ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

January 17, 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 15, 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 – Spanish Energy Company Breached

On January 4, 2026, actor "spain" announced on the dark web forum BreachForums that they had breached Endesa, a Spanish energy company. On January 5, 2026, actor "glock" posted the same advertisement on the dark web forum DarkForums. ZeroFox assesses it is almost certain these personas are being operated by the same threat actor. According to spain/glock, the sales post was approved by both forums' moderation teams, and the data was verified—likely lending significant credibility to the post. Endesa confirmed in a statement that a threat actor gained unauthorized and illegitimate access to its systems and extracted sensitive personally identifiable information (PII). It is almost certain that the advertisements on the dark web forums will attract significant attention from potential buyers, especially considering that Endesa has confirmed the breach.

ZeroFox Intelligence Brief – Iran Protests Leading to Likely U.S. Response

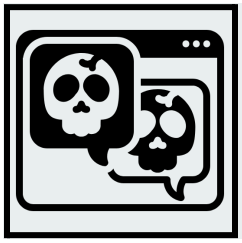
The Iranian government is under mounting pressure as nationwide protests, initially sparked by a failing economy, continue to rage across the country. The protests began on December 28 over the collapse of the Iranian rial and a new price structure for government-subsidized gasoline. Economic stress, loss of public trust in the government, and military defeats have likely combined to create the ideal conditions for the massive spread of this uprising. Despite the government's weakness, it very likely maintains the ability to put down the latest round of protests in the absence of external intervention. Even if this round of protests is suppressed and Iran returns to the status quo, it is highly likely the population will remain discontented, and a new round of protests will likely begin in 2026. U.S. involvement would likely change the calculus for outcomes in Iran. However, the U.S. Department of War is unlikely to conduct sophisticated military operations. The Trump administration is more likely to use diplomacy, increased global pressure, and low-level strikes to influence Iranian behavior.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Threat Actor Claims Access to Target's Internal Development Environment

What we know:

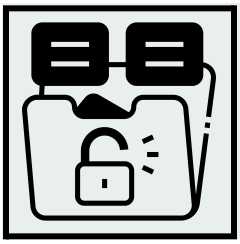
- An unknown threat actor has reportedly attempted to sell internal source code of American retailer Target Corporation on Gitea, a software development host platform.
- The threat actor has reportedly posted screenshots as evidence in a private hacking community, advertising a total dataset of about 860 GB.

Background:

- Researchers reportedly found multiple repositories on Gitea that appeared to be a sample of Target's internal code and developer documentation.
- The alleged Gitea links have since been removed, and Target's developer Git server has also become inaccessible from the internet.

Analyst note:

- If the breach is legitimate, the leaked data is likely to help threat actors to further compromise Target's internal network, leading to exfiltration of sensitive data, remote code execution (RCE), and other malicious activity.
- Downstream entities are also likely to be impacted. Online services and billing systems are likely to be disrupted.



Instagram Acknowledges Bug; Says There Is No Data Breach

What we know:

- Instagram has acknowledged a systematic bug that enabled threat actors to send password reset emails reported by users.
- However, Instagram has denied all data breach claims on its X account.

Background:

- Researchers discovered a dataset containing data of 17.5 million instagram users being sold on a dark web forum.
- The data was allegedly harvested in 2024 from an unconfirmed API leak. However, Meta has denied being aware of any API leaks or new data breaches.

Analyst note:

- The leaked data is likely scraped data gathered over several years.
- Despite that, threat actors will likely leverage the data to deploy sophisticated social engineering attacks, share emails containing hidden malicious links, and impersonate the victims for financial advantage.

Illegal Service Provider Enabling Fraud Disrupted

What we know:

- Working together, researchers and law enforcement have successfully disrupted RedVDS, a cybercrime service used to support phishing, business email compromise (BEC), and fraud operations.
- The operation seized RedVDS domains and servers and dismantled payment networks tied to the service.

Background:

- The threat group operating and developing RedVDS, dubbed Storm-2470, was reportedly responsible for at least USD 40 million in fraud-related losses.
- Since September 2025, RedVDS-enabled activity has resulted in the compromise or fraudulent access of over 191,000 email accounts spanning more than 130,000 organizations globally.

Analyst note:

- Threat actors are likely to reuse stolen credentials, phishing kits, and mailing lists from prior RedVDS campaigns to sustain BEC and fraud operations while testing new services or developing in-house hosting capabilities to reduce future disruption risk.

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 on January 12 and January 13. CISA released three Industrial Control System (ICS) advisories addressing YoSmart YoLink Smart Hub, Rockwell Automation FactoryTalk DataMosaix Private Cloud, and Rockwell Automation 432ES-IG3 Series A vulnerabilities on January 13. Microsoft has patched more than 100 vulnerabilities, including one actively exploited and two publicly disclosed zero-day flaws. A Broadcom Wi-Fi chipset flaw (without a CVE identifier at the time of writing) enables unauthenticated attackers to disable a router's network using a single crafted Wi-Fi frame to bypass WPA2/WPA3 protections. China-linked threat actors exploited multiple VMware ESXi vulnerabilities in zero-day attacks, reportedly to gain complete control overESXi hypervisor. Google released fixes for 10 security flaws, including three high-severity vulnerabilities in V8 and Blink (CVE-2026-0899, CVE-2026-0900, and CVE-2026-0901). Adobe rolled out security updates for 11 products as part of its January 2026 Patch Tuesday updates. These updates address a total of 25 vulnerabilities, including a code execution flaw. SAP released 17 security updates on its January 2026 Security Patch Day, including four critical vulnerabilities that enable threat actors to carry out SQL injection, RCE, and full system compromise. CVE-2025-12420 is an authentication bypass flaw that enables unauthenticated attackers to impersonate any user, including admins, and perform actions via artificial intelligence (AI) agents.

HIGH

CVE-2025-8110

What happened: CVE-2025-8110 is a zero-day path traversal vulnerability affecting Gogs, a popular self-hosted Git service. A symlink bypass of an older patched RCE flaw enables authenticated users to overwrite files outside the repository.

- **What this means:** Threat actors are likely to abuse the path traversal to overwrite arbitrary files on the Gogs server, enabling RCE, service disruption, or persistence.
- **Affected products:**
  - Gogs versions 0 through 0.13.3

HIGH

CVE-2026-22861

What happened: CVE-2026-22861 is a heap-based buffer overflow vulnerability in a function of a source file in the iccDEV library, which is an open source collection of tools from the International Color Consortium (ICC).

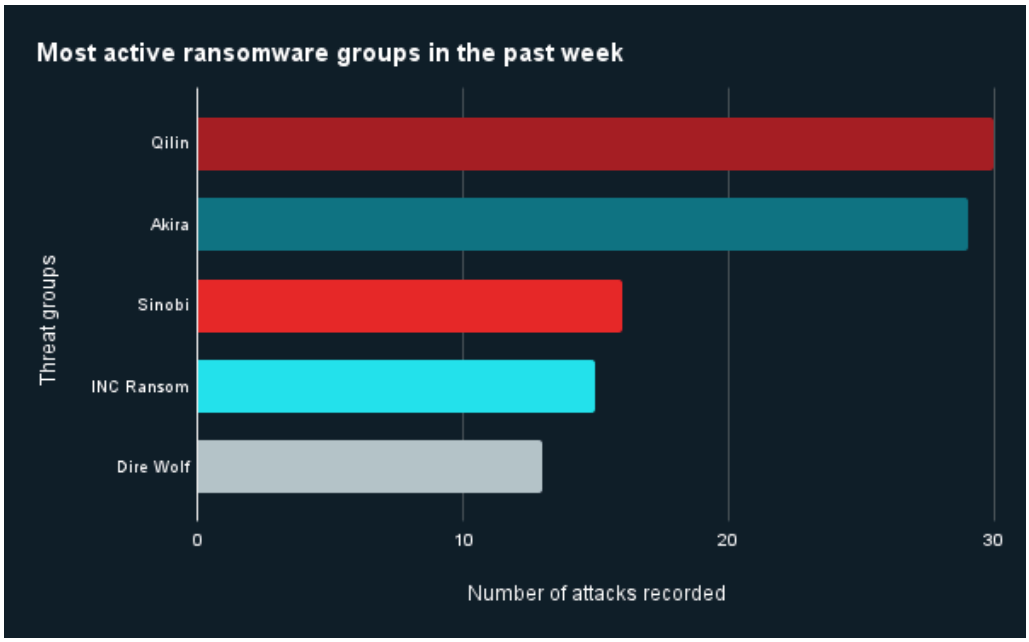
- **What this means:** The flaw impacts applications that process ICC color profiles, enabling memory corruption or code execution. Applications using iccDEV are likely to crash or be compromised by malicious ICC profiles, enabling attackers to cause denial of service and execute arbitrary code.
- **Affected products:**
  - iccDEV versions before 2.3.1.2

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

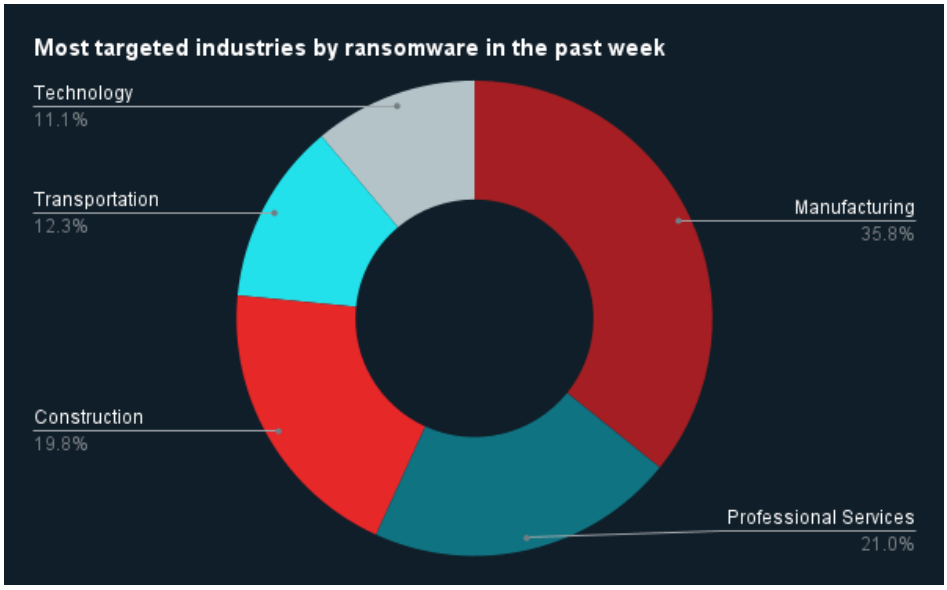
Ransomware Round-up from Past Week

Last week in ransomware: In the past week, Qilin, Akira, Sinobi, INC Ransom, and Dire Wolf were the most active ransomware groups. ZeroFox observed at least 133 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 Sinobi.



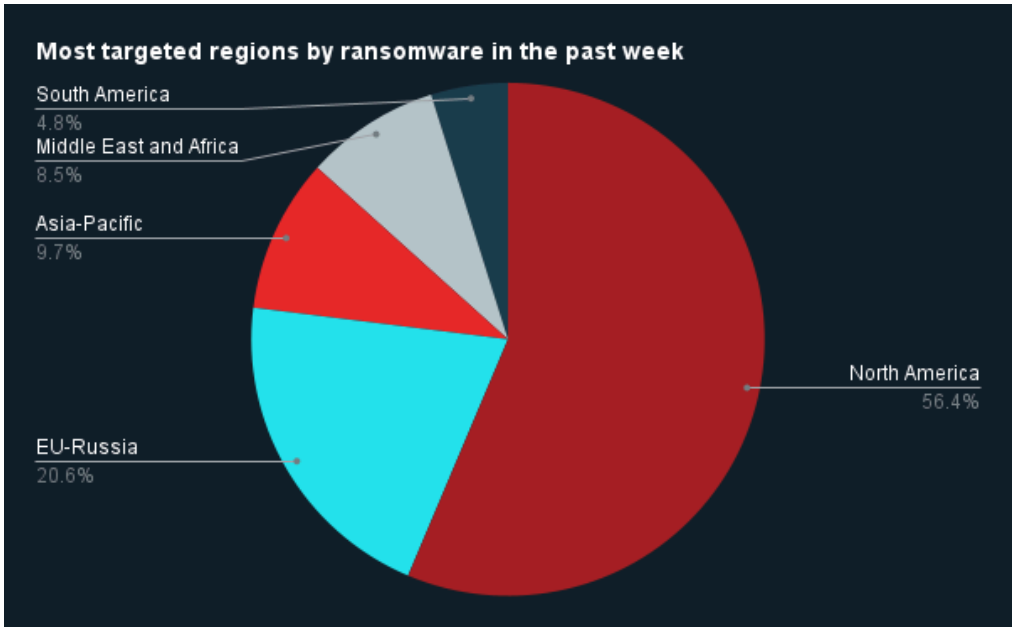
Source: ZeroFox Internal Collections

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



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

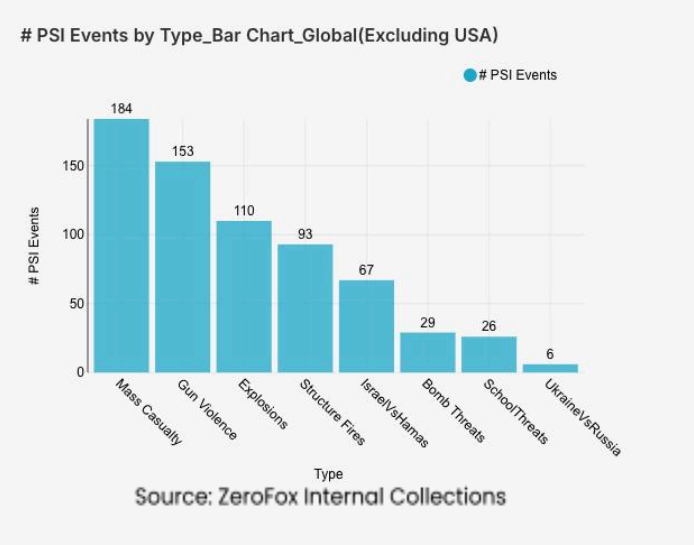
Past Week's Three Most Impactful Breaches

Targeted Entity	Department of Education in Victoria	Vida Y Salud-Health Systems	Central Maine Healthcare (CMH)
Compromised Entities/victims	Current and former students	34,504 Texas residents	More than 145,000 individuals
Compromised Data Fields	Personal information, including birth dates, home addresses, phone numbers, email addresses, and encrypted passwords	Names, addresses, dates of birth, Social Security numbers, driver's license numbers, account numbers, and claim numbers	Full names, dates of birth, treatment information, dates of service, provider names, health insurance information, and Social Security numbers
Suspected Threat Actor	Unnamed	Unnamed	Unnamed
Country/Region	Australia	Texas	Maine
Industry	Education	Healthcare	Healthcare
Possible Repercussions	Social engineering, spear-phishing, blackmail, extortion, and account takeovers	Identity fraud, parking ticket scam, spear-phishing, and social engineering	Insurance fraud, identity fraud, social engineering, blackmail, and extortion

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

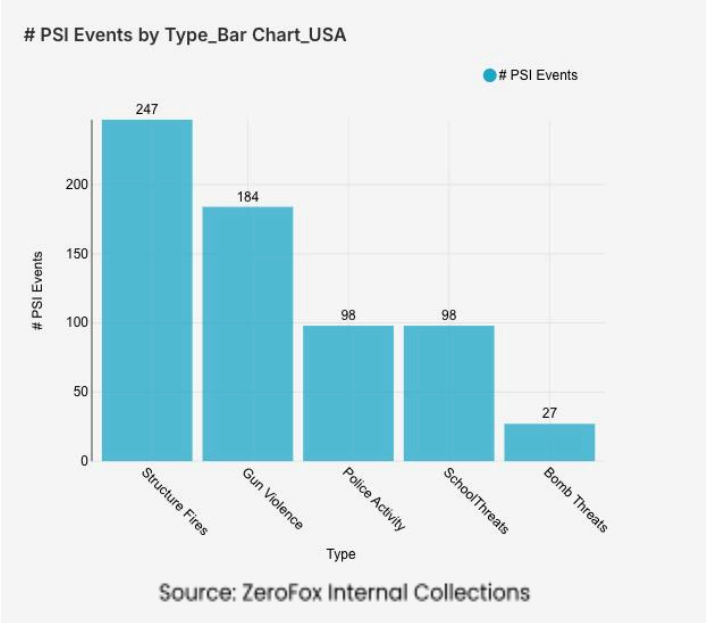


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 5 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being India, the Netherlands, and Syria (in that order). Approximately 60 percent of these events were explosions, and the three aforementioned countries accounted for about 38 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 43 percent from the previous week. Events related to Russia's war in Ukraine increased by 20 percent. The top three most-alerted subtypes were gun violence, which saw a 23 percent decrease from the previous week; explosions, which also decreased by 23 percent; and structure fires, which decreased by 11 percent. Notably, bomb threats increased by 81 percent, and threats related to schools increased by 160 percent.

- **What this means:** Even with a small decrease in global mass casualty events this week, regional volatility persisted within certain conflict zones. Russia's war in Ukraine saw an increase in alerts despite recent peace negotiations, marked by a missile barrage on January 8 near Lviv, just 50 miles from NATO-ally Poland's border. Concurrently, the Israel-Hamas conflict also saw a significant uptick in alerts, with the Israeli Defense Force releasing footage of a firefight in Rafah that killed six gunmen on January 14. Both bomb threats and school threats saw sharp increases this week, as several Indian schools in Amritsar and Moga received bomb threat emails on January 14, followed by a bomb threat against a court complex in Ludhiana on the same day. The Netherlands experienced an explosion at an electrical substation on January 14, which caused power outages across Amsterdam. A ceasefire collapsed in Syria on January 9, triggering an offensive near Aleppo; additionally, the United States launched retaliatory airstrikes against ISIL near Palmyra on January 10 after an ambush killed three American personnel. Overall, the current global landscape is defined by a volatile mix of intensifying regional conflicts and targeted threats against public institutions and infrastructure.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were California and Pennsylvania, which together made up 17 percent of this week's nationwide total. Gun violence across the United States overall increased by 16 percent from the week prior. Police activity alerts increased by 81 percent, and the top contributing states were Texas and California. Structure fires decreased by 14 percent, and the top two contributing states for this subtype were California and New York. Notably, bomb threats increased by 286 percent, and threats related to schools increased by 250 percent.

- **What this means:** Recent data indicates a volatile domestic security landscape in the United States, primarily driven by sharp increases in bomb threats and school threats. Texas has emerged as the primary epicenter for these disruptions; on January 14, Frisco Independent School District campuses were locked down after a second round of threatening emails within a week. This follows a broader FBI investigation, launched January 8, into a viral social media threat targeting 14 schools in the Dallas-Fort Worth area. General police activity alerts have spiked nationwide, largely fueled by U.S. Immigration and Customs Enforcement (ICE) activity in Minnesota as part of "Operation Metro Surge." In the city of Minneapolis, tensions reached a breaking point on January 14 and 15, after a federal agent shot a man in the leg during an enforcement operation one week after the fatal shooting of Renee Nicole Good. Federal officials have confirmed roughly 2,500 arrests in the Minneapolis area alone since the surge began. Overall, the current U.S. physical security landscape is defined by an intersection of high-frequency institutional threats and a significant expansion of federal law enforcement operations.

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%