictions – including protecting victims' identities if they paid the ransom, his emphasis on the importance of establishing trust with a victim, and the existence of certain ethical guidelines pertaining to targeting – also positively influenced our assessment of his credibility. Aleks also seemed to be forthcoming in sharing personal information about himself, including his immediate family, highlighting his openness and a degree of vulnerability. Lastly, we generally found him responsive to our requests to maintain an ongoing dialogue and he was willing to answer our questions with what seemed like full transparency.

PROFESSIONAL BACKGROUND AND ACTOR MOTIVATION

By learning about Aleks' professional background and personal interests and beliefs, we came to understand what drove him to engage in cyber criminal activities, how he selects his targets, his thoughts on the ransomware threat landscape, and more. However, we should note that Aleks' views are his alone and may not necessarily represent those of the broader LockBit group. Additionally, we cannot corroborate many of the claims he makes about the ease of targeting certain geographic regions and entities.

Aleks' life is kept busy by his underground criminal activity, but he also claims to have legitimate interests and hobbies, including world history, culinary arts, and music. These conversations were representative of the fact that this threat actor, and others like him, lead seemingly normal lives that are filled with family demands, work deadlines, and leisure activities.

We are confident that the threat actor is a male and resides in the Siberian region of Russia and has probably been an active ransomware operator for at least several years. We estimate that he is in his early 30s and believe that he has at least a university-level education. Aleks claims he is self-taught in cyber-related skills such penetration testing, network security and intelligence collection, both open-source and in the cybercriminal underground. He has been studying and training in IT since the 2000s, when the onset of widespread internet availability sparked his initial interest in what was then a new technology. This included

Confirmed theories

This information was shared with us by Aleks and confirms our previous assessments.

- While no longer active, Maze was once a franchise/affiliate program.
- A selection process existed for Maze and still does for LockBit.
- LockBit has a profit-sharing requirement that the affiliate has to meet for the first four or five ransoms. This also used to be the case for Maze, which its actors shut down in 2020.
- Keeping your word to the victim is an important part of LockBit's business model.

network protocols and the entire line of dial-up protocols (up to v42.bis), which allowed the use of old telephone dial-up lines and a Motorola modem.

After gaining a good understanding of networks, Aleks began to focus on the markup and scripting languages such as HTML, CSS and JavaScript, along with small web frameworks like CodeIgniter. Subsequently, he began to write plugins for these frameworks while also learning how the databases are organized. He spent ample time understanding particular issues within networks as well as the technology behind them. Over time, Aleks' strong understanding of IT technologies helped him secure a job at an IT company while finishing his college degree. After graduation, he continued his work in the IT field.

Despite Aleks' education and aptitude, he expressed a general sense of disappointment, at times even resentment, for not being properly appreciated within the Russian cyber industry. His frustration was evident during our conversations, with him disparaging several well-known Russian cybersecurity companies. He also remarked that, "In the West, I would probably work in white [hat security] and earn easily..." suggesting that his perceived underappreciation and low wages drove him to participate in unethical and criminal behavior.

Aleks shared several examples of times he felt underappreciated by his peers in the IT and cybersecurity field. During his work, he periodically encountered various security errors while setting up websites. He was naturally curious about such unsecured sites that showed errors or were not working properly. In these cases, he would try to understand the problem and then notify the site's administrators to help fix the issue. However, he was often met with complete disregard for both the problem itself and his efforts to offer a solution. Aleks continued to experience similar scenarios with other websites, including a well-known Russian social networking site.

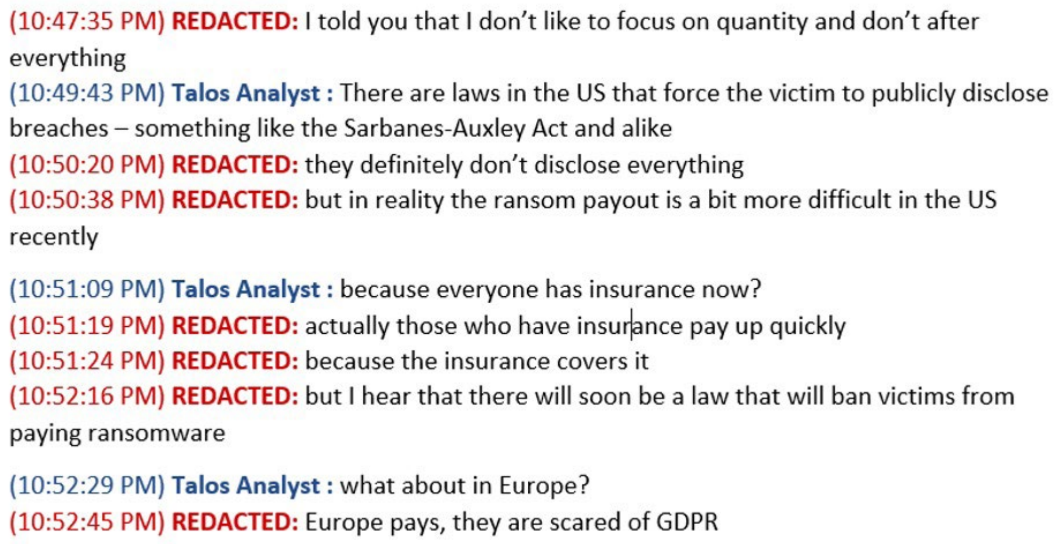
Based on our conversations, it was clear that Aleks was frustrated with being unable to warn about vulnerabilities and often felt like his well-intentioned efforts were ignored. This became a significant motivator for him to pursue unethical and/or criminal work. Recounting one such experience, he told us, "I found a blind SQL injection on a Russian website. I reported and no one reacted, so I dropped it. I realized that our Big Brother (the Russian one) doesn't care about cybersecurity." He surmised that interactions like this encouraged researchers to find other ways to use their skills for financial gain, suggesting many are turning to illegal activities.

Aleks also shared his pessimistic view on bug bounty programs in which vendors pay independent researchers for finding bugs and vulnerabilities in their products. According to him, there has been a strong tendency recently to "deceive" people who report such security flaws. He said that companies are making efforts to find loopholes that allow them to forgo paying the researcher based on technicalities in the completeness of their report. However, this stands completely at odds with our professional observations from the security community. It may be the case that Aleks chooses to view vulnerability programs through this lens to account for his own decision to not participate in them or because he has heard inaccurate stories from other threat actors.

RANSOMWARE OPERATIONS AND TTPS

Once Aleks made the decision to turn to illicit cyber activity, he dabbled in several different types of attacks, including attempting to compromise websites and distributed denial-of-service (DDoS) attacks. He said he eventually settled on ransomware because of its profitability and because it gave him the opportunity to "teach" companies the consequence of not properly securing their data.

Aleks' personal background and desire to be compensated for his skills influences not only his motivation for engaging in illicit activity, as described above, but also his guiding principles around how to carry out such operations. He attested to having a moral code and personal convictions, including a strong sense of patriotism, that influences his target selection. Despite his claims, however, we found several instances in which he made conflicting claims about his ethics and actual conduct. For example, he told us that "for a cybercriminal, the best country is Russia,“ while later explaining that he will not target citizens of the former Soviet Union or "friends of Russia," such as entities within the People's Republic of China, a close Russian ally. Aleks also suggested that entities in post-Soviet states are not as lucrative from an operational perspective and therefore are not worth his time. We believe that Aleks' personal security is likely another factor in his targeting choices, as attacking Russian entities would probably put him at additional risk to retaliation. He went on to note that companies within the United States and the European Union "will pay quicker and more," suggesting those regions are where he focuses his targeting.



(10:47:35 PM) **REDACTED:** I told you that I don't like to focus on quantity and don't after everything

(10:49:43 PM) **Talos Analyst :** There are laws in the US that force the victim to publicly disclose breaches – something like the Sarbanes-Auxley Act and alike

(10:50:20 PM) **REDACTED:** they definitely don't disclose everything

(10:50:38 PM) **REDACTED:** but in reality the ransom payout is a bit more difficult in the US recently

(10:51:09 PM) **Talos Analyst :** because everyone has insurance now?

(10:51:19 PM) **REDACTED:** actually those who have insurance pay up quickly

(10:51:24 PM) **REDACTED:** because the insurance covers it

(10:52:16 PM) **REDACTED:** but I hear that there will soon be a law that will ban victims from paying ransomware

(10:52:29 PM) **Talos Analyst :** what about in Europe?

(10:52:45 PM) **REDACTED:** Europe pays, they are scared of GDPR

Figure 2: A redacted and translated portion of our conversation in which Aleks talked about ransomware payments in the U.S. and Europe. (Editor's note: We mistakenly referred to the Sarbanes-Oxley Act as the "Sarbanes-Auxley Act [sp]" in this correspondence.)

Additionally, Aleks claims that he avoids targeting entities related to health care, labor unions and education. He criticized other ransomware operators that do not share similar ethical views, saying "just because you are a criminal doesn't mean you have to stop being a human being." In a later conversation, he went further, adding that "if you are attacking hospitals during COVID-19, you are a [expletive]." Talos notes that although the Aleks claims to not attack health care institutions, we have reason to believe this is not the case. He shared information with us during our conversations that presumably would only be known by those involved in such operations, such as that "hospitals pay 80 to 90 percent of the time because they simply have no choice." Moreover, his impassioned denial about being involved in such activity is somewhat suspicious and suggests he might be overcompensating to hide potential falsehoods.

Regarding entities Aleks does target, he tends to focus on IT firms that he thinks should be practicing better network security. In our conversations, he made clear that he wanted to "teach them" to employ better security measures. He also has geographic preferences, noting that the Middle East has many "easy" targets with "weak cybersecurity." He added that the EU is the most lucrative area, as Europeans are very concerned with data privacy. Aleks noted that the General Data Protection Regulation (GDPR) law plays to his favor, as victim organizations are more likely to pay ransoms for fear of facing legal consequences if the compromise becomes public knowledge. The United States is also lucrative, but, according to Aleks, its laws around data breaches negatively affect the threat actor's degree of influence during a ransomware operation. In such situations, he explained, the actor has less leverage since U.S. laws require victim companies to publicly disclose breaches anyway. (We note, however, that incentive to pay the ransom might still exist regardless of any legal or regulatory requirements if the victim believes it would avoid having data leaked.) Given these differences, he prefers targeting the EU, noting, "I do not like to work in the U.S. because getting paid is harder there, the EU pays better and more."

He added that if a victim organization has cyber insurance, the ransom payment is "all but guaranteed." This statement aligns with current data showing that ransomware attacks accounted for more than 40 percent of cyber insurance payments in North America during the first half of 2020.

Aleks also revealed more technical components of his ransomware operations, including many of his tactics and tools. He uses common tools and malware that many other malicious actors incorporate into their attack framework, such as Masscan, Shodan, Cobalt Strike, Mimikatz and PowerShell, among others. He also uses information-gathering tools such as ZoomInfo to research possible targets. Aleks suggested that the dark web provides a lot of information on potential targets and their business details. He claimed that ransomware operators can assess their target's worth by either finding stolen information about the company on the dark web from a previous compromise or from insiders at the target organization who sell this information directly on these underground platforms.

Aleks also mentioned that he gains an operational advantage from white hat research that reveals new vulnerabilities and the common delay in users' implementation of new protections. He takes advantage of the gap in time between a vulnerability release and subsequent patching, claiming, "We use white hat research against them. As soon as a CVE is published, we take advantage of it because it takes a long time for people to patch." Essentially, Aleks claims his operations are successful because he is more agile than network administrators by staying current on security news that he incorporates into future attacks. While he lacks the resources of a state actor that would allow him to carry out more sophisticated, stealthy operations, he still maintains an advantage over defenders due to his ability to act quickly based on publicly available information.

Aleks emphasized that one of the most important aspects of his operation is the trust he establishes with his victims. He revealed that without "keeping your word," it would be impossible for him to continue his operations. This comes into play when the ransomware victim pays. Aleks insisted that he deletes the victim's stolen information and never reposts it. At the same time, however, Aleks said he will also follow through with leaking the stolen information if the victim does not meet their conditions.

We also talked extensively with Aleks about how he believes LockBit and other groups execute and manage their attacks. During this part of the interview, he shared his perspective on executing an attack that many researchers already see in the wild. In order to access the victim's network, ransomware operators first try to obtain information about the victim's domain space, including details about the Autonomous System, IP address blocks, or external access gateways that belong to the victim organization. After that, attackers leverage virtual private servers with bulletproof hosting providers and data centers that are usually in Russia (because these providers do not commonly respond to abuse notifications) to scan the externally facing domain space and IP block of the victim's network. Aleks mentioned that operators use scanners such as Masscan, Nmap, and other add-ons, such as RustScan, that enhance scanning speed.

After identifying and confirming various accessible services, such as RDP, a common next step of the attack is using already-compromised accounts to login to the victim organization. This is typically done by searching for the victim's data on the dark web and purchasing it to attempt to log in as the organization's user. If successful, the operator escalates privileges by exploiting a known vulnerability. According to Aleks, any useful information about the victim system is collected and leveraged with open-source tools such as winPEAS and linPEAS. These are primarily leveraged to disable security features, including damaging or disabling the antivirus driver and disabling or bypassing antivirus solutions. These malicious activities are initiated by a series of C2 commands.

Once persistence is established on the victim network, a variety of follow-on attacks are executed. For example, adversaries sometimes attack LLMNR and NBT-NS to obtain the administrator's hashed password, which is then transmitted to the cloud. The operators will use private cloud services found on the dark web to crack the password. Sometimes, tools such as Google Colab and Colabcat are also used during this process. At the same time, an obfuscated stager (using the Artifact Kit or Shelter Pro) is dropped into the random-access memory of the victim machine, allowing the actors to avoid saving any information in the file system. After that, pentesting tools like Cobalt Strike are used to connect with the C3 Custom Command and Control.

To connect the stager with the attacker's C2 infrastructure, various obfuscation parameters are employed using Malleable C2 (in the case of Cobalt Strike), such as the obfuscation of the user agent field. Next, attackers try to collect as much information as possible about the network using automated frameworks such as BloodHound. After that, the ransomware is executed and the operators wait for the victims to contact them.

We also discussed the general structure of the LockBit group, which Aleks described as a business-oriented process where communication is rapid and the dedication to the bottom line is the ultimate goal. For example, Aleks claims that he can directly communicate with the LockBit development team and that he can publish victim information directly to the LockBit blog. According to him, he has privileged information about potential new features that may be added to future versions of LockBit and has the capability to provide technical feedback. During one of our conversations in early September, Aleks claimed that LockBit would be making updates to its ransomware soon. The following month, security researchers from Sophos published new findings indicating that LockBit had started leveraging new methods to stay undetected, confirming our subject's claim and bolstering his credibility.

Aleks also spoke at length about other threat groups, adding that he considered working with other ransomware outfits but chose not to participate with them for several reasons. He specified that the Maze group takes a very high amount of the ransom that is paid – up to 35 percent – leaving operators with less desirable margins compared to other ransomware groups. Aleks explained that while LockBit does not "demand as much as Maze" from their victims, they also have a better profit-sharing ratio. Separately, he also mentioned that "REvil can make your files unstable and Netwalker slows the system down too much." REvil (also known as Sodinokibi) is a highly profitable ransomware group that makes money from compromising lucrative targets and selling its ransomware as a service to other cybercriminals. While Aleks generally works alone, he communicates with other ransomware groups through underground forums. He said the nature of these relationships are business-like, with the actors exchanging information on tactics, malware development, and financially focused agreements.

CONCLUSION

At the time of this writing in in early December, we are still in direct contact with Aleks through Jabber and we continue to collect as much information as we can. In mid-October, Twitter suspended his @uhodiransomwar account because it violated the Twitter Rules against publishing stolen personal data of individuals.

Our interviews with Aleks gave us unique insight into the human side of a threat actor and left us with several valuable takeaways for executives and cybersecurity leaders to consider. As a result of these interactions with Aleks, we were able to confirm many common assumptions about such threat actors, including their background and motivations. Our conversations also revealed the ordinary nature of cyber attacks, which, in this case, still rely heavily on unpatched systems and simple tools.

One of our most interesting takeaways was Aleks' decision-making process that led him to participate in major cyber crimes, or at least the decision-making process he wants us to believe he followed. It is not unusual for criminals to view their own actions as justifiable after the fact even if there was no real moral ambiguity to the crime. In this case, the lack of jobs that meet his satisfaction, appear to be the introductory course to cybercrime. His feelings of underappreciation, resentment, and economic incentive are common motivators of illicit cyber activity, and his story, as portrayed to us, illustrates how one could be driven toward cybercrime.

There appears to be an underlying contradiction in Aleks' portrayal of his personal story in which he presents himself as being guided by certain moral codes, while his actions seem to be more opportunistic, financially motivated and self-serving. This is not unusual, as criminals often rationalize their actions to justify their crimes. Aleks' judgement of other criminals is a good example of this, as it seems he derides them to differentiate himself from their bad behavior.

Based on our conversations with Aleks about LockBit, we believe that the ransomware and its operations will expand in the near future, as there does not seem to be significant barriers to enter the market if one has certain technical skills. Given that there appears to be dedicated development and confirmed success of LockBit's operations, the group will most certainly attempt to capitalize on Maze's recent alleged retirement. Additionally, the spike in remote working and distance learning due to COVID-19 has increased the number of potentially vulnerable victims, making the conditions for LockBit and other ransomware operators even more favorable to continue to expand their operations.