ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

May 31, 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 May 29 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: What Is Next in the India-Pakistan Conflict

Tensions between India and Pakistan are likely to simmer in the short term, with sporadic violations of the ceasefire agreement across the northern and western border regions of India. In the event of future conflicts, India is likely to strike Pakistani government and military infrastructure rather than only remote terrorist infrastructure, as it has done in the past. India is very likely to use the Indus Water Treaty (IWT) with Pakistan as a weapon of conflict—or at least leverage it—in future relations with Pakistan. There is a roughly even chance that the IWT will become the cause of new escalations. India and Pakistan are likely to see developments in existing trade arrangements with each other and their trading partners in countries such as China, Turkey, and the United States.

ZeroFox Intelligence Flash Report: Comprehensive Ponzi Scheme Platform Advertised for Sale

On May 23, 2025, an actor using the alias "d3fn0d3" posted on the predominantly Russian-speaking deep and dark web (DDW) forum Exploit advertising the sale of a "complete investment platform" designed to facilitate a Ponzi scheme. According to the advertisement, the investment platform includes features and services such as access to a dashboard feature, verified logins for numerous payment platforms, and established know-your-customer (KYC) protocols. Although scam-related services are very common in DDW marketplaces and forums, ZeroFox has rarely observed the sale of comprehensive platforms such as the one allegedly advertised by d3fn0d3. D3fn0d3's advertisement is unlikely to reflect a new trend, with a more likely chance that the actor is seeking to recuperate funds from an already established platform they no longer wish to operate. While ZeroFox cannot currently ascertain the threat posed by this platform, it is almost certainly heavily dependent upon its post-purchase management.

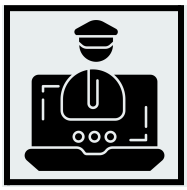
ZeroFox Intelligence June 2025 Geopolitical Assessment

Russia is pushing a military escalation strategy in its war with Ukraine, as Western states continue to urge the two countries to end the war diplomatically. The Trump administration will very likely pursue alternative methods of imposing tariffs after a trade court blocked the majority of the tariffs U.S. President Donald Trump announced on April 2, 2025. While the situation in Gaza is unsustainable, Israeli Prime Minister Benjamin Netanyahu is likely to resist pressure to end the war with Hamas completely and instead seek alternative ways to continue the conflict at a low intensity. The first-ever

judicial elections in Mexico will very likely harm international investment, with elected judges more likely to be perceived as being influenced by criminal groups and politics. Military conflict between India and Pakistan is unlikely in the short term; however, core issues remain that will manifest in hybrid forms of retaliation—like reducing shared water resources, trade bans, and cyberattacks—that risk escalating into armed conflict.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings



Global Dark Web Crackdown Targeting Online Drug and Criminal Networks

What we know:

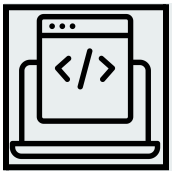
- A global law enforcement operation has made 270 arrests of dark web vendors and buyers across 10 countries, dismantling networks trafficking in drugs, weapons, and counterfeit goods.

Background:

- This operation, called Operation RapTor, identified the suspects based on intelligence from the takedowns of dark web marketplaces Nemesis, Tor2Door, Bohemia, and Kingdom Markets.
- The suspects had conducted thousands of sales on illicit marketplaces, using encryption tools and cryptocurrencies.
- Additionally, authorities have seized over EUR 184 million (approx. USD 207 million) in cash, cryptocurrencies, and other assets.

What is next:

- It is likely that the dismantled criminal networks could spawn further collectives and marketplaces with improved defenses to better evade detection.
- The arrests could provide law enforcement with key intelligence on future threats and the tactics of similar offenders.



SilverRAT Source Code Briefly Exposed on GitHub

What we know:

- The full source code of SilverRAT, a remote access trojan (RAT), was briefly leaked on GitHub before being taken down. The leaked SilverRAT repository included its full source code, build instructions, and weaponized features.

Background:

- SilverRAT is a Middle East-linked RAT sold as malware-as-a-service (MaaS), providing cybercriminals with stealthy system control, cryptocurrency monitoring, and data exfiltration capabilities.

Analyst note:

- Cybercriminals, including low-skilled actors, could use SilverRAT's briefly exposed source code to create similar malware for espionage and data theft. A new variant could be created to target specific entities like governments and financial institutions, depending on the actor's motivation.

Hackers Steal USD 223 Million from Cetus Protocol on Sui Blockchain

What we know:

- Hackers have stolen USD 223 million in cryptocurrency from decentralized exchange (DEX) Cetus Protocol operating on the Sui and Aptos blockchains.

Background:

- Cetus Protocol has paused its smart contract and USD 162 million of the compromised funds. Hackers reportedly exploited a vulnerability in Cetus' smart contract, which led to flash loan-style attacks. The crypto project has also announced a USD 5 million bounty for information on the hackers.
- A flash loan allows users to borrow assets without collateral, provided the loan is repaid within the same blockchain transaction.

Analyst note:

- There is a roughly even chance that the hackers will accept the white-hat settlement offered by Cetus Protocol since their transactions are being tracked. In the short term, Cetus Protocol investors are likely to move to other platforms, causing CETUS to lose its value.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has 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 one vulnerability to its Known Exploited Vulnerabilities (KEV) catalog and released three Industrial Control Systems (ICS) vulnerabilities on May 22 and May 27. A threat actor was observed exploiting a newly patched remote code execution (RCE) vulnerability tracked as CVE-2025-32432 in Craft content management system (CMS) to deploy malicious payloads. DragonForce ransomware group has compromised a managed service provider by exploiting a series of older vulnerabilities (CVE-2024-57727, CVE-2024-57728, and CVE-2024-57726) in the SimpleHelp remote monitoring and management (RMM) platform to exfiltrate data and deploy ransomware. Three vulnerabilities—CVE-2025-34027, CVE-2025-34026, and CVE-2025-34025—in the Versa Concerto SD-WAN orchestration platform enable remote attackers to bypass authentication, achieve RCE, and access system endpoints.

HIGH

CVE-2025-20152

What happened: This already patched vulnerability in Cisco's Identity Services Engine (ISE) affects its RADIUS message processing feature. An attacker is able to exploit the bug by sending a specific authentication request to a network access device (NAD), leading to a denial-of-service (DoS) condition.

- **What this means:** The vulnerability is likely to be used by threat actors—especially politically motivated actors—to carry out distributed denial-of-service (DDoS) attacks targeting critical infrastructure entities.
- **Affected products:**
  - Cisco ISE configured with RADIUS authentication services

MEDIUM

CVE-2025-5224

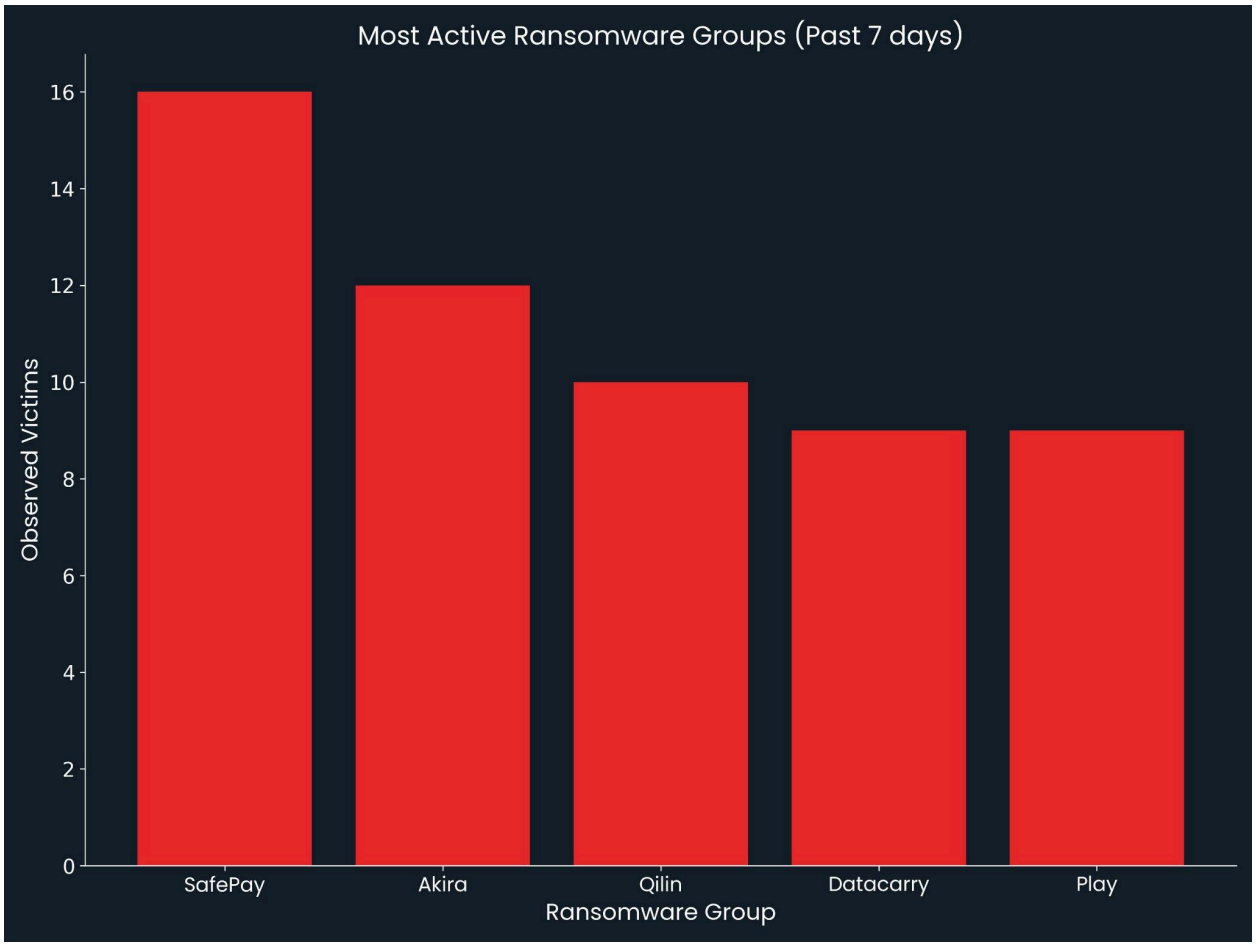
What happened: This vulnerability in Campcodes' Online Hospital Management System involves an unknown function, wherein the manipulation of an argument leads to an SQL injection. The exploit has been disclosed to the public. The vulnerability could enable threat actors to inject malicious SQL queries that manipulate the database.

- **What this means:** Threat actors are likely to use this vulnerability to steal sensitive user information, including credentials and financial data. It is likely to be used in ransomware attacks targeting the healthcare industry.
- **Affected products:**
  - Campcodes Online Hospital Management System version 1.0

Ransomware and Breach Intelligence

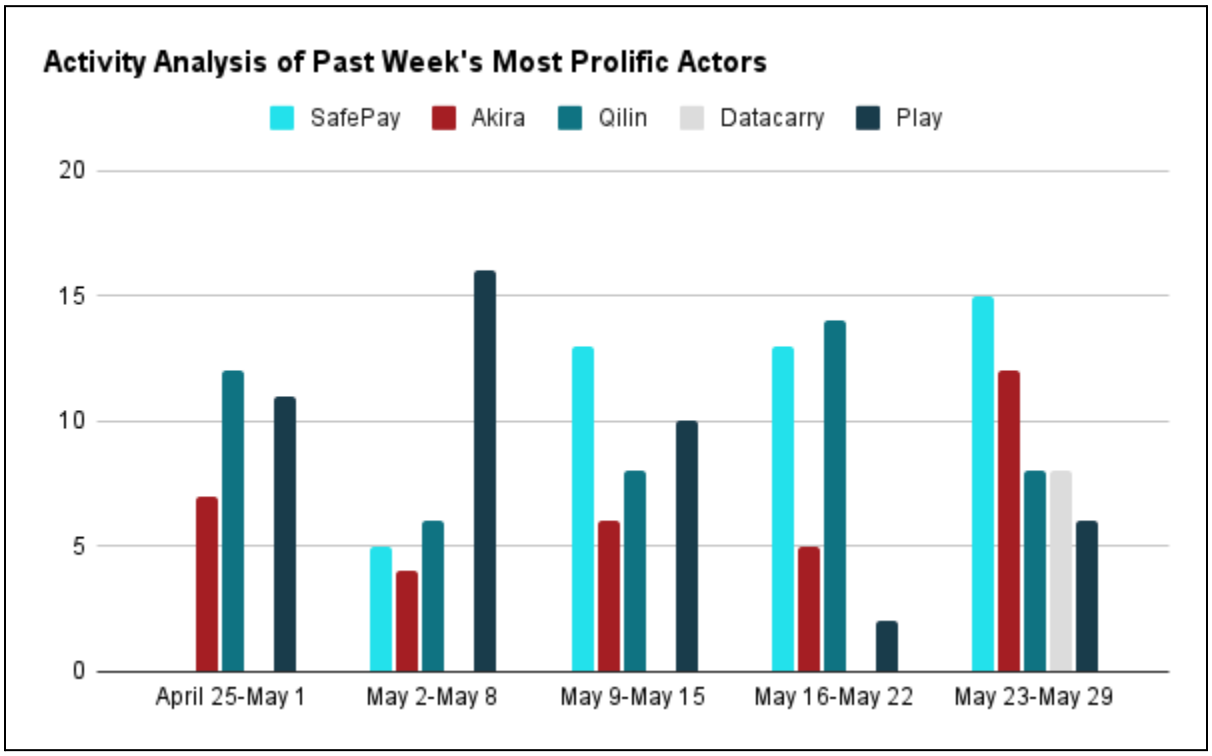
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup for the Past Seven Days



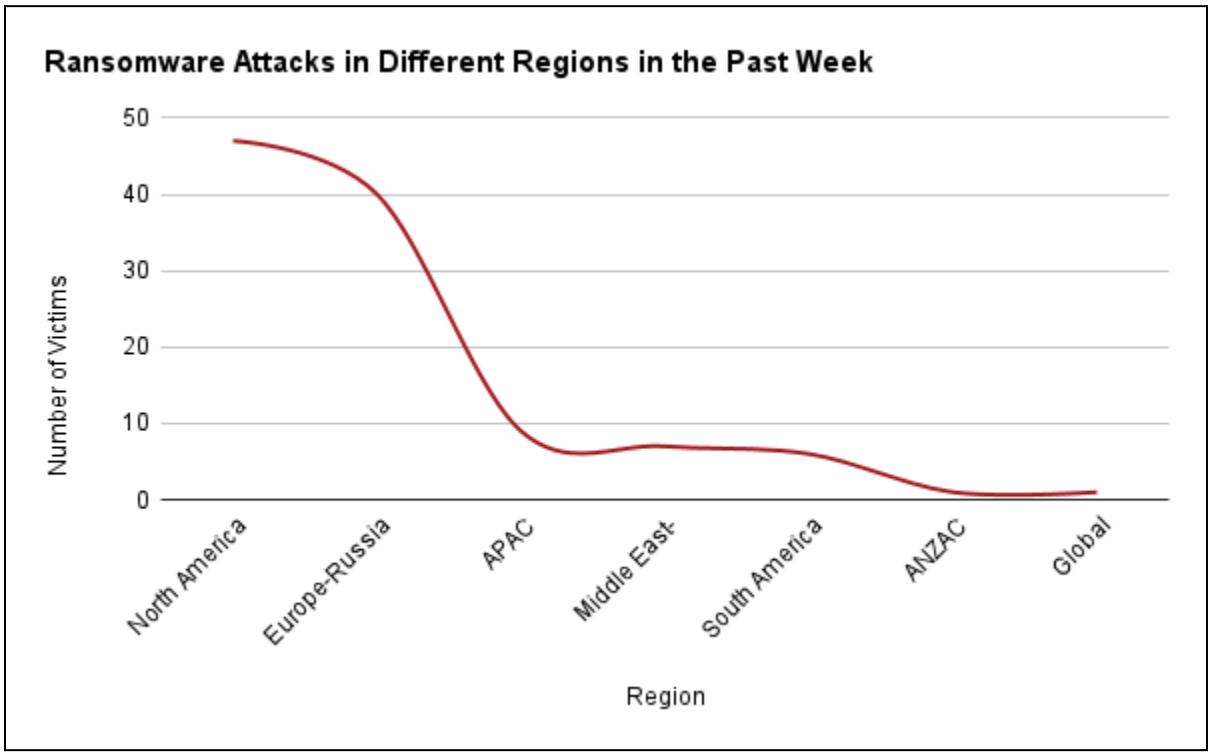
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, SafePay, Akira, Qilin, Datacarry, and Play were the most active ransomware groups. ZeroFox observed at least 115 ransomware victims disclosed, most of which were located in North America. The SafePay ransomware group accounted for the largest number of attacks.



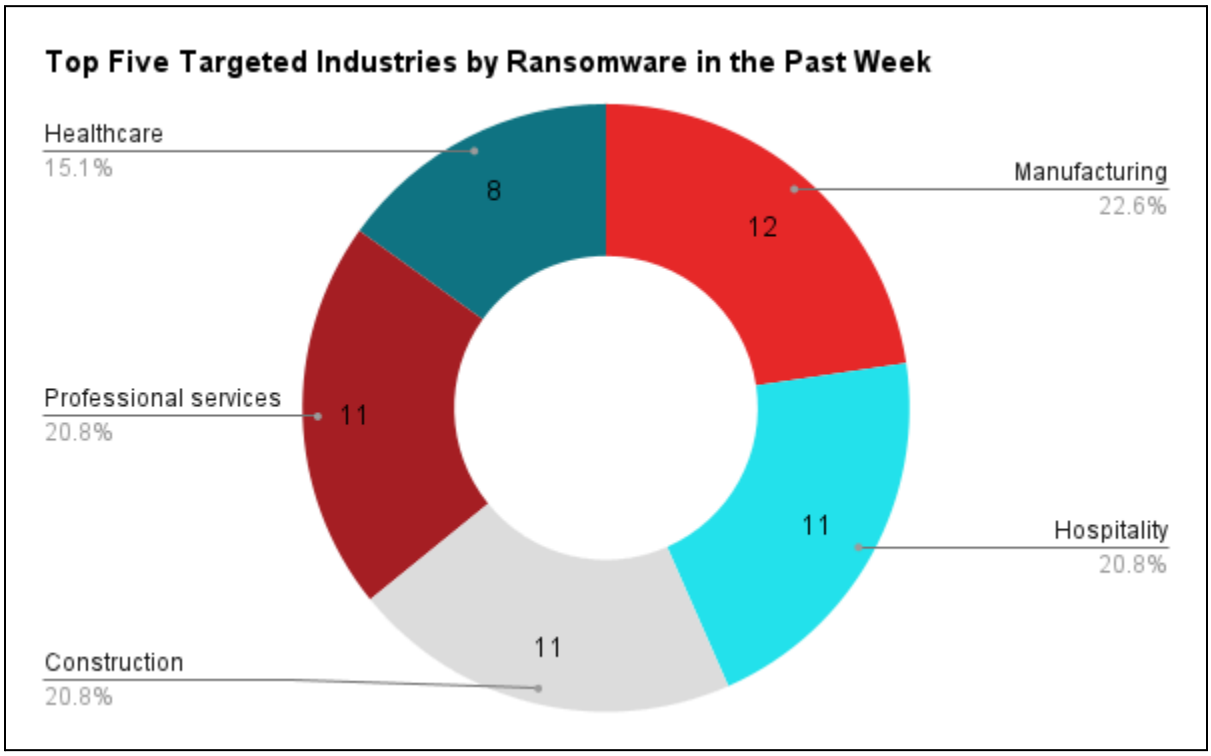
Source: ZeroFox Internal Collections

Threat group activity trend: In the past week, ZeroFox observed that SafePay, Akira, Qilin, Datacarry, and Play were the most prolific threat actor groups. The graph above shows their activities over the past five weeks. Qilin and Play have been active throughout all five weeks, with at least 48 and 45 attacks, respectively. ZeroFox observed activity by the Datacarry ransomware group in week 5, with no activity detected by this actor in the preceding weeks.



Source: ZeroFox Internal Collections

Regional ransomware trends: In the past seven days, ZeroFox has observed that North America was the most targeted region by ransomware attacks, followed by Europe-Russia.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing, hospitality, construction, professional services, and healthcare were the industries most targeted by ransomware attacks. The manufacturing industry was the top target, with 12 attacks.

Recap of major ransomware events observed in the past week: Nearly a month after notifying customers of a cyberattack, Canadian electric utility Nova Scotia Power has acknowledged that it is dealing with a ransomware incident. MathWorks, a provider of mathematical computing and simulation software, has disclosed that a recent ransomware attack is the cause of its ongoing service outage. A foreign national has pleaded guilty in the United States for participating in a May 2019 international Robbinhood ransomware attack that resulted in massive losses to victims. The 3AM ransomware group has adopted the combined attack strategy already used by Black Basta and other groups to gain initial access and deploy ransomware. The Interlock ransomware group is targeting educational institutions with a newly discovered RAT called NodeSnake.

Major Data Breaches in the Past Seven Days

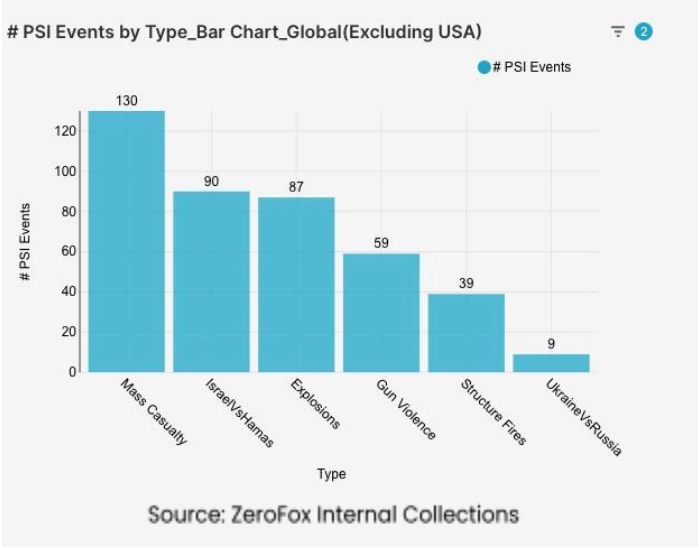
Targeted Entity	Adidas	LexisNexis	Tiffany & Co.
Number of Firms/Victims Affected	Yet to be determined	364,000	Yet to be determined
Compromised Data Fields	Consumer contact information	Names, dates of birth, phone numbers, postal and email addresses, Social Security numbers, and driver license numbers	Names, addresses, phone numbers, email addresses, internal customer ID numbers, and purchase history
Suspected Threat Actor	Yet to be determined	Yet to be determined	Yet to be determined
Country/Region	Turkey and South Korea	United States	South Korea
Industry	Retail and manufacturing	Professional services	Retail
Possible Repercussions	Phishing and social engineering attacks, malware distribution, impersonation scam, and two-factor authentication (2FA) bypass fraud	Identity theft, account takeover, impersonation scams, phishing and social engineering attacks, stalking, espionage, and ransomware	Phishing and social engineering attacks, impersonation scams, physical security risks, account takeovers, and ransomware

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

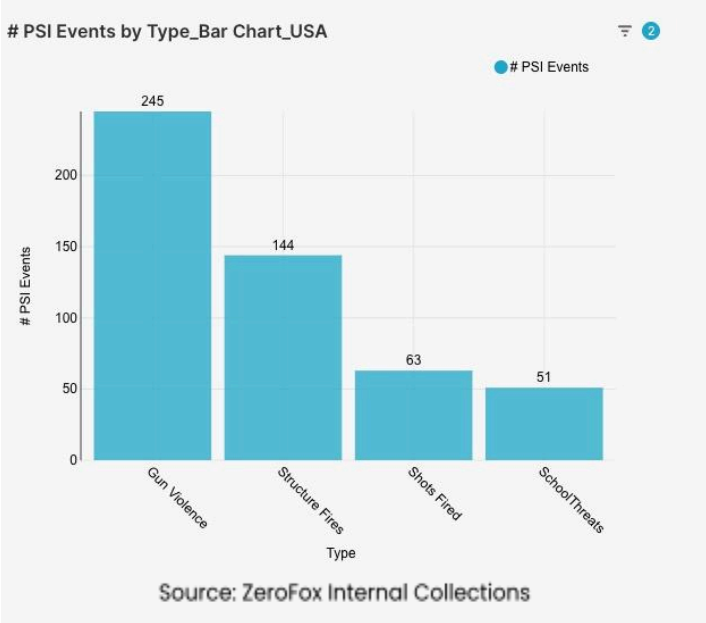


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was a 15 percent decrease in mass casualty events this week from the previous week, with the most contributions from Palestinian territories, India, and Lebanon (in that order). Approximately 67 percent of these events were explosions, and the three aforementioned countries accounted for about 41 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 11 percent from the previous week. Events related to Russia's war in Ukraine increased by 50 percent. The top three most-alerted subtypes were explosions, which saw a 17 percent decrease from the previous week; gun violence, which decreased by 14 percent; and structure fires, which decreased by 5 percent. Global protest activity increased by 11 percent.

- **What this means:** This week, the Ukraine-Russia conflict saw a significant increase in alerts. Despite a recent prisoner swap, the two countries have continued to launch drone and missile attacks, with Ukraine reporting 364 aerial threats from Russia and Russia claiming to have downed over 100 Ukrainian drones in an overnight incursion. In a rare rebuke, U.S. President Donald Trump stated that Russian President Vladimir Putin is "playing with fire." Palestinian territories had the highest number of mass casualty alerts this week, one of which included a strike against a Gaza City school that killed more than 30 people on May 26. Last weekend in Liverpool, a driver injured at least 50 people by ramming a car into a crowd of soccer fans on May 25. Police say it is not an act of terrorism and that the suspect acted alone. Finally, worldwide protests have increased in the past week; for instance, teachers unions in Mexico have been protesting since May 15 demanding changes in working and educational conditions. This reflects a broader global trend of increased activism driven by economic hardships, political repression, and demands for democratic accountability.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and shots fired. 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 shots fired are confirmed shootings without human victims. The top two states that had the most gun violence alerts were California and Pennsylvania, which together made up 16 percent of this week's nationwide total. Gun violence across the United States overall decreased by 4 percent from the week prior. Structure fires decreased by 20 percent, and the top two states for this subtype were California and Maryland. Shots fired alerts did not increase or decrease from the previous week, but the top two contributing states this week were Ohio and California. Notably, school-related threats decreased by 53 percent across the nation.

- **What this means:** School-related threats dropped sharply this week, likely influenced by the end of the academic year in many districts and proactive threat monitoring following earlier school safety scares this spring. This is also likely the reason why police activity was not in the top three subtypes, as it typically correlates positively with school-related threats. Structure fires dropped notably as well, potentially due to milder weather and recent public fire safety campaigns, especially in fire-prone states like California, where last week's cooler temperatures and tighter fire codes likely helped reduce incidents. Gun violence alerts saw a slight nationwide decrease, despite California and Pennsylvania continuing to contribute significantly. Pennsylvania had two mass shootings this week: on May 26, 11 people were shot in Philadelphia, and five people were shot on May 23 in Chester. We expect these incidents to increase in the coming months; The Gun Violence Archive shows that June, July, and August have had the highest total number of mass shootings over the past decade.

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%