ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

October 18, 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 October 16, 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 - Scattered Lapsus$ Hunters Announce Temporary Dissolution

Threat collective Scattered Lapsus$ Hunters (SLSH) posted on its Telegram channel on October 11, 2025, that it was ceasing activities until 2026, likely in an effort to reduce law enforcement (LE) scrutiny while retooling and figuring out the group's next steps. SLSH is touting the launch of an EaaS campaign—a growing trend offered by threat collectives—on its Telegram channel. This announcement was posted several hours before the one indicating SLSH was dissolving and is almost certainly indicative of the group's intent to remain a prominent threat collective in the cybercrime landscape throughout 2026 and gain further market share of potential affiliates. The announcement to temporarily dissolve is almost certainly due to increased scrutiny by LE elements. It is very likely SLSH will use the pause to review its operational security and seek ways to avoid further LE disruptions.

ZeroFox Intelligence Flash Report - Rumored New Coalition of Ransomware Groups Yet to Materialize

On September 15, 2025, an account associated with the ransomware and digital extortion (R&DE) collective DragonForce posted on the dark web forum Russian Anonymous Marketplace (RAMP), announcing a coalition with Qilin and LockBit, two other prominent ransomware-as-a-service (RaaS) collectives. In the post, DragonForce explained that the coalition is about uniting efforts as they collaboratively develop their direction—likely meaning that the collectives will assist each other in enhancing their products and services to better serve their affiliates and maximize profits, while also evading law enforcement (LE). Notably, ZeroFox has not observed either Qilin or LockBit publicly confirming or denying the alleged coalition. However, both Qilin and LockBit are known to post only rarely on RAMP. It is unlikely that DragonForce's announcement of a coalition with LockBit and Qilin represents a formalized amalgamation of the three collectives.

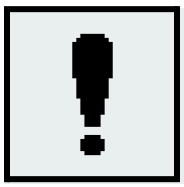
ZeroFox Intelligence Flash Report- Incident Report: U.S. Secretary of War Calls for European-Led NATO

On October 15, 2025, U.S. Secretary of War Pete Hegseth called for a European-led North Atlantic Treaty Organization (NATO). While Hegseth said the United States will continue to fulfill its obligations to NATO, a security alliance created initially after World War II to deter Soviet military aggression in

Europe, he reiterated that a European-led NATO and a strong Ukraine would be the biggest deterrents against Russia, rather than the U.S. military. His comments are likely part of a wider U.S. shift away from spearheading foreign policy commitments abroad and instead relying on the most powerful regional actors to take the lead on their own national security priorities.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Android Users at Risk of New Pixel Attack

What we know:

- A new attack called Pixnapping, a pixel-stealing side-channel attack, enables a malicious app to covertly extract rendered screen content—including two-factor authentication (2FA) codes and other app data—without any special permissions on Android devices. This is done by forcing victim devices' pixels into the system rendering pipeline.
- The technique reportedly works on modern Android versions (demonstrated on Android 13–16) and can enable threat actors to recover sensitive information in under 30 seconds after the victim installs and opens the malicious app.

Background:

- The attack abuses Android intents and the window-blur composition path and then leverages a GPU compression or timing side-channel to measure color-dependent effects and reconstruct individual pixels.
- A flaw, tracked as CVE-2025-48561 and fixed in September, makes Android devices vulnerable to Pixnapping, though researchers have observed a workaround that re-enables Pixnapping.

What is next:

- Since the attack requires no special permissions, threat actors could distribute weaponized apps via third-party stores.
- Threat actors could harvest confidential information, chat histories, and email content without user knowledge.
- Attackers could steal 2FA codes to carry out account takeovers and target email, banking, social media, and crypto accounts to exfiltrate data and establish reconnaissance for targeted phishing, surveillance, or fraud campaigns.

Fake Job Hunters Impersonate Major Job Portal

What we know:

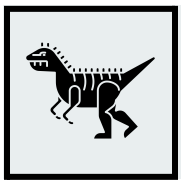
- A phishing campaign has been impersonating a major job platform to target job seekers with fake job offers and steal their login credentials.
- The scam reportedly uses multiple languages and fake recruiter identities to appear legitimate.

Background:

- Victims are lured through emails containing "Book a Call" links that lead to fake Cloudflare pages and spoofed login screens designed to harvest credentials.
- Attackers also use hidden web formatting and newly registered domains to evade email security filters and detection systems.

Analyst note:

- These threat actors are likely to continue to diversify their tactics to refine their phishing kits to mimic more job platforms, impersonate multiple brands, stay undetected for longer, and develop phishing templates for specific industries, roles, and languages.



China-Based Threat Group Weaponizing Open-Source DFIR Tool Velociraptor

What we know:

- A China-based threat group, known as "Storm-2603," is reportedly exploiting Velociraptor, an open-source digital forensics and incident response (DFIR) tool, to carry out ransomware attacks.

Background:

- Storm-2603 is known for deploying Warlock and LockBit ransomware.
- After gaining initial access using On-Premises SharePoint vulnerabilities, the threat group reportedly installs outdated versions of Velociraptor with a privilege escalation flaw (CVE-2025-6264), to communicate with a configured command-and-control (C2) server.

Analyst note:

- Threat actors could exploit this legitimate DFIR tool to escalate privileges, move laterally, harvest credentials, exfiltrate sensitive data, disable and evade defenses, and deploy malware.

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 six vulnerabilities to its known exploited vulnerabilities (KEV) catalog on October 14 and October 15. Additionally, CISA released fourteen Industrial Control Systems (ICS) advisory on October 14 and October 16. It also released an advisory warning that a nation-state threat actor is exploiting vulnerabilities in F5 devices and software, which could enable attackers to access credentials, API keys, and sensitive data, potentially compromising federal networks. Microsoft's October 2025 Patch Tuesday delivers fixes for 172 vulnerabilities, including six zero-day flaws. The October 2025 Patch Tuesday also prompted security advisories from major ICS and Operational Technology (OT) vendors, such as Siemens, Schneider Electric, Rockwell Automation, ABB, Phoenix Contact, and Moxa. Fortinet and Ivanti have also released their October 2025 security updates, addressing multiple vulnerabilities across various products. Adobe announced patches for over 35 vulnerabilities across its products, including a critical-severity flaw (CVE-2025-49553) in the Adobe Connect collaboration suite. SAP has released 13 new security notes and four updates to previously released security notes as part of its October 2025 Security Patch Day. Threat actors are exploiting CVE-2025-11371, a zero-day flaw in Gladinet CentreStack and Triofox that allows unauthenticated local access to system files. Researchers have disclosed two critical flaws (CVE-2023-40151 and CVE-2023-42770) in Red Lion Sixnet RTU devices, which could enable code execution with highest privileges if exploited. Operation Zero Disco is an active campaign exploiting CVE-2025-20352, a critical Cisco SNMP flaw, to install Linux rootkits and gain persistent remote access to vulnerable network devices. A command injection vulnerability (CVE-2025-9976) has been discovered in the Station Launcher App of Dassault Systèmes' 3DEXPERIENCE platform. Microsoft has patched a critical ASP[.]NET Core vulnerability in the Kestrel web server component that enabled attackers to bypass security mechanisms. Several recently patched vulnerabilities in Fuji Electric's V-SFT product could enable attackers to gain unauthorized access to industrial systems.

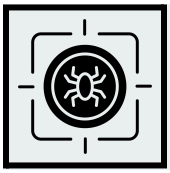
HIGH

CVE-2025-61884

What happened: Oracle has released a security alert for this vulnerability in Oracle E-Business Suite (EBS) that can be exploited remotely without authentication. The flaw enables attackers to

gain access to sensitive resources over the network and has already been actively exploited in the wild.

- **What this means:** Anyone with network access could exploit vulnerable Oracle EBS systems without needing login credentials. Organizations running affected versions are advised to immediately apply Oracle's out-of-band patch or mitigation steps to prevent data exposure and system compromise. Successful exploitation could lead to data theft, exfiltration, or extortion attempts.
- **Affected products:**
  - Oracle EBS versions from 12.2.3 through 12.2.14



CRITICAL

CVE-2025-5947

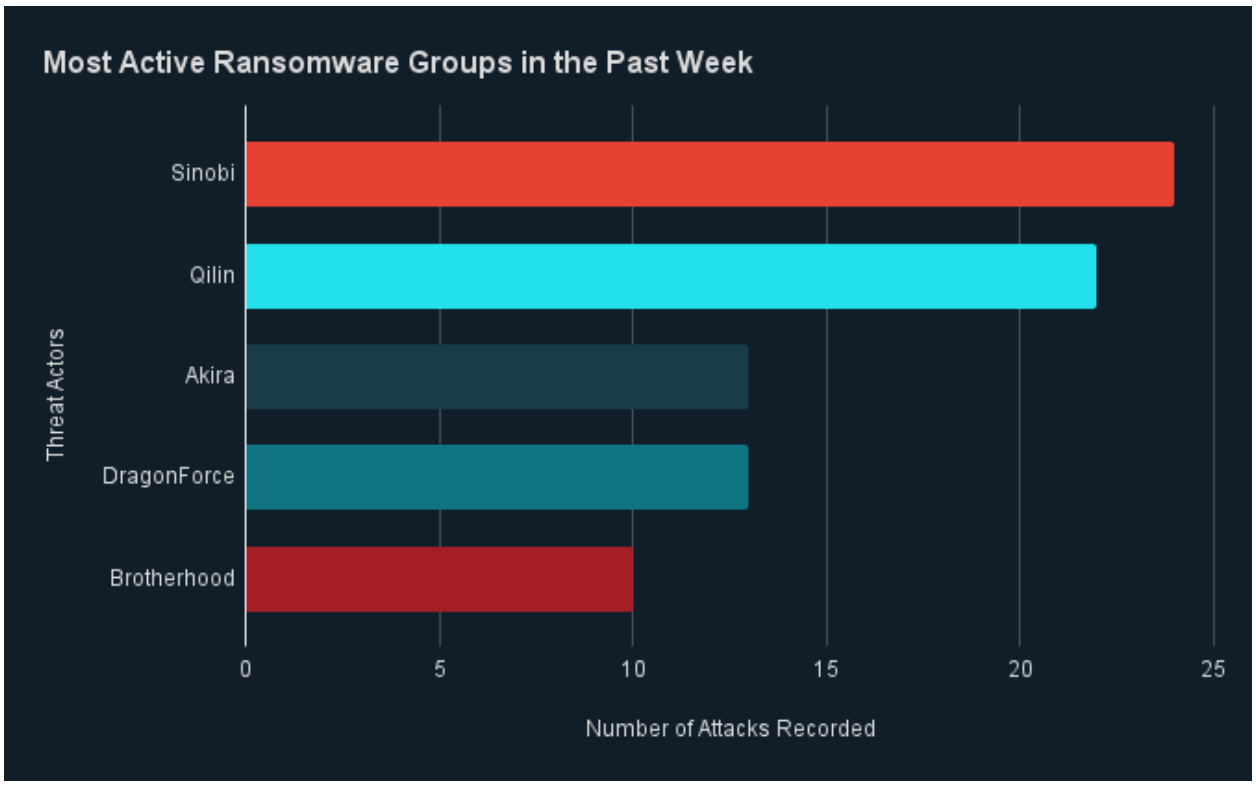
What happened: An authentication bypass vulnerability that enables attackers to log in as any user, including administrators, was discovered in the bundled plugin of the Service Finder WordPress theme. Threat actors are exploiting this flaw to hijack vulnerable websites.

- **What this means:** This vulnerability allows complete takeover of affected WordPress sites without authentication, enabling attackers to inject malicious code, redirect visitors to phishing pages, or host malware. Since exploitation is active, website owners using the Service Finder theme are recommended to immediately update or disable the vulnerable plugin, reset admin credentials, and scan for indicators of compromise to prevent further abuse.
- **Affected products:**
  - All Service Finder Bookings versions till 6.0

Ransomware and Breach Intelligence

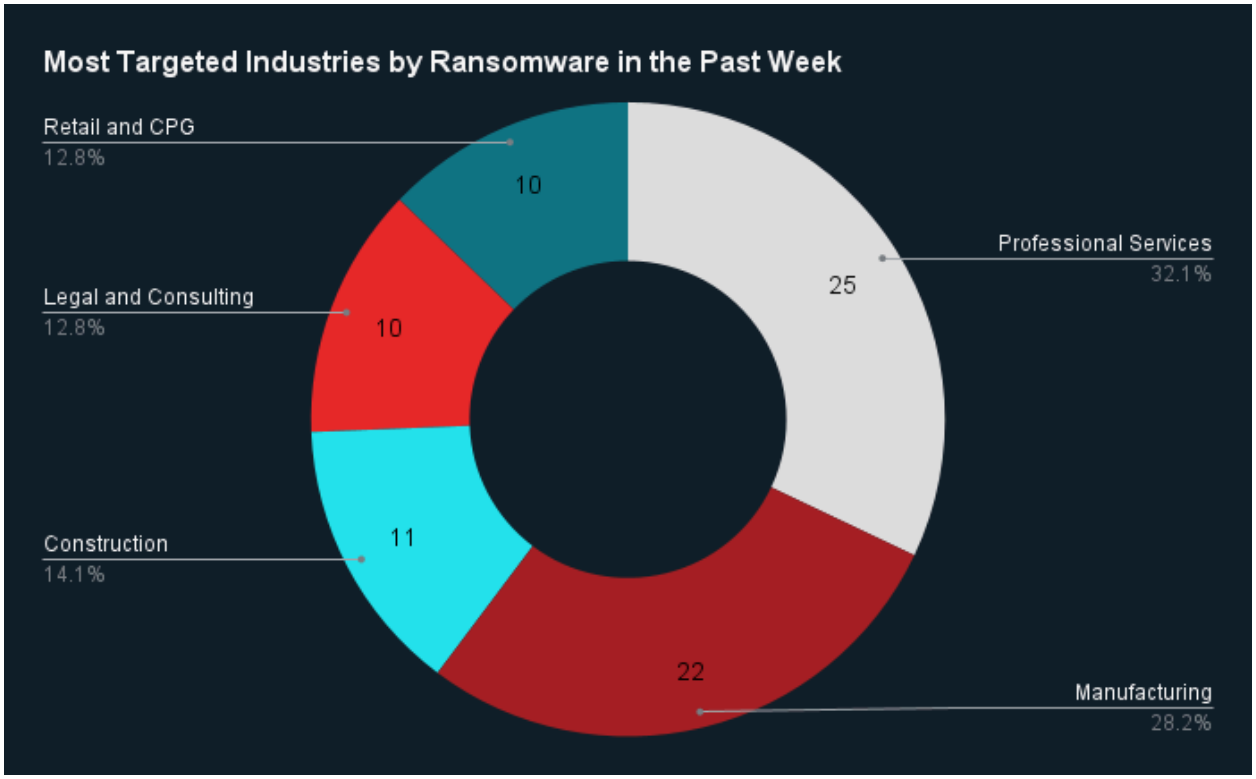
Ransomware and Breach Intelligence Key Findings

Ransomware Trends: Threat Groups, Industries, and Regions



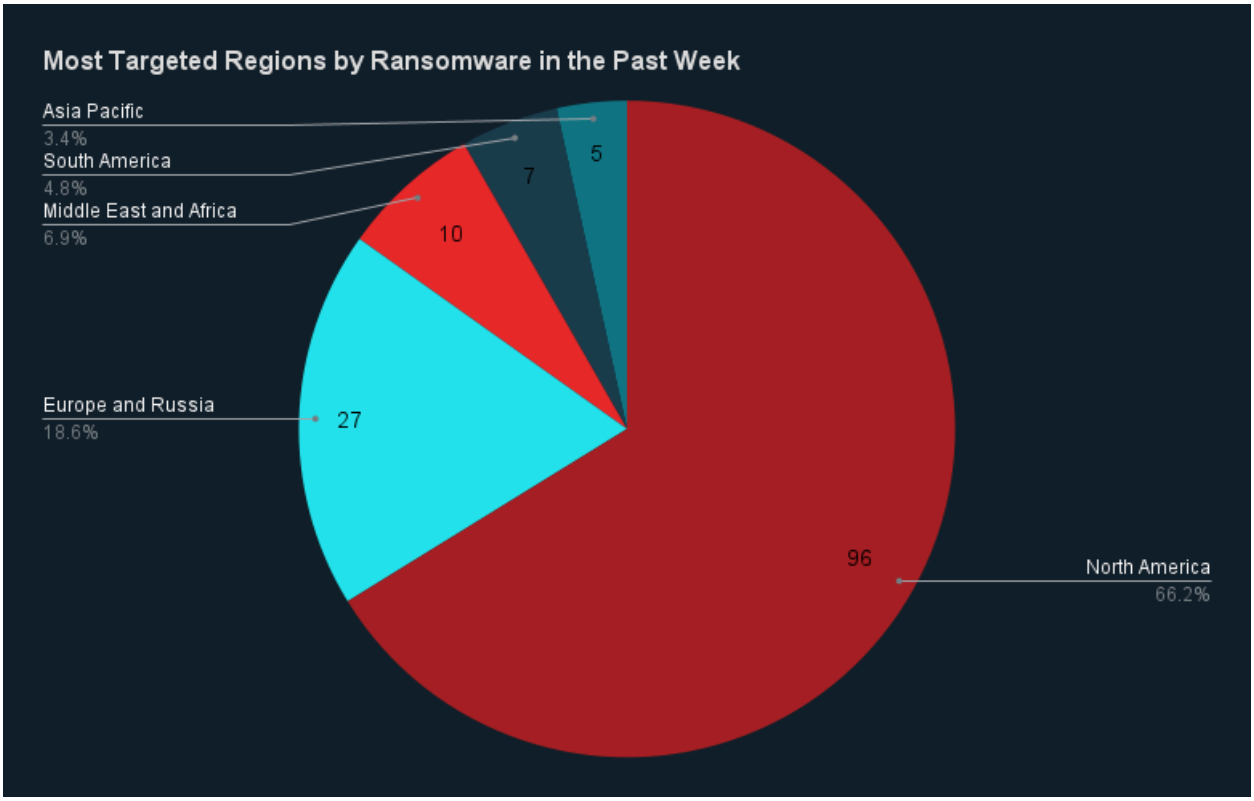
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Sinobi, Qilin, Akira, DragonForce, and Brotherhood were the most active ransomware groups. ZeroFox observed close to 139 ransomware victims disclosed, most of whom were located in North America. The Sinobi 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 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 Europe and Russia. There were at least 96 ransomware attacks observed in North America, while Europe and Russia accounted for 27, Middle East and Africa for 10, South America for seven, and Asia-Pacific (APAC) for five.

Recap of major ransomware events observed in the past week: Earlier this week, ZeroFox observed an uptick in Qilin ransomware's victim claims on its leak site. As of October 15, 2025, the group has disclosed nearly 60 victims. ZeroFox also observed R&DE collective DragonForce announcing a coalition with Qilin and LockBit ransomware groups. A China-based threat groupStorm-2603 is reportedly exploiting Velociraptor, an open-source DFIR tool, to carry out ransomware attacks.

Data Breaches Reported in the Past Week

Targeted Entity	SimonMed	Qantas Airways	MANGO
Compromised Entities/victims	1,275,669 individuals	Over a million customers	Customers
Compromised Data Fields	Personally identifiable information (PII) of individuals, including protected health data, diagnosis, health insurance information, and driver's license numbers	PII including phone numbers, birth dates, and home addresses	First names, emails, contact details, and postal codes
Suspected Threat Actor	Medusa ransomware group (unconfirmed)	Scattered Lapsus$ Hunters	N/A
Country/Region	United States	Global	N/A
Industry	Healthcare	Transportation	Retail and CPG
Possible Repercussions	Phishing, social engineering, identity theft, and insurance fraud	Phishing, ransom demand from the affected company, and fraud	Phishing and ransom demand from the affected company

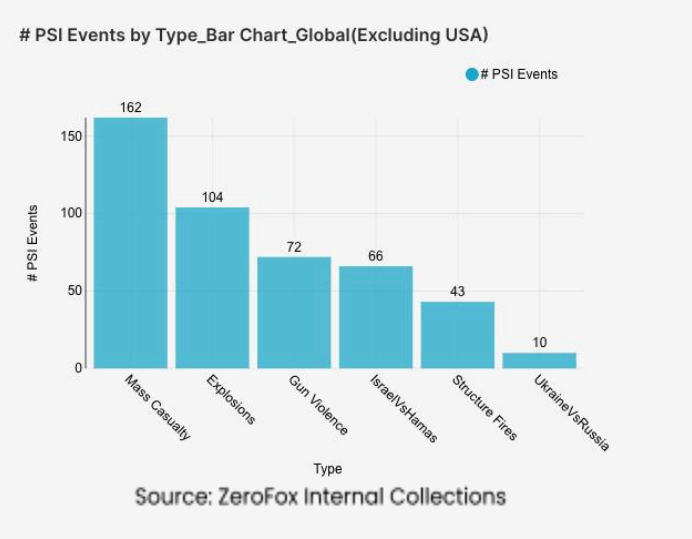
Three major breaches observed in the past week

Other major data breaches observed in the past week: UK-based outsourcing and professional services company Capita has been fined EUR 14 million (approx. USD 18.7 million) for a 2023 data breach incident that exposed the personal information of 6.6 million people. Threat group Crimson Collective offered to sell 570 GB of compressed data allegedly exfiltrated from Red Hat for USD 400,000– 500,000. Threat collective Scattered Lapsus$ Hunters has published sample data

sets, allegedly exfiltrated from six organizations, on its leak site; Vietnam airlines and Qantas airways are among the six listed organizations. UK trade union Prospect has notified its members of a data breach that has reportedly exposed their names, contact details, birth dates, disabilities, employment information, and more.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

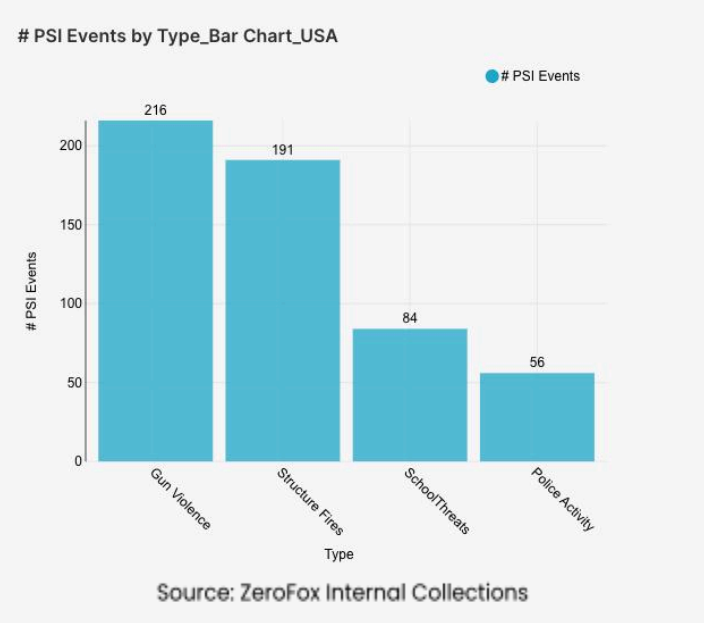


Physical Security Intelligence: Global

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 Pakistan, India, and Mexico, in that order. Approximately 64 percent of these events were explosions, and the three aforementioned territories and countries accounted for about 34 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) decreased by 47 percent from the previous week. Events related to Russia's war in Ukraine decreased by 29 percent. The top three most-alerted subtypes were explosions, which saw a 14 percent increase from the previous week; gun violence, which decreased by 8 percent; and structure fires, which decreased by 16 percent.

- **What this means:** This week's data highlights the volatility of global physical security, with violence concentrated in a few key areas. For example, recent mass casualties in Pakistan, sparked by heavy shelling and retaliatory airstrikes along the Afghanistan-Pakistan border on October 15, killed dozens of soldiers and civilians. Both countries later agreed to a temporary ceasefire, but fears of a full-blown conflict continue to concern citizens. Explosions increased this week, with India being a top contributor due to Diwali festivities causing fire hazards; for instance, nine people were injured in an explosion on October 15 at the house of a firecracker trader in Sultanpur, Uttar Pradesh. Conversely, alerts related to major protracted conflicts saw notable decreases, with the most dramatic decline in alerts happening with the Israel-Hamas dispute. A U.S.-brokered ceasefire deal between Israel and Hamas was implemented on October 10, leading to an exchange of hostages and prisoners, and ultimately a pause in hostilities. However, on October 16, a senior Hamas official accused Israel of flouting the ceasefire by killing at least 24 people in shootings since the start of the ceasefire. As of now, both the Afghanistan-Pakistan and Israel-Hamas peace agreements are intact but fragile.

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 Pennsylvania, 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 decreased by 31 percent, and the top contributing states were California and Colorado. Structure fires increased by 2 percent, and the top two states for this subtype were California and New York. Domestic protest activity increased by 6 percent.

- **What this means:** Criminal incidents remain a central public safety concern this week, and despite an overall decrease in gun violence incidents, there have been seven mass shootings in the United States within the last seven days. One such instance on October 12 occurred as part of an ongoing feud in Saint Helena Island, South Carolina and resulted in 20 people shot, of which four were reported dead; another shooting, which resulted in six dead and 10 injured, happened in Leland, Mississippi after a high school homecoming on October 10. Domestic protest activity increased in the past week, signaling a rise in public action. For example, local activism against the Israel-Hamas conflict has been a consistent source of recent protest activity, with groups planning weekly vigils and demonstrations in multiple cities. Meanwhile, a much larger "No Kings Day 2.0" movement against the current administration is scheduled to take place on October 18, with organizers expecting millions to rally across the country. The latest round of protests comes amid growing frustration about the ongoing government shutdown and opposition to President Trump's military crackdown on Democratic-led cities across the United States. The overall domestic security landscape remains active, marked by ongoing violence and a distinct increase in domestic political protests.

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%