ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

September 20, 2025

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 (EDT) on September 18, 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 2
ZeroFox Intelligence Brief: China's Influence Operations Against Taiwan 2
ZeroFox Intelligence Flash Report: Prominent Threat Collective Announces Disbandment 2
ZeroFox Intelligence Brief: Detecting and Countering Synthetic Media 2
| Cyber and Dark Web Intelligence Key Findings 5
CrowdStrike Namespace Targeted in Expanding Npm Supply Chain Attack 5
Over 200 New CopyCop Sites Push AI-Generated Disinformation 6
AI Pentest Tool Villager Raises Concerns over Chinese Firm's Motives 6
| Exploit and Vulnerability Intelligence Key Findings 9
CVE-2025-21043 9
CVE-2025-10386 10
| Ransomware and Breach Intelligence Key Findings 12
Weekly Ransomware Overview: Key Threat Groups, Impacted Regions, Industries, and Major Attacks 12
Major Data Breaches in the Past Week 15
| Physical and Geopolitical Intelligence Key Findings 18
Physical Security Intelligence: Global 18
Physical Security Intelligence: United States 19
| Appendix A: Traffic Light Protocol for Information Dissemination 20
| Appendix B: ZeroFox Intelligence Probability Scale 21

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief: China's Influence Operations Against Taiwan

China has deployed various digital information warfare tactics against Taiwan on platforms such as TikTok, X (formerly, Twitter), YouTube, and Facebook—almost certainly to weaken the Taiwanese public's independence resolve. Disinformation tactics are wielded alongside soft power through cultural exchanges, influencer partnerships, and other long-term engagement strategies. In July 2025, the Communist Party of China's information campaign almost certainly attempted to sway the mass recall vote in Taiwan that aimed to remove center-right Kuomintang (KMT) lawmakers from the legislature, who are perceived to be more pro-China. ZeroFox assesses it is very likely the Chinese state is behind the recruitment of Taiwanese social media influencers to participate in propaganda tours of China, which frequently conclude with the participants denouncing the Taiwanese government or its ruling political party. A successful information campaign by China risks the erosion of public trust in Taiwanese democratic institutions and the weakening of Taiwan's identity, both domestically and internationally.

ZeroFox Intelligence Flash Report: Prominent Threat Collective Announces Disbandment

On September 11, 2025, the prominent threat collective "Scattered Lapsus$ Hunters" announced on its public Telegram channel that it was ceasing operations. The message also appeared on the homepage of breachforums[.]hn, with a link to the collective's Telegram page. In the post, Scattered Lapsus$ Hunters explained that it is intentionally disbanding now that its objectives have been fulfilled. The collective emphasized that this decision is not a defeat or reaction to law enforcement (LE) pressure but rather the planned conclusion of a campaign. Although Scattered Lapsus$ Hunters claims to have ceased operations, it is likely that its Indicators of Compromise (IOCs) remain relevant for detection and hunting and that credentials and malware associated with the threat collective are still active or may resurface in future incidents.

ZeroFox Intelligence Brief: Detecting and Countering Synthetic Media

Advancements in the quality of synthetic media now available have made it an attractive and powerful tool for threat actors across the cybercrime landscape. By manipulating imagery, video, or audio, attackers can better increase their chances of bypassing traditional security measures and enhance social engineering campaigns. In the next 12 months, AI detection tools will very likely remain heavily reliant on forensic analysis of digital artifacts such as pixel-level inconsistencies, metadata anomalies, and signal-based markers introduced during synthetic generation. Over the next one to three years, advances in GenAI models will very likely diminish the reliability of current forensic indicators. The convergence of detection with authentication frameworks will very likely shift the burden of proof from detecting fakes to verifying authenticity.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

CrowdStrike Namespace Targeted in Expanding Npm Supply Chain Attack

What we know:

- Security researchers have identified a large-scale npm supply chain attack (dubbed "Shai-Hulud") that has compromised at least 187 packages, including popular ones, such as @ctrl/tinycolor and several under CrowdStrike's namespace.
- The malware is self-propagating; it modifies packages to inject a malicious bundle[.]js script that steals developer and continuous integration credentials, creates unauthorized GitHub Actions workflows, and exfiltrates data.
- This follows the recent "s1ngularity" GitHub campaign in early September, which affected over 2,000 accounts via AI-powered malware targeting source code repositories.

Background:

- The supply chain attack compromised multiple CrowdStrike npm packages—including @crowdstrike/commitlint, @crowdstrike/glide-core, and eslint-config-crowdstrike—across several versions.
- The worm propagates automatically through affected maintainers' packages, creating new malicious repositories and continuing the infection chain.
- The malicious bundle.js uses TruffleHog to scan systems for secrets such as GitHub tokens, npm tokens, and certain keys and then exfiltrates them to a hardcoded webhook.

What is next:

- It is likely that several open-source packages across multiple ecosystems are now at risk.
- If not contained immediately, this rapidly progressing campaign could lead to other developers or companies using compromised dependencies and unknowingly importing malware into their own systems.
- Exposed packages could be exploited in further attacks, including unauthorized cloud access, continuous integration and continuous delivery (CI/CD) pipeline compromises, and lateral movement across organizations.
- Users could detect the campaign by analyzing their build logs and cross-checking them with already documented IoCs for suspicious elements.

Over 200 New CopyCop Sites Push AI-Generated Disinformation

What we know:

- Threat group "CopyCop" (or "Storm-1516") has launched over 200 new fake news websites impersonating local outlets and political organizations worldwide.
- Researchers observe the network uses self-hosted AI models to mass-produce disinformation targeting elections and political leaders.

Background:

- CopyCop, a Russia-backed disinformation network, reportedly uses self-hosted Llama 3 large language models (LLMs) to generate fake news sites, rewrite articles, and create deepfakes to amplify pro-Kremlin narratives.

Analyst note:

- It is likely that these sites will be weeded out in the near future in major countries.
- However, the campaign could expand into more divisive and smaller nations, where threat actors are likely to deploy tailored disinformation to exploit local grievances, deepen divisions, and shape political outcomes with less resistance.

AI Pentest Tool Villager Raises Concerns over Chinese Firm's Motives

What we know:

- Villager, an AI-driven penetration testing tool released publicly on the Python Package Index (PyPI) and promoted for its red teaming capabilities, has raised concerns among cybersecurity researchers after being downloaded over 10,000 times since July 2025.

Background:

- The tool is traced to a former Chinese capture-the-flag (CTF) competitor ("HSCSEC"), linked to an AI development firm called Cyberspike, which has a dubious history.
- The AI-integration in Villager enables automation in reconnaissance, vulnerability exploitation, and other tasks.

Analyst note:

- Villager is likely to be misused by threat actors, similar to legitimate red teaming tool Cobalt Strike.

- The tool is hosted on Cyberspike's infrastructure and connected to its private GitLab repository, which likely indicates an attempt to control Villager's potential misuse.

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 17 Industrial Control System (ICS) advisories on September 16 and September 18, 2025. Apple issued over 50 security patches alongside the release of iOS 26, iPadOS 26, and macOS Tahoe 26. On the other hand, Apple has reportedly warned certain customers of targeted spyware attacks. Cybersecurity researchers have found four vulnerabilities, together dubbed "Chaotic Deputy," that affect open-source cloud-native platform Chaos Mesh, of which three are critical. Cisco has released patches for three vulnerabilities in its IOS XR software. CVE-2025-20248 can enable attackers to bypass image signature verification; the other two bugs are an Address Resolution Protocol (ARP)-based denial-of-service (DoS) vulnerability (CVE-2025-20340) and an Access Control List (ACL) bypass vulnerability (CVE-2025-20159). Certain Industrial Cellular Gateway models from Planet Technology have a Missing Authentication vulnerability, enabling unauthenticated remote attackers to manipulate the device through a specific function. A buffer overflow vulnerability in Apple CarPlay (CVE-2025-24132) is yet to be patched by most vendors and all car manufacturers, leaving vehicles exposed to privacy breach or causing a compromise of vehicle systems.

CRITICAL

CVE-2025-21043

What happened: This out-of-bounds write vulnerability was exploited as a zero-day bug, targeting Samsung Android devices through malicious image parsing. This vulnerability in a closed-source image parsing library reportedly enables threat actors to execute arbitrary code on devices running Android 13 or later.

- **What this means:** If patches are not deployed, threat actors could exploit the flaw to harvest sensitive data from communication apps—including payment details, screenshots, and location information.
- **Affected products:**
  - The affected products are included in this update.

HIGH

CVE-2025-10386

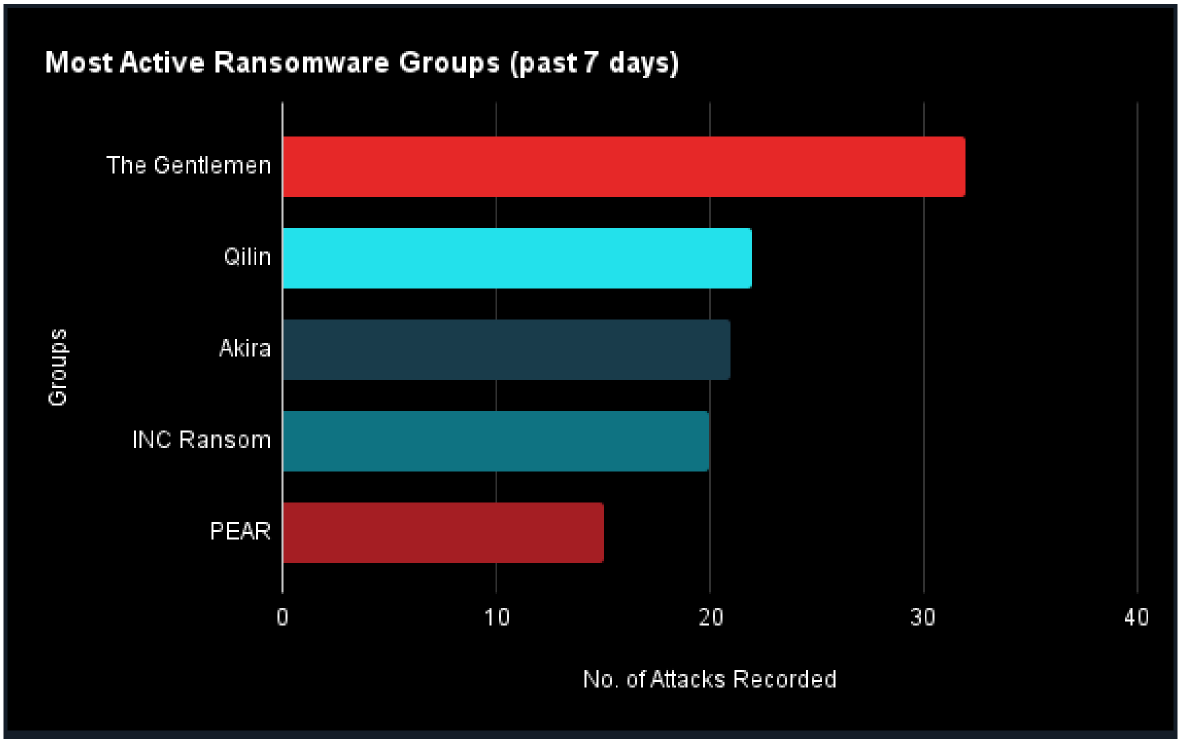
What happened: A public exploit is available for this remotely exploitable script-injection flaw. Successful exploitation enables attackers to execute arbitrary client-side scripts to hijack sessions, steal credentials, or deliver malware.

- **What this means:** This is likely to result in account takeover, user impersonation, targeted phishing, credential theft, and escalation into broader network compromise.
- **Affected products:**
  - Yida ECMS Consulting Enterprise Management System 1.0

Ransomware and Breach Intelligence

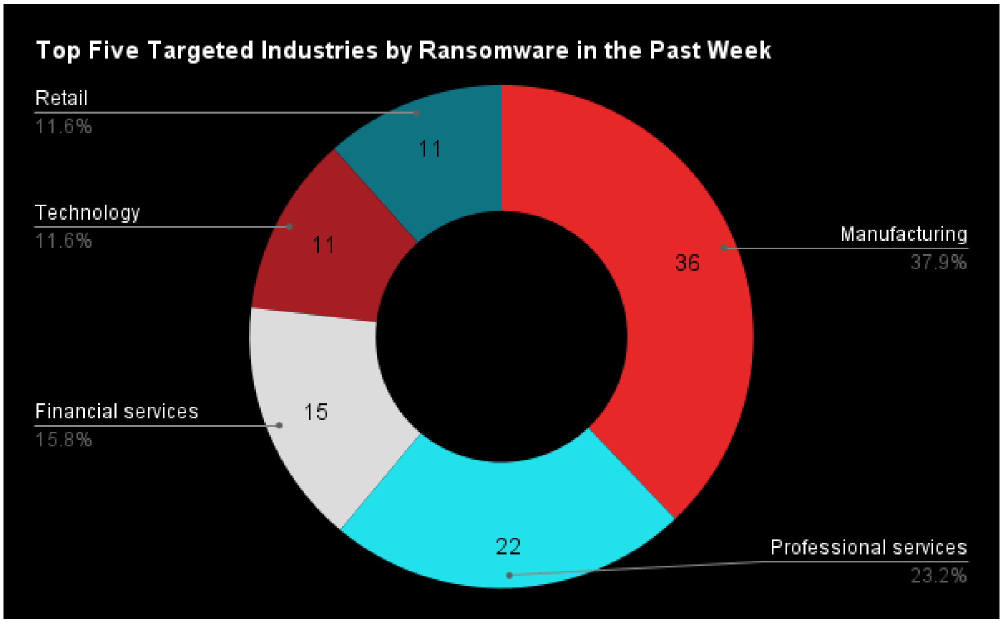
Ransomware and Breach Intelligence Key Findings

Weekly Ransomware Overview: Key Threat Groups, Impacted Regions, Industries, and Major Attacks



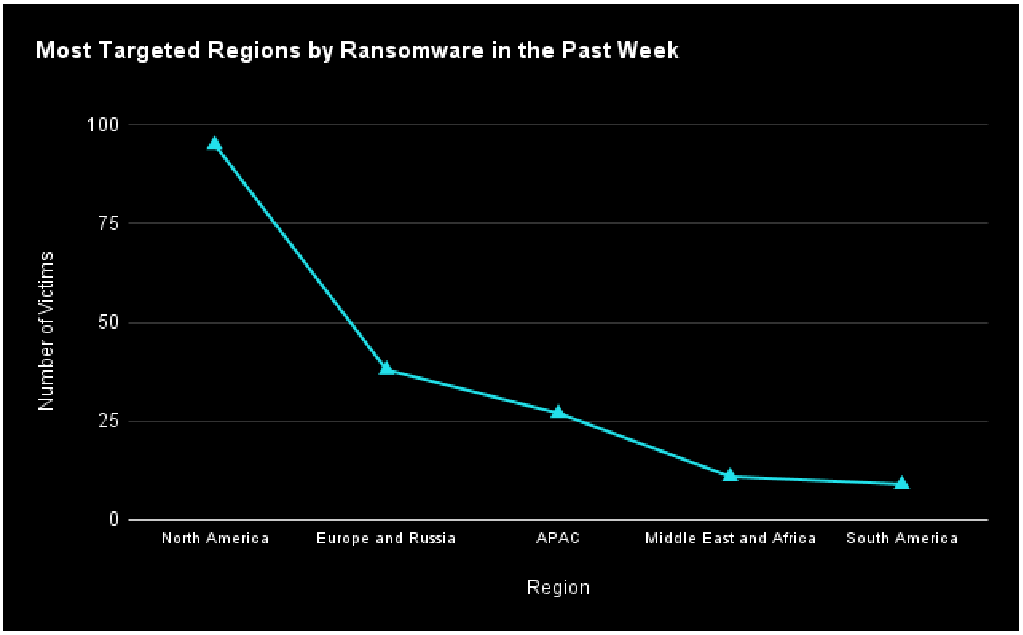
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, The Gentlemen, Qilin, Akira, INC Ransom, and PEAR were the most active ransomware groups. ZeroFox observed at least 183 ransomware victims disclosed, most of whom were located in North America. The Gentlemen 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 professional services, financial services, technology, and retail.



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 95 ransomware attacks observed in North America, while Europe and Russia accounted for 38, Asia-Pacific (APAC) for 27, Middle East and Africa for 11, and South America for nine.

Recap of major ransomware events observed in the past week: Insight Partners, a venture capital and private equity firm based in New York, is alerting thousands of individuals that their personal information was compromised in a ransomware attack. The KillSec ransomware group targeted Brazilian healthcare provider MedicSolution and stole over 34 GB of data. Ransomware group INC Ransom has claimed responsibility for a cyberattack on Panama's Ministry of Economy and Finance (MEF) that reportedly stole over 1.5 TB of data. Yurei, a new ransomware group, uses open-source malware for double-extortion attacks but has a flaw that allows victims to partially recover their encrypted data.

Major Data Breaches in the Past Week

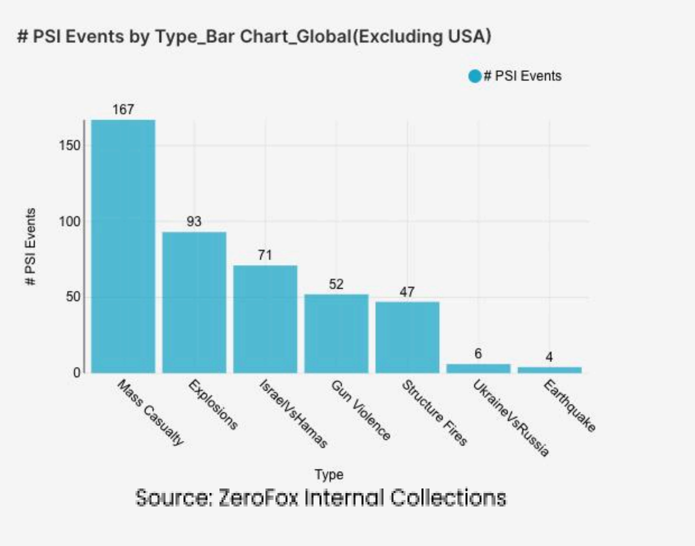
Targeted Entity	FinWise	Great Firewall of China	SonicWall
Compromised Entities/victims	689,000 customers	600 GB of data	N/A
Compromised Data Fields	Customer information, including full names and other personal data	Confidential materials from the system's development, including source code, internal communications, work logs, and technical documentation	Firewall configuration backup files
Suspected Threat Actor	Yet to be determined	Enlace Hacktivista	Yet to be determined
Country/Region	United States	China	Global
Industry	Financial services	Government and technology	Technology
Possible Repercussions	Identity theft, phishing and social engineering attacks, financial fraud, unauthorized access or exfiltration, and insider exploitation	Source code exploitation, espionage or intelligence gathering, supply chain attacks, system infiltration, and social engineering	Firewall exploitation, network intrusion, unauthorized access, targeted attacks, and configuration manipulation

Three major breaches observed in the past week

Other major data breaches observed in the past week: A major UK rail operator has disclosed a data breach that resulted in customers' contact information and travel history being stolen. The ShinyHunters extortion group has reportedly claimed to have stolen more than 1.5 billion Salesforce records from 760 companies by exploiting compromised Salesloft Drift OAuth tokens. Tiffany has disclosed that the May 2025 data breach impacted over 2,500 customers, with attackers gaining access to gift card information, including names, contact details, and PINs. In the span of a week, three U.S. healthcare providers disclosed major breaches impacting nearly 856,000 people.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings



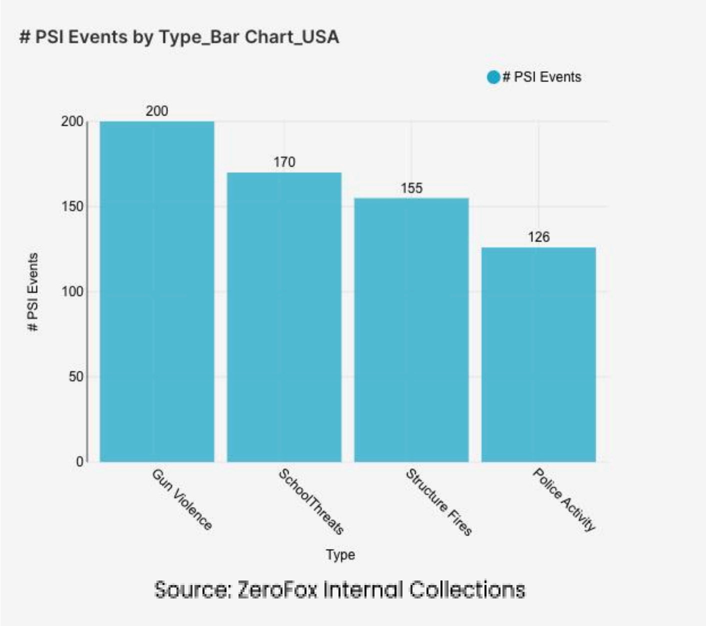
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 1 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian Territories, India, and Syria, in that order. Approximately 56 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 40 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) decreased by 16 percent from the previous week. Events related to Russia’s war in Ukraine decreased by 25 percent. The top three most-alerted subtypes were explosions, which saw a 13 percent decrease from the previous week; gun violence, which decreased by 28 percent; and structure fires, which decreased by 16 percent. Notably, alerts under the earthquake subtype tripled in volume from the previous week.

- **What this means:** Based on recent global events, the data reflects a week marked by shifting conflict dynamics. Despite an overall decrease in alerts related to Israel-Hamas this week, which may be attributed to a slight pause in attacks while evacuations took place, a new Israeli ground offensive on Gaza City on September 16 has resulted in numerous strikes and a rising death toll, with the United Nations Secretary-General warning that Israel does not appear interested in a ceasefire as it continues its campaign. Meanwhile, the decrease in alerts for Russia's war in Ukraine aligns with a recent report showing a slight dip in the average monthly rate of Russian territorial gains. The International Working Group on Russian Sanctions has also proposed new restrictions targeting Russia’s energy and financial sectors as well as its access to Western military technologies. Additionally, Russia was hit with four earthquakes in the Kamchatka Peninsula on September 15, which correlates with the sharp increase in overall earthquake alerts this week. All of the aforementioned data reveals a complex global landscape, wherein localized conflicts and shifting threat types continue to shape the international security environment.

Physical Security Intelligence: United States

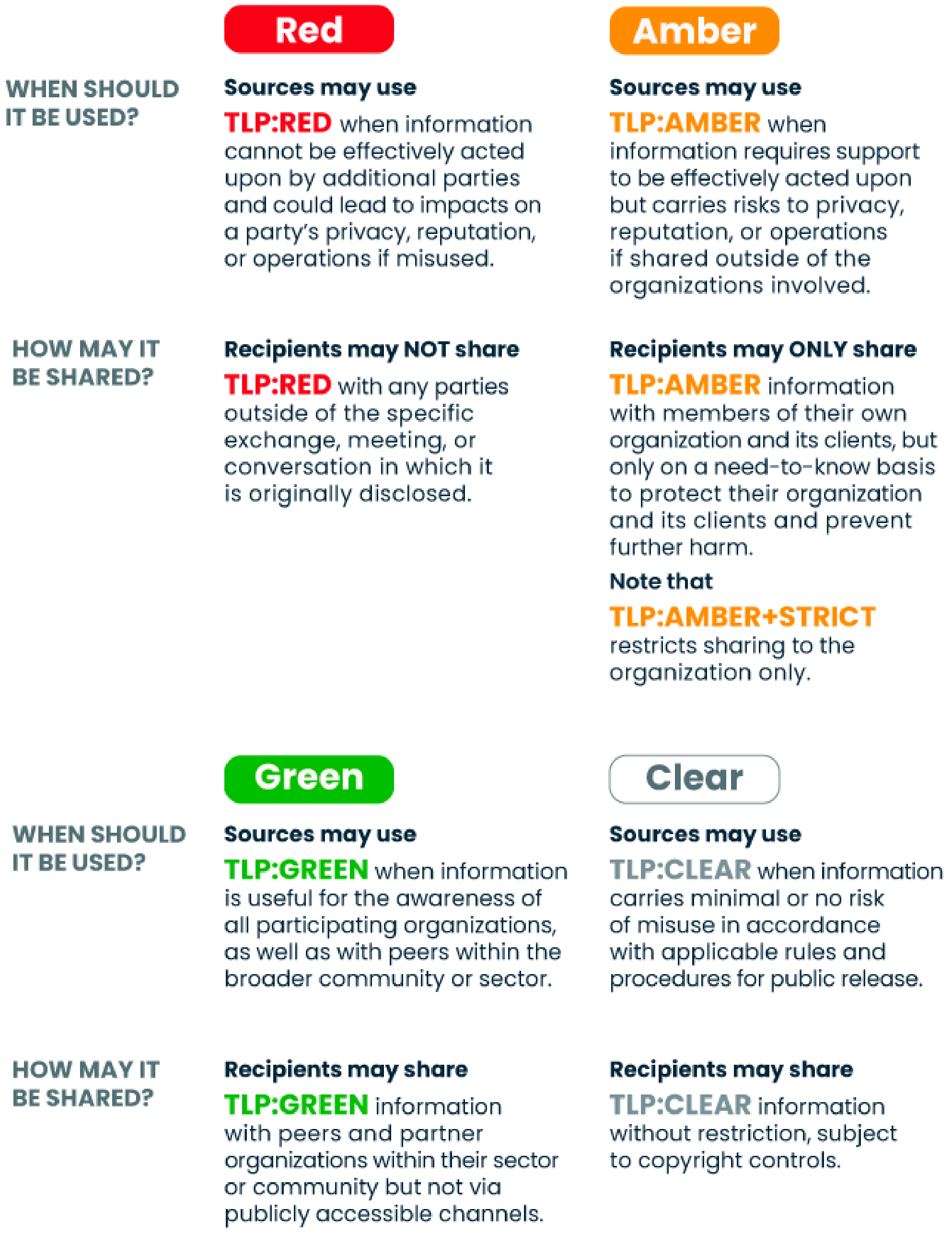


Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, 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 23 percent of this week's nationwide total. Gun violence across the United States overall decreased by 10 percent from the week prior. Police activity alerts increased by 50 percent, and the top contributing states were Texas and California. Structure fires decreased by 13 percent, and the top two states for this subtype were New York and California. Notably, threats related to schools (not including protest activity) increased by 62 percent.

- **What this means:** Over the past week, the data indicates a rise in police activity and threats despite an overall decline in gun violence and structure fires. The most notable trend is the sharp increase in threats related to schools; for instance, on September 11, a student opened fire at a high school in Colorado, critically injuring two students before killing himself. The incident, which is now the latest example of a school shooting, sparked further threats against students, who later organized walkouts to protest gun violence. This also follows a week of coordinated death threats against Black students at several Historically Black Colleges and Universities (HBCUs) across the country, forcing them into lockdown. Police activity nationwide increased significantly, potentially due to the heightened law enforcement presence typically seen on the anniversary of the 9/11 attacks. Meanwhile, New York had the highest number of structure fires, as evidenced by a five-alarm fire in Brooklyn, New York City, on September 17, which caused extensive damage and took over seven hours to control. Together, the data presents a mixed and volatile picture of the United States, marked by a rise in social tensions, targeted threats against institutions, and man-made disasters.

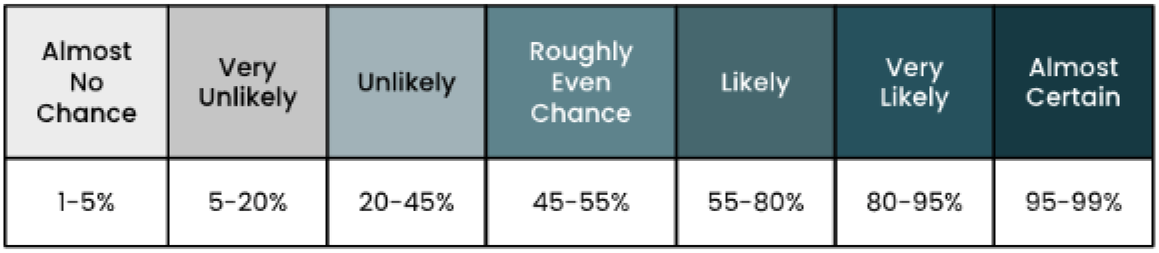
Appendix A: Traffic Light Protocol for Information Dissemination



	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%