ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

January 31, 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 29, 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 - Cl0p Lists Latest Wave of Victims on Leak Site

Ransomware and digital extortion (R&DE) collective Cl0p has claimed at least 46 victims on its victim shame site over the past week (an unusually high number in the short time period), portending an increase in operational tempo in the near term that is likely to increase their notoriety and pressure victims to pay the demanded ransoms. Since first observed in Q1 2022, Cl0p has had notable quarters of high-tempo activity very likely related to targeted extortion campaigns followed by several periods of relatively low activity. Although Cl0p has posted an extensive list of alleged victims on their leak site in the past week, they have not yet provided any details about an ongoing campaign or the type of data allegedly compromised.

ZeroFox Intelligence Flash Report - Iran Situation Update

The Iranian government is reportedly conducting a brutal crackdown on anti-regime protests. Media reports have stated the death toll is as high as 35,000 protestors; however, human rights researchers have thus far confirmed approximately 6,000 are dead, with at least 18,000 deaths still under investigation. In response to the crackdown, the United States has moved an aircraft carrier and several destroyers into the region. This likely indicates a U.S. intention to force Iran to ease the crackdown measures, stop executing protesters, 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 in the next two weeks. Anti-regime activists briefly took control of Iran's state-run television to broadcast calls for further protests, and Iranian-backed threat actor collective "Handala Hack" used Starlink to conduct attacks against Israeli targets—despite a nationwide internet shutdown. Regardless of any military responses, cyber operations targeting Iran are almost certain to continue—and will likely increase—for the foreseeable future. Both the United States and Israel likely view the government in Iran as weak and are very likely to use cyber warfare to disrupt Iran's repression apparatus.

ZeroFox Intelligence Flash Report - Luxshare Allegedly Breached by RansomHouse

On January 9, 2026, ransomware and digital extortion (R&DE) collective "RansomHouse" announced an alleged breach of Luxshare Precision Industry Co. Ltd. (Luxshare)—one of the largest third-party

manufacturers for tech giant companies—on its dark web victim leak site. Luxshare is a China-based major electronics manufacturer whose partners include, but are not limited to, Apple, Nvidia, LG, Geely, and Tesla—companies whose data has allegedly been exposed in the RansomHouse breach. Although some reports suggested the now-defunct "RansomHub" collective claimed responsibility for the alleged attack, it is almost certain that RansomHouse is the R&DE responsible for the breach; any alleged affiliations or cooperation between the two collectives remain unconfirmed. The data allegedly exposed by RansomHouse could very likely be sold to competitors and used for reverse engineering or by criminals seeking to manufacture counterfeit devices and technology.

ZeroFox Intelligence Flash Report - European Law Enforcement Raids Black Basta Actors' Homes

On January 15, 2026, law enforcement agencies from Ukraine and Germany raided the homes of two individuals suspected of conducting activities as part of the Black Basta ransomware collective. In addition to the raids, the alleged leader of Black Basta—a Russian individual identified as Oleg Evgenievich Nefedov—was placed on both EUROPOL's Most Wanted list and Interpol's Red Notice list. Black Basta first appeared in April 2022 and has likely conducted successful attacks against at least 500 companies across North America, Europe, and Australia. In that time, the collective has likely earned hundreds of millions of dollars in illicit ransom payments. ZeroFox assesses that Black Basta likely ceased operations in early 2025 and has not been active since. Initially, there were indications that Black Basta actors may have transitioned to the CACTUS ransomware group; however, CACTUS has also been inactive since mid-2025.

ZeroFox Intelligence Assessment - Winter Olympic Games Milano Cortina 2026

ZeroFox assesses civil unrest in Italy has an unlikely chance of disrupting aspects of the 2026 Winter Olympics; however, this situation should be continuously monitored for changes as the Games and related events approach. In the weeks leading up to the Games, there has been a spike in anti-American sentiment, particularly related to recent U.S. foreign and immigration policy. ZeroFox did not identify any evidence of active or coordinated threats on the deep and dark web (DDW) targeting the Games. However, we identified threats that pose a passive risk, including compromised credentials and botnet logs for sale, as well as suspicious domains impersonating official 2026 Winter Olympics branding. Additionally, ZeroFox identified accommodation and ticket scams that pose a risk to attendees and viewers.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Long-Term Espionage Reportedly Targeting UK Govt Officials

What we know:

- Chinese state-linked espionage group Salt Typhoon allegedly maintained long-term access to phones used by senior UK government aides, raising concerns that sensitive communications since at least 2021 have been exposed.
- The suspected intrusion reportedly targeted phones used by senior aides to former UK prime ministers Boris Johnson, Liz Truss, and Rishi Sunak, though it remains unclear if the prime ministers' own devices were compromised.
- As of reporting, it is unconfirmed whether Salt Typhoon's access to critical communication lines has been removed.

Background:

- The activity was uncovered in 2024 following U.S. disclosures of widespread Chinese-linked telecom breaches, with officials warning attackers could record calls at will.
- Salt Typhoon has previously been reported compromising telecom providers to covertly collect communications and metadata without infecting individual devices.

Analyst note:

- If Salt Typhoon still maintains its access, it is likely to continue exfiltrating senior aides' real-time movements and routines, as well as meetings and travel-related information, to the Chinese government.
- China is likely to use this information to anticipate UK policy decisions, negotiation positions, and internal discussions and leverage this knowledge in future global policy meetings.

FBI Seizes Russian Dark Web Forum RAMP

What we know:

- The Federal Bureau of Investigation (FBI) has seized popular Russian-language dark web forum Russian Anonymous Marketplace (RAMP), which was used by cybercriminals to advertise and promote various cybercrime services, including ransomware operations.

Background:

- RAMP's onion site and its clearnet domain (ramp4u[.]io) display a seizure notice, and the domain server names reflect those used during FBI seizure operations.
- However, the FBI has yet to release an official statement. "Stallman", an alleged former RAMP operator confirmed the seizure on dark web platform XSS.

Analyst note:

- The seizure is likely to expose forum users' data, including emails, IP addresses, and messages, especially of those lacking robust operational security.
- Law enforcement is likely to use the data to disrupt or apprehend other cybercriminals. Other Russian-language dark web forums are likely to witness more traffic due to RAMP's seizure.

ShinyHunters Targeting Over 100 Organizations in SSO Credential Stealing Campaign

What we know:

- Threat group ShinyHunters is reportedly targeting more than a hundred organizations in its ongoing single sign-on (SSO) credential stealing campaign.
- Canva and Epic Games are among the organizations being allegedly targeted.

Background:

- Even though the organizations are reportedly being targeted, there is no evidence of breach.
- A leak site associated with threat collective "Scattered Lapsus$ Hunters" has been rebranded to "ShinyHunters".

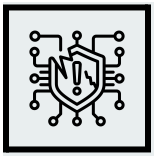
Analyst note:

- Ongoing targeting of organizations suggest ShinyHunters is very likely attempting to breach cloud environments and steal sensitive data.
- ShinyHunters has also reportedly approached some victim entities with ransom demands.

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 seven vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on January 23, January 26, and January 27, 2026. It also added four Industrial Control System (ICS) advisories on January 27. A critical sandbox escape vulnerability, tracked as CVE-2026-22709, has been discovered in the popular Node.js library vm2, which enables attackers to execute arbitrary commands on the underlying host operating system. OpenSSL released patches for 12 security flaws, including a high-severity remote code execution (RCE) flaw, as part of its January 2026 Patch Tuesday updates. Cybersecurity researchers have disclosed two new eval injection vulnerabilities (CVE-2026-1470 and CVE-2026-0863) in the n8n workflow automation platform that could enable RCE.

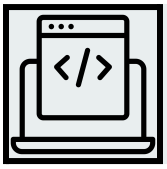


HIGH

CVE-2026-21509

What happened: This is a security feature bypass flaw that can enable attackers to exploit malicious Office files to circumvent Object Linking and Embedding (OLE) protections via user interaction. Microsoft has issued emergency out-of-band updates to fix this flaw.

- **What this means:** Attackers are likely to continue exploiting malicious Office documents to bypass OLE security controls in vulnerable systems. Affected devices are likely to increase the risk of initial access, malware delivery, and lateral movement.
  - **Affected products:** The affected products are listed in this advisory.



CRITICAL

CVE-2026-24858

What happened: This is a zero-day authentication bypass vulnerability in Fortinet products when FortiCloud SSO is enabled that is being actively exploited. Fortinet has blocked FortiCloud SSO connections from devices running vulnerable versions. This comes after reports of FortiGate firewalls being compromised on January 21, 2026.

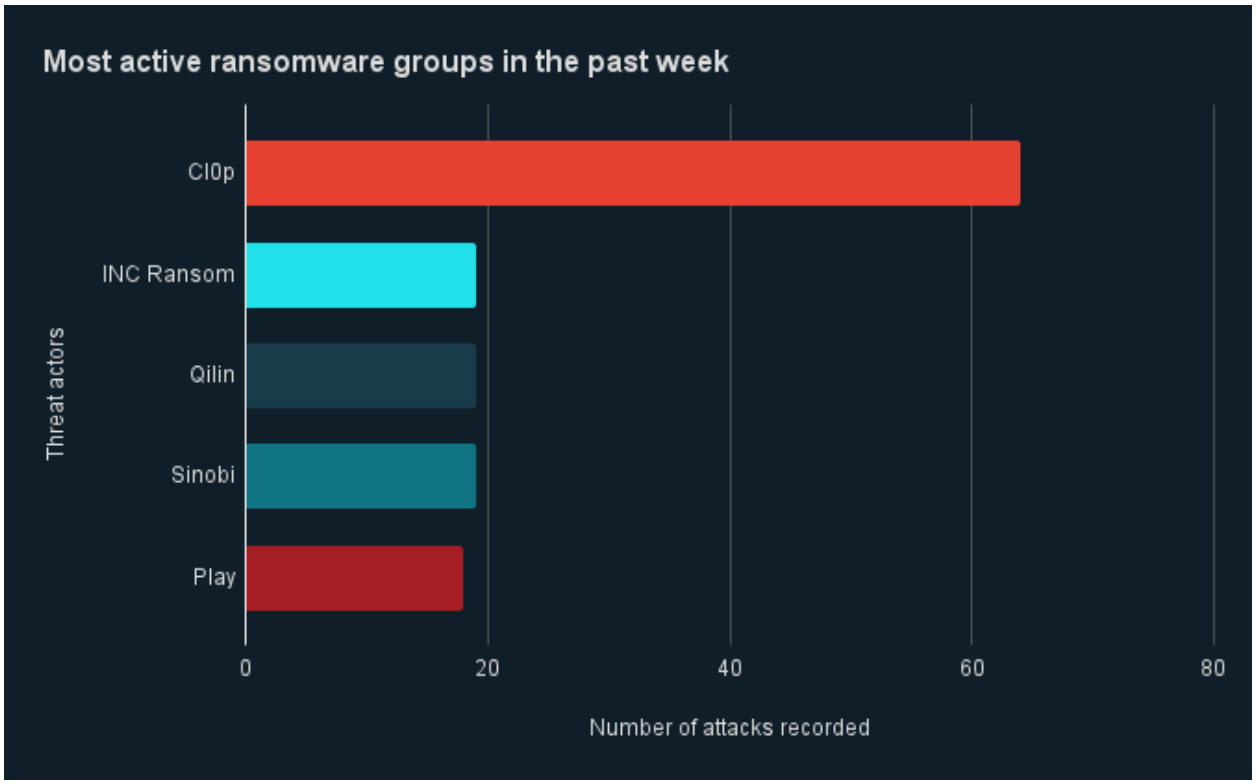
- **What this means:** Compromised systems are very likely at risk of enabling further intrusions into networks, which can facilitate attacks such as data theft, disruptions, and malware infection.
    - **Affected products:** The affected products are listed in this advisory.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

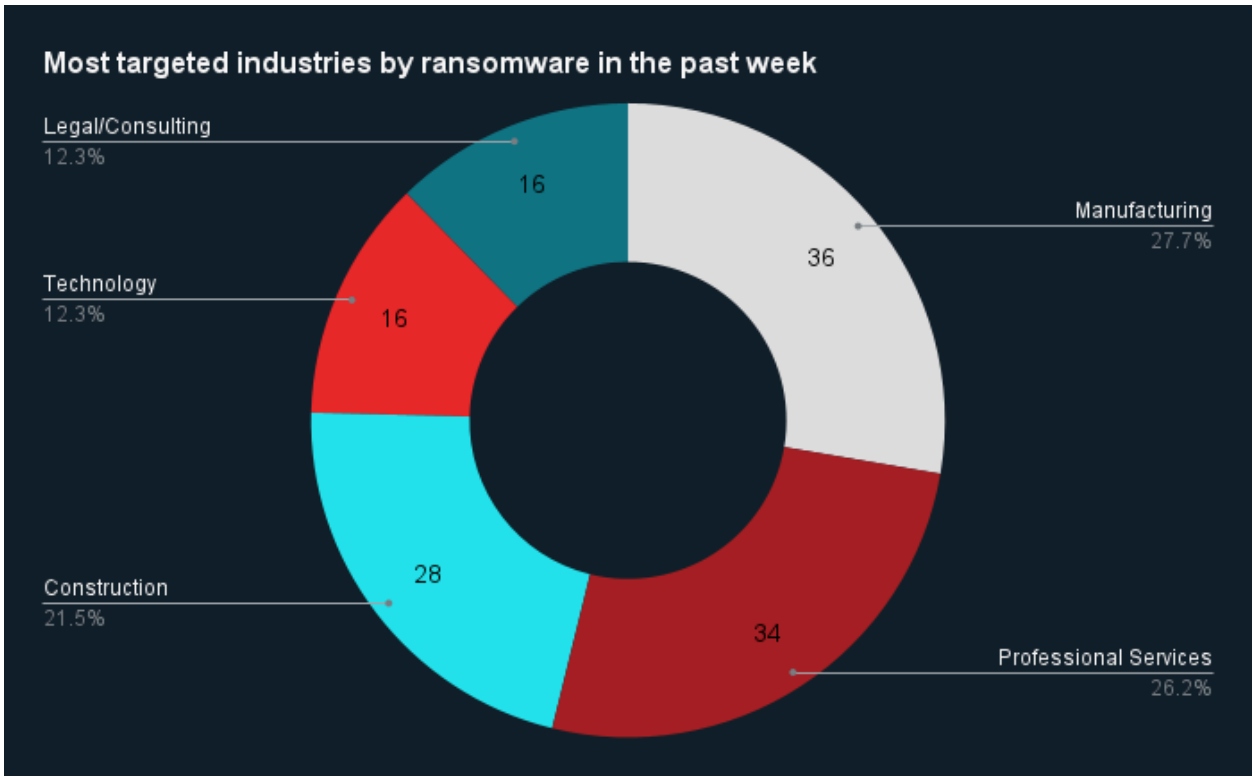
Ransomware Trends: Groups, Industries, Regions

Last week in ransomware: In the past week, ZeroFox has observed that the Cl0p was the most active ransomware group, followed by INC Ransom, Qilin, Sinobi, and Play. ZeroFox observed close to 206 ransomware victims being disclosed, most of whom were located in North America.



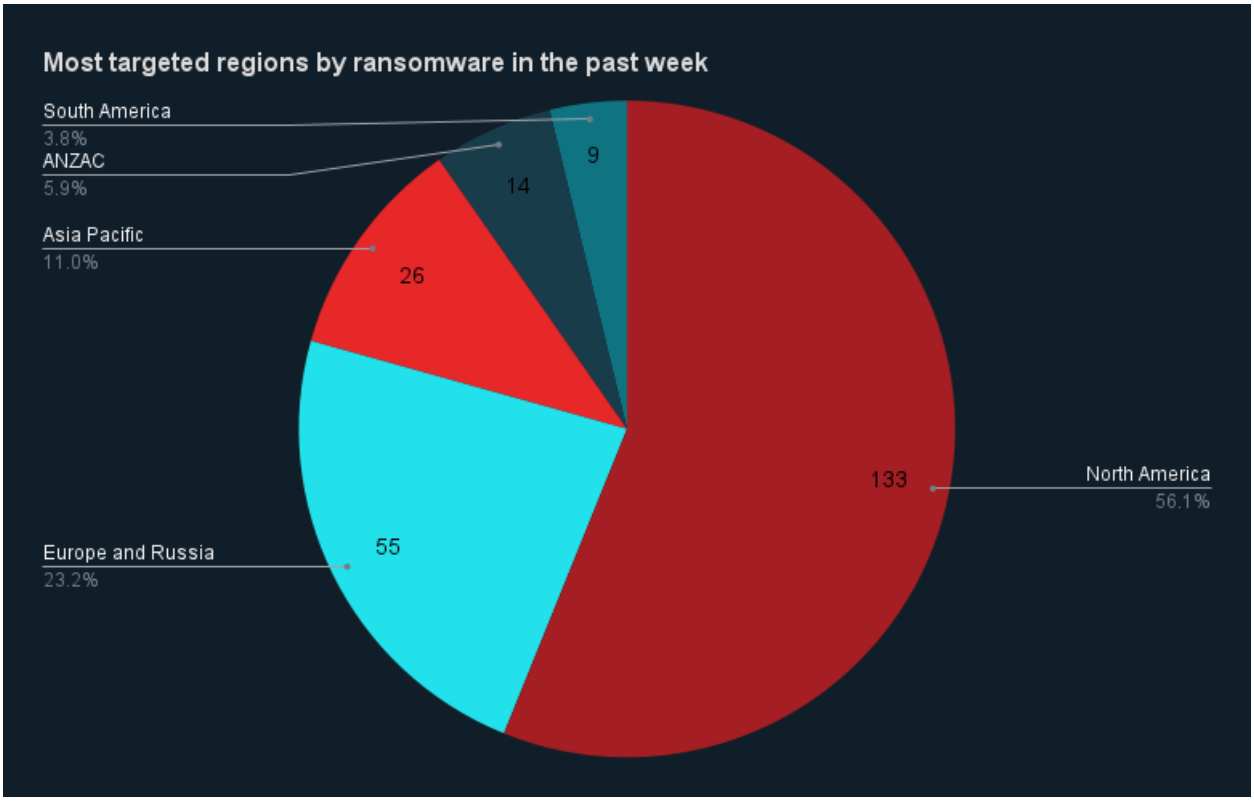
Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by professional services and 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 133 incidents observed in North America, while Europe and Russia accounted for 55, Asia-Pacific for 26, Australia and New Zealand (ANZAC) for 14, and South America for nine.



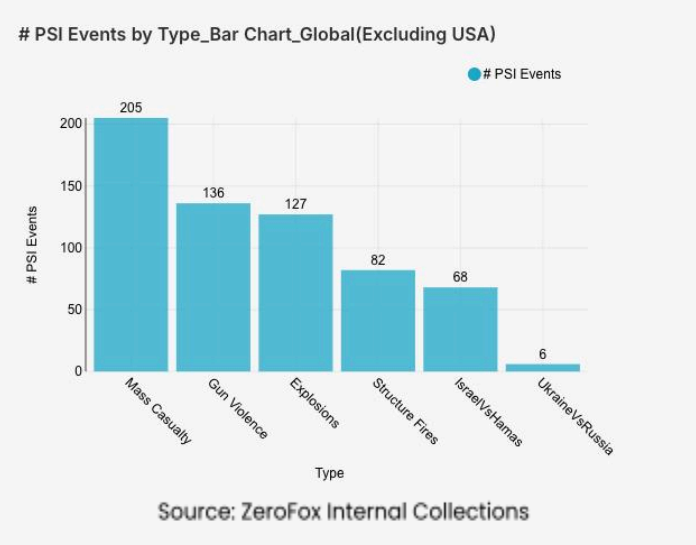
Source: ZeroFox Internal Collections

Major Data Breaches Reported in the Past Week

Targeted Entity	Crunchbase	Unimed	Call-On-Doc
Compromised Entities/victims	400 MB of compressed files with over two million records	Patients	Over one million user records
Compromised Data Fields	Personally identifiable information (PII)	Internal documents, government records, patients' PII and other data, and payment details	Patients' PII and health data, including sensitive details such as sexually transmitted diseases
Suspected Threat Actor	ShinyHunters extortion group	DarkForums user ByteToBreach	BreachForums user iProfessor
Country/Region	North America	Brazil	United States
Industry	Professional Services	Healthcare	Healthcare
Possible Repercussions	Extortion, resale of data, misuse of data for phishing, social engineering attacks, and identity fraud	Phishing, social engineering attacks, identity theft, and insurance fraud	Exposed individuals are likely to be targets of blackmail, extortion, phishing, and social engineering campaigns

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings



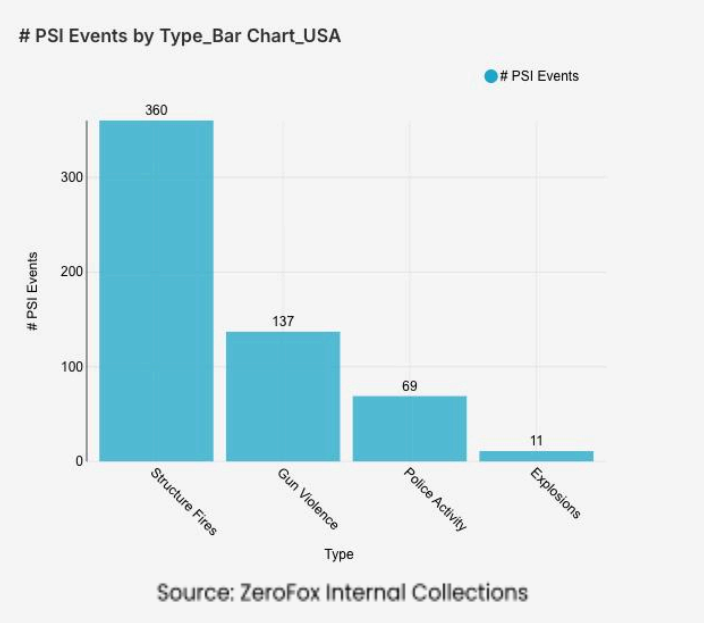
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was an 8 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being India, Mexico, and the Palestinian territories, in that order. Approximately 62 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 37 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) increased by 15 percent from the previous week. Events related to Russia's war in Ukraine increased by 50 percent. The top three most-alerted subtypes were gun violence, which saw an 18 percent decrease from the previous week; explosions, which increased by 12 percent; and structure fires, which decreased by 24 percent.

- **What this means:** Global mass casualty events increased this week, driven heavily by explosive incidents and gun violence. In India, security forces were on high alert for Republic Day (January 26) following the seizure of 10,000 kg of explosives in Rajasthan as part of a planned attack. Mexico experienced a mass casualty event on January 26, when gunmen opened fire at a soccer field in Salamanca, killing 11 and injuring 12, an attack linked to the ongoing Santa Rosa de Lima and Jalisco New Generation cartel war. Russia's war in Ukraine saw a significant increase in activity this week as well, with Russian forces launching over 700 drones and escalating daylight ballistic missile strikes on civilian centers such as Kharkiv within the last week. Meanwhile, despite a fragile ceasefire, Palestinian territories saw a rise in general alerts as military raids and intermittent violence persist. While global gun violence saw a slight decline, the increase in explosions underscores a shift toward more lethal, indiscriminate tactics in these primary conflict zones.

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 22 percent of this week's nationwide total. Gun violence across the United States overall decreased by 28 percent from the week prior. Police activity alerts decreased by 27 percent, and the top contributing states were California and Texas. Structure fires increased by 9 percent, and the top two states for this subtype were California and New York. Notably, explosions increased by 83 percent.

- **What this means:** Recent trends in United States public safety highlight a complex environment of decreasing direct interpersonal violence but increasing structural and infrastructure-based risks. Structure fires increased this week, exacerbated by extreme winter conditions. In New York, firefighters battled a four-alarm blaze in a Bronx building on January 28, while California continues to face a housing crisis following the Palisades and Eaton fires. The sharp increase in explosions is typified by the January 28 federal report on a deadly natural gas blast at a Pennsylvania nursing home; cold temperatures in general are correlated with heightened usage of heating devices, which increase structure fire and gas explosion risks. In Minnesota, public safety concerns continue with regard to federal immigration deployment (Operation Metro Surge), which has led to high-profile fatalities and subsequent unrest and police activity. These incidents, occurring amidst a historic winter storm that claimed over 100 lives across 20 states this week, underscore a week defined more by infrastructure failure and environmental hazards than by organized conflict.

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%