ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

February 7, 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 5, 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 - Possible ShinyHunter SSO Phishing Campaign Identified

In late January 2026, actors claiming to be well-known threat collective "ShinyHunters" are reportedly orchestrating extortion-focused voice phishing or vishing attacks targeting single sign-on (SSO) accounts hosted by Okta, Google, and Microsoft at several major organizations. Concurrently, ZeroFox has observed that a leak site associated with threat collective "Scattered Lapsus$ Hunters" has been recently renamed to ShinyHunters and lists six organizations as victims. Given the fact that some of the companies listed on the leak site have disclosed intrusions but not exfiltration of sensitive data, it is very likely that the threat actors are advertising either recycled data or data that is not sensitive and is available in the open source.

ZeroFox Intelligence Flash Report - FBI Seizes Dark Web Forum RAMP

On January 28, 2026, the Federal Bureau of Investigation (FBI) seized the dark web forum RAMP in a coordinated action with the U.S. Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the U.S. Department of Justice (DoJ). The RAMP forum's primary purpose was to advertise ransomware-as-a-service (RaaS) activities, and it was the only known dark web forum where such activity was explicitly permitted. Following news of the seizure, screenshots from a suspected leaked RAMP database appeared in a Telegram channel—including an email address allegedly used by well-known RaaS operator "LockBit" to register on RAMP. The seizure of RAMP is likely to have a significant impact on the cybercriminal community in the short term. As RAMP was the only known dark web forum to explicitly allow RaaS operations on its platform, it is an environment that will not be easy to replace quickly. It is also highly likely that arrests derived from the seizure of the RAMP forum will be made within the next six months.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 3

The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

Monthly Geopolitical Assessment February 2026

The United States has moved military hardware towards the Middle East. This likely indicates a U.S. intention to force Iran to ease the crackdown measures and establish a more peaceful stance towards its neighbors in the Middle East. If Iran does not comply, it is very likely that a U.S. military strike will occur by mid-February. The removal of Venezuelan President Nicolás Maduro makes it more likely that there will be further U.S. military operations against nations with adversarial relationships with the United States, close military relations with either Russia or China, or energy resources. Western nations are likely to escalate their crackdown efforts on shadow fleet vessels carrying sanctioned energy resources. Although the conditions for moving to phase two of the Israeli-Hamas ceasefire agreement have largely been reached, it is unlikely that the peace plan will advance in any meaningful way in the near- to medium-term—and there is a roughly even chance that the conflict will see a major escalation in fighting in that same timeframe. Several meaningful and uncertain elections are scheduled for February 2026. Japan's snap election is likely to have consequential negative impacts on the global economy if the ruling party loses. Intensifying geopolitical risks impacting supply chains will likely be a dominant theme of 2026.

ZeroFox Intelligence Event Assessment – Super Bowl LX

Super Bowl LX is scheduled to take place on February 8, 2026, in Santa Clara, CA, at Levi's® Stadium, home of the San Francisco 49ers. Security planning involving local, state, and federal resources will undoubtedly take place, with likely added emphasis on mitigating potential disruptions from immigration-related tensions, which have been occurring nationwide. Previous iterations of the Super Bowl have inspired a range of fraudulent activity by financially motivated threat actors targeting attendees pertaining to a range of services, including accommodations, betting, and ticketing. ZeroFox has identified numerous scams related to Super Bowl LX, and our deep and dark web (DDW) monitoring team has also observed the sale of compromised account credentials for National Football League (NFL) employees, customer data, and fake tickets.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Notepad++ Hijacked by Suspected Chinese Threat Actors

What we know:

- The developer of open source code editor Notepad++ has confirmed a compromise involving its update infrastructure by a suspected Chinese state-sponsored threat actor group.
- Researchers have attributed the breach to China-linked threat group Lotus Blossom.
- The developer claimed that the issue has been addressed in the December 2025 security patch with the release of version 8.8.9.
- Notepad++ has been migrated to a new hosting provider since the breach for better security measures.

Background:

- According to the developer, the attackers targeted the hosting infrastructure rather than a vulnerability within the Notepad++ codebase between June and December 2025.
- After gaining unauthorized access to the hosting server, the threat actors reportedly redirected traffic from specific users to attacker-controlled servers to deploy a backdoor named Chrysalis.
- The threat actors exploited an insufficient update verification control vulnerability in older versions of the utility.
- The developer emphasized that not all users of Notepad++ received malicious updates and that only specific users were targeted.

Analyst note:

- Threat actors are likely to push malicious updates to unpatched versions of Notepad++, which can enable network intrusion.
- This is likely to lead to supply chain compromise, impacting multiple developers and organizations.
- Since Chrysalis is relatively new and advanced, simple malware removal is unlikely to be effective, enabling persistent access on compromised systems.

Fintech Firm Loses USD 40 Million After Exec Devices Hacked

What we know:

- Step Finance, a decentralized finance (DeFi) platform and analytics tool, has reportedly lost USD 40 million worth of crypto assets after sophisticated threat actors compromised devices belonging to the company's team of executives.

Background:

- The attackers gained access to treasury wallets and critical authentication credentials during the attack, enabling them to bypass multiple security layers.
- Additionally, the investigation revealed that the attackers moved funds across multiple blockchain networks to obscure the transaction trail.

Analyst note:

- Considering similar incidents in the past, the attack vector highlights a shift from smart contract exploits that are hard to break to personnel targeting using humans as weak links to trick.

Italy Stops Russia-Attributed Cyberattacks on High-Profile Targets

What we know:

- Italy said it has thwarted alleged Russian-origin cyberattacks targeting its foreign ministry facilities, including its Washington embassy and Olympics-related websites and hotels.

Background:

- The cyberattacks come as the Winter Olympic Games in Italy are scheduled to begin on February 6, 2026.

Analyst note:

- Although no other details of the attack has been confirmed as of writing, it is likely that Russia's cyberattacks are retaliatory actions against the International Olympic Committee (IOC) for its restrictions preventing Russian athletes from competing under the Russian flag and only allowing them to participate as Individual Neutral Athletes (AINs).

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 four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog and released three Industrial Control System (ICS) advisories (CVE-2026-1633, CVE-2026-1632, and CVE-2025-10314) on February 3, 2026. N8n has patched two remote code execution (RCE) vulnerabilities; CVE-2026-1470 enables authenticated users to bypass sandbox restrictions and execute arbitrary code on the underlying host, while CVE-2026-0863 enables sandbox escape via the Python Code node. SolarWinds Web Help Desk has patched an RCE vulnerability (CVE-2025-40551) caused by an untrusted data deserialization flaw that enables unauthenticated attackers to execute arbitrary commands on unpatched devices, potentially leading to full system compromise. CVE-2025-8088 is a WinRAR RCE flaw that is reportedly being abused by China-linked Amaranth-Dragon actors to run malicious code when targets open specially crafted RAR archives. Ivanti has patched two actively exploited zero-day flaws (CVE-2026-1281 and CVE-2026-1340) in Endpoint Manager Mobile that enabled unauthenticated RCE, potentially allowing attackers to gain admin control, move laterally, and access sensitive device and user data.

HIGH

CVE-2026-25253

What happened: CVE-2026-25253 is a token exfiltration flaw in OpenClaw's Control UI that trusts an unvalidated gateway URL and enables cross-site WebSocket hijacking (WebSocket is a computer communications protocol.)

- **What this means:** A hijacked link can steal gateway tokens and grant attackers operator-level access, enabling configuration changes and one-click RCE on the host. Threat actors are likely to leverage this flaw to craft malicious links to steal gateway tokens and execute arbitrary commands on victim devices.
  - **Affected products:** OpenClaw versions before 2026.1.29

CRITICAL

CVE-2026-25049

What happened: CVE-2026-25049 is an RCE flaw in the n8n workflow automation platform that stems from weak sanitization of server-side JavaScript expressions and bypasses existing sandbox protections.

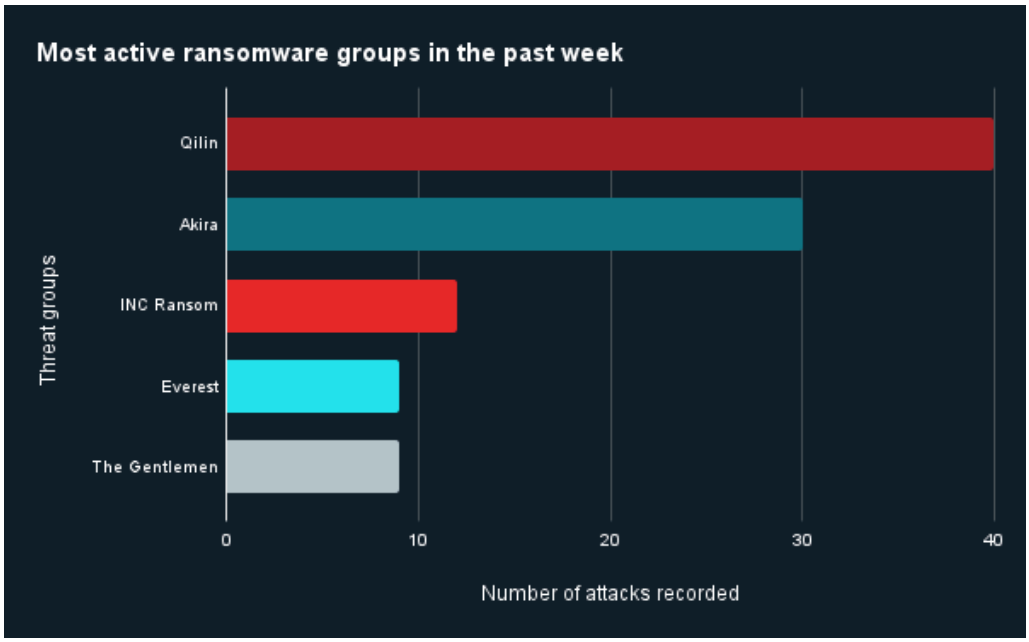
- **What this means:** The flaw enables an authorized user to create or edit workflows and exploit them to escape the n8n environment and execute arbitrary system commands on the host. Threat actors are likely to leverage this flaw to craft malicious workflows that can lead to full server compromise and post-exploitation data theft.
  - **Affected products:** n8n versions prior to 1.123.17 and 2.5.2

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

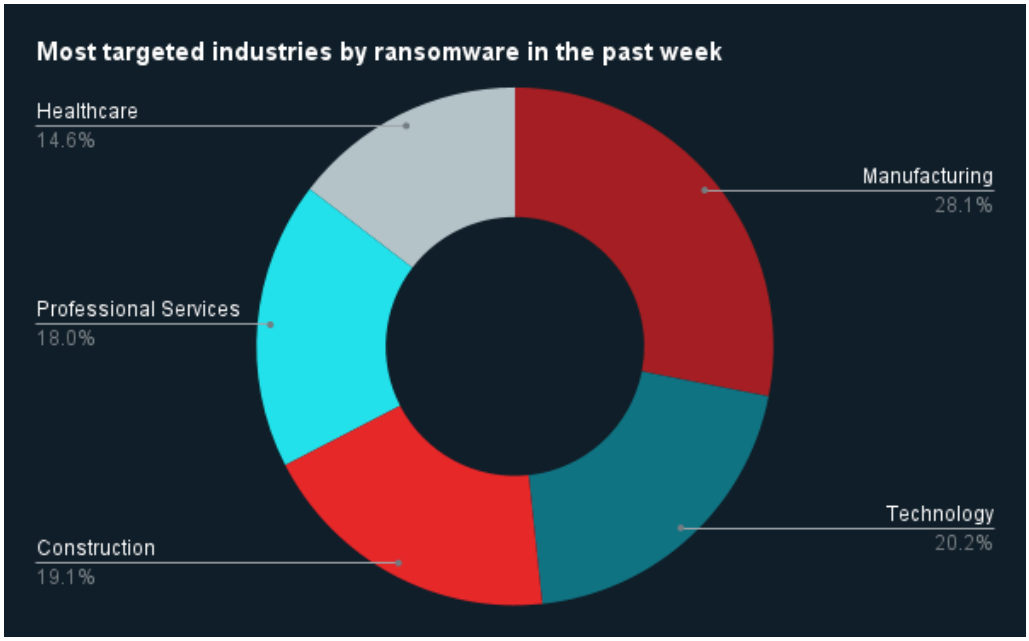
Ransomware Round-up: Most Active Groups, Regions, and Industries

Last week in ransomware: In the past week, Qilin, Akira, INC Ransom, Everest, and The Gentlemen were the most active ransomware groups. ZeroFox observed at least 130 ransomware victims disclosed, most of which are located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Akira and INC Ransom.



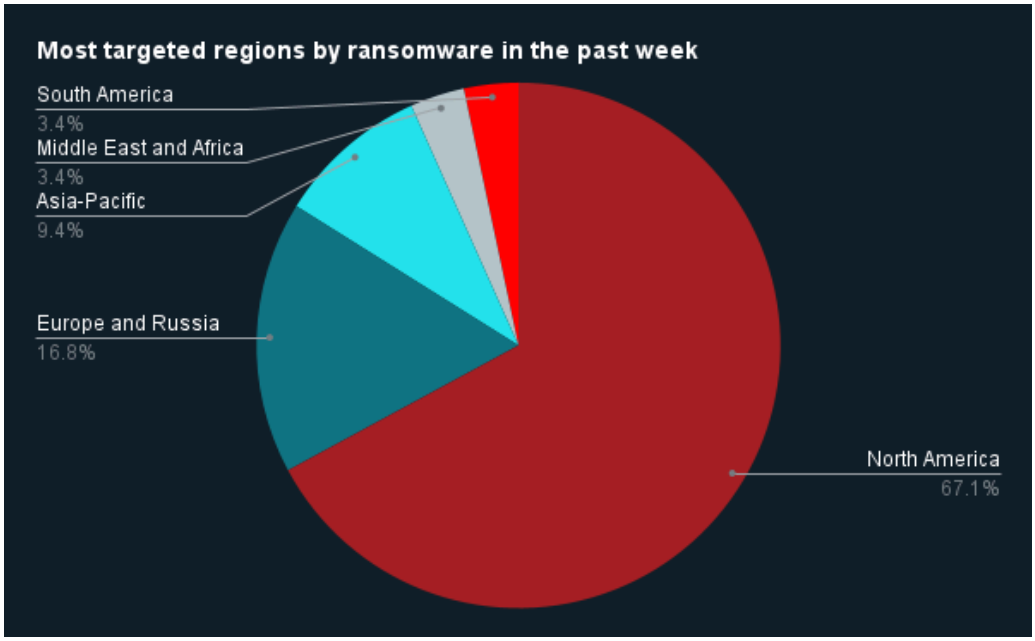
Source: ZeroFox Internal Collections

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.



Source: ZeroFox Internal Collections

Major Data Leaks Reported in the Past Week

Targeted Entity	NationStates	Moltbook	Coinbase
Compromised Entities/victims	NationStates users	Private data of approximately 17,000 human operators of artificial intelligence (AI) agents	Information of approximately 30 customers
Compromised Data Fields	Email addresses, passwords, IP addresses, and browser User Agent strings used to log in	1.5 million Application Programming Interface (API) authentication tokens, 35,000 email addresses, and private messages between AI agents	Email addresses, names, dates of birth, phone numbers, Know Your Customer (KYC) information, cryptocurrency wallet balances, and transactions
Suspected Threat Actor	A NationStates user	N/A	Scattered Lapsus$ Hunters
Country/Region	Australia	Global	United States
Industry	Media/Entertainment	Technology	Financial Services
Possible Repercussions	If the data remains exposed, phishing attacks and account takeovers are likely.	Targeted social engineering attacks, persistent gateway for identity theft and multi-stage extortion, and lateral movement across the corporate network to take over the domain controller	Crypto theft, account takeovers, social engineering, phishing, and identity theft

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%