



Brief

LockBit Targeting of the United Kingdom, 2022–2023

B-2023-12-01b

Classification: TLP:CLEAR

Criticality: Medium

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

December 1, 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 5:00 PM (EST) on November 30, 2023*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | LockBit Targeting of the United Kingdom, 2022–2023

Executive Summary

LockBit is ransomware used by threat actors to infect and extort victims. The strain, identified as early as September 2019, is run as a ransomware-as-a-service (RaaS) offering with a subscription-based business model involving the selling or leasing of malicious code to multiple, fee-paying affiliates on dark web forums. LockBit 3.0—currently the most prolific extortion operation—has been equipped with worm-like capabilities that enable self-propagation across a compromised network. The strain is renowned for its speed of compromise, leveraging strong cryptography to render thousands of files inaccessible to users within seconds. Backups are removed to prevent file recovery attempts.

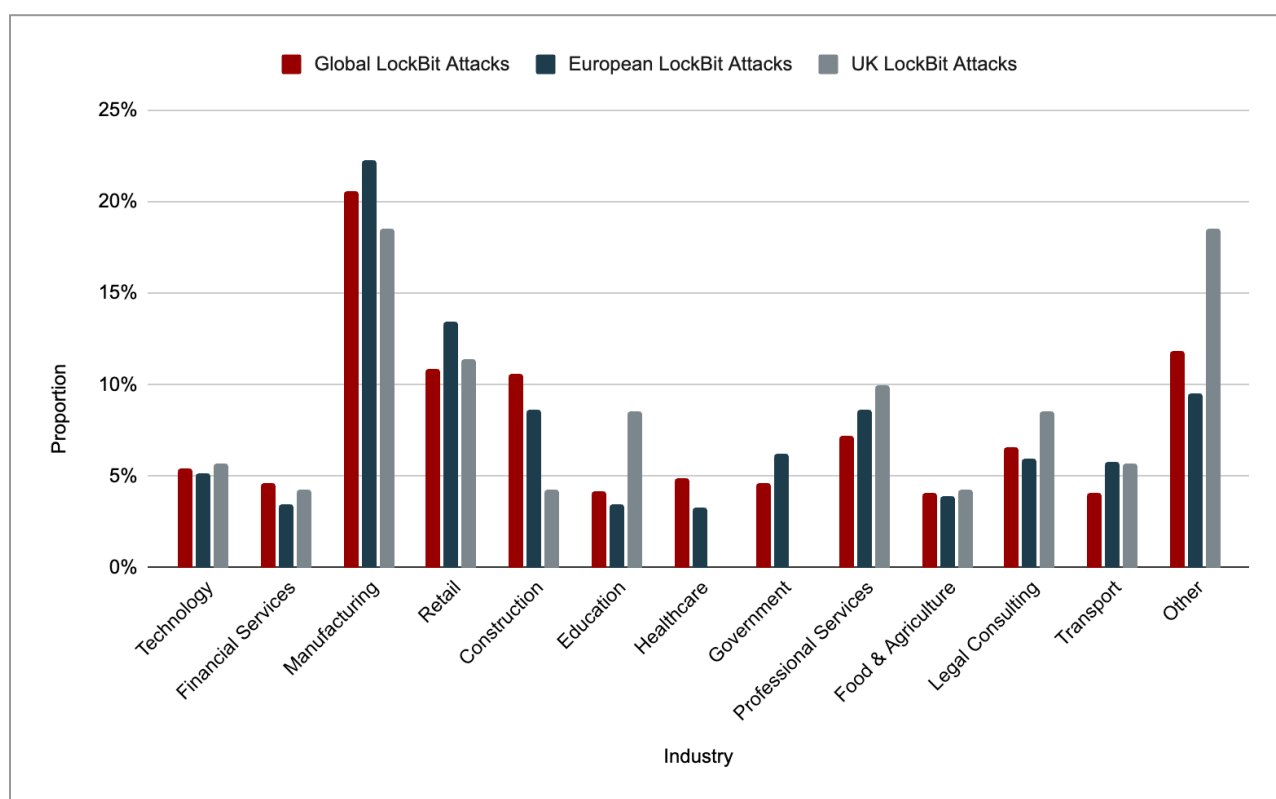
This report outlines the threat from LockBit to UK-based organizations over the last two years. All data and analysis included in this report are based on ZeroFox collections only and do not include data from third parties. This report should be read in conjunction with [ZeroFox Intelligence Brief – Ransomware & Digital Extortion – LockBit Targeting, B-2023-11-17a](#).

Details

Between January 2022 and November 2023, LockBit has been the primary ransomware and digital extortion (R&DE) threat to UK-based organizations. On a quarterly average, LockBit has accounted for approximately 20 percent of all R&DE attacks against UK-based organizations.

In the reporting period, LockBit's most frequently-targeted industries in the UK have been:

- Manufacturing
- Retail
- Professional Services
- Education
- Legal & Consulting



LockBit Industry Targeting as a Proportion of Its Total Attacks

Source: ZeroFox

When considering LockBit’s operation as a whole, there is no evidence to indicate a disproportionate focus on targets in the UK. The proportion of LockBit deployment against UK-based targets has been consistent with total R&DE attacks in the UK. However, it is likely specific LockBit affiliates have a bias towards targeting particular countries or regions, with it more likely than not that some have a focus on UK-based targets.

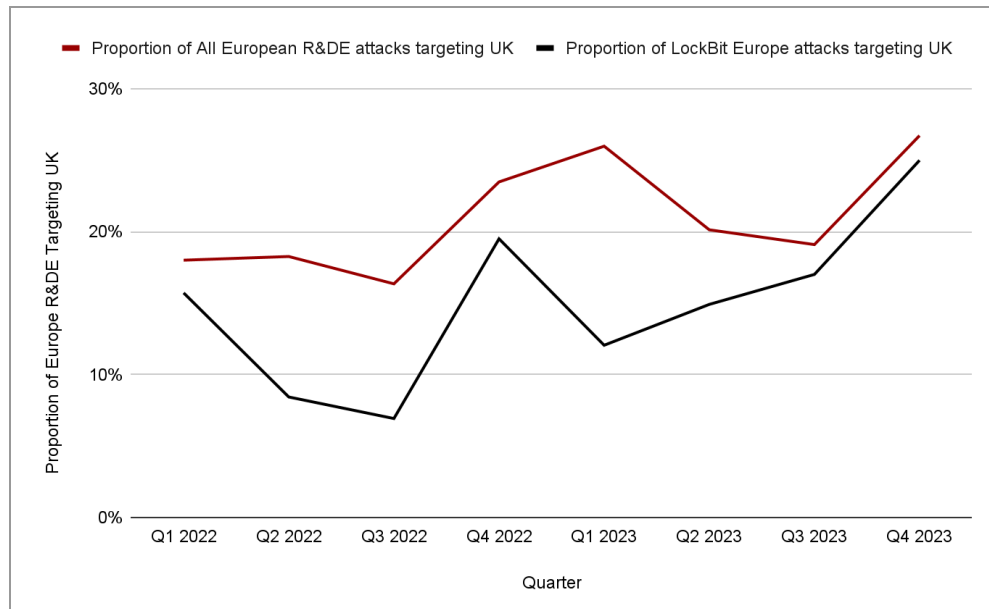
Quarter	Percent of Total R&DE Targeting UK	Percent of LockBit’s R&DE Targeting UK
Q1 2022	6.2%	6.8%
Q2 2022	6.1%	3.1%
Q3 2022	4.9%	2.3%
Q4 2022	6.0%	5.8%
Q1 2023	6.6%	3.5%
Q2 2023	5.3%	4.4%
Q3 2023	5.3%	4.8%
Q4 2023*	8.0%	7.9%

How LockBit’s Targeting of the UK Compares to R&DE as a Whole

Source: ZeroFox

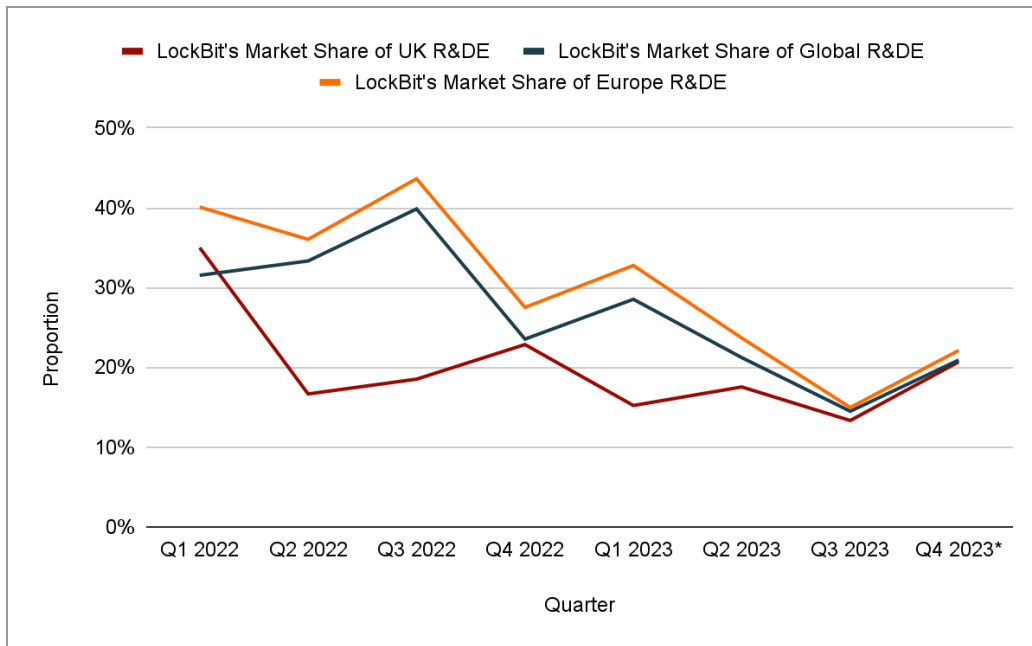
*Q4 2023 data as of November 30, 2023

The UK consistently accounts for approximately 20 percent of total European R&DE attacks. LockBit’s Europe-focused targeting has decreased, whereas its attacks against the UK have remained broadly consistent—meaning UK organizations represent an increasing proportion of LockBit’s Europe-focused targeting. This likely indicates that, while LockBit affiliates focused on targeting wider Europe have reduced activity or pivoted to other strains, UK-focused affiliates continue to leverage LockBit and maintain their operational tempo.

**Proportion of European R&DE targeting the UK***Source: ZeroFox*

*Q4 2023 data as of November 30, 2023

While LockBit remains the primary R&DE threat to UK-based organizations (accounting for approximately 20 percent of all R&DE attacks against UK-based organizations on average), diversification of the R&DE threat landscape is driving LockBit to account for an increasingly smaller proportion of total R&DE against the UK. Despite the frequency of LockBit attacks against the region remaining high, other groups—including newly formed, highly prolific collectives—are demonstrating an even greater focus on targets in the country. This mirrors LockBit’s market share decline more broadly in Europe and around the world.



Proportion of R&DE for Which LockBit is Responsible

Source: ZeroFox

*Q4 2023 data as of November 30, 2023

ZeroFox anticipates LockBit will remain the primary R&DE threat to the region over the next two quarters, with attacks very likely to remain frequent. However, LockBit's falling UK market share and the rise of highly-prolific strains driving an increase in UK-focused targeting means security teams will need to monitor for, and mitigate the threats from, an increasingly diverse range of extortion operations.

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies, with phishing-resistant MFA, complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of relevant cyber threats and associated TTPs.
- 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 process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.
- Deploy robust External Attack Surface Management solutions for ongoing Lockbit-targeted discovery.

| 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%