ZEROFOX INTELLIGENCE

Assessment

Q2 2026 Ransomware Wrap-Up

A-2026-07-06a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

July 6, 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 10:00 AM (EDT) on July 6, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

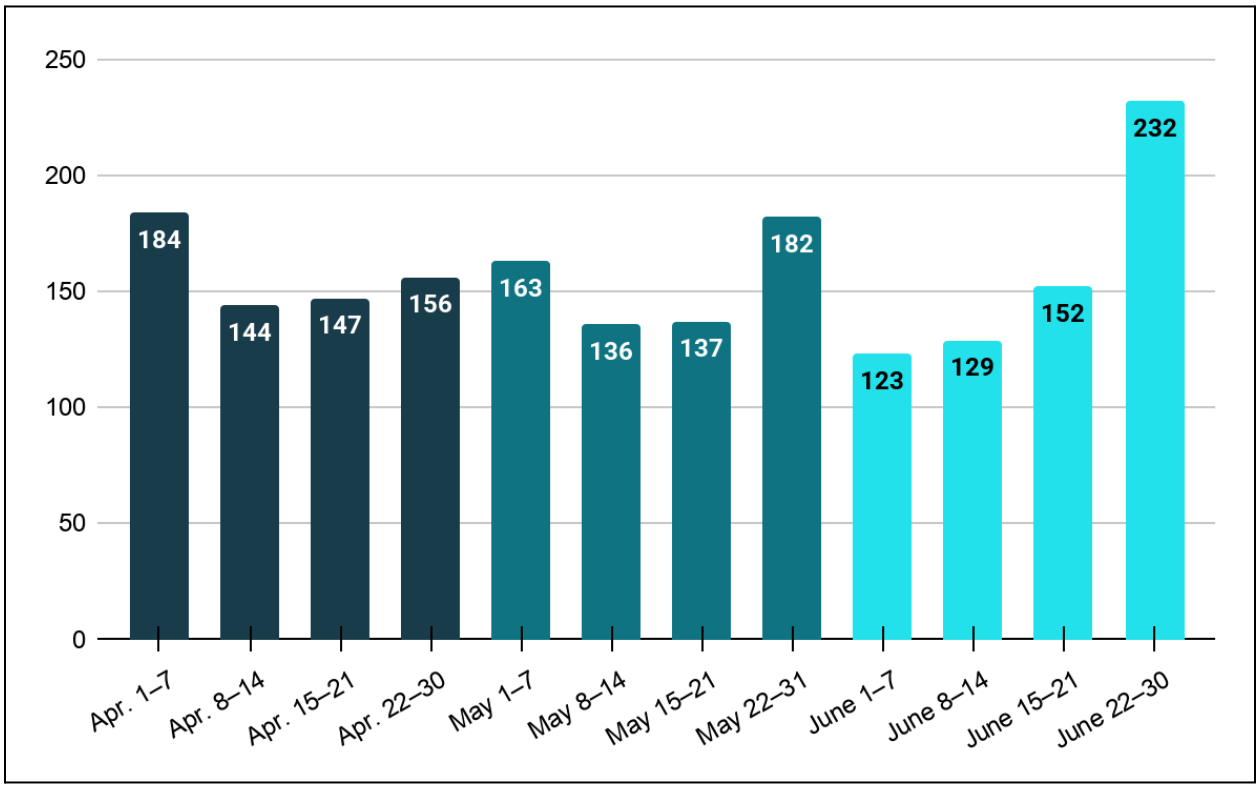
Assessment
Q2 2026 Ransomware Wrap-Up

Key Findings

- ZeroFox observed at least 1,885 separate ransomware and digital extortion (R&DE) incidents in Q2 2026, a decrease of approximately 8.5 percent from Q1 2026. However, Q2 2026 marked an overall increase of R&DE incidents year-over-year from Q2 2025 and Q2 2024.
- The global R&DE threat environment is almost certainly undergoing a geographic shift. Although historically the largest volume of incidents has occurred in North America, the region's proportional share is declining. Europe experienced significant year-over-year increases in R&DE incidents the first half of 2026, while the Asia-Pacific region has experienced uninterrupted quarter-over-quarter share growth since Q1 2024—and both are gradually absorbing larger shares.
- Qilin concluded Q2 2026 as the most active ransomware collective globally (at least 295 separate incidents), signaling both its dominance in the first half of 2026 and an unbroken 12-month period as the leading ransomware threat actor that began in Q2 2025.

Q2 2026 Overview

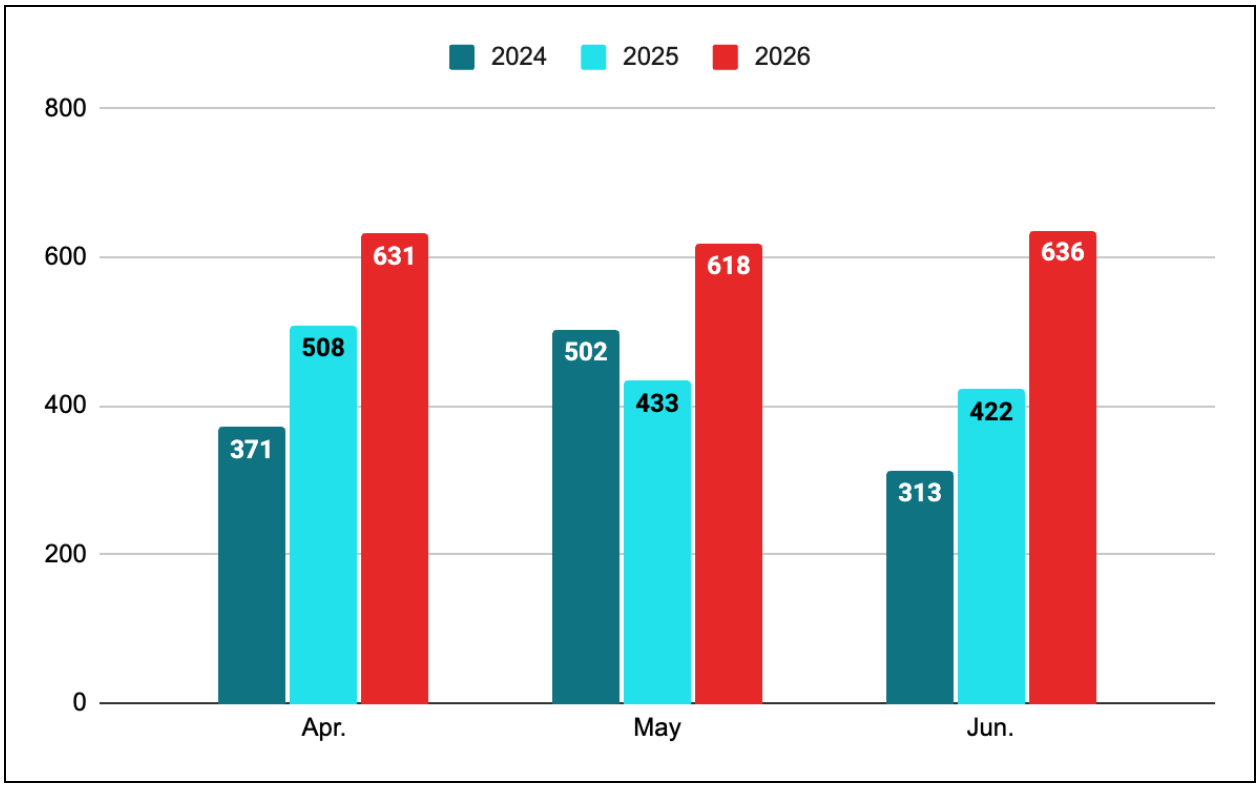
ZeroFox observed at least 1,885 separate R&DE incidents in Q2 2026, a decrease of approximately 8.5 percent from the 2,059 incidents recorded in Q1 2026. However, Q2 2026 marked an overall increase of incidents year-over-year from 2025 and 2024, which saw at least 1,363 and 1,186 incidents, respectively.



R&DE incidents by week in Q2 2026

Source: ZeroFox Intelligence

April has seen steady rises from 2024 to 2026, with at least 631 R&DE attacks in Q2 2026. May experienced a sharp increase of approximately 42.7 percent in Q2 2026, with approximately 618 R&DE incidents observed. June recorded at least 636 incidents in Q2 2026, accounting for 33.7 percent of all global R&DE incidents for the quarter. This represents a 50.7 percent year-over-year increase from June 2025's 422 incidents—the steepest year-over-year growth rate of any month in Q2 2026.



Q2 R&DE incidents (2024–2026)
Source: ZeroFox Intelligence

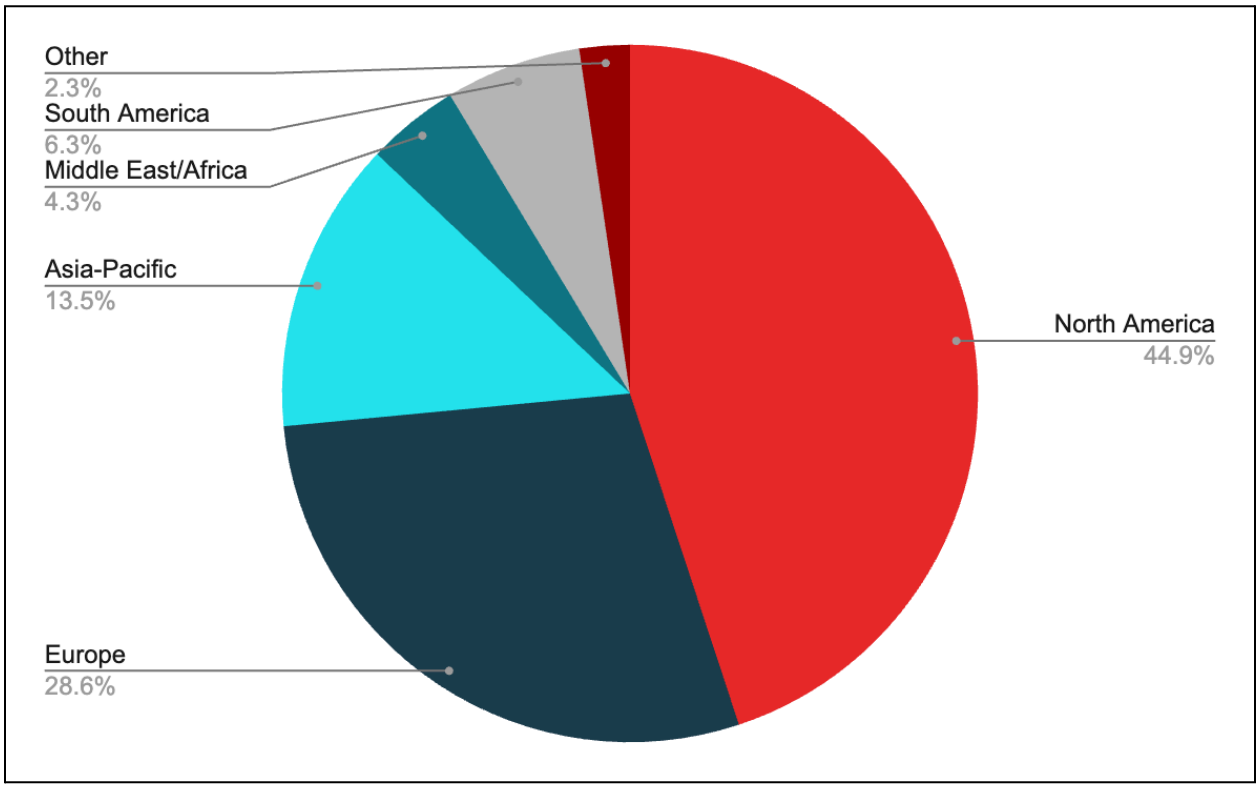
Regional Trends

While regional R&DE targeting patterns in Q2 2026 were largely consistent with those observed during previous months, the global R&DE threat landscape is shifting towards a geographic diversification. North America-based organizations were the most targeted by a substantial margin, accounting for nearly 45 percent of all Q2 2026 incidents (or at least 846 incidents). This is a notable decrease from the 54.4 percent average share observed over the previous 12 months and the 56.6 percent seen in Q2 2025—and a roughly 24 percent decrease in incident volume from Q1 2026.

- Despite this decline in global share, North America saw a 9.6 percent increase in raw incident volume year-over-year from Q2 2025—likely indicating that the region is not experiencing less targeting in absolute terms but, rather, that threat actor activity is expanding into other regions at a faster rate.

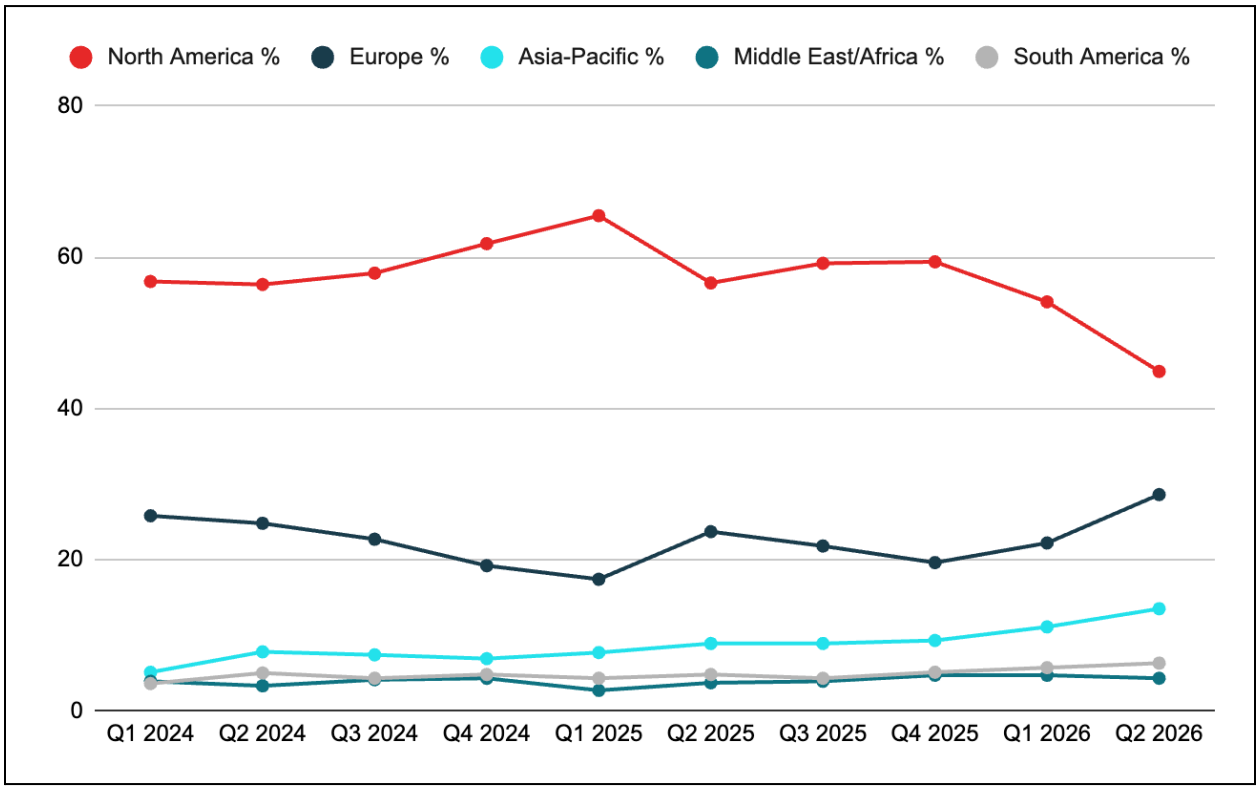
Europe-based organizations were the second most targeted group in Q2 2026, accounting for roughly 28.6 percent of all R&DE incidents—up from approximately 23.7 percent in Q2 2025 and representing a record high in both raw count and global share. Europe recorded at least 538 incidents in Q2 2026 (a 17.5 percent increase from Q1 2026 and a 66.6 percent increase year-over-year from Q2 2025), significantly outpacing the overall global incident growth rate of 38.3 percent over the same period.

- From Q1 to Q2 2026, Europe recorded a total of at least 996 incidents—a 48.4 percent increase over the 671 incidents recorded during the same period in 2025.
- This growth is part of a broader upward trend in European targeting since Q4 2025, during which Europe's share of R&DE incidents has risen each quarter to its current high of 28.6 percent—likely suggesting the region is absorbing a disproportionate share of expanding threat actor activity.



R&DE targeting by region in Q2 2026
Source: ZeroFox Intelligence

Asia-Pacific-based organizations accounted for 13.5 percent of all Q2 2026 R&DE incidents, nearly tripling the region's 5.1 percent share recorded in Q1 2024 and more than doubling its raw incident count year-over-year from 121 incidents in Q2 2025 to 255 in Q2 2026. Unlike Europe, which has experienced share volatility across the dataset, Asia-Pacific has experienced uninterrupted quarter-over-quarter share growth since Q1 2024—representing the most sustained regional R&DE targeting trend and likely indicating a structural shift in threat actor geographic focus rather than isolated campaign activity.



R&DE targeting percentage shares by region (Q1 2024–Q2 2026)
Source: ZeroFox Intelligence

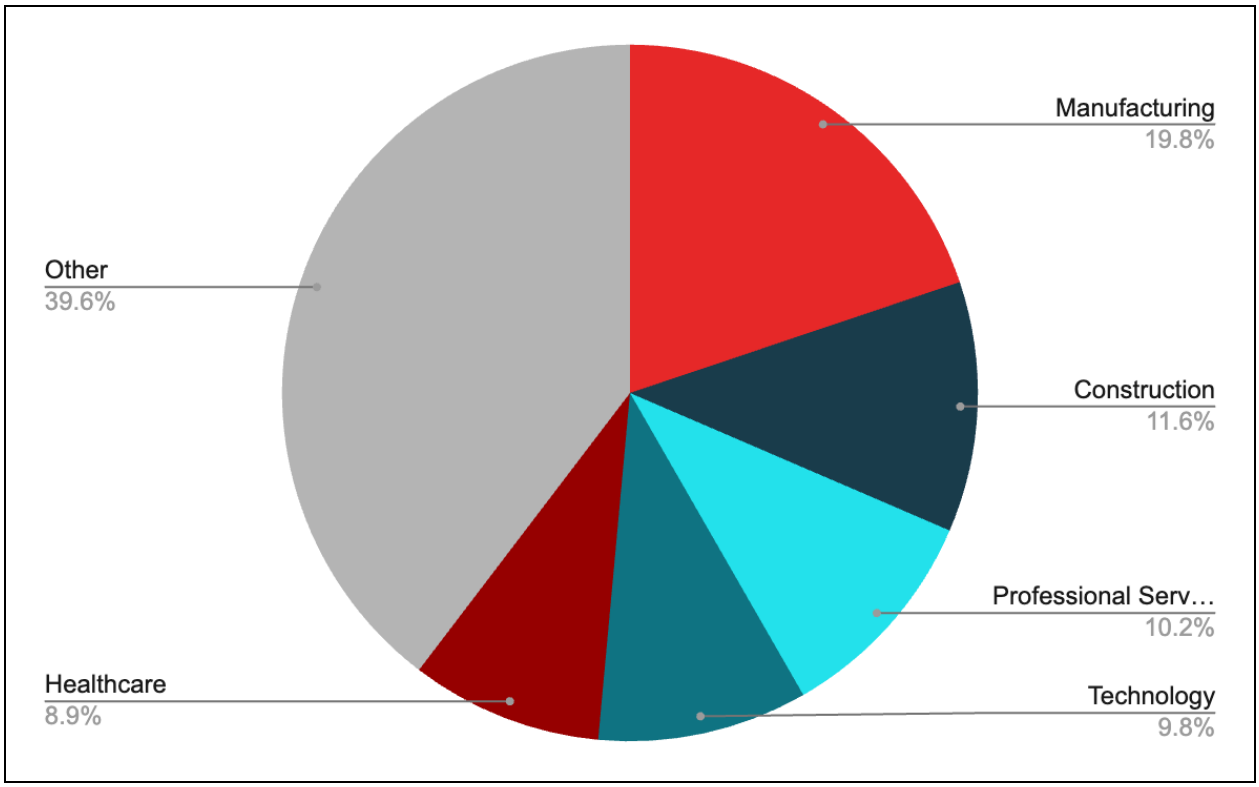
R&DE collectives typically operate opportunistically, with targeting patterns largely influenced by the availability of network accesses sold or advertised on deep and dark web forums. These patterns are further shaped by the technical capabilities and operational preferences of individual affiliate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

- The disproportionate targeting of North America-based entities is likely partly attributed to the geopolitical focus 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 almost certainly contributes to the accessibility of North American assets.

Industry Trends

In Q2 2026, ZeroFox observed that organizations in the manufacturing industry were the targets of a higher number of R&DE incidents than other industries, with at least 374 R&DE incidents (a decrease from the 419 observed in Q1 2026). Nearly 20 percent of all R&DE incidents targeted entities in the manufacturing industry in Q2 2026, which is consistent with the approximately 20 percent ZeroFox observed in Q1 2026 and Q4 2025. [Analyst Note: Manufacturing has consistently been the most targeted industry since at least 2021.]

- In Q2 2026, organizations operating within the manufacturing industry almost certainly 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 Q2 2026 included manufacturing, construction, professional services, technology, and healthcare; together, R&DE attacks on these industries accounted for approximately 60 percent of all incidents.
- In Q2 2026, R&DE targeting patterns slightly shifted away from the retail sector towards technology, whereas the top five most targeted industries in Q1 2026 remained the same as in Q4 2025.

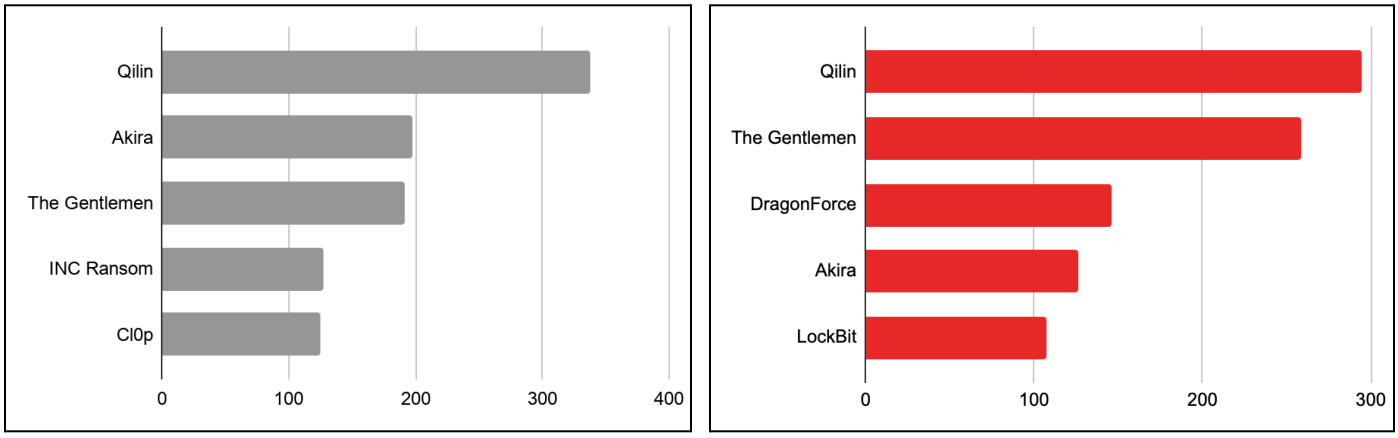


Most heavily targeted industries in Q2 2026
Source: ZeroFox Intelligence

Prominent Collectives

ZeroFox observed that the five most active R&DE collectives in Q2 2026 were almost certainly Qilin, The Gentlemen, DragonForce, Akira, and LockBit. This is a change from Q1 2026, with only Qilin, The Gentlemen, and Akira remaining in the top five over the quarter. These top five most active collectives accounted for nearly half (49.5 percent) of all global R&DE attacks in Q2 2026 (a slight increase from the previous quarter) and were responsible for a combined total of at least 933 incidents.

- Qilin remained the most prominent R&DE collective in Q2 2026, accounting for at least 295 incidents; The Gentlemen climbed to the second most prominent, replacing Akira's Q1 2026 standing.

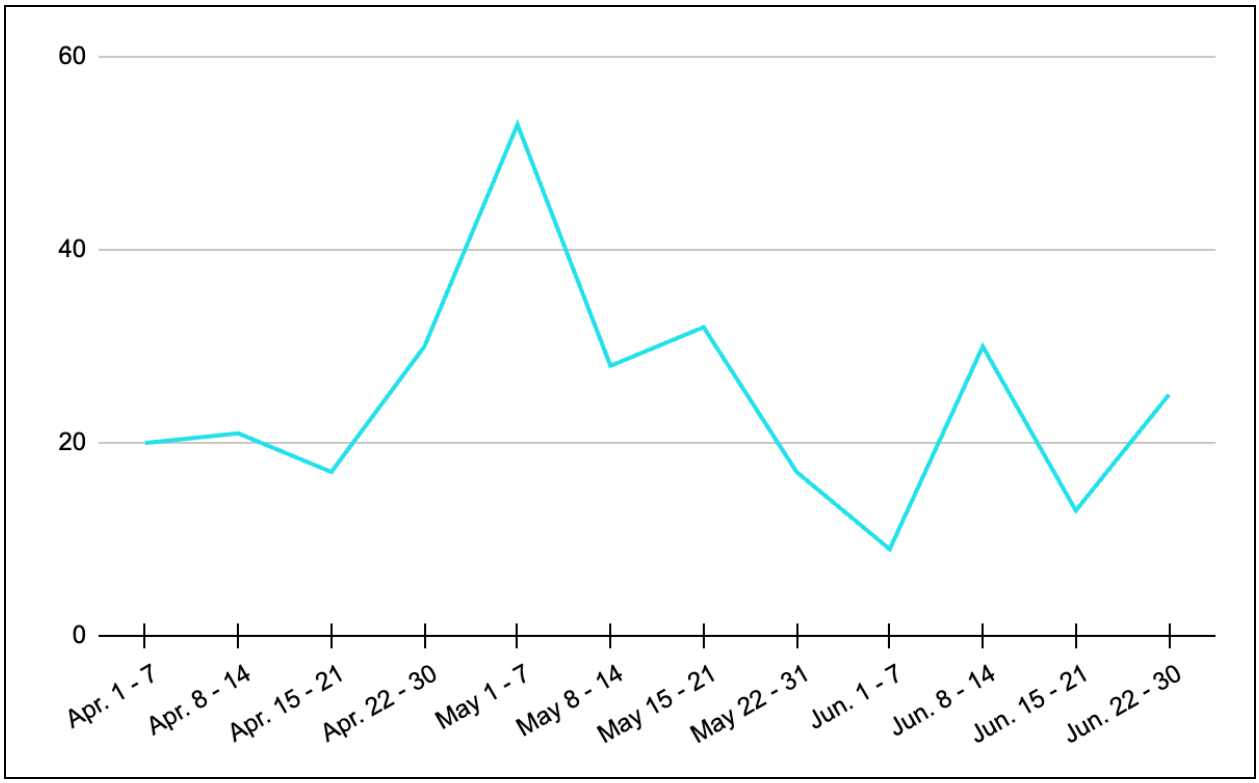


Top five most prominent R&DE collectives in Q1 2026 (left) and Q2 2026 (right)
Source: ZeroFox Intelligence

Qilin

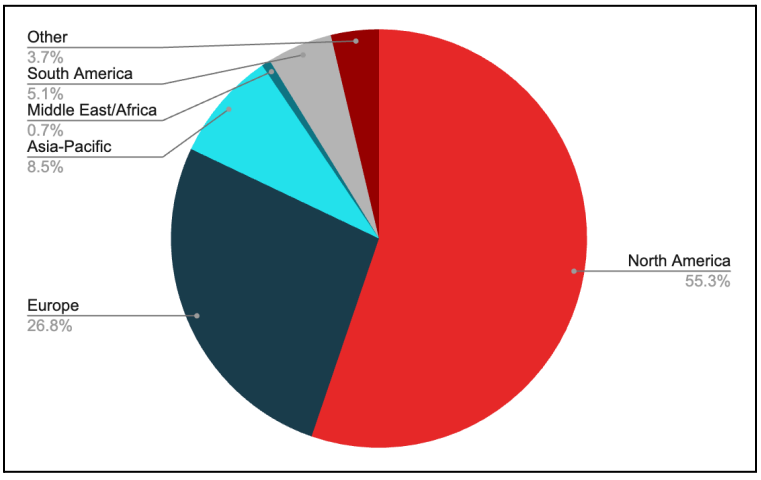
Qilin is a sophisticated Russian-language R&DE threat collective that primarily offers ransomware-as-a-service (RaaS) to its affiliates network and targets high-value critical infrastructure with its double extortion model. Qilin has continued to disproportionately target organizations in the North America region, which represents 55.3 percent of the collective's victims. Manufacturing, construction, professional services, healthcare, and retail were the top five most-targeted sectors by the collective.

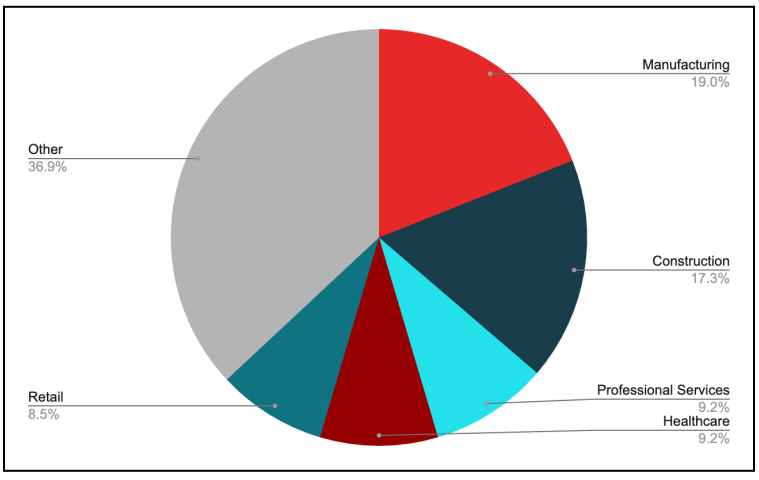
- Qilin concluded Q2 2026 as the most active ransomware collective globally (at least 295 separate incidents), signaling both its dominance in the first half of 2026 and an unbroken 12-month period as the leading ransomware threat actor that began in Q2 2025.
- The collective is very likely to continue or exceed its current operational tempo—outpacing other collectives by a substantial margin—and will likely remain consistent with its established tactics, techniques, and procedures (TTPs), targeting geographically dispersed, multi-sector entities with double-extortion operations.



Qilin's Q2 2026 R&DE incidents by week

Source: ZeroFox Intelligence





Qilin's most targeted regions (left) and industries (right) in Q2 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%