ZEROFOX Intelligence

Flash

ALPHV and NoEscape Disrupted, Affiliates Likely Pivoting to Alternative Operations

F-2023-12-14b

Classification: TLP:CLEAR

Criticality: Medium

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

December 14, 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 11:00 AM (EST) on December 14, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | ALPHV and NoEscape Disrupted, Affiliates Likely Pivoting to Alternative Operations

› Key Findings

- Disruption to the operations of prolific ransomware & digital extortion (R&DE) collectives ALPHV (aka BlackCat) and NoEscape will likely drive former affiliates to pivot to other R&DE offerings.
- Disruption to ALPHV's operation has most likely been caused by a currently-undisclosed law enforcement operation against the cartel. NoEscape operators have reportedly conducted an exit scam, stealing ransom payments and closing down the group's web panels and data leak sites.
- If affiliates and R&DE collective operators are unable to continue deploying these strains, they will very likely pivot to other well-known R&DE offerings or rebrand and launch their own extortion operations.

| Details

Disruption to the operations of prolific R&DE collectives ALPHV (aka BlackCat) and NoEscape will very likely drive former affiliates to pivot to other R&DE offerings. Other R&DE collectives, such as LockBit, are likely actively seeking to capitalize on the disruption to these two collectives' extortion operations by recruiting their highly-capable former affiliates—a common practice by such groups.

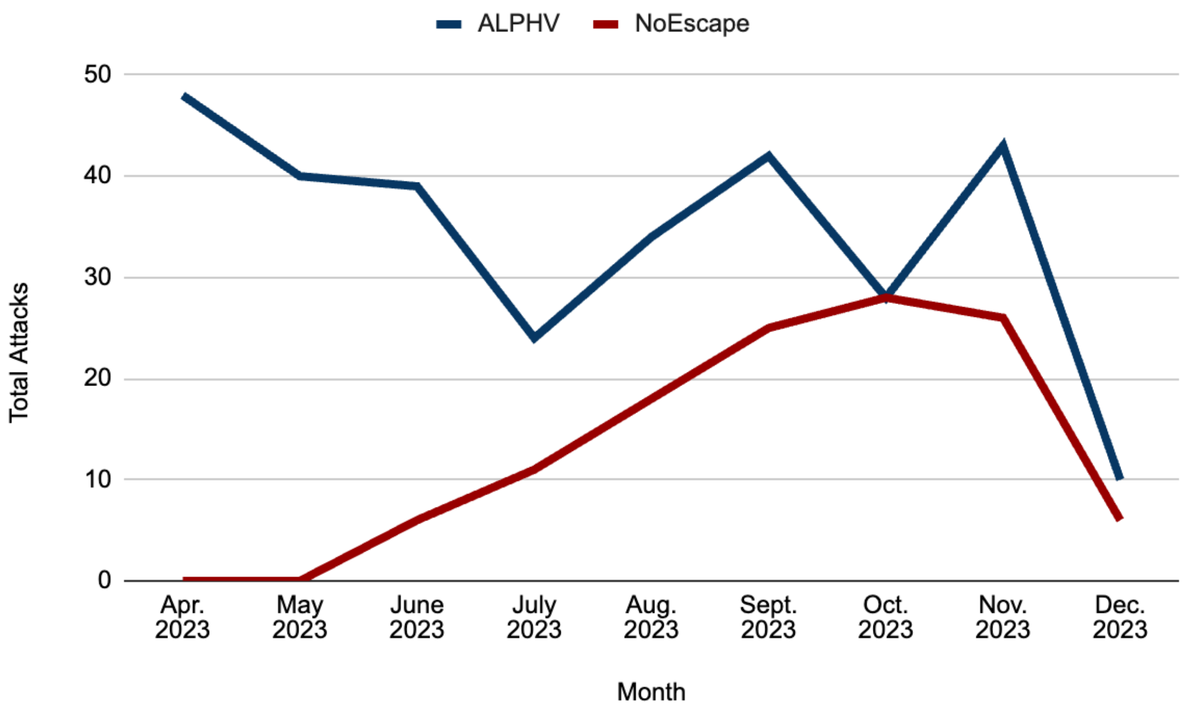
- Since as early as December 7, 2023, ALPHV's blog and Tor-based leak site have experienced long periods of downtime, with negotiation channels very likely to have been impacted. While the cause of the outage is currently unknown, speculation is widespread within deep and dark web communities (DDW), as well as in other open sources.

Despite ALPHV's public claim that the outage was due to repairs being made to its servers, the most likely cause of this outage is a currently-undisclosed law enforcement operation against the cartel, judging from credible DDW sources.

- Similar impacts have been observed prior to disclosure of authorities' takedowns and seizing of REvil and Hive's infrastructure.

- Additionally, NoEscape's Tor website was taken offline recently; affiliates have alleged that its operators conducted an exit scam, stealing ransom payments and closing down the group's web panels and data leak sites.

ALPHV has been one of the most prominent R&DE threats to the majority of industries globally over the last two years, and NoEscape has been one of the most prolific strains in recent months. Prior to the disruption to operations outlined in this report, ZeroFox had observed significant declines in ALPHV and NoEscape activity in recent weeks.



Total ALPHV and NoEscape R&DE Attacks: April 2023 - Present

Source: ZeroFox Collections

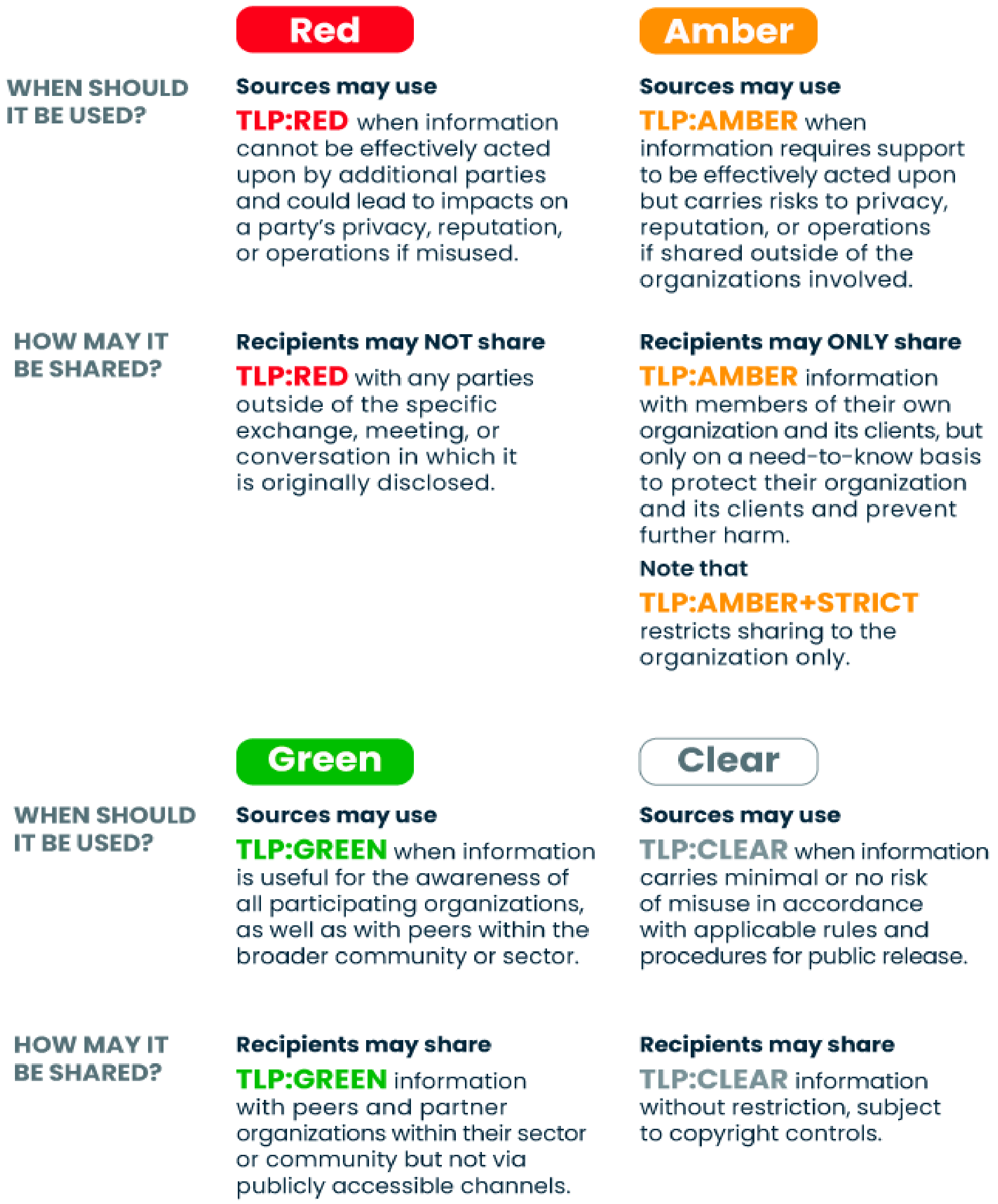
Disruption to these R&DE collectives' operations will very likely result in an only-temporary suppression of the threat from its operatives. If unable to continue deploying the strains, affiliates will very likely:

- Quickly pivot to other well-known R&DE offerings and continue targeting victims at scale and at pace.
- Rebrand and launch their own extortion operations; ALPHV affiliates have a history of rebranding, with the operation stemming from the DarkSide and BlackMatter extortion operations.

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 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

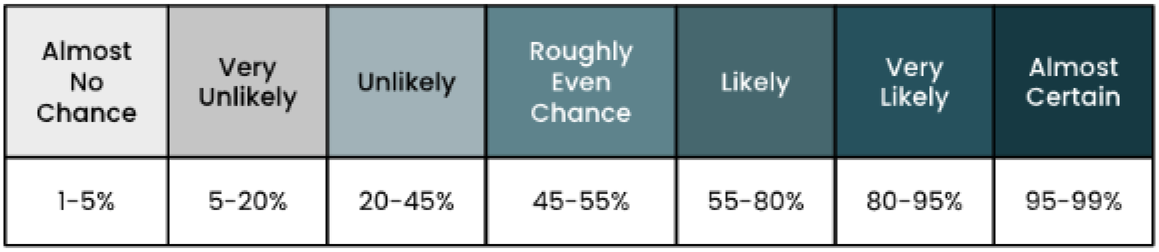


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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%