



| Flash |

Ransomware Incidents Reach Record High in Q1 2025

F-2025-04-24a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

April 24, 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 09:00 AM EDT on April 24, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

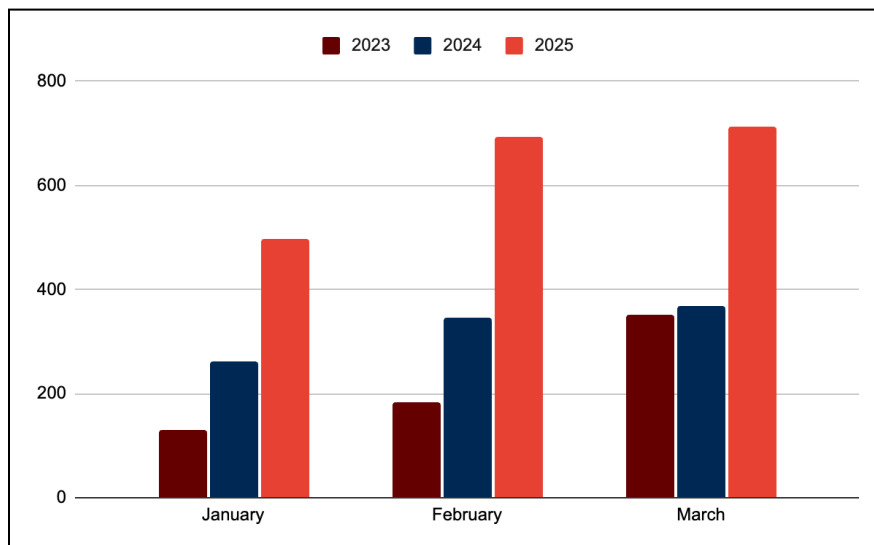
| Flash | Ransomware Incidents Reach Record High in Q1 2025

| Key Findings

- ZeroFox observed at least 1,961 separate ransomware and digital extortion (R&DE) incidents during the first three months of 2025, a significantly higher total than that observed during any previous three-month period.
- North America-based entities were the most targeted by a significant proportion, accounting for approximately 65 percent of incidents—slightly higher than the average of 58 percent observed throughout 2024.
- Organizations in the manufacturing industry were targeted by more R&DE incidents during Q1 2025 than those in other industries, a trend that has continued since at least 2021.
- The most active R&DE collectives during the first three months of 2025 were almost certainly ClOp, RansomHub, Akira, Lynx, and Qilin. This is a notably different picture to that from the final quarter of 2024, with only two out of five of the same collectives appearing in both lists.

Q1 2025 Overview

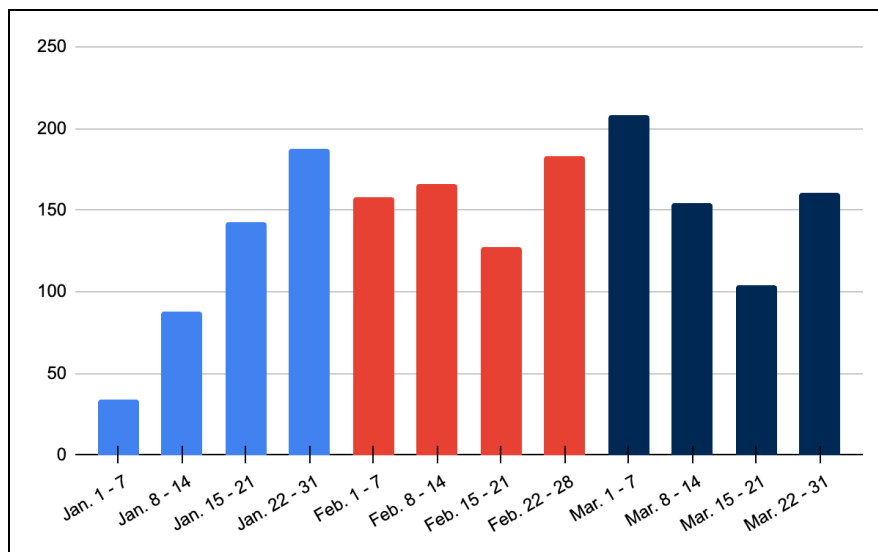
ZeroFox observed at least 1,961 separate R&DE incidents during the first three months of 2025, a significantly higher total than that observed during any previous three-month period, and even higher than the already record-breaking 1561 incidents of 2024's last quarter. This high attack tempo was also notably exhibited during the initial months of the year, a period that has typically and historically been composed of a lower number of incidents than subsequent months. This high number of attacks reflects a longer-term upward trajectory of R&DE incidents observed across regions and industries, which gained traction in May 2024 and continues as of the writing of this report.



Q1 R&DE incidents 2023-2025

Source: ZeroFox Intelligence

Regional targeting patterns in the first quarter of 2025 were largely consistent with previous months. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 65 percent of incidents—an increase from the 58 percent average observed throughout 2024. This uptick continues a trend observed since as early as 2022, whereby North America-based entities account for a steadily-increasing proportion of R&DE victims.



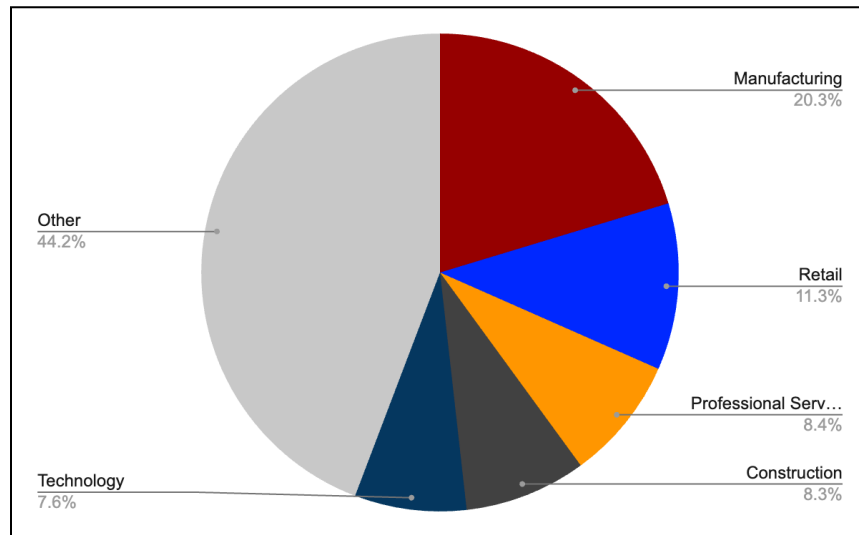
Q1 R&DE incidents by week

Source: ZeroFox Intelligence

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

- The disproportionate targeting of North America-based entities can be partly attributed to the geopolitical motivations and ideological beliefs of financially motivated threat collectives, fueled by opposition to “Western” political and social narratives.
- There is a likely chance that some financially motivated threat collectives have been emboldened by the low risk of extradition, particularly given currently-reduced international law enforcement collaboration taking place between the U.S. and Russia.
- North America hosts a wide variety of robust industries that comprise substantial and fast-growing digital attack surfaces. The widespread integration of technologies like cloud networking services and internet of things (IoT) devices contributes to the accessibility of North American assets. Additionally, while U.S.

federal employees have mostly returned to working in the office, other sectors have increased remote working arrangements.



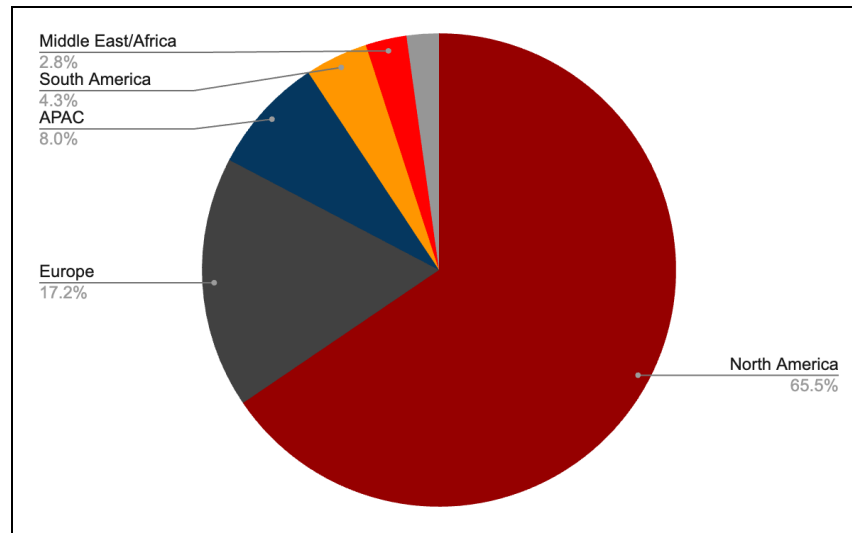
R&DE targeting by region, Q1 2025

Source: ZeroFox Intelligence

Organizations in the manufacturing industry were targeted by more R&DE incidents during Q1 2025 than those in other industries, a trend that has been observed since at least 2021. Approximately 20.3 percent of all incidents targeted entities in the manufacturing industry during Q1 2025, a slight increase from the 17.7 percent observed throughout the previous year.

- Organizations within the manufacturing sector are very likely often considered high-reward targets by R&DE collectives, due to factors such as low tolerance for business downtime and the widespread use of potentially-vulnerable operational technology (OT) infrastructure behind automation efforts.

Other industries heavily targeted during Q1 2025 include retail, professional services, construction, and technology, which together with manufacturing accounted for approximately 55 percent of all incidents. These industries were also the most targeted during 2024, demonstrating relatively consistent targeting patterns.



Top five most-targeted industries, Q1 2025

Source: ZeroFox Intelligence

Some other sectors and industries, although targeted less frequently, experienced a slight increase in the proportion of R&DE incidents they were subjected to in the first three months of 2025 compared to 2024.

- The proportion of attacks targeting healthcare organizations globally increased from seven percent to eight percent. While a small difference, this increase is notable due to the sector's general criticality as well as such organizations being "off limits" to many R&DE affiliates.
- The proportion of attacks targeting organizations in the logistics sector increased from approximately 2.6 percent to five percent—representing an almost two-fold increase. This was almost certainly contributed to primarily by the extortion collective CI0p, which heavily targets logistics organizations.

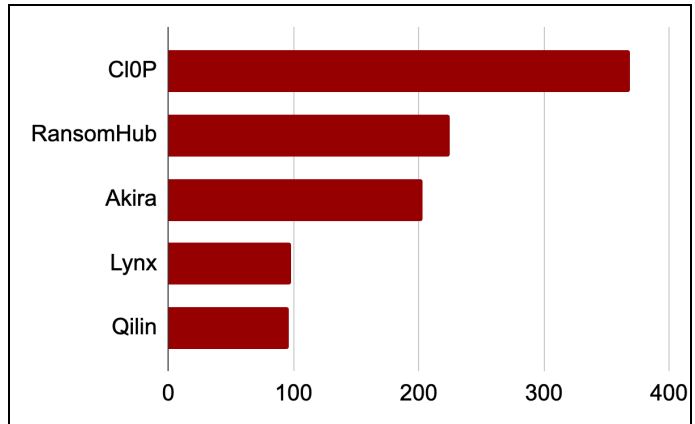
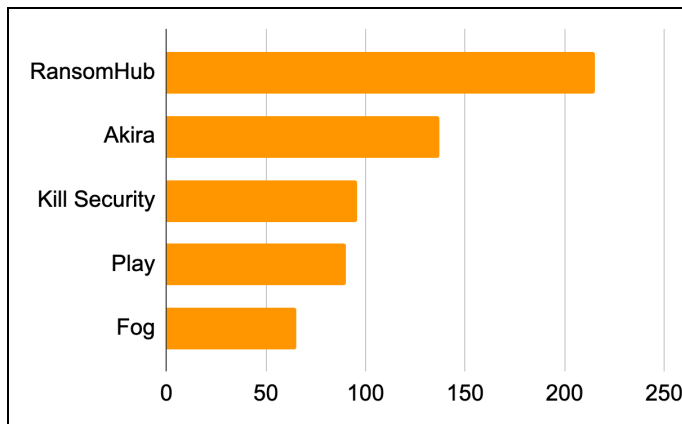
Prominent Collectives

The most active R&DE collectives during the first three months of 2025 were almost certainly CI0p, RansomHub, Akira, Lynx, and Qilin. This is a notably different picture from the final quarter of 2024, with only two out of five of the same collectives appearing in both lists.

Flash | Ransomware Incidents Reach Record High in Q1 2025

F-2025-04-24a

TLP: CLEAR



Top 5 most-prominent R&DE collectives during Q4 2024 (left) and Q1 2025 (right)

Source: ZeroFox Intelligence

CI0p

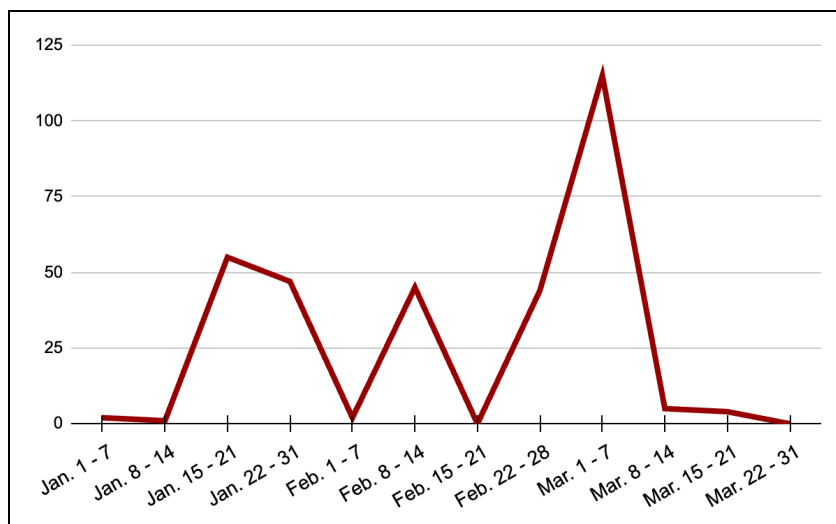
During the first three months of 2025, CI0p was responsible for at least 370 separate attacks, accounting for approximately 18.7 percent of all incidents, more than any other collective. This spike in activity followed a lull throughout Q4 2024 and an overall low-tempo year.

- In December 2024, CI0p compromised the secure managed file transfer (MFT) platform Cleo, leading to the subsequent exploitation of customer organizations that were added to the collective's victim leak site throughout Q1 2025.
- The alleged victims of this compromise were disproportionately associated with the supply chain and logistics industries and were primarily based in North America.

Flash | Ransomware Incidents Reach Record High in Q1 2025

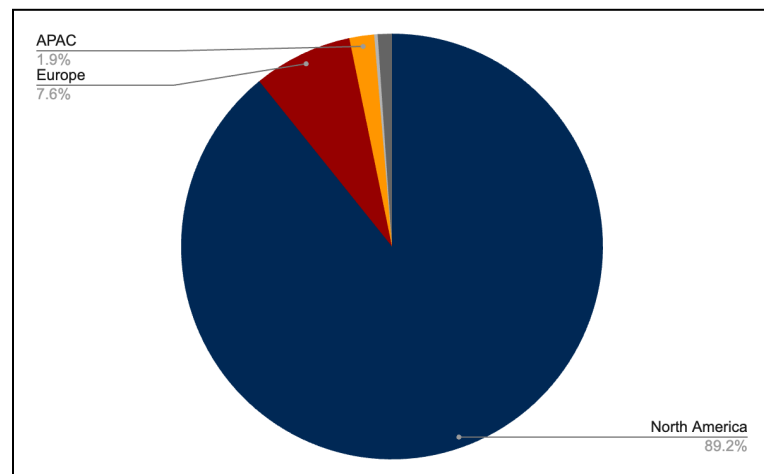
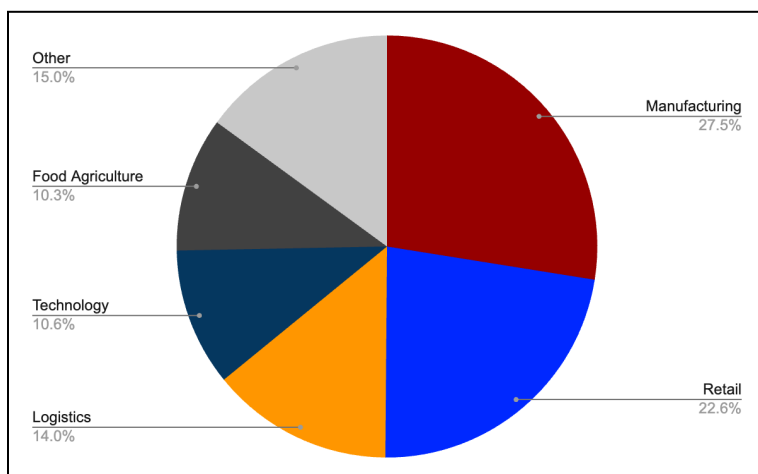
F-2025-04-24a

TLP: CLEAR



CI0p attacks by week, Q1 2025

Source: ZeroFox Intelligence



CI0p's most-targeted industries (left) and regions (right), Q1 2025

Source: ZeroFox Intelligence

During Q1 2025, CI0p disproportionately targeted North America-based organizations, which represented approximately 89 percent of the collective's victims—significantly higher than 65 percent observed across the broader threat landscape. This follows a longer-term trend exhibited by the collective of implicating North America-based organizations in large-scale MFT compromises.

In line with historical precedents, CI0p activity is very likely to decrease significantly in the coming weeks, prior to the collective's next successful extortion campaign.

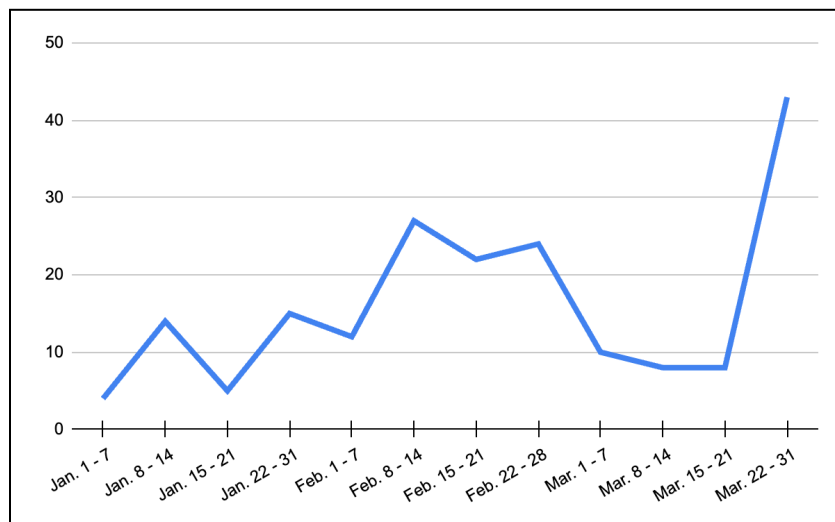
Flash | Ransomware Incidents Reach Record High in Q1 2025

F-2025-04-24a
TLP: CLEAR



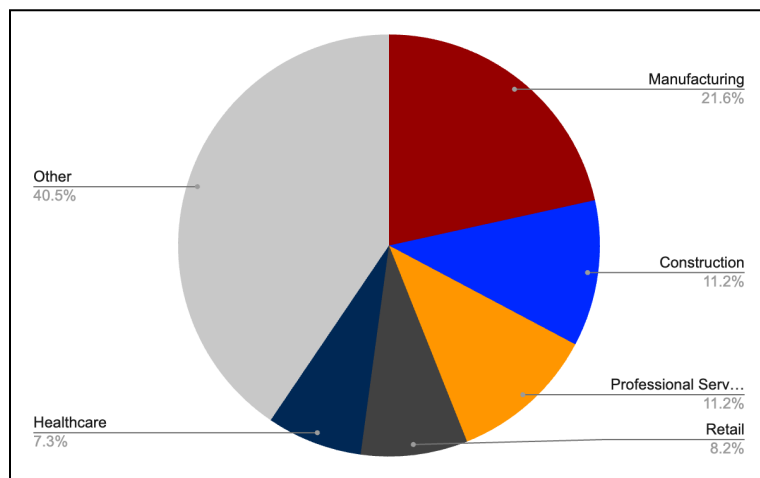
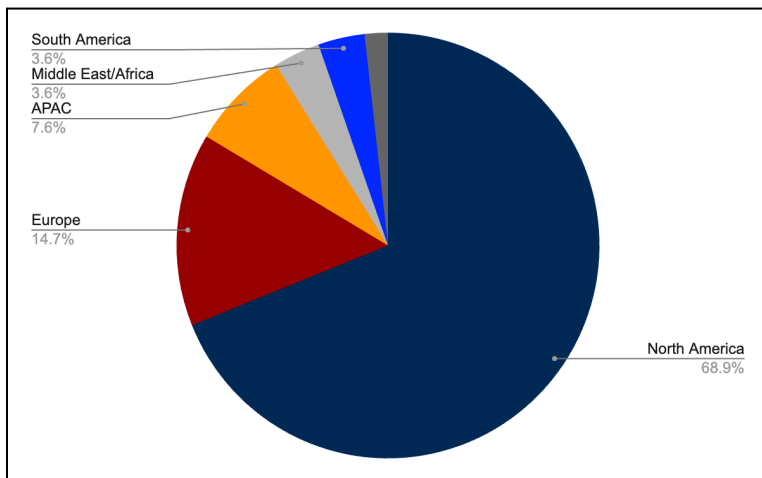
RansomHub

RansomHub has remained a prolific extortion collective since its initial observation in February 2024, responsible for at least 500 separate incidents throughout last year-equating to over ten percent of all R&DE activity. During Q1 2025, RansomHub conducted at least 225 attacks, more than any previously observed three-month period.



RansomHub attacks by week, Q1 2025

Source: ZeroFox Intelligence



RansomHub's most-targeted regions and industries, Q1 2025

Source: ZeroFox Intelligence

During Q1 2025, RansomHub's targeting by region was among the most diverse of any prominent R&DE collective, with slight proportional undertargeting of Europe-based organizations, and slight overtaking of organizations situated within the majority of other regions. The collective also remains broadly consistent with global averages in terms of industry targeting.

RansomHub, their dark web victim leak page, and their associated user account within deep web forums, became inactive in early April and remain inactive as of the writing of this report. Rumors within these forums suggest that the collective has become associated with another digital extortion outfit—DragonForce, though details remain unclear. RansomHub is very likely to stay non-operational during the coming weeks, posing a significantly reduced threat to organizations.

Akira

Akira, first observed in March 2023, averaged approximately 67 attacks per month during the first three months of 2025, a significant increase compared to the 25 attacks per month observed throughout the previous year. This uptick began in December 2024, when the collective uploaded approximately 93 victims to their dark web victim leak site—a higher total than in any other previous month. These totals resulted in Akira being the second-most prominent R&DE outfit of 2024 and the third most prominent of Q1 2025.

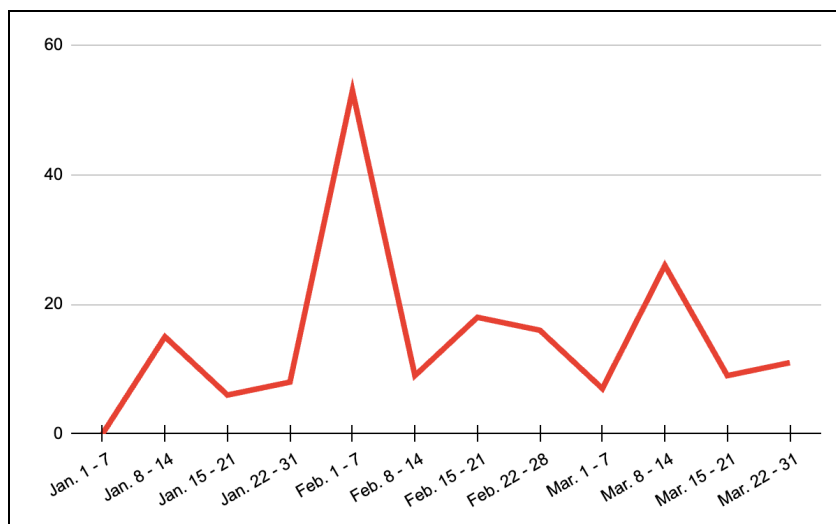
- In February 2025, Akira was responsible for more incidents than any other collective, with at least 96 incidents, having surpassed both Cl0p and Randomhub – the two top contributors to Q1 2025's R&DE landscape.
- This shift marks a departure from Akira's historically consistent, low-volume operations.

Historically, Akira has targeted North America-based organizations at a far higher rate than observed across the R&DE global threat landscape. Throughout Q1 2025, approximately 71 percent of Akira's victims were based in the region, rising to approximately 81 percent in Q4 2024. This dropped to 60 percent in Q1 2025; however, it coincided with the collective's significantly increased activity tempo, resulting in proportionally higher-than-average targeting of Europe and APAC-based entities.

Flash | Ransomware Incidents Reach Record High in Q1 2025

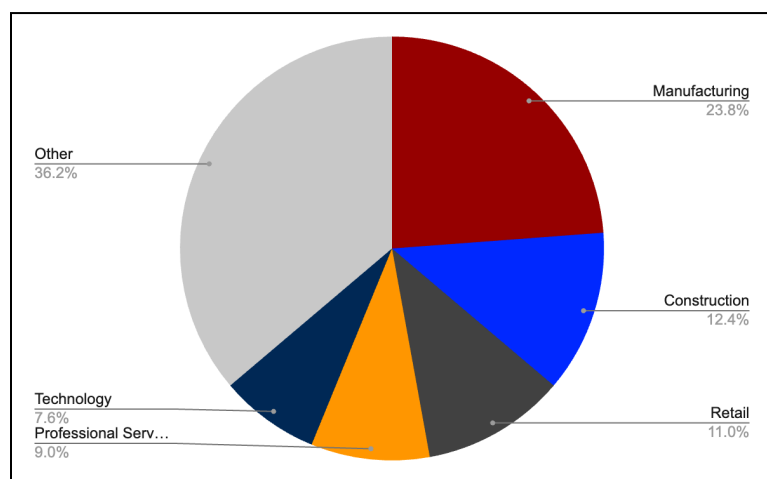
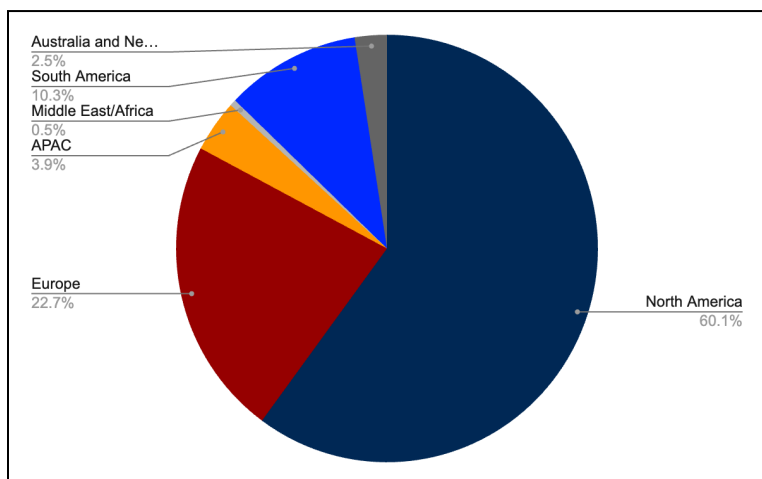
F-2025-04-24a

TLP: CLEAR



Akira attacks by week, Q1 2025

Source: ZeroFox Intelligence



Akira's most-targeted regions and industries, Q1 2025

Source: ZeroFox Intelligence

Akira's targeted industries are largely in line with the R&DE global threat landscape, though manufacturing is slightly overproportionate and healthcare is slightly under-targeted. These discrepancies are negligible and unlikely to reflect a concerted strategy.

Although the past two quarters have broken records for R&DE activity, the overall number of incidents has slightly declined as of the writing of this report. This reduction is

primarily due to RansomHub's inactivity and a slowdown in victim disclosures by CI0p. In contrast, several other collectives are gaining momentum—Qilin marked its most prolific month in April 2025, Play carried out at least 39 attacks during the same period, and DragonForce continues to operate at a steady pace.

| 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%