From Russia With… LockBit Ransomware: Inside Look & Preventive Solutions

advanced-intel.com/post/from-russia-with-lockbit-ransomware-inside-look-preventive-solutions

AdvIntel August 26, 2021

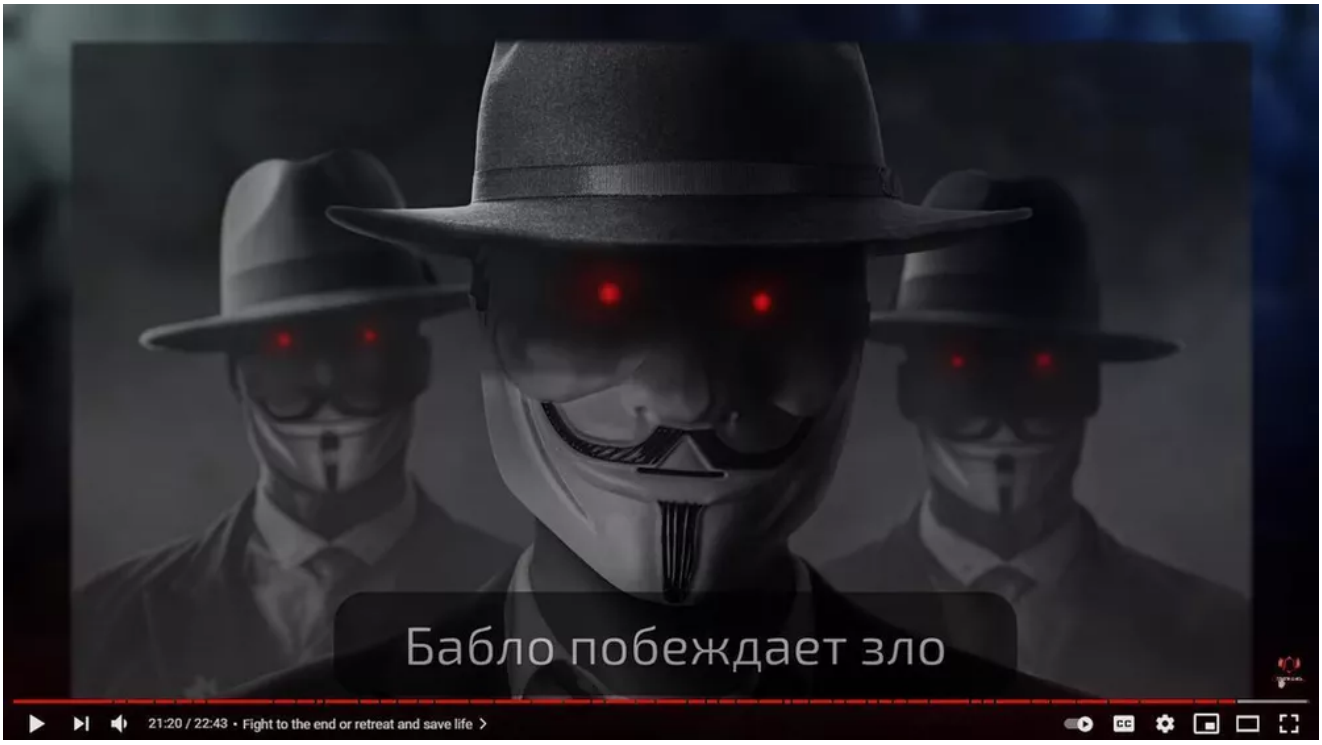
- Aug 26, 2021
-
- 9 min read

By Anastasia Sentsova

A recent interview with a LockBit ransomware gang representative fulfills their purpose of promoting the syndicate and attracting new talented pen-testers. It emphasized all of the technical features of this ransomware and its competitive edge

against other groups, as well as promoted LockBit's reported efforts to protect their affiliates.

This interview is much more than just another ransomware promo - soaked in politics, it hints at the implied relationships between ransomware operators and the Russian political system. Who are these ransomware operators - untouchable caste or regime pawns? The hint is there - just make sure to carefully read between the lines.



Source: Russian OSINT YouTube Channel LockBit Interview

"Money (greed) Beats Evil"

Key Takeaways

- In a recent interview by a Russian-speaking tech blog YouTube channel "Russian OSINT" published on August 23, 2021, (in Russian), the representative of the LockBit 2.0 ransomware group shared insights of their operations and their views of the ransomware business in general.
- Such interviews are commonly weaponized by the RaaS syndicates and cybercrime to serve as a public relations practice in order to attract new affiliates, intimidate the public, and promote their advanced technical features.

- The public outreach of LockBit was likely intended to strengthen the syndicate's media standing and ensure the trust of potential affiliates by promoting alleged high-level moral and business standards claimed by this group.
- An interview has clear political overtones as it covers various aspects such as syndicates' victim's preference and the reflection of current geopolitical agenda, specifically - the US-Russia relationships. The syndicate's rhetoric and public stance have clear similarities with the current political message propagated by the Russian state.

Background

Ransomware has become the main player within the cyber-geopolitical board game. The Russian-language segment of the ransomware community clearly dominates the dark market as well as world media front pages. A relatively novel ransomware group, LockBit 2.0, joined the cybercrime arena in July of 2021 and has a high potential of becoming the leading extortionist syndicate by bringing talented hackers together in order to achieve for-profit or even political goals.

On August 23, 2021, a Russian-speaking tech blog YouTube channel "Russian OSINT" published an interview with the representatives of LockBit uncovering details of their operations. Media interviews became routine for ransomware syndicates and have taken place in large numbers over the past year across various platforms reaching both Russian- and English-speaking audiences. Building public relations is an essential part of the ransomware business model as it is used to not only grow the business but also attract talented pen-testers.

Investigative Analysis

AdvIntel summarizes 5 essential points of the interview with the LockBit 2.0 representative and uncovers the interpretation behind their words.

1. Operations

“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.”

By listing their technical features, the syndicate hopes to attract the most talented hackers out there to enrich their team with sophisticated pen testers. Time is money in ransomware operators' minds - one business day is all it takes to get a victim’s network as a hostage, they say.

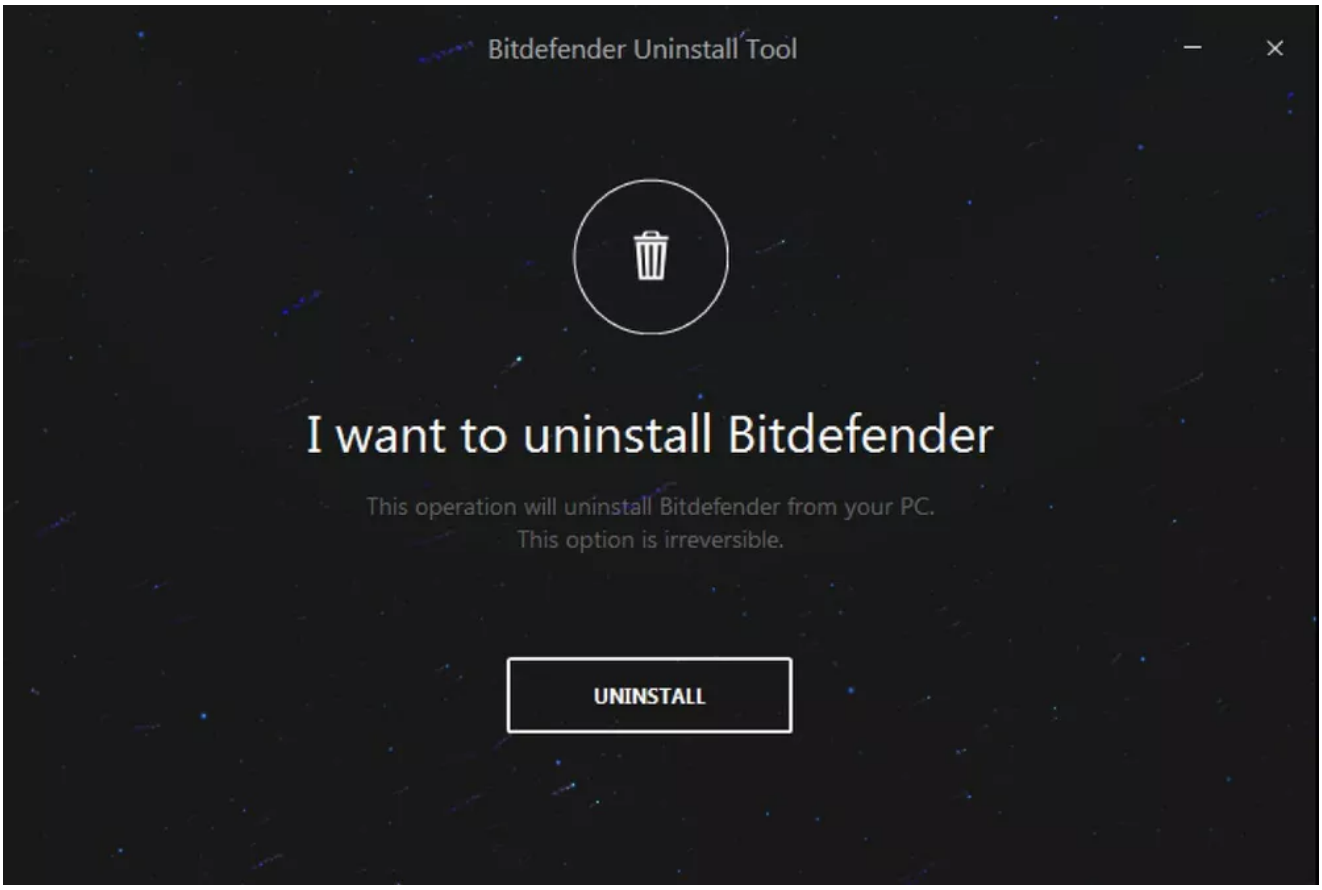
The LockBit 2.0 representative claims their ransomware to have the most advanced technical features allowing it to stand up among its competitors. Stated features include:

1) the fastest encryption speed and data exfiltration

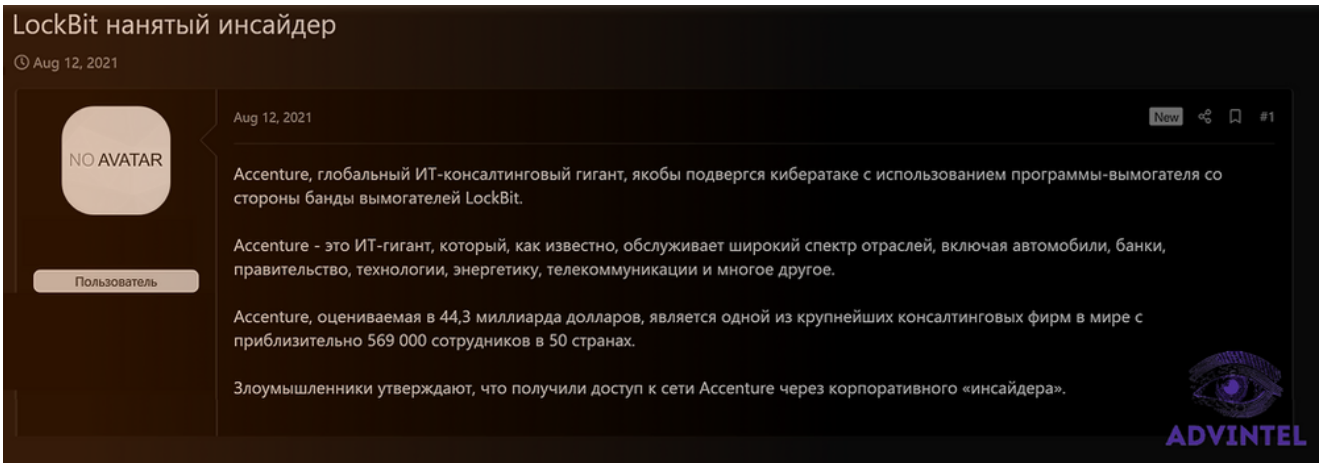
2) automated process of distribution and encryption.

3) Immediate data exfiltration

According to the representative, it takes one run to encrypt the whole victim's network in the shortest amount of time. In addition, affiliates no longer need to fiddle with servers and cloud storage and “*waste time on tedious network routines, subsequently losing data after the first complaint to the cloud provider*.” All victim data is being stored in their data leak website where each file can be downloaded separately.



LockBit referenced the use of BitDefender as a solution against ransomware attacks. At the same time, it is known that ransomware groups are focused on bypassing this tool, including the use of the official Bitdefender Uninstall Tool in order to disable the defenses



Another widely discussed offensive capability that LockBit may have but which has not been mentioned in the interview is insider hiring. In the underground discussions (including the one on the image above) actors reported that for the high-profile attacks including the Accenture incident LockBit has been using insiders to initiate the operation.

Source: (Russian-language underground forums)

2. Victimology

“We do not attack healthcare and educational institutions, as well as social services and charities. Anything that contributes to the development of human beings and their safety remains untouched. ”

Indeed, ransomware syndicates claim to care about morals and promote a high level of morality for future victims. However, as seen by numerous examples of other groups, most importantly, DarkSide, REvil, and BlackMatter, such “moral agendas” never go beyond such flamboyant phrases. LockBit is likely no exception.

In reality, pushing the “social responsibility” agenda is just one more point for the syndicate in order to score high reputation points and establish a positive - as much as it can be - image of a business partner with high values for easier negotiations. *“We value our reputation and destroy all of the victim's data if the ransom is paid, guaranteeing full confidentiality of the deal”,* - they add.

The bulk of the RaaS victimology is for-profit corporations as they are perceived as victims paying large ransoms without causing massive social and political backlashes.

A “loud” attack (media-covered) is bad for the company because it causes them reputational losses. A quiet attack is good for both - the company and for our money.

This being said, except for proper cybersecurity defenses, nothing saves critical industries such as healthcare and education from a ransomware attack.

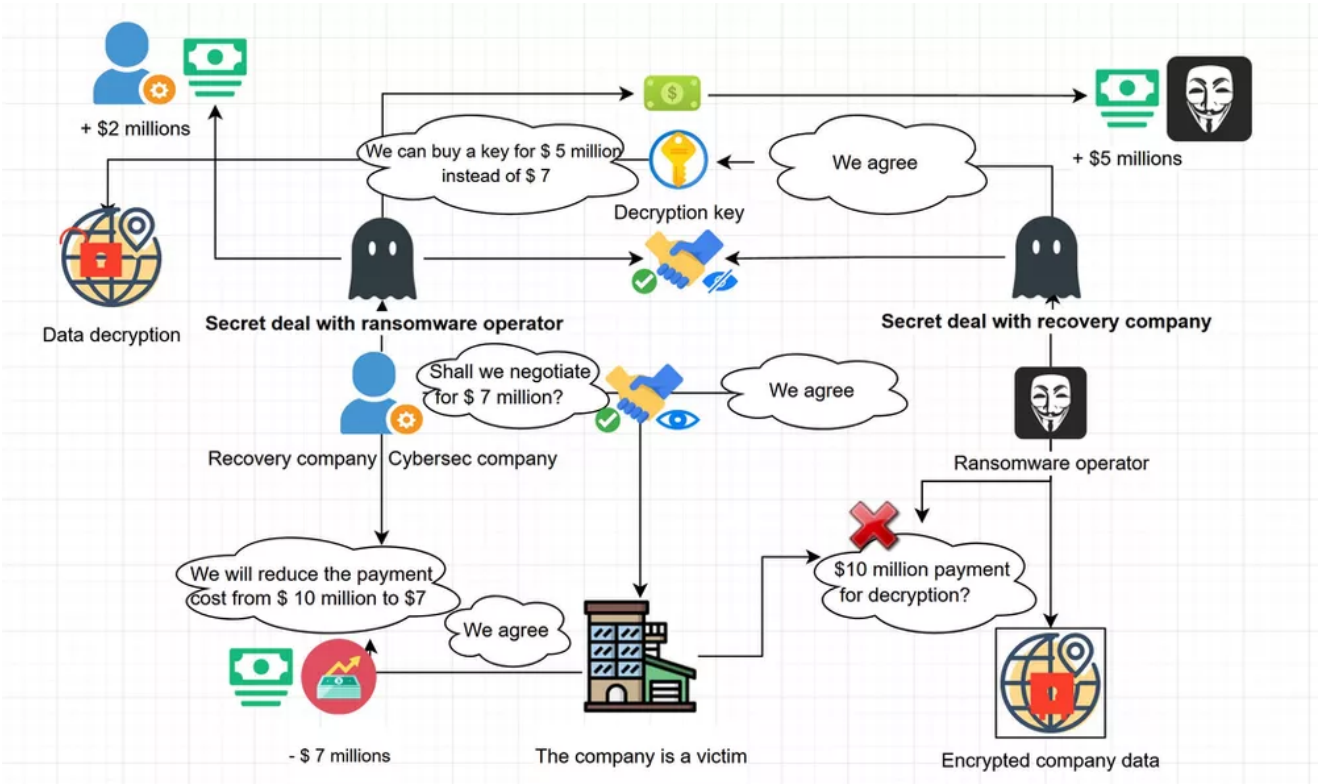
Source: Russian OSINT YouTube Channel LockBit Interview

3. Internal Structure & Affiliates

“Our program lets affiliates handle negotiation processes with encrypted companies. Thus, we are not cheating anyone for money like Avaddon, DarkSide and REvil did.”

By addressing the set of high business standards, the representative stresses a series of incidents inside of ransomware operations that caused a backlash from the underground community. Avaddon, DarkSide, and REvil indeed performed exit scams or scammed their own affiliates by interfering in negotiations between the victim and affiliate and hijacking the ransom payment from an affiliate. It is noteworthy how LockBit attempts to address the distrust of RaaS created by these three groups and pacify the affiliates’ fears.

According to the representative, from now on, LockBit ransom payment is made entirely to the affiliate's wallets. The affiliate then transfers 20% of the payment to the LockBit leadership. This, in turn, will help to improve relationships with future and existing affiliates and rehabilitate ransomware reputation across the underground community.



Infographic reflects a scheme which, according to the cybercriminals, is used by cybersecurity companies and was mentioned by the LockBit 2.0 representative. According to LockBit, incident response companies make a profit by obtaining a decryption key for a lower price compared to a ransom requested from the victim thus keeping the difference in their pockets.

Source: Russian OSINT YouTube Channel LockBit Interview

4. Operational Environment & Strategy

Although ransomware syndicates repeatedly deny any allegations of cooperation with the state (primarily the Russian state), the words of the LockBit representative surprisingly correlate with the rhetoric of Russian officials that is actively propagated in the local media.

“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.”

Such statements are widespread across Russian media outlets. Weaponizing the subject of racial tensions in the U.S. has been religiously practiced even by the early Soviet and propaganda. Just like its Socialist predecessor today, the Russian state intentionally focuses on this narrative in order to cover up major failings of its own judicial system and ongoing human rights violations. At the same time, Russian state propaganda refers to the US's leading role in the global finances to justify the hardship of the domestic economic crisis.

> **The LockBit representative has been the first member of the cybercriminal community, which traditionally is very apolitical, who has started to publicly reiterate these key concepts of the regime's narrative.**

Moreover, according to Russian media, the United States is continuing to be the main enemy and even threat to the world. The latest observation of Russian media demonstrates an increase in discussions centered around the cyber domain and cyber warfare. Responding to the increasing geopolitical tensions, the Russian state media channels push the agenda to deny any involvement of the government or security apparatus in the cybercriminal activity. The state media is also occupying prime time with alarmist reports predicting possible upcoming cyber attacks coming from the U.S.

LockBit transfers this narrative as well by stating:

"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."

Source: Russian OSINT YouTube Channel LockBit Interview

5. Security

“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 (for security services) to put pressure or intimidate us by any other means.”

The fact that the group claims no fear of being arrested by law enforcement does not indicate direct cooperation with the government. However, such an approach does imply that RaaS activities may be fully in line with the Russian state agenda as long as the actors follow the order. The rule is still the same - to whitelist CIS countries (The Commonwealth of Independent States) - except for Ukraine and the Baltics. This list is also being extended to the state’s partners that share geopolitical or economical interests, for example, Turkey, Syria, Iran, and China. As long as ransomware syndicates comply with these rules, there is no incentive for Russian law enforcement to go after cybercriminals as they technically operate “outside” of the country's borders.

Moreover, Russia has no extradition treaty with the United States, while the two states face a lack of security cooperation driven by geopolitical issues that lead to disputes over extradition. It is not surprising, therefore that the representative states:

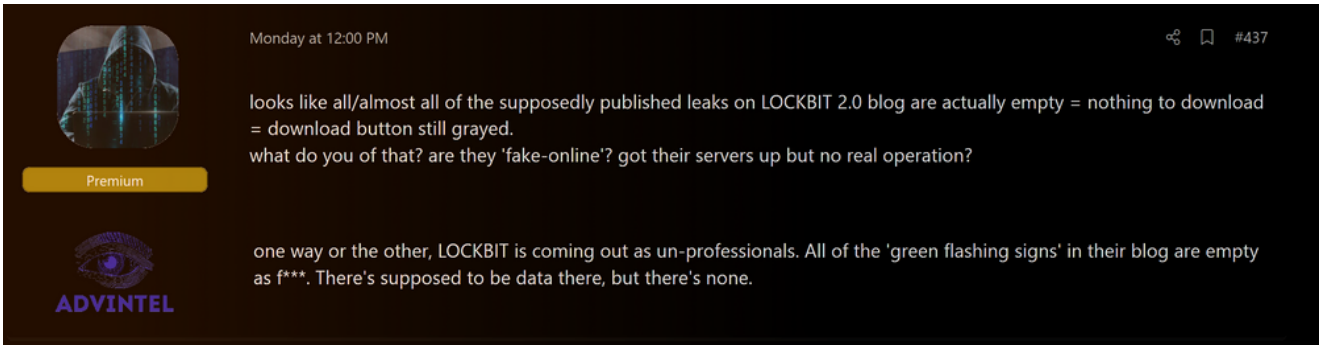
"We benefit from the hostile attitude of the West (towards Russia). It allows us to do conduct such an aggressive business and operate freely within the borders of the former Soviet (CIS) countries."

Despite the so-called freedom, the representative admits that their actions bring a lot of stress to their life. Indeed, from the outside ransomware business might look like a gangster action movie, the only difference being that in reality there is life and freedom at stake. *"I don't sleep very well at night"*, said the LockBit representative and they probably have a good reason to say so. The recent geopolitical events - most importantly the Russia-US summit have put ransomware into the spotlight. With the ongoing pressure from the President Biden administration against cyber threats originating from the region, the Russian underground has been experiencing waves of paranoia. The cybercriminal groups are attempting to keep a low profile in order to avoid a takedown by the Russian law enforcement - a takedown which the regime can use to bolster their negotiations with the US.

Conclusion

RaaS interviews became a normal practice for ransomware businesses to demonstrate their power to attract new affiliates and intimidate the public. The LockBit interview is unique as it has a clear political context that correlates with the Russian state narrative.

At the same time, these public interactions are most importantly an attempt to address the public trust crisis which RaaS is facing with their own affiliates - current or prospective. Exit scams and disappearances of large syndicates such as REvil, make LockBit one of the major players in the field and require the gang to provide a positive message.



A comment left by one of the cybercrime community members on the day of the interview publishing highlighting major flaws in LockBit's activities

Source: (Russian-language underground forums)

Despite a clear political statement involved, the whole spectacle probability originated as LockBit's attempt to reshuffle internal power struggles and improve the image within the underground community. An improvement that the group definitely requires.

Mitigations & Recommendations

- LockBit 2.0 is known for actively exploiting public-facing applications. Therefore monitoring endpoints should be the first mitigation strategy. The group specifically prefers the following infrastructural endpoints:
- Corporate VPN - especially Citrix/FortiNET
- Externally exposed RDPs
- As a top-tier ransomware group, LockBit likely investigates recent CVEs including ProxyLogon and Microsoft Exchange exposure. Monitoring exposed endpoints and application of CVE-addressing patches is required.
- LockBit prioritizes network investigation which enables them to steal sensitive data. Therefore, disrupting network movements via creating segregated segments of network, clear access hierarchy, and additional security for active directory, domain admin, and local domains can significantly complicate their operations.
- Multifactor authentication is required to protect employees' accounts from obtaining account credentials by actors that might be used to escalate privileges and move laterally within the network.
- It is suggested to perform daily backups and keep them offline to avoid data loss.

Translation and transcript of the full LockBit interview in English and Russian prepared by AdvIntel is available below:

AdvIntel-LockBit-Interview_Translation-&-Transcript

.pdf

Download PDF • 4.31MB

IoCs

File Hashes

Sha256 - 0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049

URLs

hxxp://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion

hxxp://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did[.]onion

hxxp://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid[.]onion

T1562.001: Impair defenses: disable or modify tools

T1070.001: Indicator removal on host: clear Windows Event Logs

T1041: Exfiltration Over C2 Channel

T1486: Data encrypted for impact

T1489: Service stop

T1490: Inhibit System Recovery