ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

December 27, 2025

ZEROFOX®
Weekly Intelligence Brief

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. 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 6:00 AM (EST) on December 25, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Major Ransomware Attack on Romanian Water Management Authority

What we know:

- Romania's cybersecurity agency has confirmed a ransomware attack targeting approximately 1,000 IT systems in regional water administrative units.
- While the ransomware attack affected the Geographic Information System (GIS) server, databases, email, web services, Windows workstations, and other systems, services remained unaffected.

Background:

- Threat actors exploited built-in Windows BitLocker encryption to lock files for ransom demand.
- While investigations remain ongoing, no specific threat actor or group has publicly claimed responsibility, as of writing.

Analyst note:

- The development comes as multiple European countries have blamed Russia for escalating cyberattacks targeting their critical infrastructure entities for supporting Ukraine.
- Multiple European countries are very likely to experience an escalation in cyberattacks targeting their critical infrastructure as the Ukraine-Russia conflict rages on.
- There is a roughly even chance that Russian threat actors, including state-sponsored ones, are behind the Romanian ransomware attack.

United States Charges 54 Individuals for ATM Jackpotting Using Ploutus Malware

What we know:

- The U.S. government has accused 54 individuals of stealing millions of dollars through Automated Teller Machine (ATM) jackpotting, a type of cyber and physical attack, in the United States.

- The accused individuals are allegedly linked to Venezuelan terrorist organization Tren de Aragua (TdA).

Background:

- The accused first carried out external reconnaissance at target ATMs, before opening the hood or door of the machines to install a hard drive infected with Ploutus malware.
- The malware would issue unauthorized commands associated with the Cash Dispensing Module of the ATM in order to force withdrawals of currency.

Analyst note:

- Law enforcement action is likely to help recover at least part of the stolen funds from the accused and block any associated money laundering network.
- The development also calls for the need for stronger external security measures and alarms to prevent criminals from physically tampering with ATMs and deploying malware-infected hard drives.

Malicious Npm Package Snoops on WhatsApp Chats, Steals Credentials

What we know:

- A malicious npm package called “lotusbail”, designed as a fully functional WhatsApp Application Programming Interface (API), has been found capable of stealing WhatsApp credentials, intercepting messages, harvesting contacts, and ensuring persistent access.

Background:

- Users have downloaded the npm package at least 56,000 times since it was first uploaded in May 2025 by user "seiren_primrose". The npm package contains a malicious WebSocket wrapper that routes authentication information and messages, enabling the threat actor to capture credentials and messages.

Analyst note:

- Such malicious npm packages are very likely to aid large-scale supply chain attacks through which threat actors can capture vast amounts of sensitive data and credentials. Copycat packages are likely to crop up in the future posing and functioning as legitimate tools, while hiding malicious codes.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, one on December 19 and the other on December 22. Of these, CVE-2025-14733 is a critical remote code execution (RCE) vulnerability infecting over 115,000 internet-exposed WatchGuard Firebox firewalls. It also released 10 Industrial Control System (ICS) advisories on December 18 and December 23. Threat actors are distributing info-stealing backdoor through malicious GitHub repositories that masquerade as proof-of-concept exploits for recently disclosed vulnerabilities, including CVE-2025-59295, CVE-2025-10294, and CVE-2025-59230. Hewlett Packard Enterprise Company (HPE) has patched a critical vulnerability (CVE-2025-37164) in its OneView software that enabled RCE by unauthenticated attackers.

HIGH

CVE-2023-52163

What happened: Attackers are actively exploiting this missing authorization vulnerability in DigiEver DS-2105 Pro network video recorders that enables remote, unauthenticated command execution through the time_tzsetup[.]cgi interface. CISA has added the flaw to its KEV catalog.

- **What this means:** Organizations using video recorders with CVE-2023-52163 risk losing control of their surveillance environments, as active exploitation is likely to enable attackers to manipulate footage, disable monitoring, or covertly intrude on corporate networks. They can effectively turn unpatched security infrastructure into an attack surface before the January 12, 2026, federal patch deadline.
- **Affected products:**
  - Digiever DS-2105 Pro 3.1.0.71-11 devices

CRITICAL

CVE-2025-68613

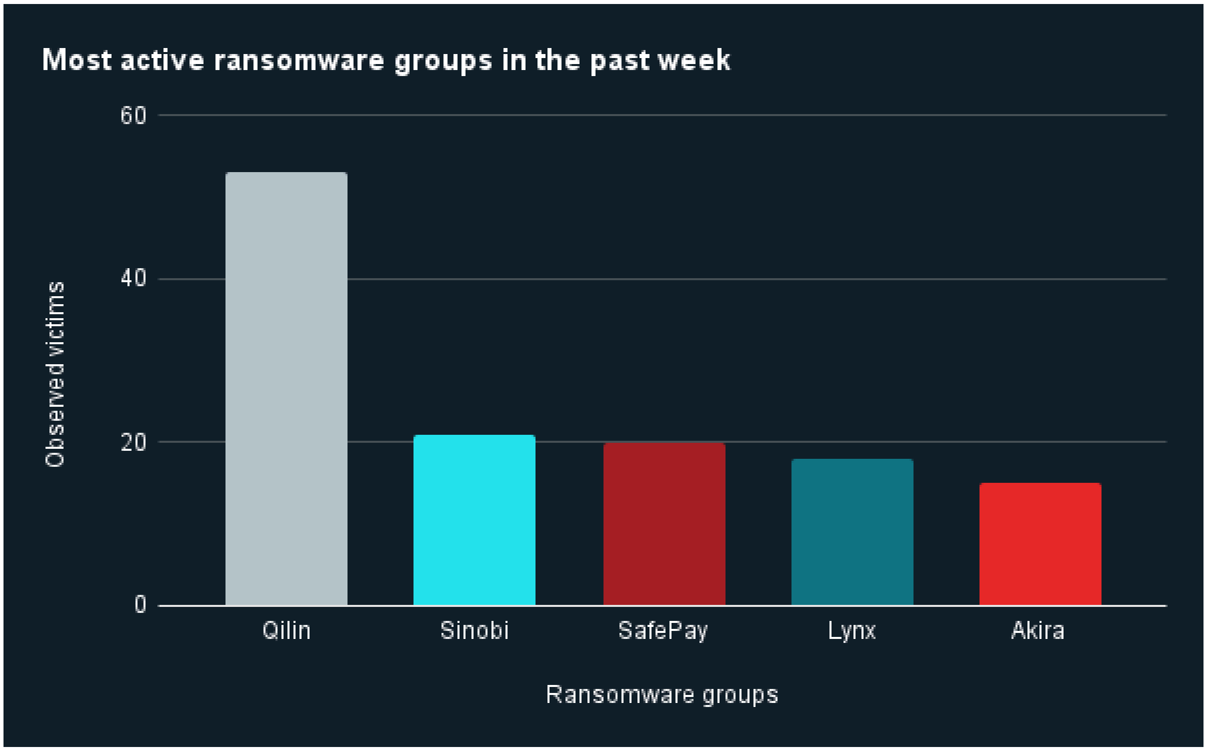
What happened: N8n has patched this critical RCE vulnerability that enabled authenticated users to run arbitrary code via workflow expressions. Researchers identified more than 103,000 exposed instances worldwide, and fixes were released in versions 1.120.4, 1.121.1, and 1.122.0.

- **What this means:** Threat actors are likely to exploit unpatched, internet-facing n8n instances to fully take over automation servers, steal credentials, manipulate workflow, and conduct system-level command execution. Additionally they are likely to exploit the bug to pivot deeper into internal networks, leaving organizations, particularly across the United States and Europe, vulnerable to large-scale compromise.
- **Affected products:**
  - All n8n versions from 0.211.0 up to, but not including, 1.120.4

Ransomware and Breach Intelligence

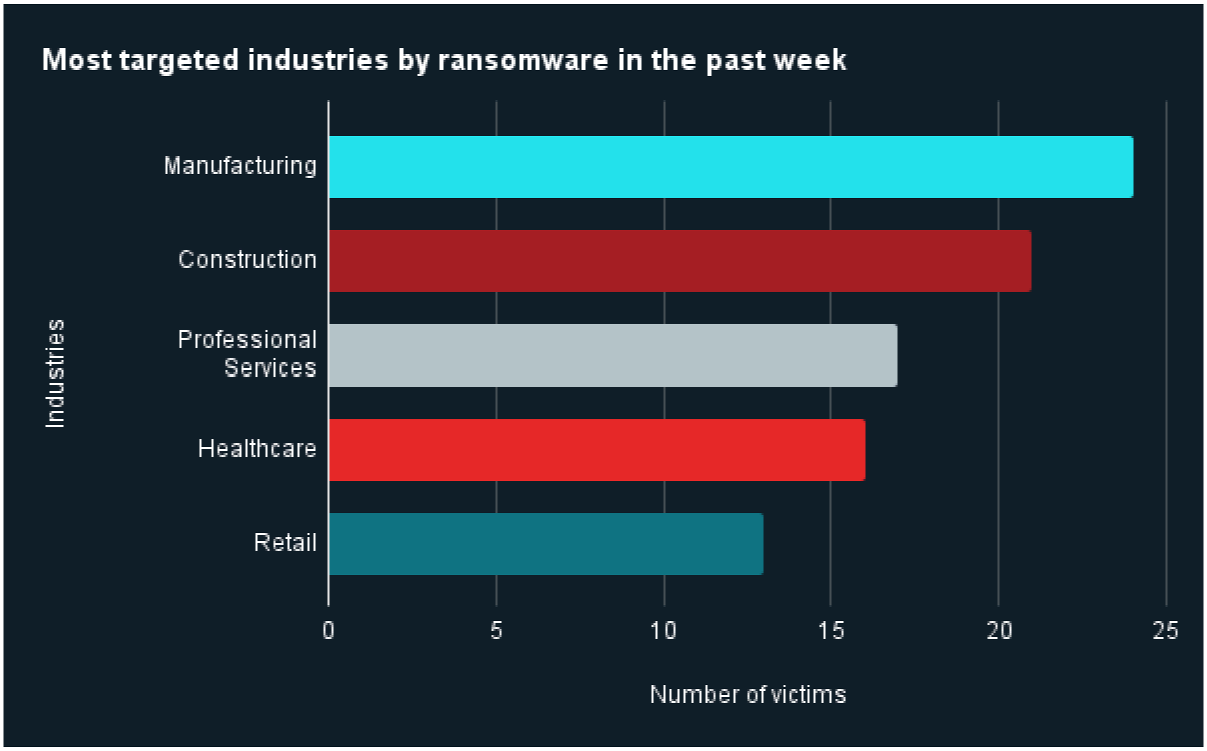
Ransomware and Breach Intelligence Key Findings

Ransomware Groups' Activities Across Industries and Regions



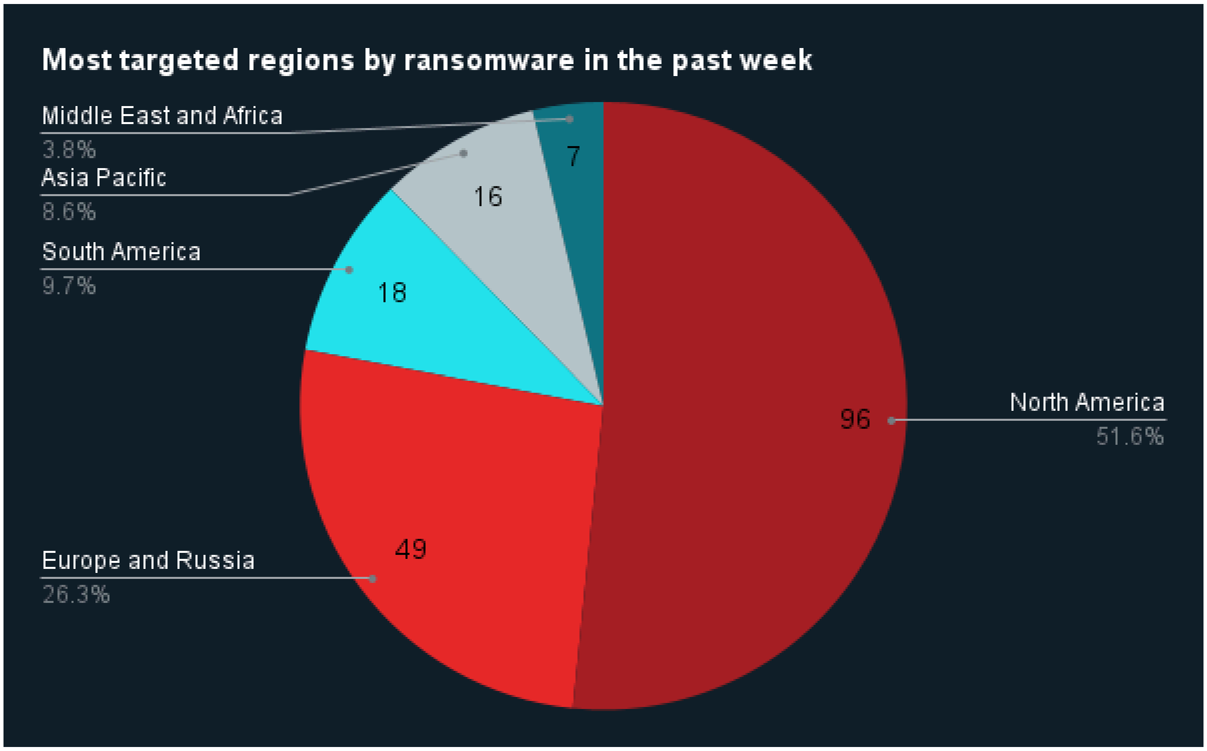
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Sinobi, SafePay, Lynx, and Akira were the most active ransomware groups. ZeroFox observed close to 161 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Sinobi.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by construction.



Source: ZeroFox Internal Collections

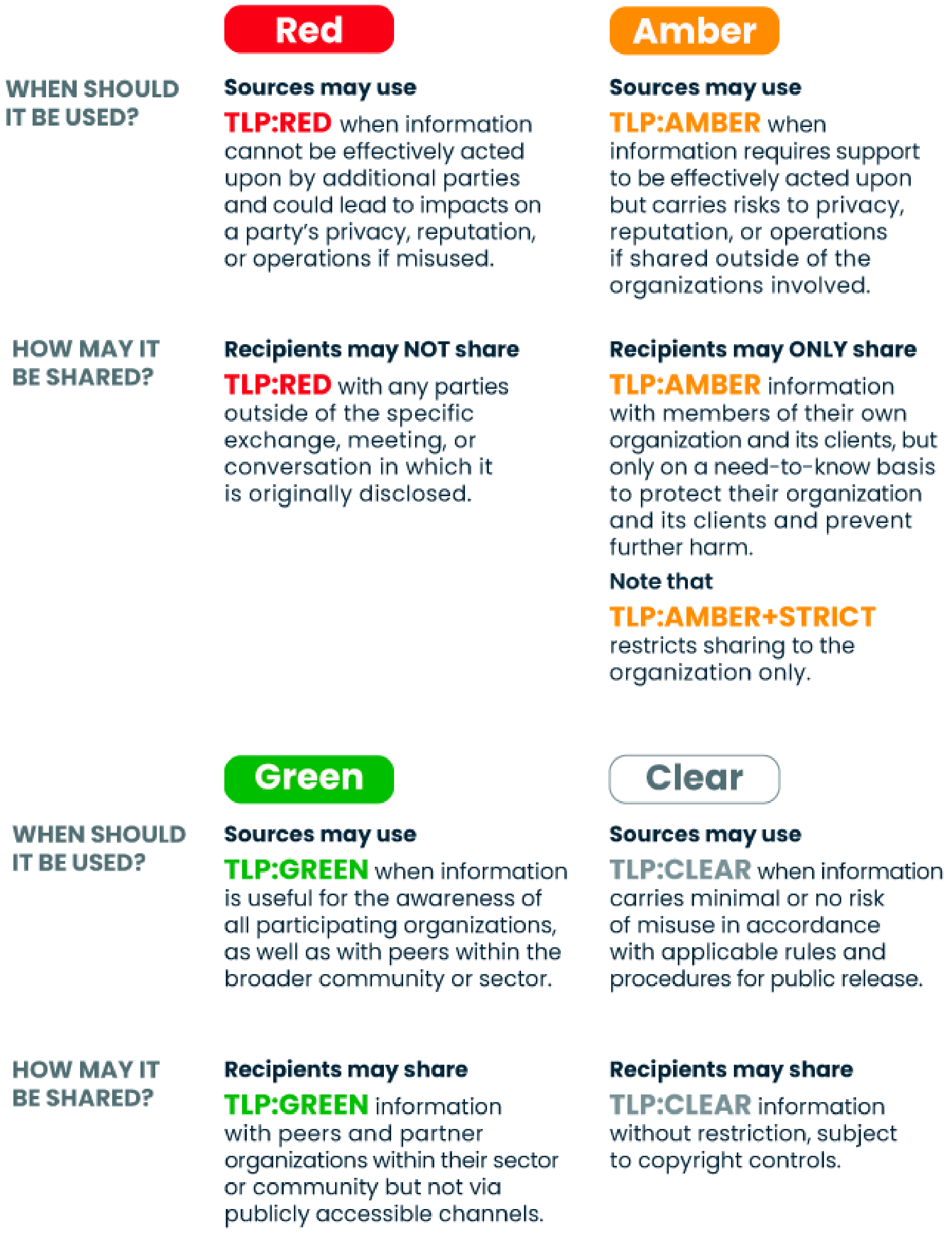
Regional ransomware trends: Over the past seven days, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia. There were at least 96 ransomware attacks observed in North America, while Europe and Russia accounted for 49, South America for 18, Asia-Pacific for 16, and Middle East and Africa for seven.

Major Breaches the Past Week

Targeted Entity	Aflac	University of Phoenix	Nissan
Compromised Entities/victims	22.65 million individuals	3.5 million individuals	21,000 customers of Nissan Fukuoka Sales Co., Ltd.
Compromised Data Fields	Full names, dates of birth, home addresses, Social Security numbers (SSNs), driver's license numbers, government-issued ID numbers (e.g., passports, state ID cards), medical information, and health insurance information	Full names, dates of birth, SSNs, bank account numbers, and bank routing numbers	Full names, physical addresses, phone numbers, email addresses, and customer data used in sales operations
Suspected Threat Actor	Scattered Spider	FIN11	Crimson Collective and ShinyHunters
Country/Region	United States	United States	Japan
Industry	Insurance	Education	Transportation
Possible Repercussions	Identity theft and financial fraud due to exposure of SSNs and government IDs; medical identity theft and insurance fraud risks; and increased phishing, social engineering, and scam campaigns targeting affected individuals	Identity theft, credential-based follow-on attacks, increased ransomware and extortion risk, account takeover attempts, and third-party risk	Phishing, social engineering, and identity-based fraud targeting affected customers, as well as supply chain cyber risks

Three major breaches observed in the past week

Appendix A: Traffic Light Protocol for Information Dissemination

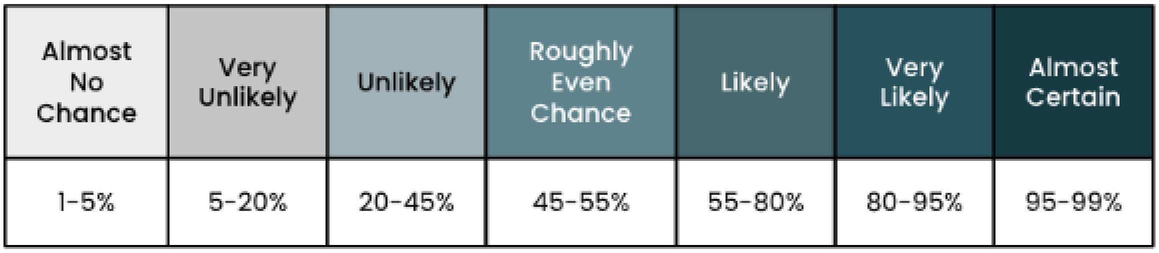


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%