LockBit Targeting

Ransomware & Digital Extortion

TLP:CLEAR

ZEROFOX Intelligence

Key Findings

- LockBit has been the primary ransomware and digital extortion (R&DE) threat to almost all industries in all locations.
- While LockBit will very likely remain one of the greatest R&DE threats, the proportion of total attacks that LockBit accounts for is on a downward trajectory.
- Diversification of the R&DE threat landscape is being driven by new threat collectives demonstrating proficiency at pace and prolific LockBit affiliates likely choosing to instead deploy other strains or create their own.
- While the LockBit threat will very likely remain high, security teams should monitor for an increasingly diverse spectrum of R&DE operations.

LockBit Profile

LockBit is a ransomware strain 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. The operation was initially known as *ABCD* due to the naming extension it added to encrypted files; this was later changed to a *.lockbit* extension, and the operation was renamed accordingly. Developers have distributed several variants to encrypt files: *.abcd*, *LockBit 1.0*, *LockBit 2.0*, and *LockBit 3.0*—currently the most prolific extortion operation.

LockBit 3.0 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.

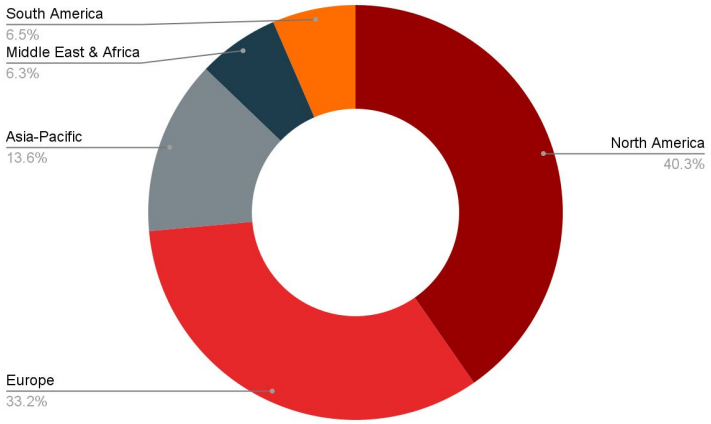
LockBit operators are known to leverage a variety of intrusion vectors to compromise victims' systems, including phishing, credential stuffing, and Remote Desktop Protocol (RDP) exploitation. One of the most widely-reported intrusion vectors is the leveraging of Virtual Private Network (VPN) remote access to gain access to victim networks. Operators typically leverage double extortion tactics, threatening to release exfiltrated sensitive information if ransom demands are not met.

Disclaimer: All data and analysis included in this report is based on ZeroFox collections only. This does not include data from third parties.

Targeting Overview

Between January 2022 and September 2023, the LockBit ransomware strain has been the primary digital extortion threat to all regions, and almost all industries, globally. It has been the most frequently deployed R&DE strain since January 2022, compromising the highest number of known targets in almost all of the seven quarters analyzed.

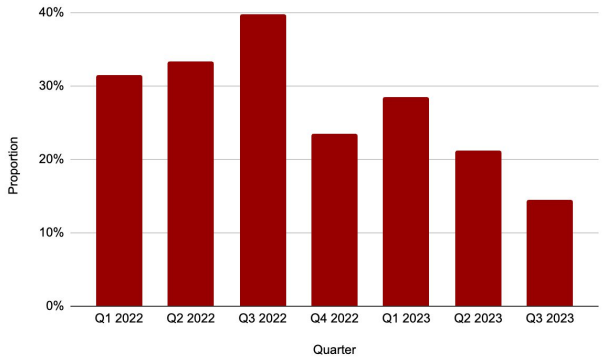
LockBit Attacks by Region
January 2022 - September 2023



Source: ZeroFox Intelligence

Although, on average, LockBit has been leveraged in more than a quarter of global attacks each quarter, the proportion of total R&DE attacks that LockBit accounts for is on a downward trajectory. This very likely reflects the increasing diversification of the R&DE landscape, with newly-formed collectives demonstrating increasingly rapid proficiency, largely owing to the proliferation of off-the-shelf tools that lower barriers to entry for would-be threat actors.

LockBit Attacks as a Proportion of Total R&DE Attacks



Source: ZeroFox Intelligence

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 16, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Intrusion Vectors

Exploit Internet-Facing Applications

In 2023 alone, affiliates have exploited vulnerabilities in internet-facing systems to deploy LockBit, including, but not limited to:

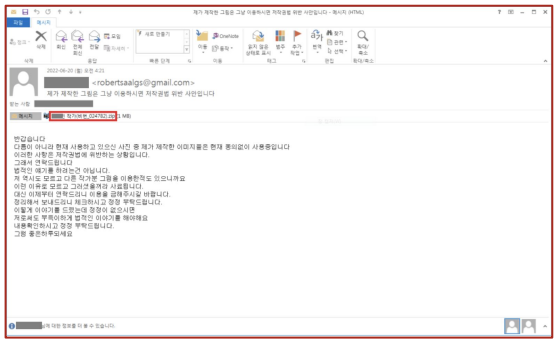
- CVE-2023-4966: A Buffer Overflow vulnerability in Citrix NetScaler ADC and NetScaler Gateway
- CVE-2023-0669: A Remote Code Execution vulnerability in Fortra GoAnywhere Managed File Transfer (MFT)
- CVE-2023-27350: An Improper Access Control vulnerability in PaperCut MF/NG
- CVE-2023-20269: An Unauthorized Access vulnerability in Cisco ASA and FTD software

Historically, LockBit affiliates are also known to have exploited:

- CVE-2021-44228: A Remote Code Execution vulnerability in Apache Log4j logging tool
- CVE-2021-22986: A Remote Code Execution vulnerability in F5 BIG-IP and BIG-IQ Centralized Management iControl REST
- CVE-2020-1472: A Privilege Escalation vulnerability in NetLogon
- CVE-2019-0708: A Remote Code Execution vulnerability in Microsoft Remote Desktop Services
- CVE-2018-13379: A Path Traversal vulnerability in Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network

Phishing (including Spear Phishing)

Affiliates leverage phishing and spear phishing to gain access to victims' networks. Threat actors have been observed using a variety of lures, including attaching malicious documents to fraudulent resume and copyright-related emails. When these malicious attachments are engaged with, the payload is executed.



LockBit phishing email disguised as a copyright claim
Source: hXXps://asec.ahnlab[.]com/en/35822/

External Remote Services

LockBit affiliates are known to exploit RDP to gain access to victim networks. Threat actors leverage legitimate user credentials obtained via credential harvesting to access external-facing remote working services.

Drive-by Compromise

Threat actors deploying LockBit have been observed gaining access to a system via a user visiting a website over the normal course of browsing. The user's web browser is typically targeted for exploitation, but adversaries may use malicious domains for Application Access Token acquisition.

Valid Accounts

LockBit operators are known to obtain credentials of existing accounts to gain initial access. Compromised credentials are used to bypass access controls, establish persistence, escalate privileges, and evade detection.

Initial Access Brokers

ZeroFox has identified LockBit affiliates that purchase access from Initial Access Brokers on the deep and dark web (DDW), creating established relationships with sellers of access. Sales are increasingly moving towards private, off-forum channels rather than occurring in DDW marketplaces or forums. Established LockBit affiliates very likely work closely with specific brokers to lower the cost of securing access.

Access sold off-forum is typically cheaper, meaning LockBit affiliates are likely able to obtain discounts and even be alerted in advance to upcoming accesses that will be listed for sale. This will likely make LockBit extortion attacks increasingly difficult to intercept in advance by DDW monitoring—and only prevented by a tight security posture and proper training against social engineering, phishing, and good overall company cyber hygiene.

In 2023, there has been an increase in access advertised into third-party vendors of major corporations and government entities. This is due to the potentially weaker security postures of third parties hired by larger organizations and the elevated privileges and accesses that come with being integrated into the larger entity.

Targeting By Region

North America (NA)

LockBit has consistently been the primary R&DE threat to NA-based organizations, accounting for approximately 25 percent of all R&DE attacks in the region. Like most extortion operations, LockBit attacks predominantly target NA.

Between 2022 and 2023, LockBit's most frequently-targeted industries in NA are:

1. Manufacturing
2. Construction
3. Retail
4. Legal & Consulting
5. Healthcare

LockBit affiliates are increasingly focused on targeting NA-based organizations. While on average 40 percent of LockBit victims are based in the region, this is on an upward trajectory and is expected to reach nearly 50 percent by the end of 2023. This reflects a broader trend across the R&DE landscape, whereby NA accounts for an increasing proportion of global R&DE attacks.

Historically, LockBit has been consistently under-deployed in attacks against NA when compared with R&DE attacks as a whole. The proportion of LockBit's attacks targeting the region is typically lower than broader averages. This is likely due to the spread of affiliates leveraging the strain and access sold to them by access brokers. LockBit is likely popular with threat actor circles that have been focused on targeting other regions, such as Europe. However, there is evidence to suggest that this trend is shifting, with LockBit operatives increasingly focused on NA-based targets.

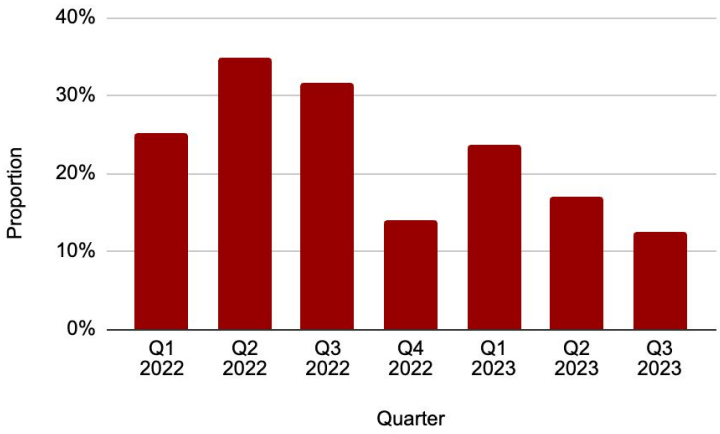
How LockBit's Targeting of NA Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting NA	% of LockBit's R&DE Targeting NA
Q1 2022	45.23%	36.10%
Q2 2022	42.52%	44.39%
Q3 2022	45.29%	35.91%
Q4 2022	48.28%	28.47%
Q1 2023	52.45%	43.43%
Q2 2023	52.90%	42.29%
Q3 2023	55.80%	47.88%

Source: ZeroFox Intelligence

While LockBit remains one of the most prolific targeters of NA-based organizations, diversification of the R&DE threat landscape is driving a reduction in LockBit's regional market share; LockBit accounts for an increasingly small proportion of total R&DE against NA. 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 region.

Proportion of R&DE Against NA for Which LockBit is Responsible



Source: ZeroFox Intelligence

ZeroFox anticipates LockBit will increasingly focus on NA-based targets over the next two quarters, with the strain likely to remain the primary R&DE threat to the region. Attacks will very likely remain highly frequent, and ZeroFox expects that the proportion of LockBit attacks targeting NA will likely exceed the global average.

However, diversification in the threat landscape and the rise of highly prolific, newly-formed collectives such as Akira, NoESCAPE, and LostTrust place increasing importance in understanding the changing threat landscape. Security teams within NA-based organizations must prepare for not only LockBit-based extortion threats but also an increasing number of other R&DE operations targeting the region.

Europe

LockBit remains the primary R&DE threat to Europe-based organizations, despite a downward trend in the total number and proportion of its attacks against the region. On average, LockBit accounts for over 30 percent of all R&DE attacks against Europe-based organizations.

Between 2022 and 2023, LockBit's most frequently-targeted industries in Europe are:

1. Manufacturing
2. Retail
3. Professional Services
4. Construction
5. Legal & Consulting

LockBit goes against the broader trend in Europe-focused R&DE targeting. In 2023, there has been a significant increase in R&DE attacks against Europe-based organizations; this increase is commensurate with the global increase in R&DE, meaning the region accounts for a consistent proportion of global attacks. However, LockBit attacks do not reflect this broader trend; there is a downward trend in total attacks against Europe and a fall in the proportion of LockBit's attacks targeting Europe.

LockBit affiliates are likely increasingly moving away from Europe-focused targeting. While, on average, approximately 33 percent of LockBit victims are based in the region, this is on a downward trajectory. Affiliates are very likely shifting their focus towards organizations based in other regions, such as North America. ZeroFox notes the possibility that LockBit has shifted away from politically-inspired targeting of European organizations following Russia's war in Ukraine and towards purely financially-motivated targeting.

How LockBit's Targeting of Europe Compares to R&DE as a Whole

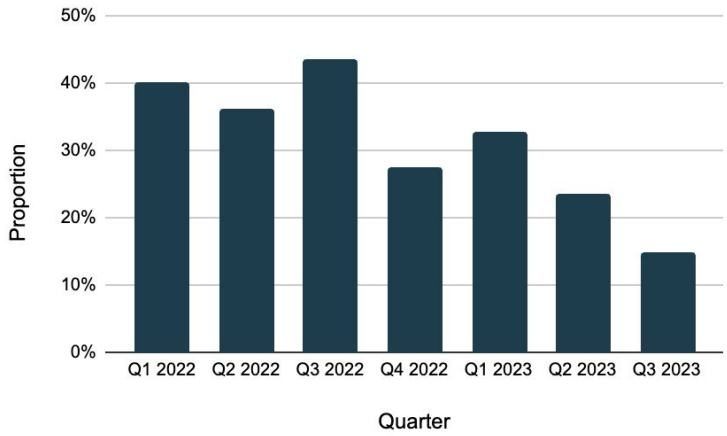
Quarter	% of Total R&DE Targeting Europe	% of LockBit's R&DE Targeting Europe
Q1 2022	34.15%	43.41%
Q2 2022	33.50%	36.22%
Q3 2022	29.89%	32.73%
Q4 2022	25.60%	29.93%
Q1 2023	25.50%	29.29%
Q2 2023	26.45%	29.52%
Q3 2023	27.59%	28.48%

Source: ZeroFox Intelligence

Historically, LockBit has been consistently over-deployed against Europe-based targets when compared with R&DE attacks as a whole. The proportion of LockBit attacks targeting Europe typically exceeds broader averages. This is unlikely to remain the case in coming quarters; LockBit's proportion of attacks targeting Europe is anticipated to fall below global averages as affiliates' focus shifts away from Europe and other strains become more prevalent in the region.

Diversification of the R&DE threat landscape means that, while LockBit remains one of the most prolific targeters of Europe-based organizations, its market share is falling. LockBit accounts for an increasingly small proportion of total R&DE against Europe. Other groups—including newly-formed, highly-prolific collectives—are demonstrating an even greater focus on targets in the region.

Proportion of R&DE Against Europe for Which LockBit is Responsible



Source: ZeroFox Intelligence

ZeroFox anticipates LockBit affiliates will continue to move away from Europe-focused targeting towards organizations in North America. While the strain is likely to remain the primary R&DE threat to the region over the next two quarters—and attacks will very likely remain highly frequent—the proportion of LockBit attacks targeting Europe will likely continue to decrease, falling below total R&DE averages.

With other highly-prolific strains driving a significant increase in attacks against Europe-based organizations, security teams in the region will need to monitor for, and mitigate the threats from, an increasingly diverse range of extortion operations.

Asia Pacific (APAC)

LockBit is the primary R&DE threat to APAC-based organizations, responsible for approximately 40 percent of all R&DE attacks in the region. On average, nearly 15 percent of all LockBit attacks target APAC-based organizations.

Between 2022 and 2023, LockBit's most frequently-targeted industries in APAC are:

1. Manufacturing
2. Retail
3. Construction
4. Technology
5. Professional Services

LockBit bucks the broader trend in APAC-focused R&DE targeting. In 2023, the total number of APAC attacks has increased; this increase is commensurate with the global increase in R&DE attacks—meaning the region accounts for a consistent proportion of global R&DE attacks. However, LockBit attacks against APAC have not increased, with the total number of attacks against the region remaining broadly consistent and a fall in the proportion of its attacks targeting the region.

LockBit affiliates remain focused on targeting the APAC region. When compared with all R&DE strains, LockBit is consistently—and significantly—over-deployed in attacks against APAC-based targets. The proportion of LockBit attacks targeting APAC consistently exceeds total R&DE averages. This is likely due to the spread of affiliates leveraging the strain; LockBit is likely popular with threat actor circles typically focused on targeting APAC. Despite a drop in the proportion of LockBit's attacks targeting APAC in Q3 2023, ZeroFox anticipates this will increase.

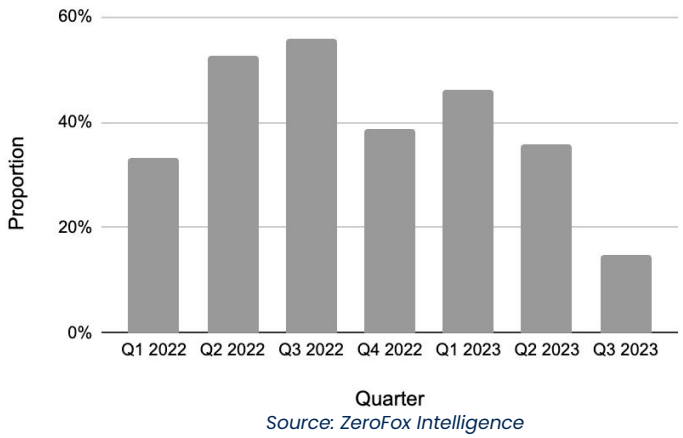
How LockBit's Targeting of APAC Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting APAC	% of LockBit's R&DE Targeting APAC
Q1 2022	8.31%	8.78%
Q2 2022	10.37%	16.33%
Q3 2022	10.69%	15.00%
Q4 2022	12.03%	19.71%
Q1 2023	9.08%	14.65%
Q2 2023	8.32%	14.10%
Q3 2023	6.50%	6.67%

Source: ZeroFox Intelligence

LockBit accounts for an increasingly small proportion of total R&DE against APAC-based organizations, with a fall in its market share. This is very likely driven by diversification of the R&DE threat landscape. While remaining one of the most prolific targeters of APAC-based organizations, other groups—including newly-formed, highly-prolific collectives—are demonstrating an increased focus on targets in the region.

Proportion of R&DE Against APAC for Which LockBit is Responsible



Source: ZeroFox Intelligence

ZeroFox anticipates LockBit affiliates will consistently target organizations based in APAC, remaining one of the primary R&DE threats to the region over the next two quarters. However, ZeroFox anticipates that LockBit will account for a decreasing proportion of attacks targeting the region, with other strains rising to prominence. Security teams in the region will need to monitor for, and mitigate the threats from, an increasingly diverse range of extortion operations.

Middle East and Africa (MEA)

LockBit is the primary digital extortion threat to MEA, responsible for approximately 33 percent of all R&DE attacks that occur in the region. On average, approximately 6 percent of LockBit's attacks target MEA-based organizations.

Between 2022 and 2023, LockBit's most frequently-targeted industries in MEA are:

1. Manufacturing
2. Government
3. Construction
4. Professional Services
5. Retail

In 2023, the total number of R&DE attacks against MEA has increased; this rise is commensurate with the global increase in R&DE attacks, meaning the region accounts for a consistent

proportion of global R&DE attacks.

LockBit bucks the broader trend in MEA-focused R&DE targeting. Since the start of 2023, the region, which accounts for consistent proportion of global attacks, has seen a significant increase in total R&DE attacks. LockBit attacks against MEA-based organizations have remained broadly consistent. However, not only do MEA-based organizations represent an increasing proportion of LockBit victims, Lockbit is increasing its market share of total R&DE attacks in the region.

When compared with R&DE as a whole, LockBit is consistently over-deployed against MEA-based targets. The proportion of LockBit attacks targeting the region typically exceeds total R&DE averages.

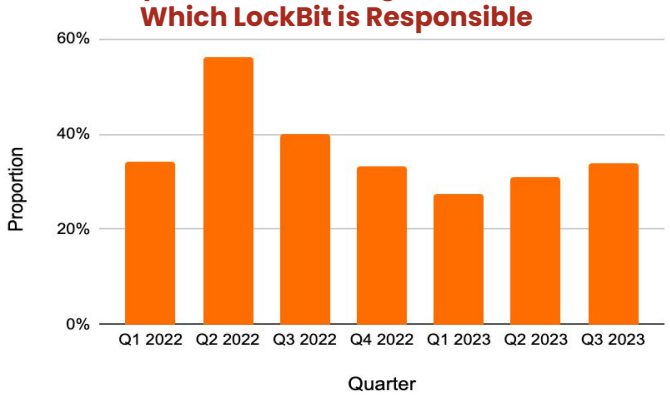
How LockBit's Targeting of MEA Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting MEA	% of LockBit's R&DE Targeting MEA
Q1 2022	5.38%	5.85%
Q2 2022	4.25%	7.14%
Q3 2022	4.53%	4.55%
Q4 2022	3.61%	5.11%
Q1 2023	5.76%	5.56%
Q2 2023	4.21%	6.17%
Q3 2023	4.39%	10.30%

Source: ZeroFox Intelligence

Unlike in all other regions where LockBit's market share is falling, LockBit attacks continue to dominate R&DE in the region. On average, affiliates are responsible for approximately 37 percent of all attacks in the region. It is likely MEA has a less–diverse threat landscape than other regions, meaning that the diversification of the R&DE threat landscape seen elsewhere has not impacted the strain's dominance.

Proportion of R&DE Against MEA for Which LockBit is Responsible



Source: ZeroFox Intelligence

ZeroFox anticipates LockBit will remain the primary R&DE threat to organizations based in MEA, continuing to account for more than one third of attacks in the region.

South America (SA)

While historically the primary R&DE threat to SA-based organizations, LockBit is no longer the preeminent threat to the region. In 2023, there has been a downward trend in the total number and proportion of LockBit attacks against SA-based targets. On average, LockBit is responsible for approximately one third of the R&DE attacks that occur in the region.

Between 2022 and 2023, LockBit's most frequently-targeted industries in SA are:

1. Manufacturing
2. Retail
3. Financial Services
4. Construction
5. Food & Agriculture

In 2023, the total number of SA R&DE attacks has remained broadly consistent but represents an increasingly small proportion of global R&DE attacks. LockBit attacks largely reflect this broader trend, with a reduction in total attacks targeting the region and a fall in the proportion of its attacks targeting SA.

LockBit affiliates are likely moving away from SA-focused targeting. While on average 7 percent of its victims are based in the region, this is on a downward trajectory. LockBit affiliates are likely shifting their focus towards organizations based in other regions, including North America.

LockBit is consistently over-deployed against SA-based targets when compared with R&DE attacks as a whole. The proportion of LockBit attacks targeting the region typically exceeds total R&DE averages. This is unlikely to remain the case in coming quarters, with LockBit's proportion of attacks targeting SA anticipated to fall below global averages.

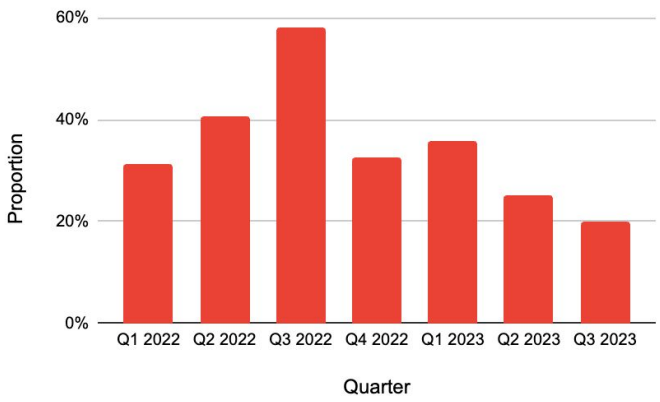
How LockBit's Targeting of SA Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting SA	% of LockBit's R&DE Targeting SA
Q1 2022	5.38%	5.37%
Q2 2022	6.29%	7.65%
Q3 2022	5.62%	8.18%
Q4 2022	6.36%	8.76%
Q1 2023	4.03%	5.05%
Q2 2023	5.61%	6.61%
Q3 2023	2.64%	3.64%

Source: ZeroFox Intelligence

Diversification of the R&DE threat landscape means that, while LockBit remains one of the most prolific targeters of SA-based organizations, its market share is falling. LockBit accounts for an increasingly small proportion of total R&DE against SA. Other groups—including newly-formed, highly-prolific collectives—are demonstrating an even greater focus on targets in the region.

Proportion of R&DE Against SA for Which LockBit is Responsible



Source: ZeroFox Intelligence

ZeroFox anticipates LockBit affiliates will move away from SA-focused targeting towards organizations in North America. While the strain is likely to remain the primary R&DE threat to the region over the next two quarters—and attacks will very likely remain highly frequent—the proportion of LockBit attacks targeting SA will likely continue to decrease, falling below total R&DE averages. Security teams in the region will need to monitor for, and mitigate the threats from, an increasingly diverse range of extortion operations.

Targeting By Industry

LockBit is leveraged to target organizations of all sizes in almost all sectors, from "big game" hunting to small-medium sized businesses. As with many extortion cartels, operators target organizations that may represent value for money or a perceived quick return on investment.

As one of the most prolific RaaS operations, LockBit's vast array of affiliates results in one of the most varied sets of targeted victims. LockBit operators are particularly aggressive towards organizations within the manufacturing and construction industries, though they have demonstrated a willingness to attack organizations in almost all sectors.

LockBit Targeting Trends Compared with Total R&DE

Industry Vertical	Lockbit Attacks as a Proportion of Total Industry Vertical R&DE 2022-2023	Trajectory of Total R&DE Against Industry Vertical	Trajectory of LockBit Targeting Against Industry Vertical
Government	34%	→	↓
Legal / Consulting	33%	↑	→
Construction	32%	↑	→
Food & Agriculture	29%	↑	→
Transport	28%	→	↓
Retail	26%	→	↓
Manufacturing	26%	↑	→
Professional Services	24%	↑	↑
Healthcare	20%	↑	→
Financial Services	20%	↑	↑
Education	18%	↑	↑
Technology	16%	↑	→

Source: ZeroFox Intelligence

LockBit's affiliates appear to be shifting their focus, driven by two key factors.

Firstly, affiliates are very likely consciously moving towards organizations they believe are more likely to pay ransom demands. While attacks against the manufacturing and construction industries remain high, ZeroFox has identified an increase in LockBit attacks against professional services, education, and financial sector companies—both in terms of total number of attacks and the proportion of total R&DE attacks for which LockBit accounts.

The shift in industry targeting is also likely driven by prolific affiliates leaving or decreasing their activity with LockBit, choosing instead to deploy other strains or create their own. 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 launching their own operations. These new threat collectives are demonstrating proficiency at a faster pace than previously observed and are more than offsetting the decline in LockBit's activity. This will likely drive significant change across the R&DE threat landscape in coming quarters.

Forward Look

- LockBit attacks will very likely remain one of the greatest R&DE threats against almost all industries in all locations.
- LockBit attacks will very likely predominantly target organizations based in North America and Europe.
- However, LockBit is likely to account for an increasingly small proportion of the total R&DE attacks. New threat collectives are likely to demonstrate proficiency at a faster pace than previously observed and will likely more than offset the decline in LockBit activity. This will likely drive significant change across the R&DE threat landscape in coming quarters.
- Current LockBit affiliates are likely to increasingly 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.
- LockBit Tactics, Techniques, and Procedures (TTPs) are unlikely to change significantly in the short to medium term. The most likely changes will occur post-intrusion, with affiliates adapting extortion tactics to exert increasing pressure on victims to pay ransoms.

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 solution for ongoing Lockbit-targeted discovery.

How ZeroFox Can Help

Understand the strategic threat faced by your organization by leveraging **ZeroFox On-Demand Investigations** for custom threat intelligence. Understand TTPs used by threat actors—including LockBit—targeting your organization by obtaining threat actor profiles and updates.

Utilize **ZeroFox Cyber Attack Surface Assessments** for a comprehensive assessment of all perimeter-facing and external digital assets to help mitigate potential exposures.

Employ **ZeroFox Platform's Intelligence Search** capability to help you identify compromised account credentials and vulnerabilities. You can also investigate network and infrastructure Indicators of Compromise (IOCs) of interest, including C2 domains, botnet-infected hosts, domain registrations, and phishing-related email addresses and phone numbers.

Leverage **ZeroFox Advanced Web Search and Dark Ops Curated Intelligence** to alert you to early warnings of threat actor chatter regarding your brand and update you on new extortion targets.

Utilize **ZeroFox's API Threat Intelligence Data Feeds** to correlate alerts in your environment with known threat actor Indicators of Attack/IOCs.

Should your organization be impacted by a data breach, utilize **ZeroFox Incident Response Services** to swiftly deploy **IDX data breach products and services** to mitigate the impact to you and your customers.

LockBit IOCs

Search for LockBit IOCs via the ZeroFox Platform Intelligence Search function here.

LockBit TTPs

Reconnaissance

Active Scanning: Scanning IP Blocks (T1595.001)
- Affiliates scan IP blocks to gather information.

Resource Development

Compromise Infrastructure: Domains (T1584.001)
- Affiliates hijack domains and subdomains.

Initial Access

Exploit Public-Facing Application (T1190)
- Affiliates exploit vulnerabilities in internet-facing systems such as Log4Shell.

External Remote Services (T1133)
- Affiliates exploit RDP to gain access to victim networks. Actors leverage legitimate user credentials obtained through credential harvesting to access external-facing remote services.

Phishing (T1566)
- Affiliates leverage phishing and spear phishing to gain access to victims' networks.

Drive-by Compromise (T11989)
- Affiliates gain access to a system through a user visiting a website over the normal course of browsing.

Valid Accounts (T1078)
- Affiliates obtain credentials of existing accounts to gain initial access.

Execution

Command and Scripting Interpreter: PowerShell (T1059.001)
- Affiliates abuse PowerShell commands and scripts for execution.

Command and Scripting Interpreter: Windows Command Shell (T1059.003)
- Affiliates use batch scripts to execute malicious commands.

Windows Management Instrumentation (T1047)
- Affiliates leverage Windows Management Instrumentation (WMI) to execute malicious commands and payloads.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
- Affiliates achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.

Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
- Affiliates hijack the search order used to load DLLs.

Software Development Tools (T1072)
- Affiliates have been identified leveraging Chocolatey, a command-line package manager for Windows.

System Services: Service Execution (T1569.002)
- Affiliates leverage PsExec to execute commands or payloads.

Persistence

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
- Affiliates add a program to a startup folder or reference it with a Registry run key. Affiliates enable automatic logon for persistence.

Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)
- Affiliates execute malicious payloads by hijacking the search order used to load DLLs.

Valid Accounts (T1078)
- Threat actors leverage compromised user accounts to maintain persistence.

Privilege Escalation

Access Token Manipulation (T1134)
- Affiliates modify access tokens and bypass access controls.

Domain Policy Modification: Group Policy Modification (T1484.001)
- Affiliates modify Group Policy Objects for lateral movement and can force group policy updates.

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)
- Affiliates bypass UAC mechanisms to elevate privileges.

Boot or Logo Autostart Execution (T1547)
- Affiliates enable automatic logon for privilege escalation.

Defense Evasion

Obfuscated Files or Information: Software Packing (T1027.002)
- Affiliates perform software packing or virtual machine software protection to conceal their code leveraging tools, such as Blister Loader.
- Affiliates send encrypted host and bot information to its C2.

Use Alternate Authentication Material (T1550)
- Affiliates have been identified leveraging alternate authentication material (such as password hashes, Kerberos tickets, and application access tokens) to move laterally within an environment and bypass normal system access controls.

Indicator Removal: Clear Windows Event Logs (T1070.001)
- The executable clears the Windows Event Logs files.

Indicator Removal: File Deletion (T1070.004)
- The executable will delete itself from the disk.

Execution Guardrails: Environmental Keying (T1480.001)
- LockBit will only decrypt the main component or continue to decrypt data if the correct password is entered.

Impair Defenses: Disable or Modify Tools (T1562.001)
- Affiliates modify and/or disable security tools, including EDR and antivirus, to avoid possible detection. This includes leveraging Backstab, Defender Control, GMER, PCHunter, PowerTool, Process Hacker, or TDSSKiller to disable EDR processes and services. Affiliates also leverage Bat Armor to bypass the PowerShell execution Policy.

LockBit TTPs

Credential Access

Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
- Affiliates search for common password storage locations to obtain user credentials.
- Affiliates leverage PasswordFox to recover passwords from Firefox Browser.

OS Credential Dumping: LSASS Memory (T1003.001)
- Affiliates leverage Microsoft Sysinternals ProDump to dump the contents of LSASS.exe.

OS Credential Dumping: Cached Domain Credentials (T1003.003)
- Affiliates access cached domain credentials used to enable authentication if a domain controller is unavailable.

Brute Force (T1110)
- Affiliates leverage VPN or RDP brute force credentials.

Discovery

Network Service Discovery (T1046)
- Affiliates may use SoftPerfect Network Scanner, Advanced Port Scanner, and AdFind to enumerate connected machines.

System Information Discovery (T1082)
- Affiliates identify system information, including hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices.

System Location Discovery: System Language Discovery (T1614.001)
- LockBit does not infect machines with language settings that match a defined exclusion list.

Lateral Movement

Remote Services – RDP (T1021.001)
- Affiliates leverage Splashtop remote desktop software.

Remote Services – Server Message Block (SMB)/Admin Windows Shares (T1021.002)
- Affiliates leverage Cobalt Strike and target SMB shares.

Lateral Tool Transfer (T1570)
- Affiliates may transfer tools or other files between systems in a compromised environment.

Archive Collected Data: Archive via Utility (T1560.001)
- Affiliates have been observed using 7-zip to compress and encrypt data prior to exfiltration.

Command & Control

Application Layer Protocol: File Transfer Protocols (T1071.002)
- Affiliates use FileZilla for C2.

Application Layer Protocol: Web Protocols (T1071.001)
- Affiliates use ThunderShell as a remote access tool to communicate via HTTP.

Protocol Tunnel (T1572)
- Affiliates use Plink to automate SSH actions on Windows.

Non-Application Layer Protocol (T1095)
- Affiliates use Ligolo to establish SOCKS5 or TCP tunnels from a reverse connection.

Remote Access Software (T1219)
- Affiliates use AnyDesk, Atera RMM, ScreenConnect, or TeamViewer for C2.

Exfiltration

Exfiltration Over C2 Channel (T1041)
- Affiliates exfiltrate data over existing C2 channels.

Automated exfiltration (T1020)
- Affiliates leverage Stealbit to exfiltrate data from a target network.

Exfiltration Over Web Service (T1567)
- Affiliates leverage publicly available file-sharing services to exfiltrate data.

Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
- Affiliates exploit existing communications with cloud services like Google Docs to transmit data directly to cloud storage rather than using a C2 channel.

Impact

Data Encrypted for Impact (T1486)
- Affiliates encrypt data on target systems to interrupt availability to system and network resources. Threat actors modify the user's directory and file permissions and demand a ransom in exchange for a decryption key. LockBit can encrypt Windows and Linux devices, as well as VMware instances.

Inhibit System Recovery (T1490)
- LockBit deletes OS features that enable the recovery of corrupted systems, like backup, shadow copies, and automatic repair.

Service Stop (T1489)
- LockBit inhibits critical services on a system to render those services unavailable to legitimate users. LockBit terminates processes and services.

Defacement: Internal Defacement (T1491.001)
- Affiliates change the host system's wallpaper and icons to the LockBit 3.0 wallpaper and icons. Attackers also display a ransom note and payment instructions on a victim's internal websites and desktop wallpapers.

Data Destruction (T1485)
- LockBit deletes log files and empties the recycle bin.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

APPENDIX A:

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 the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns 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%

APPENDIX B:

Traffic Light Protocol for Information Dissemination

TLP:RED

HOW IT IS 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.

HOW IT IS SHARED

Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP:AMBER

HOW IT IS USED

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 IT IS SHARED

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.

TLP:GREEN

HOW IT IS 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.

HOW IT IS SHARED

Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP:CLEAR

HOW IT IS USED

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 IT IS SHARED

Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

READY TO SEE FOR YOURSELF?

› Request a Demo:
Sign up on zerofox[.]com/request-a-demo

› Learn More:
Visit zerofox[.]com
Contact us at sales@zerofox[.]com / 855.736.1400