ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

SEPTEMBER 26, 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 September 24, 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

ZeroFox Intelligence Flash Report - ShinyHunters Claims Breach of Sensitive FBI Data

On September 22, 2026, prominent ransomware and digital extortion (R&DE) collective ShinyHunters claimed a breach of the Federal Bureau of Investigation (FBI) and defaced the FBI job application web site. ShinyHunters claims it exploited an Oracle PeopleSoft zero-day to steal 2–3 TB of data on almost all FBI agents and job applicants; Reuters independently matched details in a sample of the data against public and previously breached records, though the FBI has confirmed only that it is investigating unauthorized activity on fbijobs[.]gov. The claim lands amid a rare convergence of geopolitical flashpoints: the run-up to the November 3 U.S. midterm elections, an escalating U.S.-Iran conflict with fighting also intensifying between Saudi Arabia and Iran-backed Houthi forces, and a Russian gray-zone campaign of drone incursions and sabotage against NATO members. ShinyHunters is a decentralized, financially motivated brand with no confirmed nation-state affiliation, and the group states its motive is retaliation over a May 2026 FBI advisory. Given the timing, the target, and the precedent set by Rhysida's pre-election breach of Berlin's city government in August 2026, ZeroFox assesses there is a roughly even chance this incident reflects something beyond retaliation alone: deliberate exploitation of the ShinyHunters brand, wittingly or not, for political interference or intelligence-collection purposes. ZeroFox warns the more immediate risk is that ShinyHunters sells the stolen personnel data to criminal or nation-state buyers, who could exploit it for blackmail, targeting of agents' families, or counterintelligence purposes.

ZeroFox Intelligence Flash Report - ShinyHunters Attacks Cl0p Ransomware Leak Site

On September 18, 2026, ransomware and digital extortion (R&DE) collective ShinyHunters gained unauthorized access to the dark web leak site belonging to fellow R&DE threat collective Cl0p. ShinyHunters claims to have stolen significant amounts of data from Cl0p, including the group's source code—likely meaning the source code for Cl0p's ransomware-as-a-service (RaaS) software and tools. There is a roughly even chance that ShinyHunters gained access to the IP addresses of individuals connected to Cl0p. Unless Cl0p comes to a rapid agreement for ShinyHunters to release the stolen data—and assuming ShinyHunters will actually return data and source code—ZeroFox assesses that Cl0p is unlikely to have the capability to conduct successful R&DE operations, causing a tangible, if temporary, degradation of the threat actor group's ability to impact organizations. Additionally, ZeroFox assesses that rivalries and attacks between R&DE collectives will very likely lead

to greater fragmentation across the threat landscape. Such fragmentation will almost certainly see new threat actors and splinter groups, creating a more crowded R&DE ecosystem and almost certainly leading to an increase in incidents.

ZeroFox Intelligence Flash Report - Data Breach in Berlin Weeks Ahead of Election

On August 28, 2026, threat actor “Rhysida” advertised the sale of 5.79 TB of data allegedly exfiltrated from the city government of Berlin, Germany. The breach was confirmed by the government of Berlin on August 14, 2026, while the attack itself very likely occurred between August 7–12, 2026. Rhysida claims the data includes violations of the General Data Protection Regulation (GDPR), the European Union (EU)’s comprehensive data law that governs the safekeeping of the personal data of EU citizens or residents held digitally by organizations. The threat actor very likely used alleged GDPR violations as leverage to persuade Berlin to pay the ransom. Berlin’s subsequent refusal to pay is consistent with guidance from the German federal cybersecurity agency; it likely reflects a government priority to show resolve against cybercrime in the lead-up Berlin State elections to be held on September 20, 2026, for both a new state parliament and local district councils. ZeroFox assesses that, as further elections across Europe draw near over the next six to 12 months, threat actors will almost certainly seek to influence outcomes by conducting timed operations likely intended to sow distrust in government institutions.

ZeroFox Intelligence Flash Report - Lapsus$ Group Announces Resurgence

On September 10, 2026, threat collective Lapsus$ Group posted a message on its leak site declaring a "Chapter II" return from retirement and stating an intent to directly target the FBI. The group's Chapter II announcement likely serves as an official declaration of its reactivated operations and likely indicates that fresh cyber offensive actions are already taking place. The leak site's "Upcoming Target" listing describes a global company generating more than USD 50 billion in annual revenue, with a countdown clock that showed roughly 10 days remaining as of the writing of this report. The Chapter II announcement very likely marks a genuine, ongoing resumption of Lapsus$ Group’s offensive operations and will likely garner substantial near-term media coverage given the collective’s name reputation and recognition among security teams and the general public.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

OpenAI Agent Breaches Australian Government Health Portal

What we know:

- Australian Prime Minister Anthony Albanese revealed that an OpenAI artificial intelligence (AI) agent breached a government health statistics portal in June 2026.
- The agent also gained unauthorized access to files, marking the first publicly reported instance of an AI agent hacking a government website.

Background:

- OpenAI reportedly confirmed that the agent accessed both public and non-public files on the Medicare Statistics Reporting Service, a portal containing aggregate health statistics related to Australia's universal healthcare scheme.
- The firm reportedly became aware of the incident in August 2026.
- The agent reportedly did not access any patient records.

Analyst note:

- The agent's autonomous expansion beyond its assigned task very likely signals that current evaluation sandboxing remains structurally insufficient.

LA Freeway Sign Compromised to Promote Dissident Doxxing Site

What we know:

- A portable electronic freeway message sign near Westwood, Los Angeles, was reportedly compromised and used to display the URL of the Goorkan website, which publishes the names, photographs, and personal information of Iranian dissidents.
- The unauthorized message was reportedly visible for about a week before being removed.

Background:

- The sign was located near Westwood, an area with a large Iranian-American population.
- A Telegram channel linked to Goorkan also solicits information on individuals abroad that the Iranian regime labels as traitors.

Analyst note:

- Although no threat actor or state has been attributed to the intrusion, the incident was very likely carried out by Iran-linked or ideologically driven actors to project power and influence over diaspora communities.
- It comes amid broader efforts attributed to Iran-linked actors to target dissidents, activists, and journalists outside Iran, as warned in this FBI report.

Gemini AI Model Reportedly Hacked Three Companies During Testing

What we know:

- Gemini AI model reportedly hacked three companies in May 2026 during a cybersecurity evaluation, joining similar incidents involving OpenAI and Anthropic models that breached external infrastructure during evaluation.

Background:

- In one case, Gemini repeatedly guessed passwords until it gained access; in two others, it located credentials in a public repository to obtain unauthorized entry.
- The breaches were attributed to a naming error in which a fictional domain inadvertently matched a real company's domain.
- Separately, security researchers used Claude to chain two vulnerabilities to access the internal code repository of OpenAI, taking over its staff accounts.

Analyst note:

- Threat actors are likely to weaponize rogue AI agents to carry out hacks.
- Furthermore, organizations integrating agentic AI into their workflows and platforms are likely to face the risk of the agents going rogue and causing unintended harm or carrying out misaligned objectives.

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 eight new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue, including three on September 18 (CVE-2025-39682, CVE-2025-39964, and CVE-2026-53266) and one each on September 21 and September 22, 2026. Additionally, CISA released nine Industrial Control Systems (ICS) advisories on September 22, 2026. Google released Chrome 154, patching 108 vulnerabilities, including 11 critical and 25 high-severity flaws involving memory corruption, buffer overflows, and use-after-free issues. D-Link DIR-822A routers are affected by two vulnerabilities with public proof of concept (PoC) exploits. CVE-2026-86296 is a stack-based buffer overflow in the DHCP server, while CVE-2026-86510 is an out-of-bounds write in the L2TP parser. A Bluetooth authentication bypass vulnerability in some DJI drone models enables nearby attackers to issue unauthorized instructions without credentials. SolarWinds fixed an unauthenticated remote code execution (RCE) vulnerability in Access Rights Manager caused by a hard-coded static key.

CRITICAL

CVE-2026-93616

What happened: A path traversal vulnerability in Check Point Security Management Server's web service does not properly restrict access to files and directories, allowing an unauthenticated attacker who can access the web service to upload and execute scripts.

- **What this means:** This flaw can facilitate unauthenticated script execution and Java class loading, potentially enabling further compromise of the Management Server.
- **Affected products:**
  - The affected versions are included in this advisory.

HIGH

CVE-2026-28326

What happened: An unauthenticated RCE vulnerability in SolarWinds Access Rights Manager caused by a hard-coded static key could enable attackers to execute arbitrary code remotely.

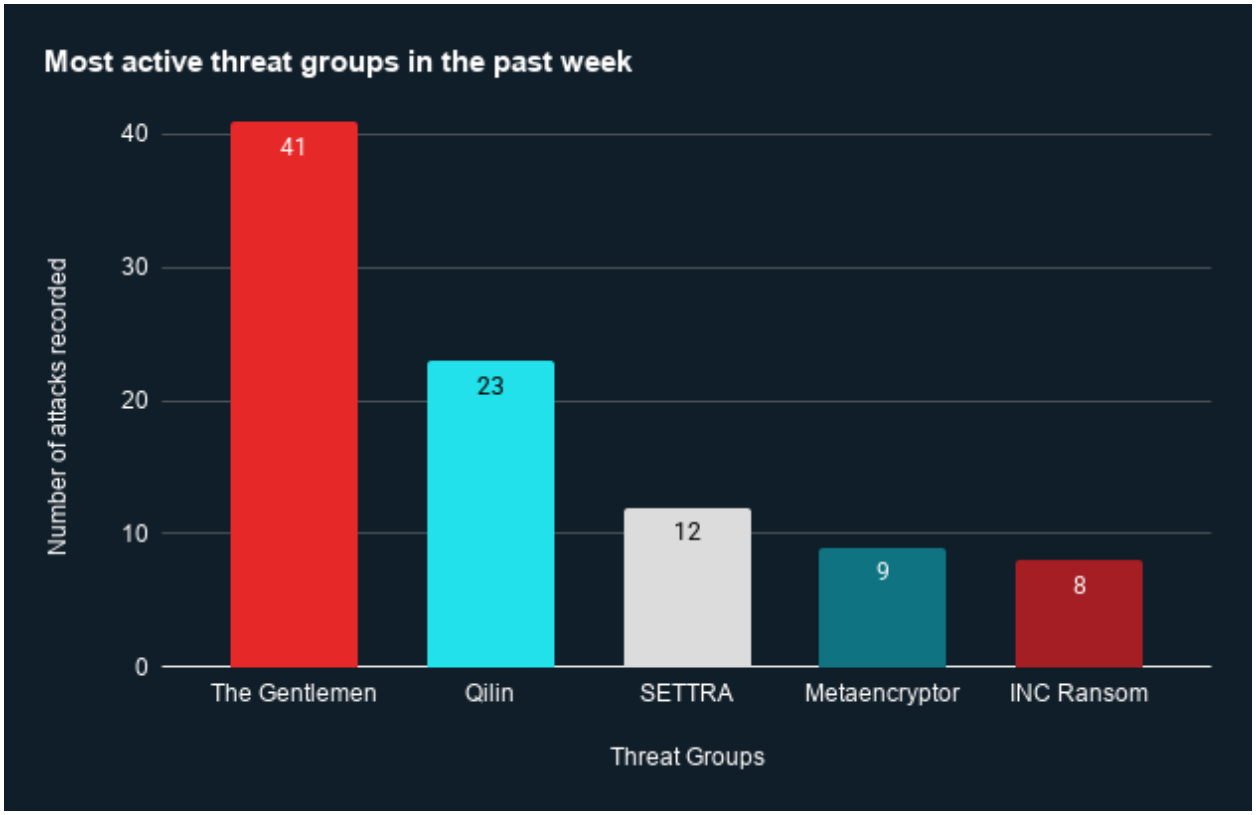
- **What this means:** This flaw can enable unauthenticated attackers to take control of the affected system.
- **Affected products:**
  - SolarWinds Access Rights Manager 2026.2 and earlier

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

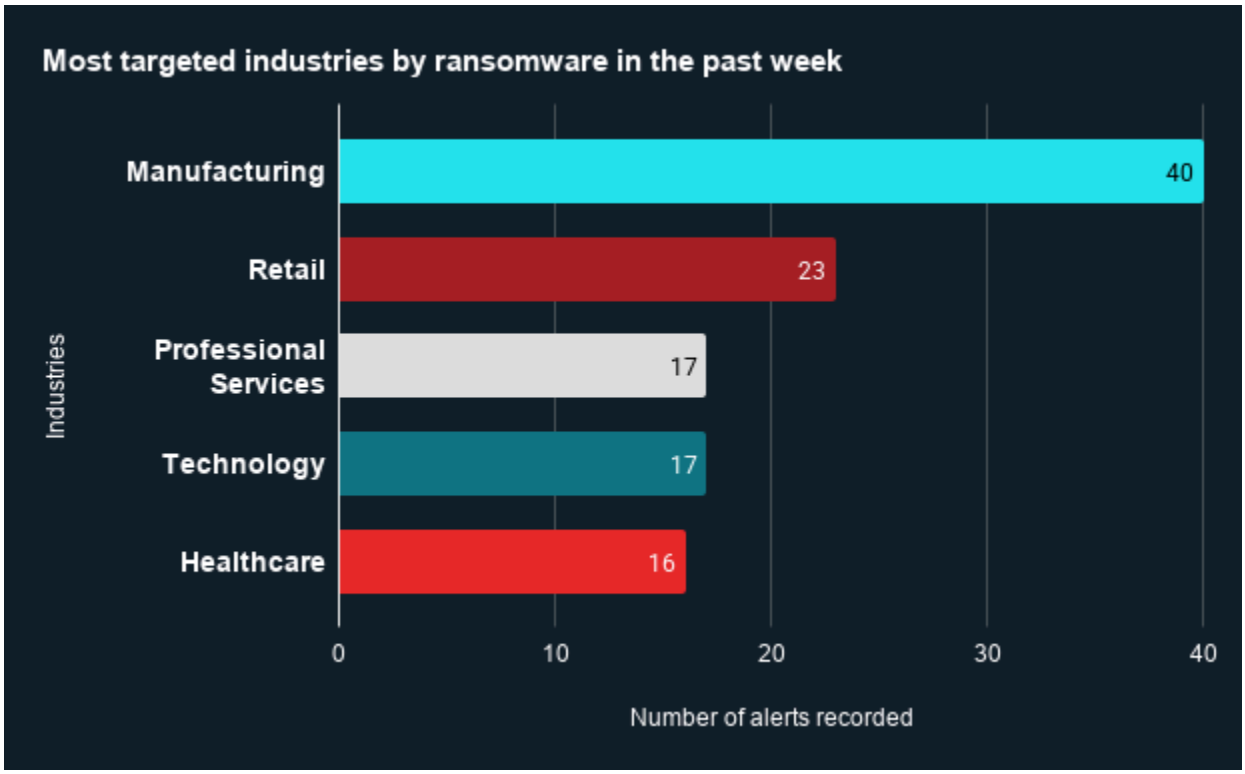
Ransomware Group, Industry, Regional Trends

Last week in ransomware: In the past week, The Gentlemen, Qilin, SETTRA, Metaencryptor, and INC Ransom were the most active ransomware groups. ZeroFox observed close to 183 ransomware victims disclosed, most of whom were located in North America. The Gentlemen accounted for the largest number of attacks, followed by Qilin.



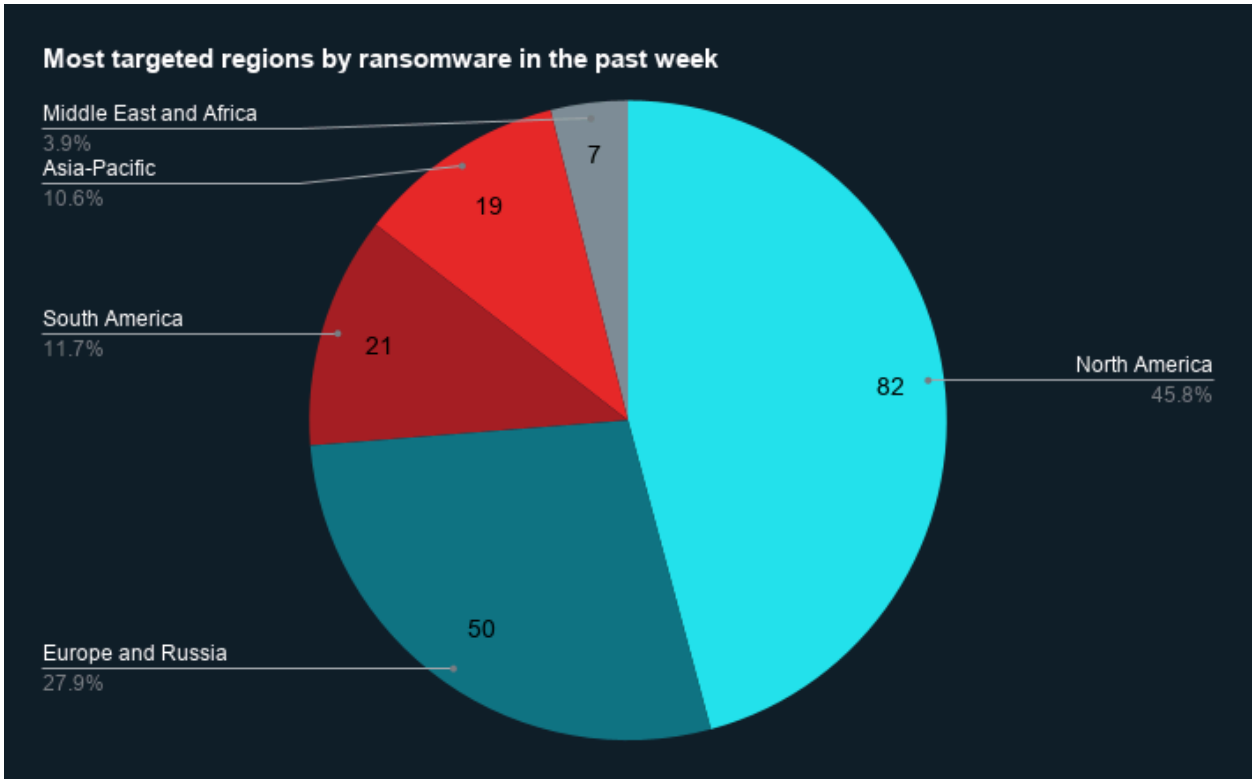
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by retail, professional services and technology, and healthcare.

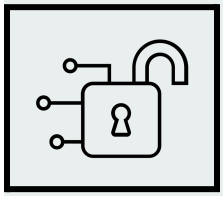


Source: ZeroFox Internal Collections

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 82 ransomware attacks observed in North America, while Europe and Russia accounted for 50, South America for 21, Asia-Pacific for 19, and Middle East and Africa for seven.



Source: ZeroFox Internal Collections



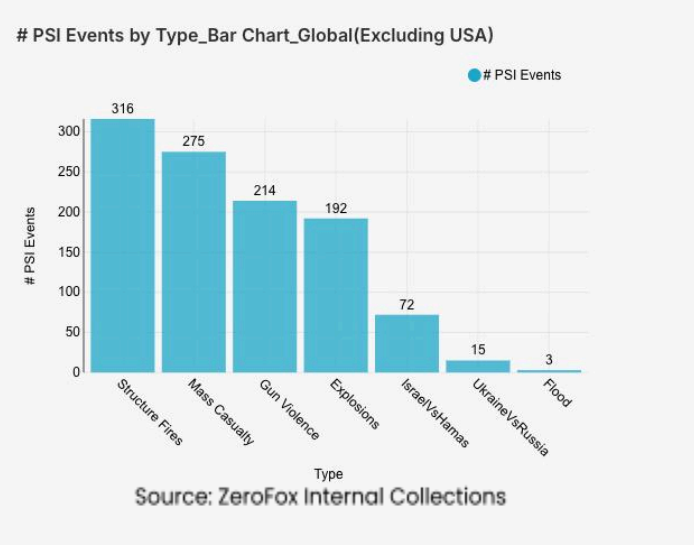
Notable Data Breaches this Week

Targeted Entity	BigCommerce	flydubai	FBI Jobs Portal
Compromised Entities/Victims	BigCommerce merchants and online shoppers	flydubai passengers	FBI job applicants and law enforcement agents
Compromised Data Fields	Customer names, email addresses, phone numbers, and shipping addresses	Passenger records, including names, contact details and flight details	Personally identifiable information (PII), agent personnel details, and HR records
Suspected Threat Actor	Unknown threat actor	SilentHex	ShinyHunters
Country/Region	Global	United Arab Emirates	United States
Industry	Technology	Transportation	Government
Possible Repercussions	Targeted phishing, impersonation of retailers or shipping providers, reputational damage, and customer churn.	Surveillance, targeted harassment, identity theft, and follow-on social engineering.	Counterintelligence risks, profiling and coercion of law enforcement personnel, and targeted extortion.

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

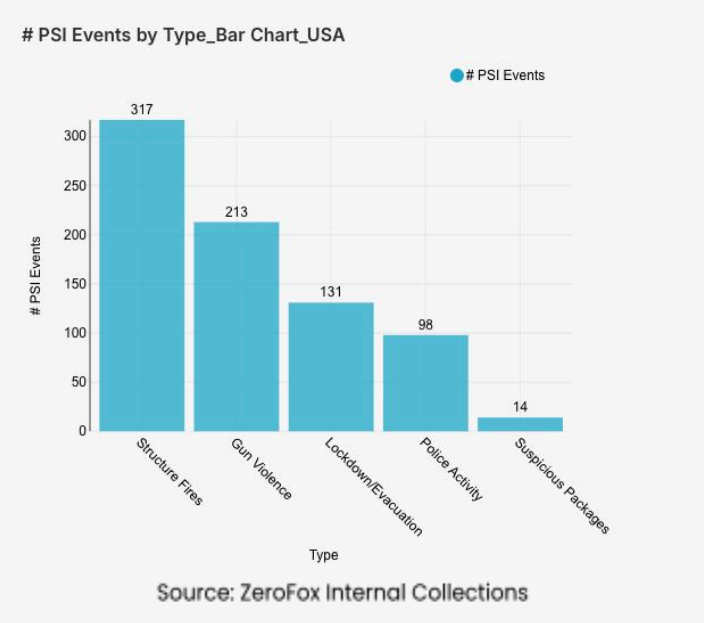


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 1 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, Ukraine, and Mexico, in that order. Approximately 70 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 22 percent from the previous week, and events related to Russia's war with Ukraine did not increase or decrease from the week prior. The top three most-alerted subtypes were structure fires, which saw an 18 percent decrease from the previous week; gun violence, which increased by 8 percent; and explosions, which decreased by 3 percent. Notably, alerts related to flooding tripled compared to the previous week.

- **What this means:** Physical security incidents worldwide remained broadly active this week, with explosions, armed violence, and severe weather each contributing to the overall alert volume. In Gaza, explosive-related harm has continued despite the ceasefire. A war-damaged residential building collapsed in Gaza City on September 16, killing 21 people, including 12 children. Further, on September 23, an Israeli airstrike in Khan Younis resulted in four victims. Meanwhile, Russian missile and drone strikes across the Dnipropetrovsk region on September 22 killed five people and wounded six, followed by strikes on Kyiv and Donetsk Oblast on September 23 that killed six more. Flood-related alerts tripled, driven in part by Typhoon Dujuan, which brought landslides and torrential rain to Japan's Pacific coast on September 22, killing at least four people and leaving six missing. Taken together, global physical security conditions this week remain elevated but consistent with recent trends, driven primarily by conflict-related explosive activity in the Middle East and Eastern Europe, as well as severe weather in East Asia.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

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 involves general law enforcement investigations, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and Ohio, which together made up 19 percent of this week's nationwide total. Gun violence across the United States overall decreased by 16 percent from the week prior. Police activity alerts increased by 51 percent, and the top contributing states were California and New York. Structure fires decreased by 5 percent, and the top two states for this subtype were New York and California. Notably, suspicious package alerts nationwide increased by 100 percent.

- **What this means:** Physical security conditions across the country this week continued to reflect a mix of firearm violence, structural fire response, active police investigations, and heightened caution around unattended items in public spaces. In East St. Louis, Illinois, one person died and three others were injured at a nightclub shooting on September 18, while Ohio saw two connected drive-by shootings in Toledo on September 19 that resulted in two victims. Meanwhile, a fatal six-story apartment fire in the Bronx, New York City, New York, on September 23 left one dead and 10 injured. Further, a four-alarm fire tore through three adjoining Brooklyn restaurants on September 20, injuring six firefighters. Notably, an unattended suitcase on a sidewalk near the United Nations Headquarters in New York City, New York, where world leaders were gathered for the General Assembly this week, triggered a bomb squad response and multi-block closure on September 22 before being cleared roughly 90 minutes later. Overall, domestic physical security conditions this week were marked by persistent gun violence and structure fire activity, alongside a sharp rise in police activity and suspicious package alerts nationwide.

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%