ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 22, 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 August 20, 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 - European Intelligence Seeks Broader Authority to Defend Against Russian Hybrid Warfare

On August 11, 2026, the German cabinet approved draft legislation strengthening the capabilities of its intelligence services. Germany, like other European members of NATO, likely anticipates that recent Ukrainian military success against Russia will trigger further Russian attempts to undermine European support for Ukraine. Expect other European supporters of Ukraine to move forward with their own measures to prevent and respond to Russian hybrid warfare measures. Ukraine has increasingly targeted key Russian economic sectors, which has successfully curtailed Russia's oil refining capacity and ability to export grain. These strikes have likely inspired Russia to respond with its highest rate of attacks since the war began. Ukraine will likely need to continue making progress in its long-strike campaign. Russia will likely try to reverse Ukrainian gains by taking advantage of its lack of missile defenses and escalating its hybrid warfare campaign to weaken European support for Ukraine.

ZeroFox Intelligence Flash Report - U.S. Private Companies to Conduct Cyber Attacks

On August 12, 2026, U.S. President Donald Trump signed a National Security Presidential Memorandum (NSPM) directing the National Coordination Center (NCC) to develop a program authorizing vetted U.S. companies to conduct cyber surveillance and disruption operations against foreign Cyber-Enabled Transnational Criminal Organizations (CE-TCOs). The NSPM authorizes two activities that 18 U.S.C. § 1030 had previously not allowed for commercial actors: Cyber Surveillance Operations (covering clandestine collection from adversary systems) and Cyber Effects Operations (covering disruption, degradation, or destruction). Operating procedures and participation standards are due by mid-October. ZeroFox assesses that criminal groups are likely to develop defensive adaptations in response to adversary capabilities that combine U.S. commercial engineering speed with federal legal cover rather than be deterred by them. ZeroFox assesses with moderate confidence that the program will almost certainly proceed. However, it is likely that the October deadline will yield interim rather than complete procedures and that first-cohort vetting will run into 2027, given that the NSPM did not provide details regarding how the NCC should implement the program.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

1Password Users Targeted in Active Phishing Campaign

What we know:

- Password manager 1Password has confirmed that an active phishing campaign is targeting its users with fake payment update emails that link to fraudulent pages designed to steal account credentials.
- 1Password noted that the campaign is not the result of any breach of 1Password's systems.

Background:

- 1Password has asked affected users to report suspicious emails to the company.
- Additionally, according to one reported case on an online discussion platform, the phishing page allegedly mimics 1Password's login flow, prompting the user for their email, password, and Secret Key.
- However, a "Sign Up" prompt reportedly appeared where a "Sign In" prompt would normally be expected, helping identify the scam.

Analyst note:

- The campaign's attempt to obtain account credentials likely suggests an account takeover objective beyond credential theft, as attackers appear to be seeking multiple authentication elements.

CISA Warns of Active Threat Targeting Siemens S7 Series PLCs

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) warned that an active cyber threat is targeting Siemens S7 Series programmable logic controllers (PLCs) across multiple U.S. critical infrastructure sectors.
- Threat actors are reportedly using artificial intelligence (AI)-assisted exploitation scripts to compromise internet-exposed devices.

Background:

- After using internet scanning services to identify exposed or poorly segmented Siemens S7 Series PLCs, threat actors are reportedly using AI-generated Python scripts to gain read and write access to PLC memory, configuration data, and ladder logic programs.
- The sectors most at risk include critical manufacturing, energy, water and wastewater, chemical, food and agriculture, and commercial facilities, as well as the defense industrial base.
- The advisory comes amid a broader pattern of cyber incidents targeting local water systems across the United States, which cybersecurity experts suspect are linked to Iran.

Analyst note:

- The deployment of AI-assisted scripts against exposed PLCs almost certainly lowers the technical barrier for threat actors seeking to disrupt U.S. critical infrastructure.
- Given the ongoing targeting of domestic operational technology (OT) entities by foreign-linked actors, critical infrastructure operators with internet-exposed PLCs are very likely to face elevated risk of logic manipulation or device disruption if robust network segmentation is not implemented.

Researchers Analyze TeamPCP Archive Exposing Nearly 2,500 Organizations

What we know:

- Researchers have obtained and analyzed an archive of the data TeamPCP collected from compromised continuous integration and continuous delivery (CI/CD) build machines in its March 2026 supply chain campaign.
- The data reportedly includes credentials and other information from nearly 2,500 organizations, including major technology and industrial companies.
- The exposure of credentials does not necessarily mean the affected organizations were breached or that the data is new, but some credentials can remain usable if they were not rotated.

Background:

- The compromised data reportedly amounts to at least 153 GB and contains more than 433,000 files, including cloud credentials, application programming interface (API) keys, tokens, and other sensitive authentication data.
- Some of the stolen data is now reportedly being offered for sale on Telegram.

- In the March 2026 compromise, TeamPCP reportedly compromised Trivy, with stolen credentials subsequently used to compromise additional software, including the LiteLLM Python package.

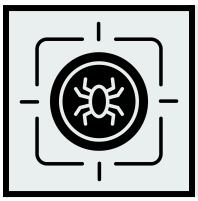
Analyst note:

- The credentials were likely harvested opportunistically from the earlier Trivy/LiteLLM supply chain campaign rather than through individual breaches of each affected organization.
- Since some of the stolen data is reportedly being sold on Telegram, any credentials that remain valid are likely to be leveraged by threat actors to access associated cloud environments, repositories, or other services, enabling further attacks.
- More information on TeamPCP can be found in this advisory.

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. CISA added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on August 17, August 18, and August 19, 2026. Additionally, on August 18, 2026, CISA released two Industrial Control Systems (ICS) advisories. GitLab disclosed two vulnerabilities (CVE-2026-19478 and CVE-2026-19650) that could enable unauthenticated attackers to remotely modify or delete public projects and user data via a GraphQL directive or execute CSRF mutations. SAP Commerce Cloud patched an improper authorization flaw (CVE-2026-58231) in its Data Hub Adapter that enables unauthenticated code execution. Additionally, a directory traversal flaw in VMware vCenter (CVE-2026-59310) is being actively exploited in the wild across more than 360 internet-accessible instances. Google and Mozilla have released security updates for Chrome and Firefox, patching 15 and 58 vulnerabilities, respectively, including critical- and high-severity flaws. Firefox 154 addresses 20 high-severity vulnerabilities, while Chrome 151 fixes two critical WebGL and Dawn buffer overflows that could enable code execution. Oracle has released 943 security patches in its August 2026 CSPU, addressing more than 1,000 CVEs, including over 150 critical-severity flaws and nearly 90 with Common Vulnerability Scoring System (CVSS) scores of 9.8 or higher. The update covers two dozen products, with Fusion Middleware and Hyperion receiving the most patches, including more than 280 remotely exploitable flaws combined.



HIGH

CVE-2026-24301

What happened: Dubbed “CoSnitch,” this is a set of three vulnerabilities in Microsoft Copilot Personal patched on August 18, 2026.

> **What this means:** The flaw enables a single crafted link to exfiltrate data from connected applications within an authenticated session and write persistent instructions into memory.

> **Affected products:**

- Microsoft Copilot Personal (patched August 18, 2026)

CRITICAL

CVE-2026-33824

What happened: This is an actively exploited remote code execution vulnerability in the Windows Internet Key Exchange (IKE) Service Extensions component.

> **What this means:** An unauthenticated attacker can exploit the vulnerability to gain code execution without any privileges by sending maliciously crafted packets to unpatched Windows systems with IKE version 2 enabled through UDP ports 500 or 4500.

> **Affected products:**

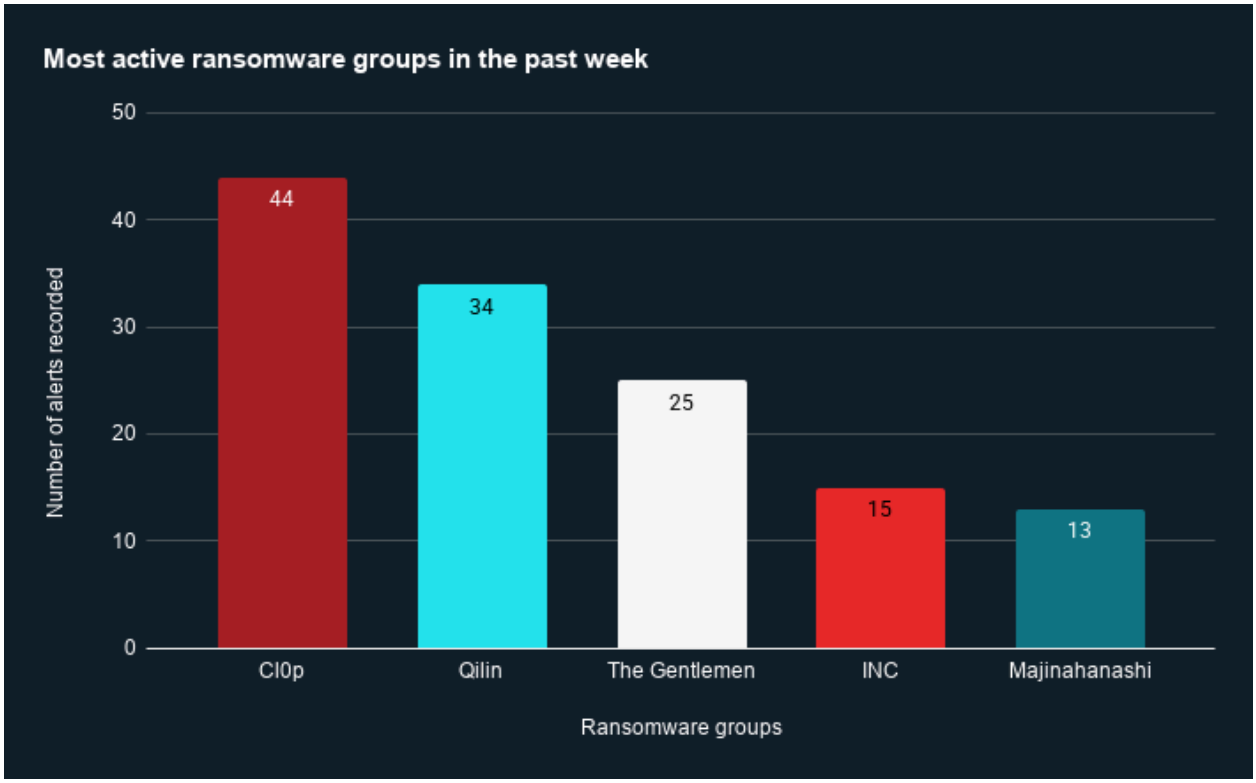
- The affected products are listed in this advisory.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

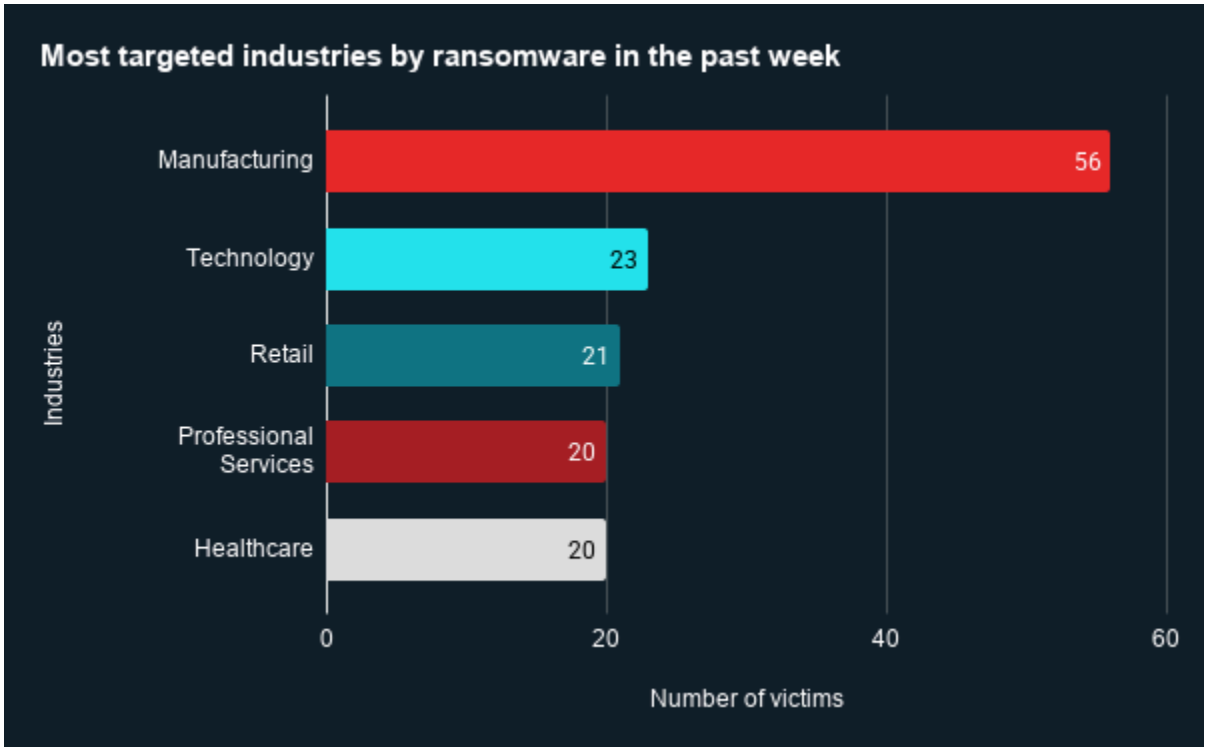
Ransomware Groups, Industries, Regional Trends

Last week in ransomware: In the past week, Cl0p, Qilin, The Gentlemen, INC, and Majinahanashi were the most active ransomware groups. ZeroFox observed close to 226 ransomware victims disclosed, most of whom were located in North America. The Cl0p ransomware group accounted for the largest number of attacks, followed by Qilin.



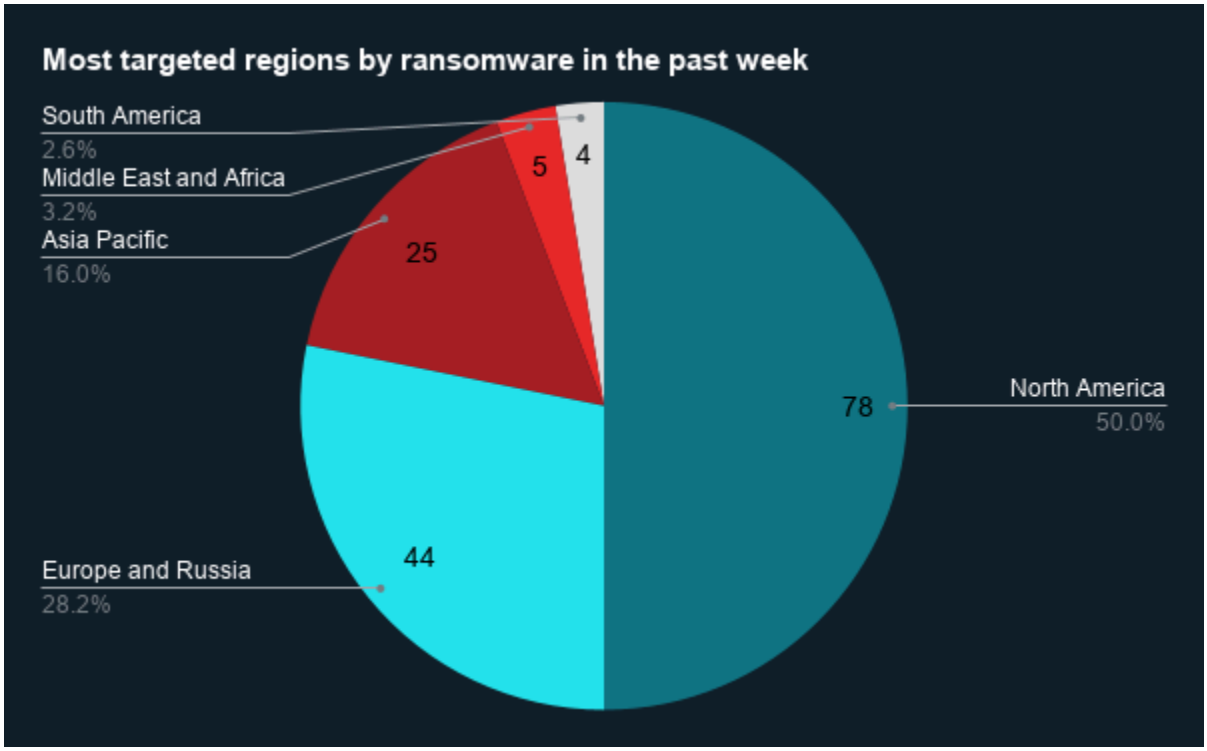
Source: ZeroFox Internal Collections

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

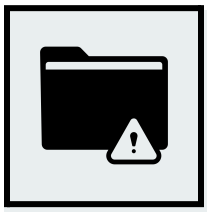


Source: ZeroFox Internal Collections

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 78 ransomware attacks observed in North America, while Europe and Russia accounted for 44, Asia-Pacific for 25, Middle East and Africa for five, and South America for four.



Source: ZeroFox Internal Collections



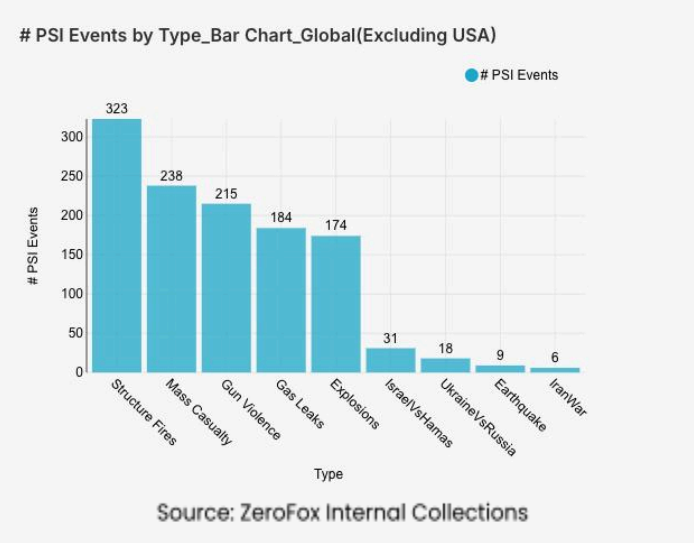
Notable Data Breaches this Week

Targeted Entity	General Directorate of Public Finances (DGFiP)	Sakura Internet	Bits of Gold
Compromised Entities/Victims	DGFiP systems and more than 600,000 taxpayers (individuals and professionals)	1,360,563 member accounts	Approximately 200,000 customers
Compromised Data Fields	Financial and tax-related information, including reference tax income, family quotient, withholding tax rate, company names, SIREN numbers, cadastral addresses, and property sizes	Customer contract, membership information, and account credentials/passwords	Customer names, national ID numbers, email addresses, phone numbers, IP addresses, bank account details, and public wallet addresses
Suspected Threat Actor	ZeroBytes	N/A	N/A
Country/Region	France	Japan	Israel
Industry	Government	Technology	Financial Services
Possible Repercussions	Targeted phishing and social engineering, identity theft, tax and financial fraud, taxpayer and business impersonation, and property-related fraud	Account takeover, phishing, and further credential stuffing attacks, business identity theft, and supply chain risk	Financial fraud, targeted phishing, SIM swapping, customer impersonation, and wallet targeting

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings



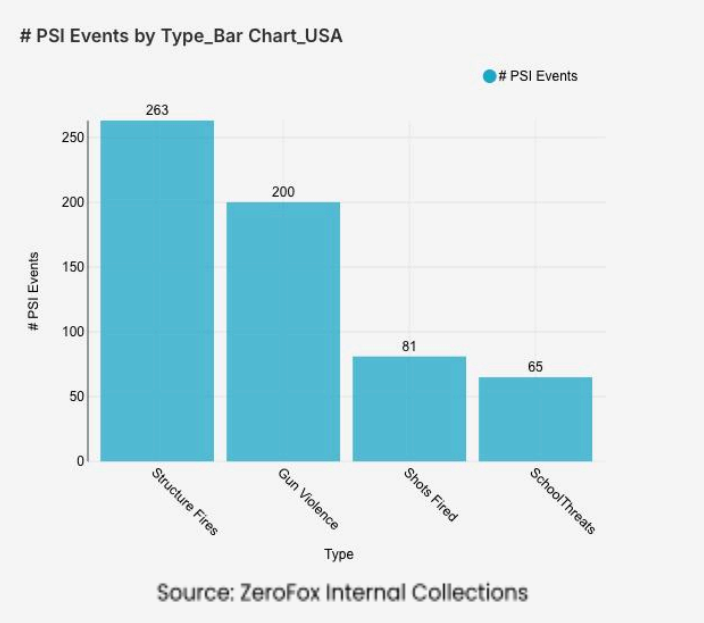
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 12 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 Ukraine, in that order. Approximately 73 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 21 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 6 percent from the previous week, and alerts related to the war in Iran decreased by 25 percent. Events related to Russia's war with Ukraine increased by 38 percent. The top three most-alerted subtypes were structure fires, which saw a 5 percent increase from the previous week; gun violence, which increased by 14 percent; and gas leaks, which increased by 32 percent. Notably, earthquakes increased by 13 percent, with the top contributing country being Indonesia.

- **What this means:** This week's slight decline in mass casualty events leaves the Palestinian territories, India, and Ukraine as top contributors, reflecting active conflict and safety crises in each. In Gaza, an Israeli strike on a police headquarters killed at least 10 people and wounded 15 on August 19, just a day after a separate strike on a cafe killed six and wounded 14. On August 19, Ukrainian drones struck a Russian oil refinery in Ufa, while a Russian attack on Zaporizhzhia killed one person and injured six, sparking fires and building damage. India saw a hotel fire in Kolkata that killed nine people on August 19, just two days after another hotel fire in West Bengal killed eight and a gas leak at a Maharashtra chemical plant killed two on August 17. Indonesia's earthquake activity remains elevated, as a 5.9-magnitude quake struck the Flores region early on August 20, part of the continuing aftershock sequence from the deadly 7.7-magnitude quake on August 15 that has already killed at least 68 people and destroyed hundreds of homes. In short, global physical security remains volatile, with active conflicts, infrastructure failures, and ongoing seismic activity continuing to drive casualties worldwide.

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 shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, shots fired alerts include shootings with no confirmed victims, 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 31 percent of this week's nationwide total. Gun violence across the United States overall increased by 1 percent from the week prior. Shots fired alerts increased by 19 percent, and the top contributing states were Illinois and Ohio. Structure fires decreased by 4 percent, and the top two states for this subtype were New York and California. Notably, school-related threats increased by 59 percent across the country.

- **What this means:** This week's domestic security environment saw continued volatility in firearm instances and man-made disasters. Gun violence and shots fired stayed concentrated in Illinois and Ohio this week; Chicago logged at least 24 people shot, six fatally, in a single weekend of shootings across the city (August 15–17). In Ohio, three teenagers were arrested on murder charges after a fatal shooting in Cincinnati on August 18. Meanwhile, New York State Police rescued a man trapped inside a burning residence in Oswegatchie on August 13, while California's Timber Fire near Big Sur continued threatening structures and forcing highway closures through August 17. School-related threats also spiked; Wheatland, California, saw three straight days of anonymous threats against Wheatland Union High School and Bear River School, including a bomb threat that prompted a search by explosive-detection K-9 teams before campuses were reopened on August 19. Meanwhile, a teenager was arrested in LaGrange, Georgia, on August 19 after allegedly threatening to shoot classmates at LaGrange Academy. Taken together, the data reflects a domestic security landscape defined by concentrated, high-casualty gun violence in the Midwest and a sharp rise in school-related threats 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%