



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

October 10, 2026

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 8, 2026*; 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 Assessment – September 2026 Ransomware Wrap-Up	
Monthly Geopolitical Report October 2026	2
 Cyber and Dark Web Intelligence Key Findings	4
PoeLLM Malware Targets Exposed AI Servers for Cryptomining	4
FBI Warns FortiBleed Campaign Remains an Active Threat	4
China-Linked Threat Actors Target AI Experts in the United States and United Kingdom	4
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2026-88779	7
CVE-2026-104286	8
 Ransomware and Breach Intelligence Key Findings	9
Ransomware Group, Industry, Regional Trends	9
Notable Data Breaches this Week	10
 Physical and Geopolitical Intelligence Key Findings	12
Physical Security Intelligence: Global	12
Physical Security Intelligence: United States	12
 Appendix A: Traffic Light Protocol for Information Dissemination	13
 Appendix B: ZeroFox Intelligence Probability Scale	14

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Assessment – September 2026 Ransomware

Wrap-Up

In September 2026, ZeroFox recorded at least 742 ransomware and digital extortion (R&DE) incidents, which was roughly 14 percent fewer than in August but approximately 33 and 80.5 percent more than in September 2025 and September 2024, respectively. North America remained the top targeted region, with roughly 47 percent of September's incidents (at least 350). However, its year-over-year growth of approximately 7 percent lagged well behind the global rate of about 33 percent, shrinking its regional share of R&DE incidents from roughly 59 percent a year earlier. Manufacturing was again the most heavily targeted industry, with at least 150 incidents (down from 175 in August), while healthcare climbed to second place with at least 82 incidents. The Gentlemen, Qilin, Akira, INC Ransom, and Storm were almost certainly the five most active collectives in September 2026, with The Gentlemen and Qilin the only two that carried over from August's top five. Q3 2026 saw a new quarterly record of at least 2,381 R&DE incidents, approximately 14 percent above the previous high set in Q4 2025 and roughly 67 percent above Q3 2025. This very likely indicates an acceleration in global R&DE activity in the second half of the year heading into Q4 2026.

Monthly Geopolitical Report October 2026

The United States will likely maintain its focus on economic tactics to secure Iranian concessions. Iran will likely respond to U.S. economic pressure with military escalation. Therefore, a prolonged period of occasional escalation by both sides, marked by economic pressure to induce concessions, is likely. Middle Eastern oil shipments have increased to 80 percent of their pre-war levels, despite continued threats to shipping in both the Red Sea and the Strait of Hormuz (SoH). Moreover, Iranian oil shipments through the SoH have completely ceased. This combination very likely signals that the United States is weakening Iran's ability to control the SoH and is therefore unlikely to accept Iranian demands over SoH control. Oil prices have nevertheless remained high, likely driven by an expectation that Iran will further escalate its attacks on the energy sector in response to U.S. success in moving oil through the strait. The past two months have marked an escalation in Russian hybrid activity, particularly against defense and dual civilian-military logistics infrastructure in Eastern Europe. If Ukraine's tactics continue to succeed, Russia will likely escalate its hybrid attacks throughout Europe to asymmetrically pressure Ukraine's partners. In Brazil's elections, a victory for opposition candidate Bolsonaro will likely bring the country closer to U.S. policy when it comes to security, trade, and relations with China. A victory for incumbent Lula da Silva will likely reignite the tensions with the United States over those issues. The United States and China agreed to extend their

existing trade truce by two months. The extension very likely reduces the immediate risk of renewed tariff escalation. However, the timing of the announcement and its shorter-than-anticipated duration very likely signal that little progress was made on key issues.

ZeroFox Intelligence Brief – Underground Economist: Volume 6, Issue 21

The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

| Cyber and Dark Web Intelligence |

Cyber and Dark Web Intelligence Key Findings



PoeLLM Malware Targets Exposed AI Servers for Cryptomining

What we know:

- An active cryptomining campaign dubbed Canto Incognito has reportedly compromised more than 3,400 servers using PoeLLM malware by targeting internet-exposed artificial intelligence (AI) and large language model (LLM) infrastructure.

Background:

- The campaign has primarily targeted LiteLLM, Ollama, Gotenberg, and Gitea deployments in the United States and Western Europe, with possible targeting of Ivanti Sentry.
- PoeLLM deploys the XMRig and Iron miners and connects compromised systems to Kryptex, a Russian cryptocurrency mining service. It then turns infected servers into scanners and exploits hosts to find additional victims.
- The malware also derives its command-and-control (C2) address from keywords in a GitHub-hosted poem.
- The activity is reportedly linked to an Italian-language threat actor.

Analyst note:

- The botnet's self-propagating design will likely enable continued growth using compromised servers to identify and infect additional vulnerable systems.
- The targeting of exposed AI infrastructure also creates risks beyond cryptomining—particularly for systems that process sensitive data or provide access to other services.



FBI Warns FortiBleed Campaign Remains an Active Threat

What we know:

- The Federal Bureau of Investigation (FBI) and partners have released an alert warning that the FortiBleed campaign remains active and targets internet-facing Fortinet FortiGate firewalls and secure sockets layer (SSL) virtual private network (VPN) gateways.
- The campaign has reportedly compromised over 86,644 devices across 194 countries.

Background:

- Attackers reuse leaked passwords and employ graphics processing unit (GPU)-powered systems to crack stored password hashes at scale.
- The operators act as access brokers, selling network access to other criminals; the access has reportedly been passed to the INC/Lynx and Payload ransomware affiliates.
- Some victims have been locked out of their Fortinet devices.

Analyst note:

- Compromised credentials are very likely to provide direct administrative access to Fortinet infrastructure of organizations without requiring exploitation of a new vulnerability.
- Operational disruptions are likely if users are locked out of their devices and threat actors modify configurations.
- Successful initial access is also likely to enable later movement within the affected network.



China-Linked Threat Actors Target AI Experts in the United States and United Kingdom

What we know:

- China-linked espionage group TA419 has been observed targeting AI experts at U.S. think tanks, universities, and law firms, including specialists in AI policy.
- The group reportedly impersonated prominent economists, AI policymakers, and an Anthropic employee in phishing campaigns to steal credentials.

Background:

- TA419 reportedly used tailored outreach and shortened links to redirect victims to fake certain login pages that used AI-in-the-middle (AitM) and Frameless browser-in-the-browser (BitB) techniques to steal credentials and session information.
- Separately, United Kingdom's intelligence agency has warned that information from the work of more than 100 UK-linked academics has been used in research funded through China Academy of General Technology (CAGT), which it assesses supports the development of espionage capabilities in areas such as AI and cybersecurity.

Analyst note:

- Targeting policy experts rather than only AI developers likely indicates an intelligence requirement for decision-making and policy direction, potentially giving China earlier insight into forthcoming restrictions, technology transfer controls, and U.S. AI strategy.

| **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 three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on [October 2](#) and [October 4, 2026](#). Additionally, CISA released six Industrial Control Systems (ICS) advisories on [October 6, 2026](#). ZeroFox observed Google releasing security patches for Chrome addressing several critical-severity use-after-free vulnerabilities. Microsoft released out-of-band updates for a high-severity authorization flaw in Microsoft Exchange Server ([CVE-2026-96940](#)). Additionally, an arbitrary file access vulnerability ([CVE-2026-21589](#)) was observed in Atlassian Data Center products.



HIGH

CVE-2026-88779

What happened: Citrix has released emergency updates for a zero-day memory buffer vulnerability in NetScaler ADC and Gateway appliances using Security Assertion Markup Language (SAML) authentication with Gateway or authentication, authorization, and accounting (AAA) functionality.

- **What this means:** The flaw is being actively exploited in targeted attacks to cause denial of service and has also been observed in attacks involving malware payloads and potential remote code execution (RCE).
- **Affected products:**
 - The affected products are [listed in the advisory](#).



CRITICAL

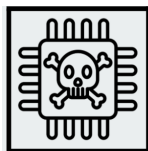
CVE-2026-104286

What happened: Fortinet has warned of this critical path traversal and NULL byte neutralization flaw that is reportedly being actively exploited in zero-day attacks.

- **What this means:** The vulnerability reportedly enables unauthenticated RCE or arbitrary file writes via specifically crafted HTTP or HTTPS requests. CISA has [added this vulnerability](#) to its KEV catalog.
- **Affected products:**
 - FortiMail management interfaces running versions 8.0.0 through 8.0.1, 7.6.0 through 7.6.6, 7.4.0 through 7.4.8, and 7.2.0 through 7.2.9

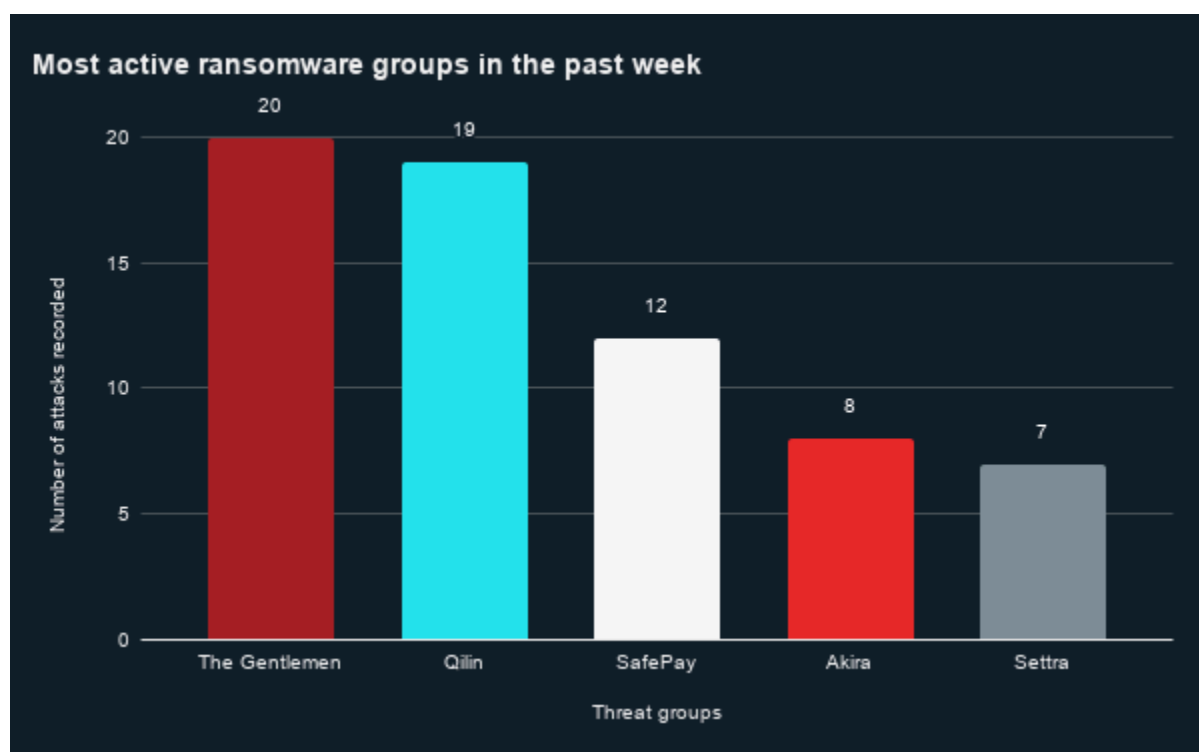
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



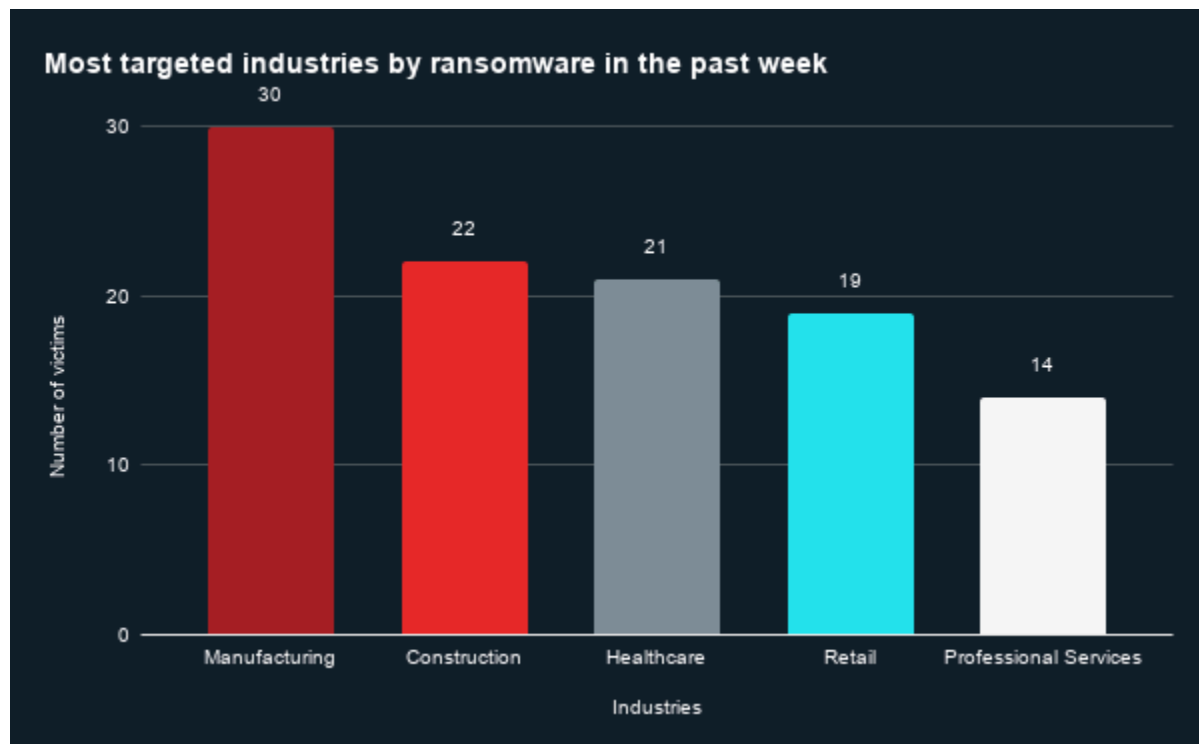
Ransomware Group, Industry, Regional Trends

Last week in ransomware: In the past week, The Gentlemen, Qilin, SafePay, Akira, and Settra were the most active ransomware groups. ZeroFox observed close to 155 ransomware victims disclosed, most of whom were located in North America. The Gentlemen accounted for the largest number of attacks, followed by Qilin.



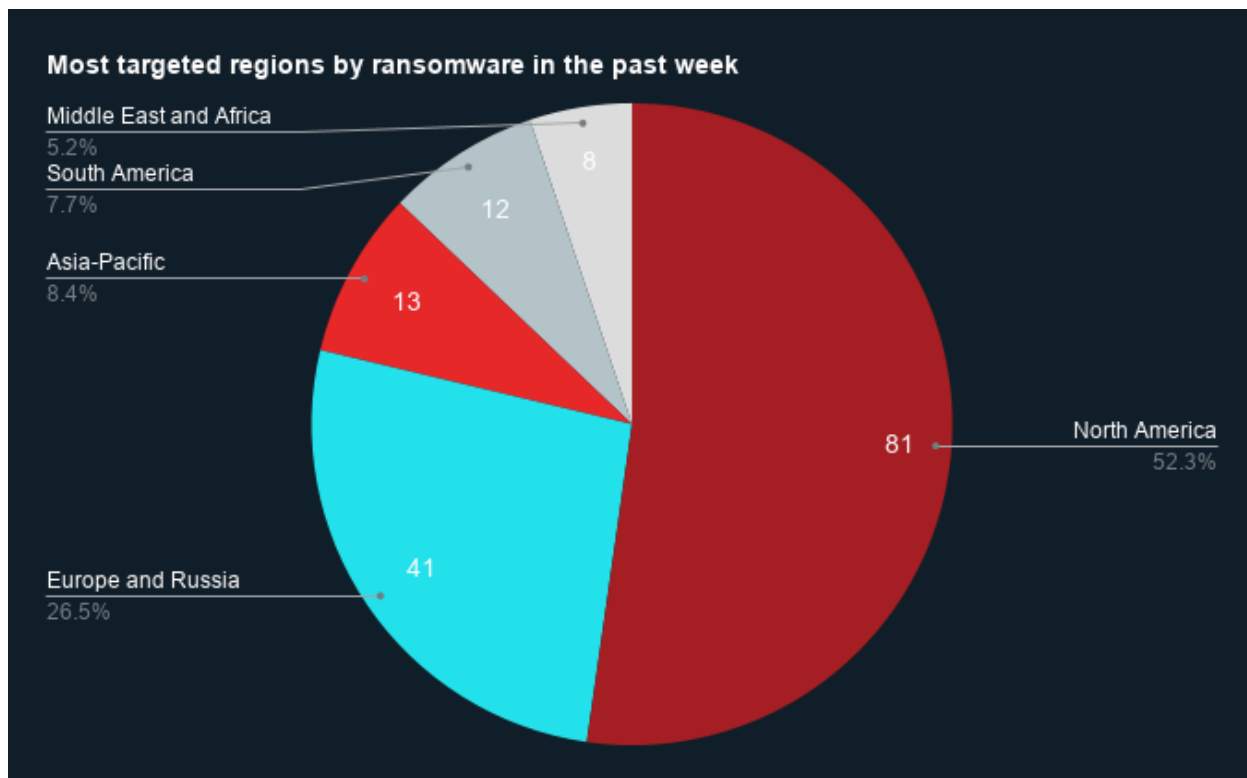
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by construction, healthcare, retail, and 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, and Asia-Pacific. There were at least 81 ransomware attacks observed in North America, while Europe and Russia accounted for 41, Asia-Pacific for 13, South America for 12, and Middle East and Africa for eight.



Source: ZeroFox Internal Collections



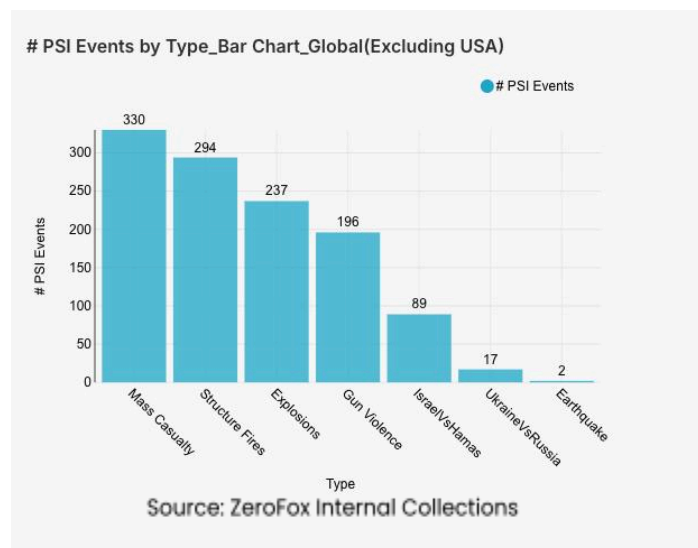
Notable Data Breaches this Week

Targeted Entity	<u>Denmark Population Registry (Central Person Register)</u>	<u>Technical University of Denmark (DTU)</u>	<u>Frontline Education</u>
Compromised Entities/Victims	Approximately 8.8 million individuals	Up to 200,000 current and former users	Frontline Education
Compromised Data Fields	Names, addresses, CPR identification numbers, dates of birth, and other registry information	Danish civil registration numbers, home addresses, employment details, and next-of-kin contact information	Employee Social Security Numbers (SSNs), email addresses, and physical addresses
Suspected Threat Actor	Unknown	Unknown	Unknown
Country/Region	Denmark	Denmark	United States
Industry	Government	Education	Education / Technology
Possible Repercussions	Exposed individuals face risks of identity fraud, phishing, and social engineering activity, while threat actors may combine data for improved targeting or gaining initial access to downstream organizations.	Identity theft, phishing, and targeted social engineering attacks.	Identity theft, fraud, and targeted phishing campaigns

Three major breaches observed in the past week

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings



Physical Security

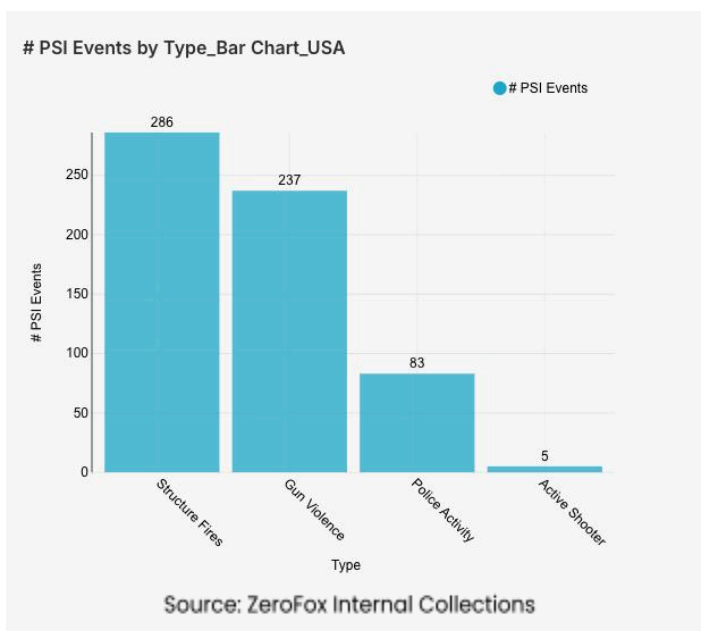
Intelligence: Global

What happened: Excluding the United States, there was a 20 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, Mexico, and Yemen, in that order. Approximately 72 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 25

percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict increased by 10 percent from the previous week, and alerts related to Russia's war with Ukraine decreased by 19 percent. The top three most-alerted subtypes were structure fires, which saw an 8 percent increase from the previous week; explosions, which increased by 17 percent; and gun violence, which increased by 6 percent. Notably, there were two major earthquakes recorded this week.

- **What this means:** Mass casualty events this week were driven largely by explosions and a mix of ongoing conflict and criminal violence. In Yemen, [Houthi attacks on Saudi airports](#) between October 6 and 8 killed three people and injured 36, including two killed and 28 wounded at Abha airport (reported October 7) and one killed and eight wounded at Riyadh's King Khalid airport. A Saudi-led coalition stated on October 7 that it had destroyed 82 Houthi military sites in response. In Gaza, [Israeli strikes on October 7](#), the third anniversary of the Hamas-led attack, killed at least four Palestinians, contributing to the rise in Israel-Hamas alerts. In Mexico, cartel gunmen attacked a bar in [Zamora, Michoacán](#), on October 2, killing four and wounding three, augmenting the overall rise in gun violence alerts. The two major earthquakes recorded this week took place in India and Japan; India experienced a [4.9-magnitude quake](#) in Uttarakhand's Chamoli district on October 6, and Japan saw a [4.8-magnitude quake](#) in northeastern Chiba Prefecture on October 8, with no tsunami warnings issued. Overall, global physical security remains volatile, with explosive violence, active war zones, and seismic activity all adding to the instability.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity includes general law enforcement presence in response to various physical security events, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were California and Illinois, which together made up 22 percent of this week's nationwide total. Gun violence

across the United States overall increased by 10 percent from the week prior. Police activity alerts increased by 9 percent, and the top contributing states were Texas and California. Structure fires decreased by 10 percent, and the top two states for this subtype were California and New York. Notably, active shooter alerts increased by 150 percent.

- > **What this means:** Gun violence, police activity, and structure fires led this week's alerts, with gun violence and active shooter alerts both increasing. The most notable example occurred in [Vienna, Georgia](#), where more than 50 shots were fired at a block party of over 1,000 people early October 4, killing two and injuring 35; [as of Wednesday](#), no arrests have been made, and no motive is known. In total, there were [eight mass shootings](#) within the last week across the nation. Illinois' high ranking was reflected in [Chicago](#), where at least two people were killed and 20 wounded over the weekend. In Texas, hundreds of U.S. and Mexican troops were deployed along the [Tamaulipas border](#) after U.S. officials said Coast Guard personnel came under fire, which Mexico disputes. In California, firefighters [rescued three people](#) from an Alameda apartment fire on October 7, and an [e-bike battery fire](#) forced an apartment evacuation in San Francisco on October 3. Meanwhile, [Tropical Storm Isaias](#) is forecast to become a hurricane, with watches issued for the northern Gulf Coast. Overall, domestic physical security remains elevated, with mass-casualty gun violence and a Gulf Coast hurricane threat driving risk.

| 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%