ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

October 11, 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 9, 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- Incident Report: Israel-Hamas Agree to Parts of New Ceasefire

Israel and Hamas agreed to the first phase of a ceasefire, which will see the remaining Israeli hostages held in Gaza freed by October 13, 2025. While this phase is likely to proceed as planned, there is only a roughly even chance that the remainder of the deal will go forward. The remaining parts of the deal contain likely unpalatable elements for both Israel and Hamas, including Hamas' disarmament and the delineation of a pathway to the creation of a Palestinian state.

ZeroFox Intelligence Assessment - Q3 2025 Ransomware Wrap-up

ZeroFox observed at least 1,429 separate ransomware and digital extortion (R&DE) incidents in Q3 2025, a slight increase of nearly 5 percent from Q2 and a drop of approximately 27 percent from the record-breaking 1,961 incidents observed in Q1 2025. By Q3 2025, the professional services industry had already experienced at least 510 attacks, surpassing the 462 incidents recorded in all of 2024—a nearly 10.4 percent increase year-over-year, with the pace suggesting up to a 47 percent increase by year end if current trends continue. The increased targeting of professional services organizations is likely driven by the industry's substantial growth in recent years, partly due to the need for niche specialized expertise, as well as the digitization of businesses globally. This, in turn, highlights vulnerabilities to the professional services industry and its clients. ZeroFox assesses that the five most active R&DE collectives in Q3 2025 were almost certainly Qilin, Akira, INC Ransom, Play, and SafePay. This is notably similar to Q2 2025—wherein the top five was composed of the same collectives—with some minor shifts.

Ransomware and Government Protected Manufacturing Jobs

The ZeroFox Q3 Ransomware report found that the manufacturing sector was once again the most popular target for ransomware and digital extortion (R&DE) attacks, with the United States and Europe the most popular locations for attacks. This is despite the sector making up a decreasing share of economic output in those regions, as manufacturing jobs have shifted to Asia. The sector's low tolerance for downtime, complex supply chains, reliance on third-party vendors, and digitization of work sites are likely behind the rise. However, there is a roughly even chance that U.S. and European prioritization of the sector—via tariffs to specifically protect domestic manufacturing jobs or government bailouts to domestic manufacturing firms affected by cyber intrusions—is incentivizing threat actors.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 20

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

Salesforce Notifies Customers It Will Not Pay Hacker Ransom

What we know:

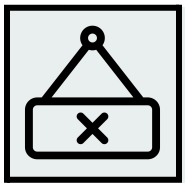
- Salesforce reportedly told its customers in an email on October 7 that it would not pay a ransom to hackers who claimed to have stolen client data and are threatening to leak it.
- Salesforce has reportedly received "credible threat intelligence" that indicates the threat actors were planning to leak data stolen in an earlier security incident.

Background:

- Salesforce has reportedly obtained “credible threat intelligence” that the hackers are preparing to leak data stolen in an earlier breach.
- On October 3, 2025, ZeroFox observed the emergence of the Scattered Lapsus$ Hunters threat collective’s new leak site.
- The collective claims to have exfiltrated listed victims’ data via the recent Salesforce breach. The listed victims have been given a ransom deadline of October 10, 2025.

What is next:

- If the hackers’ claims are true, without ransom negotiations, they are likely to contact or extort affected Salesforce customers directly, leak portions of the stolen data, or sell the dataset to other criminal groups to maintain leverage.
- Downstream companies of impacted Salesforce clients are likely to face double extortion, ransomware, and other financially motivated attacks



BreachForums[.]hn Seized in Joint International Law Enforcement Operation

What we know:

- BreachForums[.]hn has been officially seized by law enforcement, with its clear net and onion domains now displaying a joint seizure notice from the DOJ, FBI, and French agencies BL2C and JUNALCO.

Background:

- The takedown occurred as Scattered Lapsus$ Hunters was preparing to leak data from 39 Salesforce customers after a ransom demand, with a payment deadline set for October 10.

Analyst note:

- The takedown will likely delay or prevent the release of sensitive data tied to Salesforce customers briefly. Members of BreachForums and groups like Scattered Lapsus$ Hunters are likely to regroup under new domains or aliases and could also turn to other underground forums to publish the stolen data.

Chinese Cybercrime Group UAT-8099 Exploits Enterprise Web Servers for SEO Fraud

What we know:

- Chinese-language group UAT-8099 is exploiting popular enterprise web servers to steal credentials, configuration files, and certificates while manipulating search rankings for search engine optimization (SEO) fraud.
- Incidents have been reported across multiple regions, including India, Thailand, Vietnam, Canada, and Brazil.

Background:

- Active since April 2025, the group targets high-value enterprise web servers used by universities, telecoms, and tech firms and deploys web shells, BadIIS malware, and Cobalt Strike to maintain persistence and enable remote desktop access.

Analyst note:

- These intrusions enable large-scale SEO abuse, credential theft, and potential lateral movement into enterprise networks. Stolen certificates and configurations could be weaponized for supply chain impersonation, phishing, or code-signing attacks.

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) released two Industrial Control System (ICS) advisories on October 7. CISA also added eight vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on October 6 and October 7. CVE-2025-53967 is a now-patched command-injection vulnerability in Figma's developer MCP server, enabling remote code execution (RCE). CVE-2025-42706 and CVE-2025-42701 are vulnerabilities in the Falcon sensor for Windows that could enable an attacker with prior code execution access to delete arbitrary files—one due to a logic error, the other due to a race condition. CrowdStrike has patched both these vulnerabilities. CVE-2025-49844 is a critical Redis vulnerability in builds involving Lua scripting that can enable RCE but requires authenticated access; patches are available. Google has patched 21 vulnerabilities in Chrome 141, including two high-severity heap buffer overflows (CVE-2025-11205 and CVE-2025-11206) affecting WebGPU and Video components. Patches have been issued for CVE-2025-36604, a flaw in Dell UnityVSA that enables unauthenticated attackers to execute arbitrary commands via improper input handling in login redirection. DrayTek has warned of a flaw (CVE-2025-10547) in several Vigor router models that enables unauthenticated attackers to send crafted HTTP/HTTPS requests to the WebUI, causing memory corruption, crashes, and—in some cases—RCE.

CRITICAL

CVE-2025-61882

What happened: CVE-2025-61882 is a critical, unauthenticated, remotely exploitable flaw in Oracle E-Business Suite's Concurrent Processing component that enables attackers with network access via HTTP to take control of affected systems. Oracle has released an emergency update to patch the vulnerability.

- **What this means:** The security patch comes following reports of threat actor FIN11—linked to Cl0p ransomware—exploiting it in an alleged extortion campaign. However, Oracle has not confirmed whether the vulnerability is linked to the extortion campaign or if it was a zero-day flaw.
- **Affected products:**
  - Oracle E-Business Suite's Oracle Concurrent Processing 12.2.3 through 12.2.14

CRITICAL

CVE-2025-10035

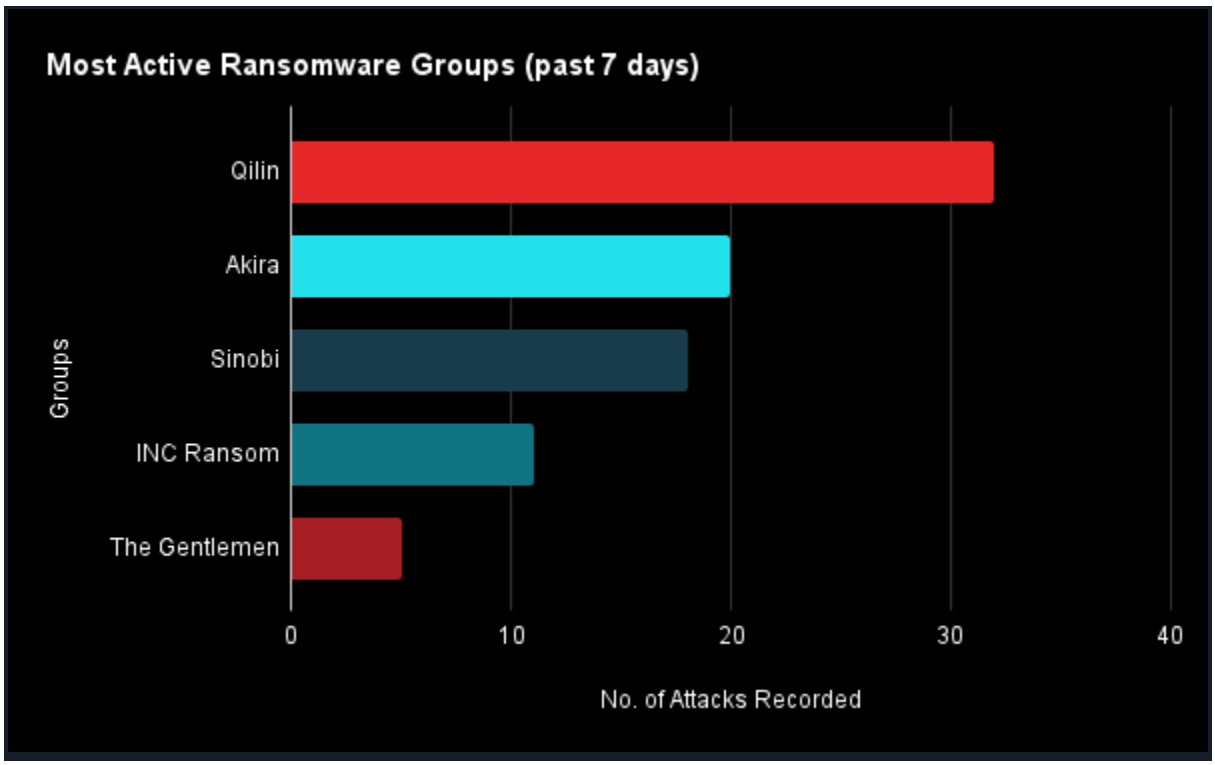
What happened: This deserialization vulnerability in Fortra's GoAnywhere MFT product has been actively exploited by Storm-1175, a cybercrime group linked to Medusa ransomware. Threat actors exploited the flaw to execute commands, maintain persistence, and deploy ransomware on compromised systems.

- **What this means:** The exploitation involved abusing the License Servlet to deserialize attacker-controlled Java objects, enabling RCE, lateral movement, and data exfiltration. Researchers have observed multiple organizations targeted, with attackers using Remote Monitoring and Management (RMM) tools, network discovery, and Cloudflare tunnels to maintain control and ultimately deploy Medusa ransomware.
- **Affected products:**
  - Fortra's GoAnywhere MFT versions 0 through 7.8.3

Ransomware and Breach Intelligence

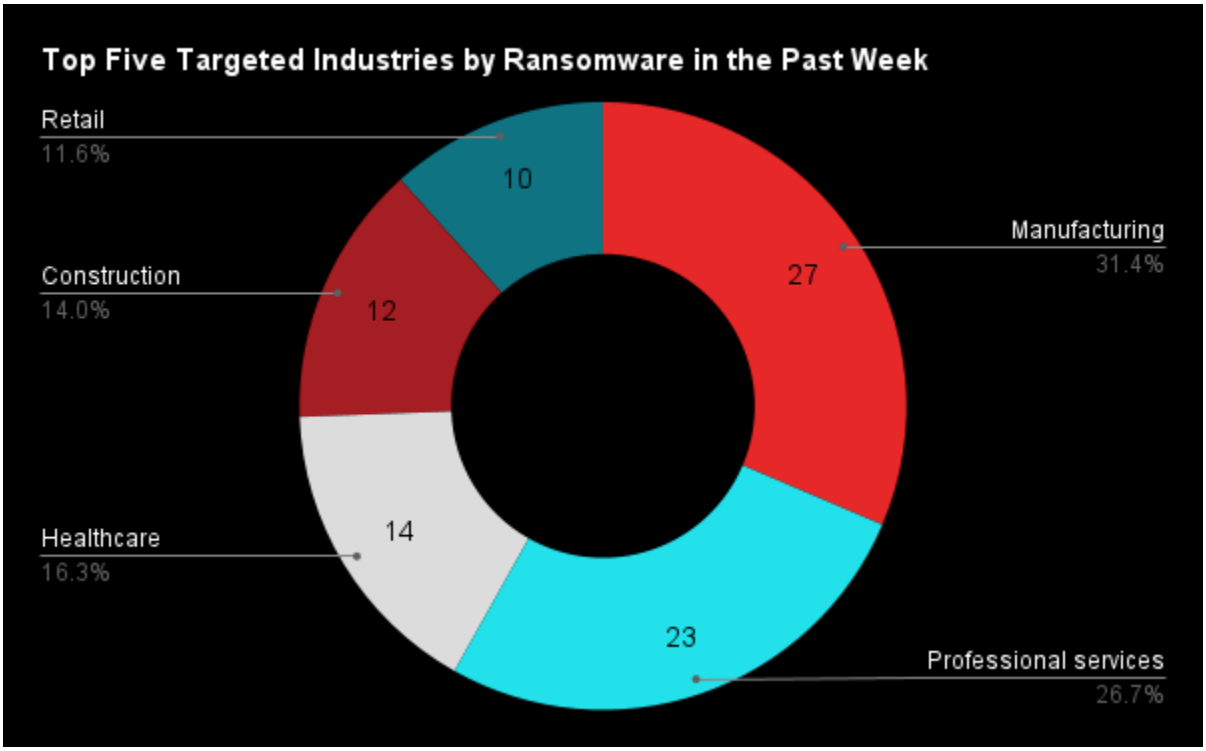
Ransomware and Breach Intelligence Key Findings

Past Week Ransomware Activity Update



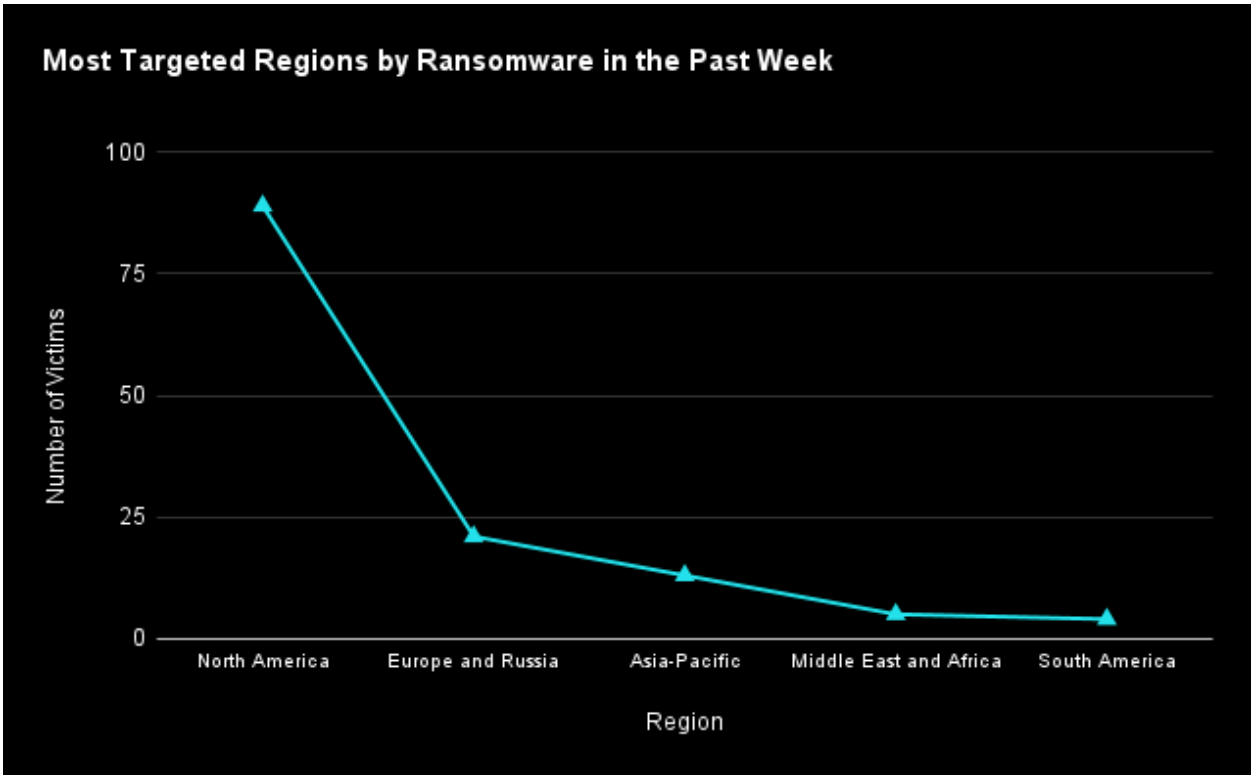
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Akira, Sinobi, INC Ransom, and The Gentlemen were the most active ransomware groups. ZeroFox observed close to 132 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Akira.



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.



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 89 ransomware attacks observed in North America, while Europe and Russia accounted for 21, Asia-Pacific (APAC) for 13, Middle East and Africa for five, and South America for four.

Recap of major ransomware events observed in the past week: Medusa ransomware affiliates are reportedly exploiting a previously patched critical deserialization vulnerability (CVE-2025-10035) in Fortra's GoAnywhere MFT software to obtain initial access. Qilin ransomware group has taken responsibility for the cyberattack on Japanese beer giant Asahi, listing the company among its victims on its data leak site. DragonForce, LockBit, and Qilin have announced a ransomware alliance, which is believed to be an effort by these financially motivated actors to strengthen and coordinate their ransomware operations.

Major Data Breaches in the Past Week

Targeted Entity	Discord	Red Hat	BK Technologies
Compromised Entities/victims	5.5 million users	570 GB of customer data from 28,000 internal GitLab repositories	Yet to be disclosed
Compromised Data Fields	Names, emails, IP addresses, support messages, attachments, and photos of government-issued IDs	800 Customer Engagement Reports (CERs) containing sensitive customer network and infrastructure details.	Non-public information, including records of current and former employees
Suspected Threat Actor	Unknown	Crimson Collective	Unknown
Country/Region	Global	United States	United States
Industry	Communication	Technology	Manufacturing
Possible Repercussions	Phishing attack, account takeover, credential stuffing, SIM swapping, identity theft, doxxing, extortion, blackmail, business email compromise (BEC) attack, malware distribution via malicious attachments, and impersonation	Phishing and social engineering attacks, BEC, credential stuffing, account takeover, supply chain compromise, ransomware, extortion or blackmail, and impersonation	Phishing and social engineering attacks, BEC, credential stuffing, account takeover, SIM swapping, identity theft, impersonation, and doxxing

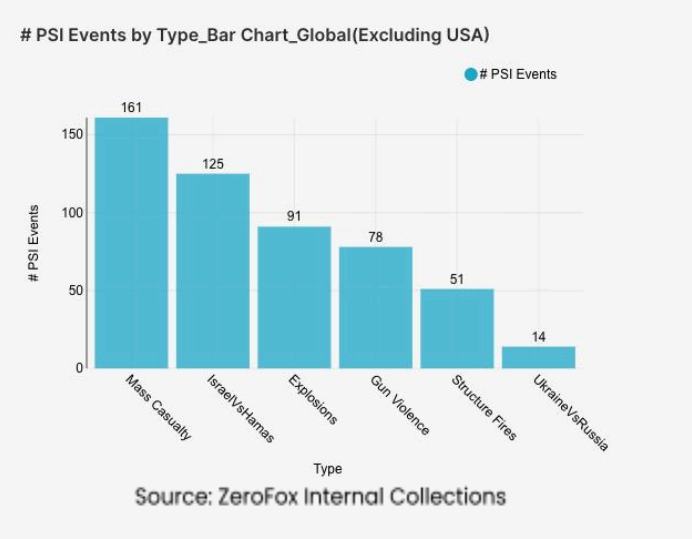
Three major breaches observed in the past week

Other major data breaches observed in the past week: Electronics distributor Avnet confirmed it experienced a data breach but clarified that the stolen information cannot be read without the use of proprietary tools. Williams & Connolly disclosed that Chinese hackers breached parts of its network in a wider campaign targeting U.S. law firms. The FBI's Washington field office is

investigating related intrusions affecting over a dozen firms and tech companies. Renault has suffered a data breach stemming from a third-party incident, with Scattered Lapsus$ Hunters recently claiming responsibility for the breach.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

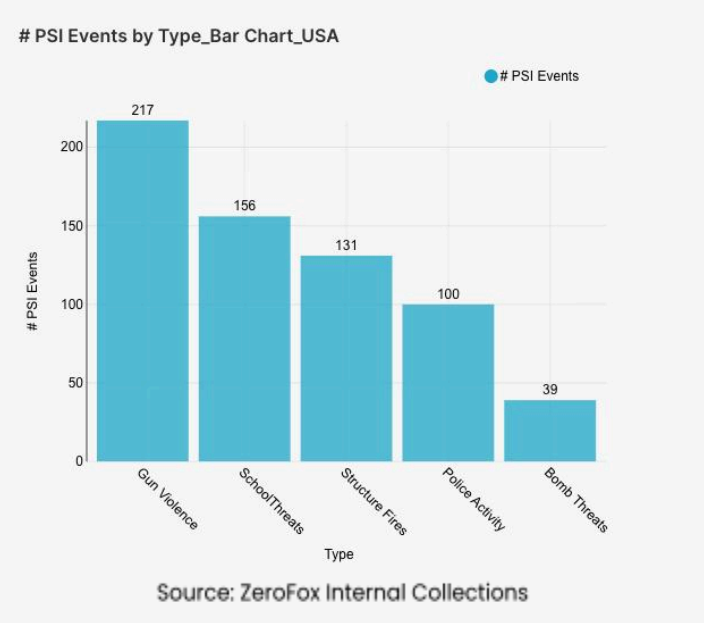


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 6 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, India, and Mexico, in that order. Approximately 57 percent of these events were explosions, and the three aforementioned territories and countries accounted for about 36 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 250 percent. The top three most-alerted subtypes were explosions, which saw a 7 percent decrease from the previous week; gun violence, which increased by 3 percent; and structure fires, which decreased by 4 percent.

- **What this means:** Despite a slight decrease in total mass casualty events globally during the reporting week, geopolitical instability intensified sharply within certain conflict zones such as Ukraine and Russia. This spike is exemplified by the recent, geographically widespread long-range missile and drone attacks by Ukraine on Russian assets, as well as a Russian drone attack on Odesa that killed five people, injured 19, and caused a mass power outage and fire on October 9. Furthermore, general alerts related to the Israel-Hamas conflict saw an increase despite both agreeing to the initial phase of a ceasefire deal on October 9, which followed reports of continuous Israeli strikes in Gaza that killed at least eight people in the 24 hours prior to the announcement. India had the second highest number of mass casualty alerts and contributed to explosion alerts overall; for instance, on October 8, eight people were injured following an explosion in a Kanpur marketplace due to illegal storage of firecrackers. All of these examples indicate that global physical security is becoming more intensely concentrated in pre-existing conflict zones, with high-casualty events such as explosions serving as the consistent primary threats to civilian safety worldwide.

Physical Security Intelligence: United States



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 New York, which together made up 22 percent of this week's nationwide total. Gun violence across the United States overall increased by 11 percent from the week prior. Police activity alerts decreased by 19 percent, and the top contributing states were Pennsylvania and California. Structure fires increased by 44 percent, and the top two states for this subtype were California and New York. Notably, protest activity increased by 20 percent.

- **What this means:** The overall spike in crime this week is partially exemplified by the persistent gun violence in top contributing states such as Illinois, where weekend shootings recently left five dead and 25 wounded in Chicago alone. There were five mass shootings in the United States within the last seven days, including one in Montgomery, Alabama, that left two dead and 12 injured. This trend is compounded by a surge in disaster and man-made risk: structure fires dramatically increased, with major incidents such as the recent Chevron refinery fire in El Segundo, California, on October 2. Furthermore, protest activity increased significantly, propelled by major civic unrest, such as the large-scale pro-Palestine demonstration in New York that led to arrests on October 2 and the ongoing anti-immigration crackdown protests in Chicago, which necessitated the deployment of the Texas National Guard. Overall, the concentration of alerts in crime and man-made disasters, coupled with a surge in domestic protest activity, indicates that US physical security risks are shifting from general public threats to specific flashpoints of violence, structural vulnerability, and deep political polarization.

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%