ZEROFOX INTELLIGENCE

Assessment

Q3 2025 Ransomware Wrap-Up

A-2025-10-03a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

October 3, 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 7:00 AM EDT on October 1, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

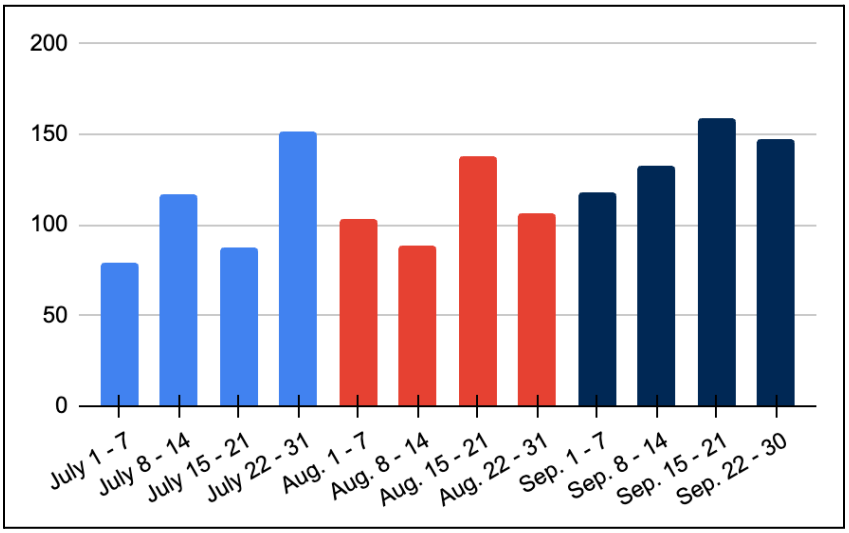
| Assessment | Q3 2025 Ransomware Wrap-Up

| Key Findings

- ZeroFox observed at least 1,429 separate ransomware and digital extortion (R&DE) incidents in Q3 2025, a slight increase of nearly 5 percent from Q2 and a drop of approximately 27 percent from the record-breaking 1,961 incidents observed in Q1 2025.
- By Q3 2025, the professional services industry had already experienced at least 510 attacks, surpassing the 462 incidents recorded in all of 2024—a nearly 10.4 percent increase year-over-year, with the pace suggesting up to a 47 percent increase by year end if current trends continue.
- The increased 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.
- ZeroFox assesses that the five most active R&DE collectives in Q3 2025 were almost certainly Qilin, Akira, INC Ransom, Play, and SafePay. This is notably similar to Q2 2025—wherein the top five was composed of the same collectives—with some minor shifts.

Q3 2025 Overview

ZeroFox observed at least 1,429 separate R&DE incidents in Q3 2025, a slight increase of nearly 5 percent from Q2 and a drop of approximately 27 percent from the record-breaking 1,961 incidents observed in Q1 2025. However, Q3 2025 marked an increase of incidents year-over-year from 2024 and 2023, which accounted for at least 1,187 and 1,139 incidents, respectively.

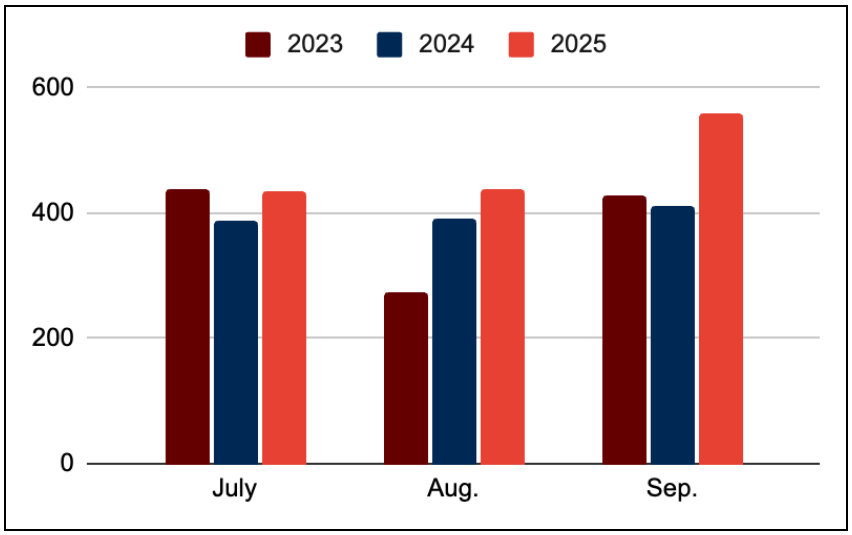


R&DE incidents by week in Q3 2025

Source: ZeroFox Intelligence

So far into 2025, ZeroFox has 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, which began in May 2024 and continues as of writing. Historically, the last quarter of the year often sees the highest number of attacks in that year; it is likely that the uptick of incidents will persist into the fourth quarter.

The average number of July incidents has remained consistent from 2023–2025 at approximately 419, while August and September have seen overall increases. September 2025 saw an unprecedented and record-high number of incidents for any month in Q3, with at least 557 attacks.



Q3 R&DE incidents from 2023–2025

Source: ZeroFox Intelligence

Regional Trends

Regional R&DE targeting patterns in Q3 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 a slight 2.6 percent increase from Q2 2025.

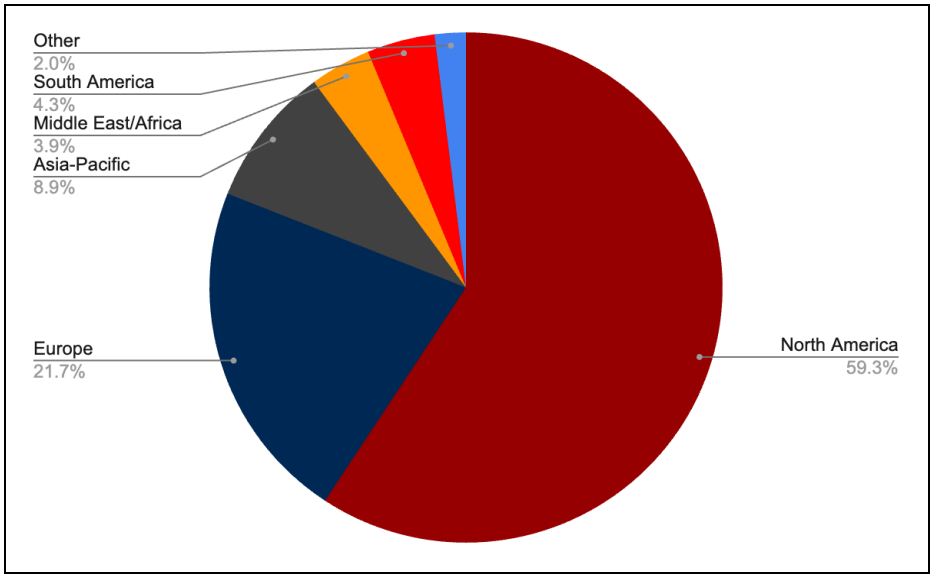
- At least 1,309 R&DE attacks targeted North-America based organizations in Q1 2025; the number dropped to 774 attacks in Q2 2025 and increased to 845 attacks in Q3 2025 (a roughly 9.2 percent increase).

Europe-based organizations were the second most targeted region in Q3 2025, accounting for nearly 22 percent of all incidents; this is a slight decrease from the approximately 24 percent observed in Q2 2025. Together, North America and Europe-based organizations accounted for 81 percent of all R&DE incidents observed during Q3 2025, which is largely consistent with other quarters.

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 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.
- 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 Q3 2025

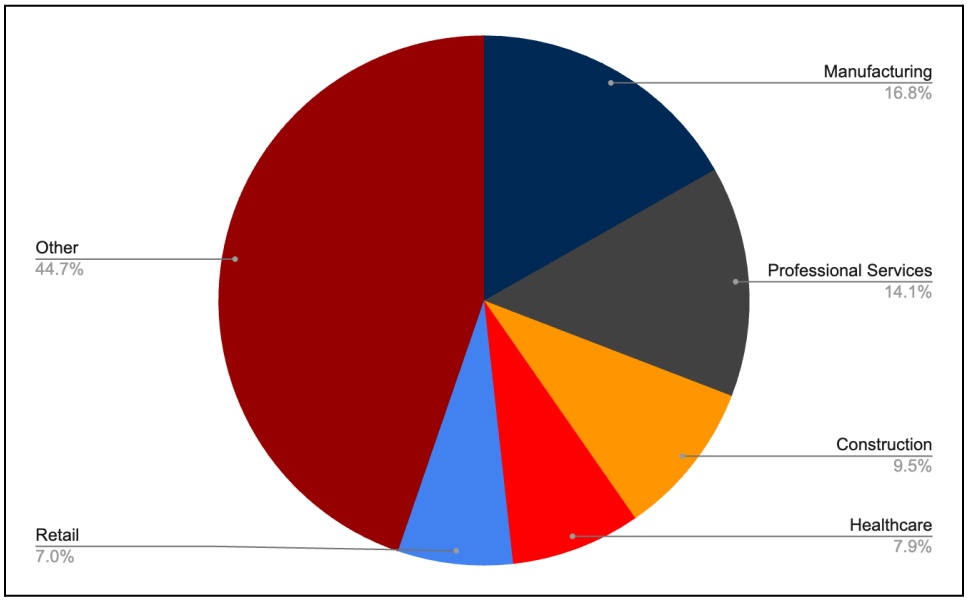
Source: ZeroFox Intelligence

Industry Trends

In Q3 2025, organizations in the manufacturing industry were targeted by a higher number of R&DE incidents than those in other industries (totaling at least 244 attacks). Nearly 17 percent of all incidents targeted entities in the manufacturing industry in Q3 2025, a slight decrease from the approximately 19 percent ZeroFox observed in Q2 2025. Manufacturing has consistently been the most targeted industry since at least 2021.

- In Q3 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.

- Other industries heavily targeted in Q3 2025 include manufacturing, professional services, construction, healthcare, and retail; together, attacks on these industries accounted for approximately 55 percent of all incidents.



Most heavily targeted industries in Q3 2025

Source: ZeroFox Intelligence

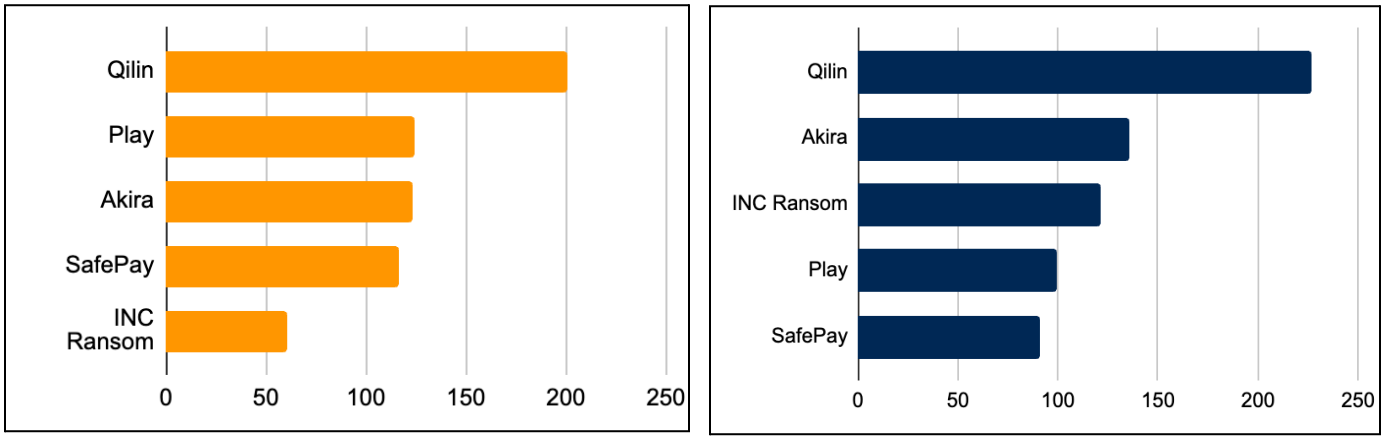
In Q2 2025, the top five industries most targeted were manufacturing, construction, healthcare, retail, and technology; in Q3, ZeroFox observed a substantial increase in the targeting of the professional services industry, while the targeting of the technology industry fell below the top five. However, the targeting of these industries regularly interchanges and is consistent with targeting trends in previous years.

- By Q3 2025, the professional services industry had already experienced at least 510 attacks, surpassing the 462 recorded in all of 2024—a nearly 10.4 percent increase year-over-year, with the pace suggesting up to a 47 percent increase by year end if current trends continue.

- 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.

Prominent Collectives

ZeroFox assesses that the five most active R&DE collectives in Q3 2025 were almost certainly Qilin, Akira, INC Ransom, Play, and SafePay. This is notably similar to Q2 2025—wherein the top five were composed of the same collectives—with some minor shifts. Together, these five collectives accounted for approximately 47 percent of all global R&DE attacks in Q2 and Q3 2025. In comparison, the top five most prominent collectives for Q1 2025 accounted for approximately 50 percent of all global R&DE attacks.



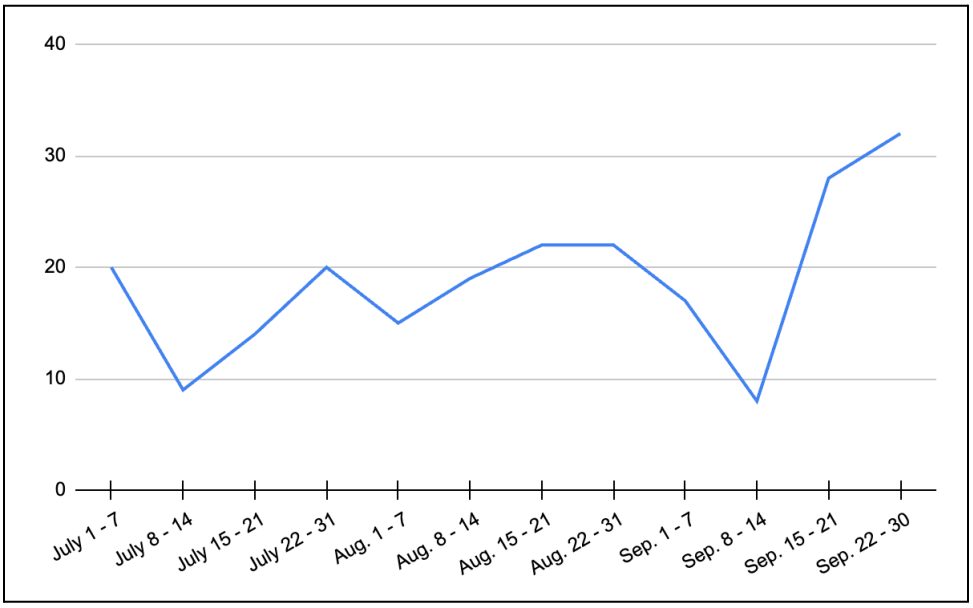
Top five most prominent R&DE collectives in Q2 2025 (left) and Q3 2025 (right)

Source: ZeroFox Intelligence

Qilin

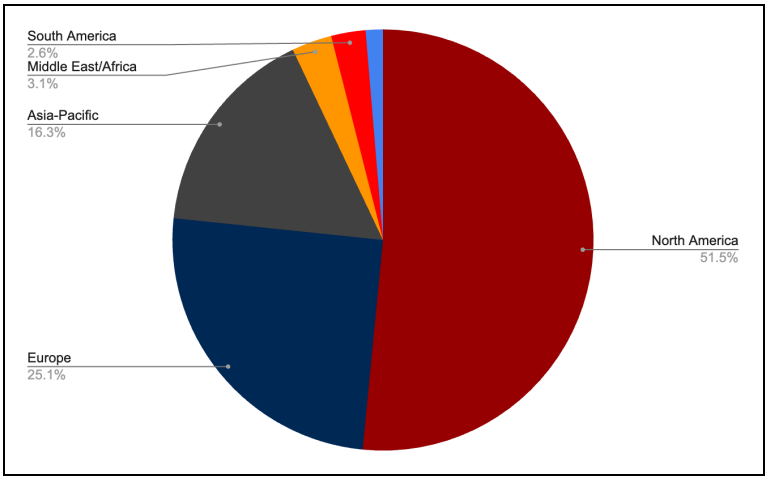
In Q3 2025, Qilin was responsible for at least 227 separate attacks, accounting for nearly 16 percent of all incidents—more than any other collective. Notably, Qilin was the fifth most prominent R&DE collective during Q1 2025, with approximately 106 incidents; the group conducted nearly twice as many attacks in Q2 2025 despite the overall global decrease of R&DE incidents; in Q3, the collective increased attacks by nearly 13 percent.

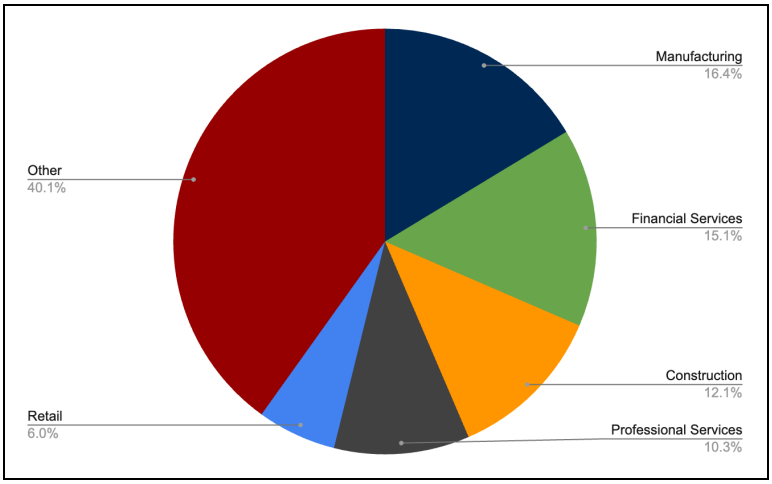
- In Q3 2025, Qilin disproportionately targeted North America-based organizations, which represented nearly 52 percent of the collective's victims; this is 12 percent lower than in Q2.
- Qilin's operational tempo began to increase significantly in Q4 2024, when the collective conducted at least 46 attacks. This continued through Q1 2025, which saw the group responsible for at least 106 incidents and Q2 2025, when it accounted for at least 201 incidents. In Q3 2025, the collective continued to increase its attack tempo, which is likely to persist into Q4.



Qilin's Q3 2025 R&DE incidents by week

Source: ZeroFox Intelligence





Qilin's most targeted regions (left) and industries (right) in Q3 2025

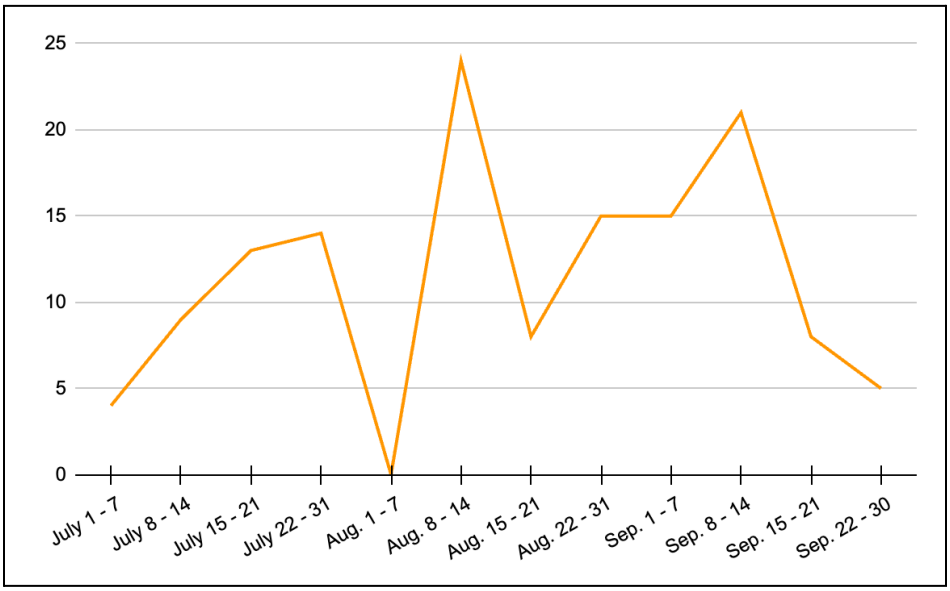
Source: ZeroFox Intelligence

Akira

In Q3 2025, Akira was the second most active collective and was responsible for at least 136 attacks, accounting for approximately 9.5 percent of all global R&DE incidents; this is largely consistent with previous quarters observed by ZeroFox. Notably, Akira's total number of incidents decreased from 203 attacks in Q1 2025 to 123 attacks in Q2 2025; in Q3 2025, the collective increased operations by approximately 10.6 percent.

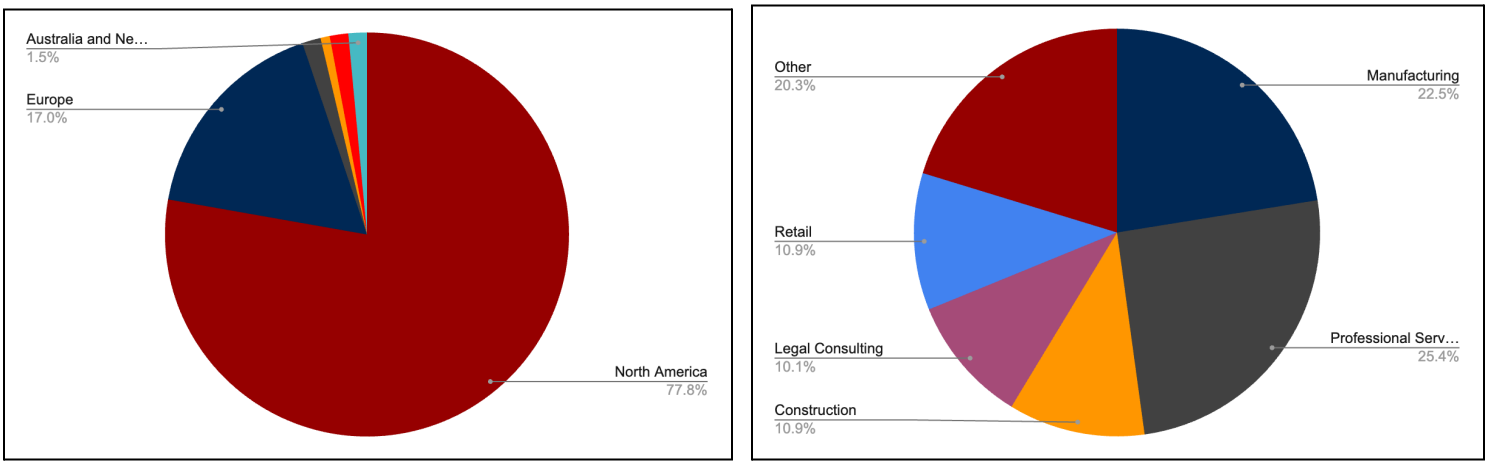
- Organizations in North America accounted for nearly 78 percent of all attacks attributed to Akira in Q3 2025, which is disproportionately above the approximately 59 percent average observed across the global R&DE landscape and significantly more than the collective's targeting of North America-based organizations in Q2.
- Similarly, organizations in Europe accounted for approximately 17 percent of all attacks attributed to Akira during Q3 2025, slightly below the approximately 22 percent average of global R&DE attacks targeting the region and significantly less than the collective's Europe-based targeting trends in Q2 2025.
- Professional services (approximately 25 percent), manufacturing (approximately 23 percent), and construction (approximately 11 percent) were the industries most targeted during this period by Akira ransomware.

Akira most often targeted the professional services industry in Q3 2025, which closely aligns with ZeroFox's observations of increased targeting of this industry in 2025. Since the end of Q1 2025, Akira has increasingly targeted organizations within the professional services industry, which was not nearly as prominent a target for the group in 2024.



Akira's Q3 2025 R&DE incidents by week

Source: ZeroFox Intelligence



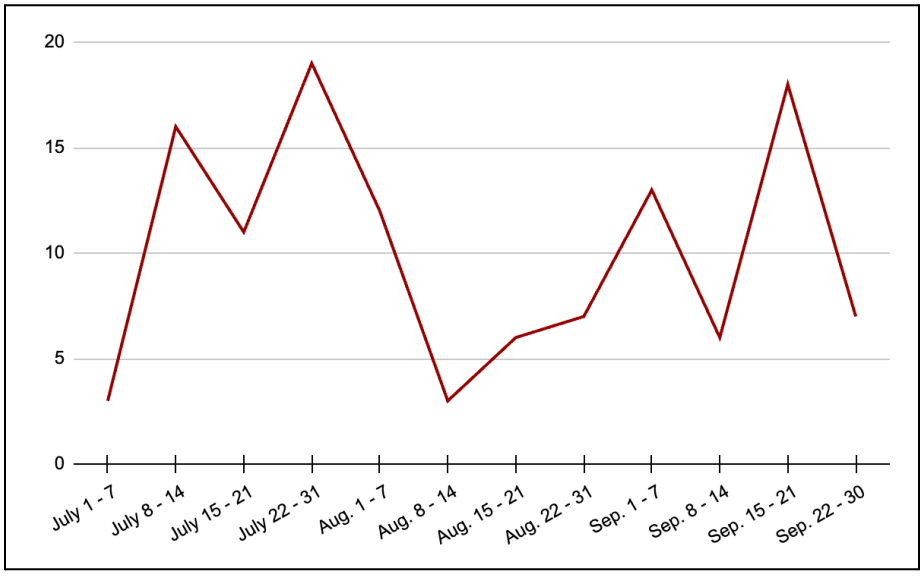
Akira's most targeted regions (left) and industries (right) in Q3 2025

Source: ZeroFox Intelligence

INC Ransom

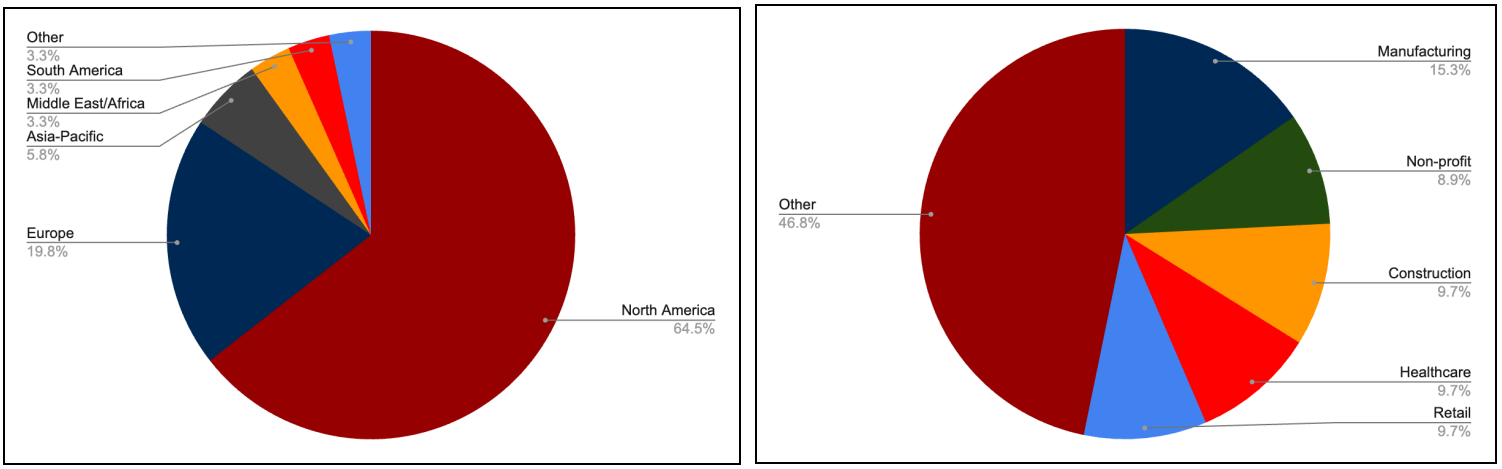
During Q3 2025, INC Ransom was responsible for at least 121 separate attacks, accounting for approximately 8.5 percent of global R&DE incidents and making it the third most active collective for this period. Notably, INC Ransom's total number of incidents increased from 61 attacks in Q2 2025 to 121 attacks in Q3 2025 (a 98.4 percent increase), demonstrating the up-and-coming collective's prominence in the global R&DE threat landscape.

- Organizations in North America accounted for approximately 64.5 percent of all attacks attributed to INC Ransom in Q3 2025, which is above the approximately 59 percent average observed across the global R&DE landscape.
- Similarly, organizations in Europe accounted for nearly 20 percent of all attacks attributed to INC Ransom during Q3 2025, slightly below the approximately 22 percent average of global R&DE attacks targeting the region.
- Manufacturing, non-profit, and construction were the industries most targeted during this period by INC Ransom. The collective's overall targeting trends are considerably more diverse than those of Qilin and Akira and lack a primary industry-based interest.



INC Ransom's incidents by week in Q3 2025

Source: ZeroFox Intelligence



INC Ransom's most targeted regions (left) and industries (right) in Q3 2025

Source: ZeroFox Intelligence

Conclusion

Similarly to the first two quarters of the year, ZeroFox continued to observe a global and industry-wide R&DE uptick throughout Q3 2025, which is very likely to persist into Q4 2025—especially since the last quarter of the year often sees the highest volume of attacks annually. The most prominent R&DE collectives are likely to remain consistent, as Qilin, Akira, INC Ransom, Play, and SafePay have conducted the most R&DE attacks for two consecutive quarters this year. Notably, INC Ransom is likely to surpass Akira and possibly Qilin next quarter if its operational tempo continues to proportionally increase as observed from Q2 to Q3 2025. Regional and industry targeting is likely to remain largely unchanged, with a roughly even chance that professional services will continue to experience an increase of attacks in Q4.

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%