



| Flash |

ALPHV Ransomware and Digital Extortion Operations Disrupted

F-2023-12-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Groups, Ransomware, Deep and Dark Web

December 19, 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 10:00 AM (EST) on December 19, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | ALPHV Ransomware and Digital Extortion Operations Disrupted

› Key Findings

- The victim leak site associated with Ransomware and Digital Extortion (R&DE) collective ALPHV has been seized by the Federal Bureau of Investigation (FBI) in a takedown operation that involved law enforcement (LE) agencies from the United Kingdom, Denmark, Germany, Spain, and Australia.
- ALPHV has publicly downplayed the significance of the operation, claiming the seized infrastructure is not used and is outdated.
- This latest takedown operation follows numerous incidents of ALPHV victim site disruption in December 2023, which has very likely contributed to the significantly reduced attack tempo observed by ZeroFox and the pivoting of affiliates toward other Ransomware-as-a-Service (RaaS) offerings.

Details

A victim leak site associated with R&DE collective ALPHV has been seized by the FBI in a takedown operation that involved LE agencies from the United Kingdom, Denmark, Germany, Spain, and Australia. On December 19, 2023, the FBI confirmed its disruption campaign against the ALPHV collective (also known as Blackcat). The takedown operation was aided by a decryption tool that enabled the recovery of stolen data

belonging to hundreds of victims, alleviating ransom demands totaling approximately USD 68 million.¹

- A search warrant unsealed today in the Southern District of Florida provided LE with visibility into ALPHV's computer networks, resulting in the seizure of several associated websites.²
- One seized website is ALPHV's previous leak site, where the details and data belonging to victim organizations would be published.³ This seizure follows previously observed periods of downtime on ALPHV's blog and Tor-based leak site, which the group claimed was due to repairs being made to its servers.⁴



Notice of seizure placed on ALPHV leak site (Dec. 19, 2023)

Source: ZeroFox Intelligence

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)

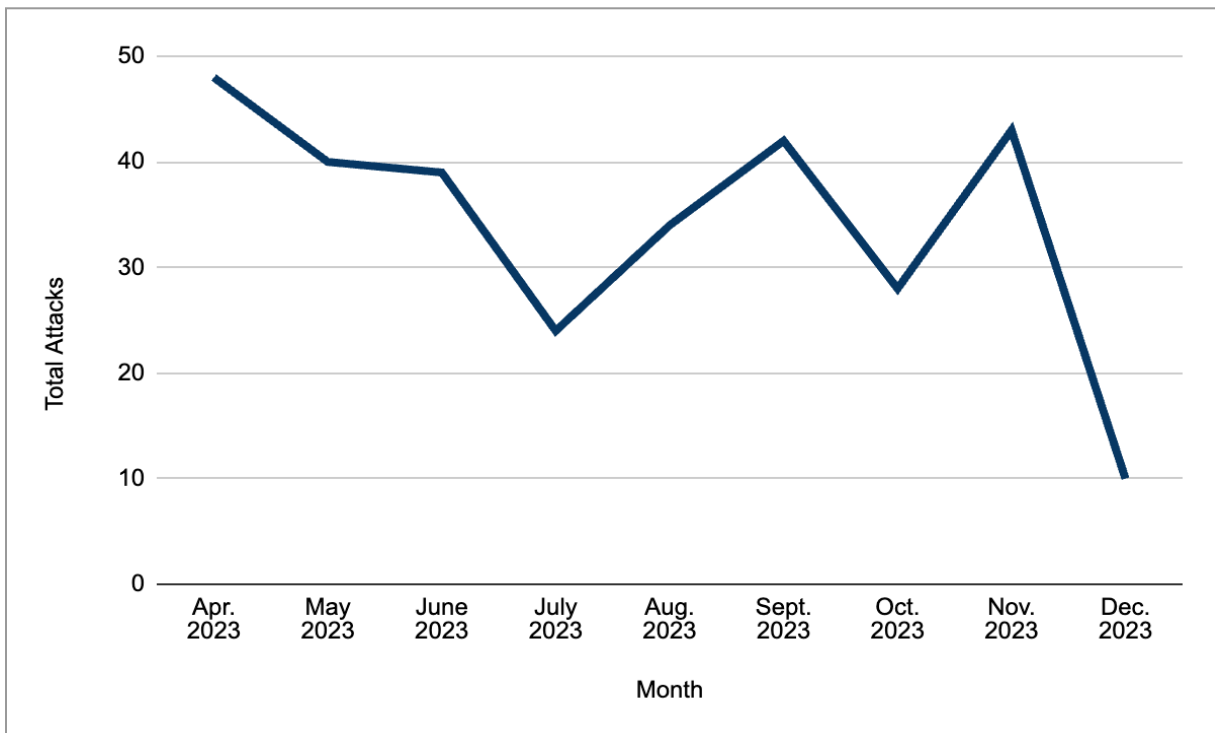
² [hXXps://www.documentcloud\[.\]org/documents/24231386-blackcat-alphv-search-warrant](https://www.documentcloud[.]org/documents/24231386-blackcat-alphv-search-warrant)

³ [hXXps://twitter\[.\]com/vxunderground/status/1737086959325983036](https://twitter[.]com/vxunderground/status/1737086959325983036)

⁴ ZeroFox Internal Collections

ALPHV has downplayed the significance of this LE activity, stating that the obtained encryption key has been replaced and new leak sites are already operational.⁵ On December 19, 2023, ZeroFox observed the addition of two separate victims to ALPHV's leak site.⁶

ZeroFox has previously reported a downward trajectory in ALPHV activity. Despite conducting more attacks during 2023 than in 2022, affiliates' activity has been decreasing since the end of Q2—both in the total number of attacks and as a proportion of all R&DE activity across the threat landscape.⁷ This is likely attributable, to some extent, to ongoing LE disruption of the group's critical infrastructure, as well as the degrading of stature and trust amongst affiliates.



Total ALPHV attacks (Q2 2023 - Q4 2023)

Source: ZeroFox Intelligence

⁵ [hXXps://twitter\[.\]com/vxunderground/status/1737091053218414592](https://twitter.com/vxunderground/status/1737091053218414592)

⁶ ZeroFox Internal Collections

⁷ ZeroFox Internal Collections

Affiliates leveraging ALPHV ransomware are likely to have been increasingly pivoting toward other RaaS offerings, such as the host of newer collectives observed since Q2 2023 that have been demonstrating fast proficiency. There is a roughly even chance that some of these groups offer more favorable terms of use or a higher percentage payout rate following successful extortion, as well as less risk of disruption by LE entities.

- It is also very likely that prominent R&DE collective LockBit, which previously stated that affiliates may transfer ongoing victim negotiations to their infrastructure, has attempted to recruit affiliates that are discontented.⁸

Ongoing disruption and the departure of affiliates are likely to heavily hinder ALPHV operations in the coming weeks, resulting in a reduced attack tempo. There is a roughly even chance that this will slightly reduce overall activity observed across the R&DE threat landscape, though any such reductions are likely to be temporary and due to opportunistic affiliates establishing themselves with other RaaS offerings.

ALPHV's claims to have sufficient operational contingency to withstand current disruptions are likely overplayed to some extent in an attempt to maintain credibility and retain affiliates. While there is a roughly even chance that ALPHV affiliates will continue to conduct attacks, the collective is likely to remain less prominent moving into 2024.

Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of R&DE threats; their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).
- 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.

⁸ [hXXps://twitter\[.\]com/g0njxa/status/1734510597201404361](https://twitter.com/g0njxa/status/1734510597201404361)

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- 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 system, and ensure all business IT assets are updated with the latest software as quickly as possible.

| 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%