



| Assessment |

September 2026 Ransomware Wrap-Up

A-2026-10-07a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Digital Extortion, Threat Actor

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

Assessment | September 2026 Ransomware Wrap-Up

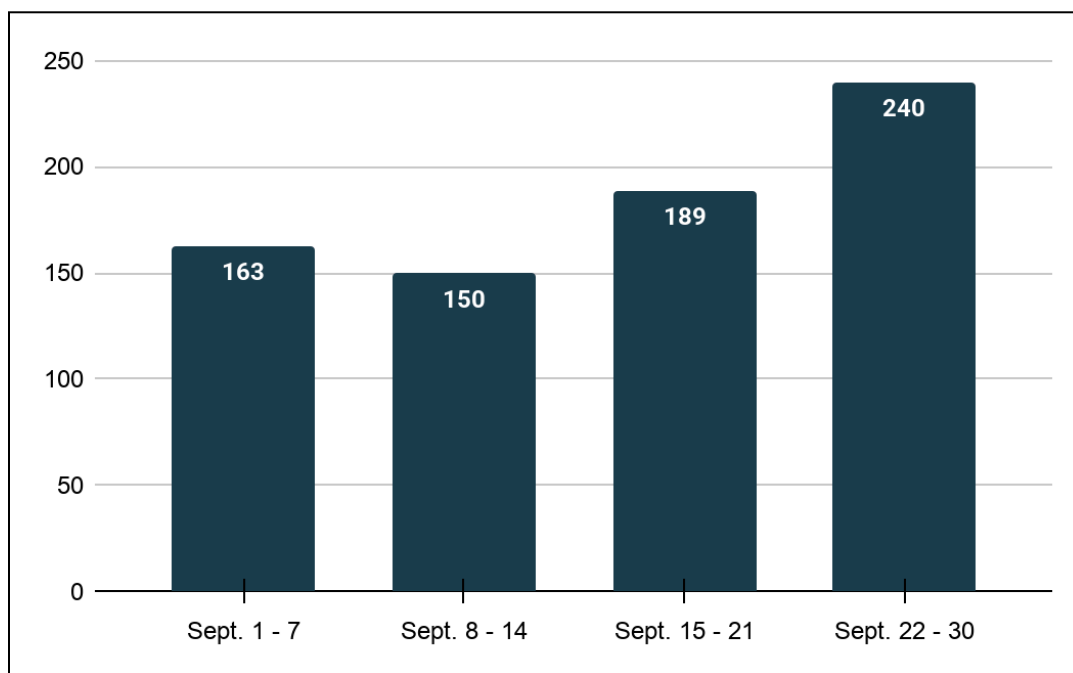
Key Findings

- In September 2026, ZeroFox recorded at least 742 ransomware and digital extortion (R&DE) incidents, which was roughly 14 percent fewer than in August but approximately 33 and 80.5 percent more than in September 2025 and September 2024, respectively.
- North America remained the top targeted region, with roughly 47 percent of September's incidents (at least 350). However, its year-over-year growth of approximately 7 percent lagged well behind the global rate of about 33 percent, shrinking its regional share of R&DE incidents from roughly 59 percent a year earlier.
- Manufacturing was again the most heavily targeted industry, with at least 150 incidents (down from 175 in August), while healthcare climbed to second place with at least 82 incidents.
- The Gentlemen, Qilin, Akira, INC Ransom, and Storm were almost certainly the five most active collectives in September 2026, with The Gentlemen and Qilin the only two that carried over from August's top five.

- Q3 2026 saw a new quarterly record of at least 2,381 R&DE incidents, approximately 14 percent above the previous high set in Q4 2025 and roughly 67 percent above Q3 2025. This very likely indicates an acceleration in global R&DE activity in the second half of the year heading into Q4 2026.

September 2026 Overview

ZeroFox observed at least 742 separate R&DE incidents in September 2026, a decrease of approximately 14 percent from the 863 incidents recorded in August 2026. Additionally, September 2026 marked an approximate 33 percent increase year-over-year from the 557 incidents recorded in September 2025 and an approximate 80.5 percent increase from the 411 incidents recorded in September 2024.



R&DE incidents by week in September 2026

Source: ZeroFox Intelligence

Regional Trends

North America-based organizations remained the most targeted in September 2026, accounting for approximately 47 percent of all R&DE incidents (at least 350 incidents). Although this represents an approximate 7 percent increase in regional incident volume

from the 327 incidents recorded in September 2025, it significantly trails the overall global growth rate of approximately 33 percent over the same period.

- As a result, North America's share of R&DE incidents fell from approximately 59 percent in September 2025, further supporting the likelihood that threat actor activity is expanding into other regions at a faster rate.
- North America's share of R&DE incidents rose slightly from the roughly 46 percent observed in August 2026, but this was likely the result of a sharp decline in European targeting rather than a reflection of increased activity in North America, as there was an approximate 12 percent decrease in incidents in North America in September 2026 as compared to August.

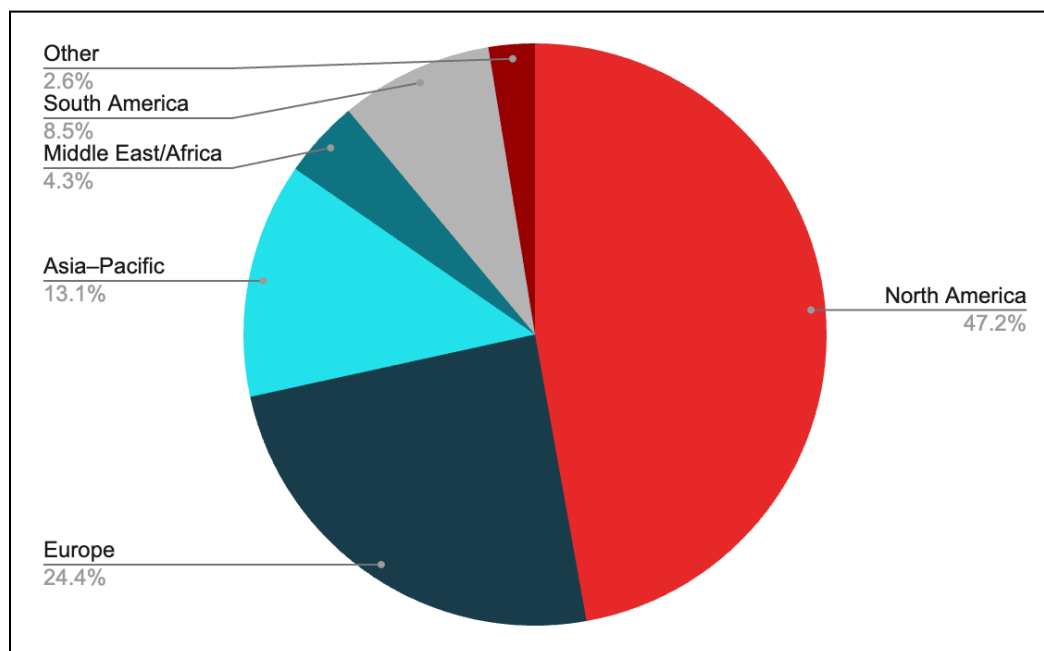
Europe-based organizations were the second most targeted region in September 2026, accounting for approximately 24 percent of all R&DE incidents (at least 181 incidents). This marks a sharp decline from August 2026's 255 incidents, when Europe accounted for roughly 30 percent of R&DE incidents, with volume falling approximately 29 percent in September. Europe alone accounted for roughly 61 percent of September's overall month-over-month decline of 121 incidents.

Asia-Pacific-based organizations accounted for approximately 13 percent of all September 2026 R&DE incidents (at least 97 incidents), largely consistent with the region's elevated share throughout 2026 and an approximate 47 percent increase year-over-year from the 66 incidents recorded in September 2025.

South America-based organizations accounted for approximately 8.5 percent of all September 2026 R&DE incidents (at least 63 incidents), more than double the 26 incidents recorded in September 2025 and the steepest year-over-year growth rate of any region (approximately 142 percent). This monthly share exceeds any quarterly share recorded for the region since at least Q1 2024 and is consistent with South America's steady share growth over the past four quarters.

- Collectively, Asia-Pacific, South America, and the Middle East/Africa accounted for approximately 26 percent of all September 2026 R&DE incidents, up from roughly 20 percent in September 2025, while North America and Europe's combined share fell from approximately 78 to 72 percent. This shift further demonstrates that the

global R&DE threat landscape is very likely undergoing a sustained geographic diversification.



R&DE targeting by region in September 2026

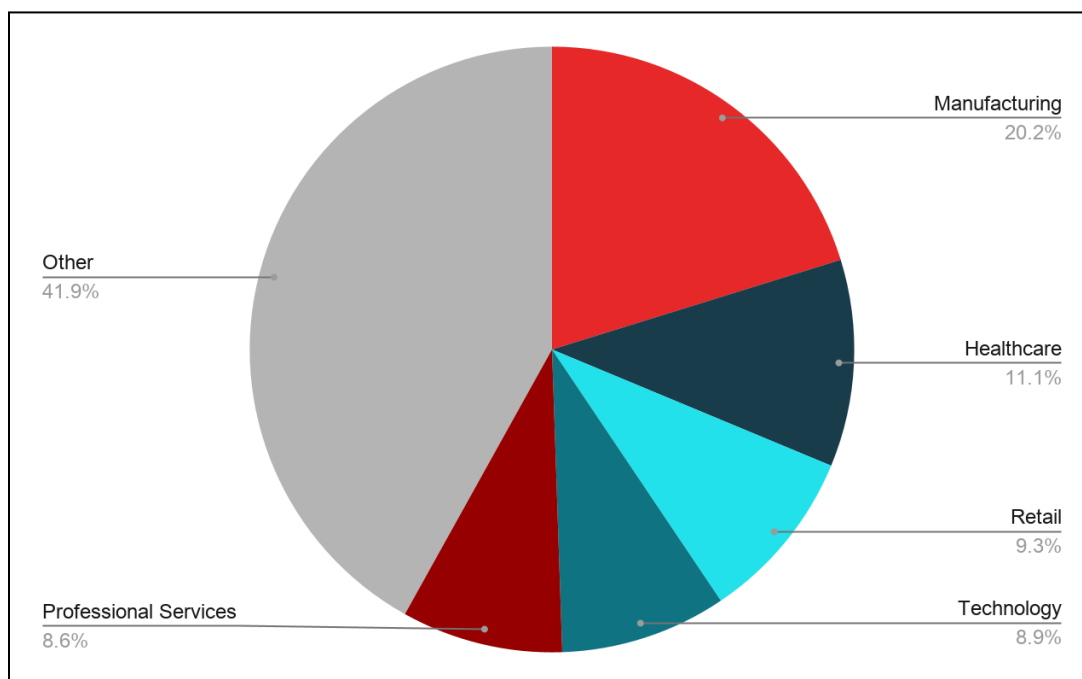
Source: ZeroFox Intelligence

Industry Trends

ZeroFox observed that the manufacturing industry remained the most targeted sector in September 2026, with at least 150 recorded R&DE incidents (a decrease from the 175 observed in August 2026). Roughly 20 percent of all R&DE incidents in September 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 September 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 September 2026 included manufacturing, healthcare, retail, technology and professional services; together, R&DE attacks on these industries accounted for approximately 58 percent of all incidents.
- The healthcare industry rose to the second most targeted sector in September 2026, with at least 82 incidents (approximately 11 percent), up from fourth in August 2026. Retail returned to the top five, while construction dropped out and professional services fell from second to fifth.



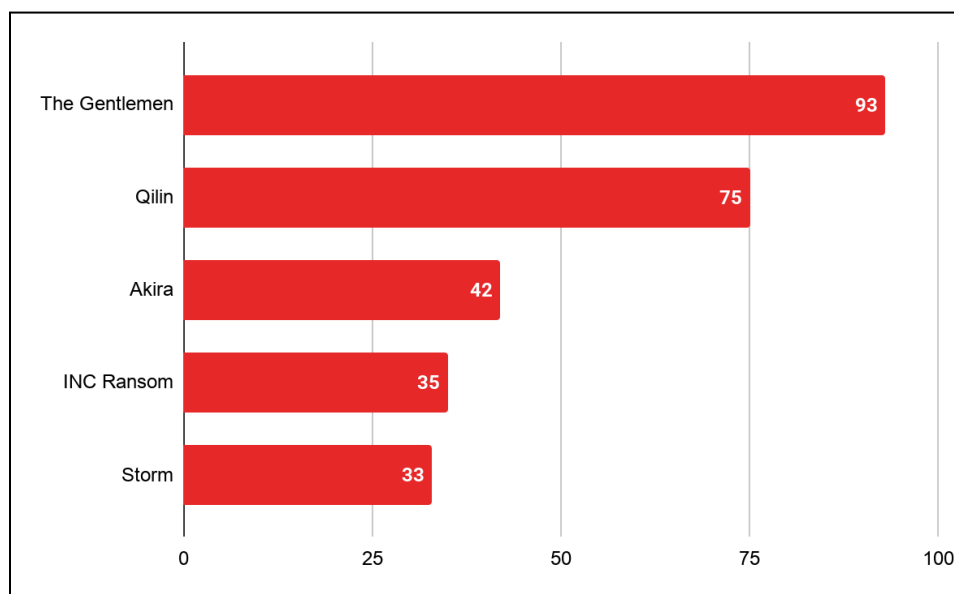
Most targeted industries in September 2026

Source: ZeroFox Intelligence

Prominent Collectives

ZeroFox observed that the five most active R&DE collectives in September 2026 were almost certainly The Gentlemen, Qilin, Akira, INC Ransom, and Storm. This is a change from the previous month, with only The Gentlemen and Qilin remaining in the top five from August 2026. These top five most active collectives accounted for roughly 37 percent of all global R&DE attacks in September 2026, which is significantly lower than the approximately 48 percent the previous month, and were responsible for a combined total of at least 278 incidents.

- The Gentlemen was the most prominent R&DE collective in September 2026, accounting for at least 93 incidents. Qilin was the second most prominent, with at least 75 incidents over the course of the month.



Top five most prominent R&DE collectives in September 2026

Source: ZeroFox Intelligence

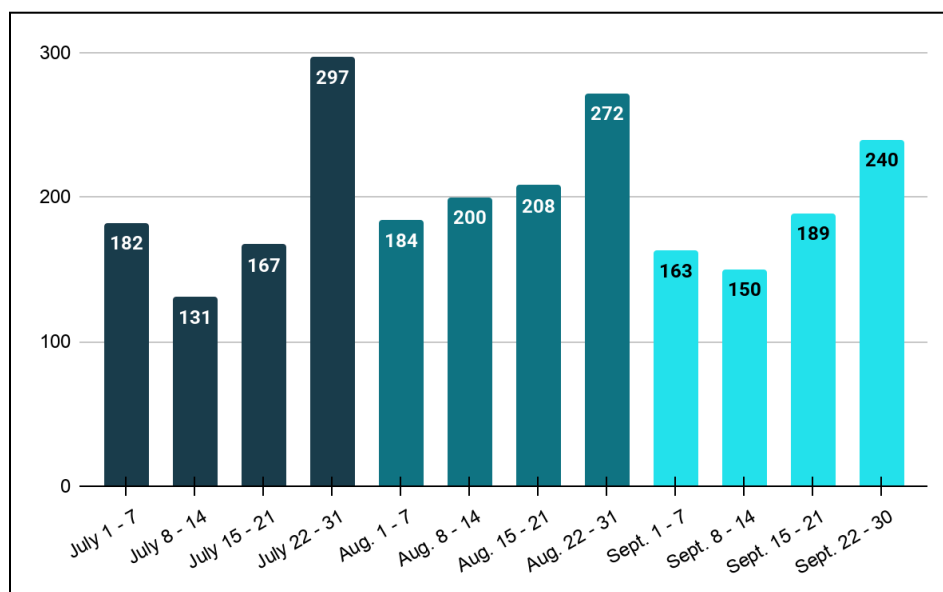
Q3 2026 Overview

ZeroFox observed at least 2,381 separate R&DE incidents in Q3 2026, which is the highest quarterly total on record and approximately 14 percent above the previous record of 2,091 incidents set in Q4 2025. This is particularly notable given that Q4 was the most active quarter in each year from 2023 to 2025, which suggests that Q4 2026 is likely to exceed this new record.

- ZeroFox has observed at least 6,325 R&DE incidents throughout the first three quarters of 2026, an increase of approximately 32 percent from the 4,793 incidents recorded during the same period in 2025.
- This means R&DE incidents to date in 2026 fall just 559 short of 2025's full-year total of 6,884. At least 618 incidents have been recorded every month so far in 2026, making it very likely that R&DE incident totals in October 2026 will surpass 2025's annual total.

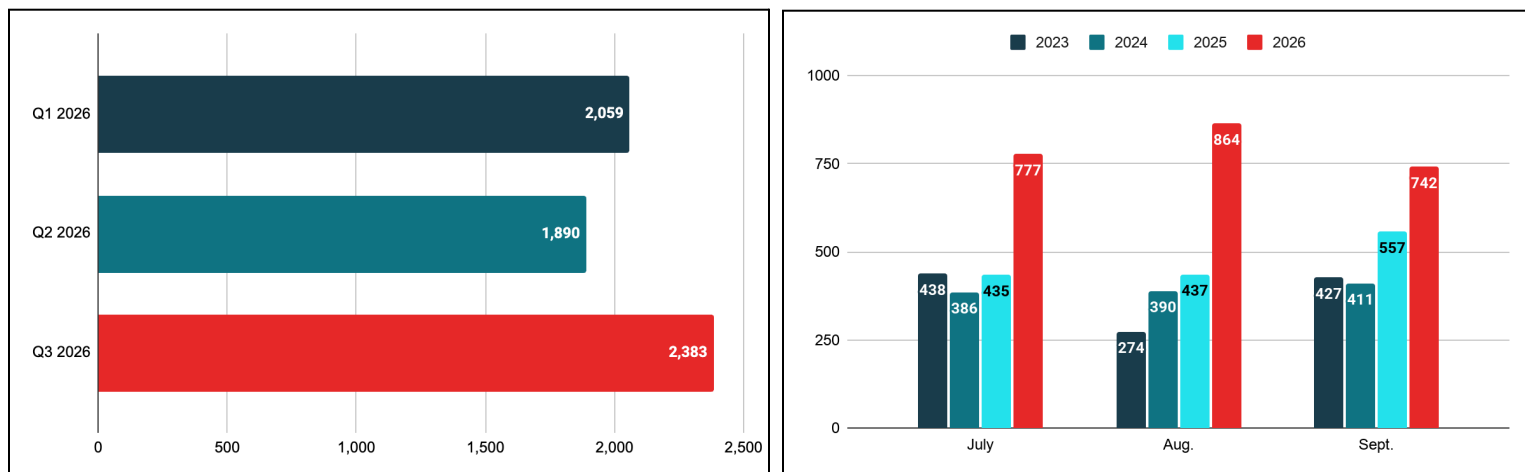
July 2026 saw at least 776 incidents, an approximate 78 percent increase from July 2025, while August 2026 recorded at least 863 incidents—nearly double the 436 incidents observed in August 2025. September 2026 broke an established seasonal pattern: in 2023, 2024, and 2025, September recorded more incidents than August. However, September 2026's 742 incidents marked a decrease of approximately 14 percent from August.

- Although September 2026 still represented an approximate 33 percent year-over-year increase, this growth rate was substantially lower than that seen in the months of July and August 2026 compared to July and August 2025.



R&DE incidents by week in Q3 2026

Source: ZeroFox Intelligence



R&DE incidents by quarter in 2026 (left) and Q3 R&DE incidents from 2023 to 2026 (right)

Source: ZeroFox Intelligence

Q3 2026 marked an increase of approximately 67 percent year-over-year from the 1,429 incidents recorded in Q3 2025 and was roughly double the 1,187 incidents recorded in Q3 2024. This growth significantly outpaces the 38.3 percent year-over-year increase observed in Q2 2026, very likely indicating an acceleration in global R&DE activity in the second half of the year.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%