ZEROFOX INTELLIGENCE

Assessment

Q4 2025 Ransomware Wrap-Up

A-2026-01-15a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

January 15, 2026

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 7:00 AM EST on January 15, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

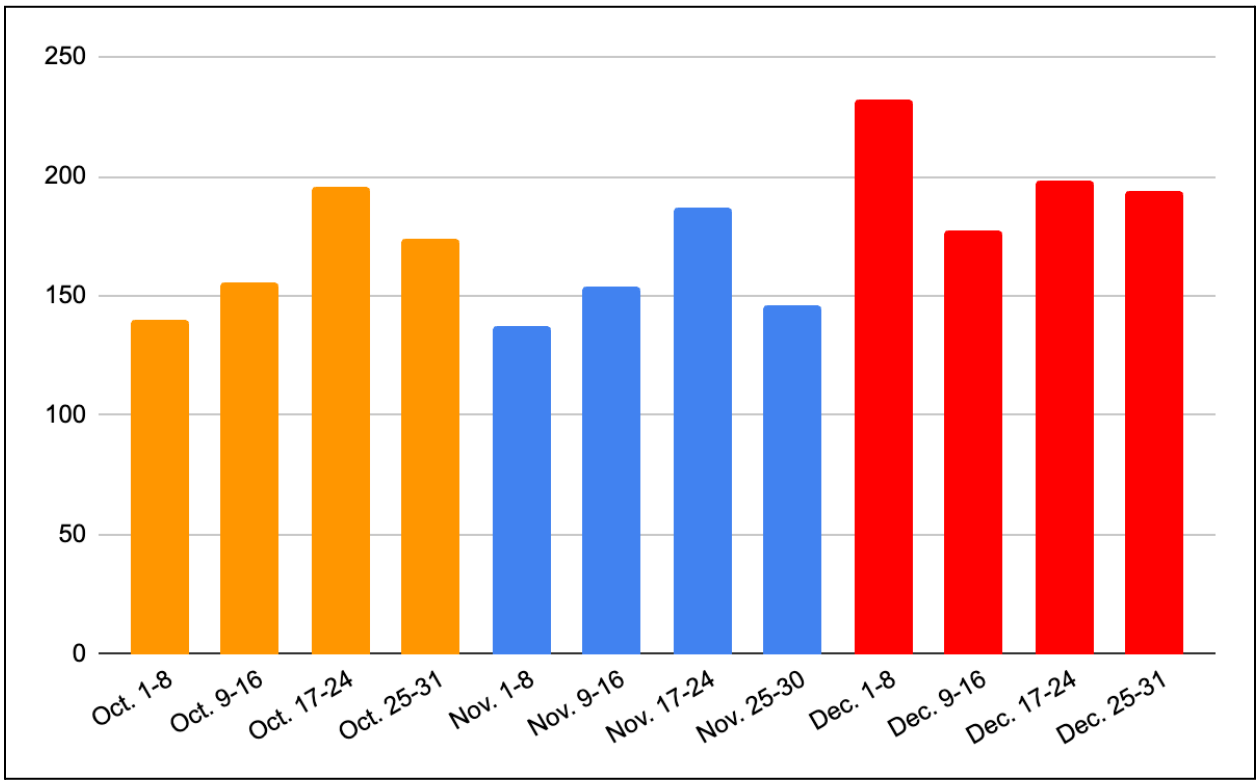
Assessment | Q4 2025 Ransomware Wrap-Up

Key Findings

- ZeroFox observed at least 2,091 separate ransomware and digital extortion (R&DE) incidents in Q4 2025, an increase of approximately 46 percent from Q3 and nearly 7 percent more than the record-breaking 1,961 incidents observed in Q1 2025.
- Throughout 2025, ZeroFox observed a higher number of attacks each quarter compared to previous years, reflecting a longer-term upward trajectory of R&DE incidents observed across regions and industries.
- Regional R&DE targeting patterns in Q4 2025 were largely consistent with those observed during previous months. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 59 percent of all incidents.
- ZeroFox observed that the five most active R&DE collectives in Q4 2025 were almost certainly Qilin, Akira, Sinobi, Cl0p, and LockBit. This is a change from Q3 2025—with only Qilin and Akira remaining in the top five from the previous quarter.

Q4 2025 Overview

ZeroFox observed at least 2,091 separate R&DE incidents in Q4 2025, an increase of approximately 46 percent from Q3 and nearly 7 percent more than the record-breaking 1,961 incidents observed in Q1 2025. Additionally, Q4 2025 marked an increase of incidents year-over-year from 2024 and 2023, which saw at least 1,556 and 1,143 incidents respectively.

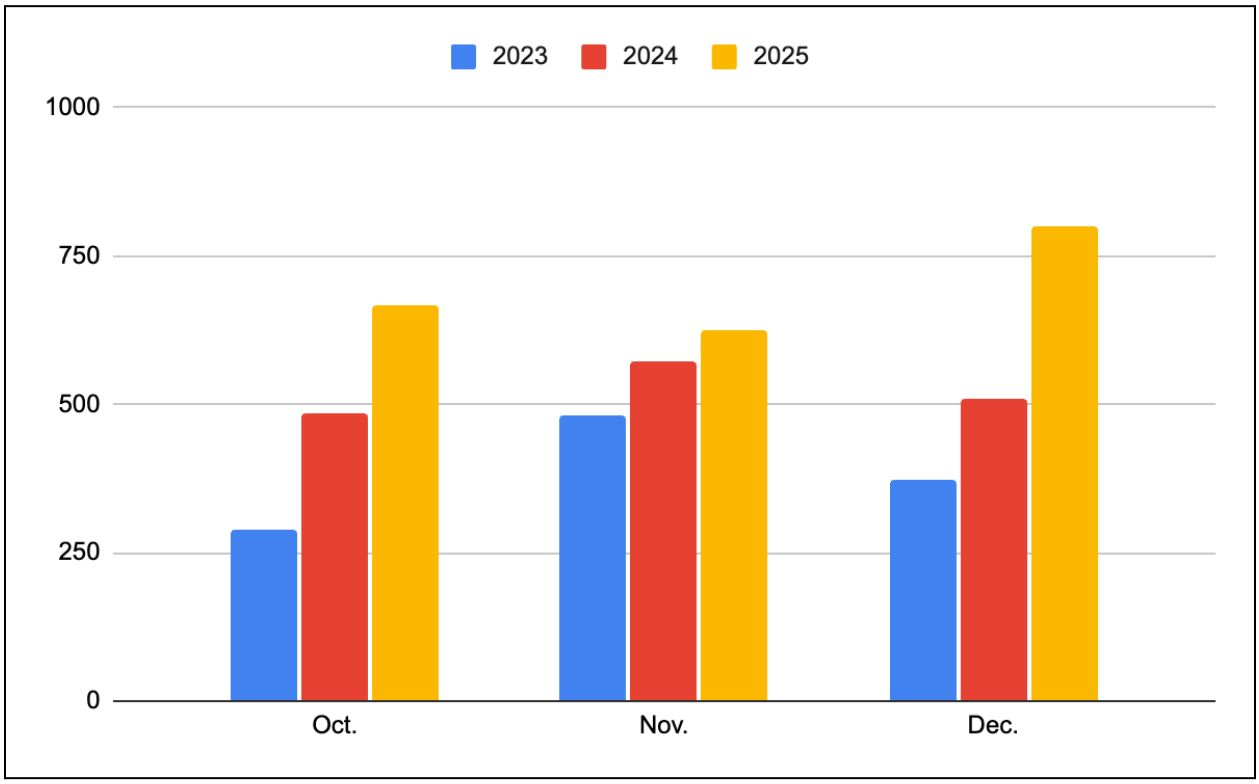


R&DE incidents by week in Q4 2025

Source: ZeroFox Intelligence

Throughout 2025, ZeroFox observed a higher number of attacks in each quarter compared to previous years, reflecting a longer-term upward trajectory of R&DE incidents observed across regions and industries that began in May 2024 and continues as of this writing. Historically, the last quarter of the year often sees the highest number of attacks, and a dip occurs in the first quarter of the next year; however, there is a roughly even chance that the 2025 trend will persist and that Q1 2026 will experience a relative spike in activity

October has seen sharp rises from 2023–2025, with at least 666 attacks in 2025. The average number of November incidents has risen steadily over the same period, with approximately 624 in November 2025, while December saw a sharp rise with approximately 801 attacks in 2025. December accounted for roughly 38 percent of all global ransomware attacks in Q4 2025.



Q4 R&DE incidents from 2023–2025

Source: ZeroFox Intelligence

Regional Trends

Regional R&DE targeting patterns in Q4 2025 were largely consistent with those observed during previous months. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 59 percent of all incidents; this is consistent with the 58 percent average observed throughout 2024 and identical to the 59 percent seen in Q3 2025.

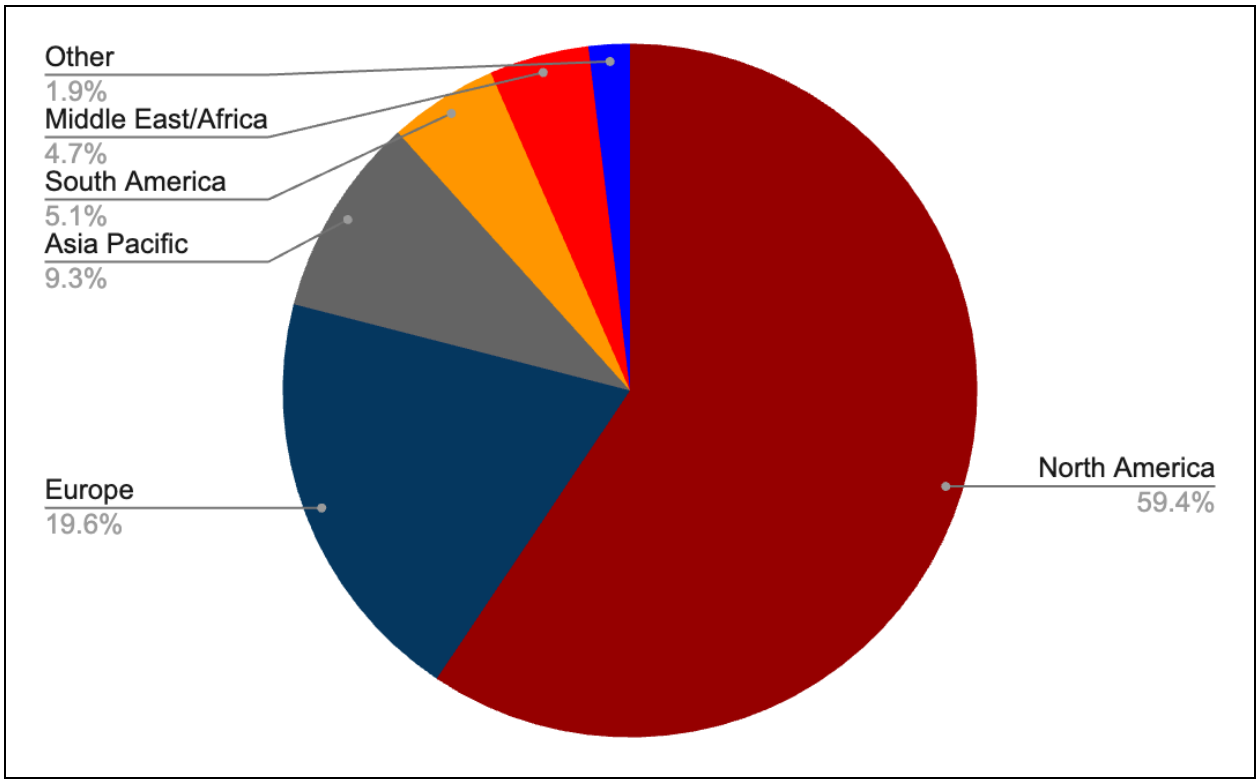
- At least 1,309 R&DE attacks targeted North-America based organizations in Q1 2025; the number dropped to 774 attacks in Q2 2025 and increased to 845 attacks

in Q3 2025 (a roughly 9.2 percent increase). In Q4 2025, North America-based organizations accounted for at least 1,239 attacks—roughly a 46 percent increase, but still 5 percent lower than the high of Q1 2025.

Europe-based organizations were the second most targeted region in Q4 2025, accounting for roughly 19 percent of all incidents; this is a slight decrease from the approximately 22 percent observed in Q3 2025. Together, North America and Europe-based organizations accounted for 78 percent of all R&DE incidents observed during Q3 2025, which is a 3 percent decrease from Q3 2025 but largely consistent with other quarters in 2025.

R&DE collectives typically operate opportunistically, with targeting patterns largely influenced by the availability of network access sold or advertised on deep and dark web forums. These patterns are further shaped by the technical capabilities and operational preferences of individual affiliate actors. Nevertheless, North America remains a consistently attractive region and is almost certainly viewed as a lucrative area for high pay-off potential targets.

- The disproportionate targeting of North America-based entities is likely partly attributed to the geopolitical motivations and ideological beliefs of financially motivated threat collectives fueled by opposition to “Western” political and social narratives.
- North America hosts a wide variety of robust industries that comprise substantial and fast-growing digital attack surfaces. The widespread integration of technologies such as cloud networking services and Internet of Things devices contributes to the accessibility of North American assets.



R&DE targeting by region in Q4 2025

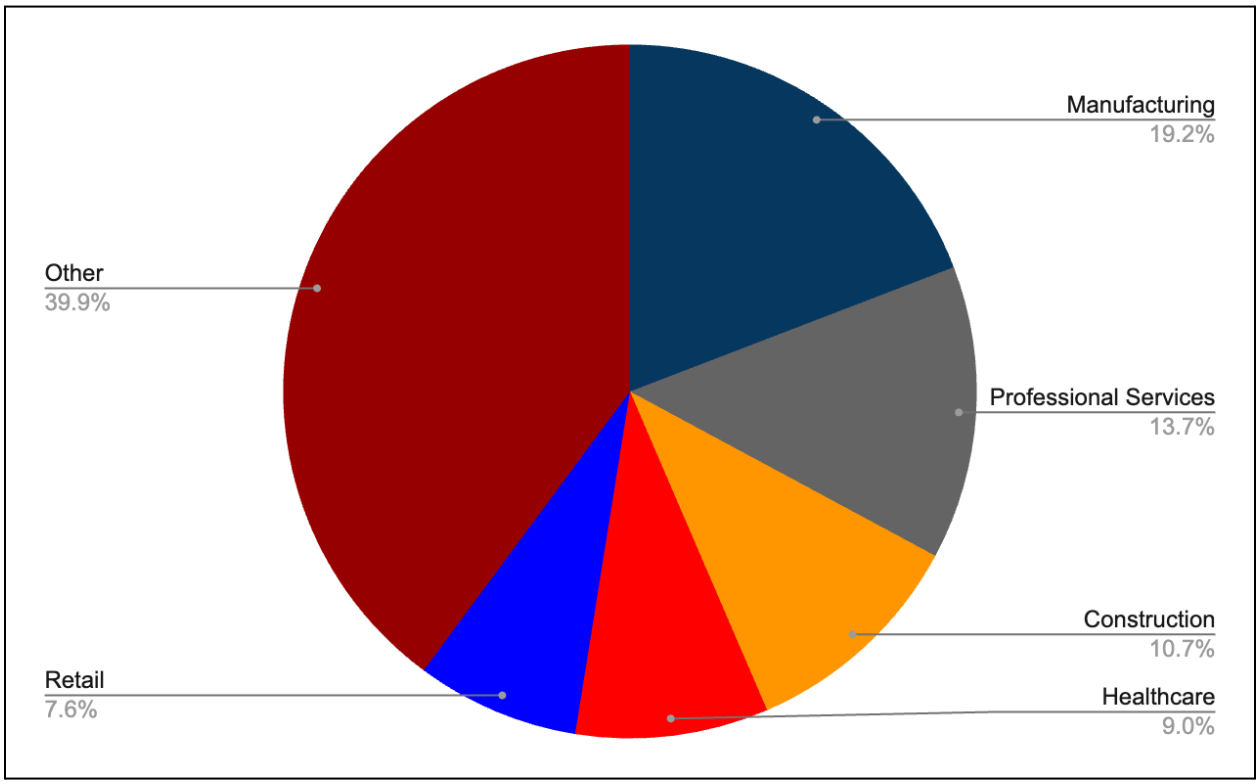
Source: ZeroFox Intelligence

Industry Trends

In Q4 2025, organizations in the manufacturing industry were targeted by a higher number of R&DE incidents than those in other industries, totaling at least 413 incidents (an increase of 69 percent from Q3 2025). Nearly 20 percent of all incidents targeted entities in the manufacturing industry in Q4 2025, an increase from the approximately 17 percent ZeroFox observed in Q3 2025. Manufacturing has consistently been the most targeted industry since at least 2021.

- In Q4 2025, organizations operating within the manufacturing industry continued to represent high-value targets for R&DE collectives. This sustained targeting is likely driven by factors such as low operational tolerance for downtime and the use of vulnerable operational technology infrastructure behind automation efforts.

- Heavily targeted industries in Q4 2025 include manufacturing, professional services, construction, healthcare, and retail; together, attacks on these industries accounted for approximately 60 percent of all incidents.



Most heavily targeted industries in Q4 2025

Source: ZeroFox Intelligence

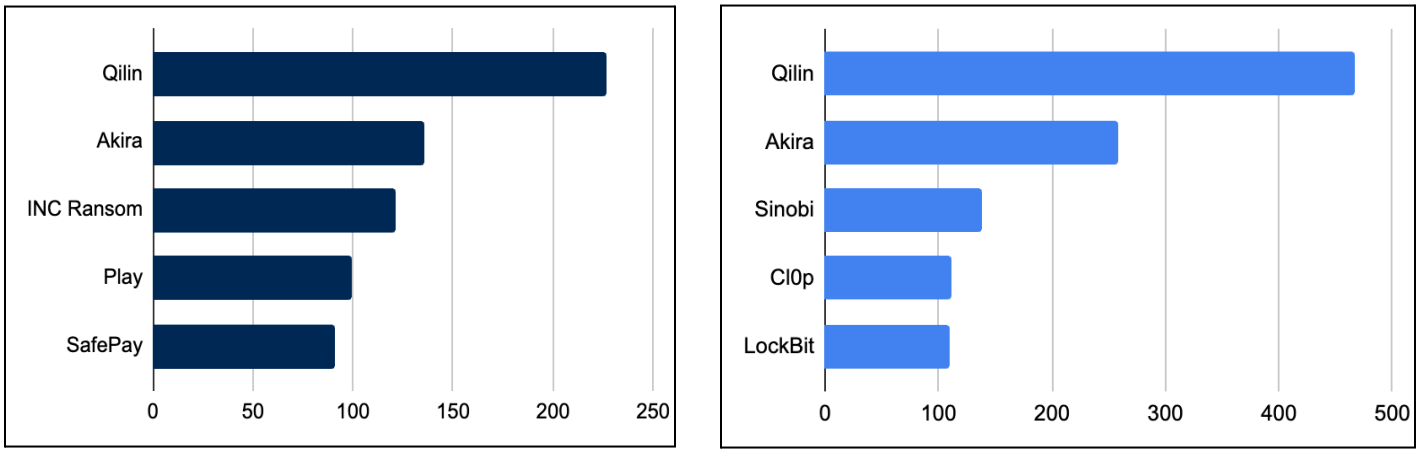
The top five most targeted industries remained the same in Q4 2025 as in Q3. However, ZeroFox observed substantial increases in the targeting of all five industries in Q4, highlighted by a 67 percent increase in targeting of the construction industry. These increases account for the rise in both overall attacks and percentage of incidents among the top five industries.

- Throughout 2025, the professional services industry experienced at least 805 attacks, surpassing the 462 recorded in 2024—a 74 percent increase year-over-year. Incidents in the professional services industry have nearly doubled every year since 2023.

- The increasing targeting of professional services organizations is likely driven by the industry's substantial growth in recent years—partly due to the need for niche specialized expertise—as well as the digitization of businesses globally. This, in turn, highlights vulnerabilities to the professional services industry and its clients. For these reasons, it is almost certain that professional services will remain in the top five most targeted industries in 2026.

Prominent Collectives

ZeroFox observed that the five most active R&DE collectives in Q4 2025 were almost certainly Qilin, Akira, Sinobi, Cl0p, and LockBit. This is a change from Q3 2025, with only Qilin and Akira remaining in the top five from the previous quarter. These two collectives alone accounted for approximately 35 percent of all global R&DE attacks in Q2 and Q3 2025, with a record-breaking 467 and 258 attacks respectively. LockBit, newcomer Sinobi, and Cl0p were the prominent collectives in Q4 2025.



Top five most prominent R&DE collectives in Q3 2025 (left) and Q4 2025 (right)

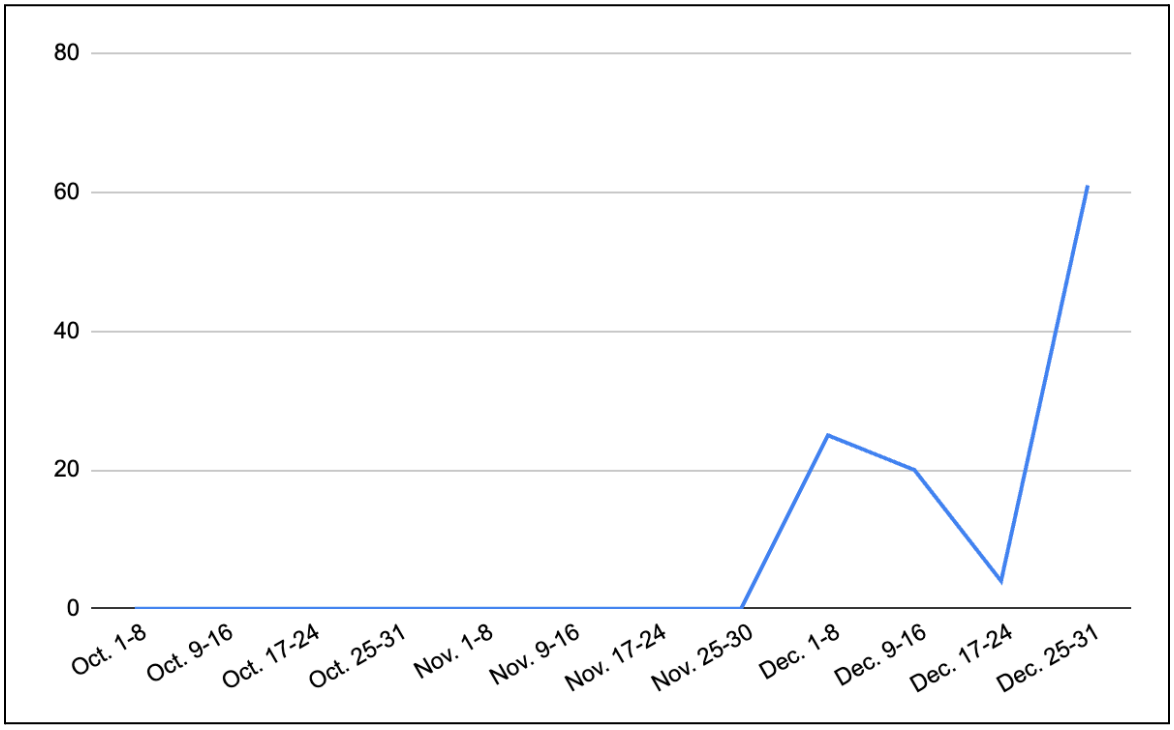
Source: ZeroFox Intelligence

LockBit

LockBit was responsible for at least 110 separate attacks in Q4 2025, accounting for roughly 5 percent of all incidents. LockBit was completely inactive in Q3 2025 and had conducted very few attacks since Q3 2024. Notably, LockBit did not conduct any attacks in Q4 2025 until December, with 55 percent of all LockBit attacks occurring the final week

of that month. The resurgence of attacks is almost certainly the result of the group launching LockBit 5.0 (a new version of their ransomware operation) in late 2025.

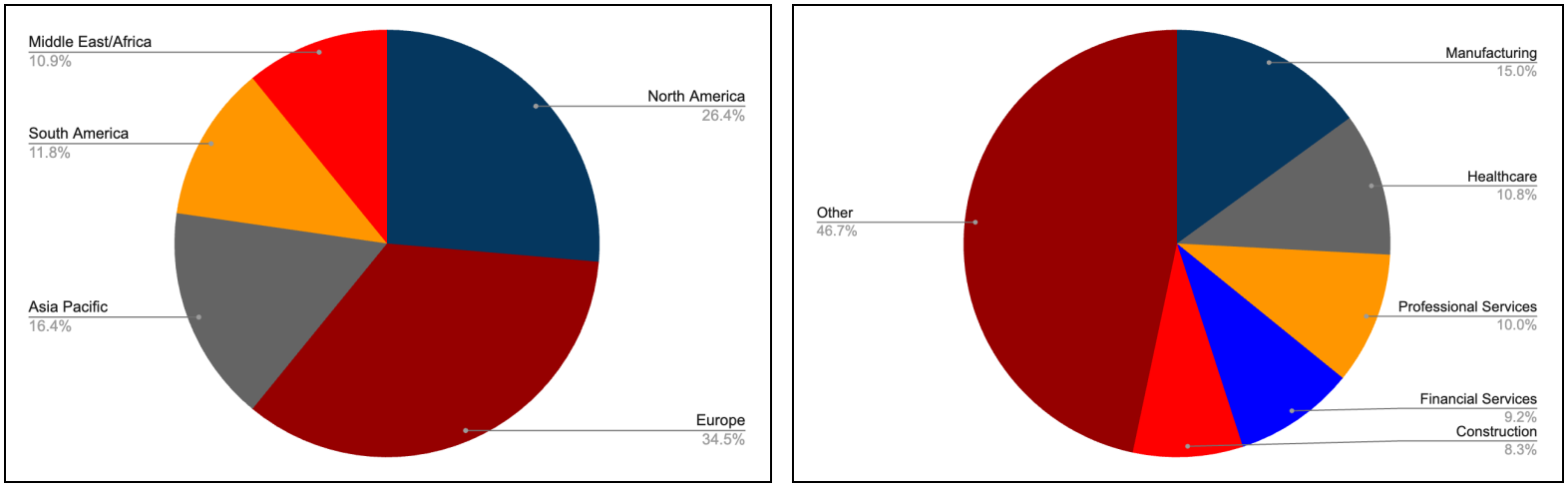
- In September 2025, LockBit announced the launch of a new ransomware tool suite called LockBit 5.0. The group claimed the updated version of their software included enhanced encryption and evasion tactics.[1]
- Prior to their hiatus, LockBit was among the most active ransomware collectives in the world, accounting for 21 percent of all ransomware attacks globally in 2023. LockBit was also responsible for 30 percent of global ransomware attacks between August 2021 and August 2022.[2]
- The return of LockBit in Q4 2025 will likely lead to an increase in attacks associated with the collective. It is very likely that LockBit will remain in the top five collectives for Q1 2026.



LockBit's Q4 2025 R&DE incidents by week

Source: ZeroFox Intelligence

[1] hXXps://www.scworld[.]com/brief/lockbit-5-0-emerges-as-ransomware-group-aims-for-revival
[2] hXXps://cybersecuritynews[.]com/lockbit-5-0-emerges/



LockBit's most targeted regions (left) and industries (right) in Q4 2025

Source: ZeroFox Intelligence

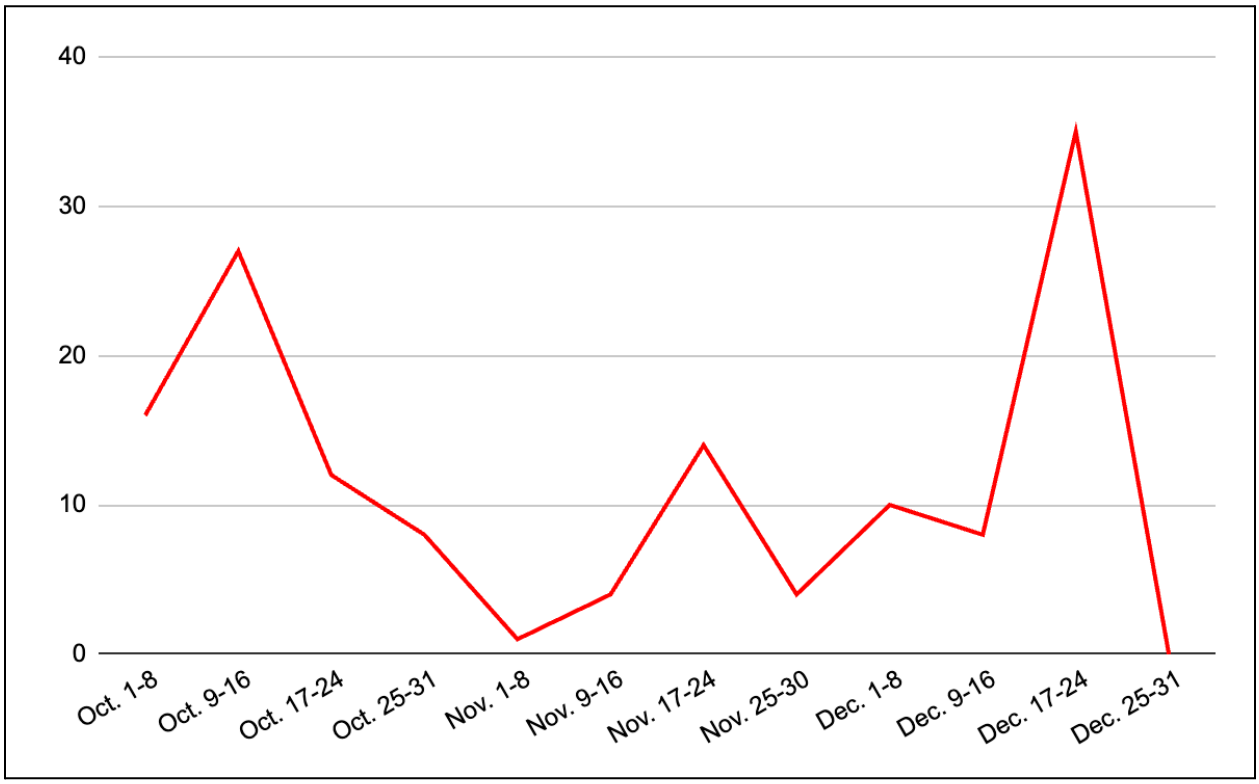
Sinobi

Having only recently emerged in Q3 2025 with at least 44 attacks, Sinobi nearly tripled their activity in Q4 with at least 139 attacks. While this number represents just 6 percent of all ransomware attacks in Q4 2025, it is significant because Sinobi is a newer collective that increased their activity approximately 216 percent over just one quarter.

- Organizations in North America accounted for nearly 82 percent of all attacks attributed to Sinobi in Q4 2025. This is disproportionately above the approximately 59 percent average observed across the global R&DE landscape but less than the collective's targeting of North America-based organizations in Q3, which was 95 percent.
- The professional services (approximately 20 percent), manufacturing (approximately 19 percent), and construction (approximately 14 percent) industries were those most targeted by Sinobi ransomware in Q4 2025.

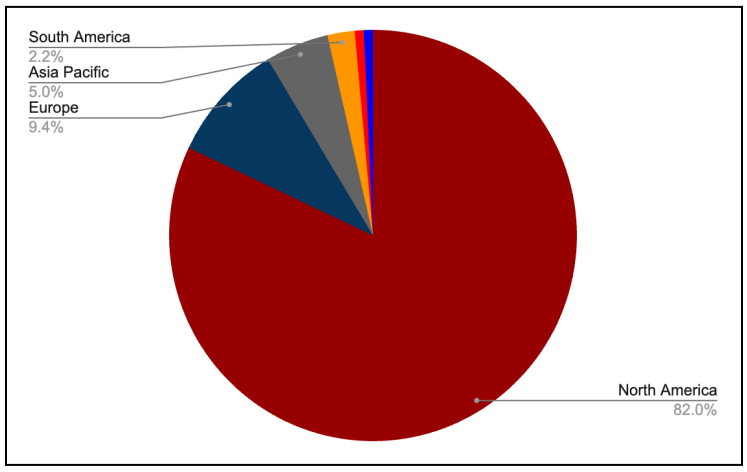
Sinobi's frequent targeting of the professional services industry in Q4 2025 closely aligns with ZeroFox's observations of increased targeting of this industry in 2025. Sinobi's emergence in mid-2025—and the dramatic increase of its operational tempo in Q4 2025—indicate the collective is likely to continue increasing its attacks in 2026, with

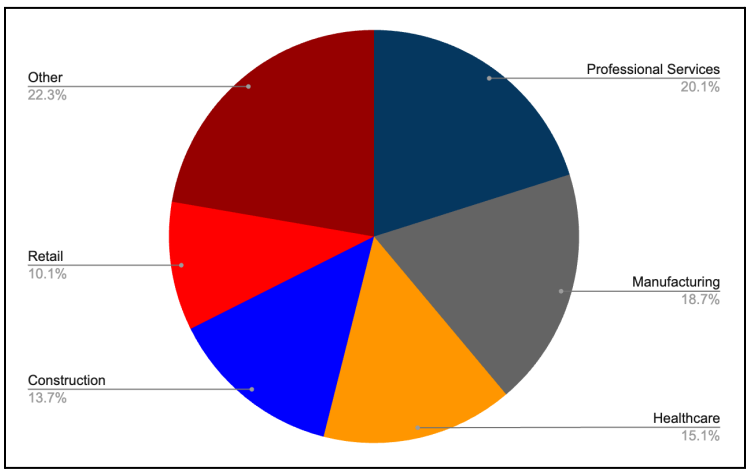
organizations in North America almost certainly remaining at the top of SInobi's targeting priorities.



Sinobi's Q4 2025 R&DE incidents by week

Source: ZeroFox Intelligence





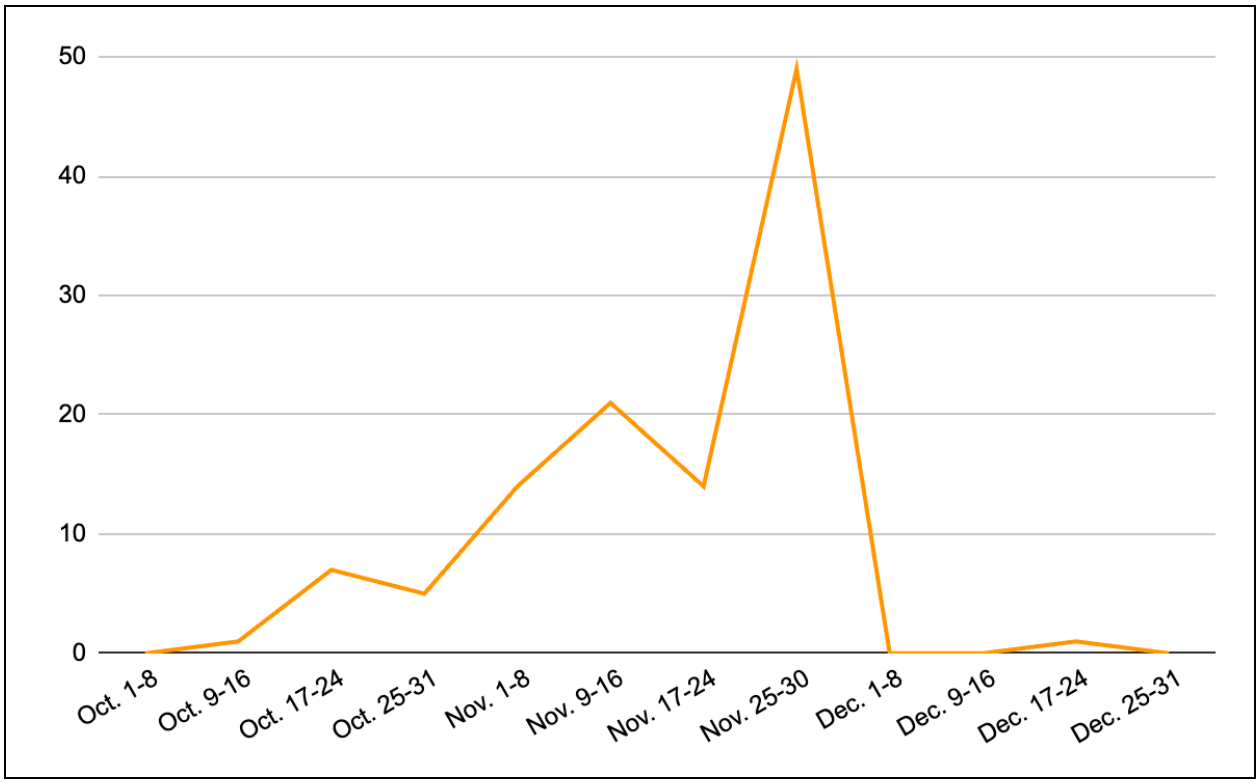
Sinobi's most targeted regions (left) and industries (right) in Q4 2025

Source: ZeroFox Intelligence

Cl0p

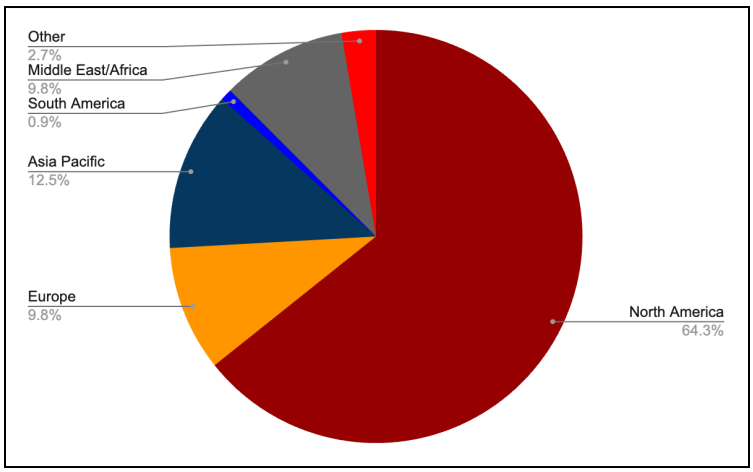
During Q4 2025, ransomware collective Cl0P was responsible for at least 112 separate attacks, accounting for 5.3 percent of global R&DE incidents and making it the fourth most active collective for this period. Notably, Cl0p's Q4 2025 attacks represent the first significant activity by the collective since its then record-setting 370 attacks in Q1 2025. (Cl0p was only responsible for a total of nine attacks in both Q2 and Q3 2025.)

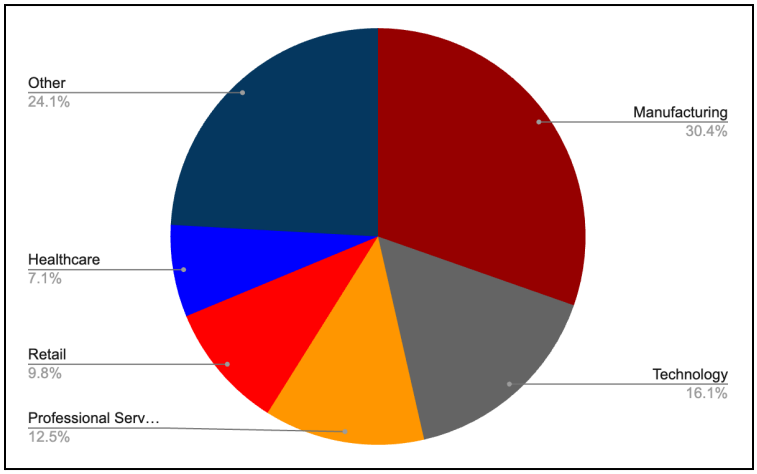
- Organizations in North America accounted for approximately 64 percent of all attacks attributed to Cl0p in Q4 2025, which is above the approximately 59 percent average observed across the global R&DE landscape.
- Organizations in the Asia-Pacific region accounted for nearly 13 percent of all attacks attributed to Cl0p during Q4 2025, which is also slightly higher than the approximately 9 percent average of global R&DE attacks targeting the region.
- Manufacturing, technology, and professional services were the industries most targeted during this period by Cl0p. Manufacturing alone accounted for approximately 30 percent of Cl0p's attacks, which is consistent with targeting trends from Q1 2025 (Cl0p's last quarter of significant activity).



Cl0p's incidents by week in Q4 2025

Source: ZeroFox Intelligence





Cl0p's most targeted regions (left) and industries (right) in Q4 2025

Source: ZeroFox Intelligence

Conclusion

Historically, the final quarter of the year has seen the highest number of R&DE attacks, and 2025 was no exception. In the past, Q1 of the following year has seen a sharp decline in attacks; however, Q1 2025 broke all single-quarter records at the time. Throughout 2025, ZeroFox observed a continual uptick quarter-over-quarter in global ransomware attacks. This trend continued unabated in Q4 2025, culminating in a new record of at least 2,091 attacks. In light of this, it is likely that R&DE attacks will remain high in Q1 2026 rather than see the same historical dip often observed in Q1 of a new year.

Qilin and Akira remained the two most active groups in Q4, with a record-breaking 467 and 258 attacks respectively. The most prominent R&DE collectives are likely to continue to fluctuate throughout Q1 2026; however, Qilin and Akira will almost certainly maintain their high level of activity into Q1 2026, with the returning LockBit likely joining them in the top five.

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%