



| Flash |

ALPHV Extortion Campaigns Continue into 2024

F-2024-02-16a

Classification: TLP:CLEAR

Criticality: Medium

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

February 16, 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 9:00 AM (EST) on February 16, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | ALPHV Extortion Campaigns Continue into 2024

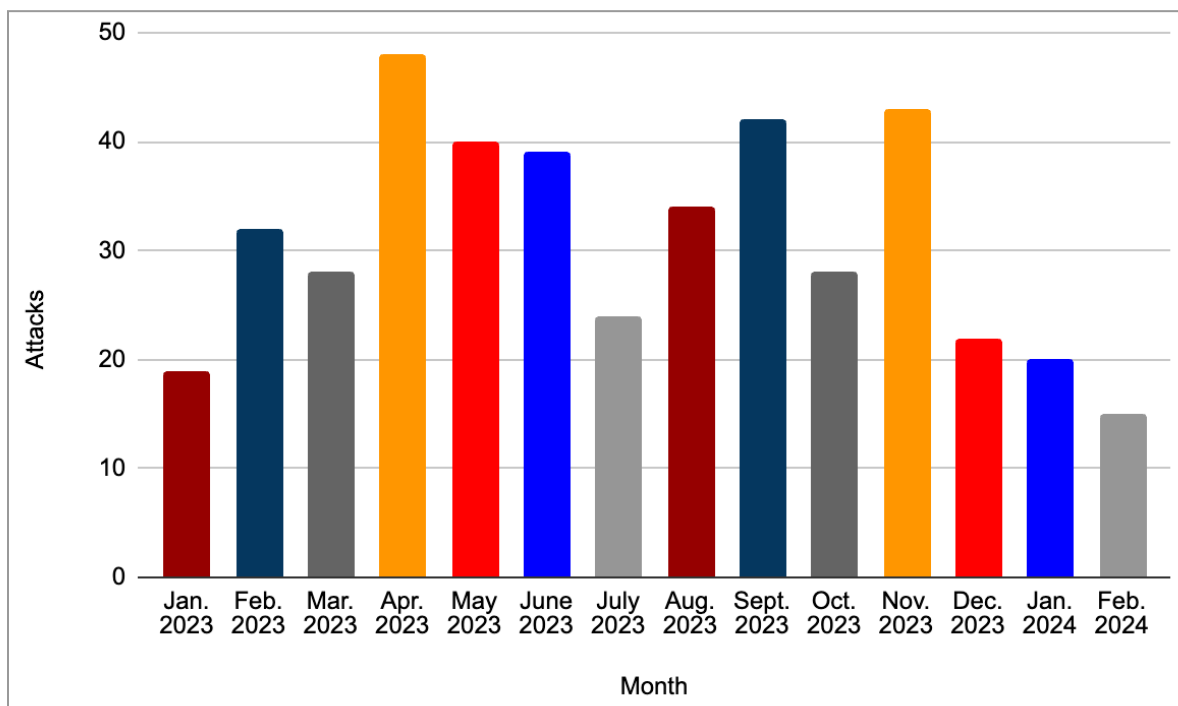
› Key Findings

- Ransomware and digital extortion (R&DE) collective ALPHV is continuing extortion campaigns in 2024, with its attack tempo very likely back on an upward trajectory following a recent disruption.
- Since the law enforcement (LE) activity reported by ZeroFox on December 19, 2023, the proportion of ALPHV attacks targeting entities based in North America has increased significantly—from a 2023 average of approximately 59 percent up to 85 percent.
- It is likely that the specific targeting of North America, as well as the increasing attack tempo, contributed to the U.S. Department of State offering a series of financial rewards for related information on February 15, 2024.
- ALPHV attacks are very likely to continue over the next two months, targeting mostly North America-based organizations. There is a roughly even chance that the current upward trajectory in activity will plateau or decline as a result of continued LE attention and scrutiny.

Details

R&DE threat collective ALPHV (also known as BlackCat and Noberus) is continuing to conduct activity in 2024, with its attack tempo having very likely returned to an upward trajectory following significant recent disruption to its operations.

- On December 19, 2023, ZeroFox reported the seizure of ALPHV's victim leak site, as well as other digital infrastructure, by several LE entities, including the Federal Bureau of Investigations (FBI) and agencies from the United Kingdom, Denmark, Germany, Spain, and Australia.
- 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
- The disruption resulted in a significant decrease in ALPHV attacks, which reduced to an average of 21 attacks per month in December 2023 and January 2024 from an average of 34 per month between January and November 2023.²



ALPHV attacks by month, Jan. 2023 – Feb. 2024

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)

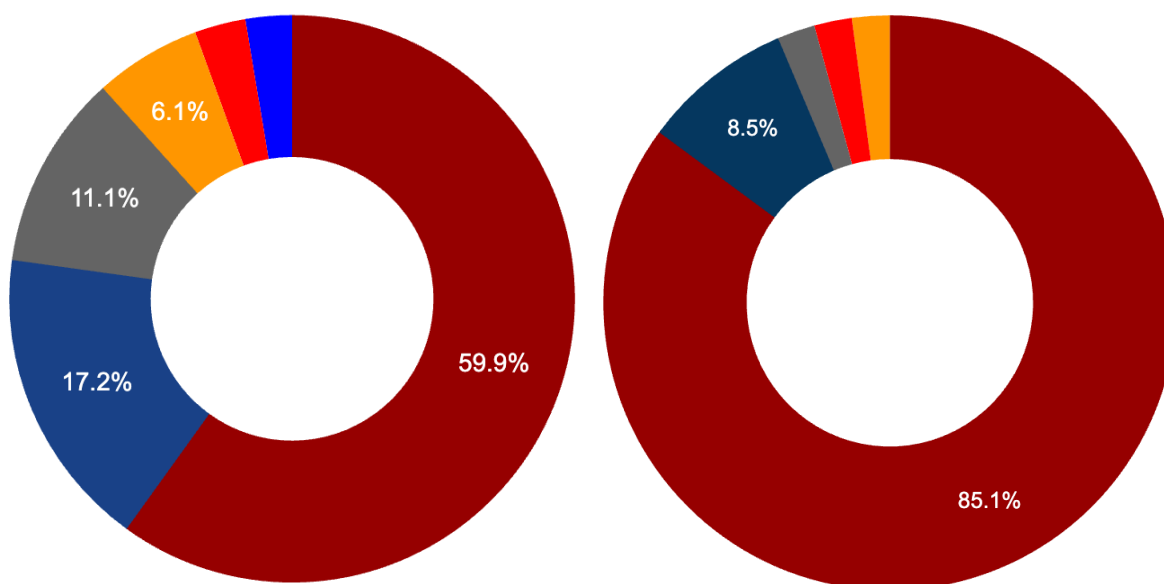
² ZeroFox Intelligence

While this disruption was almost certainly detrimental to ALPHV's operations in the immediate near term, the group has not gone longer than seven days without conducting an attack. This is very likely indicative of the group's longevity, as well as its continued possession of the expertise, affiliates, and digital infrastructure needed to conduct R&DE attacks.

- ALPHV downplayed the significance of December's LE disruption, stating that the seized leak site was old and that a new one was already operational. ZeroFox observed the addition of two separate victims to the leak site very soon after on December 19, 2023.

With 15 attacks having taken place so far in February, the group is on track to exceed the numbers seen in both December and January. This is likely an indication of recovery and the retaining of affiliates. However, It is very unlikely that Q1 2024 attack levels will return to the averages experienced throughout 2023.

● North America ● Europe ● APAC ● Middle East & Africa ● South America ● ANZAC



Proportion of ALPHV attacks by region, before and after December LE disruption

Source: ZeroFox Intelligence

Since December 19, 2023, the proportion of ALPHV attacks targeting entities based in North America has increased significantly from a 2023 average of approximately 59 percent up to 85 percent. This is very likely due to resource limitations imposed by a lack of infrastructure and affiliates, leading to the prioritization of lucrative targets—many of which are likely in the United States and Canada. It is also likely that many of these attacks are targeting networks for which initial access has been previously obtained—either through deep and dark web (DDW) brokering or the discovery of unpatched software vulnerabilities—or organizations that were already being extorted prior to LE disruption.

It is likely that the specific targeting of North America, as well as the increasing attack tempo, contributed to the U.S. Department of State offering a series of financial rewards on February 15, 2024. Users wishing to contribute information are directed to a Tor-based, [.]onion tip line.

- Up to USD 10 million is being offered for information leading to the identification or location of anyone who holds a key leadership position within the group.
- Up to USD 5 million is being offered for information leading to the arrest or conviction of anyone participating in or conspiring or attempting to participate in a ransomware attack using the ALPHV/Blackcat variant.³
- The use of a [.]onion tip line is very likely indicative of the reward being directed toward those already in proximity to DDW forums associated with the cyber threat landscape. The anonymity offered to users visiting the tip line is not specified, but it is likely high.

3

[hXXps://www.state\[.\]gov/u-s-department-of-state-announces-reward-offers-for-criminal-associates-of-the-alphv-blackcat-ransomware-variant/](https://www.state.gov/u-s-department-of-state-announces-reward-offers-for-criminal-associates-of-the-alphv-blackcat-ransomware-variant/)



U.S. Department of State reward information

Source:

[hXXps://www.state\[.\]gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/](https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/)

The offering of a large reward is likely to impact ALPHV's resurgence to 2023-level operational tempos. Some would-be affiliates seeking a Ransomware-as-a-Service (RaaS) project with which to associate will likely be dissuaded, and senior members of the collective will likely place increased emphasis on security and inconspicuous activities rather than high-profile R&DE attacks.

ALPHV attacks are very likely to continue over the next two months, targeting mostly North America-based organizations. There is a roughly even chance that the current upward trajectory in activity will plateau or decline as a result of continued LE attention and scrutiny.

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.
- 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%