ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

September 13, 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 (EDT) on September 11, 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

ZeroFox Intelligence Flash Report - Ongoing Nepal Situation Likely to Impact Tourism and Hospitality

In this Flash report, ZeroFox researchers discuss the unrest surrounding Nepal's political situation which is very likely to disrupt transport and logistics, thereby disrupting the flow of trade and operations of local and international businesses.

ZeroFox Intelligence Flash Report – Protest and Government Collapse Likely in France

French Prime Minister François Bayrou's government is almost certain to fall on September 8 over budgetary disputes. Bayrou's unpopular budget proposals have spurred a movement planning massive nationwide protests, starting September 10. Political and social unrest around these demonstrations is expected, but the size and severity of the protests will likely be impacted by whether Bayrou's budget passes. If Bayrou is forced to resign, he will be the third French prime minister removed since 2023, highlighting France's apparent inability to meaningfully address major domestic and international political issues. The political dynamics that created this paralysis are not expected to change for the foreseeable future. Therefore, further short-lived governments are likely, leaving France vulnerable to social unrest.

ZeroFox Intelligence Brief – U.S. Counter-Narcotic Actions in Latin America

The U.S. Department of War (DoW) has likely begun shifting its national security focus toward Latin America, prioritizing the fight against increasingly militarized drug cartels as other global security threats to the United States have reportedly lessened. This shift is marked by recent military actions, including a strike on a suspected Venezuelan drug vessel and the deployment of naval forces to the Southern Caribbean. The Trump administration views Venezuela as a key player in drug transit and as one of the countries most responsible for the lawlessness that has spread across the region in the last five years.

ZeroFox Intelligence Flash Report – Israel Targets Hamas In Qatar

The Israeli military has confirmed that it targeted Hamas officials in Doha, Qatar. Since the beginning of the Israel-Hamas war in October 2023, Israel has steadily broadened the scope of its targeting

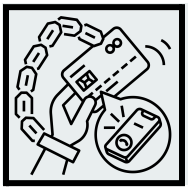
outside the Palestinian territories. Until now, Qatar has been offered some immunity to host internationally recognized terror groups due to its role as an intermediary in peace talks. Hamas representatives have conducted all negotiations abroad, and the targeting of its representatives during ceasefire discussions very likely reduces the possibility of a Gaza ceasefire or hostage release in the near-to-medium term. While a military response from Qatar is very unlikely, diplomatic blowback that further weakens ties between Israel and Middle Eastern states is likely.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 18

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



U.S. Treasury Sanctions Southeast Asian Cyber Scam Networks

What we know:

- The Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned a large network of scam centers across Southeast Asia that steal billions of dollars from Americans using forced labor and violence.
- The sanction targets centers in Shwe Kokko, Myanmar—a notorious hub for virtual currency investment scams under the protection of the OFAC-designated Karen National Army (KNA)—and 10 centers based in Cambodia.
- Many of the targeted centers in Cambodia were built as casinos by Chinese criminal actors, but became hubs for virtual currency investment scams when that activity proved more profitable.
- Additionally, the Department of Justice sentenced an individual to 51 months in federal prison for laundering over USD 36.9 million from U.S. victims in a Cambodia-based digital asset investment scam.

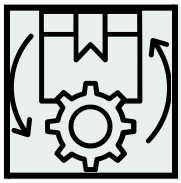
Background:

- Transnational criminal organizations (TCOs) based in Southeast Asia are increasingly targeting Americans through large-scale cyber scam operations.
- A U.S. government estimate reported Americans lost at least USD 10 billion in 2024 to Southeast Asia-based scam operations.
- Burmese scam operators have reportedly lured recruits from around the world under false pretenses, only to detain and physically abuse them, while forcing them to work for crime syndicates as online scammers.
- One of the sanctioned Cambodian entities owns a complex of buildings, including a casino and hotel, from which virtual currency scams and other illegal activities have been carried out, sometimes by victims of human trafficking.

What is next:

- U.S. citizens have faced severe financial losses due to overseas scam centers, with illicit funds funneled back through the American financial system.
- Additionally, the stolen funds could fuel further criminal activity overseas and support organized fraud networks.

- The consequences of cybercrime are not limited to the digital sphere. The sanctioned cyber scam centers have enabled human trafficking and human rights violations.
- Victims of such abuse are very likely to sustain physical and mental damage for the rest of their lives.



Supply Chain Attack Targets Popular Npm Packages with 2.6 Billion Downloads

What we know:

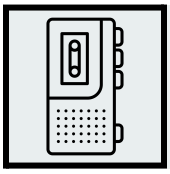
- Npm packages with more than 2.6 billion weekly downloads have been compromised in a supply chain attack.
- Threat actors have injected the packages with malware, following a phishing attack targeting the package maintainer's account.

Background:

- The malware injected into the packages is programmed to intercept cryptocurrency and web3 activity on browsers.
- Once the malware is executed, it hijacks network traffic to redirect crypto transactions to threat actor-controlled wallet addresses.

Analyst note:

- A phishing attack campaign targeting npm package maintainer accounts is likely to continue in the coming weeks.
- Popular JavaScript libraries are very likely to be targeted.
- Crypto holders and crypto organizations using compromised npm packages are likely to be affected and can face financial losses.



Spy Radios Discovered in Inverters and Battery Systems

What we know:

- Undocumented cellular radios have reportedly been discovered in Chinese-manufactured inverters and battery systems powering solar-based highway infrastructure.

Background:

- The power inverters and battery management systems (BMS) are reportedly deployed across highway infrastructure, including electric vehicle (EV) chargers, traffic cameras, weather stations, roadside signs, and warehouses.

Analyst note:

- Hidden radios could enable threat actors to remotely tamper with systems, cause large-scale infrastructure outages, steal data, sabotage roadside systems, and interfere with autonomous vehicle safety.

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 25 Industrial Control Systems (ICS) advisories on September 9 and September 11. CISA has also added one vulnerability to its Known Exploited Vulnerabilities (KEV) catalog. Microsoft's September 2025 Patch Tuesday rolled out fixes for 86 vulnerabilities affecting Windows and other products, with no evidence of active exploitation reported to date. CVE-2025-10088 is a flaw in SourceCodester Time Tracker 1.0 that enables remote cross-site scripting via the project-name parameter in /index[.]html, potentially letting attackers steal session cookies and impersonate users. SAP has released fixes for 21 new vulnerabilities across its products, including three critical flaws affecting the NetWeaver software suite. Adobe has issued a warning about a critical flaw (CVE-2025-54236) dubbed "SessionReaper" in its Commerce and Magento Open Source platforms. CVE-2025-55190 is a critical Argo CD flaw that lets API tokens with minimal project-level permissions access endpoints and retrieve all repository credentials, bypassing isolation protections for sensitive data. Cisco has released patches for three vulnerabilities in its IOS XR software. A zero-click buffer overflow in Apple CarPlay, CVE-2025-24132, allows attackers to gain control without user interaction or authentication.

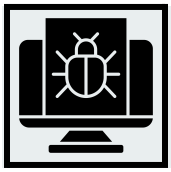
CRITICAL

CVE-2025-53690

What happened: Threat actors have been exploiting a zero-day in legacy Sitecore deployments caused by the reuse of a sample ASP.NET machine key from old Sitecore guides. Knowing this key enabled attackers to craft malicious _VIEWSTATE payloads that triggered deserialization and remote code execution (RCE). This enabled them to deploy WeepSteel reconnaissance malware in active campaigns.

- **What this means:** This vulnerability is not an ASP.NET flaw but a misconfiguration stemming from insecure deployment practices. Exploiting it gives attackers a reliable entry point into vulnerable Sitecore servers. The deployment of WeepSteel indicates that reconnaissance is just the first step and will potentially pave the way for credential theft, privilege escalation, lateral movement, and eventual ransomware or data theft. Organizations running outdated Sitecore versions are at risk of compromise, service disruption, and long-term persistence by advanced threat actors.

- **Affected products:**
  - Sitecore Experience Manager (XM), Experience Platform (XP), Experience Commerce (XC), and Managed Cloud, up to version 9.0



RATING

CVE-2025-42957

What happened: A critical vulnerability discovered in multiple SAP products, including SAP S/4HANA, is already being exploited in the wild. The flaw enables attackers with even low-level user access to bypass security checks and execute malicious code. Successful exploitation can give hackers full control over SAP systems.

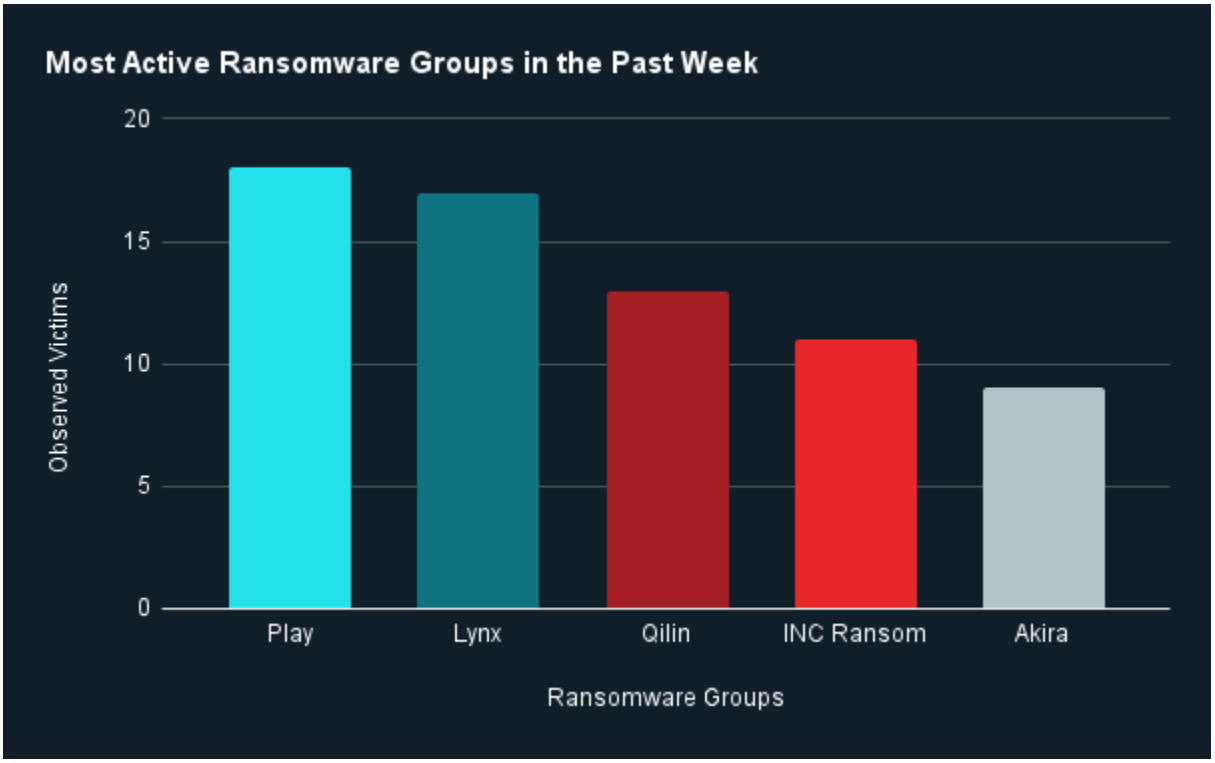
- **What this means:** SAP systems manage core business functions such as finance, supply chain, and operations. Gaining administrator-level access could enable attackers to steal highly sensitive data, disrupt mission-critical processes, and plant persistent backdoors. In worst cases, organizations will likely face large-scale operational shutdowns, financial fraud, or ransomware attacks.
- **Affected products:**
  - SAP S/4HANA (Private Cloud or On-Premise) versions S4CORE 102, 103, 104, 105, 106, 107, and 108

ZEROFOX
Weekly Intelligence Brief

Ransomware and Breach Intelligence

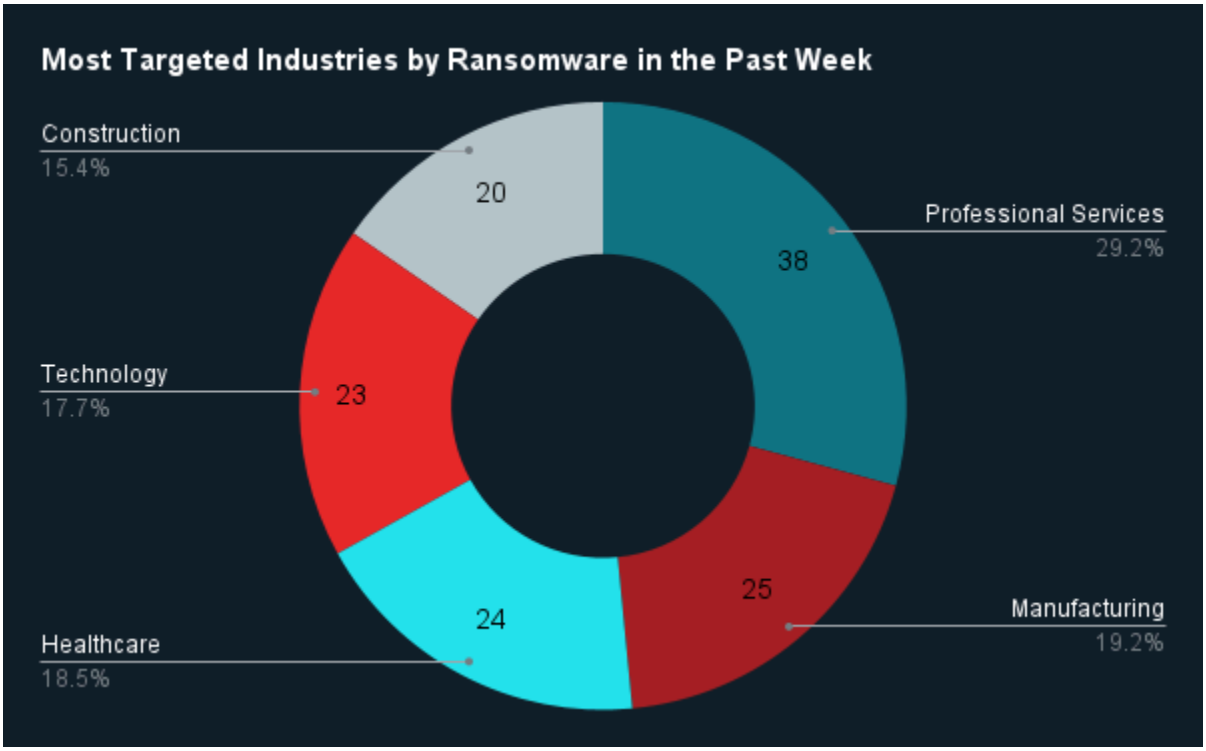
Ransomware and Breach Intelligence Key Findings

Ransomware Groups and Trends



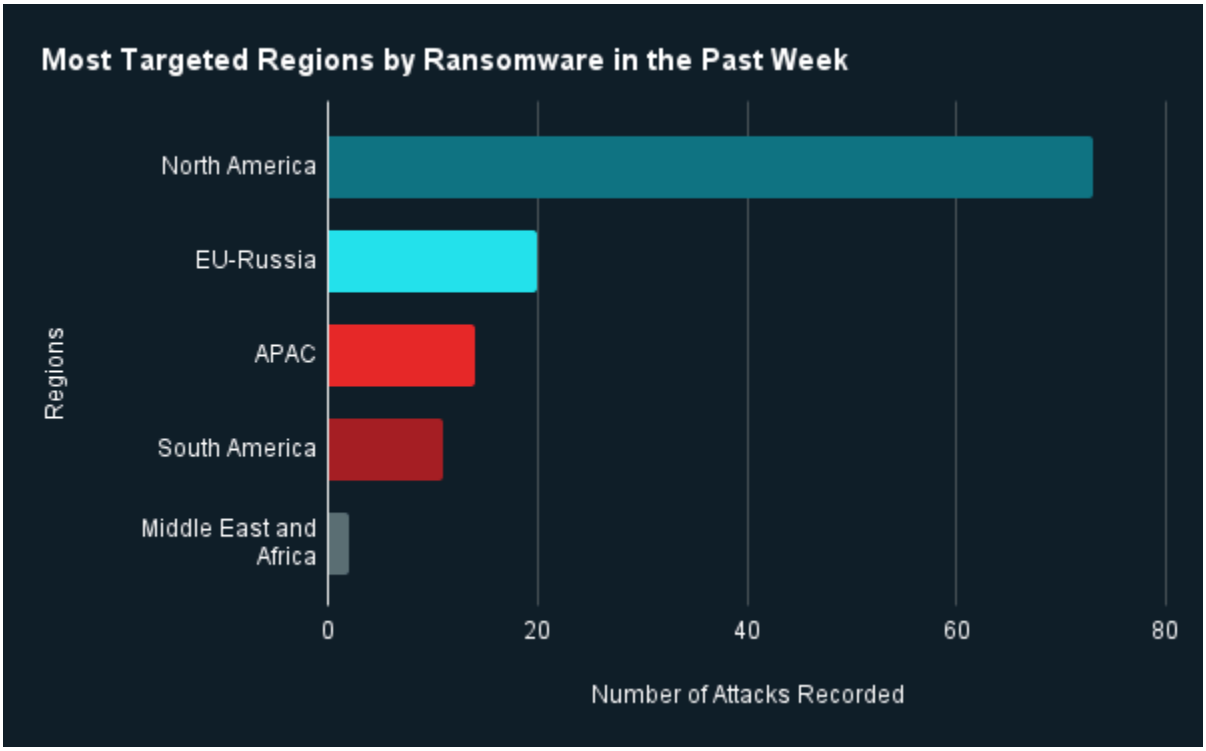
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Play, Lynx, Qilin, INC Ransom, and Akira were the most active ransomware groups. ZeroFox observed at least 100 ransomware victims disclosed, most of whom were located in North America. The Play ransomware group accounted for the largest number of attacks, followed by Lynx.



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.



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 EU-Russia. There were at least 73 ransomware attacks observed in North America, while Europe-Russia accounted for 20, Asia-Pacific (APAC) for 14, South America for 11, and Middle East and Africa for two.

Three Notable Breaches Affecting Customer Data

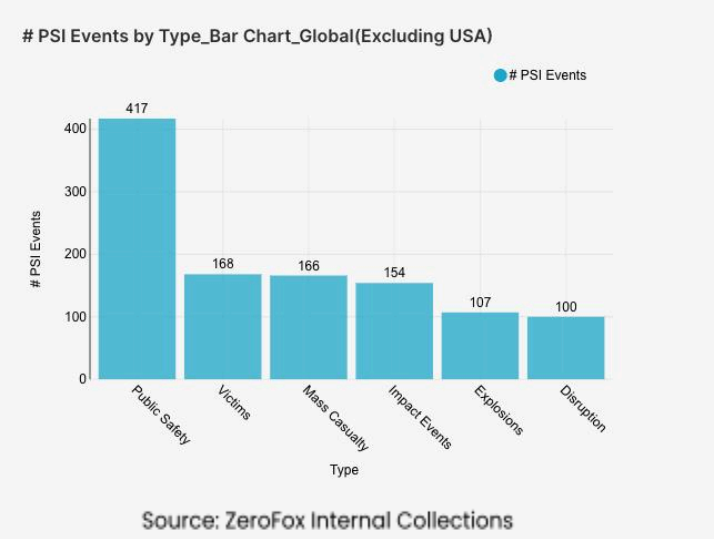
Targeted Entity	Plex	HelloGym	Wayne Memorial Hospital
Impacted Entities	N/A	1.6 million audio recordings	Data of 160,000 patients
Compromised Data Fields	Customer account information, including user names, email addresses, scrambled passwords, and unspecified authentication data	Phone recordings and voicemails containing names, phone numbers, and member requests and communications	Personally identifiable information (PII) such as names, dates of birth, Social Security numbers (SSNs), user credentials, credit card numbers, health insurance information, diagnosis and treatment information, medical history, lab results, and prescription details
Suspected Threat Actor	N/A	N/A	N/A
Country/Region	United States	United States	United States
Industry	Consumer Services	Professional Services	Healthcare
Possible Repercussions	Unauthorized payments, data sold on illegal forums, users locked out of accounts, financial scams, and identity theft	Spear phishing, deepfakes, identity theft, and financial scams	Online and physical stalking, identity theft, financial and insurance fraud, victim intimidation and extortion, and data sale on illegal forums

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

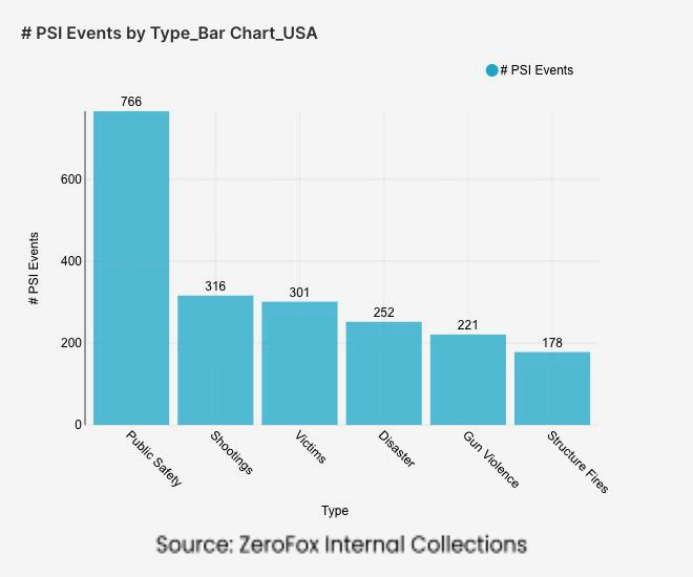


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there has been a significant upsurge in public safety concerns, with around a 24 percent increase compared to the previous week, with the primary contributing countries or regions being Nepal, Sudan, Europe, and the Middle East. The above-mentioned countries and regions accounted for about 21 percent of all public safety alerts. A notable rise in an alerted subtype is shootings, which saw a 29.87 percent increase compared to the past week. An 11.84 percent increase from the past week has been observed in Israel-Hamas conflict activity. There has been an uptick in mass casualty and impact events, including shootings and disasters.

- **What this means:** In Nepal, large acts of vandalism and arson have been committed on governmental institutions, with the country's Prime Minister KP Sharma Oli resigning owing to the unrest, resulting in governmental collapse and the Nepalese Army stepping in to restore law and order. A Russian glide bomb struck a village in Ukraine on Tuesday, 9 September, resulting in at least 24 civilian deaths and injuring 19 others. Furthermore, Poland has accused Russia of escalating North Atlantic Treaty Organization (NATO) conflict tensions after suspected Russian drones entered Polish airspace early on Wednesday, September 10. Lack of machinery and tools, further exacerbated by the ongoing Sudanese conflict, has led to difficulties in recovery operations in Sudan's western Darfur region, which was affected by a landslide on Sunday, September 6. The Israel Defense Forces (IDF) conducted a strike against Hamas officials based in Doha, Qatar, claiming to target the negotiating group for the organization. So far, six deaths have been confirmed, with Hamas claiming five of them as its staff and Qatar declaring the loss of one Qatari security officer. French President Emmanuel Macron has assigned Defence Minister Sébastien Lecornu as France's next Prime Minister, after the forced resignation of François Bayrou due to a failed confidence vote. The current trends point toward considerable escalations of conflicts on multiple international fronts.

Physical Security Intelligence: United States



What happened: In the past week, the top four most-alerted incident subtypes in the United States were public safety, shootings, victims, and disaster. The top two states with the most public safety alerts were Illinois and California, which together made up 22 percent of this week's nationwide total. This was followed by the sub-type structure fires, which are fires that affect man-made buildings.

What this means: This week, conservative activist and Turning Point USA co-founder Charlie Kirk was shot from a distance of approximately 200 yards during an event at Utah Valley University on September 10, 2025, and died shortly thereafter. The 30-hour manhunt for the suspected gunman ended on September 12, over 250 miles away, after a family friend of the suspect alerted authorities. The suspect is now in custody. There are concerns that the political violence in Utah will inspire more unrest. That same day, two students at a Colorado high school were shot by a fellow classmate, who died of self-inflicted injuries. While structure fires decreased by nearly 8 percent this week, California and New York were the states most affected by them.

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%