ZEROFOX INTELLIGENCE

Assessment

August 2026 Ransomware Wrap-Up

A-2026-09-08a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

September 8, 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 September 8, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

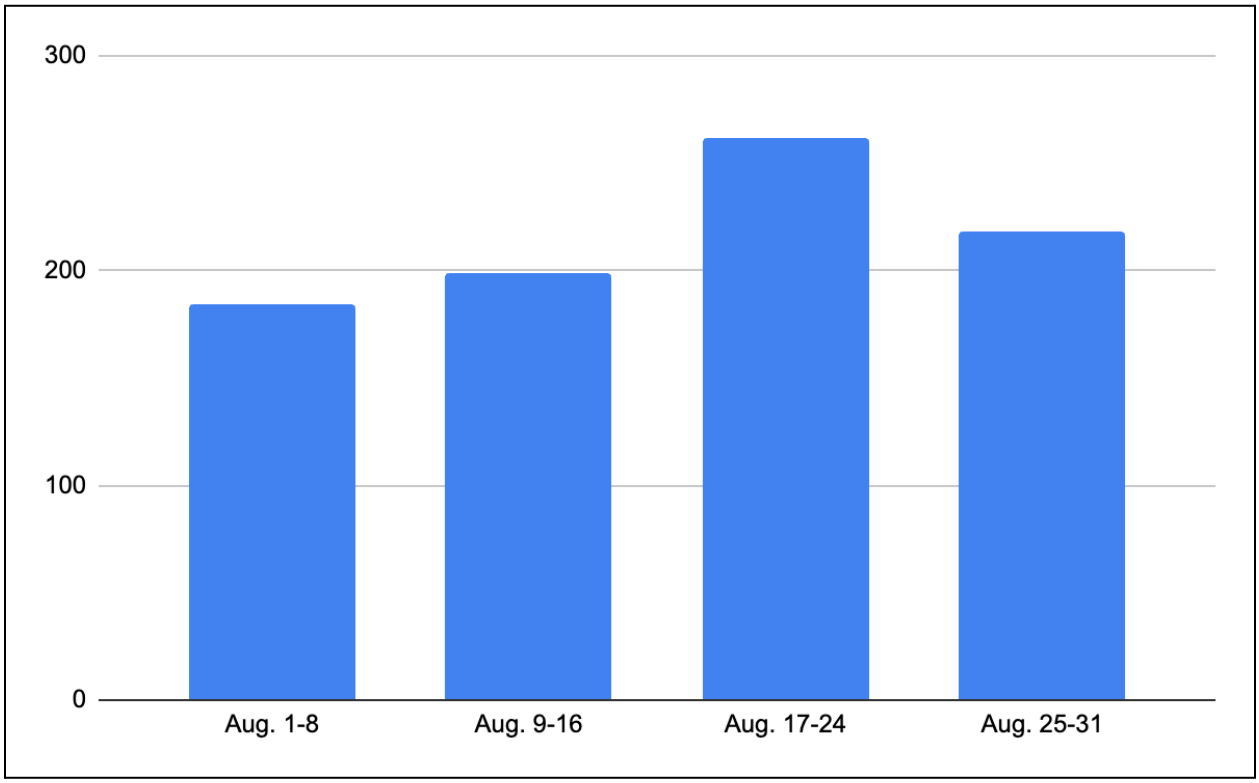
| Assessment | August 2026 Ransomware Wrap-Up

| Key Findings

- ZeroFox observed at least 863 separate ransomware and digital extortion (R&DE) incidents in August 2026, an increase of approximately 11 percent from the 776 incidents recorded in July 2026. Additionally, August 2026 marked an approximate 98 percent increase year-over-year from the 436 incidents recorded in 2025 and an approximate 121 percent increase from the 390 incidents recorded in 2024.
- North American targets saw a 50 percent increase in year-over-year incidents from August 2025; however, this was a decrease in global share from the approximate 61 percent observed in August 2025 to an approximate 46 percent observed in August 2026.
- In August 2026, ZeroFox observed that the manufacturing industry remained the most targeted sector, with at least 175 recorded R&DE incidents (an increase from the 159 observed in July 2026).
- ZeroFox observed that the five most active R&DE collectives in August 2026 were almost certainly Qilin, The Gentlemen, Cl0p, Orova, and Dire Wolf. This is a change from July 2026, with only The Gentlemen and Qilin remaining in the top five from the previous month.

August 2026 Overview

ZeroFox observed at least 863 separate R&DE incidents in August 2026, an increase of approximately 11 percent from the 776 incidents recorded in July 2026. Additionally, August 2026 marked an approximate 98 percent increase year-over-year from the 436 incidents recorded in 2025 and an approximate 121 percent increase from the 390 incidents recorded in 2024.



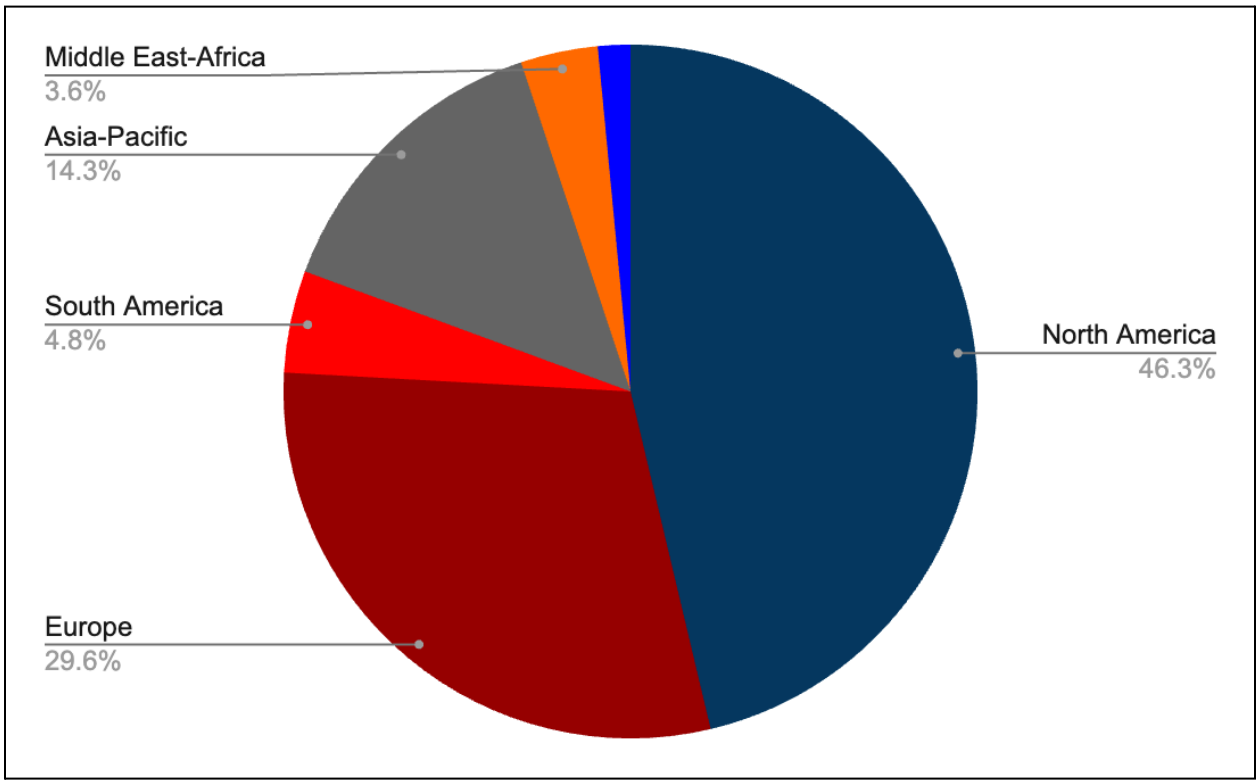
R&DE incidents by week in August 2026
Source: ZeroFox Intelligence

Regional Trends

While regional R&DE targeting patterns in August 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 August 2026 incidents (or at least 399 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 and August 2026.
- North American targets saw a 50 percent increase in year-over-year incidents from August 2025; however, this was a decrease in global share from the approximate 61 percent observed in August 2025 to an approximate 46 percent observed in August 2026.

Europe-based organizations were the second most targeted group in August 2026, accounting for roughly 30 percent of all R&DE incidents—up slightly from the approximately 27 percent in July 2026. Europe recorded at least 255 incidents in August 2026 (compared to at least 208 in July 2026), indicating that it will almost certainly remain the second most targeted region in the near future.

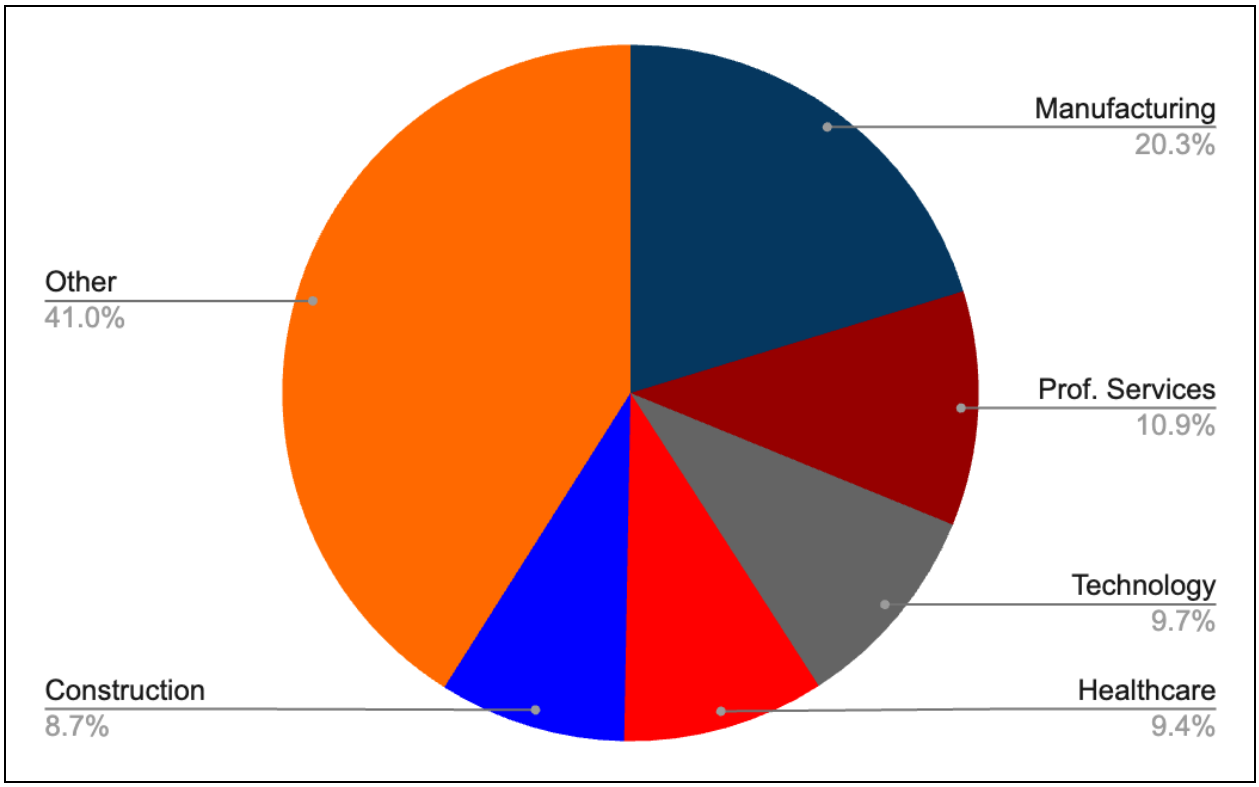


R&DE targeting by region in August 2026
Source: ZeroFox Intelligence

Industry Trends

In August 2026, ZeroFox observed that the manufacturing industry remained the most targeted sector, with at least 175 recorded R&DE incidents (an increase from the 159 observed in July 2026). Roughly 20 percent of all R&DE incidents in August 2026 targeted entities in the manufacturing industry, which is largely consistent with what ZeroFox has observed throughout 2026. Of note, manufacturing has consistently been the most targeted industry since at least 2021.

- In August 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 August 2026 included manufacturing, professional services, technology, healthcare, and construction; together, R&DE attacks on these industries accounted for approximately 59 percent of all incidents.

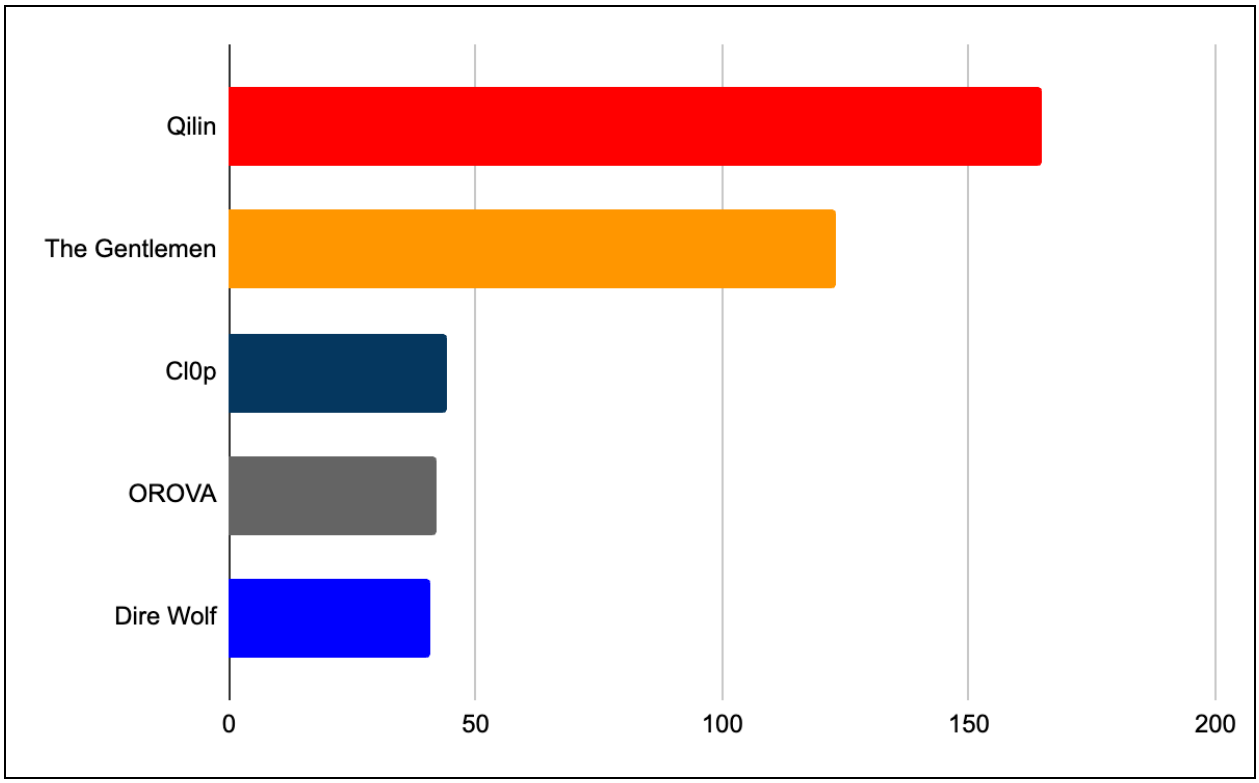


Most targeted industries in August 2026
Source: ZeroFox Intelligence

Prominent Collectives

ZeroFox observed that the five most active R&DE collectives in August 2026 were almost certainly Qilin, The Gentlemen, Cl0p, Orova, and Dire Wolf. This is a change from July 2026, with only The Gentlemen and Qilin remaining in the top five from the previous month. These top five most active collectives accounted for roughly 48 percent of all global R&DE attacks in August 2026—which is significantly higher than the approximately 34 percent the previous month—and were responsible for a combined total of at least 415 incidents.

- Qilin was the most prominent R&DE collective in August 2026, accounting for at least 165 incidents—a record number of incidents for one collective so far this year. The Gentlemen was the second most prominent, with at least 123 incidents over the course of the month.



Top five most prominent R&DE collectives in August 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%