



| Flash |

LockBit Ends 2023 with Record Number of Attacks

F-2024-01-09a

Classification: TLP:CLEAR

Criticality: Medium

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

January 9, 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 10:00 AM (EST) on January 9, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | LockBit Ends 2023 with Record Number of Attacks

› Key Findings

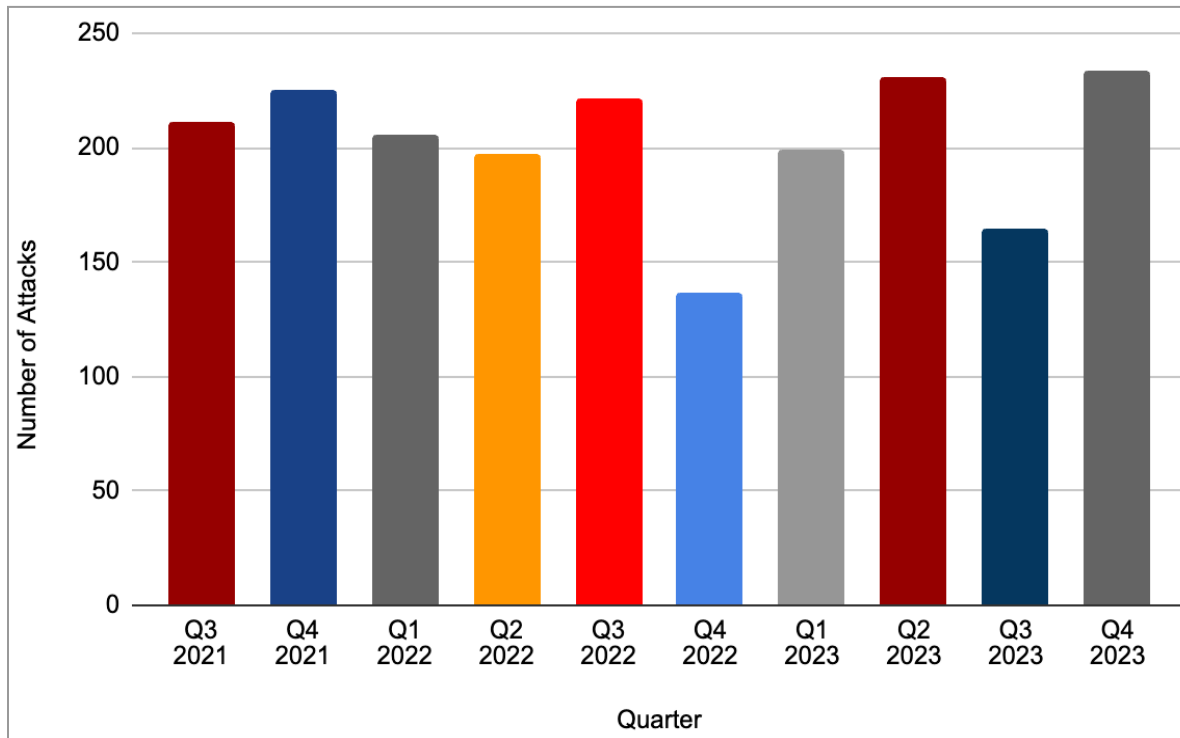
- Ransomware & Digital Extortion (R&DE) threat collective LockBit conducted more attacks during Q4 2023 (October–December) than in any other quarter, despite their activity accounting for a significantly reduced proportion of the wider threat landscape’s activity.
- It is almost certain that LockBit is benefitting from the December disruption of other R&DE collectives—particularly through procuring affiliates from ALPHV and NoEscape.
- A greater proportion of LockBit’s attacks were leveraged against the manufacturing and retail industries in Q4 2023, both of which are above the threat landscape average.

| Details

R&DE threat collective LockBit conducted at least 233 attacks during Q4 2023, the highest of any quarter observed by ZeroFox Intelligence. Q4 2023 represents a significant increase compared to the 165 attacks conducted by LockBit affiliates during Q3 2023.

- LockBit’s 2023 activity increased approximately 10 percent when compared with 2022.

- Total R&DE activity across the threat landscape in 2023 saw a 70 percent increase over 2022.



Number of LockBit attacks by quarter

Source: ZeroFox Intelligence

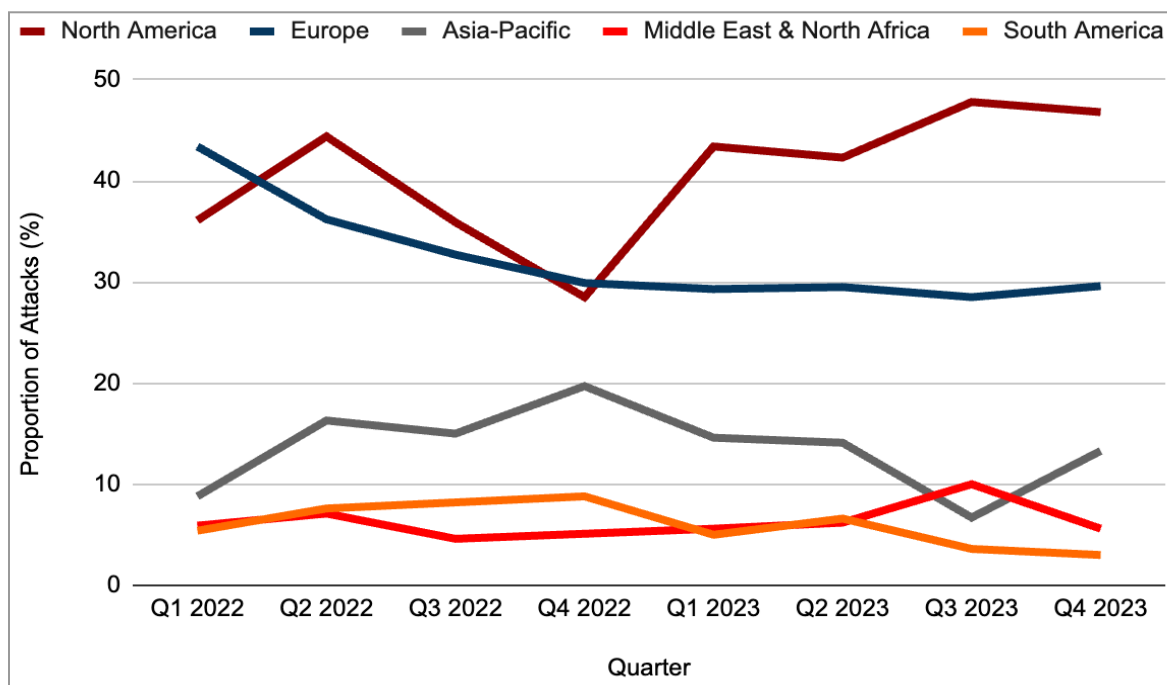
LockBit's targeting has increased almost uniformly across the landscape, with a greater number of victims across the majority of geographies and industries. A significant proportion of LockBit's increased activity results from affiliates' increased targeting of organizations in the manufacturing sector.

- Manufacturing organizations have typically comprised approximately 20 percent of all LockBit victims in 2023. However, in Q4 2023, manufacturing organizations represented 26 percent of its victims.
- This uptick is largely driven by LockBit's increased targeting of Asia-Pacific manufacturers, which rose by approximately 300 percent during Q4.

Targeting of the retail sector is also on an upward trajectory, particularly against organizations based in the Asia-Pacific and North America regions. The only industries to experience a slight reduction in LockBit targeting in Q4 2023 were education, construction, and technology.

- The Asia-Pacific region accounted for the biggest proportional increase in targeting, accounting for approximately 13 percent of LockBit victims (up from 6 percent the quarter before) and returning to levels observed in early 2023.

LockBit affiliates continue to target the majority of regions at proportionally higher rates than the wider threat landscape, with the exception of North America. LockBit's proportion of attacks targeting North America have been consistently less than the wider landscape average since Q2 2022, despite the number of attacks increasing significantly in Q4 2023.



Proportion of LockBit attacks by region
(ANZAC region omitted due to very low number)

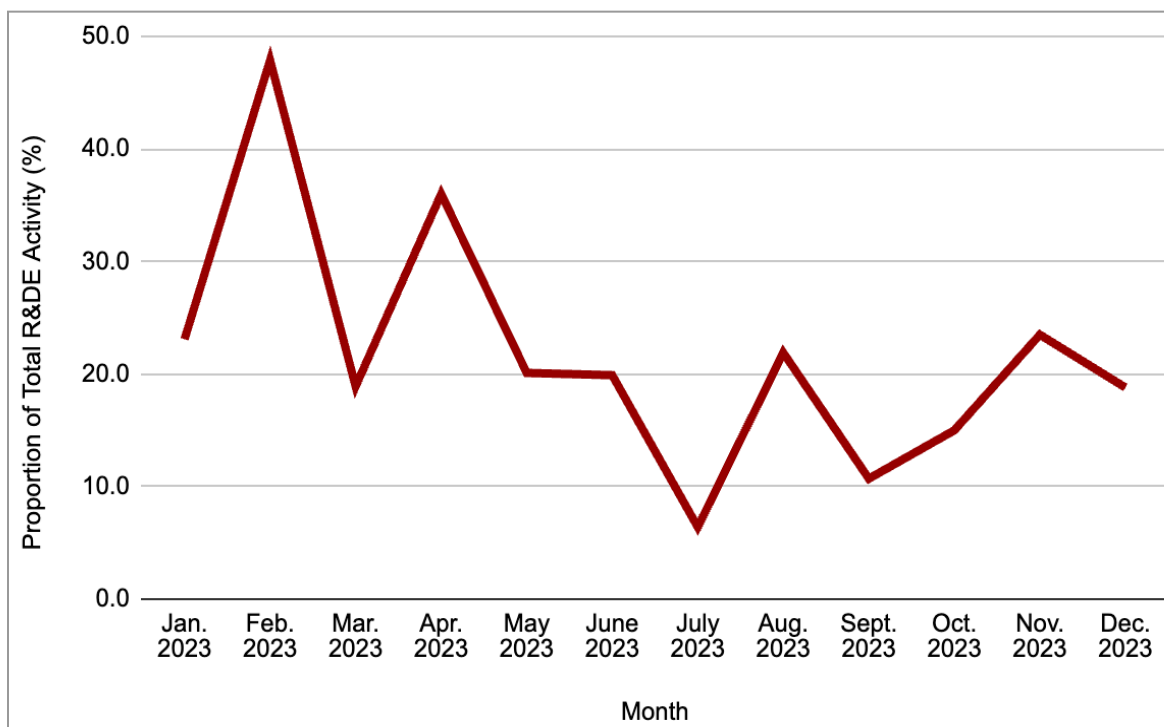
Source: ZeroFox Intelligence

LockBit is almost certainly benefitting from the disruption of other R&DE collectives in December. The collective sought affiliates from prominent ransomware outfits ALPHV

(also known as BlackCat) and NoEscape, offering the use of both its data breach site and trading panel as well as the option to transfer ongoing extortion activities to its platform.¹

Despite this, LockBit's market share of total R&DE activity continues to fall, indicating continued diversification across the threat landscape.

- While LockBit accounted for more than 35 percent of total R&DE attacks in early 2023—peaking at almost 50 percent in February 2023—it accounted for approximately 20 percent of total R&DE attacks in Q4 2023.
- In November 2023, ZeroFox published *ZeroFox Intelligence Brief: Ransomware & Digital Extortion—LockBit Targeting*, revealing analysis of LockBit's in-depth targeting patterns.



LockBit attacks as a proportion of total R&DE activity, by month

Source: ZeroFox Intelligence

¹ [hXXps://twitter\[.\]com/g0njxa/status/1734510597201404361](https://twitter.com/g0njxa/status/1734510597201404361)

It is likely that LockBit will continue to acquire additional affiliates and targeting opportunities, enabling the collective to conduct an increasing number of attacks over the next two quarters.

- There is a roughly even chance that LockBit will use this opportunity to offer potential affiliates novel and attractive services in an attempt to stand out amongst newer, highly-active R&DE collectives such as Akira, Cactus, WereWolves, and Rhysida.

However, LockBit's proportional share of R&DE activity across the threat landscape is unlikely to increase significantly due to the current upward trajectory in overall attacks and new extortion operations that are diversifying the threat landscape.

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%