ZEROFOX INTELLIGENCE

Assessment

Q1 2026 Ransomware Wrap-Up

A-2026-04-17a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

April 17, 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 (EDT) on April 17, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

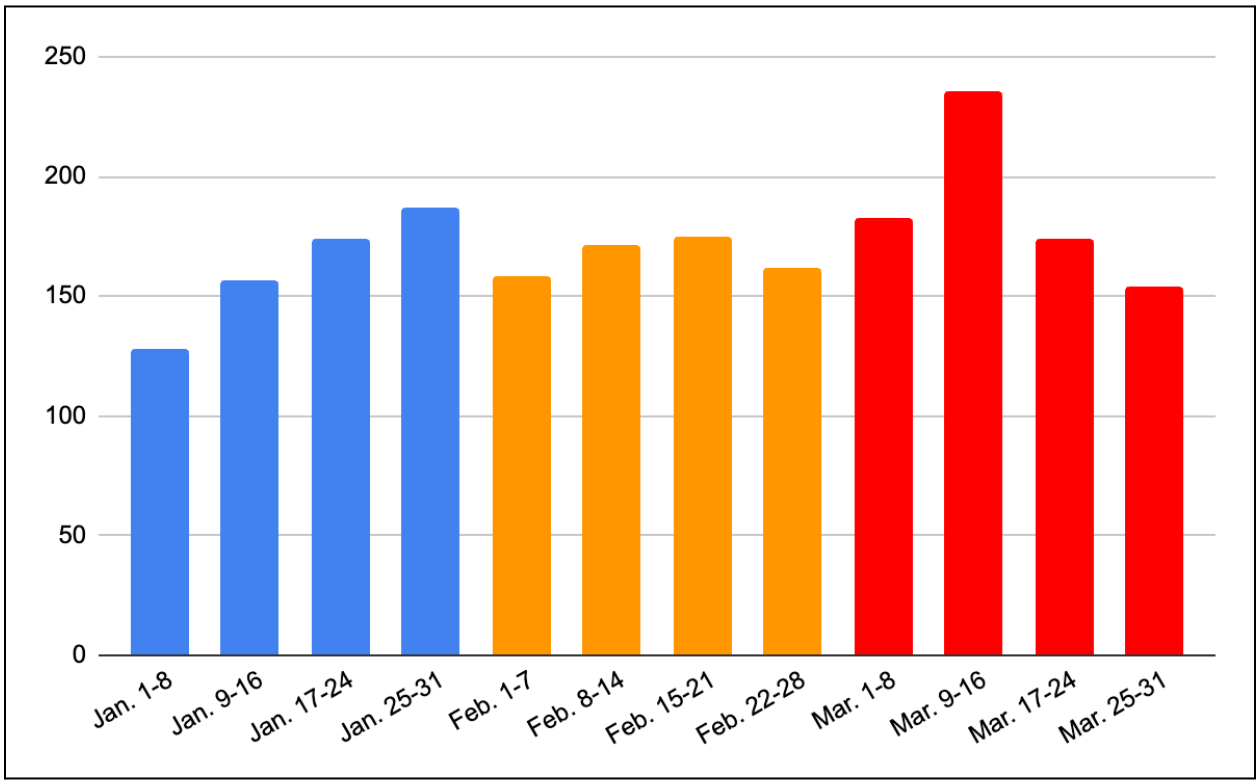
Assessment | Q1 2026 Ransomware Wrap-Up

Key Findings

- ZeroFox observed at least 2,059 separate ransomware and digital extortion (R&DE) incidents in Q1 2026, a decrease of approximately 1.5 percent from Q4 2025—which accounted for a record-breaking 2,091 incidents.
- March remained the most active month in Q1 in comparison to previous years, accounting for at least 747 incidents—which is roughly 36 percent of all global ransomware attacks in Q1 2026.
- Regional R&DE targeting patterns in Q1 2026 were largely consistent with those observed during previous months. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 54 percent of all incidents (or at least 1,114 incidents).
- ZeroFox observed that the five most active R&DE collectives in Q1 2026 were almost certainly Qilin, Akira, The Gentlemen, INC Ransom, and Cl0p. This is a change from Q4 2025, with only Qilin, Akira, and Cl0p remaining in the top five from the previous quarter.

Q1 2026 Overview

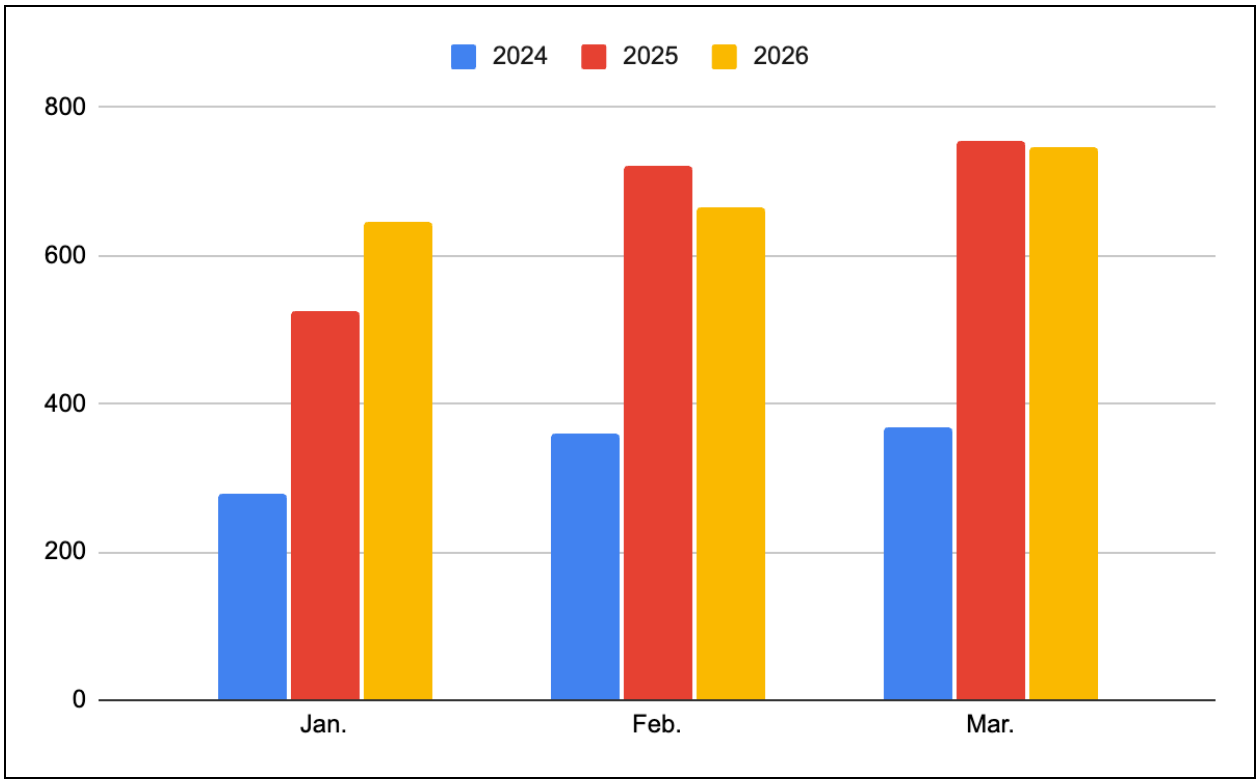
ZeroFox observed at least 2,059 separate R&DE incidents in Q1 2026, a decrease of approximately 1.5 percent from Q4 2025—which accounted for a record-breaking 2,091 incidents. Additionally, Q1 2026 marked an increase of incidents year-over-year from 2025 and 2024, which saw at least 2,001 and 1,007 incidents, respectively.



R&DE incidents by week in Q1 2026

Source: ZeroFox Intelligence

January has seen steady rises from 2024–2026, with at least 646 attacks in 2026. February experienced a decrease of approximately 8 percent from 2025, with approximately 666 incidents observed. March was the most active Q1 month in comparison to previous years, accounting for at least 747 separate incidents—which is roughly 36 percent of all global ransomware attacks in Q1 2026.



Q1 R&DE incidents from 2024–2026

Source: ZeroFox Intelligence

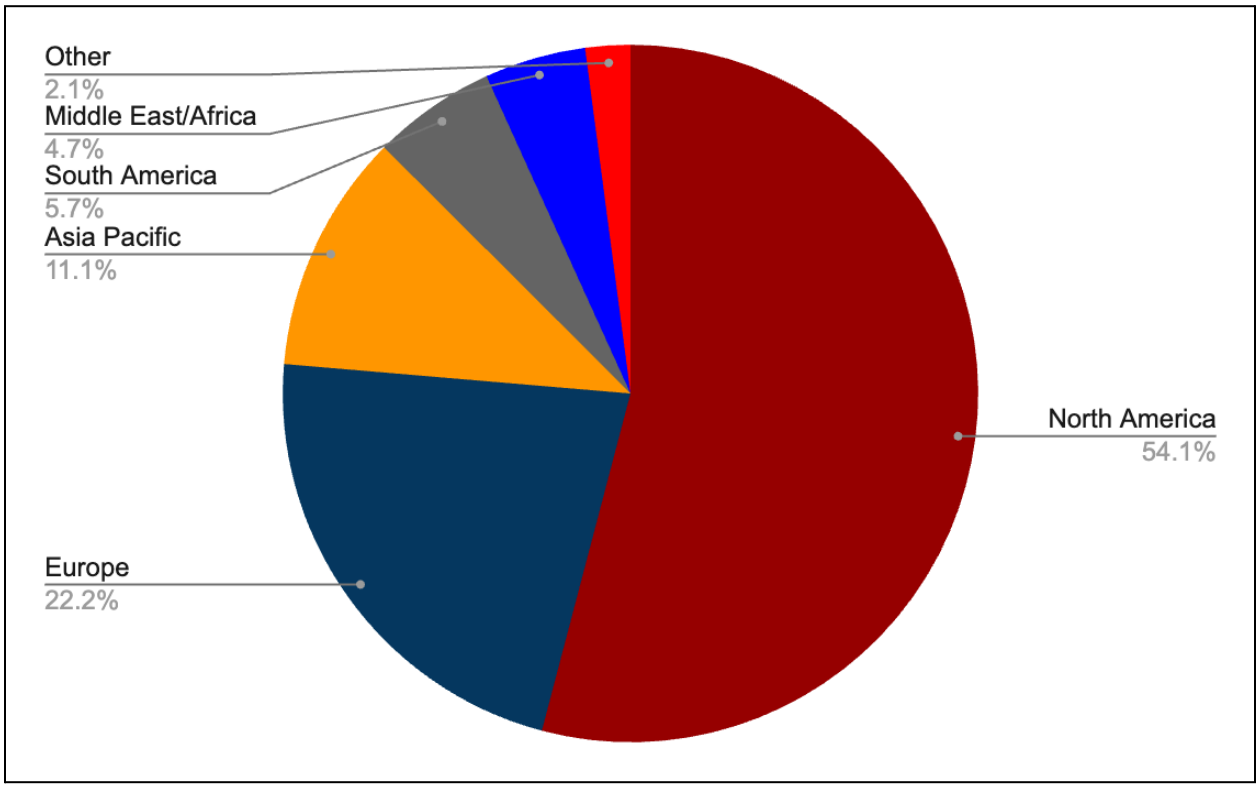
Regional Trends

Regional R&DE targeting patterns in Q1 2026 were largely consistent with those observed during previous months. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 54 percent of all incidents (or at least 1,114 incidents). This is consistent with the 51 percent average observed over the previous 12 months and a slight decrease from the 66 percent seen in Q1 2025.

Europe-based organizations were the second most targeted region in Q1 2026, accounting for roughly 22 percent of all incidents; this is a slight increase from the approximately 20 percent observed in Q4 2025. Together, North America and Europe-based organizations accounted for 76 percent of all R&DE incidents observed during Q1 2026, which is a 2 percent decrease from Q4 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.



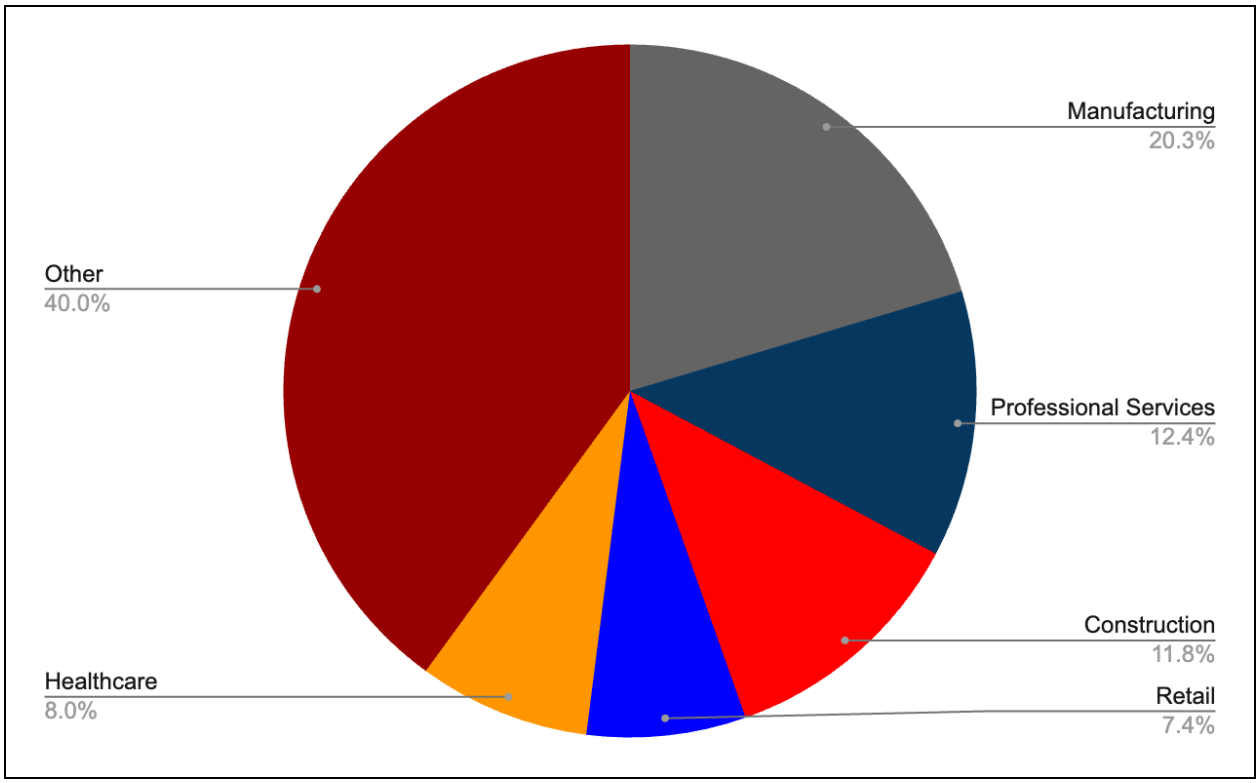
R&DE targeting by region in Q1 2026

Source: ZeroFox Intelligence

Industry Trends

In Q1 2026, organizations in the manufacturing industry were targeted by a higher number of R&DE incidents than those in other industries, totaling at least 419 incidents (a slight increase from the 413 observed in Q4 2025). Nearly 20 percent of all incidents targeted entities in the manufacturing industry in Q1 2026, which is consistent with the approximately 20 percent ZeroFox observed in Q4 2025. Manufacturing has consistently been the most targeted industry since at least 2021.

- In Q1 2026, 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 Q1 2026 include manufacturing, professional services, construction, retail, and healthcare; together, attacks on these industries accounted for approximately 60 percent of all incidents.
- The top five most targeted industries in Q1 2026 remained the same as in Q4 2025.



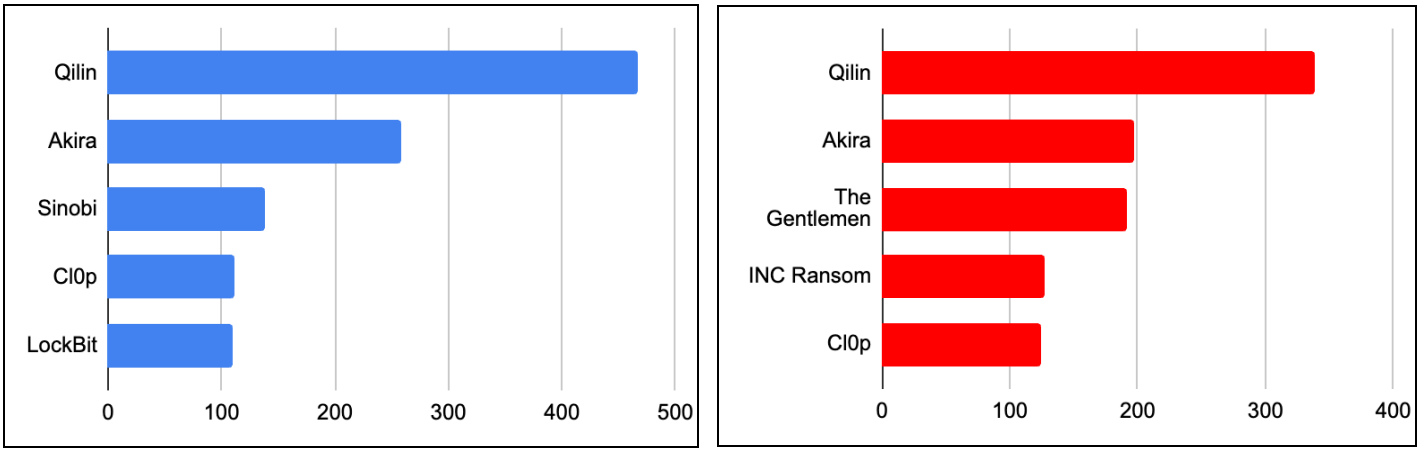
Most heavily targeted industries in Q1 2026

Source: ZeroFox Intelligence

Prominent Collectives

ZeroFox observed that the five most active R&DE collectives in Q1 2026 were almost certainly Qilin, Akira, The Gentlemen, INC Ransom, and Cl0p. This is a change from Q4 2025, with only Qilin, Akira, and Cl0p remaining in the top five from the previous quarter. These top five most prominent collectives accounted for approximately 48 percent of all global R&DE attacks in Q1 2026 and were responsible for a combined total of at least 979 incidents.

- Qilin and Akira remained the two most prominent R&DE collectives from Q4 2025 through Q1 2026, accounting for at least 338 and 197 incidents, respectively—which is approximately 26 percent of global incidents combined.



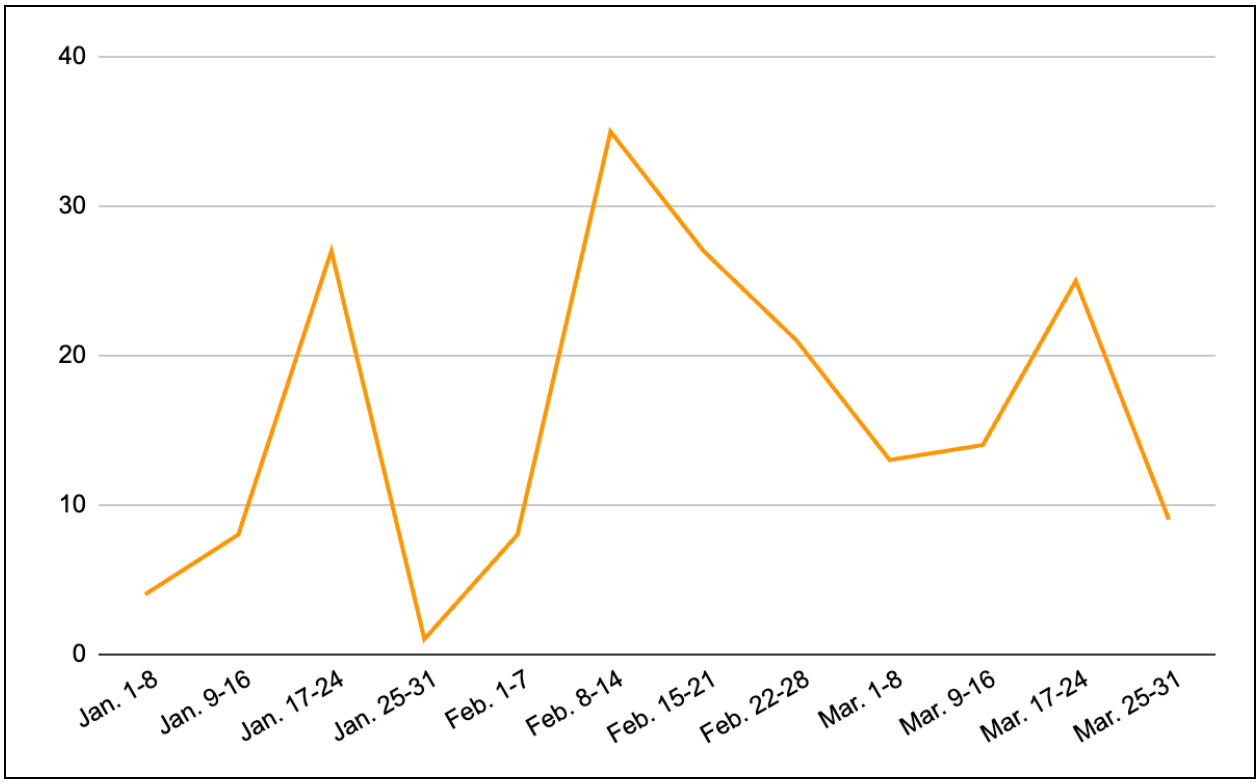
Top five most prominent R&DE collectives in Q4 2025 (left) and Q1 2026 (right)

Source: ZeroFox Intelligence

The Gentlemen

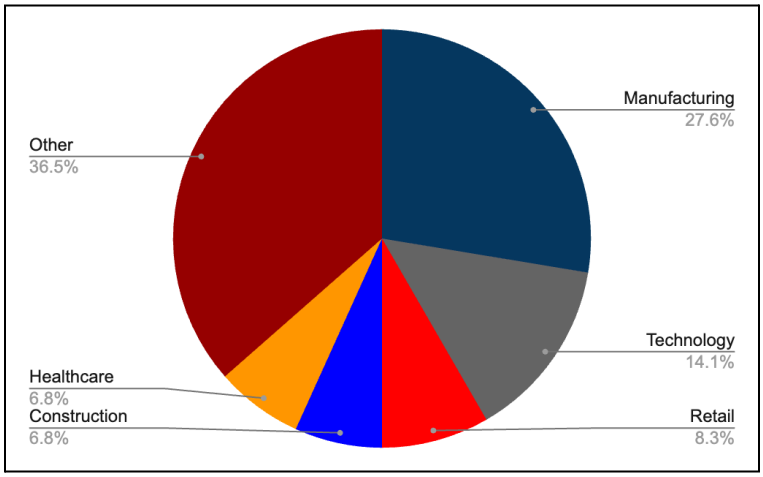
The Gentlemen was first observed in September 2025 and has since conducted at least 37 R&DE incidents in Q3 2025 and 35 in Q4 2025. However, The Gentlemen was responsible for at least 192 separate attacks in Q1 2026, accounting for roughly 9 percent of all incidents. This is a significantly higher number of incidents in comparison to previous quarters and makes The Gentlemen the third most active R&DE collective of Q1 2026.

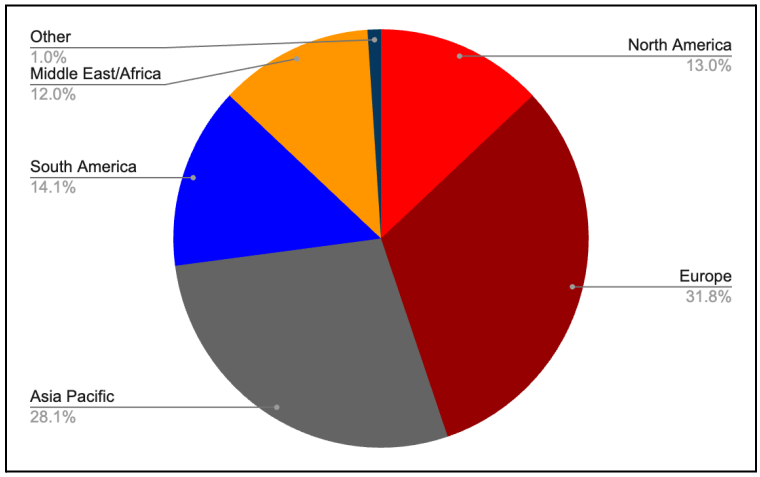
- Notably, North America-based victims accounted for approximately 20 percent of The Gentlemen's attacks in Q3 2025, 2 percent in Q4 2025, and 13 percent in Q1 2026. This largely goes against typical regional targeting trends by other R&DE collectives, at least 50 percent of whose victims are North America-based.
- Europe was the most targeted region, accounting for approximately 32 percent of all incidents.
- Manufacturing was the most targeted industry and accounted for approximately 28 percent of all incidents, which is consistent with other R&DE collectives.



The Gentlemen's Q1 2026 R&DE incidents by week

Source: ZeroFox Intelligence





The Gentlemen's most targeted industries (left) and regions (right) in Q1 2026

Source: ZeroFox Intelligence

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%