



| Flash |

LockBit Disrupted by Law Enforcement Agencies

F-2024-02-20a

Classification: TLP:CLEAR

Criticality: High

**Intelligence Requirements: Ransomware & Digital Extortion, Deep & Dark
Web, Threat Actors**

February 20, 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 20, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | LockBit Disrupted by Law Enforcement Agencies

> Key Findings

- On February 19, 2024, Ransomware & Digital Extortion (R&DE) collective LockBit's leak site was seized by law enforcement agencies in a joint operation between 11 countries dubbed "Operation Cronos."
- LockBit's affiliate panel source code, chats, and victim information have also reportedly been seized, with a free decryption key released for victims. As many as 22 known LockBit onion site links are either offline or displaying a seizure message. However, some of the collective's other dark web sites remain operational.
- The apparent success of Operation Cronos is likely to have a significant impact on LockBit's immediate operational capability and a short-term suppressive effect on the overall R&DE threat, considering the significant proportion of extortion attacks for which LockBit is responsible.
- However, the operation is unlikely to have a sustained impact on the overall threat from R&DE. Comprehensive degradation of LockBit's infrastructure will likely result in a short cessation in activity from LockBit operatives before they resume operations—either under the LockBit name or an alternative banner. It is crucial security teams continue to monitor for LockBit indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs).

Details

On February 19, 2024, R&DE collective LockBit's leak site was seized by law enforcement agencies in a joint operation between 11 countries dubbed "Operation Cronos." At the time of writing, LockBit's data leak website displays a banner stating that the site is under the control of the United Kingdom's National Crime Agency. LockBit's affiliate panel source code, chats, and victim information have also reportedly been seized.¹ Operation Cronos is ongoing, with the potential for further disruption to occur.

- As many as 22 known LockBit onion site links are either offline or displaying a seizure message. However, some of the collective's other dark web sites remain operational.
- LockBit's ransom negotiation sites are down but do not currently display a seizure notification. LockBit operatives have alleged that the servers hosting seized data remain intact, and new negotiation channels will be established.
- Law enforcement issued a free decryption tool for victims to recover their encrypted files. Two alleged LockBit operators were arrested in Poland and Ukraine, and over 200 crypto wallets associated with the operation were frozen. Additionally, three international arrest warrants and five indictments were issued targeting other LockBit-affiliated individuals.



Seizure message displayed on LockBit's leak site following law enforcement disruption

Source: ZeroFox Intelligence

¹

[hXXps://www.nationalcrimeagency\[.\]gov\[.\]uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group](https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group)

It is understood LockBit's core operatives have issued several messages to individuals on instant-messaging platform Tox confirming the seizure of parts of its operational infrastructure.

- LockBit's group administrator allegedly claimed that law enforcement agencies compromised the site by exploiting a PHP vulnerability (CVE-2023-3824).
- LockBit reportedly emailed its affiliates about unauthorized access to its systems, a potential leak of affiliates' personal information, and steps to take to mitigate the potential exposure.

The extent to which LockBit's infrastructure has been disrupted or degraded in the long term is unclear. Given the ongoing and developing nature of the operation, it is possible additional law enforcement activity will further disrupt LockBit's operational infrastructure.

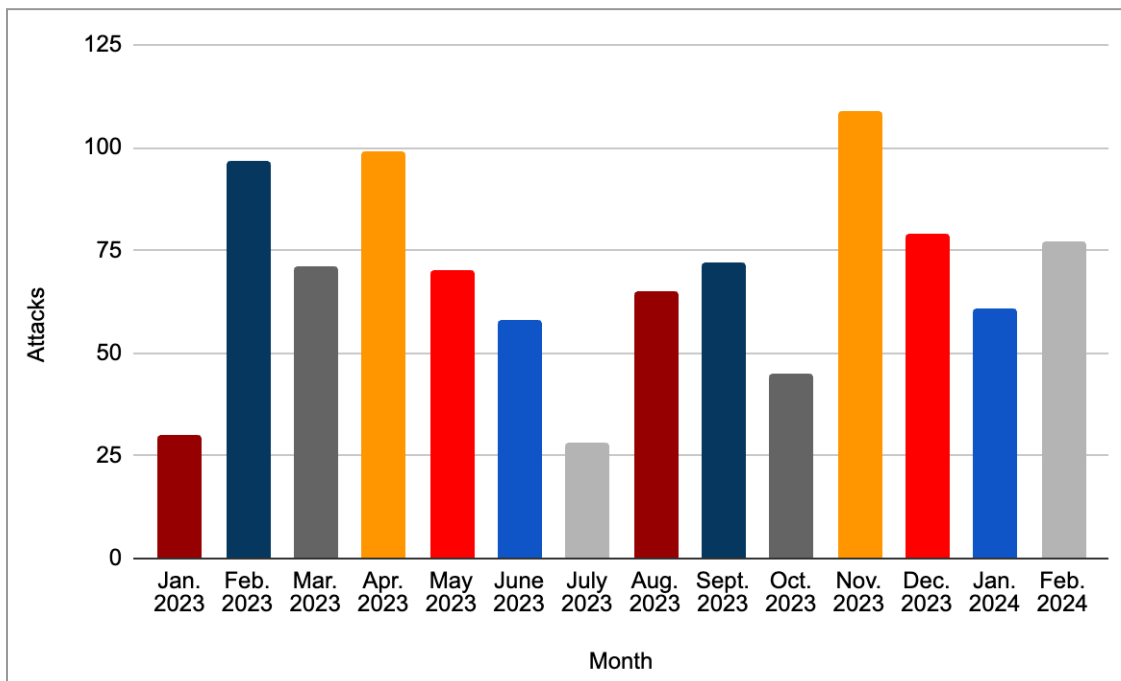
- LockBit's infrastructure has likely been significantly degraded by Operation Cronos.
- LockBit is very likely underplaying the extent to which its infrastructure has been disrupted in its outward communications to maintain the confidence of its operatives and affiliates.
- However, LockBit operatives and affiliates are very likely still able to deploy the strain against compromised networks.

The apparent success of Operation Cronos is likely to have a short-term suppressive effect on the overall R&DE threat, considering the proportion of extortion attacks for which LockBit is responsible. Even a short-term disruption to LockBit's operational activity will very likely result in a reduction in R&DE attacks globally.

- Between January 2022 and February 2024, the LockBit ransomware strain has been the primary digital extortion threat to all regions, and almost all industries, globally.
- There have been approximately 70 attacks per month leveraging the LockBit ransomware strain since the start of 2023.
- Since the start of 2024, LockBit attacks account for approximately 27 percent of all R&DE attacks globally.

However, Operation Cronos is unlikely to have a sustained impact on the threat from R&DE. It is crucial that security teams continue to monitor for LockBit IOCs and TTPs, in addition to staying on top of R&DE landscape trends to identify the banner under which these operatives will resume their extortion activities.

- If the disruption to LockBit's infrastructure is significant and long-standing, there will very likely be a short cessation in activity from LockBit operatives and affiliates before they continue R&DE operations under a new banner or join an alternative, existing operation.
- If the law enforcement operation does not comprehensively degrade LockBit's infrastructure, the group's operatives will likely attempt to revive the operation with new leak sites and backend infrastructure.
- The December 2023 disruption of R&DE collective ALPHV degraded its operational capability significantly, though not comprehensively. This enabled the collective to continue its operations in 2024, with ZeroFox observing an upward trajectory of attacks in recent weeks.



LockBit attacks by month, January 2023 – February 2024

Source: ZeroFox Intelligence

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 LockBit threats, TTPs, and 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%