



| Flash |

Ransomware and Digital Extortion Landscape Diversifying

F-2023-11-09a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Deep & Dark Web

November 09, 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 November 09, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Ransomware and Digital Extortion Landscape Diversifying

› Key Findings

- The operational tempo of ransomware and digital extortion (R&DE) collectives LockBit and ALPHV is steadily decreasing, both in the number of observed incidents and as a proportion of all R&DE activity.
- Since at least Q2 2023, several newly-observed R&DE threat collectives have conducted increasingly frequent attacks. Some of these are likely rebrands of established threat collectives and others former affiliates of LockBit and ALPHV launching their own operations.
- New threat collectives are demonstrating proficiency at a faster pace than previously observed and are more than offsetting the decline in LockBit and ALPHV activity. This will likely drive significant change across the R&DE threat landscape in coming quarters.

| Details

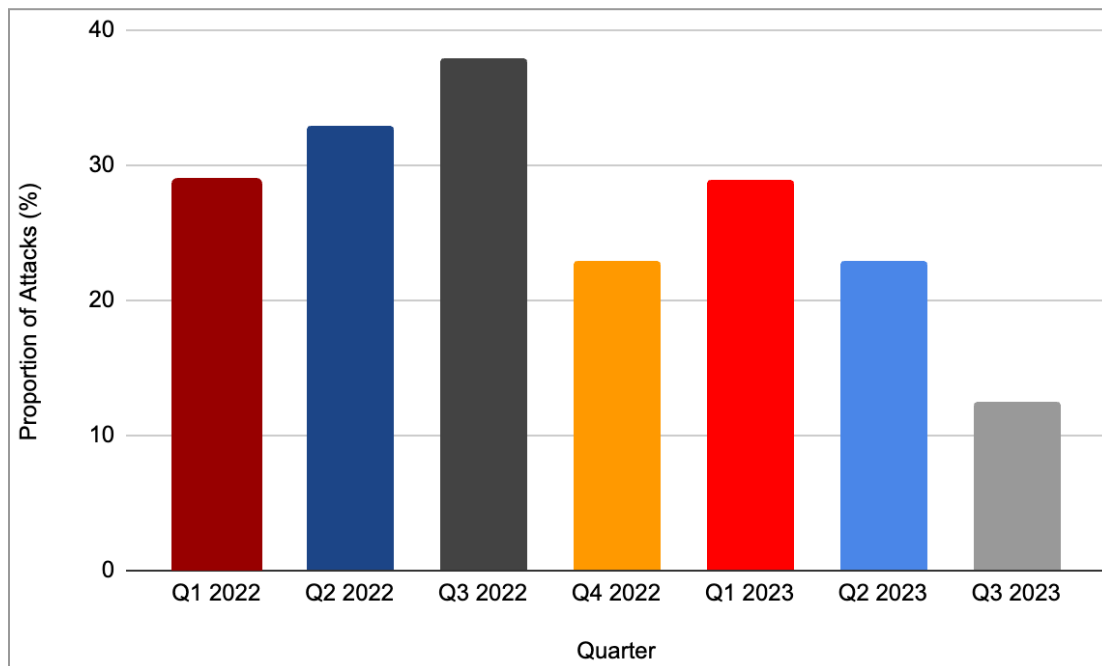
R&DE collectives LockBit and ALPHV are on a downward trajectory—both in the number of observed incidents and as a proportion of all R&DE activity. This is despite ZeroFox Intelligence observing more R&DE incidents during Q3 2023 than any other quarter to

date. This upward trajectory in R&DE incidents is likely to continue through Q4 2023, though LockBit and ALPHV's contributions will likely become less significant.

Since its inception in late 2019, LockBit has been a prominent R&DE and Ransomware-as-a-Service (RaaS) collective and has been responsible for more incidents during 18 of the past 22 months than any other group, often by a significant margin. This activity endures across all geographic regions and industries, including manufacturing, financial services, defense, construction, healthcare, and legal consultation services.

- The months in this time period in which LockBit has not been the most prominent collective have mostly been dominated by over 300 highly-successful Cl0p campaigns.

Threat collective ALPHV—also known as BlackCat—has been the second-most prominent R&DE collective since January 2021, targeting primarily the manufacturing and financial sectors in North America and the Asia-Pacific. ALPHV conducted approximately 10 percent of all R&DE attacks during this timeframe, but its activity is also on a downward trajectory.



LockBit Attacks as a Proportion of Total R&DE Activity

Source: ZeroFox Intelligence

The reduction in LockBit and ALPLV attacks is almost certainly the result of a broad and somewhat inevitable confluence of factors occurring in deep and dark web marketplaces and across the threat landscape. Opportunistic affiliates of these groups are likely increasingly opting to leverage other, newer ransomware services that may offer more favorable terms of use, improved attack flexibility, or a higher percentage payout rate following successful extortion.

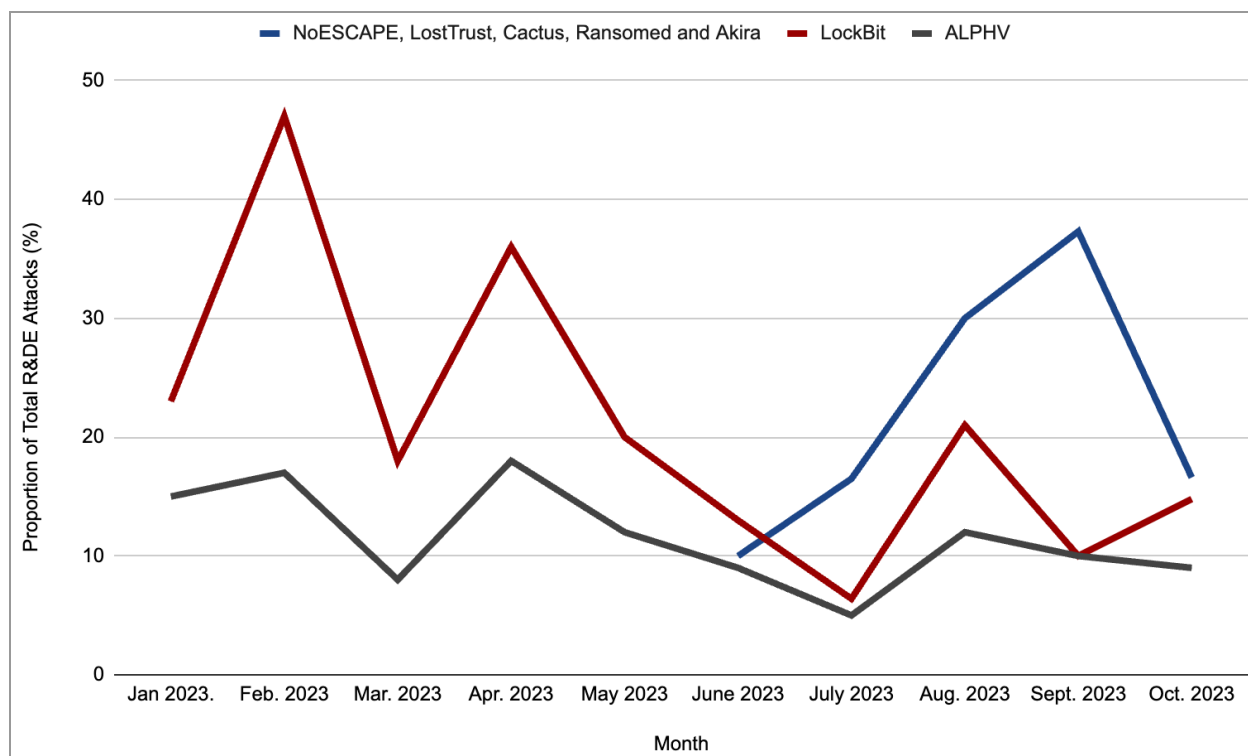
- This follows a previously-observed pattern of prominent R&DE collectives significantly reducing their attack frequency within a time period of approximately two years following their initial surfacing.

The significant increase of newer, highly-active collectives—most of which surfaced during Q2 2023—is contributing to LockBit and ALPHV attacks reducing as a proportion of total observed R&DE activity. Among these are NoESCAPE, Lost Trust, Cactus, Ransomed, and Akira, which collectively have accounted for approximately one in four incidents since the start of Q3 2023.

- Of these, Lost Trust—a likely rebrand of notorious ransomware collective MetaEncryptor—has been the most prolific, conducting more attacks than LockBit in September 2023.

Although the majority of newer groups are likely reboots of previously-established threat collectives, the increase in the proportion of attributed attacks is very likely indicative of the growing ease with which collectives can establish proficiency and begin conducting attacks against sophisticated targets. The proliferation of off-the-shelf tools, such as various as-a-service offerings, is likely a key reason for this.

- These tools lower entry barriers to would-be threat actors who may otherwise lack the resources or expertise to conduct sophisticated R&DE attacks.



Proportion of R&DE Attacks by Threat Group

Source: ZeroFox Intelligence

Recommendations

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of R&DE threats and 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.
- 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.

- 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%