ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

February 21, 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 19, 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 - DDoS Attacks Target Spanish Government Websites

Over the period of February 16-17, 2026, pro-Russia threat collectives NoName057(16) and Server Killers alleged they were responsible for coordinated distributed denial-of-service (DDoS) attacks against multiple Spanish government websites and provided check-host links to verify their claims. The alleged motivation behind their attacks was the Spanish government's perceived support of Ukraine and its participation in Operation Eastwood. On January 19, 2026, the National Cyber Security Centre (NCSC)—a part of the United Kingdom's Government Communications Headquarters (GCHQ)—issued an alert highlighting the persistent targeting of UK organizations by Russian state-aligned hacktivist groups aiming to disrupt networks. This recent coordinated string of DDoS attacks demonstrates the ongoing threat faced by NATO members and organizations perceived as pro-Ukraine posed by collectives who are considered pro-Russia. ZeroFox assesses it is very likely that pro-Russia and anti-West hacktivist collectives will continue to target Western institutions throughout 2026 and that NoName057(16) will collaborate with other pro-Russia collectives to conduct DDoS attacks against perceived pro-Western targets in the coming months.

ZeroFox Intelligence Flash Report - Sabotage and Cyber Disruptions at Milano Olympics

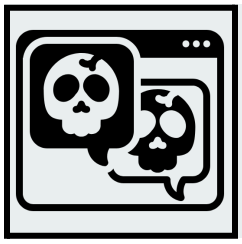
The Russian Federation has a history of targeting the Olympics with cyberattacks as revenge for its formal exclusion from the Games (such as in the Paris 2024 Summer Olympics). With Russian athletes once again slated to compete as Individual Neutral Athletes rather than represent the country and the added factor of Italy's continued support for Ukraine, Russia-aligned hackers are likely to continue targeting the cyber infrastructure of the 2026 Winter Olympics. Pro-Russian hacktivists are very likely to continue conducting low-impact attacks targeting Olympics-related events and states that oppose Russia's participation in the Games. Travel disruptions and acts of sabotage targeting transportation infrastructure have also taken place and are likely to continue through the Games. There is a roughly even chance that these efforts will result in minor disruptions to the event, dissuade spectators from attending, and lead to reputational damage for the host and the International Olympic Committee (IOC).

ZeroFox Intelligence Flash Report - 0APT Syndicate Lacking Credibility

ZeroFox assesses that newly founded and self-proclaimed ransomware-as-a-service (RaaS) collective 0APT Syndicate (0APT) is very likely a scam or hoax group. As of this writing, the group has not published any legitimate data from its list of 200 alleged victim companies; further, the purported data samples on its leak site cannot be downloaded and appear to be entirely fabricated. While little is known about the group at this time, the operators have explicitly stated that they are politically neutral and motivated solely by financial gain. Although the ransomware 0APT purports to be using is fully functional, it was first created in 2011 and most recently updated in 2023—making it unlikely the group is actually conducting data breaches, as operational ransomware groups typically update their executables more frequently. All available evidence suggests that 0APT is almost certainly a scam and not a legitimate threat at this time.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Keenadu Malware Embedded in Various Android Device Brands Globally

What we know:

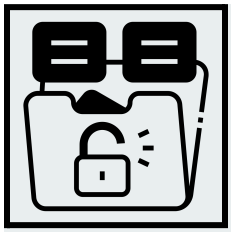
- A sophisticated Android malware strain called Keenadu has been found embedded in the firmware of various Android device brands and trojanized apps across multiple applications, including some distributed through Google Play.
- The malware strain's control and delivery mechanism, AKServer, uses geographic checks to limit exposure, shutting down Keenadu if the device is set to Chinese language and time zone.

Background:

- Keenadu reportedly spreads through compromised over-the-air (OTA) firmware, system apps, third-party tools, and Google Play apps, impacting over 13,000 users (mainly in Russia, Japan, Germany, Brazil, and the Netherlands).
- Keenadu infiltrates the core of the Android Operating System (OS) by infecting the libandroid_runtime.so library. This allows the malware to hook into the Zygote process (the parent process for all Android applications), effectively injecting malicious code into every app launched on the device.
- The malware strain is designed to avoid detection by not serving payloads until two and half months after device initialization.

Analyst note:

- The actor behind Keenadu is likely building a broad surveillance and data theft pipeline.
- Keenadu is reportedly linked to a wider ecosystem of major Android botnets, including Triada, BADBOX, and Vo1d. These connections suggest a shared supply chain infrastructure or coordinated operations between distinct Chinese-origin actors.
- The multiple distribution paths (OTA firmware, trojanized apps, Google Play exposure) likely suggest an intent to create a durable supply chain-style foothold, enabling repeat infections and access across thousands of devices globally.



ZeroDayRAT Expands Mobile Threats

What we know:

- Researchers have observed a new commercial mobile spyware platform called ZeroDayRAT being sold on Telegram as a full-service surveillance and theft toolkit for Android and iOS devices.
- ZeroDayRAT is designed to operate across Android versions 5 through 16 and iOS versions up to 26, providing broad compatibility for attackers.

Background:

- Once installed, ZeroDayRAT gives operators access to device details, messages, app activity, and real-time GPS tracking with location history.
- It also enables direct financial theft through wallet address substitution for crypto apps and banking stealer modules targeting mobile payment platforms such as Apple Pay.

Analyst note:

- Since this platform provides an easy-to-use comprehensive suite of data theft and surveillance capabilities, it is likely to see an increase in wider criminal adoption and more aggressive campaigns.
- Threat actors are likely to use phishing lures, fake app marketplaces, and executable programs such as APK files to infect more victims at scale.

Top U.S. Companies Targeted in Massive Phishing Campaign

What we know:

- A financially motivated threat actor group dubbed GS7 is running a large-scale phishing campaign known as “Operation DoppelBrand.”
- The campaign weaponizes brand impersonation to target Fortune 500 firms and other high-value entities, mainly in the United States.

Background:

- Attackers create deceptive domains using registrars and route traffic through Cloudflare to conceal their IP addresses, making them difficult to trace.
- Victims are enticed to click on these links and provide their credentials, which are then sent to attacker-controlled Telegram bots (NfResultz by GS).
- Additionally, the obtained access is used to install remote management and monitoring on victims' systems.

Analyst note:

- Threat actors are likely to act as initial access brokers (IABs), selling the infrastructure access to affiliates and other ransomware groups.
- Moreover, the remote management system is likely to serve as a persistent gateway for threat actors, using initial access as a foothold to encrypt files and demand ransom.
- They are also likely to steal trade secrets and intellectual property to try and sell it to their competitors.

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 February 13, February 17, and February 18. On February 17, CISA also released four Industrial Control System (ICS) advisories, which includes CVE-2026-1670, CVE-2026-1762, CVE-2026-1361, CVE-2026-23715, and other vulnerabilities. CVE-2026-2441 is a recently-patched use-after-free vulnerability in CSS in Google Chrome that was found being actively exploited in the wild. The flaw enables a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE-2026-1249 is an authenticated server-side request forgery (SSRF) flaw in the Sonaar MP3 Audio Player for WordPress that enables threat actors to gain unauthorized access to internal network requests via the "load_lyrics_ajax_callback" function. Intego Personal Backup for macOS contains a local privilege escalation flaw (CVE-2026-26225) due to backup task files being writable by non-privileged users but executed with elevated privileges. An attacker can craft a malicious task file to perform arbitrary file writes in protected system paths, ultimately escalating access to root.

CRITICAL

CVE-2026-22769

What happened: CVE-2026-22769 is a hardcoded credential zero-day vulnerability in Dell RecoverPoint for Virtual Machines. A suspected China-linked threat group has been exploiting this vulnerability since mid-2024 to breach VMware-focused environments.

- **What this means:** After gaining access, the attackers could deploy new Grimbolt backdoor malware and use stealthy "Ghost NIC" techniques to pivot deeper into victim networks. Threat actors are likely to gain unauthenticated remote access to VMware backup infrastructure, enabling root-level persistence and long-term control over critical systems.
  - **Affected products:** The affected products are listed in this advisory.

CRITICAL

CVE-2026-2329

What happened: This vulnerability is an unauthenticated stack-based buffer overflow in a phone's web Application Programming Interface (API) endpoint. A crafted "request" parameter can overflow a 64-byte stack buffer, enabling remote code execution (RCE) with root privileges.

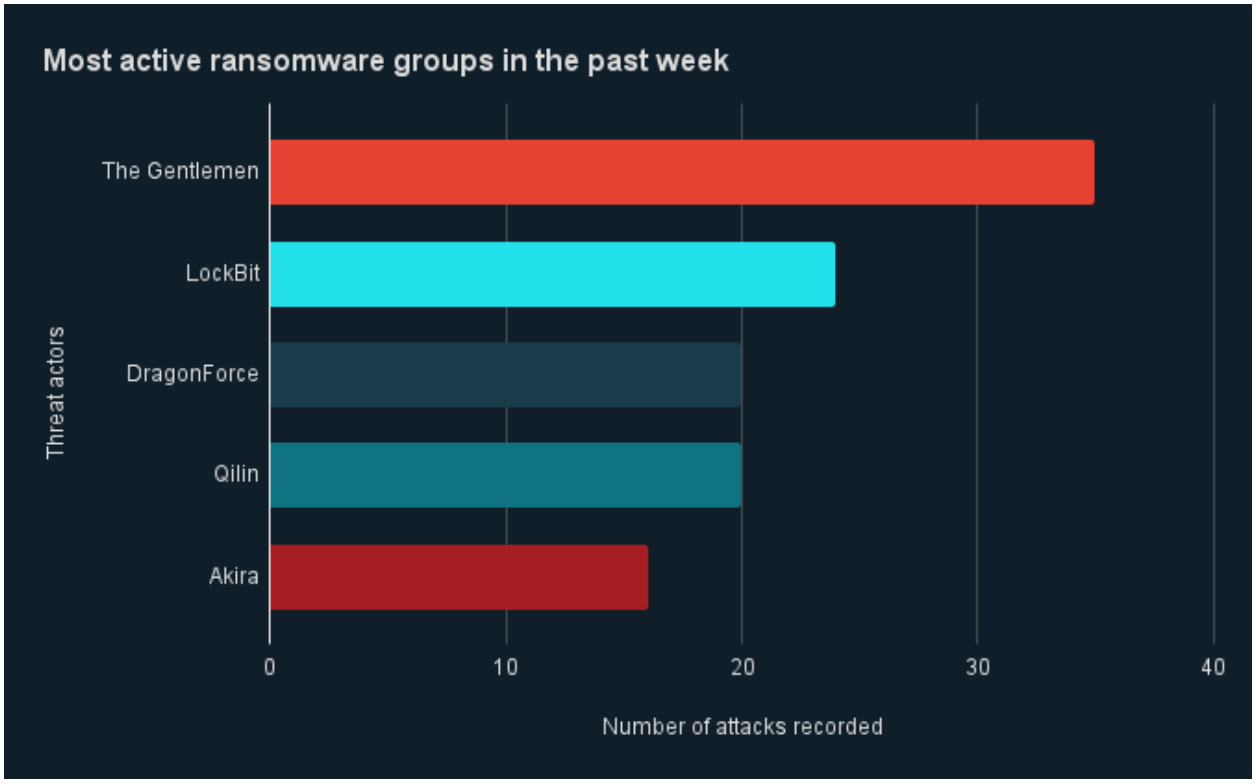
- **What this means:** This flaw in Grandstream GXP1600 VoIP phones that could let attackers remotely take full control of affected devices. Hijacked phones are likely to be exploited for call redirection and impersonation impacting operations.
  - **Affected products:** Grandstream versions GXP1610, GXP1615, GXP1620, GXP1625, GXP1628, and GXP163

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

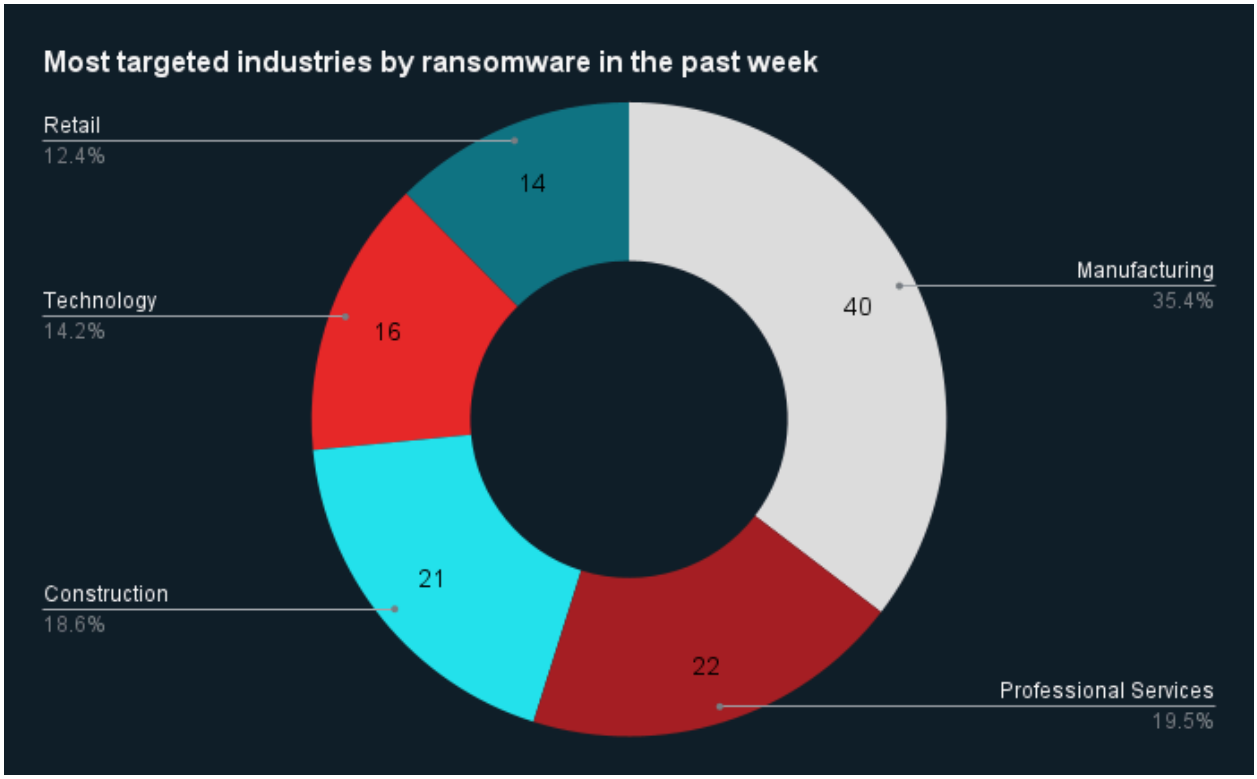
Ransomware Trends in the Past Week

Last week in ransomware: In the past week, The Gentlemen, LockBit, DragonForce, Qilin, and Akira were the most active ransomware groups. ZeroFox observed close to 173 ransomware victims disclosed, most of whom were located in North America. The Gentlemen ransomware group accounted for the largest number of attacks, followed by LockBit.



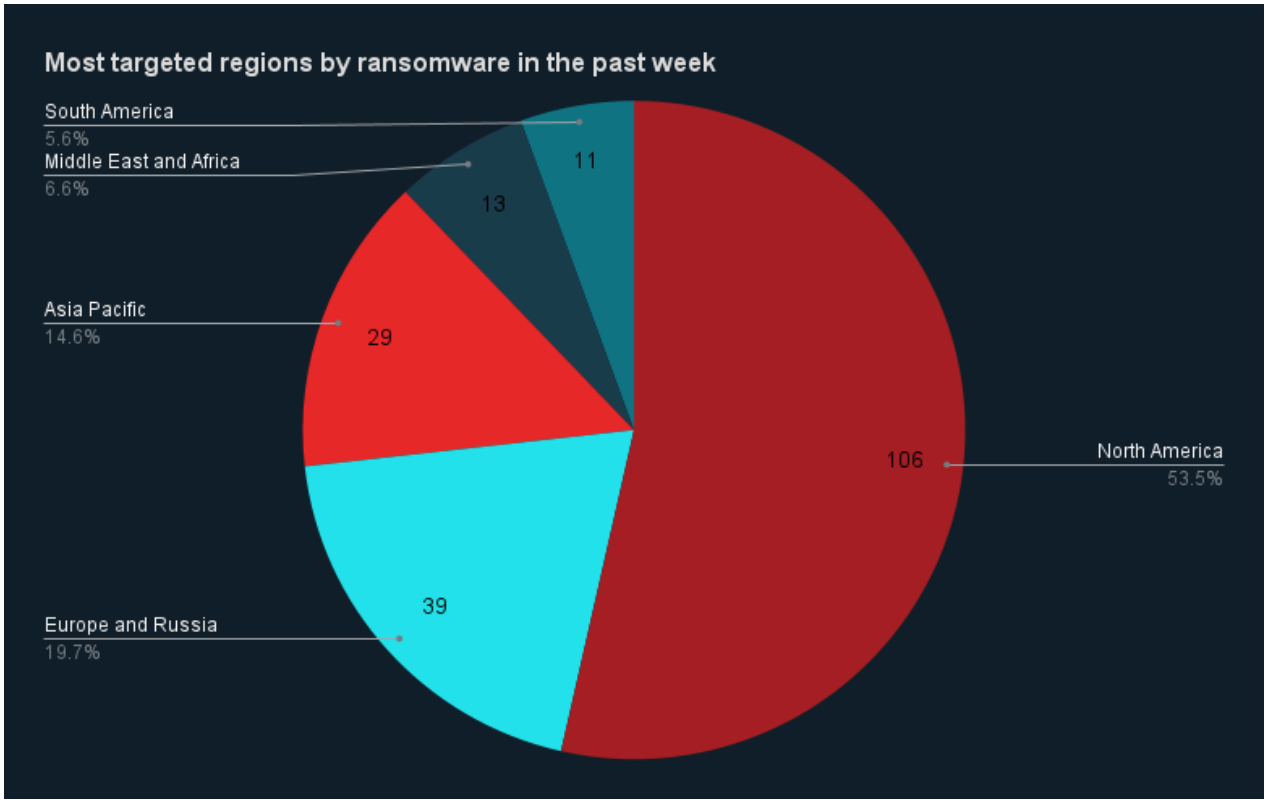
Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, manufacturing was the industry most targeted by ransomware attacks, followed by professional services, construction, technology, and retail.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past week, ZeroFox observed that North America was the region most targeted by ransomware attacks, followed by Europe and Russia. North America recorded 106 attacks, Europe and Russia recorded 39, Asia Pacific noted 29, while Middle East and Africa noted 13, and South America recorded 11.



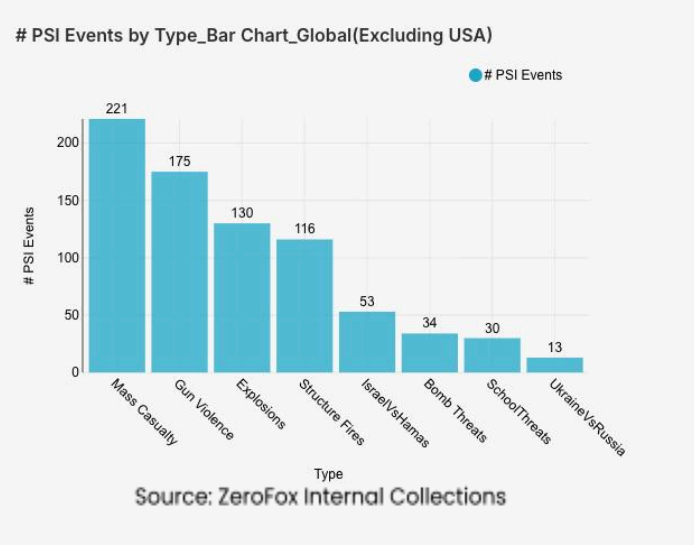
Source: ZeroFox Internal Collections

Three Major Data Breaches Reported in the Past Week

Targeted Entity	Adidas	Eurail B.V.	Figure
Compromised Entities/victims	Around 815,000 records	Customer database	2.5 GB of users' personally identifiable information (PII)
Compromised Data Fields	Names, emails, passwords, dates of birth, company details, and other technical information	Full names, passport details, ID numbers, bank account numbers, health information, and contact details	Customers' full names, home addresses, dates of birth, and phone numbers
Suspected Threat Actor	LAPSUS-GROUP	N/A	ShinyHunters
Country/Region	N/A	Europe	United States
Industry	Consumer Services	Critical Infrastructure	Financial Services
Possible Repercussions	Account takeover, compromise of stored financial details on accounts, phishing, social engineering, and identity theft attacks	Financial fraud, identity theft, phishing, and social engineering attacks	Phishing and social engineering attacks

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings

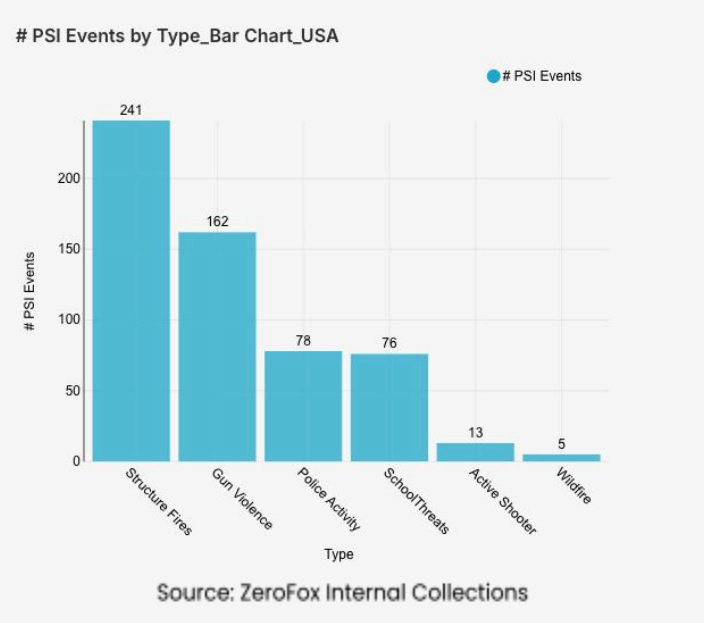


Physical Security Intelligence: Global

What happened: Excluding the United States, there was an 11 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being India, Mexico, and Russia, in that order. Approximately 59 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 33 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 30 percent from the previous week. Events related to Russia's war in Ukraine increased by 86 percent. The top three most-alerted subtypes were gun violence, which saw a 17 percent increase from the previous week; explosions, which increased by 9 percent; and structure fires, which increased by 5 percent.

- **What this means:** This week's data reveals an overall escalation in global violence. The spike in alerts related to Russia's war in Ukraine is reflected in the combined strike packages launched by Moscow this week; on February 17, Russian forces deployed 425 drones and missiles targeting energy and transport infrastructure across regions such as Kharkiv, Odesa, and Dnipropetrovsk, causing widespread power outages and contributing to the rise in explosion-related alerts. In Mexico, the increase in gun violence is underscored by an attack on February 18, where gunmen opened fire on a public playground in the state of Morelos, killing one person and injuring eight others, including several children. This incident highlights how public spaces in Mexico are increasingly caught in the crossfire of cartel-related gun violence. India saw a wave of coordinated bomb threats on February 19 against multiple schools in Noida, with many similar events earlier this week across the country as well. Global physical security remains increasingly volatile overall, as surges in explosive events, institutional threats, and gun violence in several key regions remain prominent.

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 Illinois and California, which together made up 17 percent of this week's nationwide total. Gun violence across the United States overall increased by 18 percent from the week prior. Police activity alerts decreased by 14 percent, and the top contributing states were Texas and New York. Structure fires increased by 3 percent, and the top two states for this subtype were California and New York; wildfires also showed a sharp increase of 150 percent. Notably, active shooter alerts increased by 86 percent.

- **What this means:** Recent data underscores a volatile week for U.S. physical security, marked by an increase in gun violence and active shooter alerts. On February 16, a shooter opened fire during a high school hockey game at the Dennis M. Lynch Arena in Pawtucket, Rhode Island, resulting in two fatalities and three injuries before the perpetrator died by suicide. There were seven other mass shootings in the country within the last week, six of which occurred on February 15. In California, while authorities continue to manage the aftermath of man-made disasters such as the Eaton and Palisades fires, new threats emerged this week with the Cabrillo Fire in San Luis Obispo, contributing to the slight rise in structure fire alerts. While generalized police activity alerts saw a decrease nationwide, law enforcement remains engaged in monitoring large-scale public expressions of grievance in major urban centers. Domestic physical security overall is currently defined by a high volume of gun-related incidents and a growing tension between federal enforcement priorities and localized public responses.

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%