ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

SEPTEMBER 12, 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 10, 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 – Qilin Claims Record Number of Monthly Attacks for 2026

ZeroFox observed that Qilin was the most prominent ransomware and digital extortion (R&DE) collective in August 2026, accounting for at least 165 incidents—a record number of incidents for one collective so far this year. Qilin has remained the most active R&DE collective globally, signaling both its dominance thus far into 2026 and an unbroken 17-month period as the leading ransomware threat actor since Q2 2025. Qilin accounted for a nearly 29 percent share of the top 10 most active collectives, which together were responsible for at least 6,453 incidents since April 2025 (Q2 2025). The next most active collective, Akira, had a share of approximately 14 percent, underpinning Qilin's continuous prominence. The collective is very likely to continue or exceed its current operational tempo—outpacing other collectives by a substantial margin—and will likely remain consistent with its established tactics, techniques, and procedures (TTPs) and continue to target geographically dispersed, multi-sector entities with double-extortion operations.

ZeroFox Intelligence Assessment – August 2026 Ransomware Wrap-Up

ZeroFox observed at least 863 separate ransomware and digital extortion (R&DE) incidents in August 2026, an increase of approximately 11 percent from the 776 incidents recorded in July 2026. Additionally, August 2026 marked an approximate 98 percent increase year-over-year from the 436 incidents recorded in 2025 and an approximate 121 percent increase from the 390 incidents recorded in 2024. North American targets saw a 50 percent increase in year-over-year incidents from August 2025; however, this was a decrease in global share from the approximate 61 percent observed in August 2025 to an approximate 46 percent observed in August 2026. In August 2026, ZeroFox observed that the manufacturing industry remained the most targeted sector, with at least 175 recorded R&DE incidents (an increase from the 159 observed in July 2026). ZeroFox observed that the five most active R&DE collectives in August 2026 were almost certainly Qilin, The Gentlemen, Cl0p, Orova, and Dire Wolf. This is a change from July 2026, with only The Gentlemen and Qilin remaining in the top five from the previous month.

ZEROFOX

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Xinbi Infrastructure Disrupted for Supporting Transnational Scam Operations

What we know:

- The U.S. Department of the Treasury has sanctioned Xinbi Guarantee, a Chinese-language marketplace for scam services, and seized its Telegram infrastructure and crypto wallets.
- The action also targeted two other entities for allegedly providing encrypted communications and cryptocurrency payment services that helped Xinbi maintain its criminal operations.

Background:

- Xinbi Guarantee allegedly operated a Telegram-based marketplace connecting scam operators with vendors offering money laundering, scam site creation, and trafficking-related services, with some U.S. victims' funds traced to vendors on the platform.
- The marketplace has processed more than USD 24 billion and supported scam centers, cybercrime, and money laundering.
- In March 2026, the United Kingdom had also sanctioned Xinbi Guarantee.

Analyst note:

- Following the disruption, Xinbi's operators are likely to attempt to restore disrupted services under replacement infrastructure or a different name.
- However, the targeting of the two supporting entities is likely to complicate efforts to replace the communications and payment infrastructure that supported Xinbi, likely forcing operators to diversify providers, rebuild components, and establish new cryptocurrency channels.

Thomson Reuters Breach Impacts U.S. and Canadian Court Systems

What we know:

- Thomson Reuters has reportedly confirmed unauthorized access to its court case management platform, C-Track, exposing court records across the United States and Canada.

- Separately, U.S. legal firms Quinn Emanuel and McDermott reported social engineering-related breaches involving sensitive files.

Background:

- The unauthorized access to C-Track reportedly took place in March 2026.
- The affected court records contained names and other personal information, although the specific data compromised remains unclear.
- Thomson Reuters said C-Track remains operational and that affected customers have been notified.

Analyst note:

- The incident at Thomson Reuters and the two law firms likely indicate a campaign targeting the U.S. legal sector.
- The sensitive information involving breaches at legal entities is very likely to enable threat actors to extort individuals and entities.

Scammers Extort Instagram Creators Using Fake Copyright Claims

What we know:

- Scammers are reportedly targeting Instagram creators with fraudulent copyright claims threatening content removals, account suspensions, or demonetization and demanding money to withdraw the claims.
- The activity has reportedly affected creators with large audiences, including one account with more than 1.5 million followers whose owner paid USD 50 in cryptocurrency to regain access after the account was temporarily suspended.

Background:

- The scammers exploited Instagram's copyright reporting process by submitting repeated claims and then contacting affected users through private messaging platforms such as Telegram to demand payment.
- Three individuals admitted filing copyright strikes despite not being the rights holders, while one claimant reportedly demanded USD 900 to withdraw a complaint.
- Meta said it has restored affected creators' content and added protections.

Analyst note:

- Use of artificial intelligence (AI) tools is likely to help threat actors scale this campaign further, echoing prior copyright strike extortion campaigns against YouTube creators.

- Affected creators should document and report attempts rather than pay, as payment has not reliably stopped renewed strikes.

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 nine new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on September 4, September 8, and September 9, 2026. Additionally, CISA released one Industrial Control Systems (ICS) advisory on September 8, 2026. Microsoft has patched 974 vulnerabilities across its products for September 2026 Patch Tuesday, including an improper link resolution flaw in the Windows Update Stack (CVE-2026-81963) that enables privilege escalation to System. Fortinet has patched 10 vulnerabilities across FortiMonitor OnSight, FortiPAM, FortiSandbox, FortiOS, FortiProxy, and FortiManager, including two flaws enabling unauthenticated remote attackers to bypass authentication or proxy user traffic. A zero-day remote code execution (RCE) flaw in Adobe Commerce (CVE-2026-75650) enables unauthenticated attackers to inject and execute arbitrary PHP code through failed payment emails without user interaction. Google released a Chrome security update to patch 12 vulnerabilities, including an actively exploited type confusion zero-day in the V8 engine (CVE-2026-85046) allowing RCE inside Chrome's sandbox.

CRITICAL

CVE-2026-20212

What happened: This is an actively exploited zero-day RCE vulnerability in Cisco Nexus 9000 Series switches running Silicon One-based hardware that enables an unauthenticated remote attacker to execute arbitrary code with root privileges.

- **What this means:** The vulnerability exposes TCP ports 43210 and 43211 due to binding to an unrestricted IP address. Nexus 9000 series switches with Silicon One architecture are used in modern AI data centers; successful exploitation is likely to enable threat actors to disrupt AI workloads or manipulate traffic, further resulting in outages.
- **Affected products:**
  - Cisco Nexus 9000 Series switches with Silicon One architecture

HIGH

CVE-2026-85880

What happened: This is an actively exploited zero-day vulnerability in Windows Advanced Local Procedure Call (ALPC) that enables an attacker running code in a low-privilege AppContainer to escape the sandbox and elevate privileges to System without user interaction.

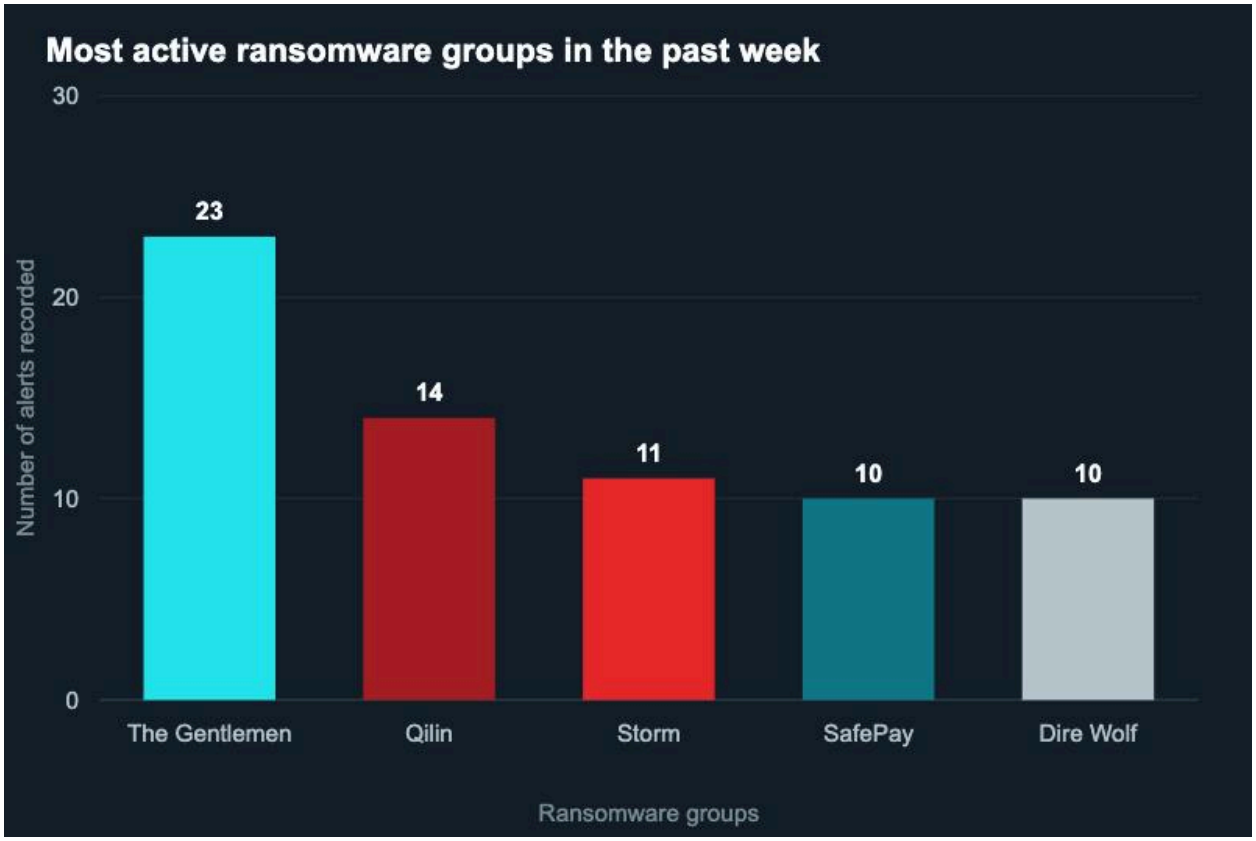
- **What this means:** Successful exploitation allows unauthenticated local attackers or compromised low-privilege processes to achieve complete administrative control on affected Windows systems.
- **Affected products:**
  - Windows 10, Windows 11, and Windows Server 2022/2025

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

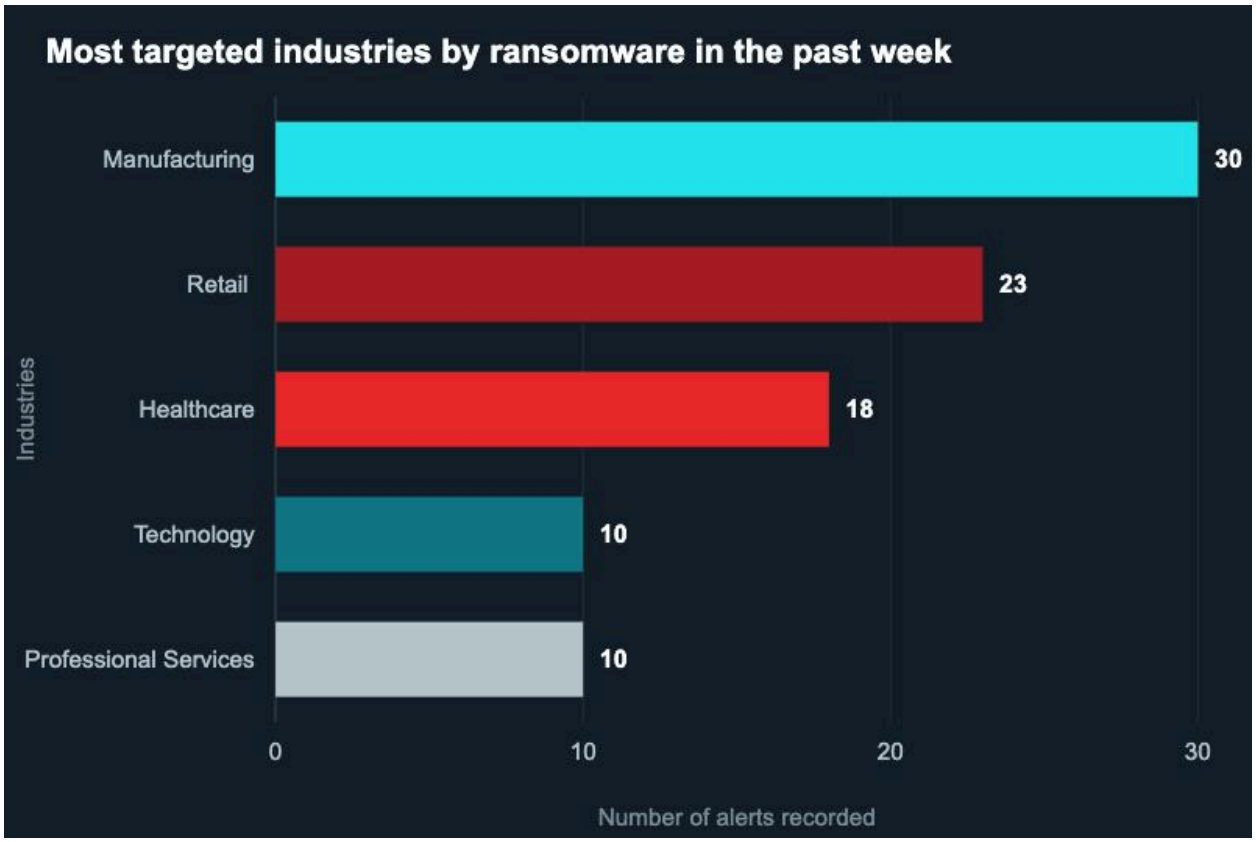
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, The Gentlemen, Qilin, Storm, SafePay, and Dire Wolf were the most active ransomware groups. ZeroFox observed close to 157 ransomware victims disclosed, most of whom were located in North America. The Gentlemen ransomware group accounted for the largest number of attacks, followed by Qilin.



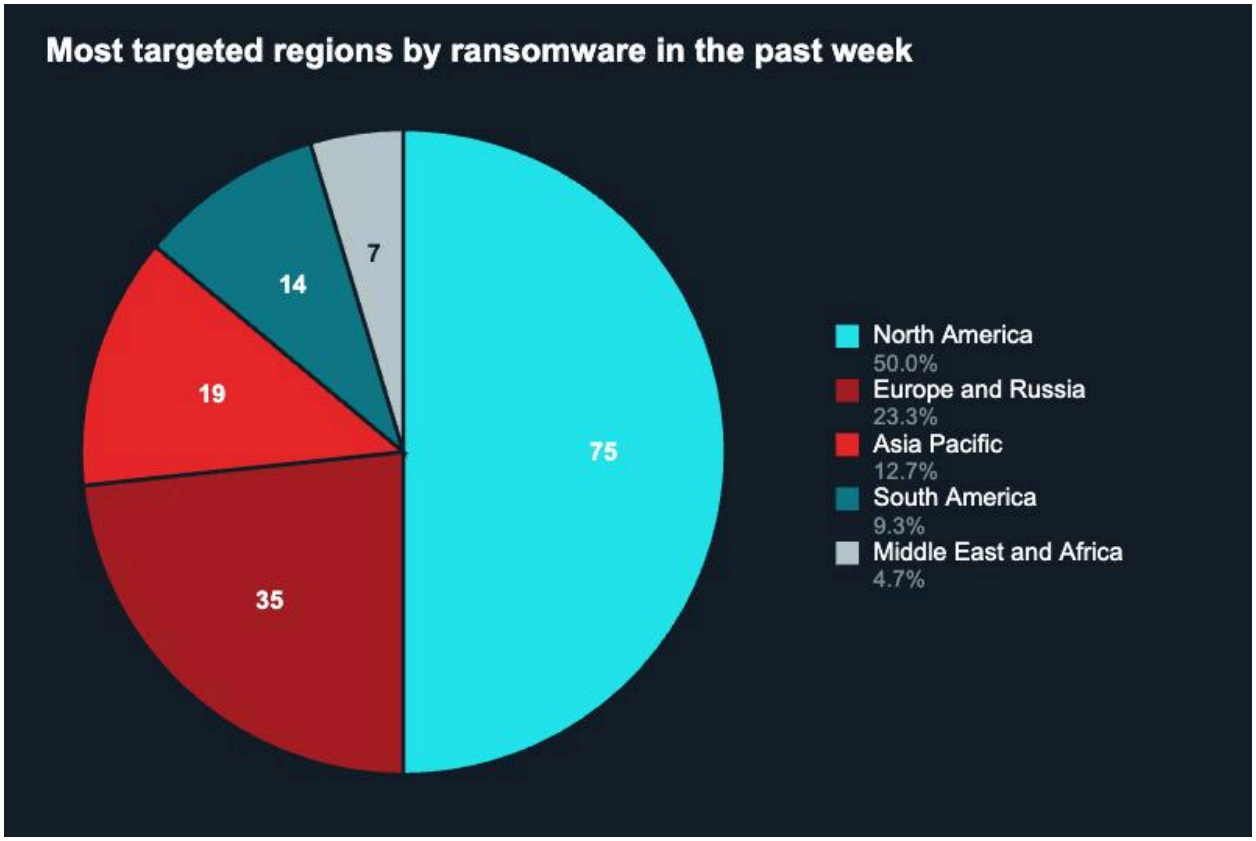
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that manufacturing was the industry most targeted by ransomware attacks, followed by retail, healthcare, technology, 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 75 ransomware attacks observed in North America, while Europe and Russia accounted for 35, Asia-Pacific for 19, South America for 14, and Middle East and Africa for seven.



Source: ZeroFox Internal Collections

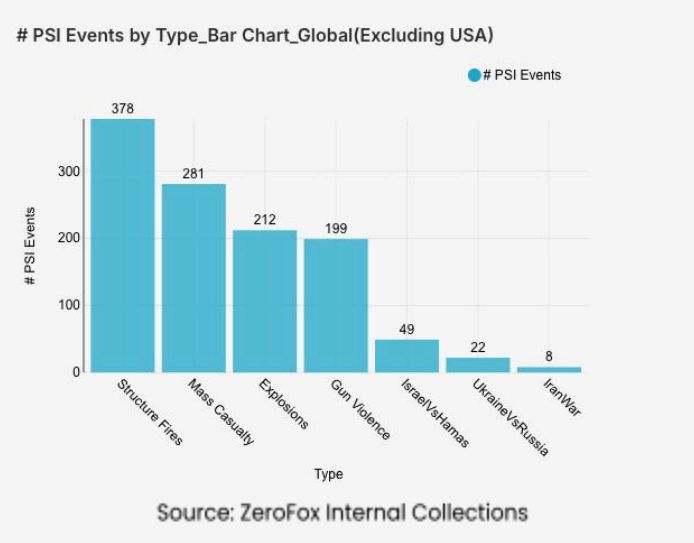
Notable Data Breaches in the Past Week

Targeted Entity	Mathspace	Florida Department of Highway Safety and Motor Vehicles (FLHSMV)	Trezor and ShipMonk
Compromised Entities/Victims	Students, parents, guardians, teachers, and employees (approximately 1.08 million accounts)	Florida driver license holders (approximately 200,000 records)	67,000 customers
Compromised Data Fields	Names, usernames, email addresses, internal user IDs, countries, time zones, account types, and activity dates	Social Security numbers (SSNs), driver identification numbers, physical details, and vehicle registration records	Names, email addresses, phone numbers, and shipping addresses
Suspected Threat Actor	N/A	ShinyHunters	ShinyHunters
Country/Region	Australia / New Zealand	United States	United States
Industry	Education	Government	Retail
Possible Repercussions	Targeted credential stuffing, spear phishing, account takeover, and student identity fraud	Deepfake identity theft, account takeover, auto insurance fraud, and targeted extortion	Targeted phishing, social engineering, impersonation, fraudulent calls or letters, and physical security risks (given the compromise of customers' shipping addresses)

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

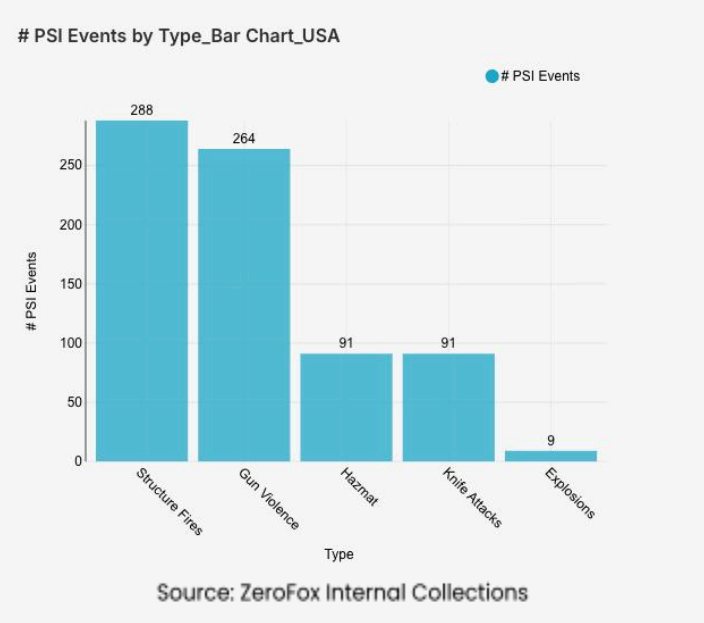


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 6 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian territories, Lebanon, and Mexico, in that order. Approximately 75 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 30 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 31 percent from the previous week, and alerts related to the war in Iran increased by 33 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 12 percent increase from the previous week; gun violence, which decreased by 3 percent; and explosions, which increased by 8 percent.

- **What this means:** This week's data reflects a physical security landscape shaped heavily by active armed conflicts and organized criminal violence rather than isolated incidents. In the Palestinian territories, Israeli strikes have continued despite ceasefire arrangements; on September 10, Israeli airstrikes killed at least four people in the Jabalia refugee camp in northern Gaza, and hit a school in Deir al-Balah on September 6 as part of a broader four-day campaign that killed eight Palestinians. Lebanon has seen a comparable escalation, with an Israeli airstrike on September 7 killing 12 people in the town of Kfar Reman, and an earlier strike in multiple locations on September 4 killing five people amid a wider bombing campaign. Continued high-intensity drone and missile exchanges between Russia and Ukraine in early September 2026—including a Russian drone strike on a residential building in Boryspil around September 4–5 and hundreds of drones and missiles exchanged nightly during that period—account for the sharp increase in war-related alerts there. Together, these trends point to a global security environment in which explosive violence, particularly from state militaries, remains the dominant driver of mass casualty risk.

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 knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, knife attacks are confirmed stabbings or slashings, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Illinois and Texas, which together made up 25 percent of this week's nationwide total. Gun violence across the United States overall increased by 29 percent from the week prior. Knife attack alerts increased by 17 percent, and the top contributing states were New York and Illinois. Structure fires decreased by 8 percent, and the top two states for this subtype were California and District of Columbia. Notably, explosions increased by 29 percent.

- **What this means:** This week's data reflects a continued concentration of gun violence in a number of states, alongside a sharp rise in explosive incidents nationwide. In Chicago, IL, police reported that at least 37 people were shot in 30 separate incidents over the Labor Day weekend alone, with eight fatalities recorded. On September 4, a fatal stabbing on a residential block in Brooklyn, NY, left a man dead, contributing to New York's share of this week's confirmed slashing incidents. Structure fires remained active despite a small decrease, with incidents such as a Beverly Hills, CA, apartment fire on September 9 that displaced residents and injured two firefighters and a Washington, D.C., rowhome fire on September 7 that displaced two residents. The notable rise in explosions was underscored by a suspected gas leak explosion at a Fairmont, WV, home on September 8 that caused significant structural damage and hospitalized a resident with burns. Overall, domestic physical security this week was defined by persistent, geographically concentrated gun violence and a rising, more volatile threat from explosive incidents, even as fire-related risk shows a modest improvement.

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%