



| Flash |

LockBit Denies Attack Against Russian Entity

F-2024-01-30b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep & Dark Web, Threat Actors

January 30, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on January 29, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | LockBit Denies Attack Against Russian Entity

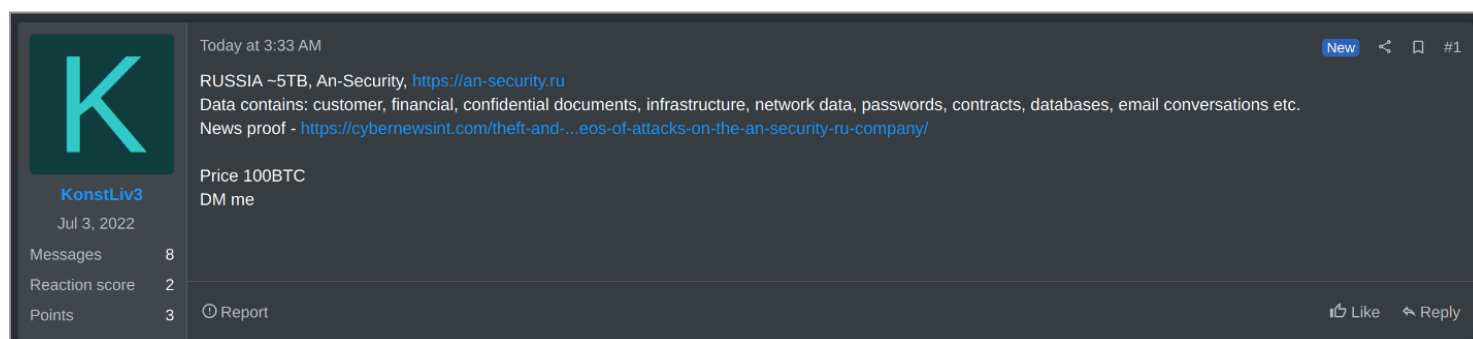
> Key Findings

- On January 22, 2024, threat actor “KonstLiv3” caused outrage in dark web community “RAMP” by claiming to have conducted a successful attack against a Russia-based organization using the LockBit malware strain—a claim that would violate the unwritten rules about using the strain to attack entities in Russia and other Commonwealth of Independent States (CIS) countries.
- On January 26, 2024, LockBit representatives made several posts in the forum, one of which claimed that the attack had been conducted by “Signature”—likely referring to a threat actor pseudonym. This was very likely an attempt to deny involvement, sanctioning, or knowledge of the attack.
- It is likely the attack took place, and threat actor KonstLiv3 is in possession of the stolen data. It is likely that a customized version of LockBit malware was leveraged.
- The negative community response to this event is almost certainly indicative of the extremely low tolerance within dark web forums for attacks against victims based in the CIS.
- The threat posed by LockBit, Clon, or the wider ransomware and digital extortion (R&DE) threat landscape to Western organizations is almost certainly unchanged.

Details

On January 26, 2024, LockBit representatives posted several statements in the predominantly Russian-speaking forum RAMP denying their involvement in an alleged extortion attack against the Russia-based security company “An-Security”—targeting that would violate the unwritten rules about using the strain to attack entities in Russia and other CIS countries. The denial followed claims made on January 22, 2024, by threat actor KonstLiv3, who allegedly used LockBit ransomware in the extortion.

- KonstLiv3, an actor with a positive—albeit limited—reputation in the forum, sought to sell digital property amounting to 5 TB of customer and financial documents, network infrastructure access data, employee passwords, contract information, email correspondence, and various databases.
- KonstLiv3 included an asking price of BTC 100, equivalent to approximately USD 3,951,000 at the time the post was published. Given the nature of both the stolen information and the target, this is almost certainly deliberately exorbitant.



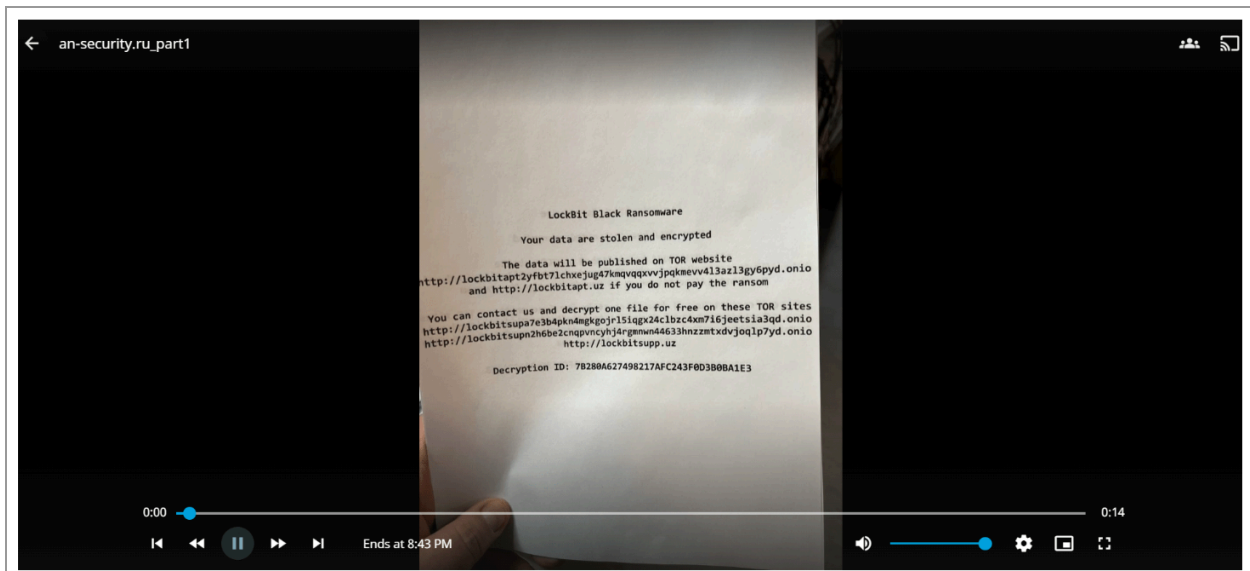
RAMP post advertising information stolen from “An-Security”

Source: ZeroFox Intelligence

The post included additional information intended to serve as proof the data has been obtained. This “News proof” consists of a URL directing to an information security magazine, which itself reported on the alleged attack. The magazine also provided screenshots of a video that suggests the prominent ransomware strain LockBit was leveraged in the attack.

- ZeroFox cannot confirm or deny the authenticity of this screenshot, where it occurred, or why the text is written in English rather than Russian.

- During extortion, LockBit typically conveys instructions to the victim electronically via the malware program.
- Using this link as “News proof” likely lowers the chance that the intent of the poster was a successful sale, as the unorthodox and low-quality approach would deter some interested buyers.
- A series of URLs pertaining to LockBit were present within both the post and the video screenshot. ZeroFox confirmed the authenticity of a link to a LockBit blog, while others such as Decryption ID URL—which promises to decrypt one stolen file for free—were confirmed invalid. Also, all are public data available via the open source.



Screenshot of a video containing a LockBit ransom note

Source:

[hXXps://cybernews\[.\]com/theft-and-disclosure-of-confidential-information-cybercriminals-share-videos-of-attacks-on-the-an-security-ru-company/](https://cybernews[.]com/theft-and-disclosure-of-confidential-information-cybercriminals-share-videos-of-attacks-on-the-an-security-ru-company/)

KonstLiv3’s post violates a widely-held understanding within Russian-speaking dark web communities that it is prohibited to target victims in the CIS. The post sparked an almost-immediate backlash, with well-regarded Russian-speaking actor “Bratislava” responding, “You crazy or what? CIS is forbidden.” KonstLiv3 was quickly banned by the RAMP moderator, and the post was locked (preventing a sale taking place).

- The CIS is an economic, political, and military intergovernmental organization that was formed in 1991 following the dissolution of the Soviet Union.

Konstliv3's post triggered widespread speculation in separate DDW forum xss about the RAMP post and the potential implication of LockBit. Bratislava asserted that the LockBit collective was not involved, suggesting instead that "kids" had used the LockBit "builder."

- Several months after its detection in June 2022, the source code of LockBit's most recent malware strain (LockBit 3.0) was widely reported to have leaked, allowing other threat actors to leverage their own, customized version of the malware.
- Although this gave rise to an increase in the use of LockBit 3.0, threat actors seeking to create their own version would need to possess a level of proficiency not dispersed amongst all extortion collectives.
- "Kids" likely refers to unknown actors that were able to leverage the leaked LockBit 3.0 source code.



Братислава
HDD-drive
Пользователь
Joined: Jul 24, 2023
Messages: 21
Reaction score: 10

Today at 9:57 AM

<http://rampjcdlqvkgkoz5oywutpo6ggl7g6tvddysustfl6qzhr5osr24xxqqd.onion/threads/russia-5tb-an-security-https-an-security-ru.1706/>

кажется это не **LockBitSupp** а может быть дети, которые используют биулдером локбита

Report



Братислава
Jul 27, 2023
Messages: 16
Reaction score: 18
Points: 3

Today at 8:35 AM

ты сумасшедший или что ?

СНГ запрещено
@vAz

Contant Tox: 5700F2F2B10F590AAEEEE1C6FA0410CA40A6CD08852B7A1FA26A37A6A06E1A40C6AAB43B8AD0D

"Они меня называют теперь сумасшедшим"

Report

Like Reply

Posted URLs allegedly pertaining to LockBit infrastructure

Source: ZeroFox Intelligence

LockBit's series of denial posts is very likely reflective of the gravity of the claims and the concern the group has for its potential implication in the attack. LockBit stated that the attack had leveraged malware based upon the leaked (LockBit) builder and accused

Signature—likely a threat actor pseudonym—of conducting the attack. LockBit further claimed that Signature is the “owner of the Clop affiliate programme” and offered a reward of USD 10,000,000 for information helping to identify the accused.

- ZeroFox cannot confirm if Signature is associated with the Clop extortion collective, and the reasoning behind LockBit’s accusation is unknown.
- The offering of such a large reward is very likely intended to serve as commitment to uncovering the attacker’s identity and to absolve LockBit of responsibility.

Another post from a LockBit representative alluded to a note allegedly received from an employee of the victim company, confirming contact between the two parties.

- The intent, channels, or reasoning behind these communications is unknown, but there is a roughly even chance that LockBit had intended to discover information that would aid in identifying the attacker.
- It is unknown whether LockBit intended or was able to return the victims’ stolen data.

It is likely the attack took place, and threat actor KonstLiv3 is in possession of the stolen data. It is likely that LockBit malware was used by a threat actor able to leverage it against a Russia-based target—almost certainly violating any terms of use associated with LockBit malware.

- The attack was very likely conducted in this fashion to discredit the LockBit collective, either to satisfy a personal rivalry between extortion operatives or to exploit the general paranoia present amongst cybercriminals to sow confusion.
- It is unlikely to have been conducted knowingly by an established LockBit affiliate, as posting such an attack in RAMP—and at such an exorbitant price—would have either been a significant misjudgment by an inexperienced threat actor or indicative of very little intent to conduct a successful sale. LockBit generally does not advertise the sale of its stolen data in DDW forums.
- ZeroFox notes the unlikely possibility that the attack did not take place; the sale was illegitimate; and the post was an attempt to sow confusion, conduct general trolling activity, or carry out a financial scam. The exorbitant asking price would likely be an attempt to increase perceived authenticity for an actor with a limited reputation.

This event is reflective of the dynamic and likely paranoid environment found in DDW forums fueled by ongoing law enforcement evasion, the internal politics of threat collectives and their affiliates, and the ever-changing norms to which participants must abide in the pursuit and retention of a credible reputation that aids in lucrative sales. The quick banning of KonstLiv3 from RAMP and the prevention of the sale reinforces the low tolerance for targeting of CIS-based organizations amongst Russian-speaking threat actor forums.

The threat posed by LockBit, Clop, or the wider R&DE threat landscape to Western organizations is almost certainly unchanged. LockBit, which conducted more attacks in Q4 2023 than any other quarter observed by ZeroFox, will continue to primarily target organizations based in North America and Europe, with particular emphasis on those in the manufacturing, retail, and construction sectors.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%