ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

July 19, 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 July 17, 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 - Arrests Made in Relation to UK Retail Cyber Attacks

On July 10, 2025, four people were reportedly arrested in the United Kingdom as part of a National Crime Agency (NCA) investigation into a series of cyber attacks that occurred in late April 2025, targeting Marks & Spencer (M&S) and other retail stores. The series of cyberattacks targeting UK-based retail organizations began in mid-April 2025 when M&S publicly confirmed that it was managing an unspecified cyber incident. Initially, no cyber threat entity publicly claimed responsibility for the attacks, but widespread reporting alluded to the "Scattered Spider" threat collective being the perpetrators. If the arrested individuals are associated with Scattered Spider, it is likely that the collective's operational tempo will reduce—particularly in the short term—with targeting pivoting toward industries and regions less likely to garner media and law enforcement attention.

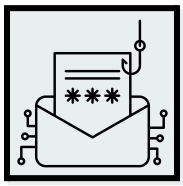
ZeroFox Intelligence Flash Report - Data Set Features Billions of Leaked User Credentials

ZeroFox has procured a significant quantity of leaked data, the existence of which was first announced by cybersecurity researchers on June 18, 2025. Among approximately 16 billion compromised data points, ZeroFox's preliminary analysis identified at least 2.7 billion lines of URL, login, and password (ULP) data, alluding to at least as many separate victims. Although initial media reporting suggested that this data was associated with a singular data breach, it is significantly more likely that it was compiled from various stealer logs. As of this writing, ZeroFox is unable to determine the usability of this data or the extent to which it is associated with contemporary accounts that may be vulnerable to compromise. Initial analysis suggests that much of the data is dated between January and June 2025, indicating a likely chance that a high proportion of the identified data would provide malicious utility to those in possession of it.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



China-Linked Attackers Targets Taiwan's Chip Industry in Phishing Campaigns

What we know:

- At least three China-linked hacking groups have launched cyber espionage campaigns between March and June 2025, targeting Taiwan's semiconductor industry and investment analysts.
- The attackers used spear-phishing tactics—often posing as job seekers or investment firms—to infiltrate organizations across the semiconductor supply chain.

Background:

- The groups were observed targeting semiconductor firms using compromised Taiwanese university emails to pose as job seekers and deliver malware via malicious PDFs or password-protected archives.
- They also impersonated a fictitious investment firm to phish financial analysts focused on Taiwan's chip sector, with operations spanning Asia as well.

What is next:

- This increased activity is likely a response to the United States' restrictions on U.S.-designed chip imports to China.
- The campaign likely threatens Taiwan's semiconductor industry, exposing proprietary chip designs, manufacturing processes, and supply chain data to foreign intelligence.
- By compromising analysts and other suppliers, the threat attackers could gain early insights into corporate strategies, giving China a strategic advantage amid these ongoing chip trade restrictions.

Four Arrested in the United Kingdom over Cyberattacks on M&S and More

What we know:

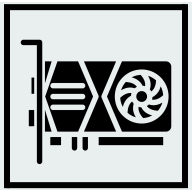
- Four individuals have been arrested in the United Kingdom under suspicion of cyber offences targeting M&S, Co-op, and a luxury department store.

Background:

- The four suspects arrested in association with the M&S cyberattack are also believed to have orchestrated another cyberattack targeting a different luxury department store, which caused major disruption and business impact.

Analyst note:

- The seizure of electronic devices could lead to the identification of co-conspirators and infrastructure. It is also likely that the findings will reveal connections to a broader cybercriminal network or a ransomware-as-a-service (RaaS) model, potentially extending the investigation beyond UK borders.



NVIDIA Urges GPU Security Against Possible Rowhammer Attacks

What we know:

- NVIDIA is urging users to turn on System Level ECC—a feature that helps detect and correct memory errors—to protect against Rowhammer attacks that can corrupt GDDR6 memory, a type of graphic processing unit (GPU).

Background:

- Researchers used a tool called GPUHammer on an NVIDIA A6000 graphics card and were able to flip bits in memory, which can silently corrupt data AI model results (dropping accuracy from 80 to 1 percent). Rowhammer attacks are hardware faults that can be triggered by software processes. System errors arise when binary digits are flipped in a memory row to cause a change in in-memory information.

Analyst note:

- Rowhammer attacks on GPU memory could enable threat actors to successfully conduct system denial-of-service, corrupt data, and escalate privileges. Enabling System Level ECC is essential in GPUs to detect and correct memory errors, ensuring reliable AI and system performance.

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) has added one vulnerability to its Known Exploited Vulnerabilities (KEV) catalog and released nine Industrial Control Systems (ICS) advisories on July 15 and July 17. Four vulnerabilities—collectively named PerfektBlue—impact the BlueSDK Bluetooth stack from OpenSynergy and can be exploited to achieve remote code execution, potentially granting access to critical vehicle systems across multiple vendors. A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could enable a remote, unauthenticated attacker to execute arbitrary code on the underlying operating system with root privileges. The Madara – Core plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to and including 2.2.3, due to inadequate file path validation in the `wp_manga_delete_zip()` function. The Bears Backup plugin for WordPress contains a remote code execution vulnerability affecting all versions up to and including 2.0.0. Threat group UNC6148 has been targeting fully-patched, end-of-life SonicWall SMA 100 series appliances since at least October 2024 to deploy a backdoor, OVERSTEP. The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to and including 1.0.4, due to a lack of file type validation in the `image_upload_handle()` function, which is triggered via the `add_booking_type` route. CVE-2025-1727 is a weak authentication vulnerability in the remote linking protocol used by End-of-Train (EoT) and Head-of-Train (HoT) systems.

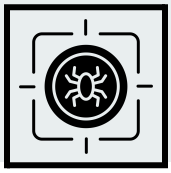
CRITICAL

CVE-2025-47812

What happened: A critical vulnerability, CVE-2025-47812, in Wing FTP Server is being actively exploited. It stems from improper handling of null (\0) bytes in the server's web interface, enabling remote attackers to inject Lua code and execute arbitrary system commands. The flaw has been addressed in version 7.4.4.

- **What this means:** This flaw enables attackers to compromise the server by injecting malicious Lua scripts during the login process. Successful exploitation can lead to full system control with root or SYSTEM-level privileges. Threat actors have been observed using it to run malicious code, conduct system reconnaissance, and install remote monitoring tools. If left unpatched, the vulnerability poses a serious risk of data theft, persistence, and broader network compromise.

- **Affected products:**
  - Wing FTP Server before version 7.4.4



CRITICAL

CVE-2025-25257

What happened: A critical SQL injection vulnerability, CVE-2025-25257, has been disclosed in Fortinet FortiWeb, with proof-of-concept (POC) exploits now publicly available. The flaw allows pre-authenticated remote code execution.

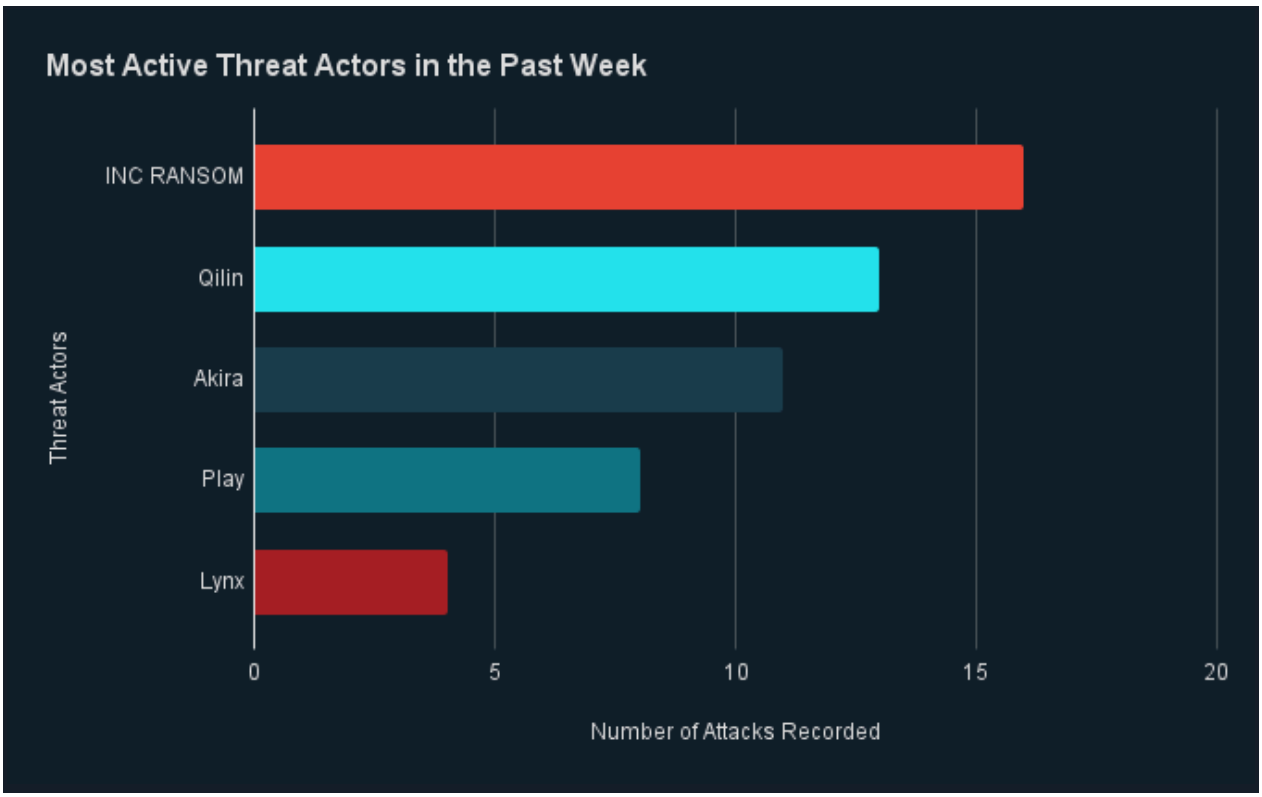
- **What this means:** This vulnerability stems from improper handling of SQL commands in HTTP(S) requests, enabling attackers to inject and execute malicious SQL code without authentication. FortiWeb, a widely used web application firewall, could be fully compromised if unpatched. Exploitation may lead to unauthorized access, data theft, server takeover, and potential lateral movement across protected networks. Fortinet has addressed the flaw in FortiWeb versions 7.6.4, 7.4.8, 7.2.11, 7.0.11, and all subsequent releases.
- **Affected products:**
  - The affected products are listed in this advisory.

.

Ransomware and Breach Intelligence

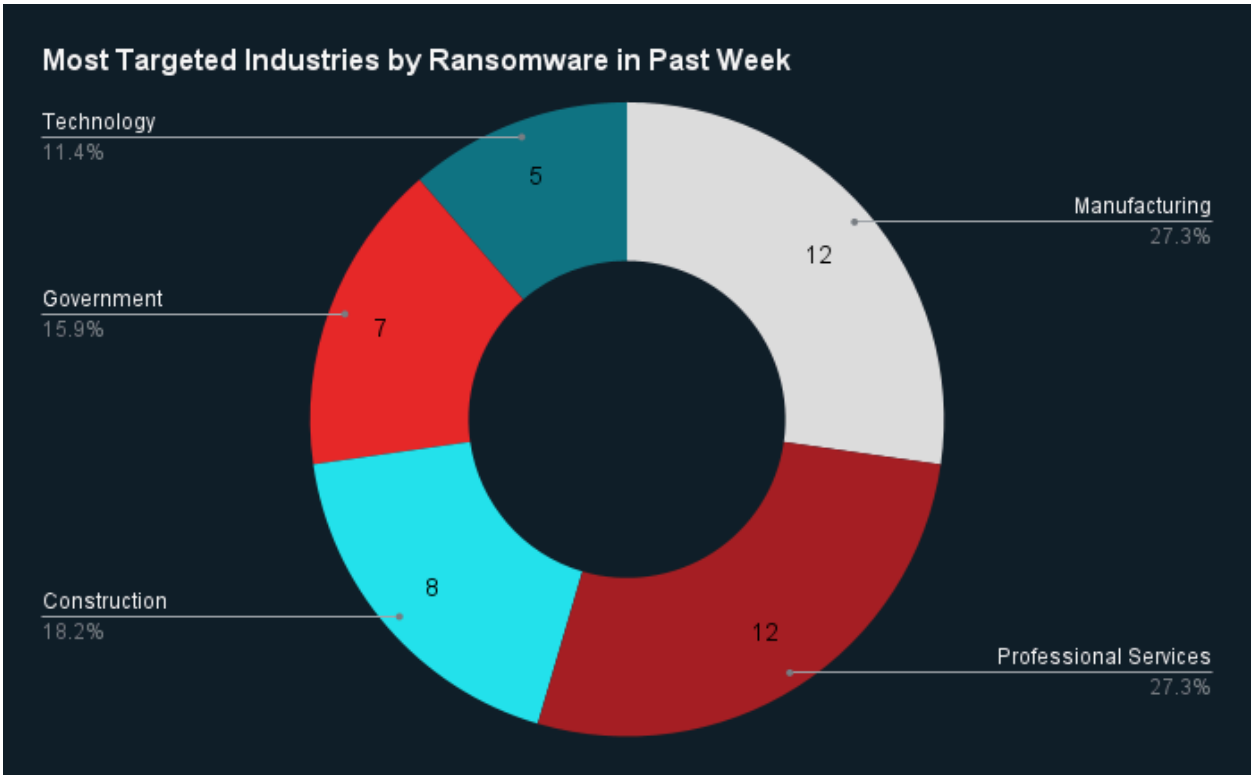
Ransomware and Breach Intelligence Key Findings

Ransomware Updates of the Week



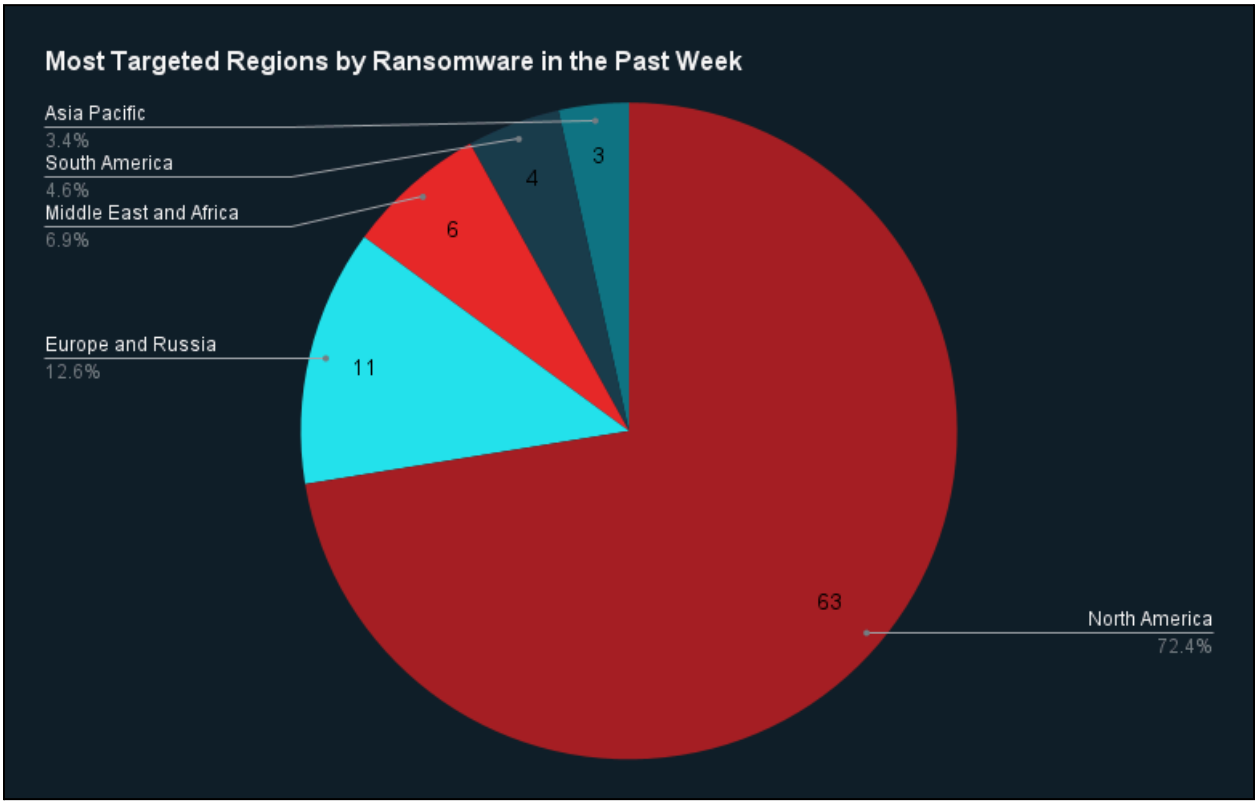
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, INC RANSOM, Qilin, Akira, Play, and Lynx were the most active ransomware groups. ZeroFox observed at least 85 ransomware victims disclosed, most of whom were located in North America. The INC RANSOM ransomware group accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing and professional services were the industries most targeted by ransomware attacks, followed by construction, government, and 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-Russia. North America witnessed 63 ransomware attacks, while Europe-Russia accounted for 11, the Middle East and Africa region for six, South America for four, and Asia-Pacific for three.

Recap of major ransomware events observed in the past week: The DragonForce ransomware group has claimed a cyberattack on U.S. department store chain Belk. Threat actors are using a stealthy phishing technique called "FileFix" in Interlock ransomware attacks to trick users into pasting disguised PowerShell commands into File Explorer. An international law enforcement operation, Operation Elicius, has dismantled a Romanian ransomware group known as Diskstation for extorting companies across Europe since 2021. A new RaaS operation named "GLOBAL GROUP" has integrated AI and mobile-friendly panels into its platform, which is very likely to appeal to a non-English speaking pool of threat actors. Meanwhile, four individuals have been arrested in the United Kingdom in connection to the ransomware attacks on M&S, Co-op, and a luxury department store. A Russian professional basketball player has also been arrested in France at the behest of the United States for allegedly being involved with a ransomware group that targeted over 900 organizations.

Significant Data Leaks in the Past Week

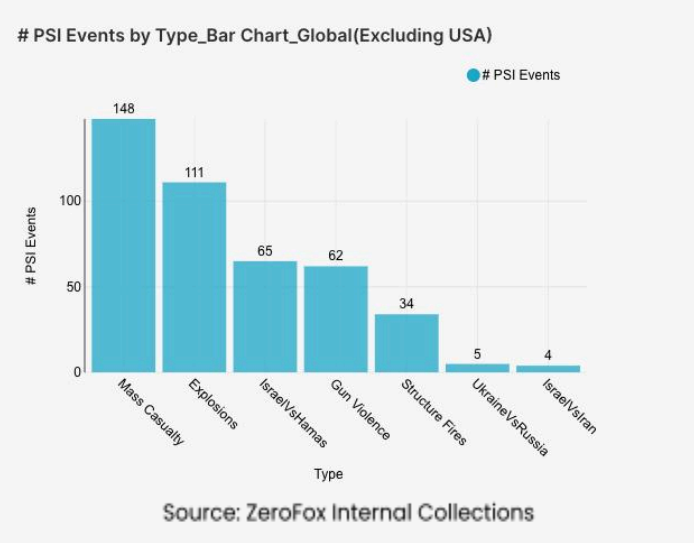
Targeted Entity	Louis Vuitton	Episource	Wiley Rein LLP
Number of Firms/Victims Affected	Yet to be determined	Over 5.4 million customers and partner organizations	Firm personnel and client organizations
Compromised Data Fields	Customers' personally identifiable information (PII), including contact details and purchase history. Financial data—such as credit card details—has not been breached.	Customer and member PII, medical data—including test results—and health insurance information.	Emails
Suspected Threat Actor	N/A	N/A	China-backed hackers
Country/Region	United Kingdom	United States	United States
Industry	Retail	Healthcare	Legal/Consulting
Possible Repercussions	LVMH customer data across multiple worldwide operations is likely impacted by the cyberattack. Exposed customers are likely to be targeted in phishing, social engineering, and impersonation attacks. The incident is very likely to negatively impact the reputation of LVMH.	Threat actors are likely to demand ransom from multiple healthcare organizations working with Episource. Exposed individuals and organizations are likely to be targeted in financially motivated blackmailing, phishing, social engineering, and impersonation attacks.	Chinese hackers were likely attempting to access sensitive negotiations and insider details on U.S. trade policies through the operation.

Three major breaches observed in the past week

Other major data breaches observed in the past week: UK retailer Co-op has disclosed that hackers stole all of the company's customer data, amounting to around 6.5 million members during the April 2025 cyberattack. The data exposed customer names, addresses, and contact details. On July 15, a 2022 data breach at the UK Ministry of Defence (MoD), exposing the PII of 19,000 Afghans who had applied to a secret relocation scheme, was disclosed publicly. The data breach came to light as the UK High Court lifted a gag order on the incident. The data leak put the lives of the 19,000 exposed Afghans at risk as the Taliban seized power in Afghanistan. MaReads, a popular Thai-language fiction and comics platform has suffered a data breach, affecting approximately 74,000 users in June 2025. The compromised data reportedly includes usernames, email addresses, phone numbers, and dates of birth. An unprotected database linked to a Texas adoption agency had exposed over 1.1 million highly sensitive records; the database has been reportedly secured.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

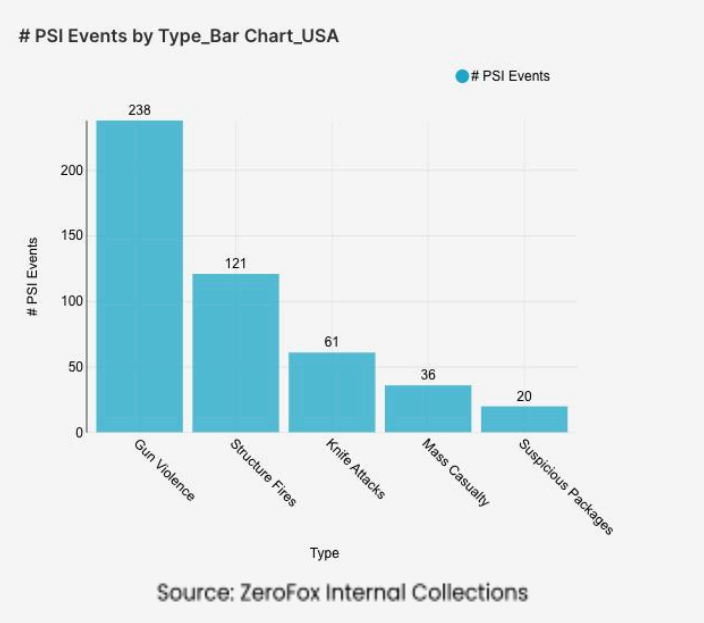


Physical Security Intelligence: Global

What happened: Excluding the United States, there was an 11 percent increase in mass casualty events this week from the previous week. Approximately 75 percent of these events were explosions, and the three aforementioned countries accounted for about 39 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 25 percent from the previous week, and alerts related to the Israel-Iran conflict increased by 33 percent. Events related to Russia's war in Ukraine decreased by 58 percent. The top three most-alerted subtypes were explosions, which saw a 26 percent increase from the previous week; gun violence, which increased by 19 percent; and structure fires, which increased by 42 percent. Global protest activity decreased by 18 percent.

- **What this means:** This week, Syria had the second highest amount of mass casualty alerts due to Israel's recent strikes in Damascus in defense of the Druze minority. Syria's Interior Ministry and Druze leaders announced a renewed ceasefire agreement after the attack, but it is not immediately clear whether the violence will end. The ongoing Israel-Hamas conflict remains a significant driver of alerts as well, with recent reports highlighting continued Israeli strikes in Gaza, including an attack on July 16, which killed 20 people at a food distribution center. Conversely, incidents in relation to the Russia-Ukraine conflict decreased, with U.S. President Trump threatening to impose further sanctions on Russia if it does not reach a ceasefire agreement within 50 days. Additionally, preparations are underway to deliver new Patriot missile systems to Ukraine, which could escalate attacks. In the United Kingdom, more than 70 people were arrested on July 12 at protests against the Palestine Action group being proscribed as a terrorist organization, which may have deterred other demonstrations from taking place, thereby contributing to the overall decrease.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, knife attacks refer to confirmed slashings and stabbings, and structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were Illinois and Pennsylvania, which together made up 18 percent of this week's nationwide total. Gun violence across the United States overall decreased by 12 percent from the week prior. Knife attack alerts decreased by 9 percent, and the top contributing states were New York and Pennsylvania. Structure fires decreased by 35 percent, and the top two states for this subtype were New York and California. Notably, suspicious package incidents increased by 82 percent.

- **What this means:** In the past week, domestic security concerns in the United States have primarily been driven by conventional criminal activities despite decreases in all top three subtypes. Although global protest activity also decreased, localized demonstrations—such as those targeting Palantir Technologies in various cities on July 14 due to its work with U.S. Immigration and Customs Enforcement (ICE) and the Israeli military—indicate ongoing public dissent on specific issues. Protest numbers may see an increase this week as part of the multiple July 17 Good Trouble Lives On demonstrations against various Trump administration policies. One striking trend was the sharp increase in suspicious package incidents; for instance, a suspicious package was discovered at the Hill County Courthouse in Hillsboro, Texas, on July 15, prompting an evacuation. The package was safely removed without incident. While overall gun violence in the United States saw an expected decrease this past week following the elevated levels typically associated with the July 4th holiday, several significant mass shootings still occurred; for instance, on July 13, two people were killed and 15 others were injured outside of a nightclub in Houston, Texas.

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%