ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

February 28, 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 26, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

© 2026 ZeroFox, Inc. All rights reserved.

This Week's ZeroFox Intelligence Reports

Why European Energy is Targeted by Cyber Threat Actors

ZeroFox has observed an increase in cyberattacks targeting the European energy sector since 2024. European states have increased investment in the energy sector since Russia's war in Ukraine began, very likely attracting both geopolitically and financially motivated threat actors. During this transition to a modern energy grid, the wider European energy sector remains vulnerable to outside forces disrupting its energy supply. Efforts to avoid energy shortages since 2022 have likely contributed to the high cost of living and an uncompetitive business landscape in Europe, which together very likely risk undermining the future investments needed to safeguard European energy. Energy insecurity and rising costs have been a key source of political unrest in Europe since the Russia-Ukraine war began. Elevated energy prices will likely continue to generate social tensions. Russia is likely limiting supplies—thus driving up prices and contributing to the overall cost-of-living crisis—in an attempt to weaken Western resolve to back Ukraine.

Mexico Insecurity Heightened Ahead of World Cup

Following the successful Mexican special forces operation that killed Mexico's top cartel leader, Nemesio Oseguera Cervantes (AKA El Mencho), retaliatory acts of violence are likely to continue over the coming weeks to dissuade further counter-narcotics operations. Mexico's residents are the primary victims of cartel-related crime, and deliberate targeting of Westerners is rare; however, retaliatory cartel violence in major Mexican cities will likely injure or kill innocent bystanders. Mexican President Claudia Sheinbaum will likely continue facing pressure from the United States and her citizens concerned over crime and the risk of a cartel-inspired wave of violence ahead of Mexico hosting World Cup 2026. Previous Mexican presidents have pursued tougher-on-crime policies, only to abandon the approach once the security situation deteriorated.

© 2026 ZeroFox, Inc. All rights reserved.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

Cyber and Dark Web Intelligence Key Findings

U.S. Sanctions Russian Zero-Day Broker Operation Zero

What we know:

- The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has sanctioned Russian company Matrix LLC (operating as Operation Zero) for stealing and selling at least eight proprietary cyber tools created exclusively for use by the U.S. government and its allies.
- OFAC has also sanctioned entities that include United Arab Emirates (UAE) firm Special Technology Services LLC FZ (STS), offensive cybersecurity company Advance Security Solutions, a suspected member of the Trickbot cybercrime gang, and other associated individuals and entities.
- Operation Zero claims the Russian government among its clients.

Background:

- Operation Zero and its associated entities traded in zero-day exploits (technical methods, code, or techniques designed to leverage vulnerabilities) to enable unauthorized access, data theft, or remote control of targeted devices or environments.
- OFAC noted that Operation Zero recruited hackers and developed business relationships using its social media accounts (mainly X and Telegram), offering millions of dollars for legitimate exploits.
- The sanctions also coincide with the sentencing of an individual in the United States for selling a U.S. company's sensitive and protected cyber-exploit components to Operation Zero.

Analyst note:

- Operation Zero's accounts on X and Telegram are likely to be removed by the platforms following the sanctions, though they remain active at the time of writing.
- The removal of social media accounts is very likely to disrupt some aspects of Operation Zero's business activities in the near term.
- Rebranding social media accounts is likely to increase the risk of impersonation by creating confusion around Operation Zero's account identity, pushing the firm to occupy dark web platforms more frequently.

© 2026 ZeroFox, Inc. All rights reserved.

- Furthermore, since Operation Zero relies on cryptocurrency to finance its activities, the sanctions are unlikely to effectively disrupt its revenue stream—particularly on those crypto platforms operating outside of U.S. jurisdiction.

Anthropic Catches Chinese Companies Copying Claude's Capabilities

What we know:

- Anthropic has accused China-linked companies DeepSeek, Moonshot AI, and MiniMax of using 24,000 fake accounts and 16 million queries to extract from its AI chatbot Claude's capabilities, through large-scale illicit distillation methods.

Background:

- Distillation is an AI-training method whereby a smaller model learns to replicate the outputs of a larger, more advanced model.
- Anthropic has alleged that DeepSeek, Moonshot AI, and MiniMax used proxy-routed fake accounts to extract Claude's advanced AI capabilities at low cost, potentially bypassing U.S. export controls and flouting safety guardrails tied to national security.

Analyst note:

- China-linked AI companies and their stolen models from Anthropic are unlikely to have robust security measures. Chinese duplicate models are likely to give threat actors a gateway to misuse Anthropic's capabilities.
- Improper security controls in distilled models are also likely to expose user IP addresses, making them susceptible to follow-on attacks such as network breaches.

© 2026 ZeroFox, Inc. All rights reserved.

Russia-Linked Actor Breaches Over 600 Fortinet Firewalls Without Zero-Days

What we know:

- A Russia-linked threat actor has reportedly breached over 600 Fortinet FortiGate firewalls across 55 countries in five weeks by brute-forcing exposed management interfaces without MFA, and not using zero-days.
- The actor is assessed to have low to moderate skillsets and was observed attempting multiple CVE exploits, but abandoned hardened systems in favor of easier targets.

Background:

- After gaining access, the attacker stole configuration files, VPN credentials, admin passwords, and network maps.
- The threat actor then used AI-assisted tools to automate reconnaissance and lateral movement.

Analyst note:

- This incident suggests that organizations failing to rotate credentials and enforce MFA will increasingly become prime targets for opportunistic, AI-enabled threat actors.
- Rather than investing in vulnerability exploitation, such actors are likely to prioritize environments where weak authentication enables scalable, automated access with minimal resistance.

© 2026 ZeroFox, Inc. All rights reserved.

Exploit and Vulnerability Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

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 five vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on February 20, February 24, and February 25. On February 24, CISA also released three Industrial Control System (ICS) advisories, including CVE-2025-29628, CVE-2026-1227, CVE-2026-21410, and other vulnerabilities. CVE-2026-27488 is a server-side request forgery (SSRF) vulnerability in OpenClaw's cron webhook handler that enables webhook targets to access internal or metadata endpoints due to missing policy checks. Zyxel has addressed CVE-2025-13942, a command injection vulnerability in the UPnP function of certain Zyxel products that could enable a remote attacker to execute operating system (OS) commands on an affected device by sending specially crafted UPnP SOAP requests.

CRITICAL

CVE-2026-20127

What happened: Cisco has disclosed that an authentication bypass vulnerability in Cisco Catalyst SD-WAN has been actively exploited as a zero-day since at least 2023. The flaw enables remote attackers to log into SD-WAN controllers and add malicious rogue peers to targeted networks.

- **What this means:** The fact that this has been a long-term, until-now undetected likely indicates that the threat actor exploiting this vulnerability is focused on surveillance and data exfiltration for espionage, rather than causing operational disruption for immediate financial gain.
  - **Affected products** are listed in Cisco's advisory.

© 2026 ZeroFox, Inc. All rights reserved.

CRITICAL

CVE-2026-22719

What happened: Broadcom has released patches for multiple vulnerabilities impacting VMware Aria Operations, including a high-severity command injection vulnerability tracked as CVE-2026-22719.

- **What this means:** The other vulnerabilities enable cross-site scripting (XSS) and privilege escalation. Successful exploitation of the vulnerabilities, individually or in a chain, is likely to aid threat actors in compromising cloud environments.
  - **Affected products** are listed in this advisory.

© 2026 ZeroFox, Inc. All rights reserved.

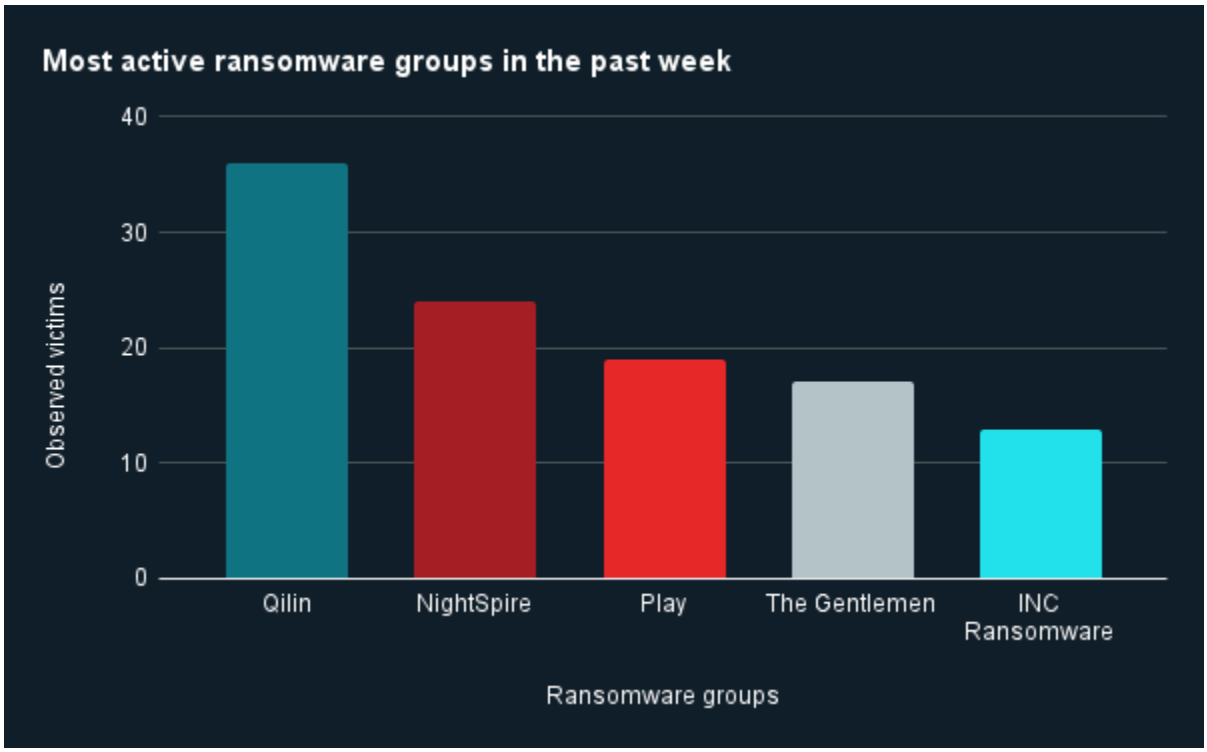
Ransomware and Breach Intelligence

© 2026 ZeroFox, Inc. All rights reserved.

Ransomware and Breach Intelligence Key Findings

Ransomware Groups, Activities, and Trends

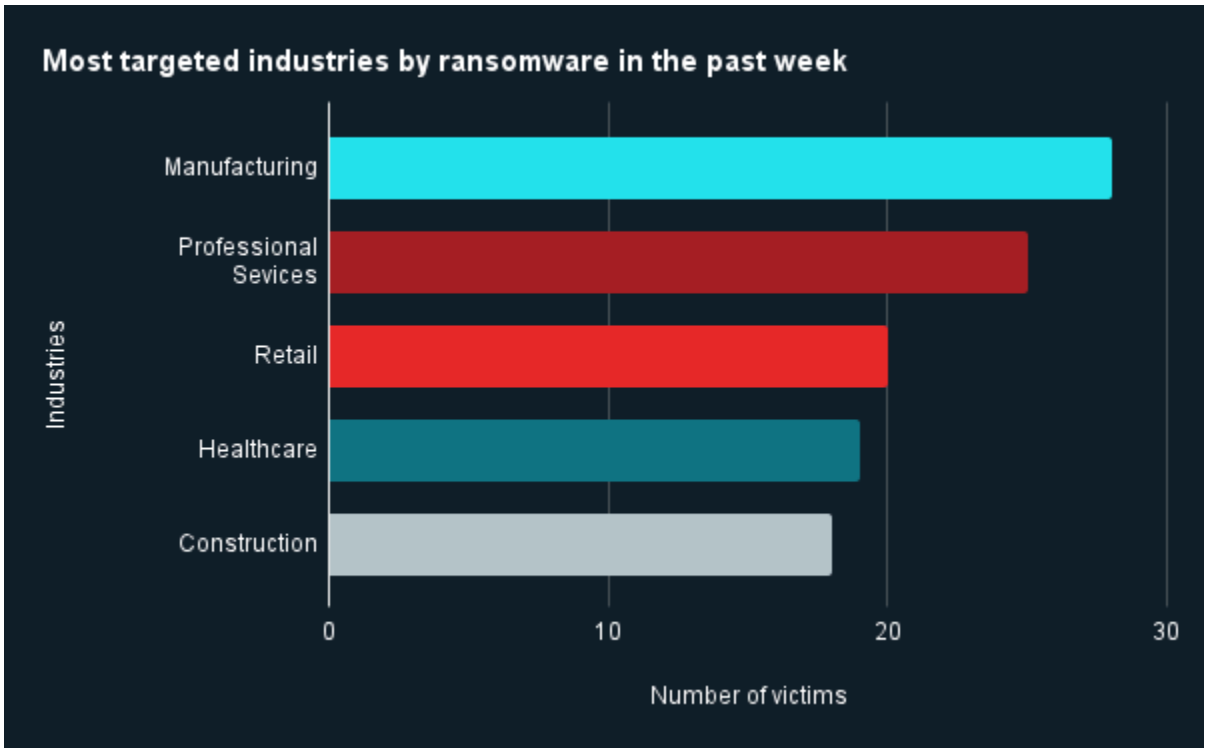
Last week in ransomware: In the past week, Qilin, NightSpire, Play, The Gentlemen, and INC Ransomware were the most active ransomware groups. ZeroFox observed close to 162 ransomware victims disclosed on the deep and dark web, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by NightSpire.



Source: ZeroFox Internal Collections

© 2026 ZeroFox, Inc. All rights reserved.

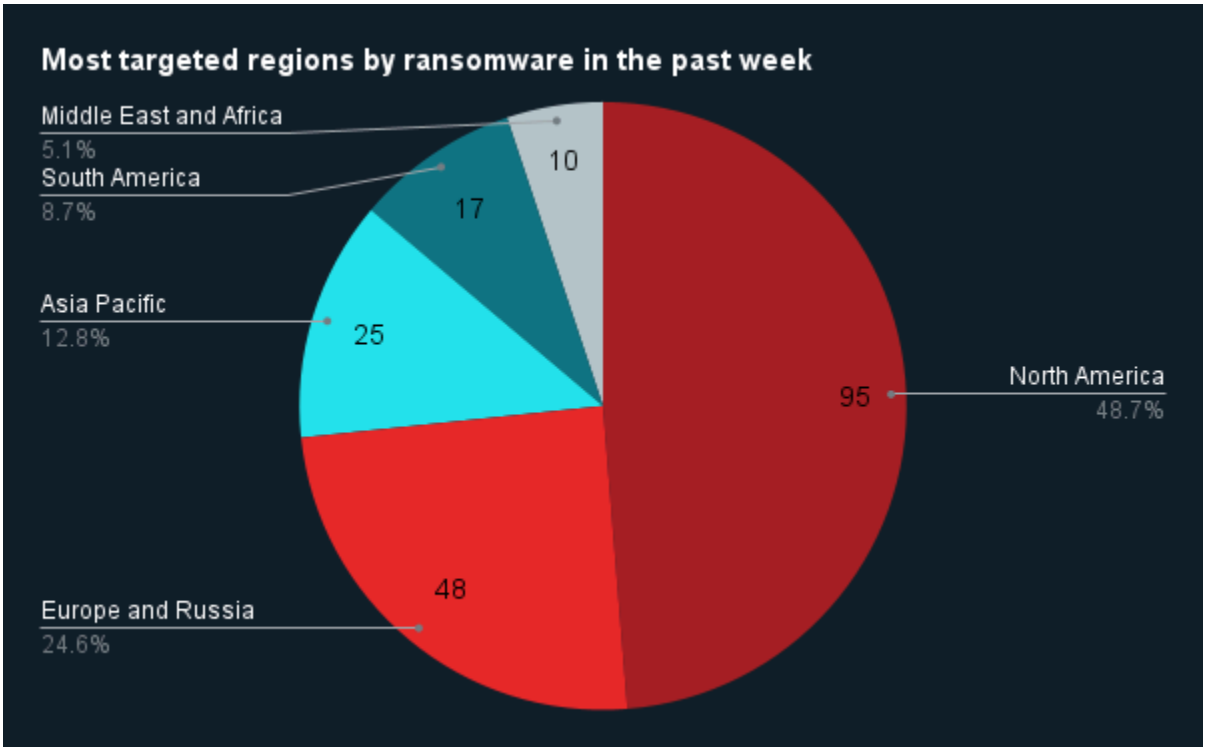
Industry ransomware trend: In the past week, manufacturing was the industry most targeted by ransomware attacks, followed by professional services, retail, healthcare, and construction.



Source: ZeroFox Internal Collections

© 2026 ZeroFox, Inc. All rights reserved.

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 95 attacks, Europe and Russia recorded 48, Asia Pacific noted 25, South America saw 17, and Middle East and Africa recorded 10.



Source: ZeroFox Internal Collections

© 2026 ZeroFox, Inc. All rights reserved.

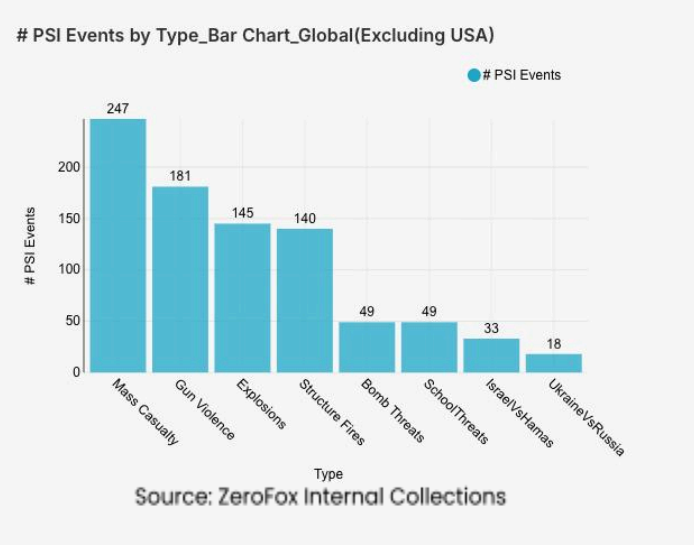
Notable Data Breaches Affecting Different Industries

Targeted Entity	PayPal	CarGurus	Ttareungyi
Compromised Entities/Victims	100 PayPal Working Capital (PPWC) customers	12 million CarGurus users' records	Over four million Ttareungyi (Seoul's public bike service) users
Compromised Data Fields	Full names, email addresses, phone numbers, business addresses, Social Security numbers (SSNs), dates of birth, and associated account information	Email addresses, IP addresses, full names, phone numbers, physical addresses, user account IDs, finance pre-qualification application data, finance application outcomes, dealer account details, and subscription information	User IDs, phone numbers, home addresses, email addresses, dates of birth, and gender
Suspected Threat Actor	N/A	ShinyHunters	Two South Korean individuals
Country/Region	United States	United States	South Korea
Industry	Finance	Automotive marketplace	Transportation
Possible Repercussions	Identity theft, financial fraud, phishing and social engineering campaigns, and further sale in dark web marketplaces	Financial fraud, credential-stuffing attacks, identity fraud, and social engineering attacks	Identity theft, phishing campaigns, doxxing, physical threats, blackmail, and extortion

Three major breaches observed in the past week

© 2026 ZeroFox, Inc. All rights reserved.

Physical and Geopolitical Intelligence Key Findings



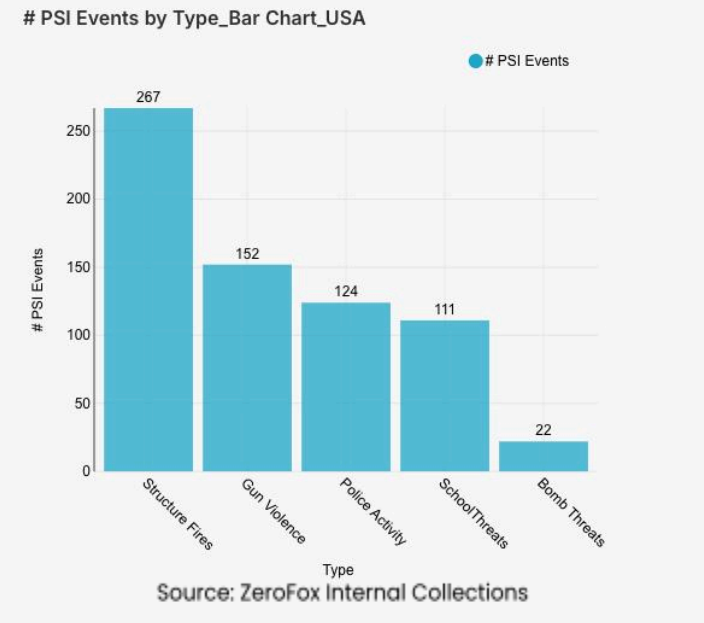
Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 12 percent increase in mass casualty events this week from the previous one, with the top contributing countries being India, Mexico, and Pakistan, in that order. Approximately 59 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 raids and attacks) decreased by 38 percent from the previous week, and events related to Russia's war in Ukraine increased by 38 percent. The top three most-alerted subtypes were gun violence, which saw a 3 percent increase from the previous week; explosions, which increased by 12 percent; and structure fires, which increased by 21 percent. Notably, bomb threats increased by 44 percent, and threats targeting schools increased by 63 percent compared to the previous week.

- **What this means:** This week's trends in global security highlight a volatile landscape, with violence concentrated in a few key areas. General alerts for the Israel-Hamas conflict have seen a decrease, possibly due to the progression of "Stage 2" of the U.S.-brokered peace framework and the establishment of a transitional Board of Peace. This stability is countered by a sharp rise in events related to Russia's war in Ukraine, as both sides intensify attacks; on February 26 Russia launched 420 drones and 39 missiles targeting Ukraine's energy sector and other critical infrastructure. Meanwhile, India has faced a localized surge in threats; a wave of bomb threats targeted schools in Delhi on February 23, causing mass evacuations during board examinations. This occurred just a few days after another group of Delhi school bomb threats on February 19. Although these specific school threats were later declared hoaxes, they contribute to the significant global spike in threats targeting educational institutions this week. Overall, a decline in some conventional conflicts this week was countered by a sharp rise in asymmetric threats, infrastructure-targeted violence, and educational and civilian vulnerabilities.

© 2026 ZeroFox, Inc. All rights reserved.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted U.S. 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 this week were Texas and Ohio, which together made up 18 percent of the nationwide total. Gun violence across the United States overall decreased by 6 percent from the week prior. Police activity alerts increased by 59 percent, and the top contributing states were New York and California. Structure fires increased by 11 percent, and the top two states for this subtype were California and New York. Notably, threats related to schools increased by 46 percent compared to the previous week, and bomb threats increased by 57 percent.

- **What this means:** Domestic security trends in the United States this week have been defined by a complex interplay of violent crime, targeted threats, and persistent infrastructure risks. Structure fires saw an increase this week, as Winter Storm Hernando brought blizzard conditions to much of the country, increasing the usage of heating devices and thus resulting in fire hazards. Additionally, there was a surge in school-related threats, exemplified by a wave of phoned-in bomb threats that affected high schools in Coppell and Anna, Texas, on February 18 and 25. As law enforcement presence is positively correlated with threats against educational institutions, there was a rise in overall police activity as well. However, federal officials report a significant drawdown in Minnesota, where fewer than 1,000 immigration agents remain following the peak of Operation Metro Surge. While shootings overall decreased somewhat, there were still six mass shootings that occurred in the last seven days, including one in Richmond, Virginia, on February 21 that resulted in 11 victims. Overall, the current state of domestic physical security is characterized by a surge in "soft target" threats and infrastructural emergencies.

© 2026 ZeroFox, Inc. All rights reserved.

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.

© 2026 ZeroFox, Inc. All rights reserved.

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%

© 2026 ZeroFox, Inc. All rights reserved.