ZEROFOX INTELLIGENCE

Assessment

July 2026 Ransomware Wrap-Up

A-2026-08-07a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

August 7, 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 August 7, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

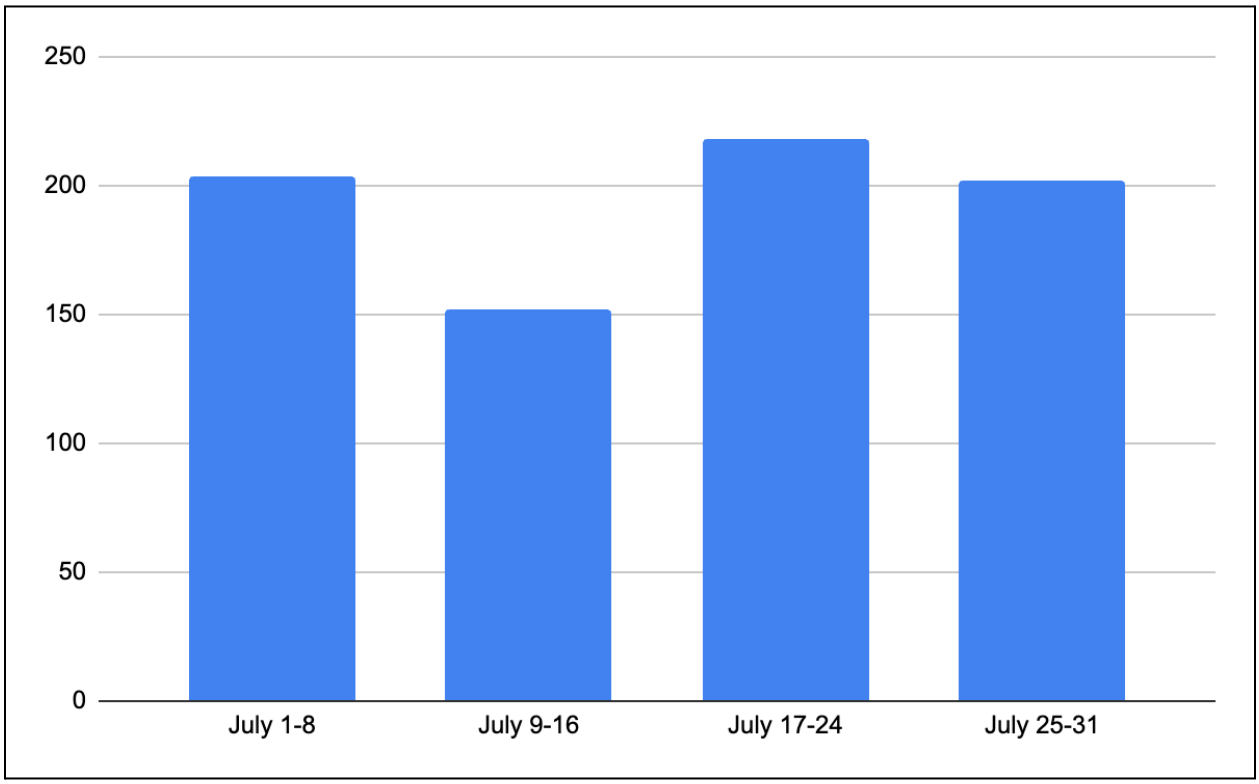
Assessment | July 2026 Ransomware Wrap-Up

Key Findings

- ZeroFox observed at least 776 separate ransomware and digital extortion (R&DE) incidents in July 2026, an increase of approximately 22 percent from June 2026. Additionally, July 2026 marked a 78 percent increase in R&DE incidents year-over-year from July 2025 and a 101 percent increase from July 2024.
- ZeroFox observed a decline in North America's global share of R&DE incidents for Q2 2026, with European organizations increasing their share. Overall, this trend continued into July 2026; North American targets saw a 12 percent decrease in year-over-year incidents from July 2025, suggesting threat actors are very likely expanding targeting efforts in other regions at a faster rate.
- The Gentlemen remained the most prominent R&DE collective in July 2026, accounting for at least 125 incidents; Qilin was the second most prominent with at least 121 incidents over the course of the month.
- Thus far, 2026 has seen an average of at least one new threat actor per week, and CRPx0 is very likely the latest new group to establish itself as a serious threat.

July 2026 Overview

ZeroFox observed at least 776 separate R&DE incidents in July 2026, an increase of approximately 22 percent from the 636 incidents recorded in June 2026. Additionally, July 2026 marked a 78 percent increase year-over-year from the 434 incidents recorded in 2025 and a 101 percent increase from the 386 incidents recorded in 2024.



R&DE incidents by week in July 2026
Source: ZeroFox Intelligence

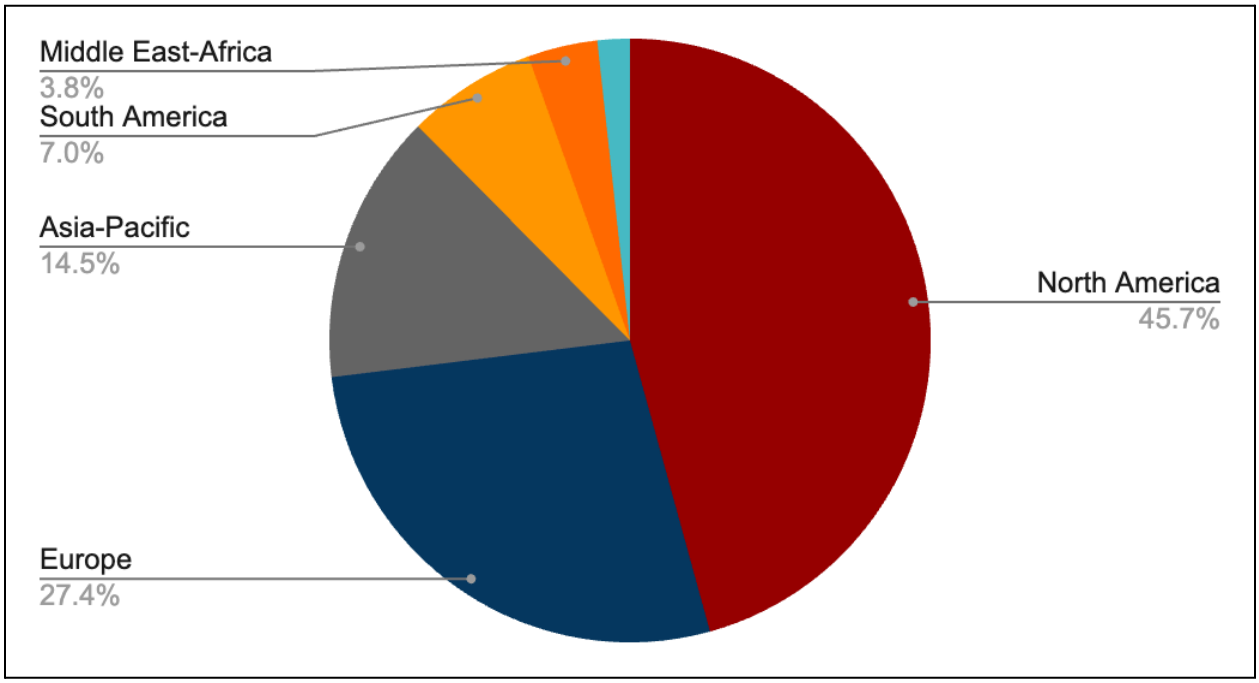
Regional Trends

While regional R&DE targeting patterns in July 2026 were largely consistent with those observed during previous months, the global R&DE threat landscape is very likely shifting toward a geographic diversification. North America-based organizations were the most targeted by a substantial margin, accounting for roughly 46 percent of all July 2026 incidents (or at least 358 incidents).

- ZeroFox had observed a decline in North America's global share of R&DE incidents for Q2 2026, with European organizations increasing their share. Overall, this trend

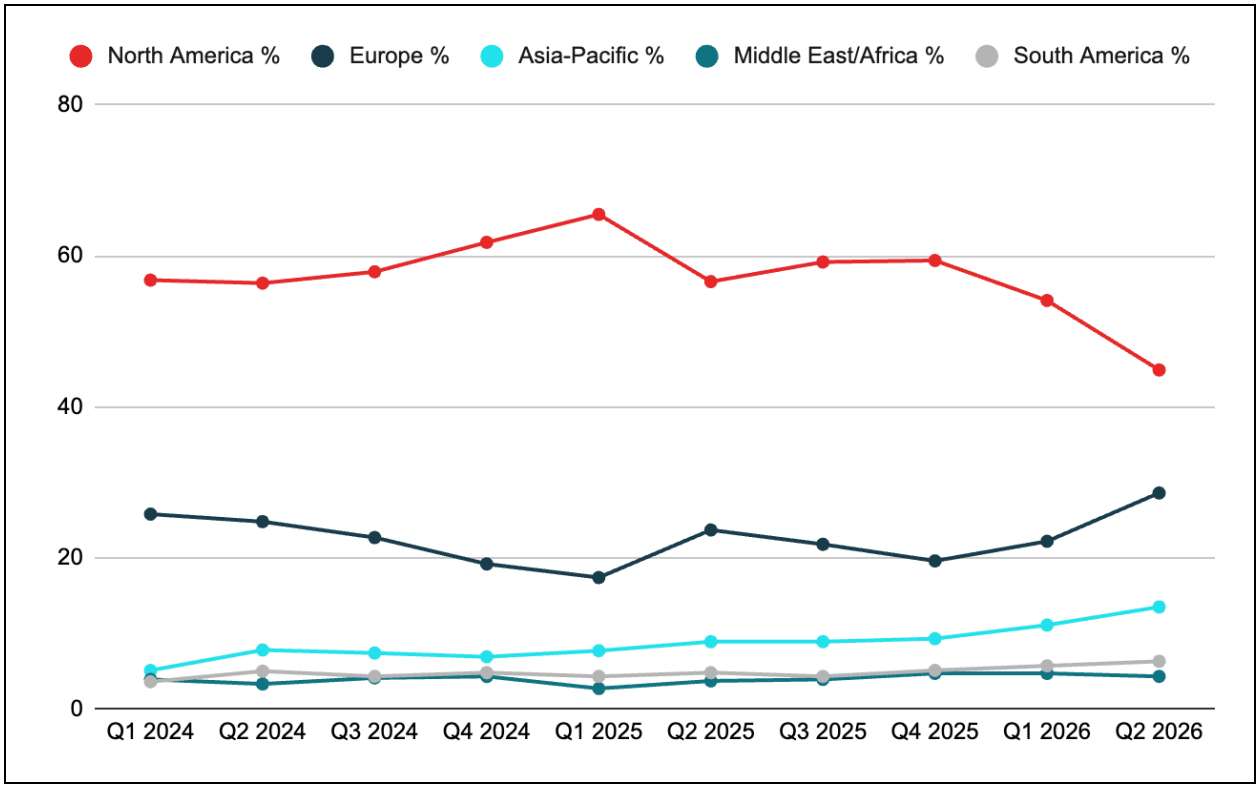
continued into July 2026; North American targets saw a 12 percent decrease in year-over-year incidents from July 2025, suggesting threat actors are very likely expanding targeting efforts in other regions at a faster rate.

Europe-based organizations were the second most targeted group in July 2026, accounting for roughly 27 percent of all R&DE incidents—down slightly from the approximately 29 percent in June 2026. Europe recorded at least 208 incidents in July 2026 (compared to at least 183 in June 2026), indicating that it will likely remain the second most targeted region in the near future.



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

Asia-Pacific (APAC)-based organizations accounted for 14 percent of all July 2026 R&DE incidents, down from the nearly 18 percent share recorded in June 2026; however, the July 2026 figure is nearly triple the approximately 5 percent observed in Q1 2024. This is an indication that threat actors very likely see APAC as a vulnerable region for targeting.



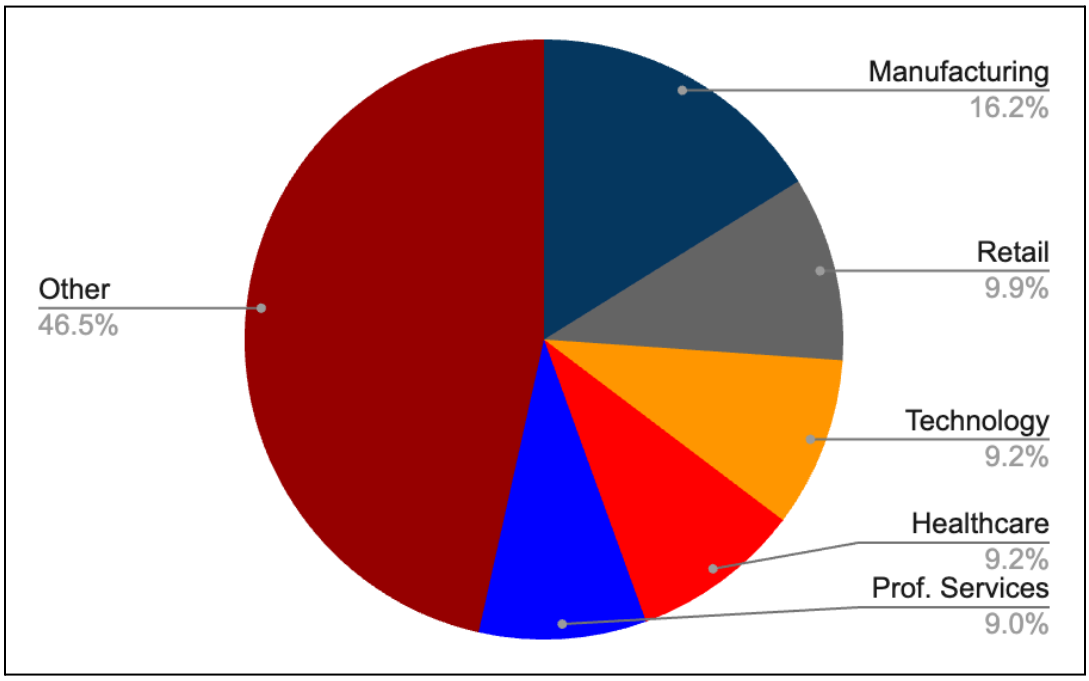
R&DE targeting by region (Q1 2024–Q2 2026)
Source: ZeroFox Intelligence

Industry Trends

In July 2026, ZeroFox observed that the manufacturing industry remained the most targeted sector, with at least 159 recorded R&DE incidents (an increase from the 138 observed in June 2026). Roughly 16 percent of all R&DE incidents in July 2026 targeted entities in the manufacturing industry, which is consistent with what ZeroFox has observed throughout 2026. Of note, manufacturing has consistently been the most targeted industry since at least 2021.

- In July 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 July 2026 included manufacturing, retail, technology, healthcare, and professional services; together, R&DE attacks on these industries accounted for approximately 55 percent of all incidents.

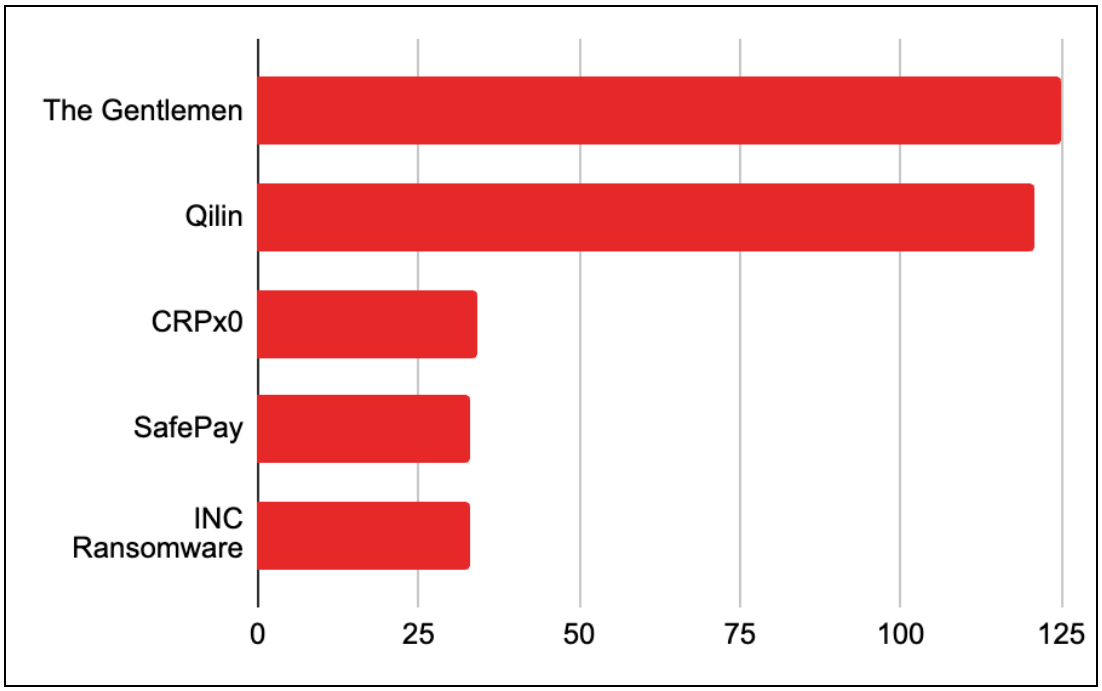


Most targeted industries in July 2026
Source: ZeroFox Intelligence

Prominent Collectives

ZeroFox observed that the five most active R&DE collectives in July 2026 were almost certainly The Gentlemen, Qilin, CRPx0, SafePay, and INC Ransomware. This is a change from June 2026, with only The Gentlemen, Qilin, and INC Ransomware remaining in the top five over the month. These top five most active collectives accounted for roughly 34 percent of all global R&DE attacks in July 2026—which is consistent with the approximately 33 percent the previous month—and were responsible for a combined total of at least 344 incidents.

- The Gentlemen remained the most prominent R&DE collective in July 2026, accounting for at least 120 incidents; Qilin was the second most prominent, with at least 118 incidents over the course of the month.



Top five most prominent R&DE collectives in July 2026
Source: ZeroFox Intelligence

CRPx0

CRPx0 is an emerging, likely Russian-language R&DE threat collective first observed when it began conducting ransomware operations in July 2026. The group was responsible for at least 34 incidents throughout the month. CRPx0 very likely started in March 2026 as a sophisticated money laundering scam but now operates a ransomware-as-a-service (RaaS) affiliate program.

- As of early August 2026, CRPx0 has already released version 2.0 of its RaaS platform despite less than a month of operation of the initial version. This indicates CRPx0 is likely an aggressive threat actor group that iterates quickly and adjusts to defensive efforts.
- Thus far, 2026 has seen an average of at least one new threat actor group per week, and CRPx0 is very likely the latest new group to establish itself as a serious threat. There is a roughly even chance the collective will continue its high pace and establish itself as one of the most active threat collectives.

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%