Q4 | 2025

Q4 North American Retail

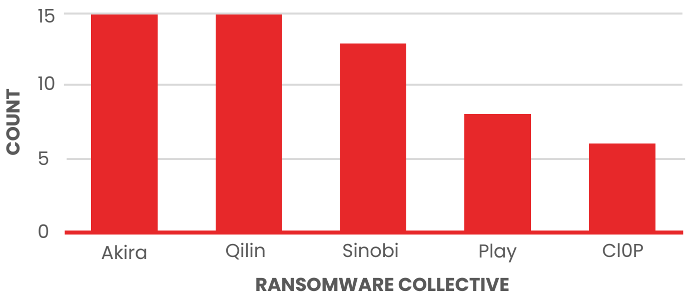
Quarterly Threat Landscape Overview

TLP:CLEAR A-2026-01-16a

ZEROFOX

Ransomware & Digital Extortion (R&DE)

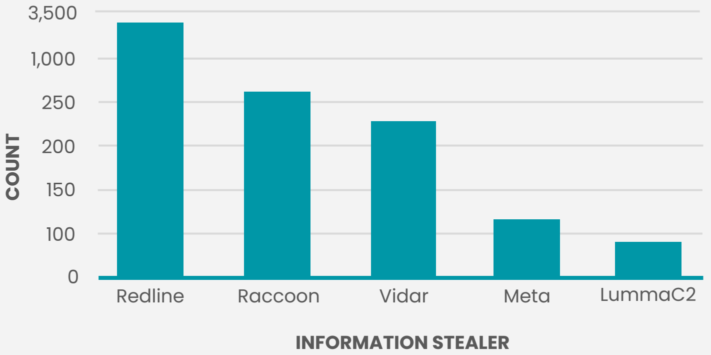
THREAT LEVEL



- In Q4 2025, the retail sector was targeted in nearly 7.6 percent of global R&DE incidents, equating to at least 164 attacks. This is roughly 8 percent more than Q3 2025.
- There were at least 1,247 R&DE attacks targeting entities in North America during Q4 2025. Retail accounted for nearly 5 percent of the total R&DE attacks, making it the fifth most impacted industry in the region.
- The top five most targeted industries in North America for Q4 2025 were manufacturing, professional services, construction, healthcare, and retail. The retail sector's share of all North American incidents rose slightly, indicating that, while overall attacks are increasing, other sectors continue to attract a larger portion of targeting.

Malware

THREAT LEVEL



- Redline was the most commonly observed information stealer targeting North American-based organizations in Q4 2025.
- Similar to other information-stealing malware, Redline is advertised in underground deep and dark web forums as a malware-as-a-service (MaaS) information-stealing trojan that targets user credentials and cryptocurrency wallets.
- Throughout 2026, infostealers will almost certainly continue to pose a significant cyber threat to organizations and industries in North America and around the globe.

Social Engineering

THREAT LEVEL

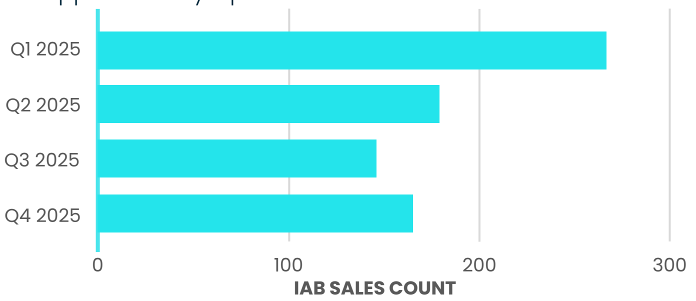
Threat actors continue to utilize social engineering techniques against the North American retail industry in order to gain initial network access.

- Ransomware collectives have been relying on social engineering tactics to infiltrate networks of entities in the retail industry, where human error remains a predominant threat vector.
- Threat actors almost certainly perceive attacking this sector as a low-risk, high-payoff activity due to its customer-facing aspects and opportunistic value.
- A series of several prominent, socially engineered cyberattacks on various European-based retail stores in the first half of 2025 very likely led to an overall increase in social engineering attacks globally—specifically in North America. In 2025, threat actors were observed increasingly relying on social engineering attacks against the retail sector.

Initial Access Brokers (IABs)

THREAT LEVEL

- North America accounted for approximately 36 percent of all IAB sales that took place in Q4 2025; in 2024, the region accounted for nearly 43 percent of total IAB sales. This decline very likely represents a diversification of target regions by threat actors, as they likely perceive Europe-based and other global organizations as increasingly lucrative.
- Of the 164 IAB sales that impacted North American-based entities in Q4 2025, roughly 3.5 percent targeted the retail sector (slightly lower than the global average of approximately 7 percent.



ZEROFOX

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 9:00 AM (EST) on January 14, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.