Weekly Intelligence Brief

Classification: TLP:GREEN

January 24, 2026

ZEROFOX®
Weekly Intelligence Brief

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 22, 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 Scorecard - Q4 2025 North American Retail Overview

In this scorecard, ZeroFox provides an overview of the Q4 2025 North American retail industry threat landscape.

ZeroFox Intelligence Flash Report - U.S. Directive to Withdraw from Global Cybersecurity Organizations

On January 7, 2026, U.S. President Donald Trump signed a Presidential Memorandum directing the withdrawal of the United States from 66 international organizations, including several global cybersecurity entities. This memorandum aligns with the Trump administration’s broader and ongoing review of U.S. participation in all international intergovernmental organizations, conventions, and treaties. There is a roughly even chance that reduced U.S. participation in international cybersecurity and digital policy efforts will affect information-sharing, coordination on standards, and the alignment of U.S. law and policy with evolving multinational cybersecurity frameworks.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

New PDFSider Malware Leveraged Against Fortune 100 Company

What we know:

- A new malware strain called PDFSider is reportedly actively being used by various ransomware groups, including Qilin, to compromise corporate networks.
- Researchers have labeled it an Advanced Persistent Threat.
- The malware has been observed in attacks against large corporations, including a Fortune 100 financial firm.
- Researchers discovered that the malware is designed to create a backdoor, enabling covert control of the infected systems.

Background:

- PDFSider is primarily delivered via spear phishing emails containing ZIP archives or using social engineering on platforms such as Microsoft Teams and Quick Assist, where attackers pose as technical support.
- The archives contain a legitimate vulnerable file with hidden malware.
- PDFSider primarily operates in memory to evade detection by traditional security solutions.
- The malware also enables the threat actor to interact using hidden shells for executing remote commands on the infected system. Upon activation, PDFSider gathers host details and creates a unique identifier for the victim to track them throughout the campaign.

Analyst note:

- Threat actors are likely to scale up the PDFSider campaign by leveraging artificial intelligence (AI)-automated phishing content and deepfake IT support lures for long-term espionage and data theft.
- They are also very likely to trick victims into opening the ZIP files containing PDFSider using specific decoy documents, such as fake internal documents from government or intelligence organizations.

UK Cyber Agency Warns of Ongoing Attacks by Pro-Russian Hackivist Groups

What we know:

- The United Kingdom's cyber agency National Cyber Security Centre has issued a warning to organizations and critical infrastructure operators regarding ongoing disruption attempts by pro-Russian hacktivist groups.
- A previous alert linked to the warning also specifically mentions hacktivist group NoName057(16).
- ZeroFox also published its assessment of the warning here.

Background:

- The alert warns that, although denial-of-service (DoS) attacks are not technically advanced, they can still disrupt entire systems and essential online services if successful.
- These attacks also drain time and money as organizations work to analyze, defend against, and recover from them.

Analyst note:

- Hacktivist groups are very likely to increase their frequency of attacks during key events pertaining to the Ukraine-Russia war, such as negotiations or defense deals.
- Additionally, hacktivist groups are also likely to make exaggerated and false claims of attacks as part of psychological operations to sow chaos.

North Korean Threat Actors Deploying Malware via Malicious VS Code Projects

What we know:

- North Korean threat actors are reportedly using malicious Visual Studio (VS) Code projects as part of fake job assessments to deliver a backdoor with remote code execution (RCE) capabilities on the target system.

Background:

- Victims are instructed to duplicate repositories on GitHub, GitLab, or Bitbucket and launch them in VS Code.
- Subsequently, threat actors abuse VS Code task configuration files to deploy BeaverTail and InvisibleFerret malware strains.

- This latest tactic is part of a long-operating campaign called Contagious Interview, which weaponizes the job application process.

Analyst note:

- Software engineers working in fintech sectors are being increasingly targeted by North Korean threat actors, which is likely to give them access to financial assets, proprietary source code, and internal systems of fintech firms.
- Compromised systems are very likely to result in financial and intellectual property theft.

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 five vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on January 21, 2026 and January 22. It also released 11 Industrial Control System (ICS) advisories on January 20 and January 22, including ICSA-26-020-01, ICSA-26-020-03, and ICSA-26-020-02. Cloudflare fixed a flaw in its ACME HTTP-01 validation logic that could enable attackers to bypass security controls and reach customer origin servers. An improper implementation vulnerability in Google Fast Pair feature of bluetooth audio devices can enable attackers to force connections to attacker-controlled devices. Zoom has patched a critical vulnerability in its Node Multimedia Routers (MMRs) that can enable a meeting participant to carry out RCE attacks. GitLab has patched an authentication bypass vulnerability impacting its community and enterprise editions of the platform that enabled attackers to obtain the target's account ID to bypass two-factor authentication. Oracle has released 337 new security patches in its January 2026 advisory for over 30 products.

HIGH

CVE-2026-22219

What happened: This is a server-side request forgery (SSRF) issue, which, when exploited, can expose cloud credentials and enable lateral movement within cloud infrastructure.

- **What this means:** Threat actors are likely to target affected devices to steal sensitive user and proprietary data.
  - **Affected products:** Chainlit versions 0 to 2.9.4

HIGH

CVE-2026-0629

What happened: This is an authentication bypass flaw affecting more than 32 of TP-Link's VIGI surveillance camera models that can enable attackers to reset admin passwords and gain full control. The vulnerability has reportedly exposed thousands of internet-facing cameras and enabled access to live video feeds and device functions.

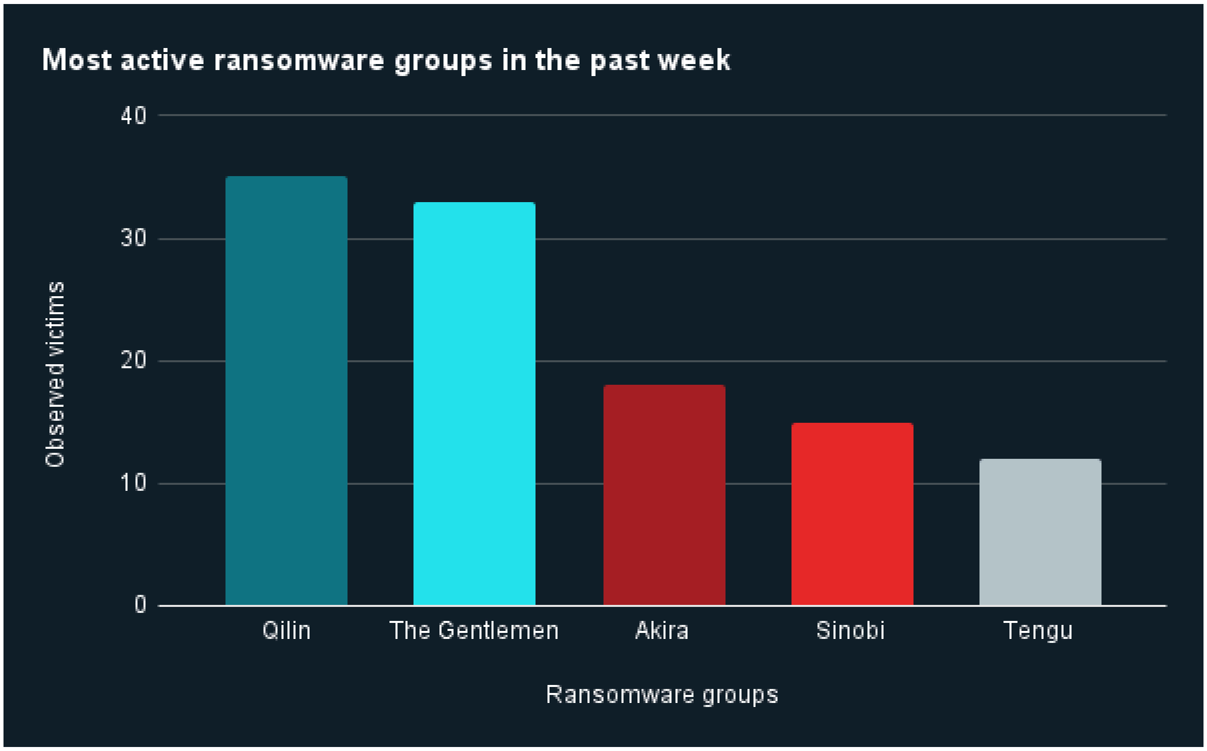
- **What this means:** Compromised VIGI surveillance cameras are likely to be enrolled in a botnet, gathering sensitive visuals and becoming a part of a network of unauthorized surveillance.
    - **Affected products:** The affected products are listed in this advisory.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

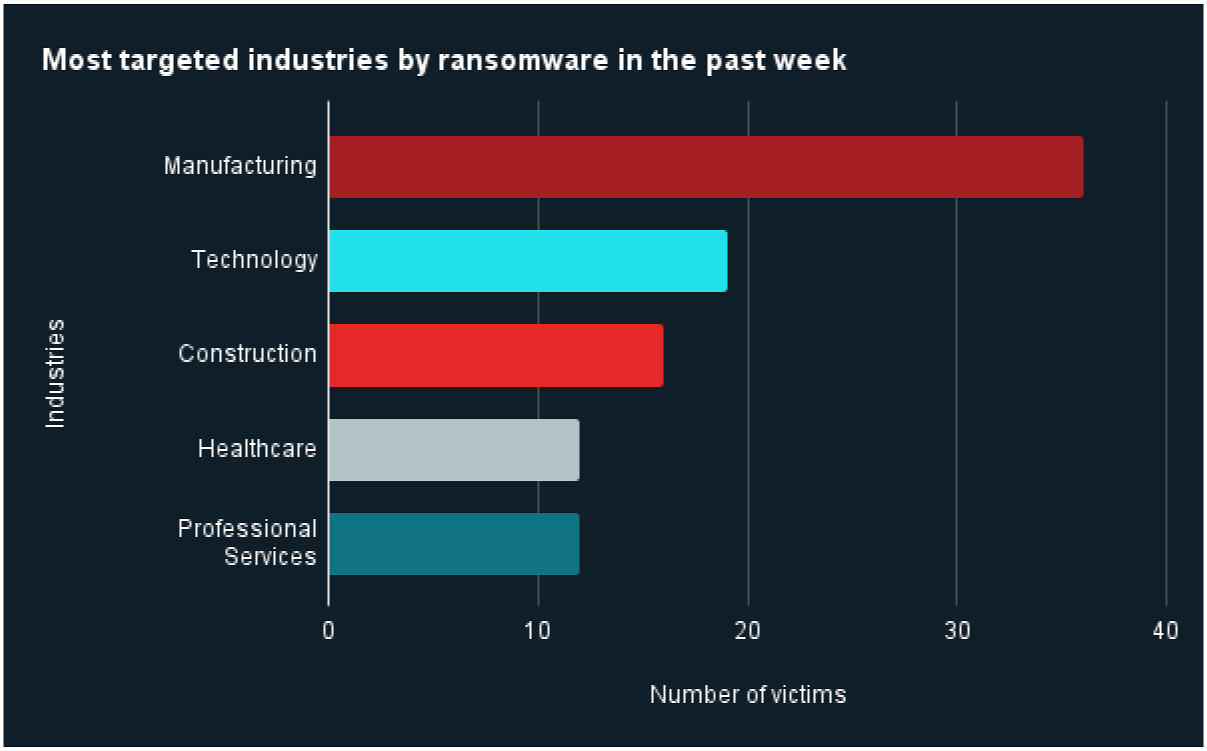
Ransomware Groups and Trends in Focus

Last week in ransomware: In the past week, Qilin, The Gentlemen, Akira, Sinobi, and Tengu were the most active ransomware groups. ZeroFox observed close to 149 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by The Gentlemen.



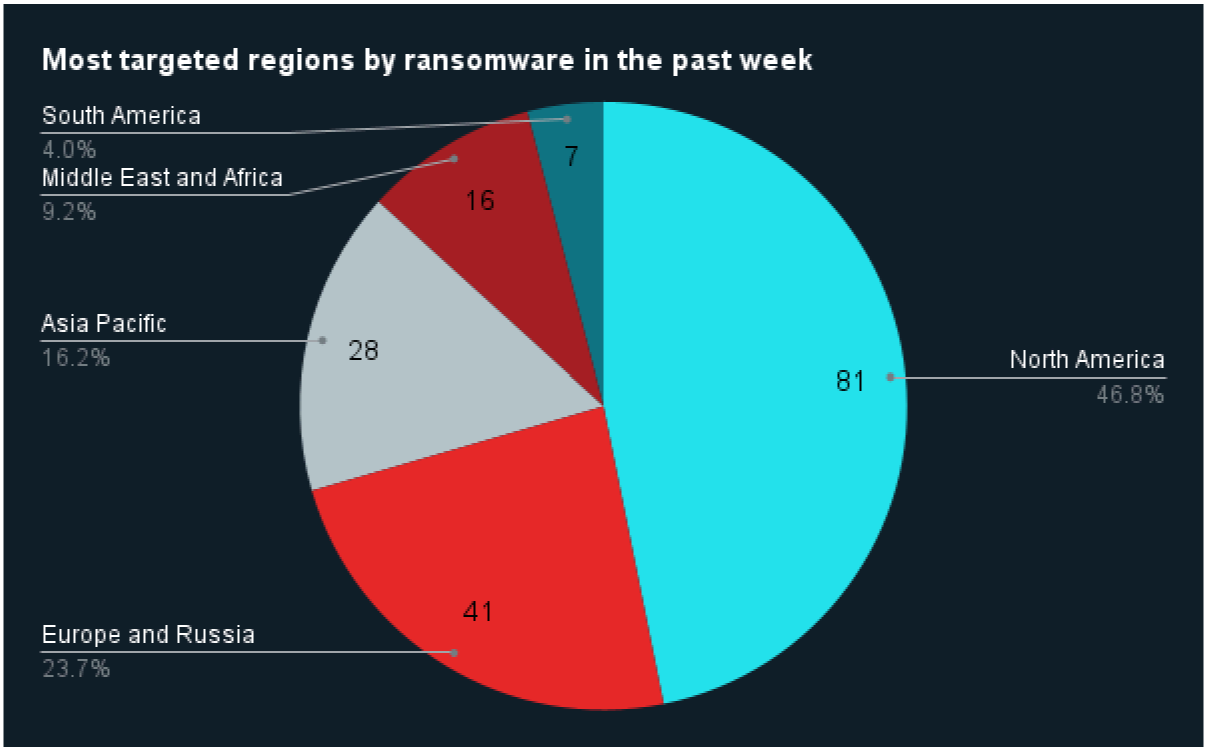
Source: ZeroFox Internal Collections

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



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 81 ransomware attacks observed in North America, while Europe and Russia accounted for 41, Asia-Pacific for 28, Middle East and Africa for 16, and South America for seven.



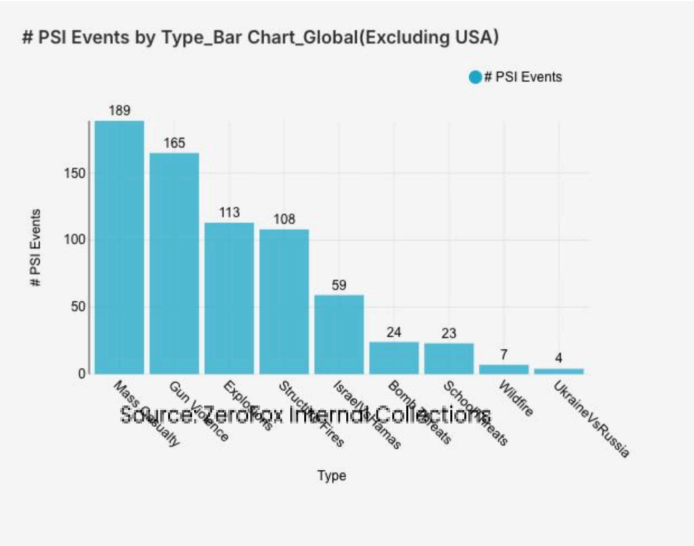
Source: ZeroFox Internal Collections

Data Breaches in Major Industries

Targeted Entity	Carlsberg Group	Canadian Investment Regulatory Organization (CIRO)	Minnesota Department of Human Services (DHS)
Compromised Entities/victims	Attendees of a Carlsberg-branded exhibition	Approximately 750,000 individuals, including member firms and registered employees (current and former clients of CIRO dealer members)	Individuals whose DHS-related billing or healthcare data was accessed (recipients of notification letters)
Compromised Data Fields	Full names, photos, and videos of individual event attendees	Annual income, dates of birth, government-issued ID numbers, phone numbers, investment account numbers, Social Insurance Numbers (SIN), and account statements	Unspecified data related to demographic records and in some cases, medical information and the last four digits of victims' Social Security numbers (SSNs)
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	Denmark, Europe	Canada	United States
Industry	Food and Beverage	Finance	Healthcare
Possible Repercussions	Profiling or doxxing using attendee information harvested from wristband IDs, misuse of images for impersonation, and social engineering	Identity theft and financial fraud, social engineering, account takeovers or investment-related scams, sale or trade of sensitive data on underground markets, exploitation of exposed information for long-term fraud, and impersonation campaigns	Misuse of compromised billing data for healthcare fraud, false claims, identity-related scams, financial abuse, improper charges, and fraud

Three major breaches observed in the past week

Physical and Geopolitical Intelligence Key Findings



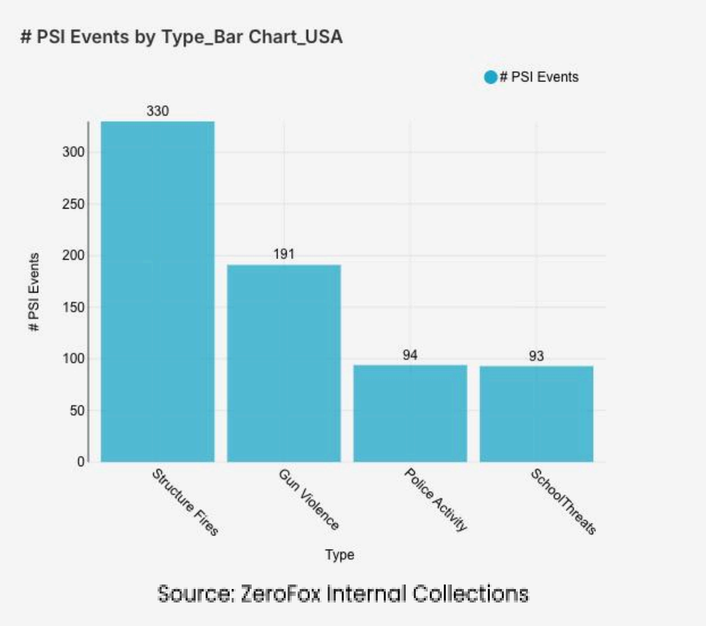
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 3 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Syria, Mexico, and India, in that order. Approximately 60 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 28 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 12 percent from the previous week. Events related to Russia's war in Ukraine decreased by 33 percent. The top three most-alerted subtypes were gun violence, which saw an 8 percent increase from the previous week; explosions, which increased by 3 percent; and structure fires, which increased by 16 percent. Notably, wildfire alerts increased by 600 percent.

- **What this means:** Despite only a slight increase in global mass casualty events this week, intense regional volatility remains prominent. In Syria, a military offensive by the transitional government against the Kurdish-led Syrian Democratic Forces (SDF) shattered a brief de-escalation; by January 22, over 100,000 civilians have been displaced following combat in Aleppo and subsequent clashes in the Raqqa and Deir ez-Zor regions. The most dramatic shift in this week's data is the increase in wildfire alerts, primarily driven by an environmental crisis in Chile. As of January 21, a "state of catastrophe" is in effect for the Biobío and Ñuble regions, where over 30,000 hectares have burned, and the death toll has reached at least 20. In Mexico, on January 21, the government extradited 37 "high-impact" cartel members to the United States in an effort to curb escalating territorial violence, such as shootings, which saw an increase in alerts this week. India has simultaneously faced a surge in threats, with Ambala becoming the latest focal point on January 19, when three schools were evacuated following anonymous bomb threat emails. Overall, the global security environment is increasingly characterized by conventional regional warfare, environmental crises, and targeted threats against public institutions.

Physical Security Intelligence: United States

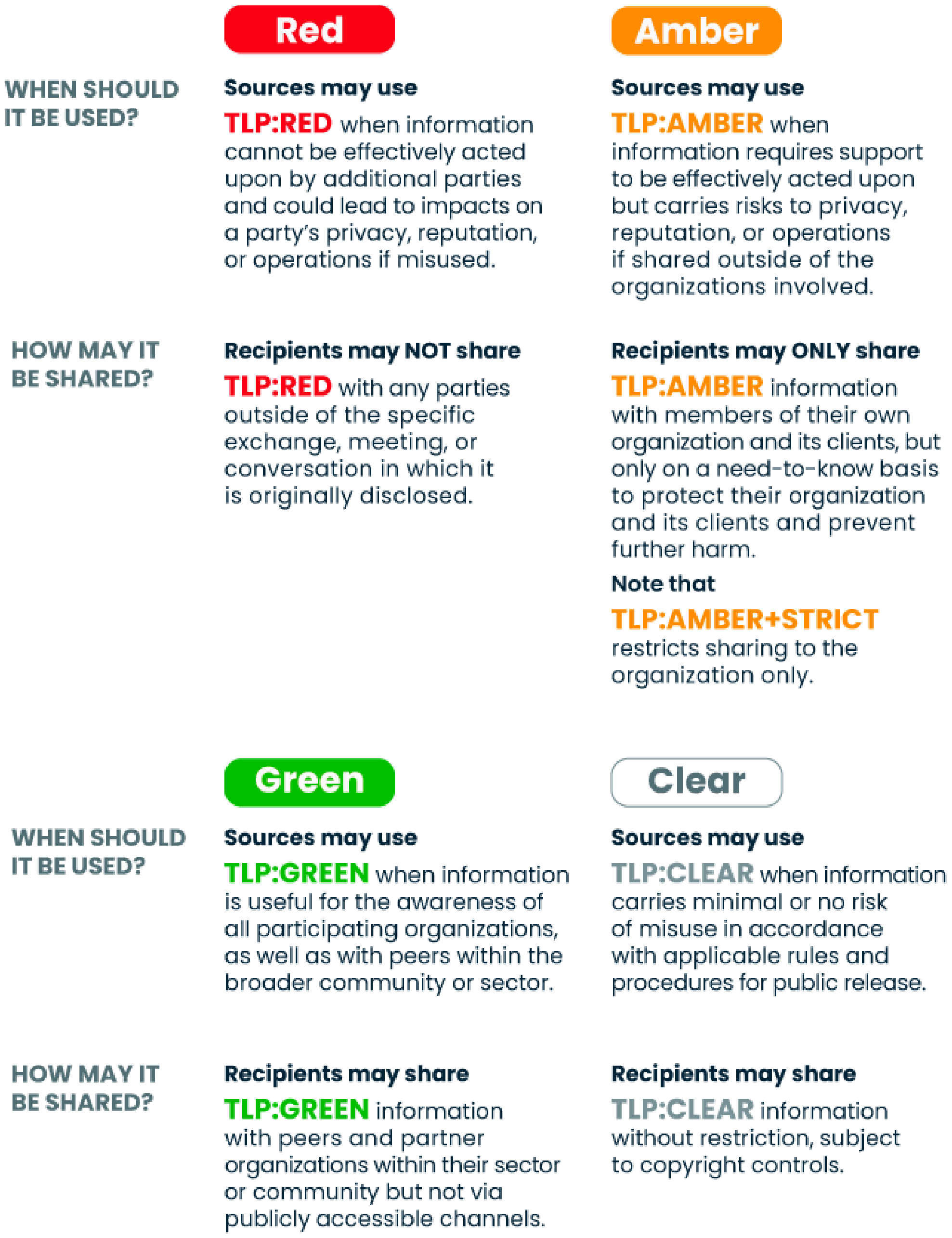


Source: ZeroFox Internal Collections

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 Georgia, which together made up 16 percent of this week's nationwide total. Gun violence across the United States overall increased by 4 percent from the week prior. Police activity alerts decreased by 4 percent, and the top contributing states were California and New York. Structure fires increased by 34 percent, and the top two states for this subtype were also California and New York.

- **What this means:** Data from the past week indicates a volatile landscape for domestic security in the United States in the past week. California and New York remain primary hubs for structural emergencies, which had the most notable increase in alerts; on January 21, the New York City Fire Department responded to a four-alarm warehouse fire in Brooklyn that caused extensive damage. While general police activity alerts decreased somewhat, law enforcement remains a priority, particularly concerning Immigration and Customs Enforcement (ICE) operations. In Minneapolis, federal officials held a press conference on January 20, confirming that "Operation Metro Surge" has resulted in 3,000 arrests over the last six weeks, though the operation continues to face a federal lawsuit from state leaders seeking its termination. Looking ahead, domestic security and physical infrastructure are facing a critical threat as a "potentially catastrophic" winter storm named Winter Storm Fern begins its sweep across more than 30 states this week. Starting January 23, the storm is expected to impact over 225 million people, stretching 2,000 miles from the Southwest to the East Coast. Overall, the current domestic landscape is defined by an intersection of institutional threats, law enforcement expansion, and environmental stressors.

Appendix A: Traffic Light Protocol for Information Dissemination

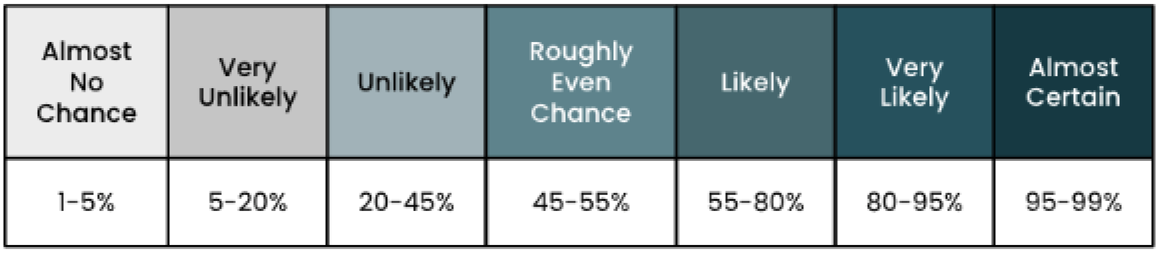


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%