ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 1, 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 July 30, 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 Brief - The Evolution of the Cybercrime-as-a-Service Market

Over the past decade, cybercrime has almost certainly reorganized from largely self-contained intrusions into a specialized service economy in which discrete capabilities are bought and sold as products. Ransomware-as-a-service (RaaS) very likely became the commercial center of this ecosystem, professionalizing through successive brands into affiliate operations with profit-sharing, recruitment, technical support, and brand management. Extortion tradecraft escalated from simple encryption to "double extortion": pairing encryption with the threat to publish stolen data. This was popularized around late 2019 and subsequently adopted across the RaaS landscape, often with dedicated data-leak sites and additional pressure tactics. The service model extended far beyond ransomware into phishing-as-a-service, initial access brokering, infostealer subscriptions, malware delivery, and distributed denial of service (DDoS)-for-hire, all supported by dark web markets, bulletproof hosting, and cryptocurrency laundering infrastructure. A sustained, multinational law-enforcement campaign repeatedly disrupted the ecosystem—yet resilience and rebranding were the recurring response, with several operations re-emerging within days to months. Generative artificial intelligence (GenAI) is an emerging accelerant rather than a demonstrated transformation. Criminal AI tooling appeared in mid-2023, and threat actors are very likely adopting AI faster than defenders can adapt to it. However, ZeroFox assesses the publicly available, corroborated evidence does not yet support specific claims about the scale of AI-driven growth.

TeamPCP Resurfaces to Sell Old Data: Assessing the Impact

TeamPCP has resurfaced, likely in an effort to repurpose previously harvested datasets to identify and pursue further intrusions; the group is less likely to conduct a net new intrusion campaign and is likely currently focused on disclosing older breaches. On July 21, 2026, ZeroFox observed new dark web activity potentially linked to threat group TeamPCP, following its relative operational silence since at least May 2026. Xploitrs (also spelled xpl0itrs), the group's alleged associate, claimed to have leaked data tied to RapidFort, a U.S.-based cybersecurity company. TeamPCP's attacks can be typically categorized into two stages: credential acquisition and credential operationalization. The majority of the data points stolen during TeamPCP's credential acquisition stage lose value once the credentials are rotated, revoked, or otherwise neutralized, making the loss severe but neutralizable. The real and lasting impact of TeamPCP's campaign almost certainly comes from the group's credential operationalization activities.

ZeroFox Intelligence Flash Report - Introduction of WhatsApp Usernames

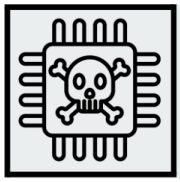
On June 29, 2026, Meta began allowing WhatsApp's three-billion-plus users to reserve a username that new contacts can use instead of a phone number, ahead of a phased, country-by-country rollout later in 2026. ZeroFox assesses the feature will likely act as a threat multiplier by increasing the credibility of impersonation and social engineering campaigns rather than introduce a fundamentally new attack method. Meta has reportedly reserved usernames tied to public figures, government entities, celebrities, and verified accounts and added limits on new-contact messaging volume and username key guessing; ZeroFox assesses these controls will likely reduce, but not eliminate, abuse. Within 48 hours of the announcement, India's Ministry of Electronics and Information Technology (MEITy) issued a formal notice warning the feature could materially increase online fraud, phishing, digital arrest scams, and impersonation attacks and temporarily paused rollout in that market; Finland's national cyber authority (Traficom) issued a similar public warning in early July. ZeroFox assesses that impersonation risk is very likely to be highest during the initial rollout window, as threat actors test platform controls and attempt to register deceptive usernames before enforcement matures.

Monthly Geopolitical Report August 2026

Three simultaneous conflicts—the war in Iran, the Russia-Ukraine war, and Iran-allied Houthi attacks in the Red Sea—are converging. The impacts of these overlapping conflicts are very likely to ripple through global supply chains. The ceasefire between the United States and Iran has effectively collapsed. The drop in oil prices to pre-war levels over the last month likely contributed to the resumption in Iranian hostilities. Deteriorating economic conditions are therefore likely to coerce the United States to return to negotiations. Even with a return to negotiations and a halt in the airstrikes, the broader uncertainty is very unlikely to end; the most likely scenario in the near term is a version of the ceasefire that breaks down periodically. U.S. Customs and Border Patrol will collect duties of 10 or 12.5 percent on imports from most major trading partners. The tariffs are only marginally lower than the rates announced back in April 2025; however, the reaction from global markets has been significantly more muted. Because these tariffs have more sound legal footing and do not expire, businesses likely feel more comfortable planning investments. Political transition talks in Venezuela begin in August but are likely to stall; therefore, the current political status quo will likely persist. In India, influential student-led protests in July have subsided following government concessions, but this calm is unlikely to persist given the country's broader, unresolved economic issues.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



LeakNet Claims Data Theft Linked to 12 Million NYC Health + Hospitals Patients

What we know:

- Data extortion group LeakNet has claimed to have stolen an 11 TB archive from U.S. municipal healthcare system NYC Health + Hospitals (NYCHH) that allegedly contains information linked to more than 12 million people.

Background:

- LeakNet published a preview of the alleged data set containing screenshots of databases, medical spreadsheets, and internal messages, with visible patient names, Social Security numbers (SSNs), medical records, and biometric data.
- NYCHH had previously disclosed a breach in March 2026 that reportedly affected 1.8 million individuals.

Analyst note:

- The significant disparity between LeakNet's claims and NYCHH's previously disclosed affected individual count likely indicates that the threat actor is either exaggerating the impact or gained access extending beyond the incident previously acknowledged by NYCHH.
- If true, the exposure will very likely expose affected patients to targeted identity theft, medical fraud, and phishing campaigns.

AI-Assisted Espionage Hits Thai Finance Ministry

What we know:

- Threat actors have reportedly targeted Thailand's Ministry of Finance using an autonomous artificial intelligence (AI) agent called Hermes to carry out parts of the espionage operation.
- The threat actors reportedly used the AI agent to expand internal access and search ministry personnel records, but so far, no evidence of data exfiltration has been found.

Background:

- Hermes reportedly performed system discovery, privilege escalation, network reconnaissance, and file enumeration, while operating in an unrestricted mode that does not require human approval.
- This is one of the latest examples of autonomous AI agents being used in cyberattacks following the JadePuffer ransomware campaign that automated an end-to-end intrusion.

Analyst note:

- The use of an autonomous agent to perform discovery and privilege escalation tasks lowers the expertise required to sustain complex intrusions, likely increasing the use of similar AI-assisted techniques in future attacks.
- As AI adoption grows in the cybercriminal world, threat actors with greater technical capabilities are likely to develop their own autonomous agents and sell them to other threat actors on dark web markets.

Healthcare System AnMed Closes 79 Facilities Following Cyberattack

What we know:

- U.S.-based nonprofit healthcare system AnMed has reportedly closed 79 of its 106 facilities temporarily following a malware-driven IT outage.
- A patient reported hospital computers displaying a 72-hour extortion demand amid the ongoing investigation.

Background:

- AnMed's urgent care, pediatric, therapy, and lab locations reportedly remain open, while offices and Imaging Services are temporarily shut.
- Separately, healthcare revenue management firm Medical Computer Business Services (MCBS) has confirmed unauthorized access to personally identifiable information (PII) and protected health information (PHI) of 1.26 million patients.

Analyst note:

- If the reported extortion demand is legitimate and remains unmet, threat actors will likely publish the exfiltrated data. Such disclosures are likely to expose PHI, trigger regulatory investigations, and cause legal liability, reputational damage, and prolonged operational disruption, particularly if critical systems remain unavailable.

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 three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on July 27 and July 29, 2026. Additionally, on July 28, 2026, CISA released seven Industrial Control Systems (ICS) advisories. Apple has patched 87 vulnerabilities in iOS and iPadOS and 155 vulnerabilities in macOS Tahoe, along with multiple vulnerabilities in macOS Sequoia, macOS Sonoma, watchOS, tvOS, and visionOS. Rockwell Automation has patched four high-severity vulnerabilities in its Arena Simulation software; the flaws (CVE-2026-8085, CVE-2026-8312, CVE-2026-8313, and CVE-2026-8314) are memory corruption issues stemming from improper validation of user-supplied data that can result in an out-of-bounds write. Attackers are actively exploiting CVE-2026-16723, a FastJson Java library vulnerability, to achieve unauthenticated remote code execution (RCE) in vulnerable Spring Boot fat-JAR deployments. The flaw is primarily being used against U.S.-based organizations across multiple sectors and does not currently have a vendor patch. CVE-2026-61511 is an unauthenticated vBulletin template-engine flaw that can lead to RCE on unpatched self-hosted forums. Attackers can send a crafted pagenav[pagenumber] request to the public ajax/render route and execute arbitrary PHP code on unpatched self-hosted forums without authentication. n8n has patched a high-severity expression-sandbox escape that could enable an authenticated workflow editor to execute operating system (OS) commands on the server hosting n8n.

CRITICAL

CVE-2026-16812

What happened: This is an actively exploited and patched OS command injection vulnerability in Arista VeloCloud Orchestrator (VCO).

- **What this means:** The flaw could enable unauthenticated remote attackers with network access to the VCO web interface to execute arbitrary OS commands by accessing privileged functionality intended for internal use.
- **Affected products:**
  - The affected products are listed here.

CRITICAL

CVE-2026-16232

What happened: This is an actively exploited and patched authentication bypass vulnerability in Check Point SmartConsole. The flaw enables unauthenticated attackers to obtain an application login token, authenticate with administrator privileges, and modify security configurations and security policies.

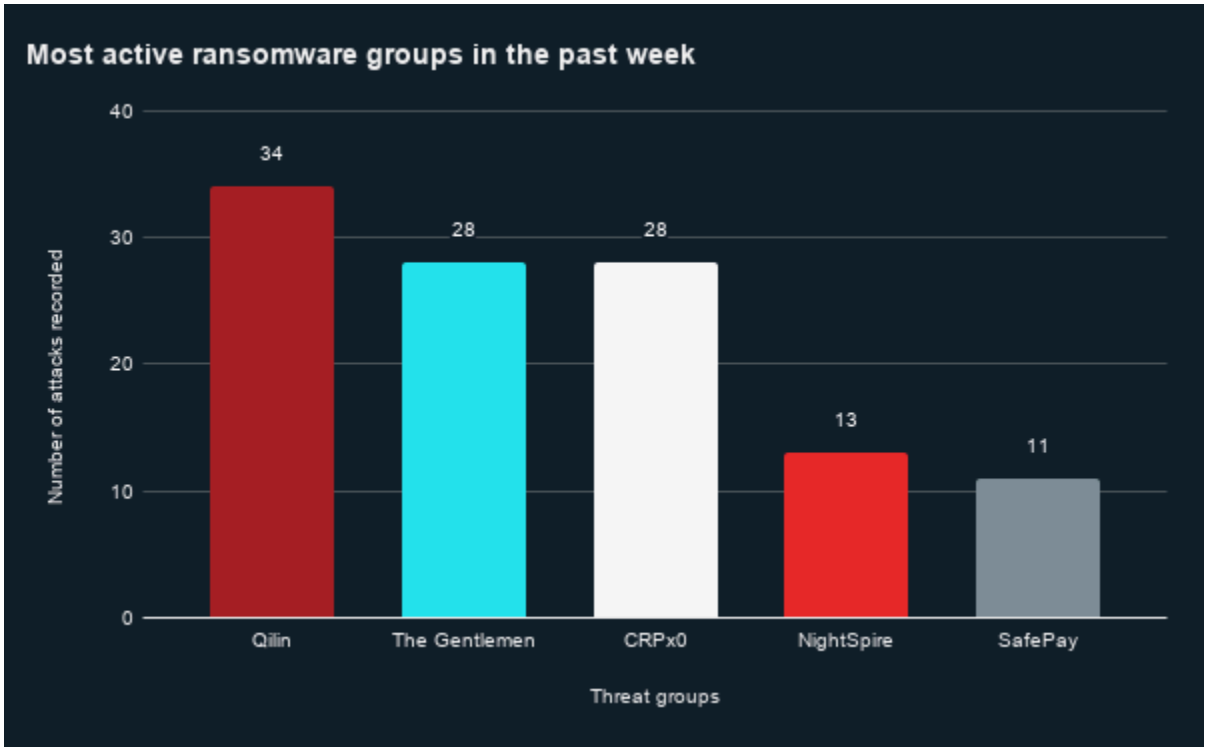
- **What this means:** Successful remote exploitation requires the Management Server IP to be internet-accessible and Trusted Clients (GUI clients) to have no restrictions.
- **Affected products:**
  - The affected products are listed here.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

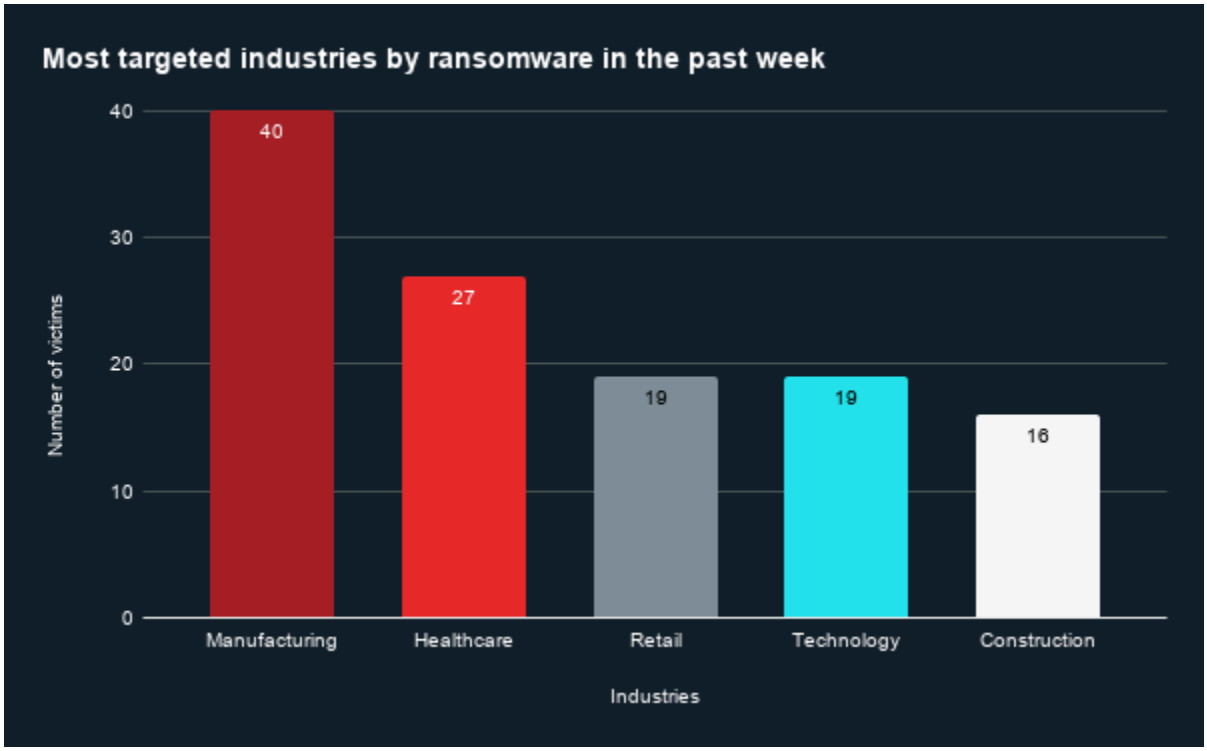
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Qilin, The Gentlemen, CRPx0, NightSpire, and SafePay were the most active ransomware groups. ZeroFox observed close to 208 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by The Gentlemen.



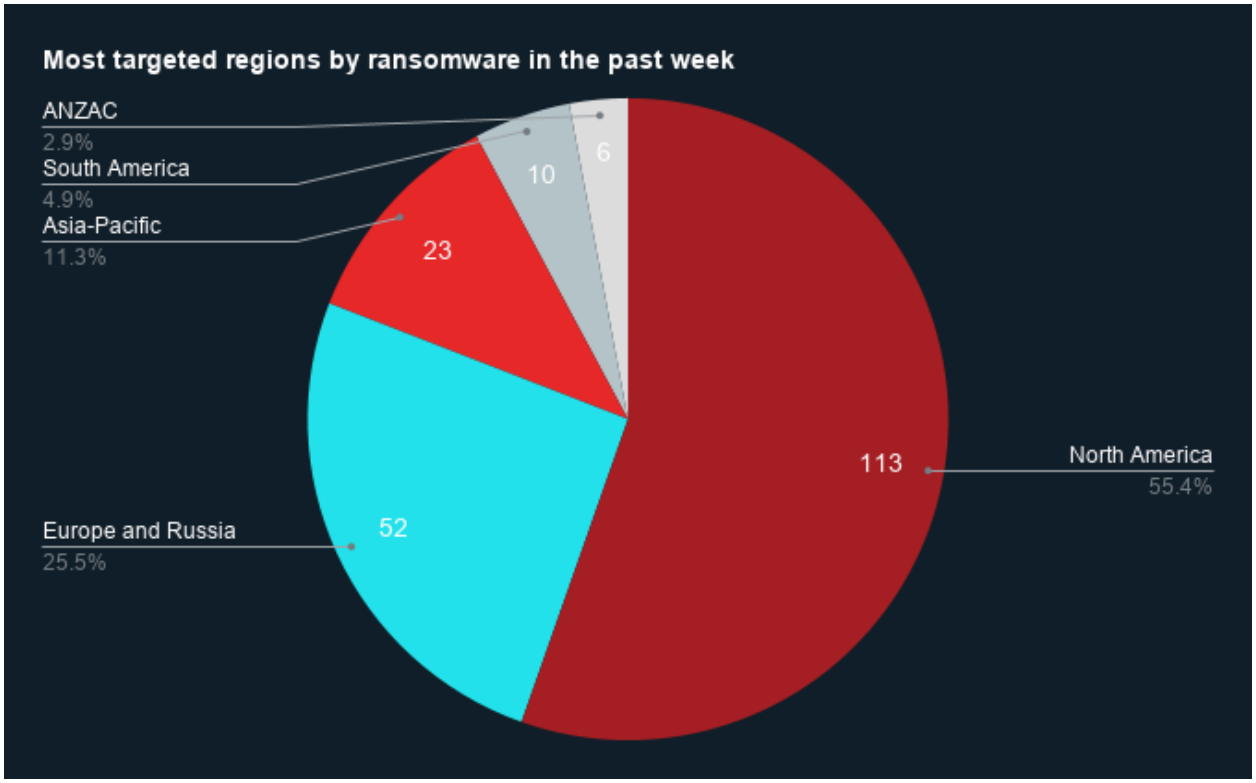
Source: ZeroFox Internal Collections

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

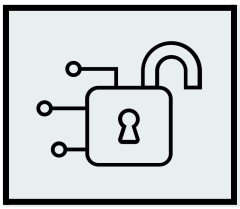


Source: ZeroFox Internal Collections

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 and Asia-Pacific. There were at least 113 ransomware attacks observed in North America, while Europe and Russia accounted for 52, Asia-Pacific for 23, South America for 10, and Australia and New Zealand (ANZAC) for six.



Source: ZeroFox Internal Collections



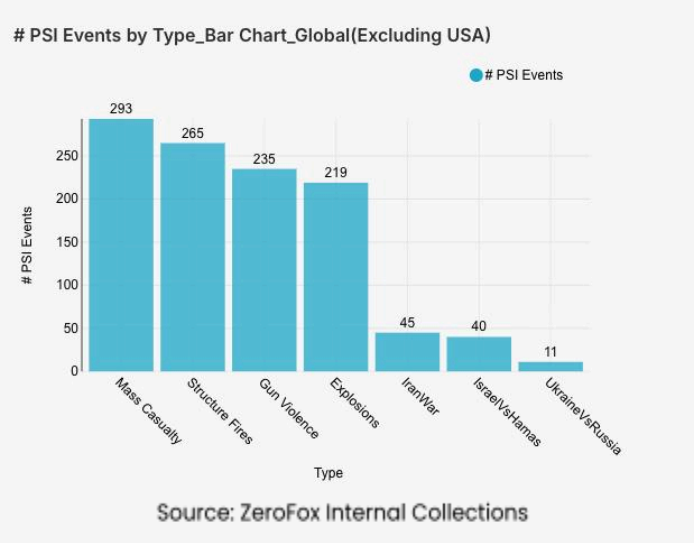
Notable Data Breaches in the Past Week

Targeted Entity	Origin Energy	Operation PAR	Bank of Baroda
Compromised Entities/Victims	2 million individuals	145,714 current and former clients	Bank customers
Compromised Data Fields	Names, addresses, dates of birth, phone numbers, account information, and partial payment card or bank account numbers	Names, dates of birth, SSN, driver's license numbers, financial account information, medical information, and health insurance information	Customer details, identification documents, loan papers, and internal audit records, as well as leaked cache comprising over 700 GB of data
Suspected Threat Actor	N/A	WorldLeaks	N/A
Country/Region	Australia	United States	India
Industry	Energy	Healthcare	Financial Services
Possible Repercussions	Identity theft and targeted phishing impersonating Origin Energy, as well as supply chain spillover across its network of third-party energy retail partners	Financial fraud using SSNs and financial account data, as well as addiction treatment and mental health records	Targeted phishing and social engineering against exposed customers, as well as repackaging and resale of banking-adjacent PII on criminal forums

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

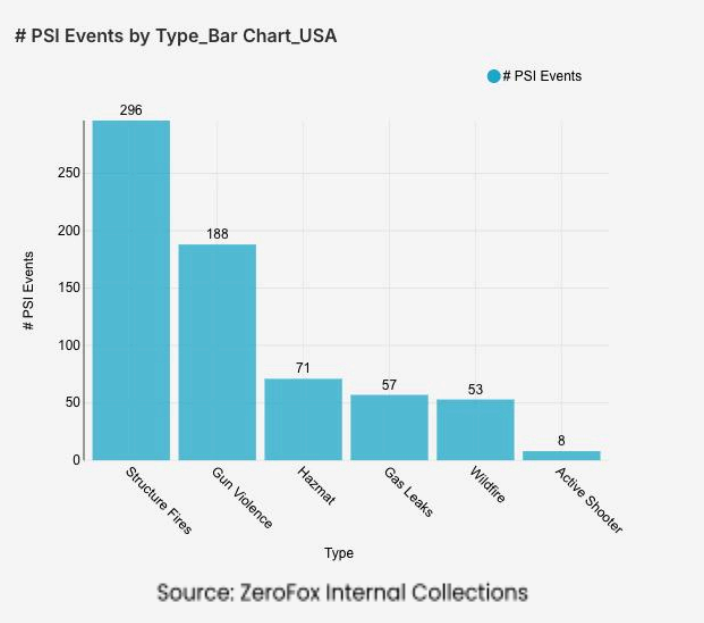


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 10 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being Iran, Pakistan, and the Palestinian territories, in that order. Approximately 75 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 24 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict increased by 67 percent from the previous week, and alerts related to the war in Iran decreased by 52 percent. Events related to Russia's war with Ukraine decreased by 15 percent. The top three most-alerted subtypes were structure fires, which saw a 25 percent increase from the previous week; gun violence, which increased by 26 percent; and explosions, which decreased by 12 percent.

- **What this means:** This week's slight drop in mass casualty events comes even as several conflicts remain volatile. In Iran, the U.S.-Israel military campaign continues; on July 29, explosions were reported across southern Iran as the United States struck targets after intercepting an Iranian missile attack, while allied strikes on Iran-backed militia in Iraq killed about 20 people. In Pakistan, violence in Khyber Pakhtunkhwa persists; on July 30, militants ambushed a police checkpoint in Hangu district, killing at least 11 officers, just days after a suicide attack on a security checkpoint in the northwest killed 27 people. Gaza fighting continues despite a nominal ceasefire, with Israeli strikes on July 30 killing several people amid ongoing mediation talks, consistent with the reported spike in Israel-Hamas alerts. Meanwhile, Russia-Ukraine activity, though seeing an overall decrease, remained deadly; a Russian missile and drone barrage overnight into July 30 killed at least eight civilians across Kyiv, Lviv, and other regions. Taken together, the data points to a global security landscape that remains highly volatile, with entrenched regional conflicts continuing to drive the majority of mass casualty activity even as week-to-week fluctuations occur.

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 gas leaks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, gas leaks involve hazmat emergencies, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were Ohio and New York, which together made up 26 percent of this week's nationwide total. Gun violence across the United States overall decreased by 2 percent from the week prior. Gas leaks also decreased by 2 percent, and the top contributing state was Maryland. Structure fires decreased by 1 percent, and the top two states for this subtype were New York and California. Notably, wildfires increased by 13 percent.

- **What this means:** This week's data reflects a domestic security status of persistent natural and man-made disasters, as well as general violence. Gun violence remains a persistent driver of U.S. emergency response; on July 26, a mass shooting during the Bite of Seattle festival at Seattle Center, Washington, left three people dead and four wounded, with the state's governor deploying a state SWAT team to assist local police. Investigators believe the shooting may have been gang-related, with two groups firing at each other. Structure fires also continue to strain fire departments, as seen in the July 25 blaze in Queens, New York, where a five-alarm fire at an apartment building injured 17 firefighters and four others, spreading across multiple wood-frame buildings. Meanwhile, wildfire activity has surged well beyond seasonal norms; as of July 29, firefighters were suppressing 84 large fires nationwide, with more than 43,000 fires having burned over 4.5 million acres so far this year. Hazmat-related gas leaks likewise remain common; in Birmingham, Alabama, an evacuation order starting on July 27 stayed in effect for several days, a scenario similar to other smaller, more frequent leaks reported across the nation this year. Overall, domestic physical security this week remained largely stable, with various disasters standing out as growing concerns.

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%