Weekly Intelligence Brief

Classification: TLP:GREEN

January 10, 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 8, 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 - Implications of Removing Venezuelan President Maduro

On January 2, 2026, a U.S. joint military operation removed Venezuela's President Nicolás Maduro by force, transporting him to a New York detention center to face charges of drug-trafficking. In the short to medium term, the U.S. State Department will likely forge relationships with the existing members of the Maduro government. The outcome will very likely include the Venezuelan government abiding by U.S. demands in exchange for remaining in power. Ahead of the operation, the Trump administration made clear that criminal and narcotrafficking groups were a national security risk towards the United States and that the U.S. military would be prioritizing the Americas region while deprioritizing its commitments elsewhere. The removal of President Maduro makes it more likely that there will be further U.S. military operations against nations with adversarial relationships with the United States, close military relations with either Russia or China (particularly if they are in the Western Hemisphere), or valuable energy resources. There are unlikely to be major supply chain impacts from the operation, as Venezuela has few ties to international markets and Maduro's removal is therefore unlikely to impact global economic growth or contribute to inflation. Over the long term, the operation is likely to lead to increased access to Venezuela's oil and mineral reserves.

ZeroFox Intelligence Brief - Underground Economist: Volume 6, Issue 1

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

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Extensions Exfiltrating Chat Conversations

What we know:

- Cybersecurity researchers have detected a new malware campaign stealing real-time chatbot conversations from over 900,000 users.
- Two malicious Chrome extensions were used to exfiltrate personal conversations and all Chrome tab URLs to a threat actor-controlled server.
- The malware deceives users by impersonating a legitimate extension, which adds a sidebar on top of any website, enabling users to chat with popular large language models (LLMs) such as ChatGPT and DeepSeek.
- The threat actors reportedly abused "Lovable," an AI-powered web development platform, to anonymize their activities and prevent researchers from tracing them back to the original actors.

Background:

- The data was exfiltrated to attacker-controlled command-and-control (C2) servers approximately every 30 minutes.
- Threat actors exploited extension permissions and misleading consent prompts that claimed to collect only "anonymous, non-identifiable analytics" to harvest private user data.
- The malicious extensions, called "Chat GPT for Chrome with GPT-5, Claude Sonnet & DeepSeek AI" and "AI Sidebar with DeepSeek, ChatGPT, Claude, and more," still remain available on a popular web store as of writing.

Analyst note:

- Installing these extensions is likely to result in identity theft, data exfiltration, corporate espionage, credential exposure, and targeted phishing campaigns, especially if sensitive personal or business information has been shared with AI chatbots.
- Threat actors are likely exploiting growing user trust in AI chatbots to access private conversation and blackmail individuals for financial extortion.

- State-sponsored actors are also likely to harvest sensitive government communications, military strategies, intelligence queries, or diplomatic discussions shared in AI chats from officials' browsers.

Threat Actor Claims to Have Breached NordVPN

What we know:

- Threat actor “1011” has claimed to have breached Virtual Private Network (VPN) service provider NordVPN’s development server on dark web platform BreachForums. However, NordVPN has denied the breach.
- This campaign reportedly successfully bypassed multi-factor authentication in victim systems.

Background:

- 1011 has claimed to have compromised Salesforce Application Programming Interface (API) keys, Jira tokens, and source code. They have also posted screenshots of database dumps and configuration samples. NordVPN has said the leak stems from a test environment and does not impact its internal systems.

Analyst note:

- NordVPN’s confirmation of the test environment being compromised via a third-party vendor still likely suggests an unsecured environment, which poses a risk of further breaches.

Threat Actor Zestix Advertises Stolen Corporate Cloud Data

What we know:

- Threat actor “Zestix” is advertising corporate data allegedly stolen from multiple organizations in critical sectors, including aviation, defense, healthcare, and government.
- The actor reportedly breached cloud environments using credentials harvested through infostealer malware strains.

Background:

- The advertised data allegedly includes sensitive files related to aircraft maintenance manuals, defense, health records, source codes, and government contracts.

Analyst note:

- If the threat actor’s claims are true, stolen cloud credentials that are still unrotated and valid are likely to be reused or resold on dark web forums to other threat actors.
- Zestix’s claims are likely to be of interest particularly to nation-state actors focused on intelligence-gathering from critical sector entities for greater geopolitical advantages.

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 two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on January 7, 2026, and released one Industrial Control System (ICS) advisory on January 6. In the ICS advisory, CISA has warned of three vulnerabilities related to Columbia Weather Systems MicroServer firmware that can enable attackers to redirect Secure Shell (SSH) connections, steal plaintext secrets, and gain admin access. If exploited, these vulnerabilities are likely to enable attackers to manipulate or delete critical weather data. An SQL injection vulnerability in the Seeyon Zhiyuan OA Web Application System involves improper handling of the unitCode parameter in a certain file path and enables remote attackers to execute arbitrary SQL queries. A vulnerability in the discontinued Totolink EX200 wireless range extender, impacting the firmware-upload error-handling logic, enables threat actors to take control of vulnerable devices. A local file inclusion and path traversal vulnerability in jsPDF library for generating PDF documents in JavaScript applications enables threat actors to steal sensitive data. Veeam has released security patches for multiple flaws in its Backup & Replication software, including a remote code execution (RCE) vulnerability. A command injection flaw in legacy D-Link DSL gateway routers is being actively exploited in the wild, which can result in RCE.

CRITICAL

CVE-2025-14346

What happened: This bluetooth vulnerability in WHILL electric wheelchairs and Model F Power Chairs can enable attackers within a bluetooth range of about 30 feet to control the devices, risking patient safety.

- **What this means:** Attackers are likely to pair with a vulnerable wheelchair over bluetooth to issue movement commands, alter configuration profiles, and override speed controls without authentication or user interaction.
- **Affected products:**
  - All versions of WHILL Model C2 Electric Wheelchairs and Model F Power Chairs

CRITICAL

CVE-2026-21858

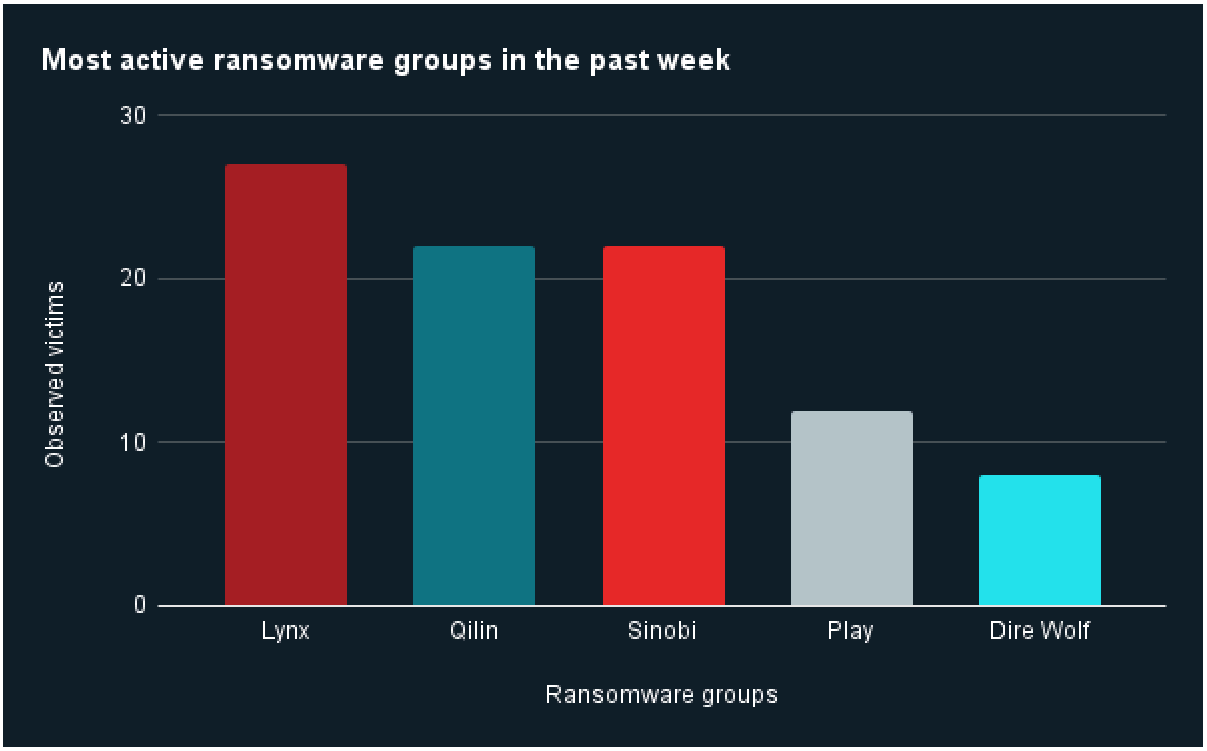
What happened: This is an unauthenticated RCE vulnerability in the n8n workflow automation platform that enables attackers to take control of local instances of n8n.

- **What this means:** Successful exploitation is likely to enable threat actors to access sensitive information and compromise downstream systems or entities.
- **Affected products:**
  - n8n versions before 1.121.0

Ransomware and Breach Intelligence

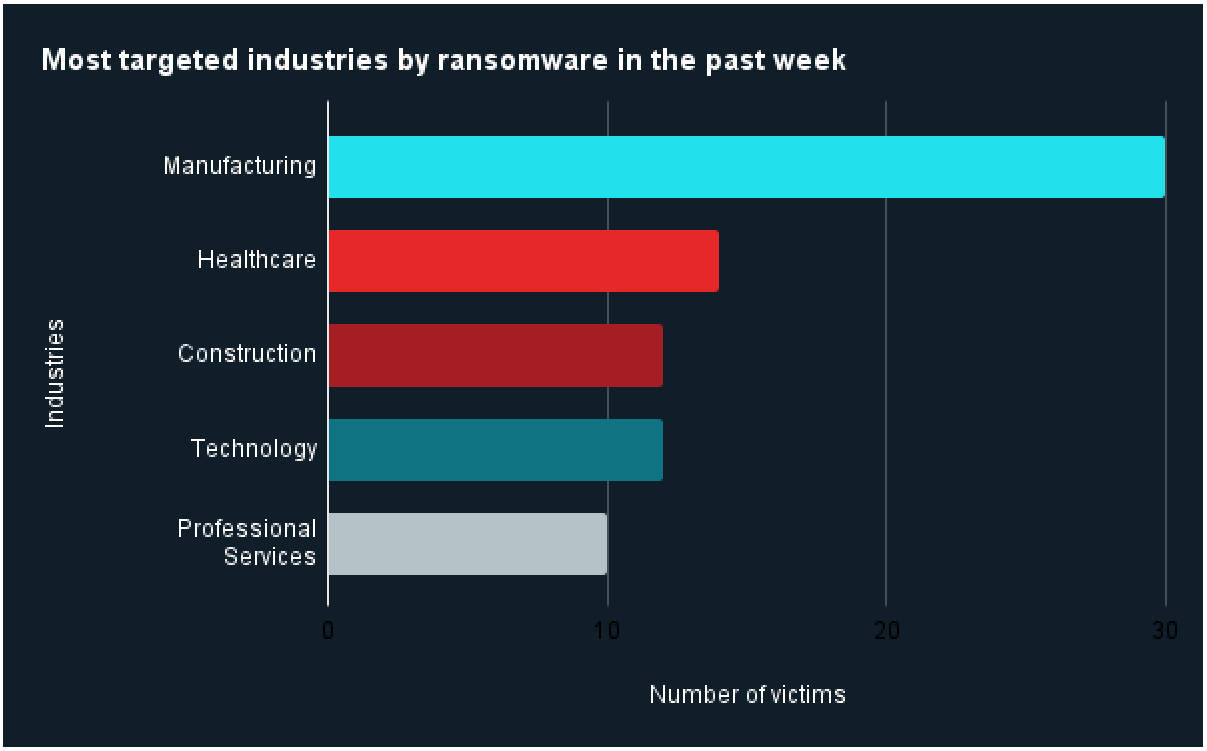
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup: Groups and Trends



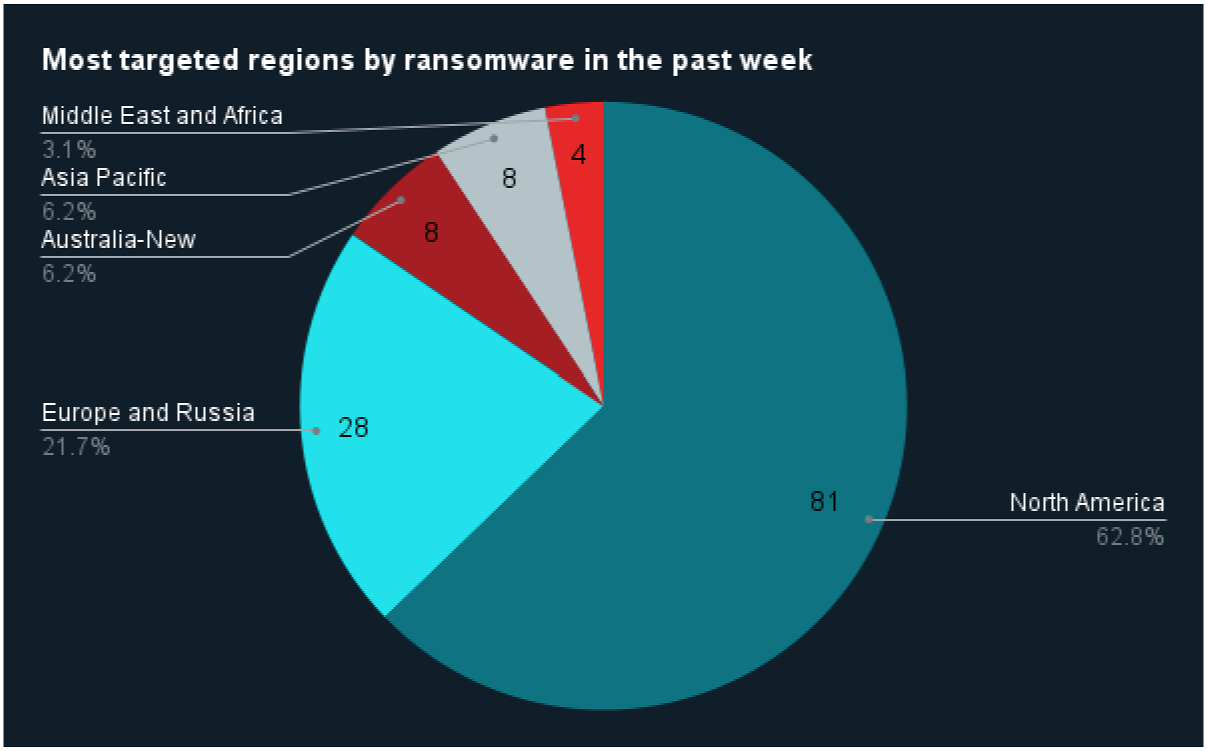
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Lynx, Qilin, Sinobi, Play, and Dire Wolf were the most active ransomware groups. ZeroFox observed close to 111 ransomware victims disclosed, most of whom were located in North America. The Lynx ransomware group accounted for the largest number of attacks, followed by Qilin and Sinobi.



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 healthcare.



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 28 ransomware attacks. Australia and New Zealand (ANZAC) and Asia-Pacific accounted for eight each, while Middle East and Africa accounted for four ransomware attacks.

Major Data Breaches Across Industries

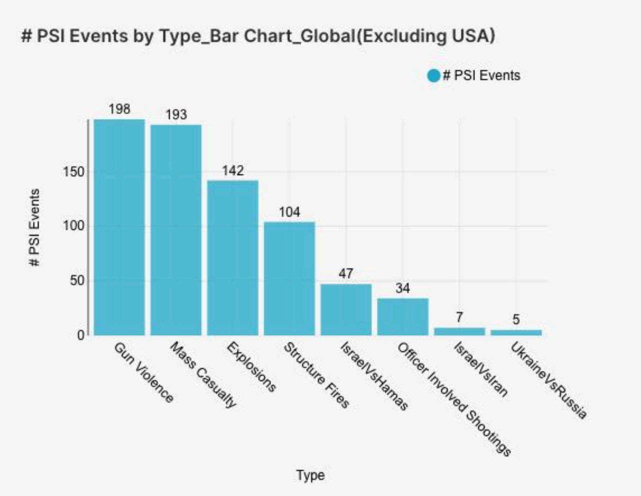
Targeted Entity	**Ledger**	**Gulshan Management Services**	**Manage My Health (MMH)**
Compromised Entities/victims	Ledger through third party payment processor Global-e	Over 377,000 individuals	Around 126,000 MMH website users
Compromised Data Fields	Ledger customer names contact information, and order data	Names, addresses, Social Security numbers, driver's license numbers, government-issued ID numbers, and financial information (bank account and credit or debit card details)	Data from the website's health documents section
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	Global	Texas	New Zealand
Industry	Finance	Retail	Healthcare
Possible Repercussions	Increased risk of targeted phishing and social engineering campaigns against Ledger customers, as well as broader exposure risks for other Global-e client brands	Identity theft, financial fraud, and tax or benefits fraud targeting affected individuals	Social engineering attacks, identity theft, and medical fraud, as well as extortion and blackmail of affected individuals

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

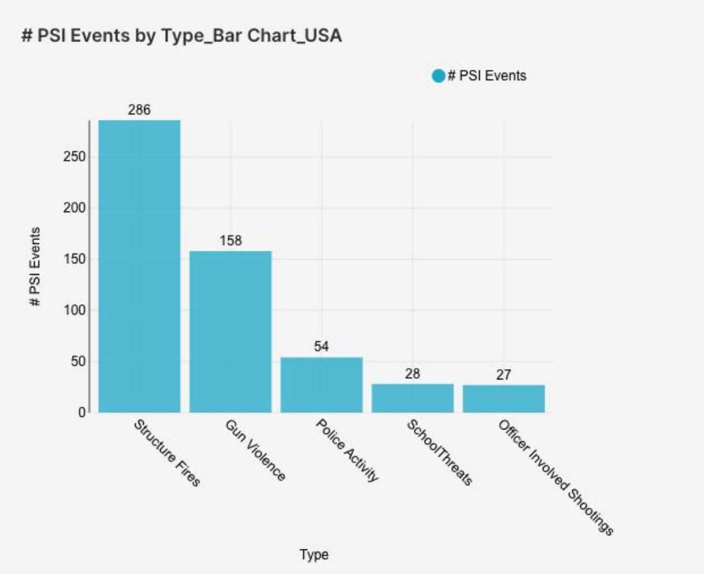


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was a 4 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being Iran, India, and Pakistan, in that order. Approximately 74 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 31 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) increased by 24 percent from the previous week. Events related to Russia's war in Ukraine decreased by 50 percent. The top three most-alerted subtypes were gun violence, which saw a 38 percent increase from the previous week; explosions, which increased by 15 percent; and structure fires, which decreased by 11 percent. Notably, officer-involved shootings increased by 42 percent, with Iran being the highest contributing country.

- **What this means:** Recent data reveals a rise in global mass casualty events this week, primarily driven by instability within ongoing conflict zones. In Iran, a significant wave of disruption sparked by economic hardship has led to intense clashes, with security forces reportedly using lethal force, resulting in at least 36 deaths as of early January 2026. The Israel-Hamas conflict continues to see an increase in alerts despite a fragile ceasefire established in late 2025, with the post-ceasefire death toll rising to over 400 victims. In contrast, activity related to Russia's war in Ukraine has seen a decrease in alerts this week, which aligns with a shift toward diplomatic frameworks discussed on January 6 despite occasional Russian strikes. Globally, the data this week underscores a shift in the nature of violence, with gun-related incidents rising due to civil unrest, while structure fires and large-scale conventional military movements in Eastern Europe show a marked decline.

Physical Security Intelligence: United States

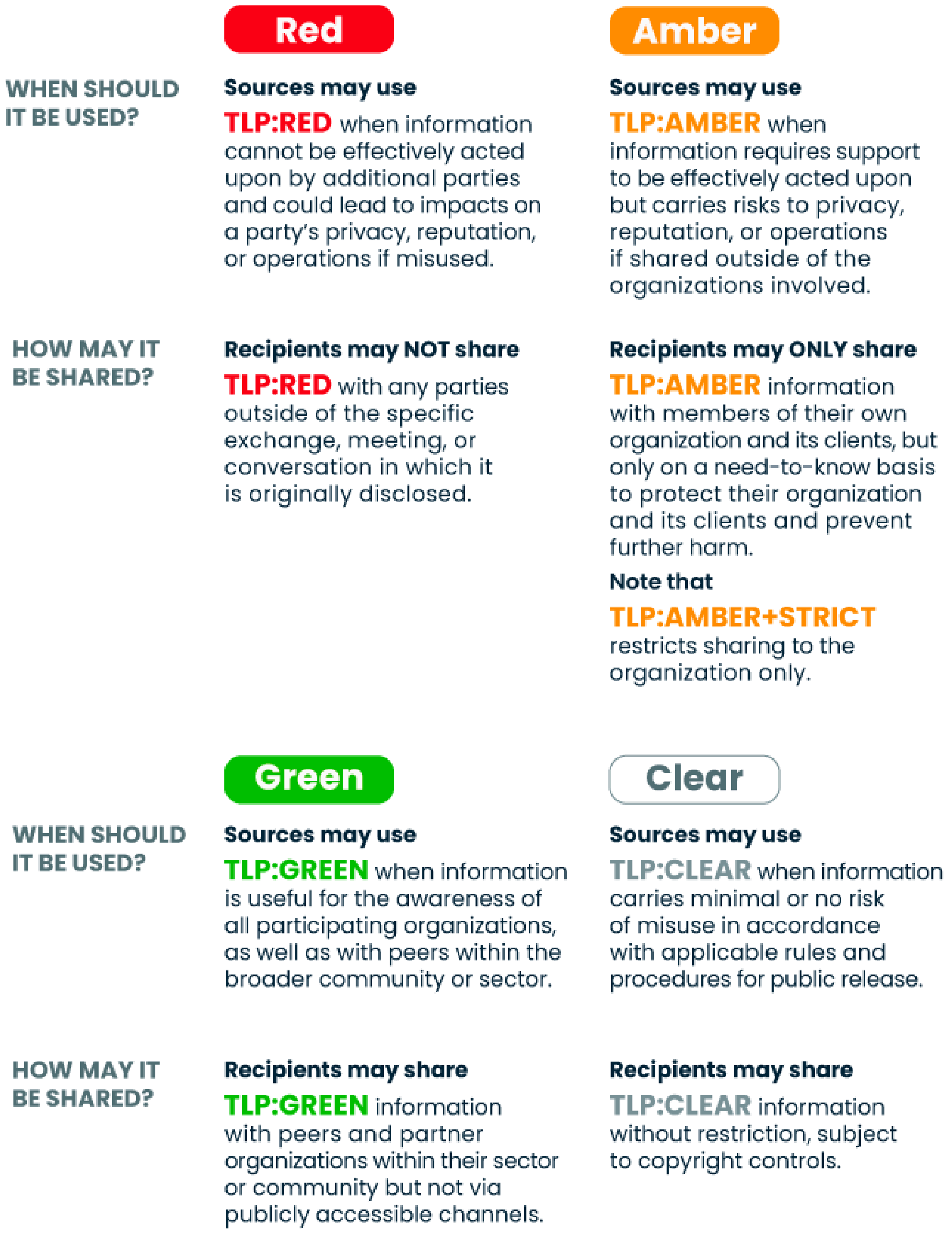


Source: ZeroFox Internal Collections

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 Texas and Tennessee, which together made up 22 percent of this week's nationwide total. Gun violence across the United States overall decreased by 7 percent from the week prior. Police activity alerts increased by 69 percent, and the top contributing states were Texas and California. Structure fires decreased by 2 percent, and the top two states for this subtype were California and New York. Notably, threats related to schools increased by 460 percent.

- **What this means:** Recent data indicates a significant shift in domestic safety priorities within the United States, with a significant increase in school-related threats. This surge is exemplified by events in Texas, where the FBI and local police investigated a social media video featuring a masked individual with firearms who targeted 14 different schools, including several elementary school campuses in Austin and high schools in the Fort Worth area. While nationwide gun violence alerts decreased somewhat, Texas and Tennessee remain the primary hot spots; for instance, there were two separate mass shootings in both Dallas, TX and Houston, TX on New Year's Day, which resulted in a total of 10 victims. General police activity alerts spiked this week, a trend influenced by Operation Metro Surge, a federal immigration crackdown powered by a sharp increase in Immigration and Customs Enforcement (ICE) manpower. On January 7, 2026, an ICE officer fatally shot a woman in Minneapolis, MN, during an enforcement operation, causing significant local disruption. The overall domestic physical security landscape this week is defined by a volatile intersection of school-related threats and a surge in high-intensity police activity driven by federal immigration enforcement operations.

Appendix A: Traffic Light Protocol for Information Dissemination

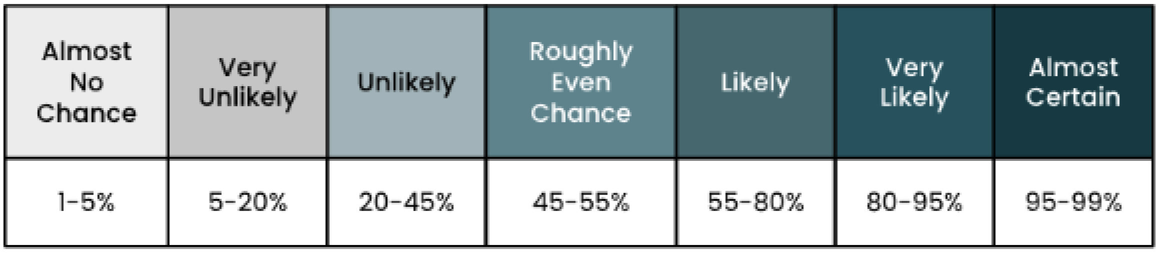


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively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