ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

December 6, 2025

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 December 4, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

Monthly Geopolitical Assessment: December 2025

Little progress has been made in advancing the ceasefire between Israel and Hamas—increasing the risk of the ceasefire ultimately collapsing—while violence has escalated in Lebanon. Both trends are likely to continue in 2026. None of the major ceasefire proposals to end Russia's war in Ukraine are likely to be accepted in the short term. However, a negotiated settlement partitioning Ukraine is likely. Taiwan, and related tensions between China and Japan over the island, have emerged as the biggest risk to the U.S.-China trade agreement. Military strikes and covert operations inside Venezuela against alleged government-sponsored drug trafficking targets remain likely in 2025. Given the government's supposed role in drug trafficking, there is a roughly even chance the operations will be perceived as aiming to topple the Venezuelan government. Political dialogue aimed at decoupling the government from wider security threats against the United States is less likely.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 24

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

ZeroFox Intelligence Flash Report - Proposed U.S. Legislation to Sanction Threat Actors

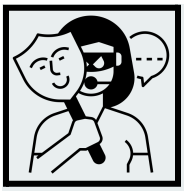
On December 2, 2025, U.S. Congressman August Pfluger proposed a bill that would formally designate foreign parties who conduct attacks against U.S. organizations as "critical" cyber threat actors. In November 2025, National Cyber Director Sean Cairncross stated the Trump administration was seeking to establish a unique, coordinated cyber strategy. In July 2025, President Trump reportedly approved USD 1 billion in funding for an offensive hacking operation run by the Pentagon, likely signalling his administration's focus on counter-cyber tactics and strategy. Given the current emphasis in Washington on taking a proactive approach to combatting cyber threats, it is very likely that the bill will pass—though it may go through minor revisions and amendments in the legislative process.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



U.S. Justice Department Hits Burmese Tai Chang Network with Domain Seizure

What we know:

- The U.S. Department of Justice (DOJ) seized the tickmilleas[.]com domain, which was actively used to defraud Americans through cryptocurrency investment fraud (CIF) scams.
- Posing as "a legitimate investment platform," the site tricked victims into depositing funds while showing fabricated returns and fake deposits to simulate real investments.
- Within one month of registration, the Federal Bureau of Investigation (FBI) identified multiple victims who had already lost money.
- A splash page now alerts visitors that the domain has been seized, effectively disrupting the scammers' operations.

Background:

- Tai Chang is connected to the Burmese groups DKBA and Trans Asia, which were designated as specially-designated nationals (SDN) on November 12 for ties to Chinese organized crime and the development of scam centers in Southeast Asia.
- Tickmilleas[.]com directed users to download fraudulent apps from Google Play and Apple's App Store, which were removed after FBI notification.
- Meta voluntarily took down over 2,000 social media accounts linked to the scheme.
- Many scams begin with unsolicited contact on social media or dating platforms, where scammers cultivate trust with targets. Victims are then guided to purchase cryptocurrency and invest through fraudulent domains and apps.

What is next:

- In 2024, the Internet Crime Complaint Center (IC3) received more than 41,000 complaints reporting roughly USD 5.8 billion in losses from CIF scams, illustrating their sophistication and reach.
- The seizure of tickmilleas[.]com, as well as two other Tai Chang–linked scam domains, is part of the ongoing efforts of the U.S. Attorney for the District of Columbia (USADC)'s "Scam Center Strike Force" to dismantle sophisticated online fraud networks.

- In the next few months, the strike force will very likely take down more Southeast Asian scam centers. These actions are also likely to raise public awareness of such overseas scams.

Authorities Shut Down Cryptomixer, Seizing EUR 25 Million in Bitcoin

What we know:

- Law enforcement agencies have taken down illegal cryptocurrency mixing service Cryptomixer, which was suspected of facilitating cybercrime and money laundering.
- During the operation, authorities seized three servers, the cryptomixer[.]io domain, over 12 TB of data, and more than EUR 25 million (approximately USD 29 million) in Bitcoin.

Background:

- Cryptomixer, active since 2016, was a hybrid web service that enabled criminals to hide over EUR 1.3 billion in Bitcoin. It pooled and randomized deposits, making transactions hard to trace before converting the "cleaned" funds into other cryptocurrencies or fiat.

Analyst note:

- Threat actors who relied on Cryptomixer will likely seek alternative cryptocurrency mixing services, moving to smaller, lesser known platforms to evade law enforcement scrutiny.

North Korean Threat Actors Load Npm Packages With Malware

What we know:

- North Korean threat actors behind the Contagious Interview campaign have reportedly added nearly 200 new malicious npm packages, which have been downloaded over 31,000 times, to deliver an updated OtterCookie malware variant.

Background:

- The malware is designed to steal browser credentials, documents, cryptocurrency wallet information, capture screenshots, read clipboard content, and log keystrokes.

- The malware strain attempts to evade sandboxes and virtual machines upon execution and then establishes a command-and-control (C2) channel for the threat actors.

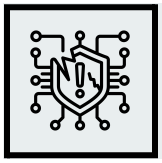
Analyst note:

- Open-source npm packages should be approached with caution as threat actors increasingly target popular packages for infections.
- Installing or executing infected npm packages is likely to compromise both the victim's system and those of downstream users and organizations.

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 three vulnerabilities to its Known Exploited Vulnerability (KEV) catalog on December 2 and December 3, 2025. CISA also released 14 Industrial Control Systems (ICS) advisories on December 2 and December 4. Google addressed 107 vulnerabilities in the December 2025 security update for Android devices, including two actively exploited zero-days (CVE-2025-48633 and CVE-2025-48572). The now-patched zero-days enabled threat actors to escalate privileges and access sensitive information. A cross-site scripting (XSS) flaw affecting specific versions of OpenPLC ScadaBR enables attackers to inject and execute malicious scripts via a file path; threat group TwoNet is reportedly actively exploiting this vulnerability. Mirion Medical has fixed five high-severity vulnerabilities in its EC2 Software NMIS BioDose software that could enable attackers to gain unauthorized access to the application, modify program executables, access sensitive information, and potentially remotely execute code. Three vulnerabilities in open-source utility Picklescan can enable threat actors to execute arbitrary code by loading untrusted PyTorch models, bypassing the tool's protections.



CRITICAL

CVE-2025-55182 and CVE-2025-66478

What happened: CVE-2025-55182, which originates in the upstream React implementation, has a downstream impact on Next[.]js applications using the App Router, creating the vulnerability tracked as CVE-2025-66478. The vulnerability in React library enables threat actors to execute code remotely in cloud environments via unsafe deserialization.

- **What this means:** This flaw is likely to enable remote attackers to compromise a large number of victim servers, potentially leading to full system control in affected devices.
- **Affected products:**
  - CVE-2025-55182: React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0
  - CVE-2025-66478: Next.js versions 15.x, 16.x, 14.3.0-canary.77 and later canary releases

CRITICAL

CVE-2025-13658

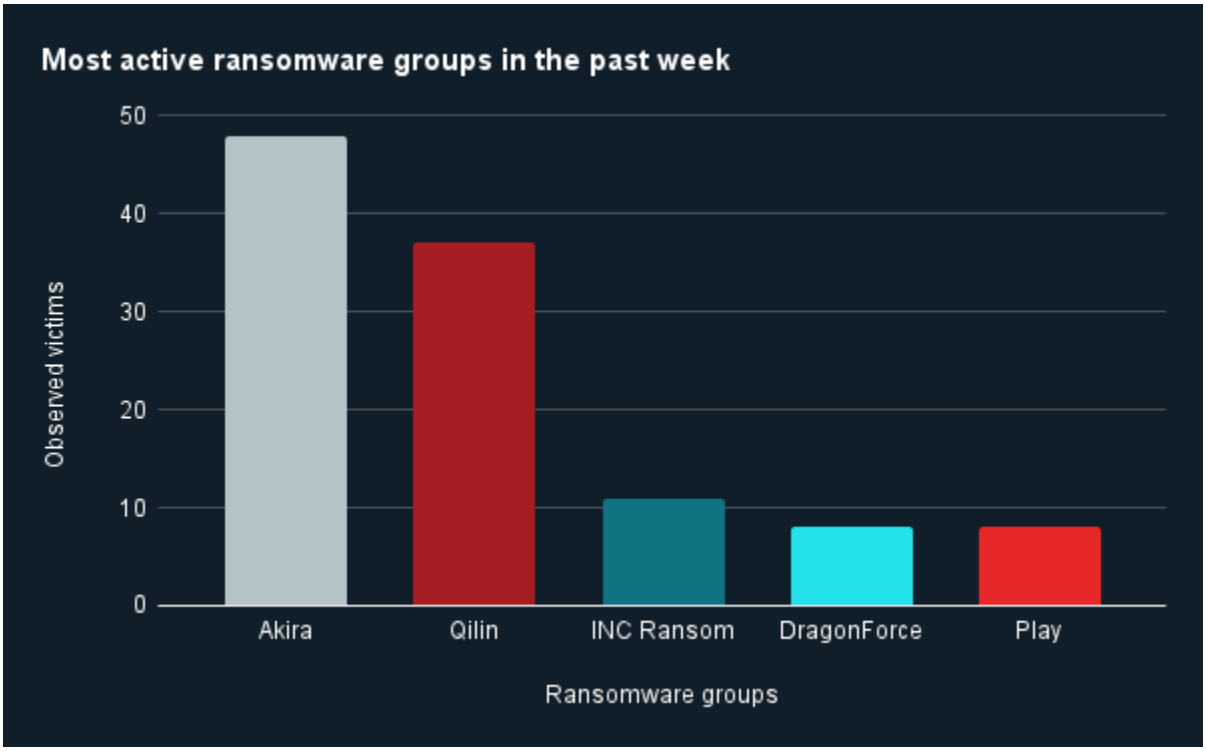
What happened: This vulnerability in Longwatch devices allows unauthenticated HTTP GET requests to execute arbitrary code via an exposed endpoint due to the absence of code signing and execution controls. Exploitation results in SYSTEM-level privileges, which could grant complete control over a device or network.

- **What this means:** Threat actors are likely to exploit this bug to disable security measures, steal data, maintain stealthy access, and escalate the attack across systems.
- **Affected products:**
  - Longwatch versions 6.309 to 6.334

Ransomware and Breach Intelligence

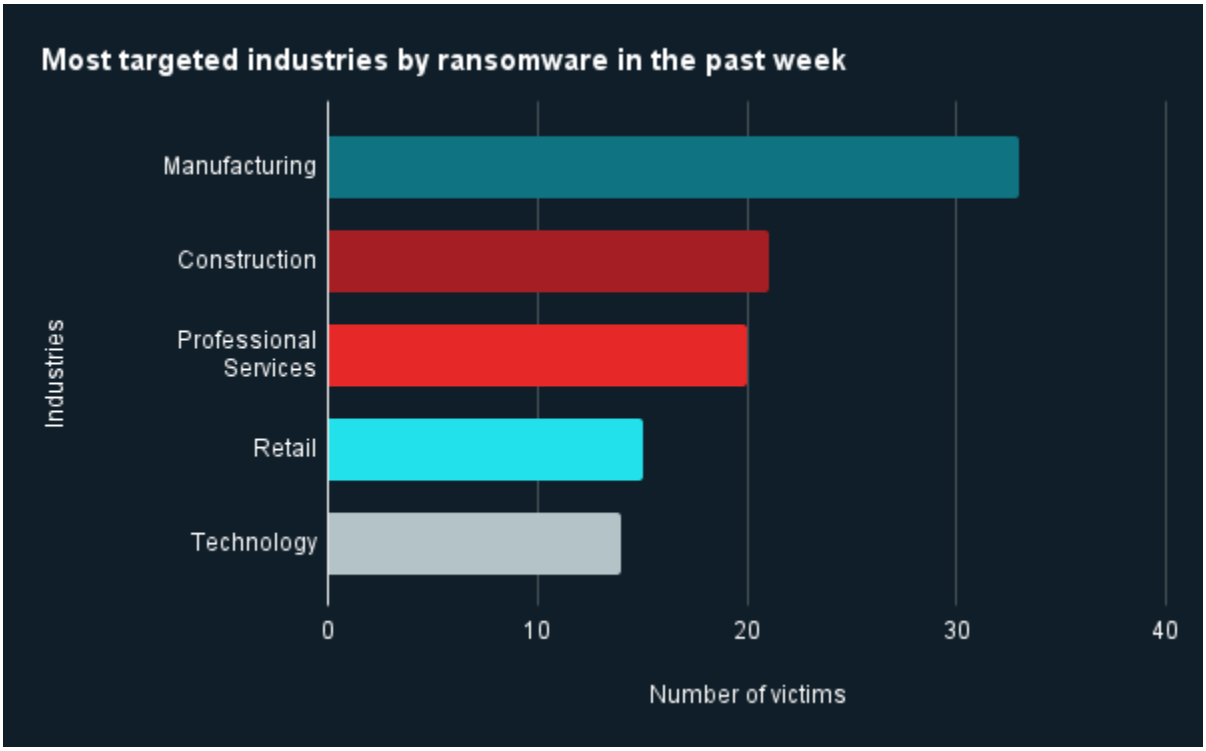
Ransomware and Breach Intelligence Key Findings

Ransomware Trends Across Industries and Regions



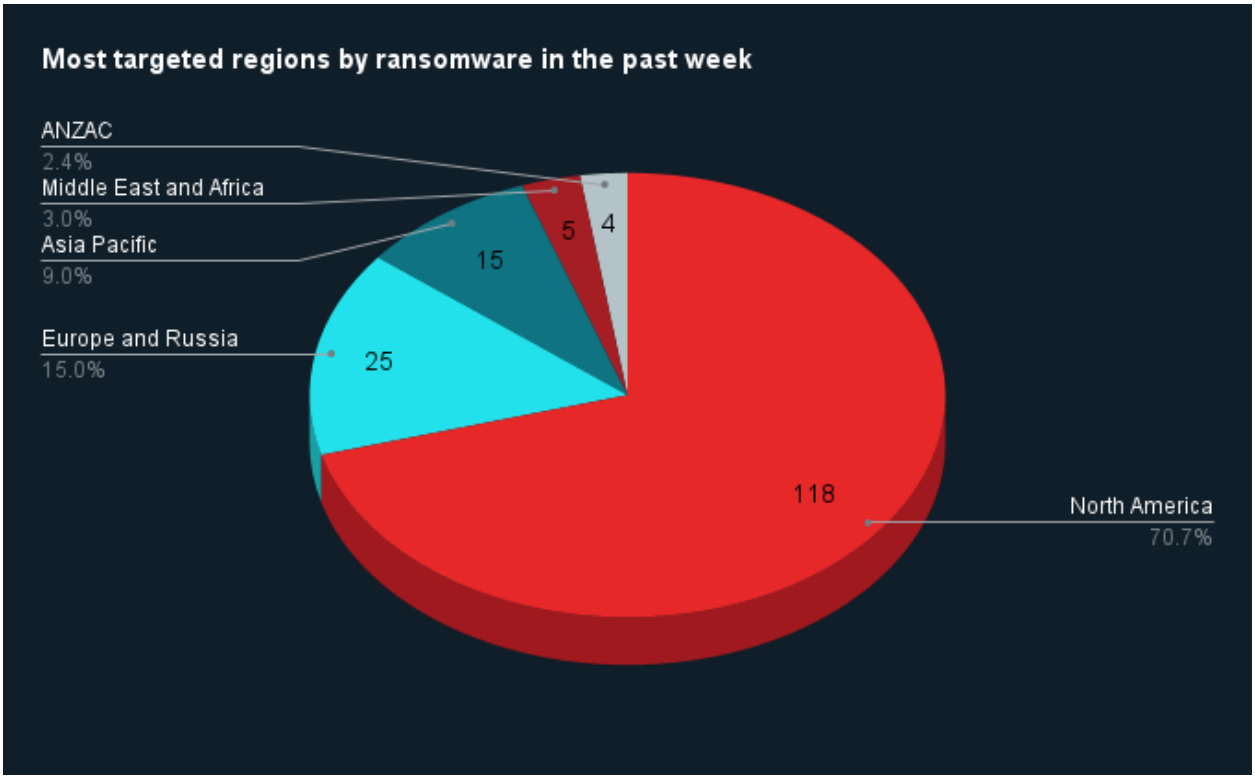
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Akira, Qilin, INC Ransom, DragonForce, and Play were the most active ransomware groups. ZeroFox observed close to 153 ransomware victims disclosed, most of whom were located in North America. The Akira ransomware group accounted for the largest number of attacks, followed by Qilin.



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 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 and Asia-Pacific (APAC) regions. There were at least 118 ransomware attacks observed in North America, while Europe and Russia accounted for 25, APAC for 15, Middle East and Africa for five, and Australia and New Zealand (ANZAC) for four.

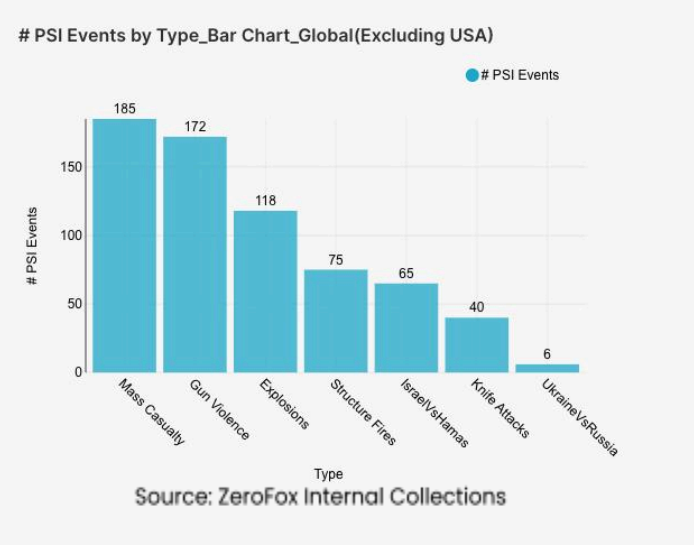
Data Breaches Compromising Personal Information

Targeted Entity	Coupang	Freedom Mobile	Illuminate Education
Compromised Entities/victims	33.7 million customers' data	N/A	10.1 million students
Compromised Data Fields	Names, email addresses, phone numbers, shipping addresses, and partial order history	First and last names, home addresses, dates of birth, phone numbers, and Freedom Mobile account numbers	Email addresses, mailing addresses, dates of birth, student records, health-related information, and other personally identifiable information
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	South Korea	Canada	United States
Industry	Retail	Telecommunications	Education
Possible Repercussions	Phishing and other social engineering attacks, as well as identity and financial fraud	Phishing, vishing, SIM swap attempts, identity theft, and account takeover, as well as potential for future exploitation if stolen data circulates or resurfaces online	Identity fraud, targeted phishing, physical stalking of students, and credential stuffing attacks

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

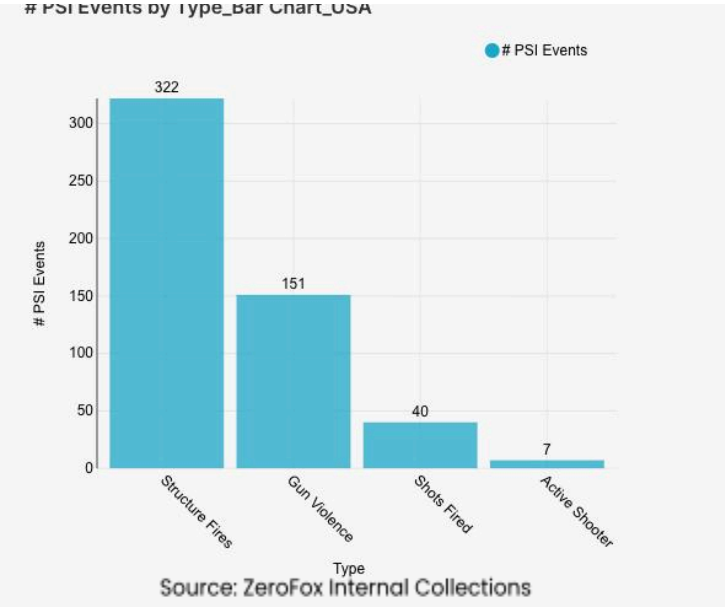


Physical Security Intelligence: Global

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 or territories being Pakistan, India, and the Palestinian Territories, in that order. Approximately 64 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 36 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 29 percent from the previous week. Events related to Russia's war in Ukraine decreased by 33 percent. The top three most-alerted subtypes were explosions, which saw a 6 percent decrease from the previous week; gun violence, which increased by 74 percent; and structure fires, which decreased by 9 percent. Notably, knife attacks increased by 38 percent from the week prior.

- **What this means:** While the global frequency of mass casualty events is slightly receding, the nature of threats is becoming more volatile, shifting away from large-scale conflict alerts and toward direct attacks. The data specifically reveals an increase in gun violence and knife attacks. The surge in gun violence is exemplified by a mass shooting in a gang-related turf war at the La Resaka bar in Tula, central Mexico, on November 30, which left seven patrons dead and critically injured five more. The jump in knife attacks was reflected by two Israeli soldiers being injured in a stabbing attack near Ramallah, with the Palestinian suspect killed at the scene on December 2. Although alerts related to the Israel-Hamas conflict and Russia's war in Ukraine decreased overall, incidents confirm ongoing hostilities; for instance, an Israeli military strike in the Gaza Strip reported on December 4 killed multiple Palestinians, and a deadly Russian missile strike in Ukraine on December 1 killed four and wounded dozens. Despite a slight drop in major conflict alerts, global physical security is becoming more volatile due to a significant rise in immediate, direct violence.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and shots fired. Structure fires are fires that affect man-made buildings, gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, and shots fired alerts involve shootings with no confirmed victims. The top two states with the most gun violence alerts were Pennsylvania and New York, which together made up 19 percent of this week's nationwide total. Gun violence across the United States overall decreased by 33 percent from the week prior. Shots fired alerts decreased by 5 percent, and the top contributing states were New York and Tennessee. Structure fires increased by 49 percent, and the top two states for this subtype were New York and California. Notably, active shooter alerts more than tripled in numbers compared to the week prior.

- **What this means:** U.S. domestic security incidents this week reveal a sharp increase in man-made disasters and an escalation of incidents with a high number of casualties. While general gun violence alerts decreased overall, active shooter alerts more than tripled. This heightened risk was exemplified by a seemingly targeted mass shooting at a toddler's birthday party on November 30 in Stockton, California, which left four people (including three children) dead and 11 others wounded. In New York, the surge in structure fires—this week's top subtype overall—included a major incident on December 1, when a resident and a firefighter were injured as a five-alarm fire spread to four homes in Queens. In San Francisco, California, fire crews responded to a house fire in the Excelsior District on December 3 that resulted in one fatality. This rise in fire alerts is often seasonal, as the incidence and severity of fires increase during the winter holiday season due to factors such as heating, decorations, and candles. The overall state of U.S. physical security is characterized by persistent domestic violence risks and a sudden escalation in man-made disasters despite some decreases in less severe crime alerts.

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%