ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 16, 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 August 14, 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 - DragonForce Announces New Service Updates

On July 31, 2025, an account associated with DragonForce, a ransomware and digital extortion (R&DE) collective, posted on the Russian-speaking dark web forum Russian Anonymous Marketplace (RAMP), announcing various new features for existing services, including updates for its crypto locker. In the post on RAMP, the account associated with DragonForce states that the lockers—which refer to the payload that encrypts target files—are now transitioning to a stable version from the previous beta version. ZeroFox observed a significant uptick in DragonForce activity, beginning in early April 2025—leading to the collective's most prominent month, in which the group conducted at least 25 separate attacks. This latest announcement by DragonForce likely indicates that the collective seeks to remain a prominent threat actor in the R&DE space and attract new affiliates.

ZeroFox Intelligence Flash Report - Threat Collectives Seemingly Announce Collaboration

On August 8, 2025, a new channel named "scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS" surfaced on instant messaging platform Telegram. The channel was launched by individuals claiming to be part of the prominent cybercrime collectives Scattered Spider, Lapsus$, and ShinyHunters. In its brief four-day lifespan, posts on the channel resembled the types of activity Scattered Spider, ShinyHunters, and Lapsus$ are known for within their own Telegram channels. In the new Telegram channel, "Shiny" alleged that BreachForums is now under the control of a French cybercrime law enforcement unit, with assistance from the U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI). Although the majority of the claims remain unverified, there is a roughly even chance that the launch of this new Telegram channel signals an intent by Scattered Spider, ShinyHunters, and Lapsus$ to collaborate in future cybercrime operations.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 16

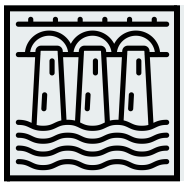
The Underground Economist is an intelligence-focused series that highlights dark web findings from our ZeroFox Dark Ops intelligence team.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Russia Linked to Dam Cyberattack in Norway, Officials Say

What we know:

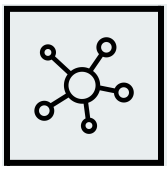
- Oslo has formally attributed a cyberattack to Russia after hackers briefly seized control of a Norwegian dam earlier this year.
- On April 7, 2025, Russian hackers briefly took control of a hydropower dam in Bremanger, Western Norway.
- They opened a flood gate, releasing 500 litres (132 gallons) of water per second for four hours before the breach was detected and stopped.
- No injuries occurred, but it marked the first time Norway officially attributed such an attack to Russia.

Background:

- Norway produces most of its electricity via hydropower, making dams critical national infrastructure.
- Intelligence agencies have warned about the growing risk of cyberattacks on Norway's energy sector.
- NATO-member Norway shares an Arctic border with Russia, supports Ukraine, and is Europe's largest gas supplier via North Sea pipelines.
- Similar warnings have been issued across Europe, with UK intelligence alleging Russia has engaged in sabotage campaigns to intimidate pro-Ukraine states.

What is next:

- It is likely that there will be increased security and monitoring of Norway's critical infrastructure, especially energy facilities.
- Potential retaliatory or defensive cyber operations by Norway or NATO allies are likely.
- Escalation of Russia–Norway tensions is likely, especially given Norway's role in European energy supply.
- The replication of such attacks in other Nordic or European states are also likely to spread fear and chaos among the public.



New AI Exploit Targets ChatGPT Connectors to Access Sensitive Cloud Data

What we know:

- A new flaw, dubbed AgentFlayer, enables attackers to steal sensitive data from users' connected accounts (such as Google Drive) without any clicks.

Background:

- Connectors allow ChatGPT to link with external apps to summarize or work with user files. Attackers can abuse this by embedding malicious prompts into otherwise normal-looking files.

Analyst note:

- This attack enables covert, automated theft of personal or corporate data without user awareness. Sensitive items like API keys, financial records, or private documents could be extracted, likely leading to account takeovers, large-scale fraud, or further targeted cyberattacks.

Law Enforcement Agencies Using TETRA Radio Risk Eavesdropping

What we know:

- Newly detected security issues in the Terrestrial Trunked Radio (TETRA) communications protocol, widely used by law enforcement and the military in various countries, can be exploited to intercept radio communications.

Background:

- The new security issues make systems susceptible to packet injection attacks, replay, brute force attacks, and decryption of encrypted traffic and also include issues stemming from an insufficient patch for another TETRA bug. The exploit depends on use-cases and configurations of a TETRA network. So far, no exploits have been detected in the wild.

Analyst note:

- If successfully exploited, the vulnerabilities are likely to expose sensitive communications of security forces and enable threat actors to monitor their movement and disrupt or jam communications temporarily.

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 five vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on August 12 and August 13. CISA also released 49 Industrial Control Systems (ICS) advisories on August 7, August 12, and August 14. CISA also issued an emergency directive on August 7 for all Federal Civilian Executive Branch (FCEB) agencies to patch vulnerability CVE-2025-53786. Microsoft's August 2025 Patch Tuesday fixed over 100 flaws, including one zero-day and 13 critical flaws, with several addressing remote code execution (RCE) vulnerabilities that allow arbitrary code execution. Ivanti and SAP have released patch advisories for more than 20 vulnerabilities. While vulnerabilities in the TETRA protocol used by law enforcement and military could enable interception and manipulation of radio communications, no in-the-wild exploits have yet been reported. CVE-2025-6543 is a patched memory overflow flaw in Citrix NetScaler that was exploited to breach critical entities in the Netherlands. According to Netherland's NCSC, attackers abused it for RCE and denial-of-service attacks. Researchers have found multiple flaws that can be exploited without authentication to crash domain controllers and systems.

CRITICAL

CVE-2025-25256

What happened: Fortinet has warned of this critical FortiSIEM flaw enabling unauthenticated remote command injection. While not confirmed as a zero-day, Fortinet acknowledged the existence of functional exploit code.

- **What this means:** The flaw is likely to enable threat actors to breach a target's network without being detected. FortiSIEM is widely used by governments, large enterprises, financial institutions, and healthcare providers.
- **Affected products:**
  - FortiSIEM 7.3.0 to 7.3.1
  - FortiSIEM 7.2.0 to 7.2.5
  - FortiSIEM 7.1.0 to 7.1.7
  - FortiSIEM 7.0.0 to 7.0.3
  - FortiSIEM 6.7.0 to 6.7.9
  - FortiSIEM 6.6 (all versions)

- FortiSIEM 6.5 (all versions)
- FortiSIEM 6.4 (all versions)
- FortiSIEM 6.3 (all versions)
- FortiSIEM 6.2 (all versions)
- FortiSIEM 6.1 (all versions)
- FortiSIEM 5.4 (all versions)

CRITICAL

CVE-2025-8088

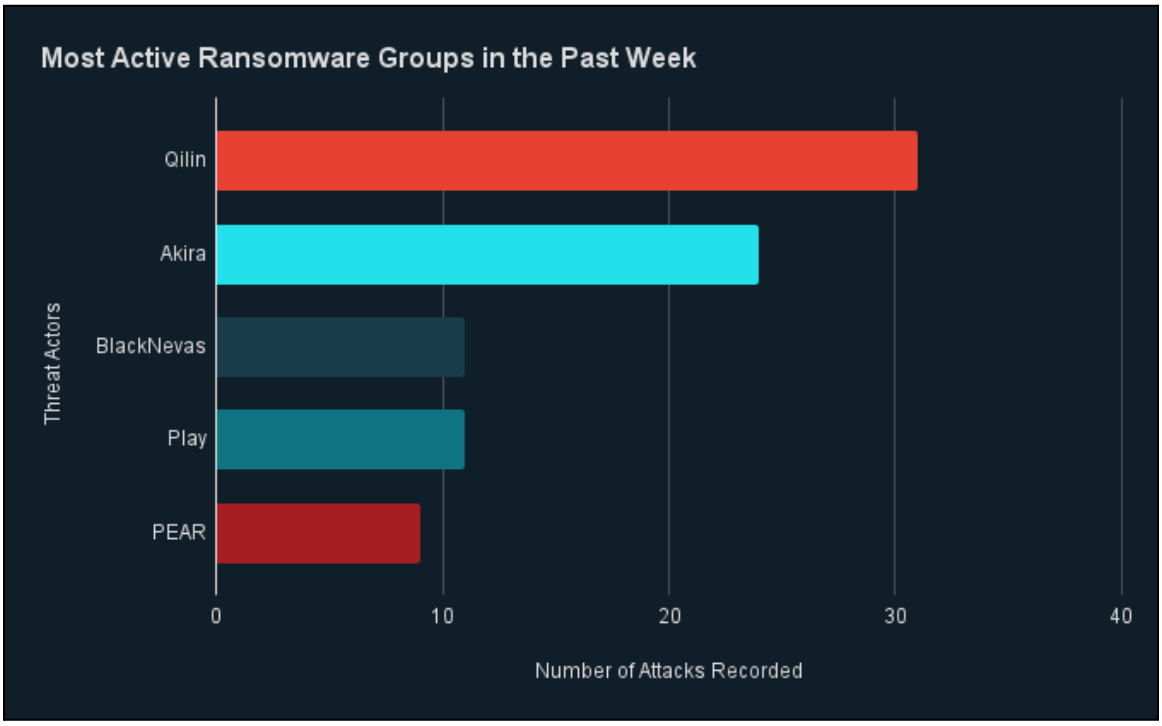
What happened: CVE-2025-8088 is a directory traversal flaw in WinRAR that enables threat actors to utilize specially crafted archives to extract files into attacker-chosen paths, enabling RCE. The flaw was exploited as a zero-day in spearphishing campaigns to deliver RomCom malware before it was patched in WinRAR 7.13.

- **What this means:** Attackers could exploit it to place executables in autorun folders, causing them to run automatically on user login. Users must manually update WinRAR, as it lacks an auto-update feature, to prevent further exploitation.
- **Affected products:**
  - WinRAR versions 0 to 7.12

Ransomware and Breach Intelligence

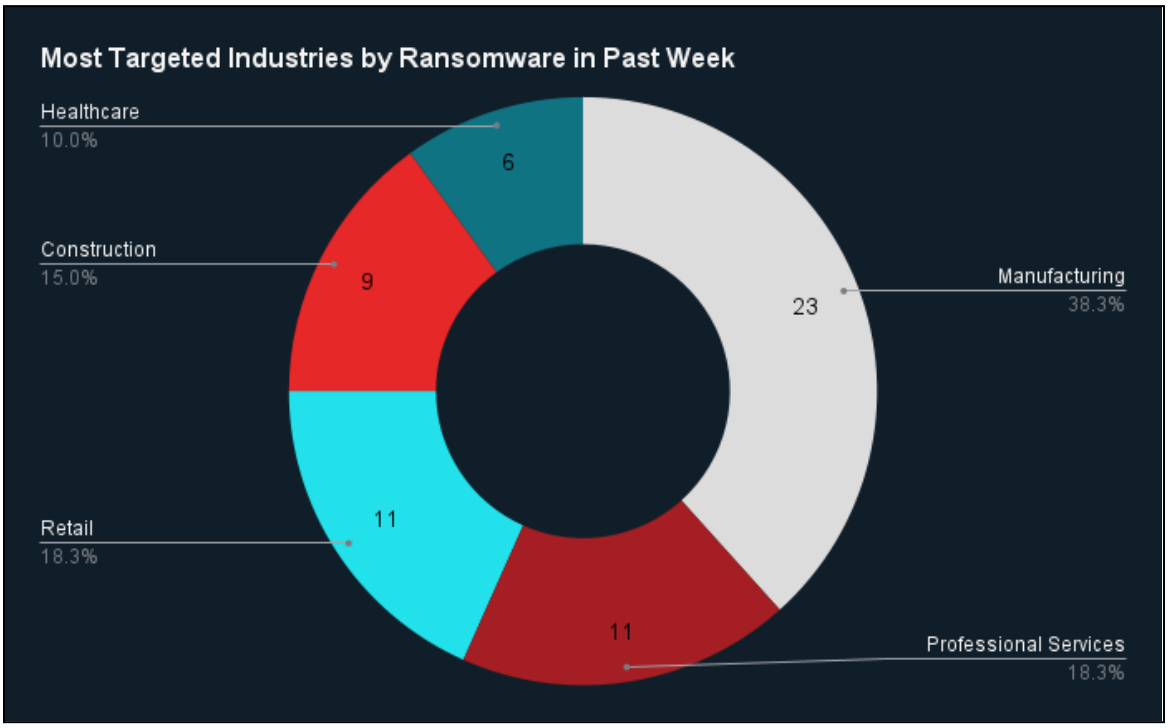
Ransomware and Breach Intelligence Key Findings

Ransomware Trends in the Past Week



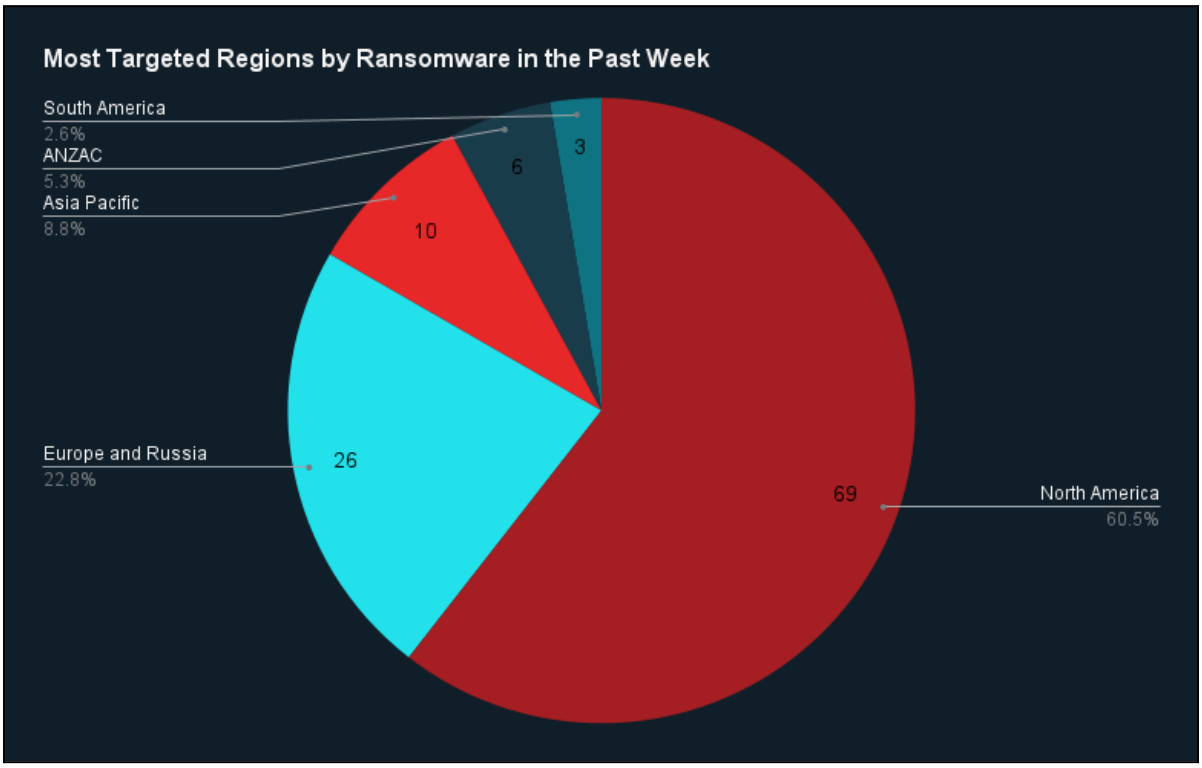
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Akira, BlackNevas, Play, and PEAR were the most active ransomware groups. ZeroFox observed at least 111 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, retail, construction, 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 69 ransomware attacks in North America, while Europe and Russia accounted for 26, Asia-Pacific (APAC) for 10, Australia and New Zealand (ANZAC) for six, and South America for three.

Recap of major ransomware events observed in the past week: The U.S. DOJ announced that, along with international law enforcement, they have dismantled key infrastructure of the BlackSuit (Royal) ransomware group, seizing four servers, nine domains, and over USD 1 million in cryptocurrency. The encryptors of Iran-linked advanced persistent threat (APT) MuddyWater's DarkBit ransomware have been cracked, allowing for free data recovery without having to pay a ransom. A North Korean hacking group known as ScarCruft has reportedly added a new ransomware called "VCD" to its playbook of attacks. The Interlock ransomware group has claimed to have stolen 43 GB of data from Saint Paul, Minnesota, on its leak site.

Major Data Breaches Reported in the Past Week

Targeted Entity	Manpower	Connex Credit Union	Air France–KLM Group
Compromised Entities/Data Set	144,189 individuals	172,000 members	Undisclosed number of customers
Compromised Data Fields	Reportedly, personally identifiable information (PII), including passport scans, identity cards, Social Security numbers (SSNs), addresses, contact details; and other data such as corporate correspondence, financial statements, HR data analytics, confidential contracts, and non-disclosure agreements.	Members' names, account numbers, debit card information, SSNs, and other government identity details.	Customer data other than financial information; this includes names, email addresses, contact details, rewards program information, and latest transactions.
Suspected Threat Actor	N/A	ShinyHunters and/or Scattered Spider	ShinyHunters and/or Scattered Spider
Country/Region	United States	United States	Global
Industry	Professional Services	Financial Services	Transportation
Possible Repercussions	Exposed individuals are likely at risk of identity theft, social engineering, and phishing attacks aimed at extorting money. Stolen corporate data likely risks reputational threats to exposed organizations.	The compromised information could be exploited for identity theft, financial fraud, and phishing attacks.	Exposed customers are likely to be targeted by phishing and social engineering attacks.

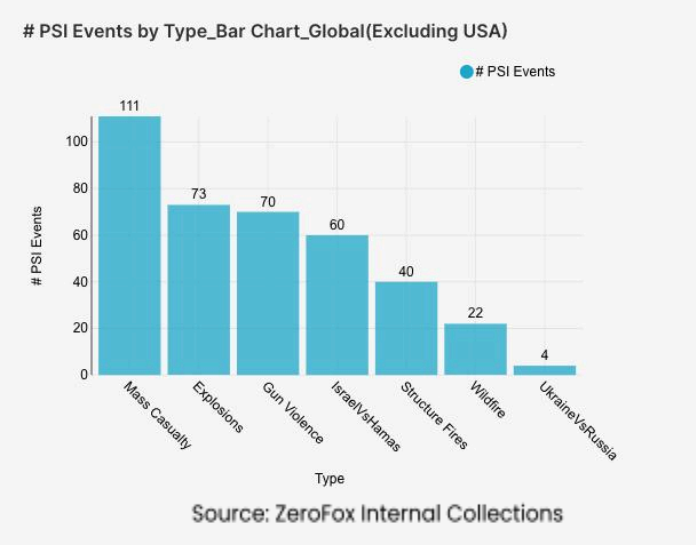
Three major breaches observed in the past week

Other major data breaches observed in the past week: French telecommunication service provider Bouygues Telecom warned that it has suffered a data breach that has resulted in 6.4 million records of customer data being exposed. Hackers "Saber" and "cyb0rg" have claimed and published a data breach exposing a North Korean government hacker. In 2024, the healthcare industry recorded over 700 data breaches—more than any other sector, including finance—which has exposed over 275 million patient records. In most cases, password-related vulnerabilities were the primary attack vector. In the past week, three oral healthcare practices in the United States announced data breaches.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

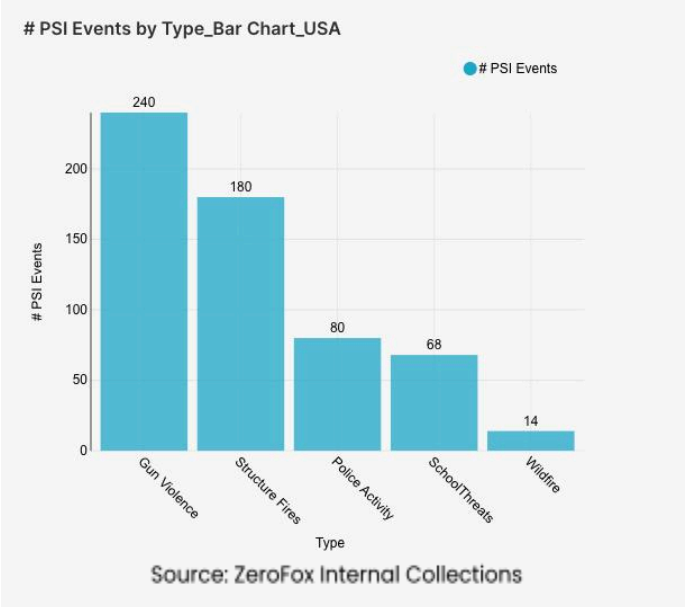
Physical Security Intelligence: Global



What happened: Excluding the United States, there was a 2 percent increase in mass casualty events this week from the previous week, with the top contributing countries and territories being the Palestinian Territories, India, and Pakistan, in that order. Approximately 66 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 33 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) decreased by 6 percent from the previous week. Events related to Russia's war in Ukraine decreased by 64 percent. The top three most-alerted subtypes were explosions, which saw a 4 percent decrease from the previous week; gun violence, which decreased by 7 percent; and structure fires, which increased by 38 percent. Notably, wildfires showed an increase of 214 percent.

- **What this means:** Despite only a small increase in mass casualty events globally, the nature of threats continues to shift week on week. In Pakistan, a series of militant attacks on August 14 targeting police left five officers dead and eight wounded in the Khyber Pakhtunkhwa province, where a government operation against insurgents has displaced 100,000 people. Similarly, in India, a soldier was killed in an exchange of fire on August 13 while foiling an infiltration bid in Kashmir, underscoring ongoing border violence. While the overall alerts for the Israel-Hamas conflict decreased somewhat, the Palestinian Territories continue to face a dire humanitarian crisis, with numerous recent incidents of strikes resulting in mass casualties. Notably, global wildfires showed a dramatic increase this week, reflecting the surge in structure fire alerts as well; across Southern Europe, intense wildfires are currently raging due to a severe heat wave, forcing evacuations and damaging large areas of land and infrastructure in multiple countries. The data reveals a complex global security landscape, marked by persistent localized violence and environmental threats, highlighting that physical security is increasingly affected by both deliberate acts and natural disasters.

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, structure fires are fires that affect man-made buildings, and police activity indicates heightened law enforcement presence for various reasons. The top two states that had the most gun violence alerts were Illinois and Ohio, which together made up 25 percent of this week's nationwide total. Gun violence across the United States overall increased by 13 percent from the previous week. Police activity alerts increased by 31 percent, and the top contributing states were California and Texas. Structure fires increased by 64 percent, and the top two states for this subtype were California and New York. Notably, threats related to schools (excluding protests) increased by 119 percent.

- **What this means:** In the past week, there was a notable shift in US physical security trends, marked by significant increases in shootings. Illinois, which recorded the highest number of gun violence incidents, saw three different mass shootings in Chicago, including one on August 11 outside of a building for senior citizens that left five injured. A major driver of the week's alerts was the start of the academic year; for instance, on August 13, a teenager in Florida was arrested after he created a false text message thread threatening a shooting at Clay High School, which resulted in a lockdown. According to a study conducted by the U.S. Secret Service, threats against schools are most likely to happen within the first week after a holiday or absence, which correlates with the dramatic increase in alerts seen this week. Structure fires also increased significantly, a trend influenced by both wildfires (such as the Gifford Fire in California) and residential incidents. The provided data highlights a complex domestic security landscape, in which rising crime rates and environmental risks are now compounded by a dramatic surge in school-related threats.

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%