ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

July 26, 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 July 24, 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 Flash Report - Major Cybercrime Forum Disrupted by Law Enforcement 2

ZeroFox Intelligence Flash Report - SEO Poisoning Abusing LLMs 2

ZeroFox Intelligence Brief - Fake Geopolitical Consultancy Jobs: China's Espionage Tactic 2

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 14 3

| Cyber and Dark Web Intelligence Key Findings 5

Key Figure Behind Major Russian-Speaking Cybercrime Forum Arrested in Ukraine 5

Joint Advisory Issued on Interlock Ransomware 6

Russia-Linked LAMEHUG Malware Using AI-Generated Commands for Attacks 6

| Exploit and Vulnerability Intelligence Key Findings 9

CVE-2025-53770 and CVE-2025-53771 9

CVE-2025-54309 10

| Ransomware and Breach Intelligence Key Findings 12

Ransomware Trends Across Groups, Industries, and Regions 12

Data Breaches Across Different Industries 15

| Physical and Geopolitical Intelligence Key Findings 17

Physical Security Intelligence: Global 17

Physical Security Intelligence: United States 18

| Appendix A: Traffic Light Protocol for Information Dissemination 19

| Appendix B: ZeroFox Intelligence Probability Scale 20

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report - Major Cybercrime Forum Disrupted by Law Enforcement

On July 23, 2025, prominent deep web forum XSS went offline; its associated web domain, xss[.]is, is currently displaying an announcement about the forum's seizure by multiple law enforcement (LE) entities. The forum outage follows an announcement by the same LE bodies about the arrest of an individual suspected of fulfilling an administrative role within XSS. Reporting suggests that the arrest, which took place in Ukraine, is part of an LE operation that commenced in 2021. While the arrest of the alleged deep web forum moderator does not itself allude to long-term disruption of the xss[.]is forum, there is a likely chance that subsequently obtained information will lead to the identification of additional individuals involved in operating the XSS forum, as well as the acquisition of critical digital infrastructure by LE.

ZeroFox Intelligence Flash Report - SEO Poisoning Abusing LLMs

ZeroFox has identified an escalation in Search Engine Optimization (SEO) poisoning campaigns using novel tactics, techniques, and procedures (TTPs) to abuse artificial intelligence (AI) large language models (LLMs) in order to increase the credibility of search results. ZeroFox assesses that threat actors are successfully tricking LLMs into believing these contact numbers and methods are credible by creating pages as questions, injecting them as PDFs into legitimate sites, and reposting them on long URL lists such as Pastebin and as comments on "crowd sourced" forums. The threat actors are purposefully exploiting the .gov and .edu domains due to their "reputation." This is also being mirrored as comments on crowd-sourced forums like Goodreads or blog-style sites such as the ZohoDesk knowledge base. These campaigns are likely to ultimately lead users to divulge their personally identifiable information (PII), suffer monetary losses, and cause reputational damage to the original brand.

ZeroFox Intelligence Brief - Fake Geopolitical Consultancy Jobs: China's Espionage Tactic

State-sponsored actors are exploiting online job platforms, such as LinkedIn and Indeed, to recruit candidates with security clearances and other insiders for intelligence-gathering under the guise of remote consultancy work. ZeroFox observed a likely espionage campaign in India using online job platforms to recruit individuals with privileged access to the Indian government's diplomatic activities. The entity used social engineering and phishing tactics to recruit citizens as unwitting informants for the operation. Cybersecurity researchers suggest that the IP addresses and domain used in the India campaign likely belong to an advanced persistent threat (APT). Similar espionage campaigns have been reported in the United States and Europe. Multiple intelligence agencies—including those of the United States and the United Kingdom—have linked such campaigns to Chinese intelligence operations.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 14

The Underground Economist is an intelligence-focused series that highlights dark web findings from our ZeroFox Dark Ops intelligence team.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Key Figure Behind Major Russian-Speaking Cybercrime Forum Arrested in Ukraine

What we know:

- On July 22, 2025, the suspected administrator of the Russian-language cybercrime forum xss[.]is was arrested in Kyiv in a joint operation by Europol and French and Ukrainian authorities.
- The forum's clearnet domain was seized and now displays an official law enforcement notice.
- A backup clearnet domain (xss[.]as) is currently inactive. However, the forum remains operational via its .onion (Tor) domain.
- On July 24, an alleged admin, "#root," claimed the main server was not affected and that efforts were underway to restore the infrastructure.
- Two newly observed domains (theazot[.]icu and theazot[.]xyz) registered in Malaysia appear to redirect users to xss.

Background:

- Xss was one of the largest Russian-speaking cybercrime forums, with over 50,000 registered users, facilitating the trade of stolen data, malware, and illicit services.
- The arrested individual also allegedly operated thesecure[.]biz, a private encrypted messaging service for cybercriminals.
- Upon analyzing the domain details for xss[.]is and breachforums[.]is, security researchers have identified a potential link to the Icelandic Police. Both domains share the same domain registration details—including email address, contact name, phone number, and physical address. Notably, the listed phone number and address are reportedly associated with the Icelandic Police.

What is next:

- Further investigation is likely needed to confirm the legitimacy of Icelandic Police contact information in domain registrations.
- Authorities could target remaining infrastructure or onion services to fully dismantle xss operations.
- The domain registration overlap with BreachForums is likely to prompt inquiries into possible alliances or shared infrastructure.

- Monitoring of deep and dark web chatter will likely be key in assessing xss's attempted comeback or operational pivot.
- The suspected administrator’s long-standing connections and insider knowledge are likely to yield valuable intelligence, enabling further identification and tracking of associated actors and infrastructure.

Joint Advisory Issued on Interlock Ransomware

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) and other organizations have issued a joint Cybersecurity Advisory, warning organizations about Interlock ransomware, which targets popular operating systems and uses double extortion tactics after breaching networks.

Background:

- Interlock has been active since late September 2024, targeting businesses and critical infrastructure across North America and Europe. It gains access through drive-by downloads and ClickFix social engineering, then spreads laterally within networks.

Analyst note:

- Interlock attacks are likely to result in network compromise, data theft, financial loss, and operational disruption. Organizations are advised to strengthen defenses via Domain Name System (DNS) filtering, firewalls, user awareness, timely patching, network segmentation, and robust access controls with multi-factor authentication.

Russia-Linked LAMEHUG Malware Using AI-Generated Commands for Attacks

What we know:

- Ukraine’s national cyber incident response team (CERT-UA) has warned about a new Russia-linked malware family called “LAMEHUG,” which uses AI-generated computer commands, aimed at system reconnaissance and data exfiltration.

Background:

- LAMEHUG is reportedly the first publicly documented malware to use a large language model (LLM) to carry out attacks. It used the Qwen 2.5-Coder-32B-Instruct LLM developed by Alibaba Cloud and hosted on the American company Hugging Face's API. The malware was found in files sent to Ukrainian government personnel via phishing emails using compromised ministerial accounts.

Analyst note:

- AI-generated dynamic commands are likely to evade detection by security software that usually inspect hardcoded commands. Generating commands using a textual description is likely to lower the technical threshold required to carry out malware campaigns.

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. CISA added eight vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on July 18 and July 20, as well as in two separate alerts on July 22, 2025. CISA also released nine Industrial Control Systems (ICS) advisories on July 22. ExpressVPN fixed a vulnerability in its app that risked exposure of users' real IP addresses by enabling certain Remote Desktop Protocol (RDP) traffic to bypass the virtual private network (VPN) tunnel. Eight vulnerabilities—including three flaws enabling operating system command execution—were discovered in Helmholz REX 100 industrial routers and have since been patched. Cisco warned that three recently patched vulnerabilities in its Identity Services Engine (ISE) were being actively exploited. A Middle Eastern surveillance company was observed exploiting a new Signaling System 7 (SS7) bypass attack to secretly track phone locations. Two unauthenticated XML External Entity (XXE) vulnerabilities in SysAid IT service management (ITSM) software were under active exploitation, enabling threat actors to hijack administrator accounts.

CRITICAL

CVE-2025-53770 and CVE-2025-53771

What happened: These are remote code execution (RCE) vulnerabilities affecting on-premise SharePoint servers. Microsoft released out-of-band security patches for the zero-days, which were actively being exploited. At least 54 organizations, including multinational organizations, were reportedly compromised.

- **What this means:** Two bugs were patched in Patch Tuesday updates, but threat actors were able to discover two zero-days (CVE-2025-49706 and CVE-2025-49704) that bypassed these patches. Microsoft observed multiple China-linked actors—such as Linen Typhoon, Violet Typhoon and Storm-2603—exploiting these vulnerabilities. The proof-of-concept exploit was also disclosed on GitHub, resulting in more threat actors joining the ongoing exploits.
- **Affected products:**
  - Microsoft SharePoint Server Subscription Edition, SharePoint 2019, and SharePoint 2016

CRITICAL

CVE-2025-54309

What happened: This zero-day vulnerability in unpatched versions of enterprise file transfer server CrushFTP is under active exploitation. The bug enables threat actors to gain administrative access through web interface.

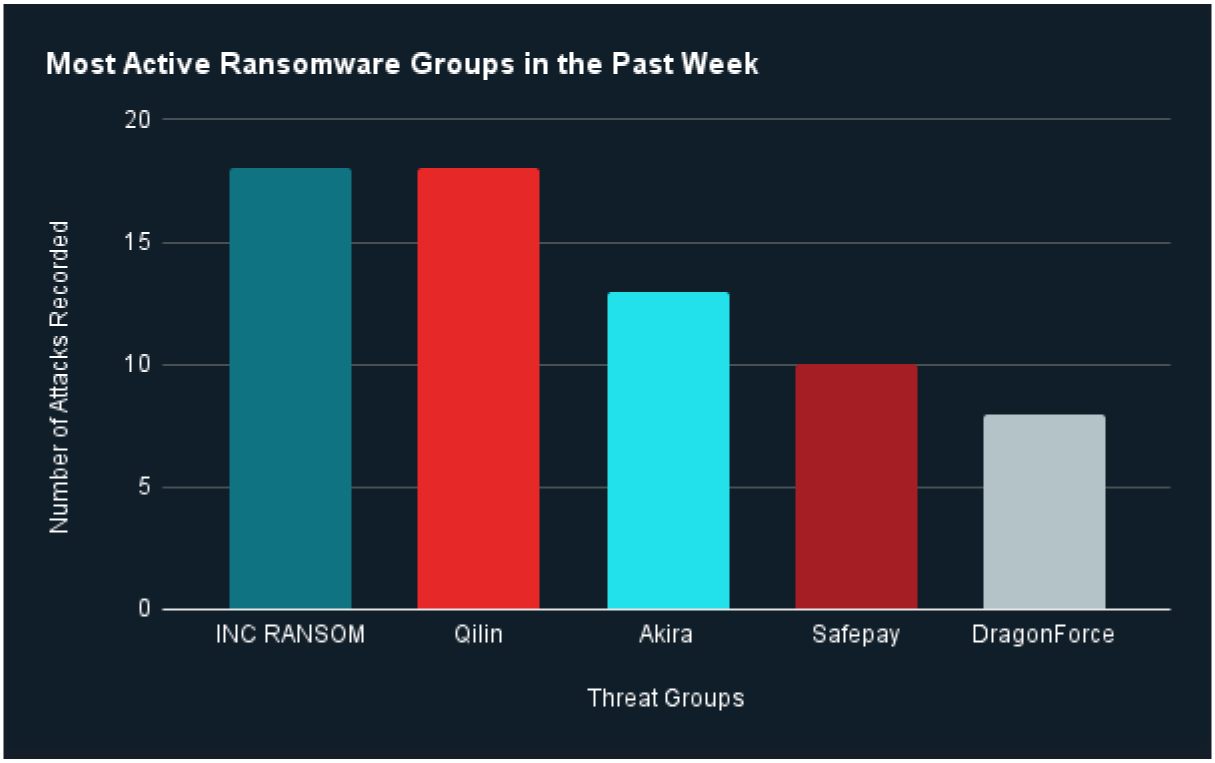
- **What this means:** Vulnerable systems are likely to be targeted in ransomware attacks or data theft campaigns. Ransomware groups such as Cl0p are known to exploit similar vulnerabilities.
- **Affected products:**
    - Versions below 10.8.5 and 11.3.4_23

.

Ransomware and Breach Intelligence

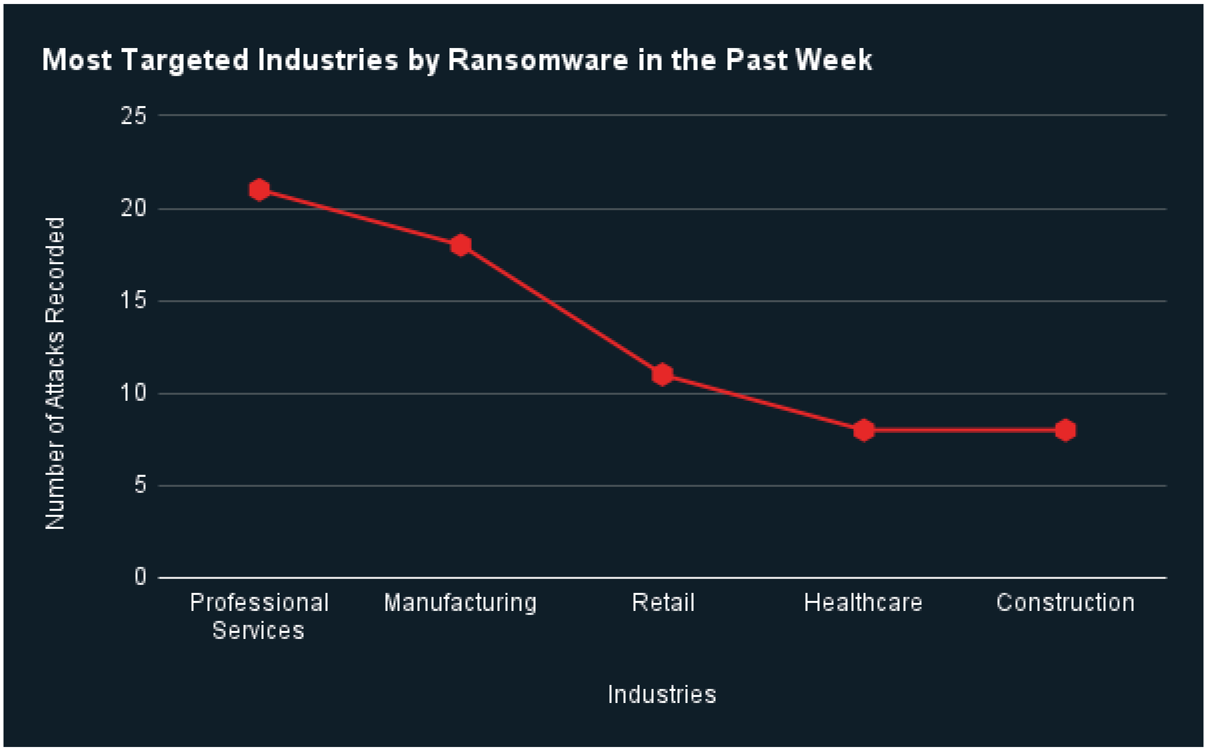
Ransomware and Breach Intelligence Key Findings

Ransomware Trends Across Groups, Industries, and Regions



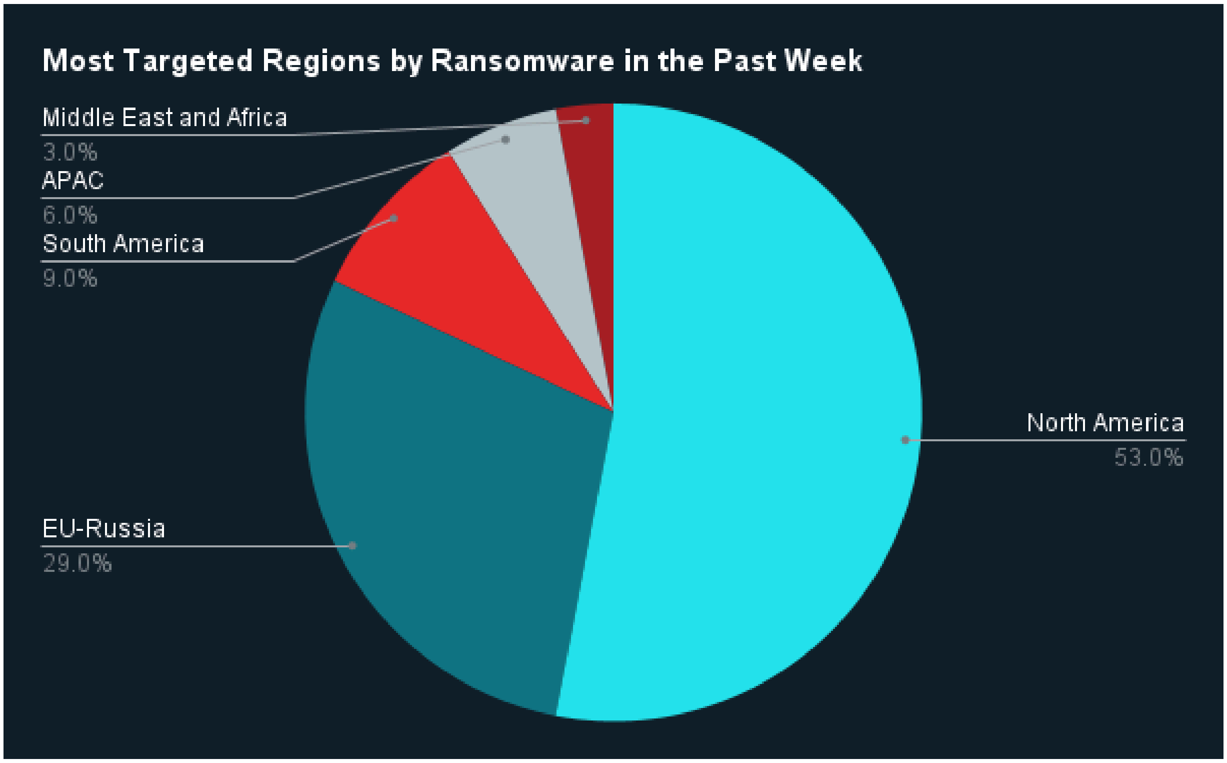
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, INC RANSOM, Qilin, Akira, Safepay, and DragonForce were the most active ransomware groups. ZeroFox observed at least 94 ransomware victims disclosed, most of whom were located in North America. The INC RANSOM and Qilin ransomware groups accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that professional services was the industry most targeted by ransomware attacks, followed by manufacturing, retail, healthcare, and 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-Russia. North America witnessed 53 ransomware attacks, while Europe-Russia accounted for 29, South America for nine, Asia Pacific (APAC) for six, and Middle East and Africa for three.

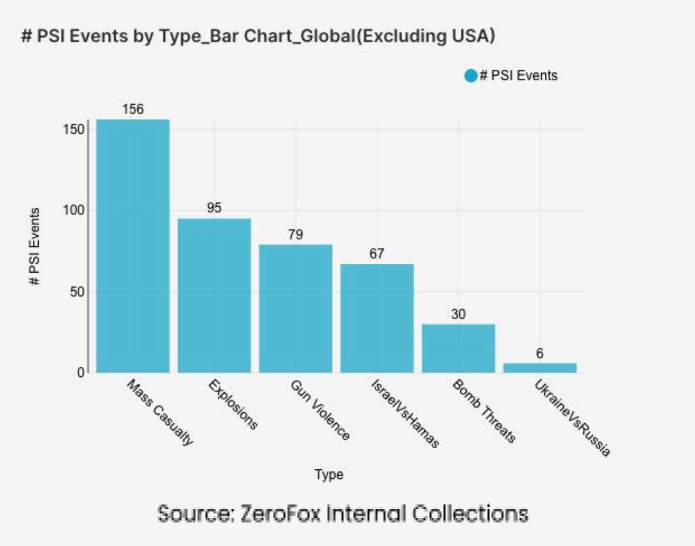
Data Breaches Across Different Industries

Targeted Entity	**Dell**	**Dior**	**Gladney Center for Adoption**
Number of Records/Victims Compromised	1.3 TB of data from Dell's Customer Solution Centers platform	Undisclosed number of Dior clients	2.49 GB of 1.1 million records
Compromised Data Fields	Old contact list and suspected sample medical data and financial information	Names, contact information, dates of birth, passport, government ID numbers, some Social Security numbers	Personal information on children, adoptive families, and staff
Suspected Threat Actor	World Leaks (Likely rebrand of Hunters International ransomware)	N/A	N/A
Country/Region	United States	United States	Texas
Industry	Technology	Fashion	Nonprofit
Possible Repercussions	Compromise of devices reusing old passwords, lateral movement within networks, supply chain attacks, impersonation, and fraud	Phishing and other social engineering attacks, financial fraud, identity theft, and account takeovers	Physical and online stalking, impersonation, social engineering, doxxing, and identity theft

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings



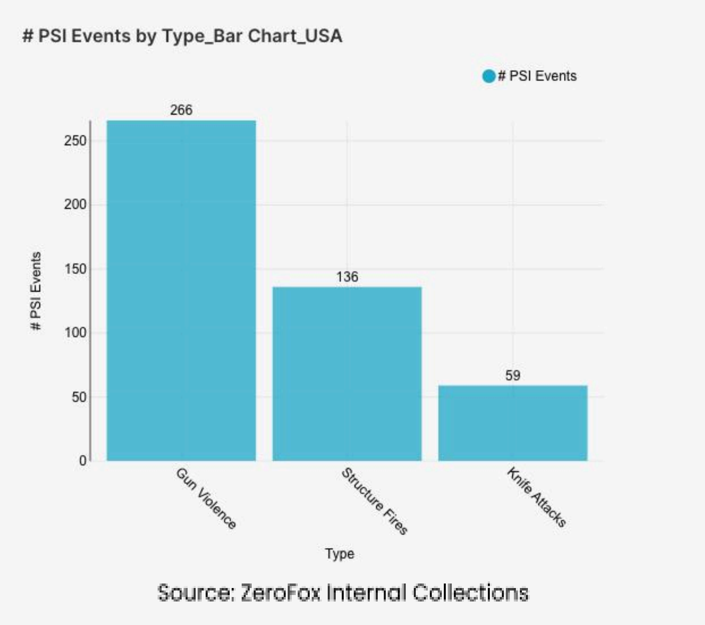
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 5 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being India, the Palestinian Territories, and Syria, in that order. Approximately 61 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 45 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 3 percent from the previous week. Events related to Russia's war in Ukraine increased by 20 percent. The top three most-alerted subtypes were explosions, which saw a 14 percent decrease from the previous week; gun violence, which increased by 27 percent; and bomb threats, which increased by 100 percent. Global protest activity increased by 18 percent.

- **What this means:** The past week has seen a notable surge in global instability and mass casualty events, with several ongoing conflicts contributing to this week's increase in alerts. The Israel-Hamas conflict continues to generate significant violence; one such event occurred on July 20, when a World Food Programme convoy in Gaza came under fire from Israeli tanks and firearms, resulting in 73 deaths and over 150 injuries. In total, between July 16 and July 23, 646 Palestinians were killed and 3,438 were injured. Meanwhile, in Syria, an explosion in Idlib on July 24, believed to have occurred at an ammunition depot, killed at least six people and injured dozens. India had the highest number of mass casualty events this week, which also correlates to the sharp increase in bomb threats; over 80 schools in Delhi and Bengaluru received bomb threats on July 18, causing widespread panic and disruption. Alerts related to Russia's war in Ukraine saw a substantial increase, as Russia has scaled up its drone attacks, frequently launching hundreds of drones nightly. Finally, the global increase in protest activity further underscores the volatile and unpredictable nature of the current international security landscape.

Physical Security Intelligence: United States

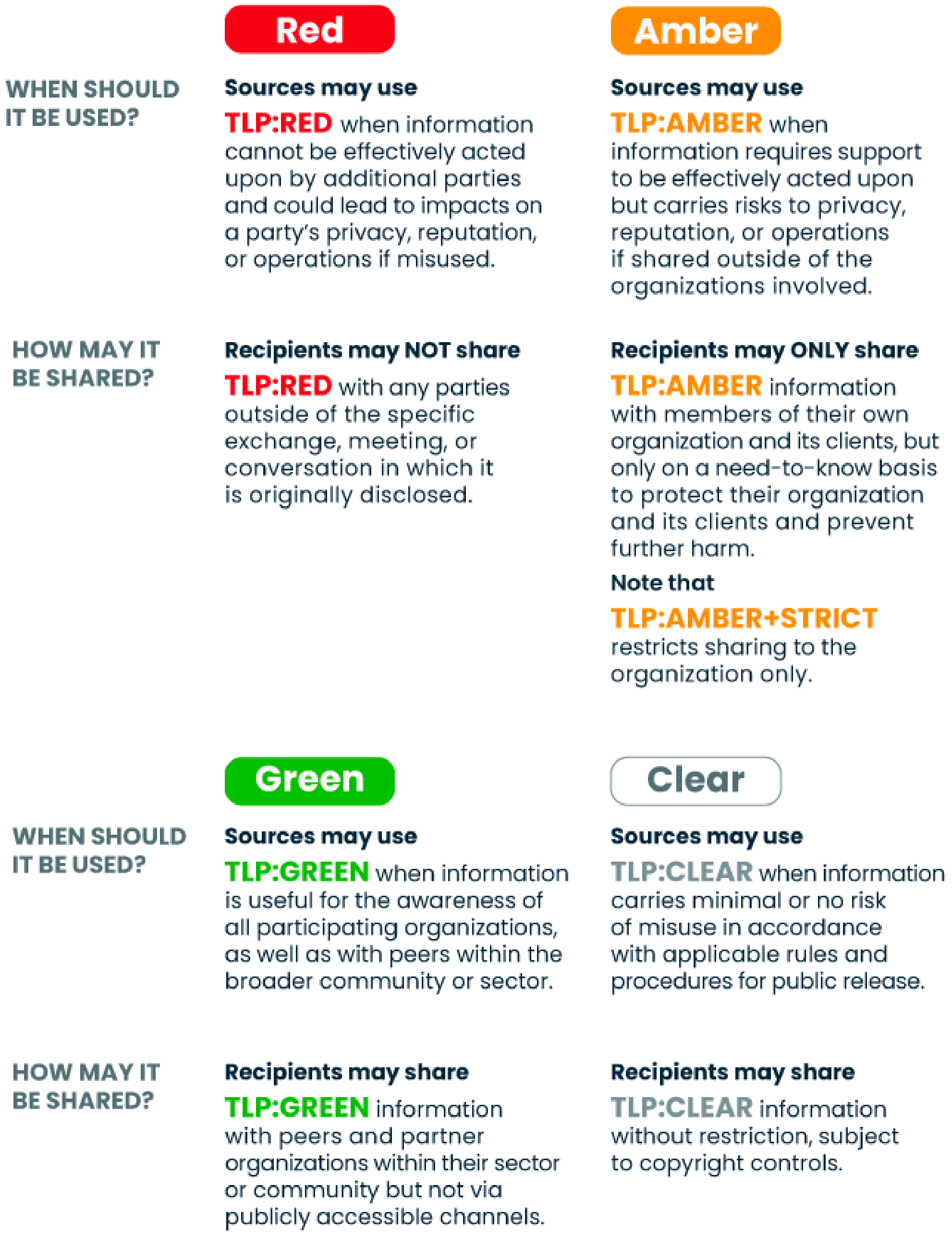


Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, structure fires are fires that affect man-made buildings, and knife attacks are confirmed instances of slashings or stabbings. The top two states that had the most gun violence alerts were Illinois and Texas, which together made up 19 percent of this week's nationwide total. Gun violence across the United States overall increased by 12 percent from the week prior. Knife attack alerts decreased by 3 percent, and the top contributing states were California and New York. Structure fires increased by 12 percent, and the top two states for this subtype were also California and New York. Notably, nationwide protest activity increased by 41 percent.

- **What this means:** This week, gun violence alerts saw an overall increase, with multiple mass shootings occurring between July 19 and July 20, including incidents in Waynesboro, Mississippi (five injured); Chicago, Illinois (four injured); and Cordova, Tennessee (one killed, four injured). While knife attacks saw a small decrease, California and New York were the top contributing states. For example, a triple stabbing, deemed a murder-suicide attempt, occurred in Queens, New York, on July 20, highlighting ongoing individual acts of violence. Structure fires also saw an increase this week, as California continues to battle its wildfire season due to high temperatures and dry climates; for instance, on the afternoon of July 23, several homes were involved in a three-alarm fire in San Jose, causing evacuations. Nationwide protest activity this week saw a sharp increase. This surge includes the "Good Trouble Lives On" protests, held on July 17 in honor of the late civil rights leader John Lewis. These demonstrations—seen in cities like Chicago, Portland, and Houston—protested various Trump administration policies, illustrating how social and political conflicts manifest in widespread public action.

Appendix A: Traffic Light Protocol for Information Dissemination

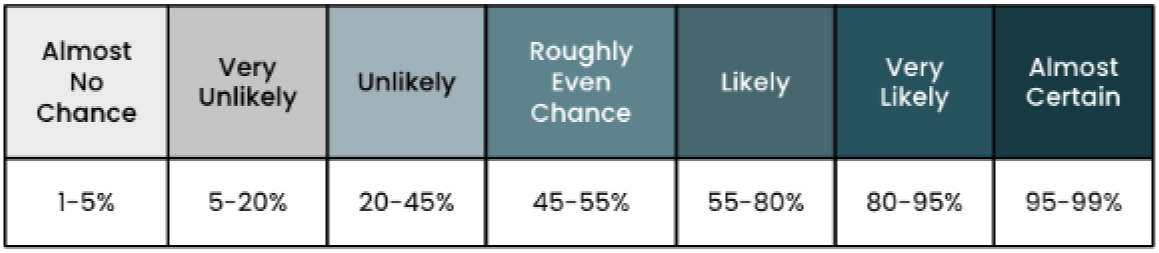


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively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