



| Flash |

LockBit & ALPHV Activity Likely Consistent with Exit Scams

F-2024-03-04a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep and Dark Web

March 4, 2023

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 March 4, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | LockBit & ALPHV Activity Likely Consistent with Exit Scams

› Key Findings

- As of March 4, 2024, operators behind both the LockBit and ALPHV ransomware and digital extortion (R&DE) operations are exhibiting behavior likely consistent with imminent exit scams against their affiliates.
- Both operations have claimed to be continuing operations following recent law enforcement (LE) activities, consistently downplaying the impact of disruptive action despite a significant reduction in observed activity.
- While ZeroFox can neither confirm nor deny the veracity of claims of scamming made by alleged LockBit and ALPHV affiliates, similar activity has been conducted by other notable ransomware collectives in the days preceding the cessation of their operations.
- Victims of outstanding or ongoing extortion attacks by LockBit and ALPHV are unlikely able to assume their stolen data will be deleted following payment of ransom demands. Regardless of whether they choose to pay ransom demands, victims are at an increased risk of stolen data not being deleted and, instead, sold on the deep and dark web (DDW) to the highest bidders.

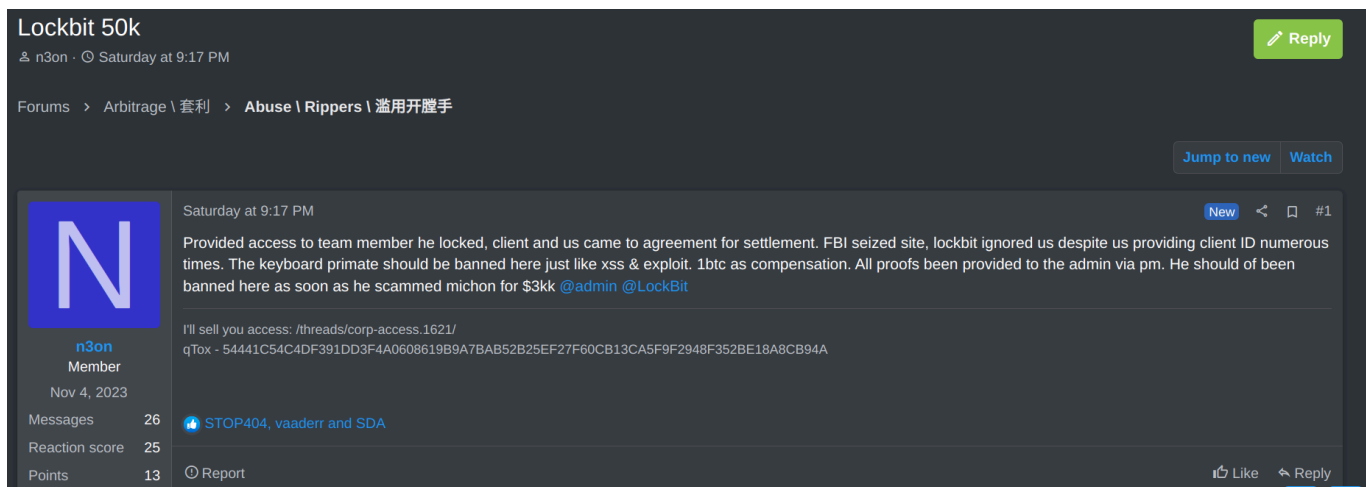
| Details

As of March 4, 2024, the operators behind both the LockBit and ALPHV R&DE operations are exhibiting behavior likely consistent with imminent exit scams against their affiliates. Since March 2, 2024, at least three separate scam allegations have been raised against the LockBit and ALPHV operations by supposed affiliates.

- These scams occur when operators become increasingly non-communicative with affiliates, ignore them altogether, or otherwise kick them out of programs without paying affiliates for successful extortions. The leadership seeks to make maximum profit out of the remaining extortion campaigns by taking the affiliates' pre-agreed-to cuts of the ransoms for themselves.
- These scams effectively terminate the relationships between core Ransomware-as-a-service (RaaS) operatives and their affiliates and damage the operations' reputations in threat actor communities irrevocably.
- ZeroFox has identified no conclusive evidence to suggest that the alleged scamming actions taken by LockBit and ALPHV are coordinated.

On March 2, 2024, well-regarded access broker and ransomware affiliate "n3on" claimed on the dark web forum RAMP that they were being ghosted (ignored) by LockBit's operators, who had refused to pay the affiliate for successfully targeting an unspecified victim.

- Claims of LockBit operators scamming affiliates have been identified on Russian-speaking DDW communities as early as January 2024.
- N3on directly attacked the admin of RAMP—another well-known and highly-regarded access broker operating under the name "Stallman"—for not banning LockBit as soon as the first scam scandal involving them was identified. Other administrators of dark web forums, including xss and Exploit, have since banned LockBit.
- Other English-speaking RAMP members were quick to support n3on's position, including "SDA", an actor who alleged to have worked with n3on.



RAMP post by “n3on” claiming LockBit is no longer cooperative

Source: ZeroFox Intelligence

Also on March 4, 2024, Russian-speaking LockBit affiliate “STOP404” announced on RAMP that they have been ghosted by LockBit, which had refused to make their payment.

- STOP404 claimed that LockBit had not communicated with the guarantor (escrow) associated with the agreed-to extortion service.
- The actor also accused LockBit of becoming a “FSB project”—the Federal Security Service of the Russian Federation—asserting that “the criminal world declares war on the garbage project.”
- Both of these allegations support the assessment that LockBit’s reputation within DDW marketplaces and amongst its affiliates has been irreparably damaged in recent weeks.

On March 3, 2024, RAMP member “notchy”, a self-proclaimed long-standing ALPHV affiliate, claimed in a post to the community that the gang’s leadership has recently scammed them out of a USD 20 million ransom payment made by OPTUM, a U.S.-based healthcare services provider.

- Notchy claims that OPTUM made the payment to ALPHV’s “management” team, yet—despite the fact notchy conducted the attack and the negotiations—they were not paid.

- Notchy posted a screenshot of alleged correspondence with ALPHV's administrator, indicating they were being ignored by the group's leadership.
- ZeroFox can neither confirm nor deny that OPTUM paid the ransom as alleged; however, notchy claimed that the victim's data remains on ALPHV's leak site and listed potential OPTUM partners that could be implicated in the alleged breach.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

AND more!

PROOF of ALPHV scam:

Notchy's post listing potential OPTUM partners implicated in the alleged breach

Source: ZeroFox Intelligence

Both LockBit and ALPHV have claimed to be continuing operations following LE activities and consistently downplayed the impact of disruptive action, despite a significant reduction in observed activity. This is very likely an attempt to preserve their reputations, ensure affiliates continue their ongoing efforts, and encourage victims in the extortion stage of attacks to meet ransom demands.

- As recently as February 29, 2024, LockBit administrators remained committed to projecting the appearance of a fully-functioning and resilient R&DE operation. Following Operation Cronos—a coordinated effort by multiple LE agencies to seize aspects of LockBit's infrastructure—much of LockBit's immediate operational capability was disrupted, and its reputation was severely damaged in DDW communities.
- Similarly, ALPHV has attempted to outwardly project the appearance of a resilient R&DE operation in 2024, listing alleged new victims on its leak site. This followed a December 2023 disruption by an international LE operation that resulted in the

alleged seizure of the collective's victim leak site and the production of a decryption tool that alleviated ransom demands amounting to approximately USD 68 million.¹

While ZeroFox can neither confirm nor deny the veracity of claims made by these affiliates, similar activity has been conducted by other notable ransomware collectives in the days preceding the cessation of their operations.

- RaaS operation NoESCAPE, which was first observed in Q2 2023 and went on to conduct a significant number of extortion attacks, reportedly stole deposits and payouts from several affiliates during an exit scam. This resulted in its banning from several prominent DDW forums, including xss and Exploit.
- Similar activities were conducted by REvil, a ransomware operation that was highly active until its disappearance in Q2 2021. Following numerous highly-lucrative extortion attacks, the collective reportedly ceased contact with its affiliates and retained their deposits.

Victims of outstanding or ongoing extortion attacks by LockBit and ALPHV are unlikely able to assume their stolen data will be deleted following payment of ransom demands. Victims are at an increased risk of stolen data not being deleted and, instead, sold on the DDW to the highest bidders.

- If their activity is indeed part of an exit scam, LockBit and ALPHV operators no longer need to adhere to the ordinary rules of R&DE operations, whereby paid ransoms result in threat actors deleting the data. Instead, the groups will likely obtain payment from victims and then sell the data to bidders on the DDW.
- If affiliates are in possession of stolen victim data—rather than the groups' core members—there is a roughly even chance that affiliates will seek to sell it in DDW forums in an attempt to recuperate losses incurred from LockBit's failure to make pre-agreed-to payments to them.

The developing situations with LockBit and ALPHV will very likely drive significant changes to the R&DE threat landscape in the first half of 2024.

¹ [hXXps://www.justice\[.\]gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant](https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant)

- Disruptive LE activity has likely either been sufficiently successful to drive LockBit and ALPHV to conduct exit scams ahead of cessation of their activities or ignited sufficient internal turmoil such that normal operations between affiliates and the core group have broken down in certain cases.
- Regardless, the relationship between these groups and their affiliates have likely been irrevocably damaged, alongside the groups' brands.
- The discord surrounding and within the groups' operations is likely to incentivize other collectives to expand their operations and compete for former resources, including affiliates, pentesters, and brokers.

Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of R&DE threats and associated tactics, techniques, and procedures (TTPs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%