ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

February 14, 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 February 12, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report - Cryptocurrency Stealer for Sale on Dark Web

On February 2, 2026, ZeroFox observed an actor using the alias "MysteryHack" advertising a malware suite called DeepLoad on the dark web forum Exploit. The actor described DeepLoad as a centralized panel for multiple types of malware; its primary function is to replace seven cryptocurrency wallet applications with counterfeit versions. The actor claimed that a second DeepLoad feature, called Anti-Metamask, is designed to remove legitimate browser-based cryptocurrency wallets and replace them with fraudulent versions. MysteryHack further claimed that they are developing a future DeepLoad module, which they described as an executable file that installs an unspecified browser extension offering fraudulent airdrops. Due to DeepLoad's wallet replacement, phishing automation, and persistent malware capabilities, ZeroFox assesses it is very likely a very sophisticated offering. DeepLoad's design is explicitly focused on actively facilitating real-time cryptocurrency theft, which almost certainly makes it an attractive malware suite in the cybercrime-as-a-service (CaaS) environment.

ZeroFox Intelligence Flash Report - Campaign to Recruit Cryptocurrency Insiders

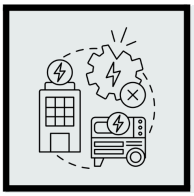
A newly registered and untested threat actor known as "LocalVulture" posted on popular dark web forum Exploit seeking potential partners to recruit insiders within large cryptocurrency exchanges—preferably those from "third-world" countries. Notably, the actor provided a guidance manual and numerous specific suggestions on how to approach and profile prospective insiders. ZeroFox assesses this is a change in previously observed tactics that is likely to reinvigorate long-standing efforts among financially motivated threat actors to infiltrate and target major cryptocurrency exchanges. In the post, LocalVulture shared three categories of insider individuals recruitment partners should target. It is likely that the actor has identified these categories in order to exploit financially motivated and inexperienced crypto exchange employees that may be more easily swayed to provide insider knowledge. LocalVulture specifies that, after identifying suitable insider targets for recruitment, partners are expected to rely on social engineering techniques to establish and maintain effective communication. ZeroFox assesses this indicates the actor is interested in conducting more sophisticated operations beyond financial fraud, such as ransomware deployment, data extortion, and cyber espionage.

ZeroFox Intelligence Flash Report - Everest Continues to Tout Prominent Brands in Latest Disclosures

On February 2, 2026, a ransomware and digital extortion (R&DE) collective known as "Everest" announced an alleged data breach of Iron Mountain on its victim leak site. ZeroFox assesses Everest has very likely overstated the volume and sensitivity of the breach in order to increase pressure on the victim to comply with its extortion demands. Everest is a Russian-language collective offering ransomware-as-a-service (RaaS) that has conducted at least 286 separate R&DE incidents since ZeroFox first observed the group in 2021. In light of sensitive reporting, ZeroFox assesses Everest has likely exaggerated the quantity and quality of its alleged victim data—and in some cases fabricated it entirely. Everest is the tenth most prominent R&DE collective thus far in 2026 in terms of number of published alleged victims; the group has primarily targeted North America-based entities and organizations in the healthcare sector. However, given Everest's historical tendency to overstate its exfiltrations, ZeroFox assesses it is unlikely their latest claims regarding the Iron Mountain breach are credible.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Former Executive Accused of Trafficking Stolen Exploits to Russian Entities

What we know:

- The U.S. Department of Justice has charged an individual for selling proprietary cyber intrusion tools to a Russia-linked broker seeking zero-day exploits.
- The accused sold eight proprietary tools and exploit packages to the Russian broker, who is suspected to cater to other Russian entities, including the Russian government.

Background:

- The individual previously served as an executive at a security services provider that supported multiple partners of the U.S. Intelligence Community, as well as other intelligence organizations across the Five Eyes alliance.

Analyst note:

- The sale of zero-day exploits to Russian entities is likely to trigger state-directed espionage and offensive cyber operations targeting military systems and civilian infrastructure.
- Immediate patching of the exposed zero-day vulnerabilities is likely to prevent an onslaught of threat actors seeking to steal sensitive information or establish long-term persistence across affected government devices and networks.

Breach of Staff Device Platform Exposes European Commission Employee Details

What we know:

- On January 30, 2026, the European Commission contained a cyberattack that targeted its Mobile Device Management (MDM) systems, which are used to manage staff phones and tablets.
- The attackers are suspected to have accessed employee names and phone numbers, but the Commission confirmed that no mobile devices themselves were compromised.

Background:

- The Commission has not confirmed the threat actors' initial access method, but the breach is believed to be part of a broader campaign exploiting Ivanti Endpoint Manager

Mobile (EPMM) vulnerabilities (CVE-2026-1281 and CVE-2026-1340) against European institutions.

Analyst note:

- Before the Commission intercepted the attack, the threat actors are likely to have gained access to confidential information stored in the MDM systems, such as device metadata, passcodes, employee names, and phone numbers.
- This access is likely to support reconnaissance of the Commission's mobile infrastructure and attempts to escalate access into broader internal systems.

UNC1069 Targets Cryptocurrency Sector

What we know:

- Financially motivated North Korean threat actor UNC1069 is targeting the cryptocurrency sector using artificial intelligence (AI)-generated videos and ClickFix lures to deliver malware for macOS and Windows users.

Background:

- The infection chain reportedly uses compromised Telegram accounts of executives in cryptocurrency firms to contact victims and lure them into fake Zoom meetings.
- While in these meetings, the victims are tricked into running commands that deliver multiple malware families to the victim's systems.

Analyst note:

- Threat actors are likely to leverage such AI-powered campaigns to target other operating systems across different sectors, including critical infrastructure.
- Furthermore, the campaign is likely to impact downstream entities by threat actors reusing the compromised data to impersonate executives for financial gain.

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—with an observed increase in injection-based remote code execution (RCE) exploits. The Cybersecurity and Infrastructure Security Agency (CISA) has added six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on February 10, 2026 and released 15 Industrial Control System (ICS) advisories, including CVE-2025-12699, CVE-2026-1495, CVE-2026-1507, CVE-2026-25084, CVE-2026-1358, CVE-2025-7740 and CVE-2025-0836 on February 10 and February 12, 2026. Apple has patched CVE-2026-20700, a zero-day RCE vulnerability in its Dynamic Link Editor (dyld) that can enable attackers with memory write capability to execute arbitrary code. Microsoft has patched close to 60 vulnerabilities, including six actively exploited zero-days and three zero-day vulnerabilities. CVE-2025-1974 is a critical-rated vulnerability that affects Kubernetes (K8s) clusters that use the ingress-nginx controller. Intel and AMD's February 2026 Patch Tuesday updates fixed over 80 vulnerabilities, including multiple high-severity flaws, across processors, firmware, drivers, and support tools. CVE-2026-26158 is a Path Traversal flaw in Busybox tar that can enable attackers to craft malicious archives containing unvalidated symlinks to overwrite critical files outside the intended extraction directory.

CRITICAL

CVE-2026-21643

What happened: A FortiClientEMS vulnerability tracked as CVE-2026-21643 can enable unauthenticated attackers to execute arbitrary code via specially crafted HTTP requests exploiting a Structured Query Language (SQL) injection flaw.

- **What this means:** Post initial access operations, unpatched versions are likely to be leveraged as footholds in enterprise environments to deploy follow-on attacks such as introducing malware and facilitating lateral movement across compromised networks.
  - **Affected products:** FortiClientEMS versions 7.4.4, 7.2, and 8.0

CRITICAL

CVE-2026-1731

What happened: CVE-2026-1731 is a pre-authentication RCE vulnerability in BeyondTrust that affects its Remote Support (RS) and Privileged Remote Access (PRA) products. The flaw stems from an operating system command injection weakness.

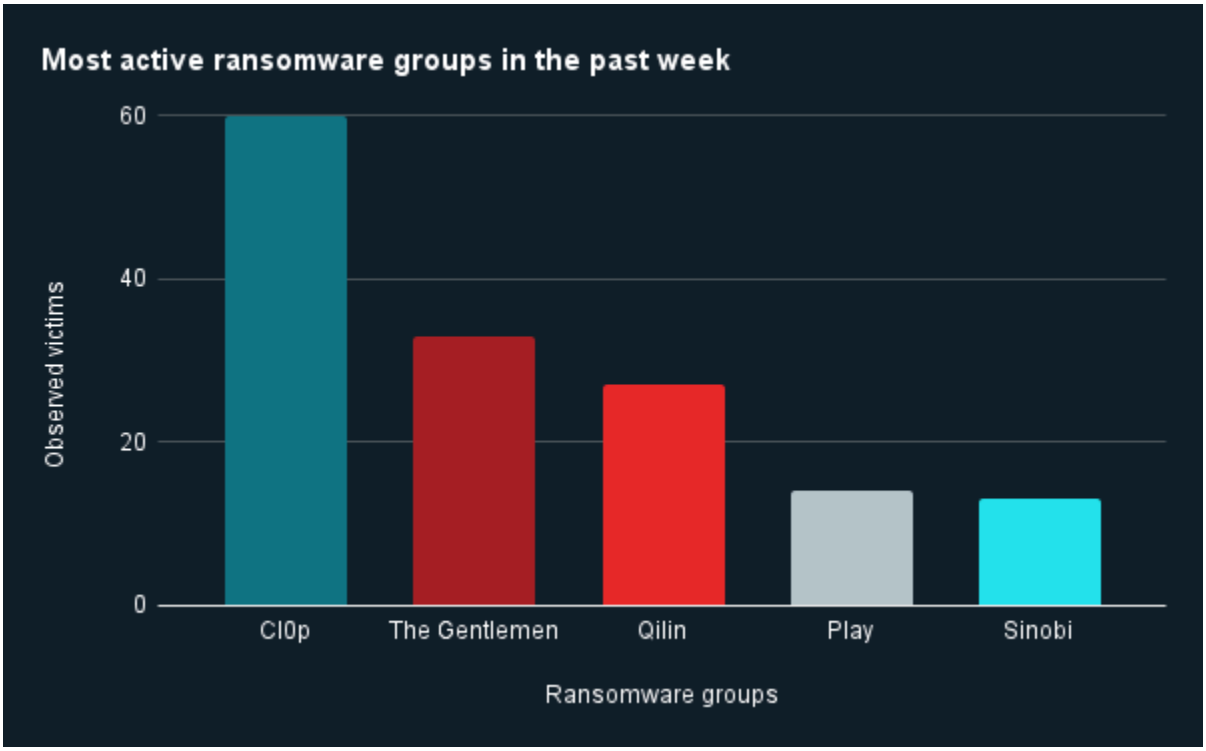
- **What this means:** The flaw enables unauthenticated attackers to execute arbitrary operating system commands without credentials or user interaction. Threat actors are likely to exploit this flaw to automate the exploits and scale up data exfiltration and service disruption.
  - **Affected products:** RS versions 25.3.1 and prior and PRA versions 24.3.4 and prior

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

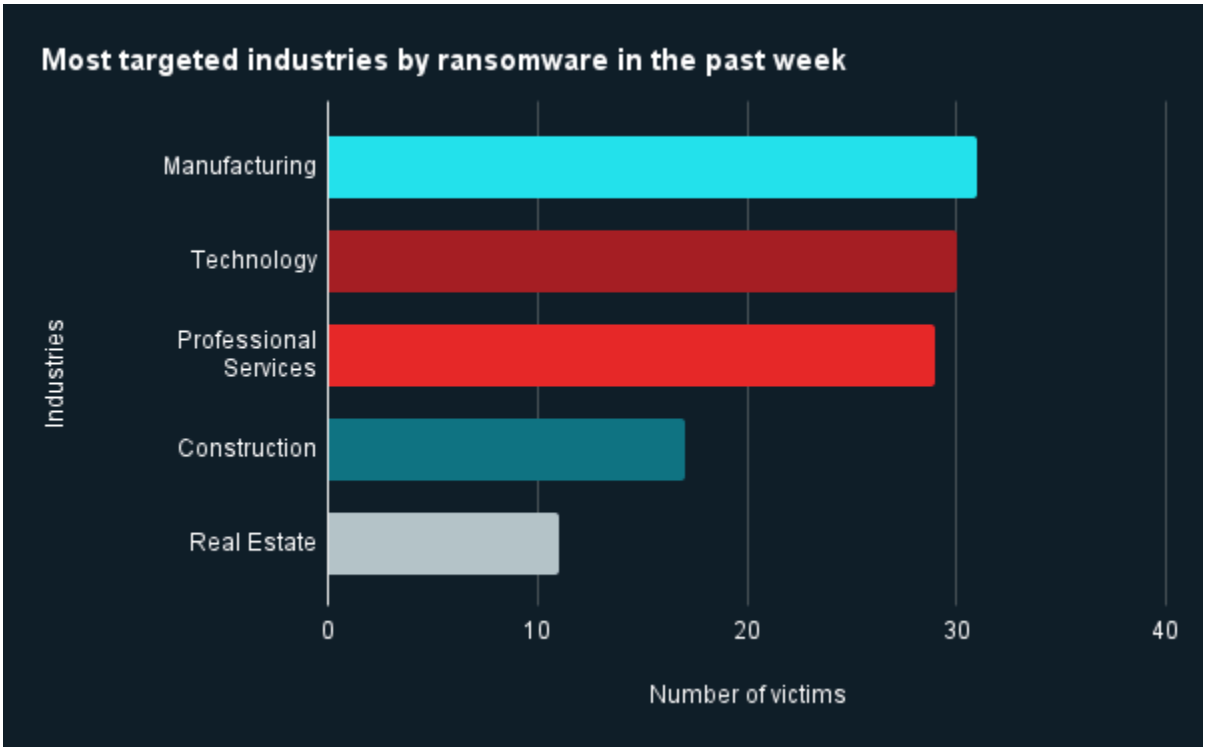
Ransomware Round-up: Most Active Groups, Industries, and Countries

Last week in ransomware: In the past week, Cl0p, The Gentlemen, Qilin, Play, and Sinobi were the most active ransomware groups. ZeroFox observed at least 191 ransomware victims disclosed, most of whom are located in North America. The Cl0p ransomware group accounted for the largest number of attacks, followed by The Gentlemen and Qilin.



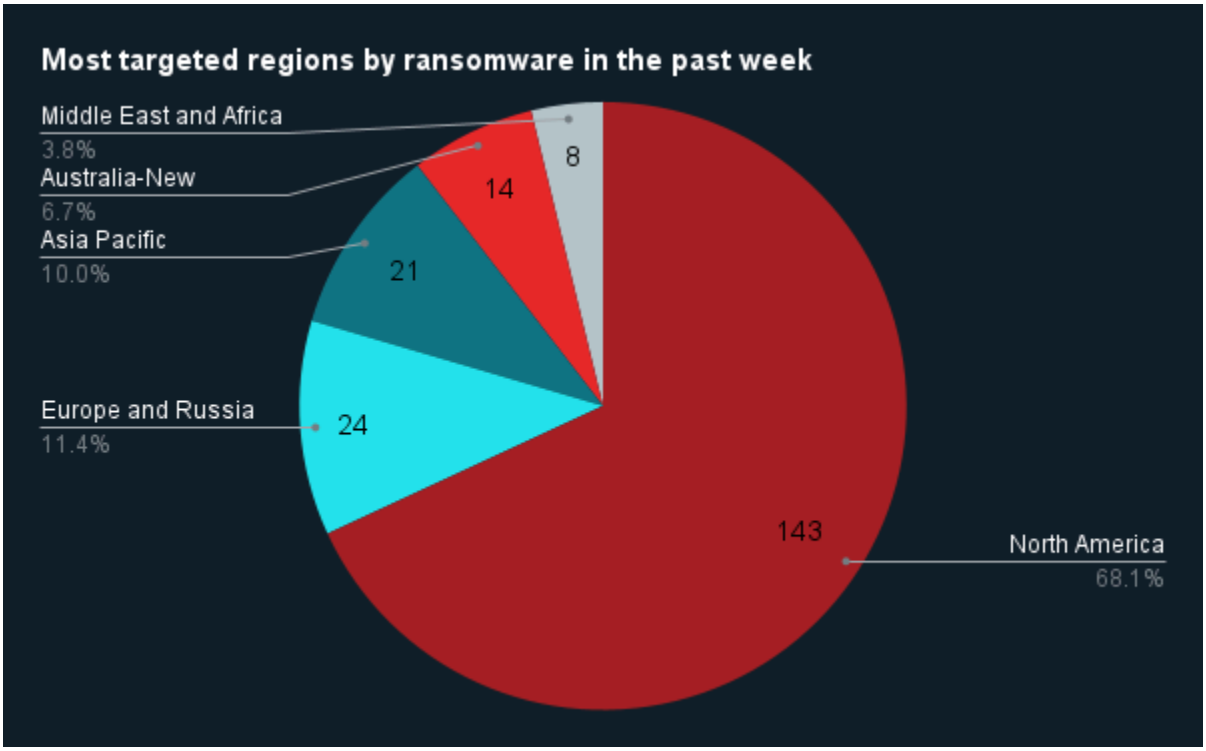
Source: ZeroFox Internal Collections

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



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 143 incidents observed in North America, while Europe and Russia accounted for 24, Asia-Pacific for 21, Australia and New Zealand (ANZAC) for 14, and the Middle East and Africa for eight.



Source: ZeroFox Internal Collections

Notable Data Breaches of this Week

Targeted Entity	The Counseling Center of Wayne and Holmes Counties (CCWHC)	European Commission	Precipio
Compromised Entities/victims	83,354 individuals	European Commission staff	At least 501 individuals
Compromised Data Fields	Potentially, full names, dates of birth, Social Security numbers (SSNs), State ID numbers, health insurance details, medical condition information, treatment provider names, and medical record numbers	Employee names and phone numbers	Names, addresses, dates of birth, medical record numbers, clinical or treatment information, medical procedure information, medical provider names, prescription information, and health insurance information
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	United States	Europe	United States
Industry	Healthcare	Government	Healthcare
Possible Repercussions	Identity theft and financial fraud due to exposure of SSNs and IDs, medical identity fraud through stolen insurance and health records, privacy violations, and increased phishing or extortion attempts	Gaining of access to European Commission's administrative networks via central infrastructure compromise, phishing, and targeting of European government bodies through the exploitation of unpatched Ivanti flaws	Exposure of sensitive protected health information (PHI), identity theft and medical fraud, and possible follow-on phishing or insurance-related scams

Three major leaks 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%