



| Assessment |

2024 Ransomware and Digital Extortion Overview

A-2025-01-08a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware and Digital Extortion, Deep and Dark Web, Threat Actor

January 8, 2025

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 January 8, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Assessment | 2024 Ransomware and Digital Extortion Overview

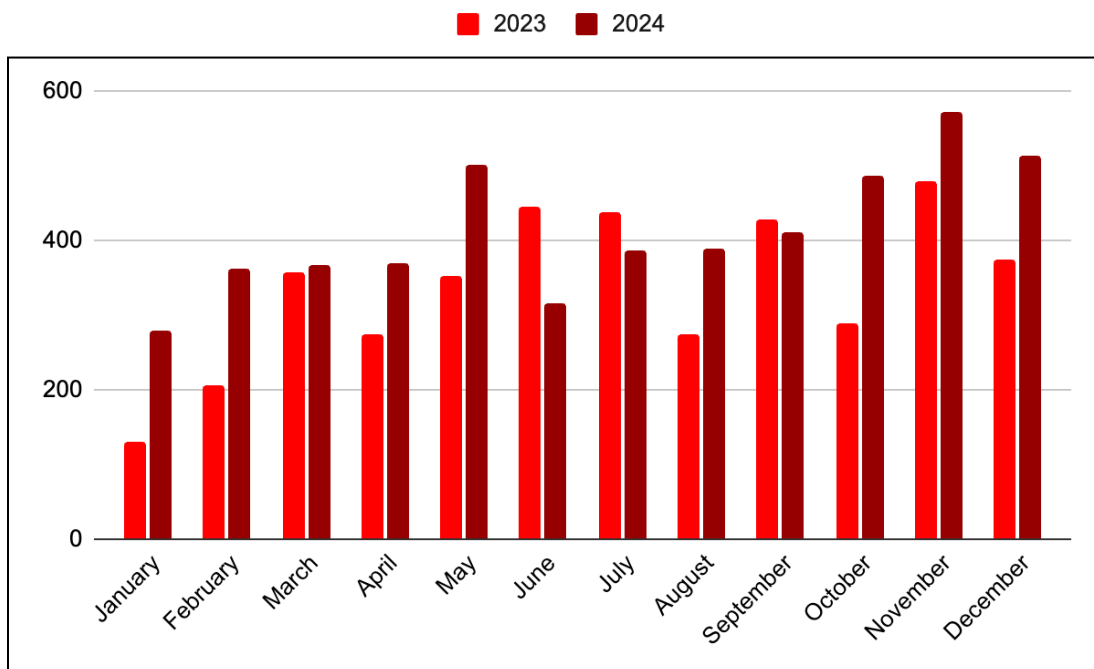
| Key Findings

- ZeroFox observed at least 4,950 separate ransomware and digital extortion (R&DE) incidents throughout 2024—significantly more than the approximately 4,000 incidents observed during 2023. As this total accounts primarily for incidents in which a victim has either failed to pay or remains in negotiations with the attackers, the true total is almost certainly significantly higher.
- LockBit, the most prominent threat actor collective in 2023, was responsible for a significantly lessened proportion of R&DE activity in 2024, owing to early-2024 law enforcement (LE) disruption operations.
- RansomHub very likely poses a greater threat to organizations across the globe than any other R&DE threat collective, having been the most prominent R&DE collective in 2024.
- ZeroFox identified 45 new R&DE collectives during 2024, compared to 35 during 2023. Many of these commenced operations, demonstrated consistency, and posed a prominent threat faster than that observed in previous years.

2024 Overview

The R&DE threat landscape underwent its most dynamic year in 2024, by a substantial margin. Q4 2023 and Q1 2024 LE operations disrupted any stability enjoyed by long-standing malicious actors and instilled a level of observable paranoia in deep and dark web (DDW) marketplaces that led to a shift in tactics, techniques, and procedures (TTPs). Many of the financially motivated collectives that contributed to 2023 being the most prolific and dangerous year for ransomware on record all but ceased operations, paving the way for an unprecedented tempo of new collectives that continue to showcase their proficiency faster than ever.

ZeroFox observed at least 4,950 separate R&DE incidents throughout 2024—significantly more than the approximately 4,000 incidents observed during 2023. As this total accounts primarily for incidents in which a victim has either failed to pay or remains in negotiations with the attackers, the true total is almost certainly significantly higher.

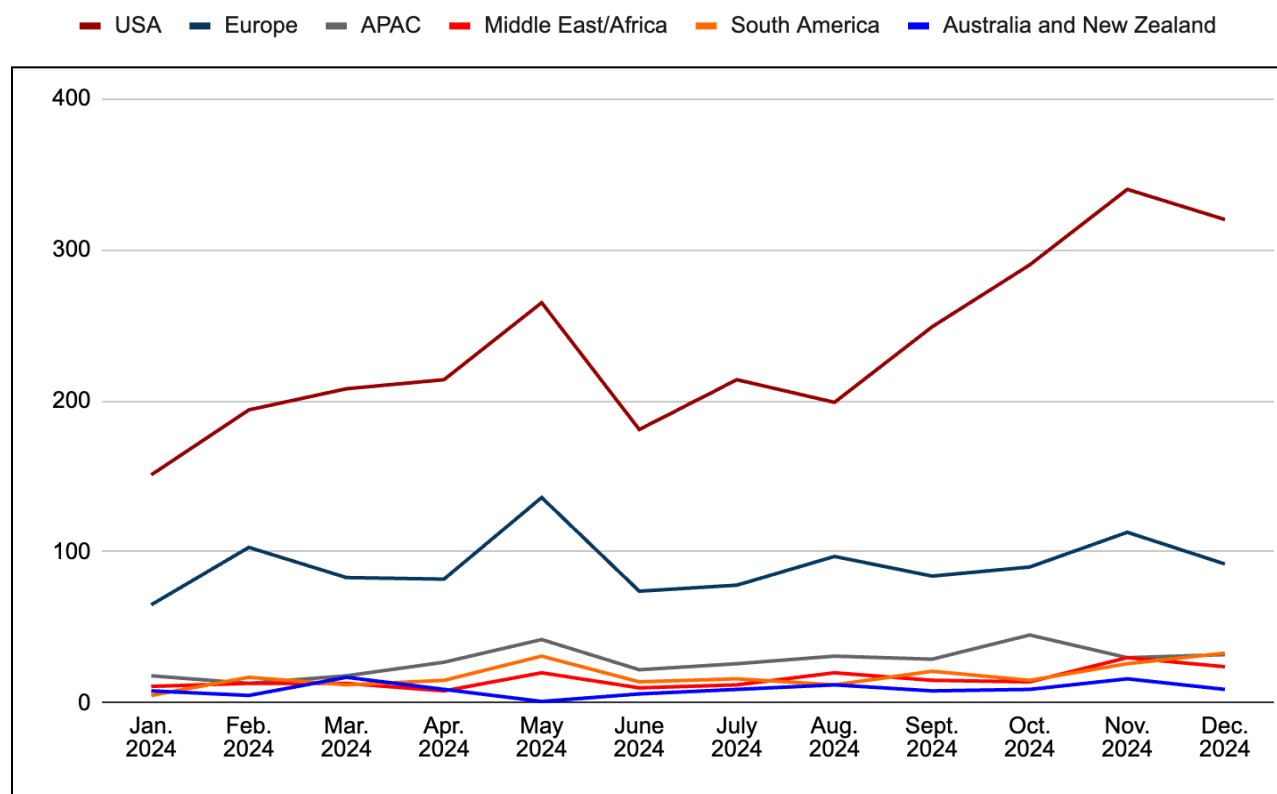


R&DE attacks by month (2023 compared to 2024)

Source: ZeroFox Intelligence

This continuously high attack tempo is in spite of a reduction of activity emanating from the prominent threat collectives that assisted in making 2023 the most prolific and dangerous year for R&DE—until 2024.

By the end of 2024, ALPHV/BlackCat had ceased operations, LockBit was exhibiting a significantly reduced attack tempo, and Cl0p—despite announcing an alleged compromise in late December—had conducted a fraction of its 2023 activity. These downward trajectories paved the way for an unprecedented tempo of new collectives that continue to showcase their proficiency faster than ever. Though the number of monthly incidents observed by ZeroFox during 2024 was largely stable, several threat collectives exhibited sharp upward trajectories.



R&DE targeting by region during 2024

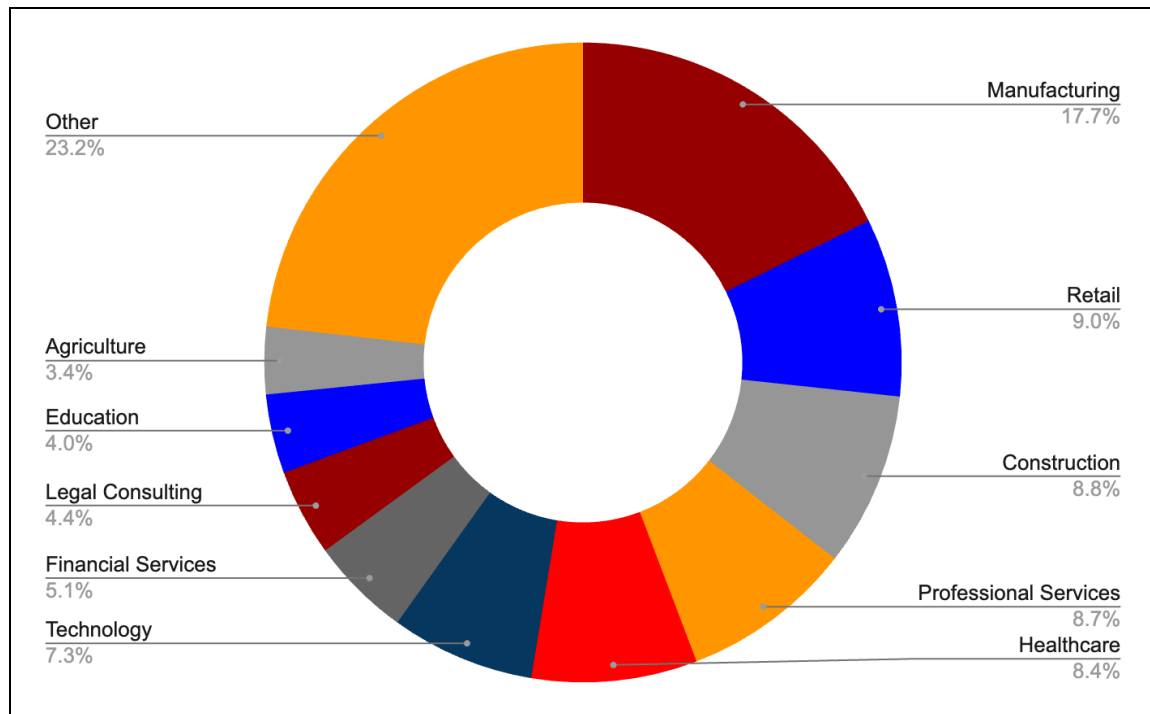
Source: ZeroFox Intelligence

North America was consistently the most-targeted region during 2024, accounting for an average of approximately 58 percent of global R&DE attacks. While this fluctuated by

month, it reflects the long-term trend of North America-based entities attracting an increasing proportion of global R&DE, alongside a slight proportional decline in the targeting of Europe, Asia-Pacific, Middle East and Africa, and South America-based entities.

R&DE collectives tend to target opportunistically, with patterns shaped most significantly by the network access that can be procured in DDW forums, and both the experience and preference of R&DE collective affiliates. However, North America is almost certainly perceived as a region comprising an abundance of lucrative, high-payoff potential targets. Others factors that influence targeting preferences include:

- The ideological affiliations of threat actors. Many R&DE threat actors are based in regions that are, to varying extents, opposed to “Western” geopolitics, international presence, and domestic activities. Targeting North America-based entities can therefore be perceived as both punitive and contributory to strategic state objectives.
- The perceived low risk of extradition and prosecution, despite comparably diligent and proactive cybersecurity practices, state security services, and international LE bodies. The increasingly widespread use of cryptocurrencies has also further enabled malicious activity, offering both anonymity and laundering options.
- Substantial digital attack surfaces, which continue to grow in size and complexity. This has been compounded in recent years by the rapid uptake and integration of technologies such as cloud networking services and internet of things (IoT) devices, as well as an increase in remote working arrangements.



Top 10 most-targeted Industries during 2024

Source: ZeroFox Intelligence

The manufacturing industry was the most-targeted industry in R&DE incidents during 2024, accounting for approximately 17.7 percent of attacks globally. This sector, alongside retail, construction, professional services, healthcare, and technology, has consistently been amongst the six most-targeted since as early as 2021.

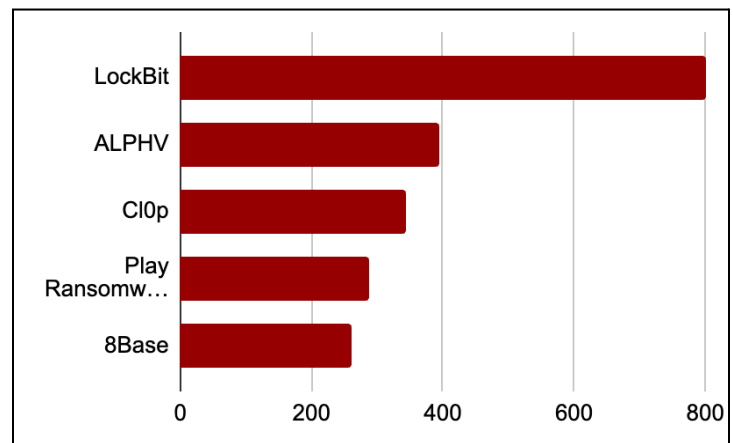
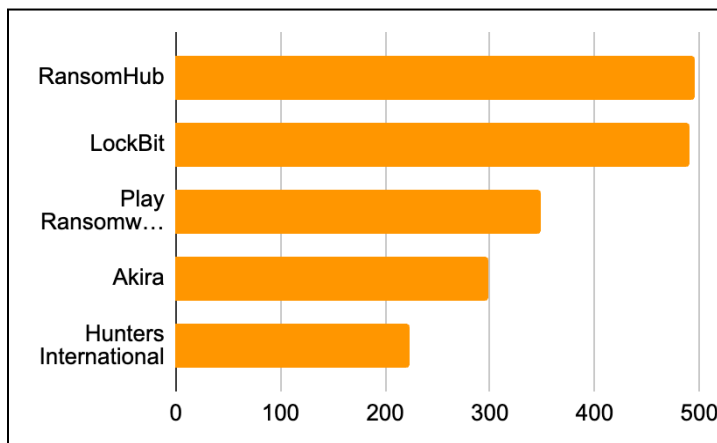
Much R&DE activity is opportunistic, with threat actors seeking and exploiting vulnerabilities across any organization using the affected software regardless of industry. A heavy reliance is also often placed upon initial access brokers (IABs), leading to extortion collectives leveraging any illicit network access that can be brokered. However, several industries are almost certainly prioritized by R&DE threat actors, largely due to the predicted profitability of a successful compromise. Factors likely contributing to the perception of a high-payoff industry include:

- A low tolerance for disrupted output or business downtime, leading to increased likelihood of extortion payment or negotiation.

- Low tolerance for damage to company branding, customer compromise, or undermined reputation.
- Prevalence of sensitive, proprietary, or customer data—particularly that which is protected by various legal frameworks.
- A generally widespread presence of legacy digital infrastructure and software, leading to an increased chance of gaining initial network access (often particularly prominent in publicly funded entities, even those whose output is considered critical).

Prominent Collectives

By the end of 2024, the greatest R&DE threat to organizations was posed by a largely different slate of collectives than seen at the same time in 2023 owing to the downfall of LockBit and ALPHV, a lack of any significant extortion campaigns by CI0p, and the notable efficacy of some newer outfits that arose in early 2024.¹



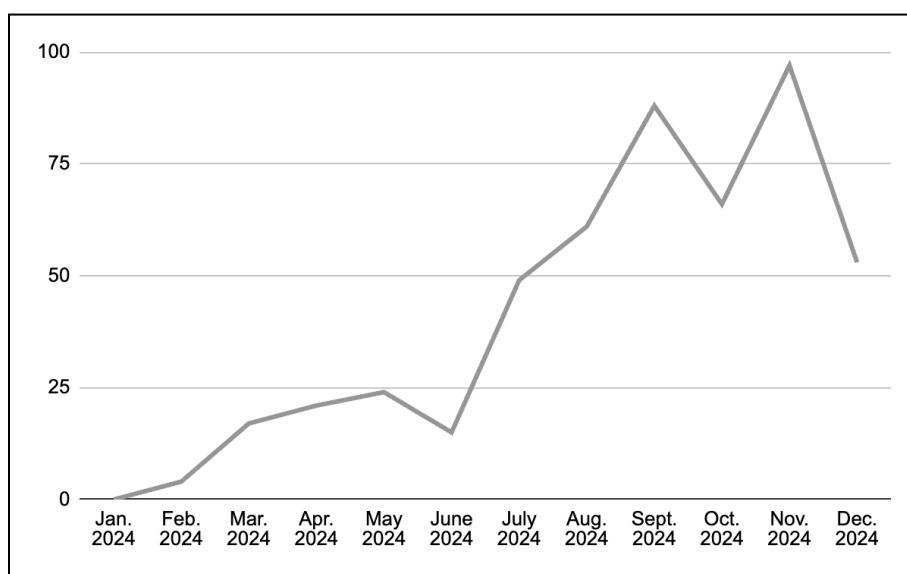
Top five most prominent R&DE collectives during 2024 (left) and 2023 (right)

Source: ZeroFox Intelligence

¹ In December 2024 CI0p claimed responsibility for a spate of data theft attacks leveraging vulnerabilities tracked as CVE-2024-50623 and CVE-2024-55956. The extent of the compromise is unclear as of the writing of this report, though there is a likely chance that victims will be named on the collective's leak site in early 2025.

RansomHub

As of the writing of this report, RansomHub very likely poses a greater threat to organizations across the globe than any other R&DE threat collective. Following the collective's initial observation in February 2024 (during which they conducted five attacks), RansomHub went on to exhibit a sharp upward trajectory in attack tempo. This peaked in November 2024, with at least 97 attacks, before reducing slightly in December 2024. RansomHub accounted for approximately 10 percent of all R&DE incidents ZeroFox observed throughout the year and conducted at least 216 attacks during Q4 2024.



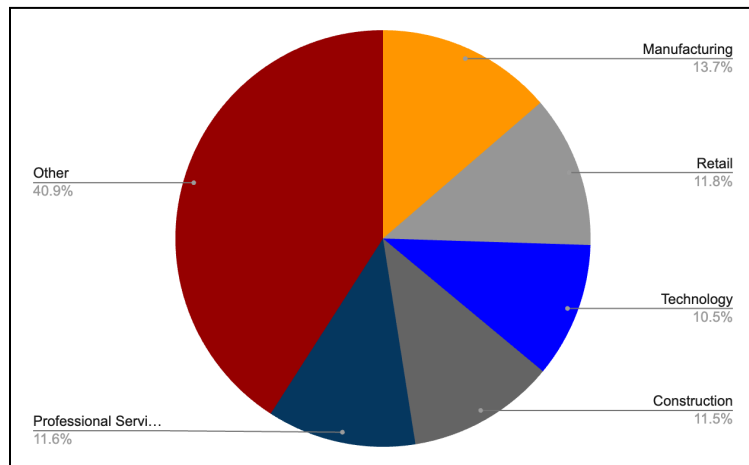
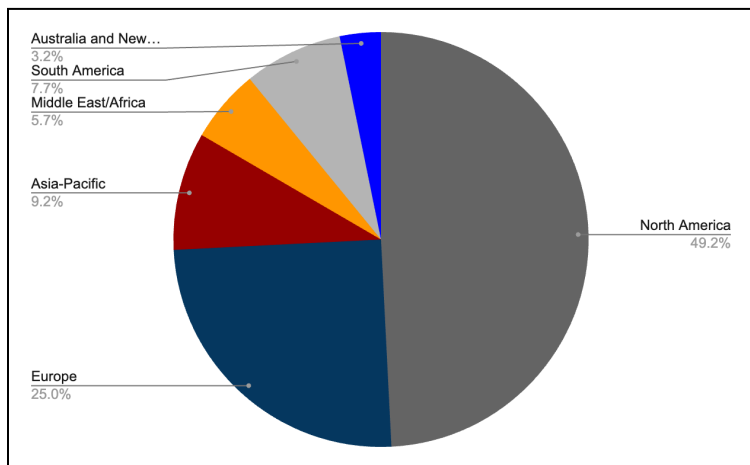
RansomHub attacks by month (2024)

Source: ZeroFox Intelligence

Payload source code overlaps have indicated there is a likely chance that RansomHub is a successor to the now-defunct extortion collective Knight, which was active between Q3 2023 and Q1 2024. The collective has also been associated with ALPHV, which initially exploited technology organization Change Healthcare in Q1 2024 before the organization was added to RansomHub's victim leak page in April 2024. This was very likely the result of affiliates who were subjected to an ALPHV exit scam moving to the RansomHub ransomware-as-a-service (RaaS).

RansomHub's notable 2024 success is the result of numerous factors:

- Unlike the vast majority of other RaaS operations, RansomHub pays its affiliates first, who then pay core members. Affiliates are also promised a 90 percent cut of any extortion funds—a highly competitive rate. This structure has very likely been successful in attracting competent affiliates—particularly from ALPHV, who may have been previously affected by exit scam activity.
- RansomHub malware has reportedly been observed being leveraged by other prominent, financially motivated collectives, such as Scattered Spider. Collaboration such as this very likely benefits RansomHub financially, as well as bolsters its reputation within DDW forums.²
- RansomHub has been observed evolving its toolset. In August 2024, the collective reportedly began deploying new malicious software designed to terminate endpoint detection and response processes before they can respond to the intrusion.³



RansomHub's most-targeted regions and industries (2024)

Source: ZeroFox Intelligence

There is a likely chance that RansomHub will remain the most prominent ransomware collective for the coming months and continue to attract affiliates. The collective will almost certainly continue to target a highly diverse array of sectors, and there is a roughly even chance that the proportion of attacks targeting organizations located in North America will increase.

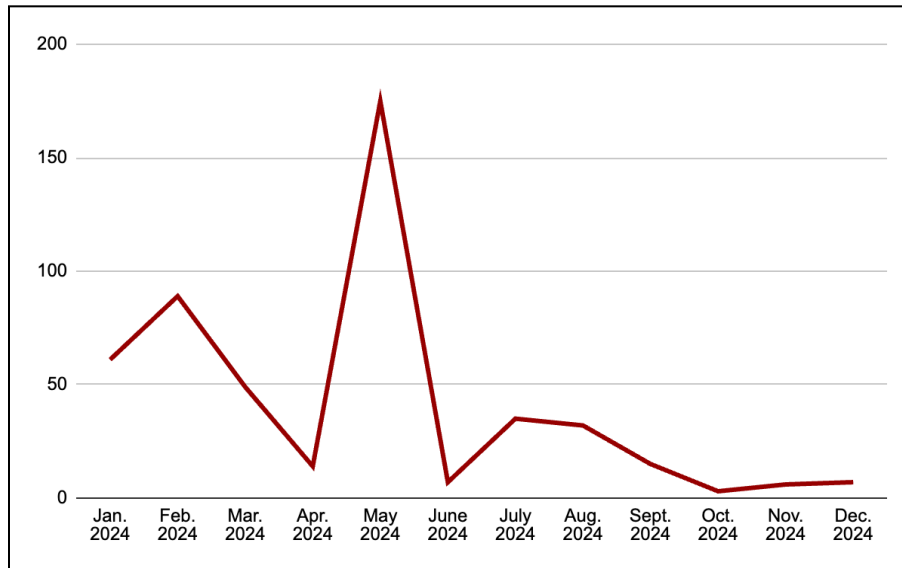
² [hXXps://thehackernews\[.\]com/2024/07/scattered-spider-adopts-ransomhub-and.html](https://thehackernews.com/2024/07/scattered-spider-adopts-ransomhub-and.html)

³ [hXXps://news.sophos\[.\]com/en-us/2024/08/14/edr-kill-shifter/](https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/)

LockBit

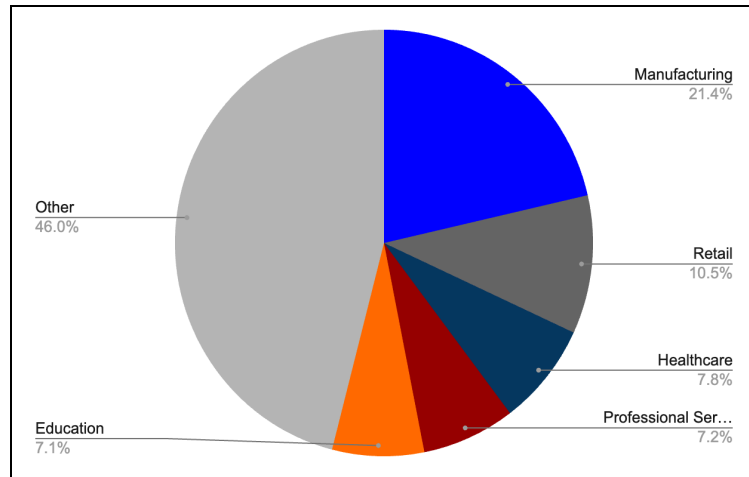
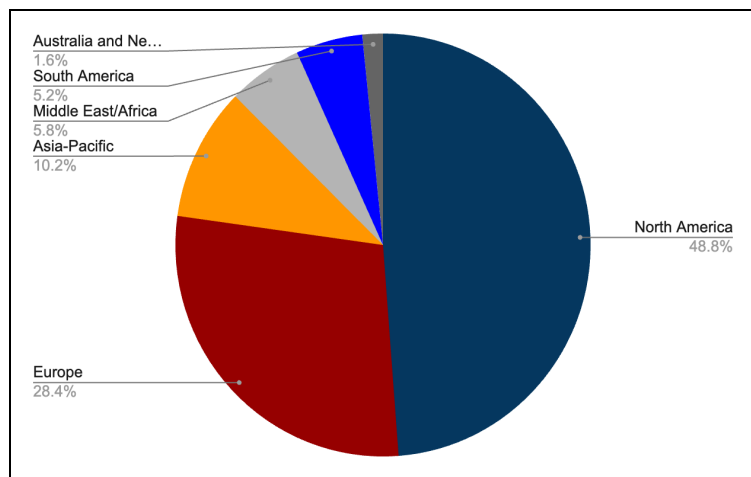
LockBit was the most prominent R&DE collective throughout 2023 by a significant margin, accounting for over 820 separate incidents and approximately 20 percent of global R&DE activity. However, in February 2024, the collective's prominence came to an end following LE operations targeting its digital infrastructure, personnel, and encryption software. LockBit has since been unable to maintain a steady attack tempo.

- Post-LE disruption, LockBit continued to upload victims to its leak site, with 175 additions observed in May 2024—indicative of a purported record-breaking month for the collective. However, this is very unlikely to reflect the collective's true current state of operations or the extent to which LE was able to disrupt its output.
- Throughout 2024, ZeroFox has observed numerous instances of victim entries being re-uploaded, updated, or refreshed—including those pertaining to older, already-exploited victims. This behavior is likely intended to inflate victim numbers, apply pressure to victims currently being extorted, and portray a facade of operational proficiency despite continued LE scrutiny.



LockBit attacks by month (2024)

Source: ZeroFox Intelligence



LockBit's most-targeted regions and industries (2024)

Source: ZeroFox Intelligence

During 2024, LockBit's regional and sector targeting contained examples of both proportional over- and under-targeting when compared to the wider R&DE threat landscape.

- LockBit has historically under-targeted North American-based entities by a substantial margin, instead prioritizing targets dispersed across the globe. This trend was on a slight trajectory to becoming less extreme before the collective's LE disruption.
- The manufacturing, retail, and healthcare sectors are among those most often targeted by LockBit, all of which are slightly proportionally over-targeted in comparison to the broader R&DE threat landscape.
- LockBit also over-targets the education and government sectors by a margin that is not negligible but is unlikely to be reflective of concerted efforts.

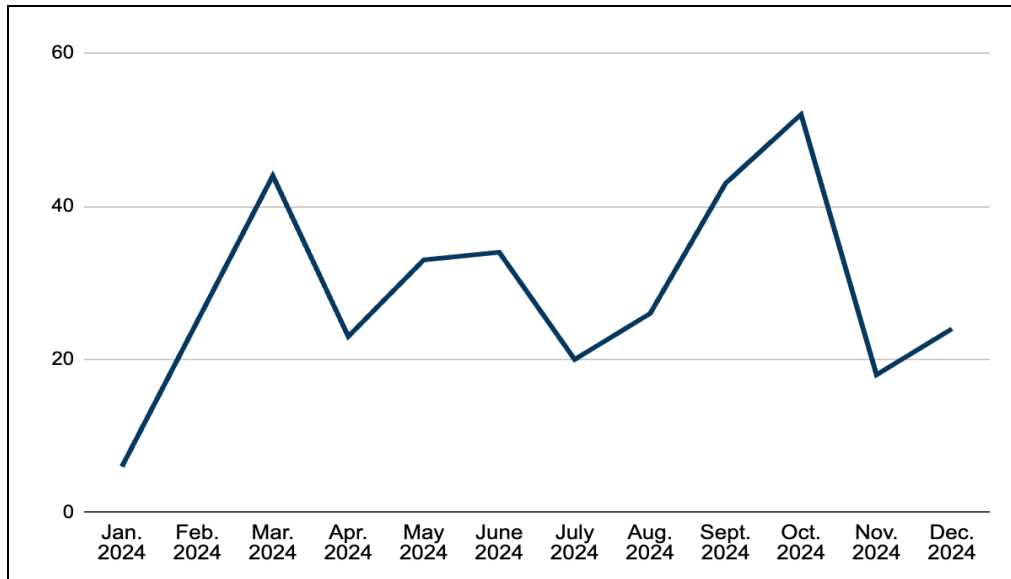
To some extent, LockBit has likely retained the expertise, reputation, and digital infrastructure needed to both continue pursuing stabilization and maintain a threat to global organizations. However, global LE entities have displayed an interest in the continued disruption of LockBit, rendering recovery efforts less likely to succeed. In Q4 2024, LockBit accounted for just one percent of global R&DE, while also displaying irregularities within targeted sectors. This is very likely indicative of a collective struggling

to maintain operational tempo and enact its tried and tested TTPs. In the following weeks and months, there is a roughly even chance that the threat from LockBit will increase.

Play Ransomware

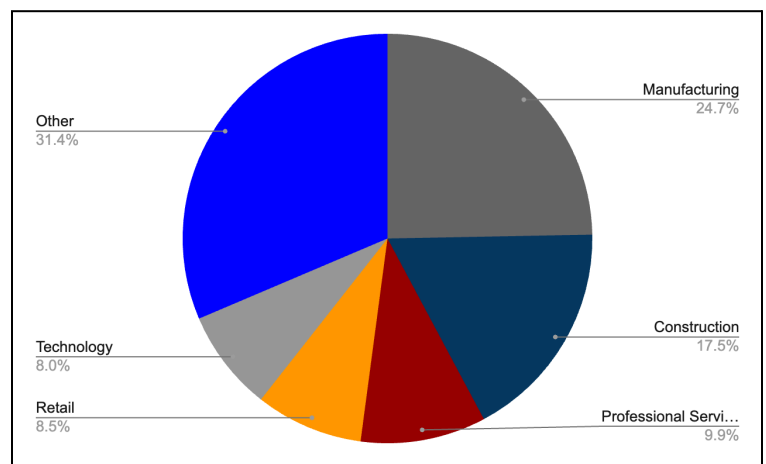
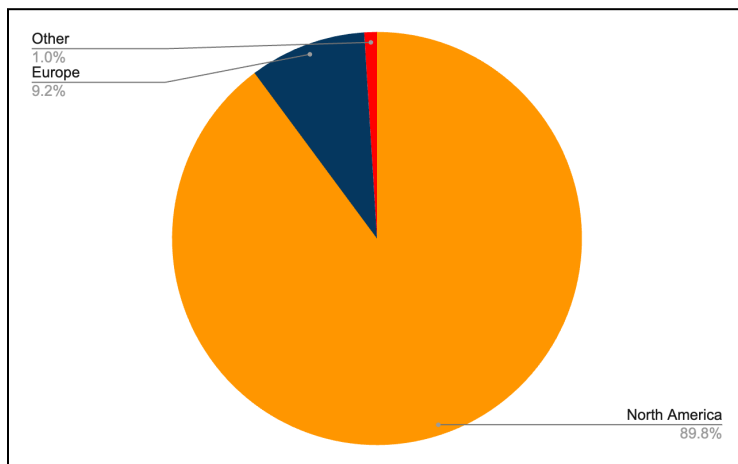
Play Ransomware posed a largely consistent threat to organizations throughout 2024, despite significant spikes and reductions in monthly activity. First observed in approximately November 2022, Play Ransomware has since conducted an average of 30 attacks per month, peaking in October 2024 with at least 52 attacks.

- Play Ransomware targets North America-based organizations almost exclusively. During 2024, approximately 89.9 percent of the collective's victims were based in this region—significantly more than the global R&DE average of approximately 58.5 percent. This is very likely reflective of established TTPs centered around the targeting of regions deemed more likely to pay larger ransoms. It is unlikely that this proportion will continue to grow, as this would require the dismissal of potentially lucrative, opportunistic targets—which is unlikely for a financially motivated collective.
- During 2024, Play Ransomware proportionally over-targeted by a large margin the manufacturing industry, which accounted for approximately 24.7 percent of victims, and the construction industry, which accounted for approximately 17.5 percent of victims. The retail and professional services industries were also proportionally over-targeted, but by lesser margins.



Play Ransomware attacks by month (2024)

Source: ZeroFox Intelligence



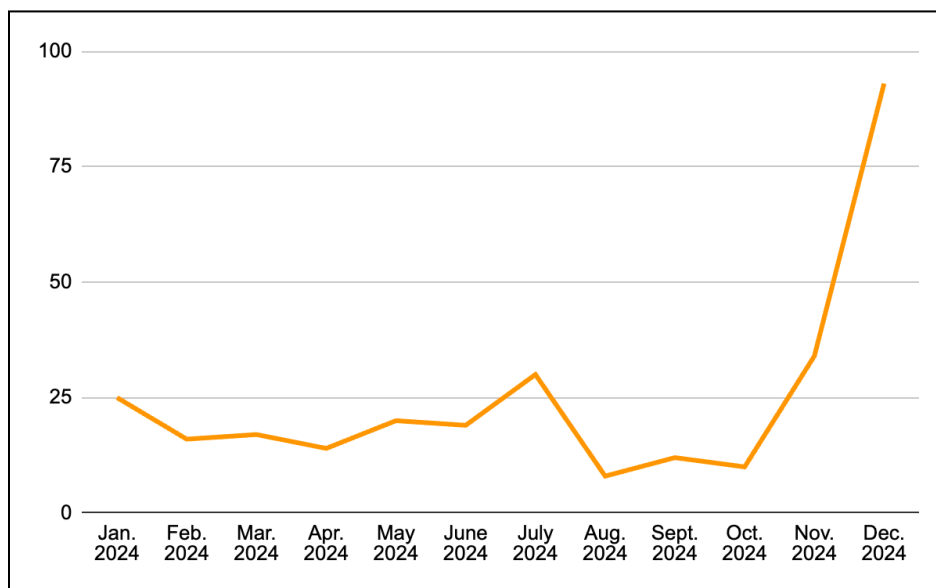
Play Ransomware's most-targeted regions and industries (2024)

Source: ZeroFox Intelligence

Akira

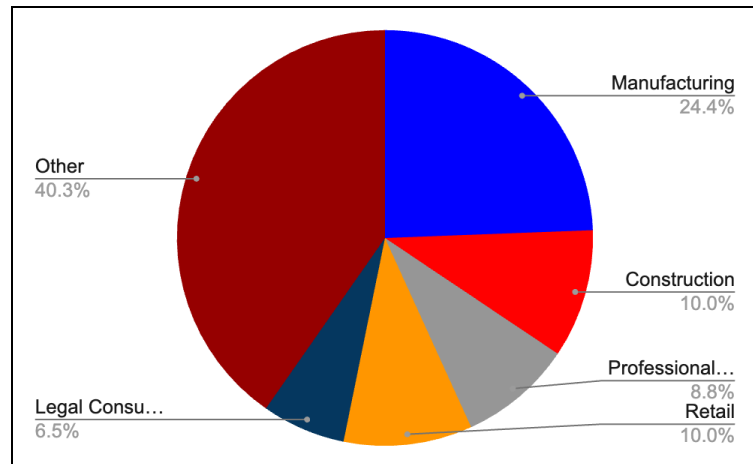
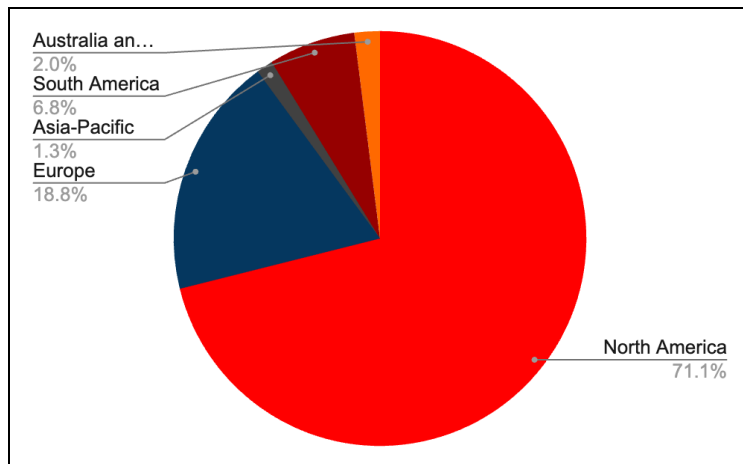
Akira, first observed in approximately March 2023, averaged 19 attacks per month between January 2024 and November 2024. However, in December, the collective added at least 93 separate victims to their leak site, bringing their 2024 monthly average up to approximately 25. This resulted in Akira being the second most dangerous R&DE threat collective of Q4 2024, and the fourth most dangerous collective of the year. It is very likely that Akira will continue to demonstrate a steady tempo of attacks through early 2025, though the activity levels observed in Q4 2024 are unlikely to sustain.

- Like Play Ransomware, Akira targets North America-based organizations at a far higher rate than observed across the R&DE global threat landscape. Throughout 2024, approximately 71 percent of Akira's victims were based in the region, rising to approximately 81 percent in Q4 2024.
- Akira's targeted industries are largely in-line with the R&DE global threat landscape, though manufacturing is slightly over-targeted and healthcare is slightly under-targeted. These discrepancies are negligible and unlikely to reflect a concerted strategy.



Akira attacks by month (2024)

Source: ZeroFox Intelligence

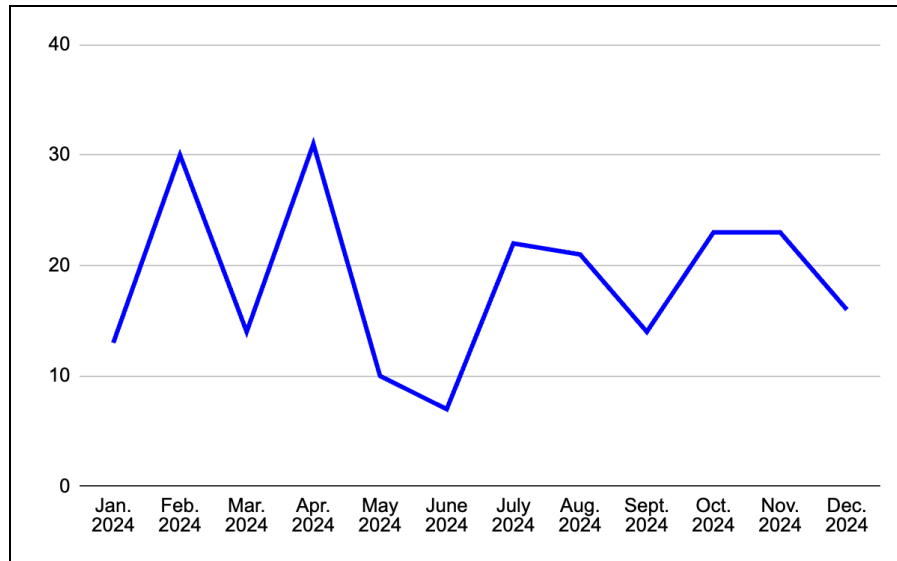


Akira's most-targeted regions and industries (2024)

Source: ZeroFox Intelligence

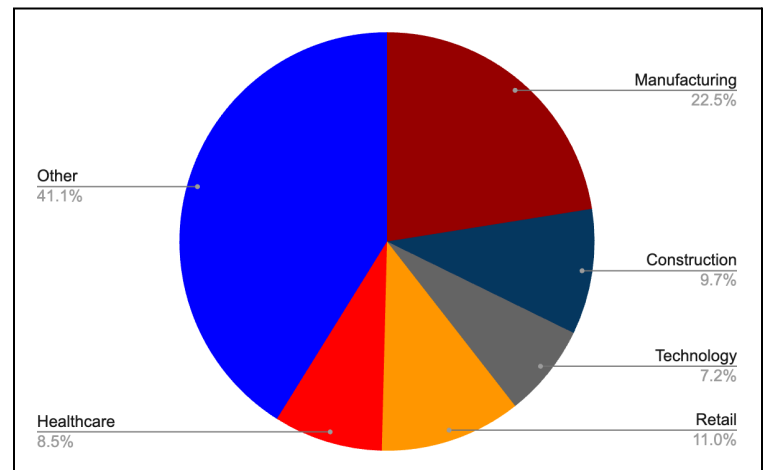
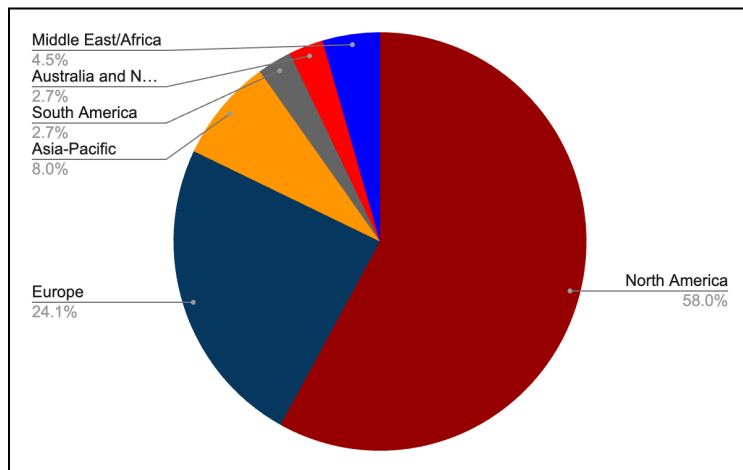
Hunters International

Hunters International, first observed in approximately October 2023, maintained a steady attack tempo throughout the year that was absent of notable spikes or reductions and averaged 19 incidents per month. Both the collective's targeted regions and industries are largely in-line with that observed from the global R&DE threat landscape, with no significant abnormalities noted.



Hunters International attacks by month (2024)

Source: ZeroFox Intelligence



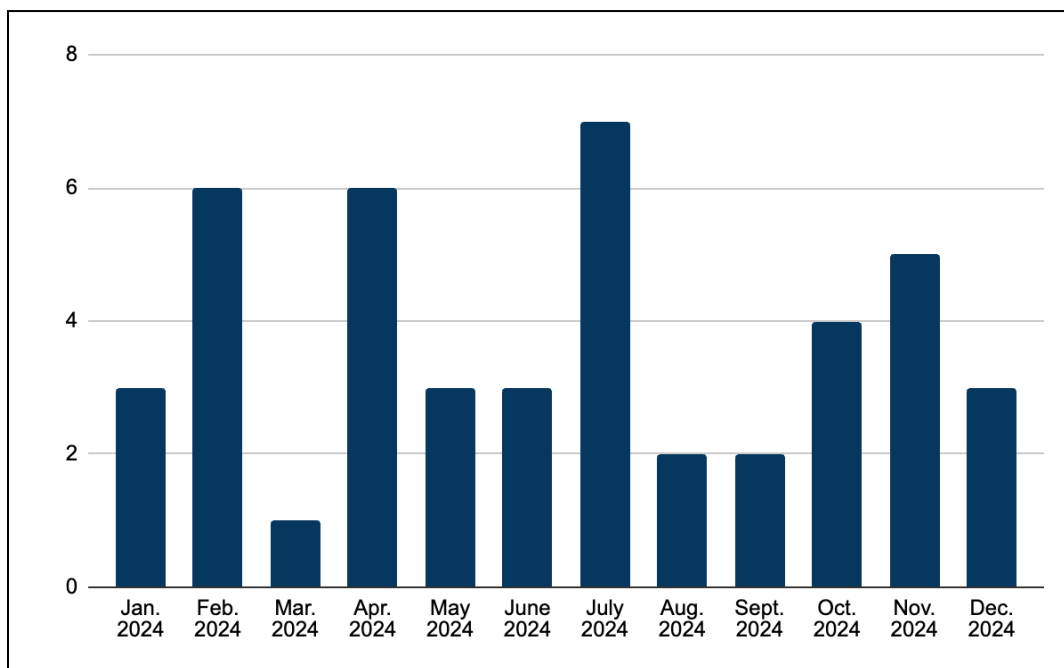
Hunters International most-targeted regions and industries (2024)

Source: ZeroFox Intelligence

Landscape Diversification

ZeroFox identified 45 new R&DE collectives during 2024, compared to 35 in 2023. Many of these commenced operations, demonstrated consistency, and posed a prominent threat faster than that observed in previous years. This led to:

- 2024 seeing the highest number of observed R&DE collectives on record, despite the downfall of 2023's two most prominent outfits, LockBit and ALPHV, and the subsequent uncertainty that plagued many DDW marketplaces.
- The R&DE threat landscape is now more diverse than ever. During 2023, 50 percent of global R&DE incidents were attributed to just five collectives, and 75 percent of incidents could be attributed to 14 collectives. However, during 2024, 50 percent of global R&DE incidents were attributed to eight collectives, with 20 collectives responsible for 75 percent of global incidents.



Number of new R&DE collectives observed by ZeroFox (2024)

Source: ZeroFox Intelligence

ZeroFox previously reported that LE operations were very likely a key contributing factor in this diversification, resulting in a sudden influx of experienced ransomware affiliates that required an RaaS operation with which to work as well as others seizing on the perceived

vacancy left by ALPHV and, to an extent, LockBit.⁴ Another likely factor is the continued professionalization of DDW marketplaces and RaaS offerings, leading to more accessible and higher-payoff services.

There is a likely chance that Q1 2025 will comprise a slight reduction in R&DE activity compared to Q4 2024, as observed in previous years. However, 2025 will very likely be a prolific year for digital extortion, as 2024's prominent threat collectives continue to establish continuity, attract affiliates, and leverage the services offered by increasingly professionalized DDW forums, services, and marketplaces. North America is almost certain to remain the most frequently targeted region, with the manufacturing, retail, construction, professional services, and healthcare industries likely to continue being perceived as the most lucrative targets.

Both new and existing collectives will almost certainly continue to test new TTPs during 2025, such as an increased emphasis on data extraction over traditional encryption methods and opting for double or triple extortion tactics in a bid to increase the chance of ransom demands being met.

⁴ <https://www.zerofox.com/blog/ransomware-threat-landscape-continues-to-diversify-in-2024/>

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 multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of R&DE threats and their associated 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 DDW 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%