# ZEROFOX®

## *Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**January 3, 2026**

### 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 January 1, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# Weekly Intelligence Brief

ZEROFOX®
Weekly Intelligence Brief

# Cyber and Dark Web Intelligence

# Cyber and Dark Web Intelligence Key Findings

## IP Management Company Breached

**What we know:**

- Decentralized intellectual property (IP) management platform Unleash Protocol has suffered a USD 3.9 million cryptocurrency theft after a threat attacker gained administrative control of its multisig governance system.
- The attacker executed an unauthorized smart contract upgrade that enabled illicit withdrawals of multiple assets.

**Background:**

- Stolen funds were bridged out and reportedly laundered through an open source mixer to obscure traceability.
- The malicious upgrade enabled illicit withdrawals of multiple assets, including wrapped IP (WIP), wrapped Ether (WETH), staked IP (stIP), and voting-escrowed IP (vIP).

**Analyst note:**

- The laundered funds are likely to be moved into fresh wallets, cashed out via other exchanges, and reused to fund future cyber operations.
- It is likely that a large amount of cryptocurrency is held back or further bridged to evade attribution.

## Phishing Campaign Targets U.S. Critical Infrastructure Using Malicious Npm Packages

**What we know:**

- A sustained phishing campaign, using 27 malicious npm packages, has been reportedly targeting critical infrastructure and adjacent organizations in the United States and allied countries to steal credentials.

**Background:**

- This operation has reportedly been observed for five months.
- At least 25 organizations across manufacturing, healthcare, plastics, and industrial automation were impacted by credential theft.

- The campaign reportedly repurposed npm and packaged content delivery networks (CDNs) as hosting infrastructure to impersonate secure document-sharing embedded in phishing pages.

**Analyst note:**

- This targeted phishing campaign is likely to impact downstream organizations spiraling into a supply chain attack.
- Since the campaign has specifically targeted U.S. and allied critical infrastructure over a sustained period of time, it is likely to be a state-linked operation.

## MongoBleed Exploitation Endangers More than 80K MongoDB Instances

**What we know:**

- Threat actors are actively exploiting a critical MongoDB vulnerability, MongoBleed (CVE-2025-14847).
- The flaw enables unauthenticated attackers to remotely leak sensitive in-memory data, including database credentials and cloud secrets, from exposed servers.

**Background:**

- The flaw abuses improper handling of zlib-compressed network messages, causing MongoDB to leak in-memory data.
- Over 80,000 MongoDB instances are exposed and users are urged to patch the flaw affecting MongoDB versions 3.6 through 8.2.3.

**Analyst note:**

- Active exploitation of MongoBleed and failure to deploy patches is likely to lead to large-scale credential and sensitive data exposure,
- Threat actors are likely to carry out follow-on attacks such as database compromise, cloud account takeover, data theft, and lateral movement into affected networks.

# 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 one vulnerability to its Known Exploited Vulnerabilities (KEV) catalog on December 29 and released two Industrial Control System (ICS) advisories on December 30. CVE-2020-12812 is an authentication bypass vulnerability in FortiOS SSL VPN that has been actively exploited. CVE-2025-52691 is an unauthenticated remote code execution (RCE) vulnerability that enables attackers to upload arbitrary files on the mail server.

**CRITICAL**

## CVE-2025-68664

**What happened:** Codenamed LangGrinch, this is a critical vulnerability in LangChain Core. It happens because LangChain trusts user supplied lc keys, which can enable attackers to trick the system into running unwanted actions, stealing confidential data, or changing how an LLM behaves.

- **What this means:** Successful exploitation may lead to data leaks, loss of access, system manipulation using arbitrary codes, especially in LangChain-powered applications that process untrusted input or expose LangChain-powered services publicly.
    - **Affected products:** LangChain Core versions listed in the advisory.

**CRITICAL**

## CVE-2025-54322

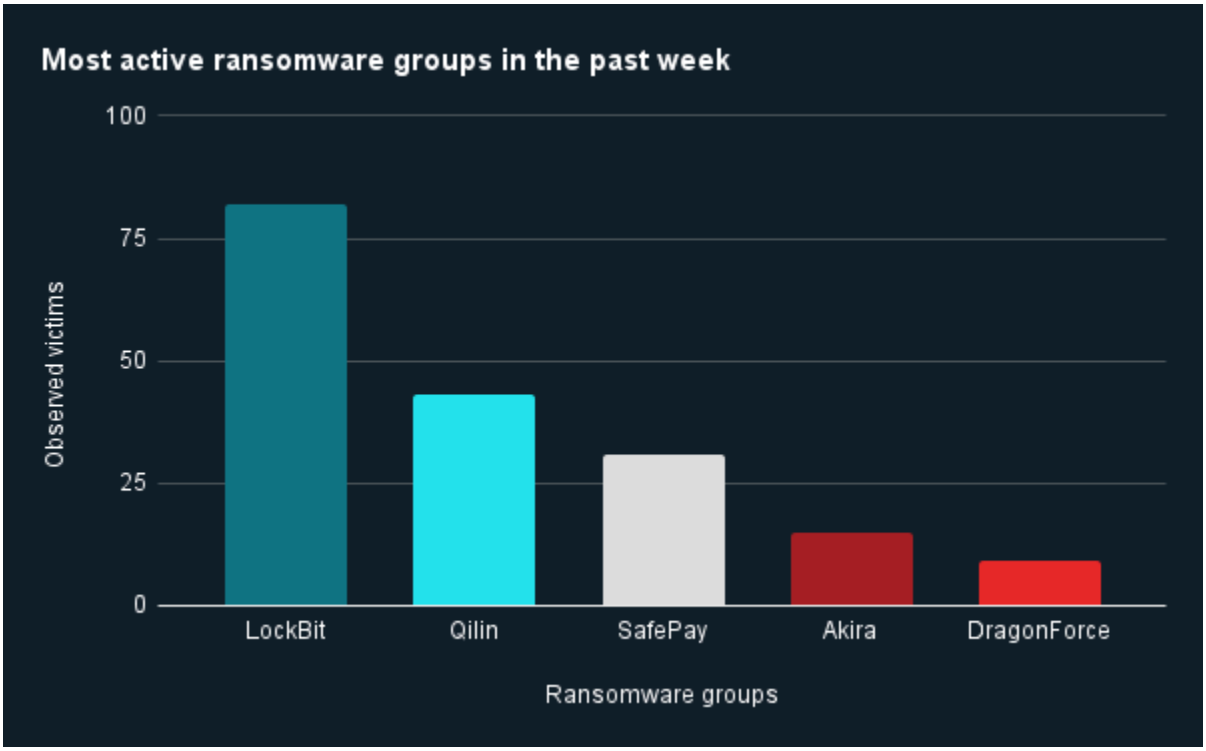
**What happened:** Threat actors are actively exploiting CVE-2025-54322, a critical remote code execution zero-day vulnerability in XSpeeder networking devices, that allows attackers to run arbitrary code on vulnerable systems. Till now over 70,000 devices worldwide have been exposed publicly.

- **What this means:** Active exploitation and delayed patching could result in full system compromise, enabling malware deployment, data theft, and lateral movement across affected networks.
    - **Affected products:** Xspeeder SXZOS versions through 2025-12-26

# Ransomware and Breach Intelligence

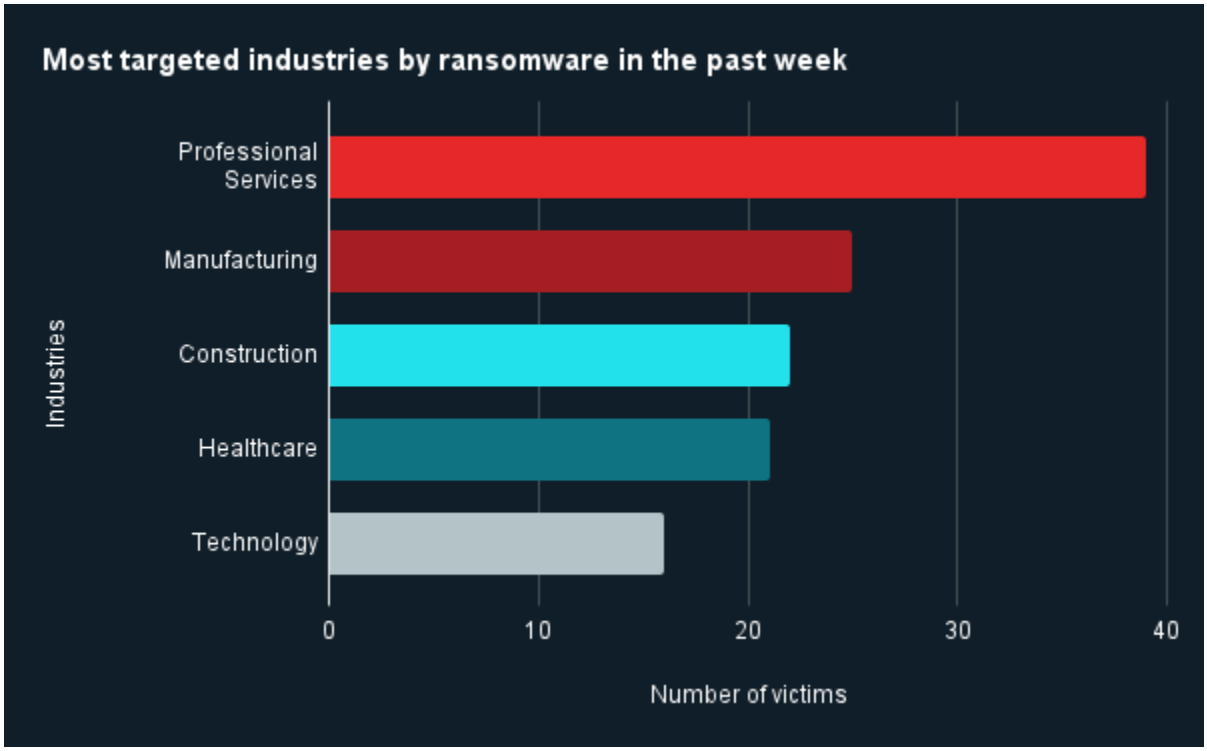
# Ransomware and Breach Intelligence Key Findings

## Ransomware Groups: Trends and Activities



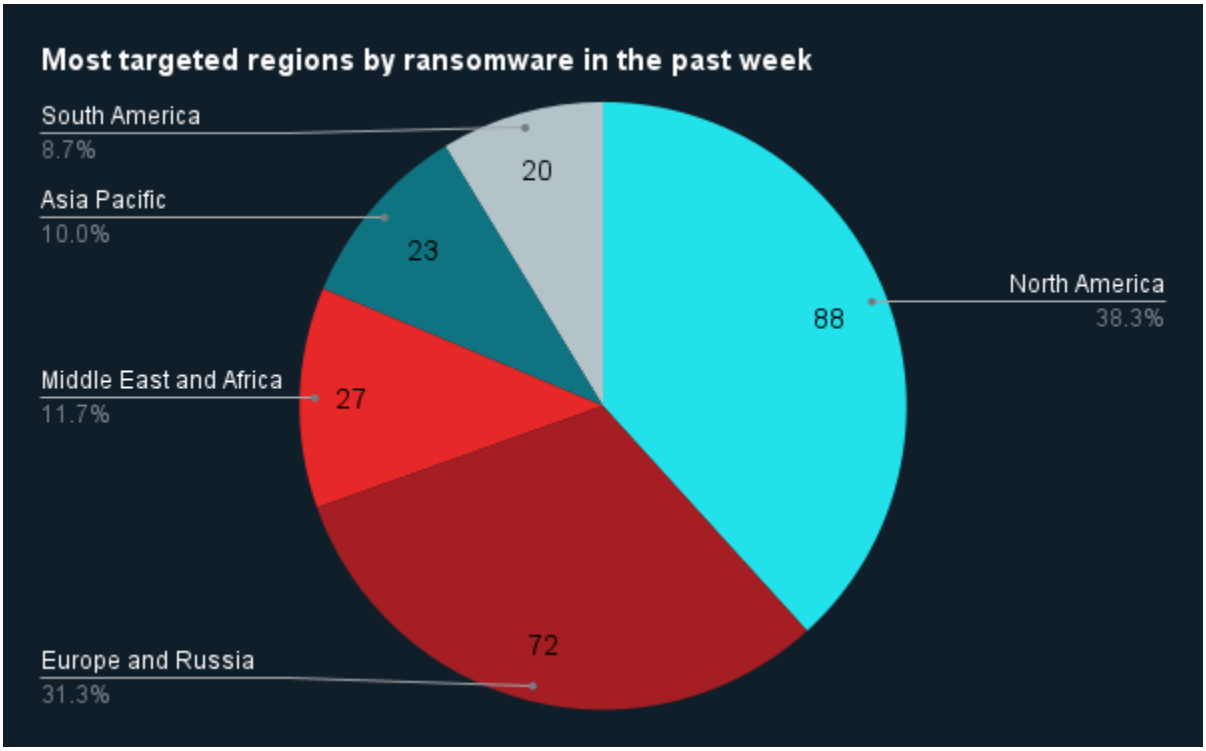

Source: ZeroFox Internal Collections

**Last week in ransomware:** In the past week, LockBit, Qilin, SafePay, Akira, and DragonForce were the most active ransomware groups. ZeroFox observed close to 200 ransomware victims disclosed, most of whom were located in North America. The LockBit ransomware group accounted for the largest number of attacks, followed by Qilin.




Source: ZeroFox Internal Collections

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




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 88 ransomware attacks observed in North America, while Europe and Russia accounted for 72 ransomware attacks, Middle East and Africa for 27, Asia Pacific for 23, and South America 20.

## Significant Data Breaches Reported in the Past Week

| Targeted Entity | European Space Agency | Wired | Sax LLP |
|---|---|---|---|
| Compromised Entities/victims | 200 GB of data impacting ESA servers outside its corporate network | 2.3 million users | 228,876 individuals |
| Compromised Data Fields | Source code, API tokens, documents, hardcoded credentials, and internal repositories | Names, email addresses, phone numbers, user IDs, IP addresses, and last session dates | Names, dates of birth, Social Security numbers, driver's license or state identification number, and passport number |
| Suspected Threat Actor | 888 | Lovely | N/A |
| Country/Region | Europe | United States | United States |
| Industry | Defense/Aerospace | Media/Entertainment | Legal/Consulting |
| Possible Repercussions | Further network intrusion, supply chain risks, sensitive data theft, national security issues | Extortion, phishing, and social engineering | Phishing, social engineering, blackmail, extortion, identity fraud |

**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% |