ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

June 14, 2025

ZEROFOX®
Weekly Intelligence Brief

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 June 12, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

© 2025 ZeroFox, Inc. All rights reserved.

This Week’s ZeroFox Intelligence Reports

FIFA Club World Cup 2025 Event Assessment

The Fédération Internationale de Football Association (FIFA) Club World Cup (CWC) soccer tournament is due to take place across the United States from June 15 to July 13, 2025. While technically a new tournament, there have been other iterations of the quadrennial event, which serves as a precursor to the FIFA World Cup due to take place in the United States in 2026. This year's event is the first-ever 32-team CWC (up from seven) and has caused controversy for placing what some see as “excessive” logistical and scheduling constraints on soccer clubs during what is traditionally the pre-season for most of them. Like other major tournaments, the FIFA CWC comes with myriad logistical issues due to the influx of fans from across the globe attending 63 matches across 11 cities. The controversy surrounding this tournament could impact attendance, and U.S. public transportation, accommodation, tourism, and security services will be put to the test. Tournament organizers are likely also concerned about anti-FIFA demonstrations, as well as protests related to the U.S. political atmosphere—particularly the perception that the country has become less accepting of immigration. Furthermore, FIFA CWC attendees may experience issues related to crime and cyber scams at the matches and related events.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 11

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

ZeroFox Intelligence Brief - Introduction to Deep and Dark Web Forums

Deep and dark web (DDW) forums and marketplaces operate in areas of the internet that are less visible to the majority of users. While most of the domains found within these areas serve legitimate purposes, many facilitate illegal activities. Many DDW forums and marketplaces have undergone varying degrees of “professionalization,” manifested by the widespread acknowledgement of “norms” by frequenting actors and the implementation of systems such as credibility rankings, escrow, and arbitration services.

© 2025 ZeroFox, Inc. All rights reserved.

ZeroFox Intelligence Flash Report - No Kings Day Activity Threatens to Prolong Ongoing Protests

Millions of people are likely to participate in “No Kings Day” protests taking place in cities across the United States. Protests in Phoenix, Houston, Chicago, Atlanta, Charlotte, and Philadelphia likely carry the highest risk for unrest due to heavy promotion by organizers.

© 2025 ZeroFox, Inc. All rights reserved.

Cyber and Dark Web Intelligence

© 2025 ZeroFox, Inc. All rights reserved.

Cyber and Dark Web Intelligence Key Findings

Over 20 Configuration Vulnerabilities Found in Salesforce Industry Cloud

What we know:

- Over 20 configuration-related vulnerabilities in Salesforce Industry Cloud have been detected.
- Salesforce fixed three issues and provided guidance for two; the other bugs reportedly stem from customer-level misconfiguration and were therefore not directly resolved at the enterprise level.

Background:

- The flaws affect key components like FlexCards, Integration Procedures, and OmniScripts.
- These components handle sensitive data and business logic in Salesforce's vertical cloud solutions.

What is next:

- The misconfigurations are likely to enable attackers to bypass security controls to access encrypted confidential data, session details, credentials for Salesforce and other company systems, and business logic.
- Breached data of customers and employees is likely to be used in phishing, social engineering, and impersonation attacks.

Major U.S. Grocery Distributor UNFI Shuts Down Systems Following Cyberattack

What we know:

- United Natural Foods, Inc. (UNFI) has taken down some systems following a recent cyberattack discovered on June 5. The incident impacted customer order processing.

Background:

- UNFI is one of North America's largest publicly traded wholesale food distributors, serving over 30,000 locations. Its customers include supermarket chains, e-commerce platforms, natural product superstores, independent retailers, and food service providers.

© 2025 ZeroFox, Inc. All rights reserved.

Analyst note:

- A growing wave of ransomware attacks targeting the retail and grocery sectors has emerged—starting in the United Kingdom and now extending into the United States. The recent attack on UNFI will likely cause delays in order processing and delivery, inventory shortages, and financial losses. Given the pattern of recent incidents, similar attacks on supply chain infrastructure are very likely to follow.

iMessage Flaw Likely Part of Spyware Campaign Targeting Key Figures in the United States and Europe

What we know:

- A zero-click vulnerability in Apple’s iMessage has reportedly been used to target high-value individuals in the United States and Europe, including politicians and executives of artificial intelligence (AI) companies.

Background:

- China is suspected to be behind the targeting. The use-after-free memory vulnerability affects the imagent process in the nickname feature of iMessage on iPhones. The flaw is also suspected to be linked to mysterious and rare iPhone crashes observed between late 2024 and early 2025.

Analyst note:

- The vulnerability is likely to enable attackers to access all data on compromised devices, including conversations on end-to-end encrypted messaging apps such as WhatsApp and Signal. The already-patched vulnerability is likely to be just one part of a larger exploit chain aiming to compromise Apple devices.

© 2025 ZeroFox, Inc. All rights reserved.

Exploit and Vulnerability Intelligence

© 2025 ZeroFox, Inc. All rights reserved.

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 four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on June 9 and June 10. CISA has also released four Industrial Control Systems (ICS) vulnerabilities. CVE-2025-5712 is an SQL injection vulnerability that affects the "/appointment.php" file via the "patient" parameter. A critical vulnerability was discovered in TOTOLINK EX1200T firmware version 4.1.2cu.5232_B20210713. A new variant of the Mirai malware botnet exploits a command injection vulnerability in TBK DVR-4104 and DVR-4216 digital video recorders, allowing attackers to take control of the devices. An out-of-bounds write vulnerability in the PCX image codec in QNX SDP versions 8.0, 7.1, and 7.0 could enable an unauthenticated attacker to cause a denial-of-service (DoS) or potentially execute code within the affected process. Google has patched a vulnerability in a now-obsolete JavaScript-disabled version of a username recovery form that risked exposure of private numbers of account users, including anonymous users. Adobe has released patches for 254 security flaws, with 225 affecting Adobe Experience Manager (AEM). Two security vulnerabilities (CVE-2025-5484 and CVE-2025-5485) have been identified in SinoTrack GPS devices that could enable attackers to control certain remote functions on connected vehicles and track their locations. Security researchers have uncovered over 20 configuration-related vulnerabilities in Salesforce Industry Cloud.

CRITICAL

CVE-2025-27531

What happened: A vulnerability involving the deserialization of untrusted data was identified in Apache InLong versions from 1.13.0 up to (but not including) 2.1.0. This flaw allowed authenticated attackers to exploit a weakness by double-writing a parameter, which enabled them to read arbitrary files on the system. The vulnerability arises from insecure handling of serialized data, which can be manipulated to execute unintended actions.

- **What this means:** This vulnerability poses a critical risk to system confidentiality, as it enables authenticated threat actors to read arbitrary files on the host by exploiting improper deserialization logic via parameter manipulation. Although authentication is required, the flaw significantly lowers the barrier for lateral movement or privilege escalation within the environment. Organizations are advised to upgrade to Apache InLong version 2.1.0, which includes the necessary security patch to mitigate this threat vector.

© 2025 ZeroFox, Inc. All rights reserved.

- **Affected products:**
  - Apache InLong versions from 1.13.0 up to (but not including) 2.1.0

CRITICAL

CVE-2025-1041

What happened: A vulnerability caused by improper input validation was discovered in the Avaya Call Management System. This flaw enables an attacker to send a specially crafted web request that could lead to the execution of unauthorized remote commands.

- **What this means:** This vulnerability can be exploited remotely and without authorization, meaning attackers do not need to log in to launch an attack. Remote command execution can lead to full system compromise, enabling attackers to manipulate data, disrupt services, or gain access to sensitive information.
- **Affected products:**
  - Affected versions include 18.x, 19.x prior to 19.2.0.7, and 20.x prior to 20.0.1.0.

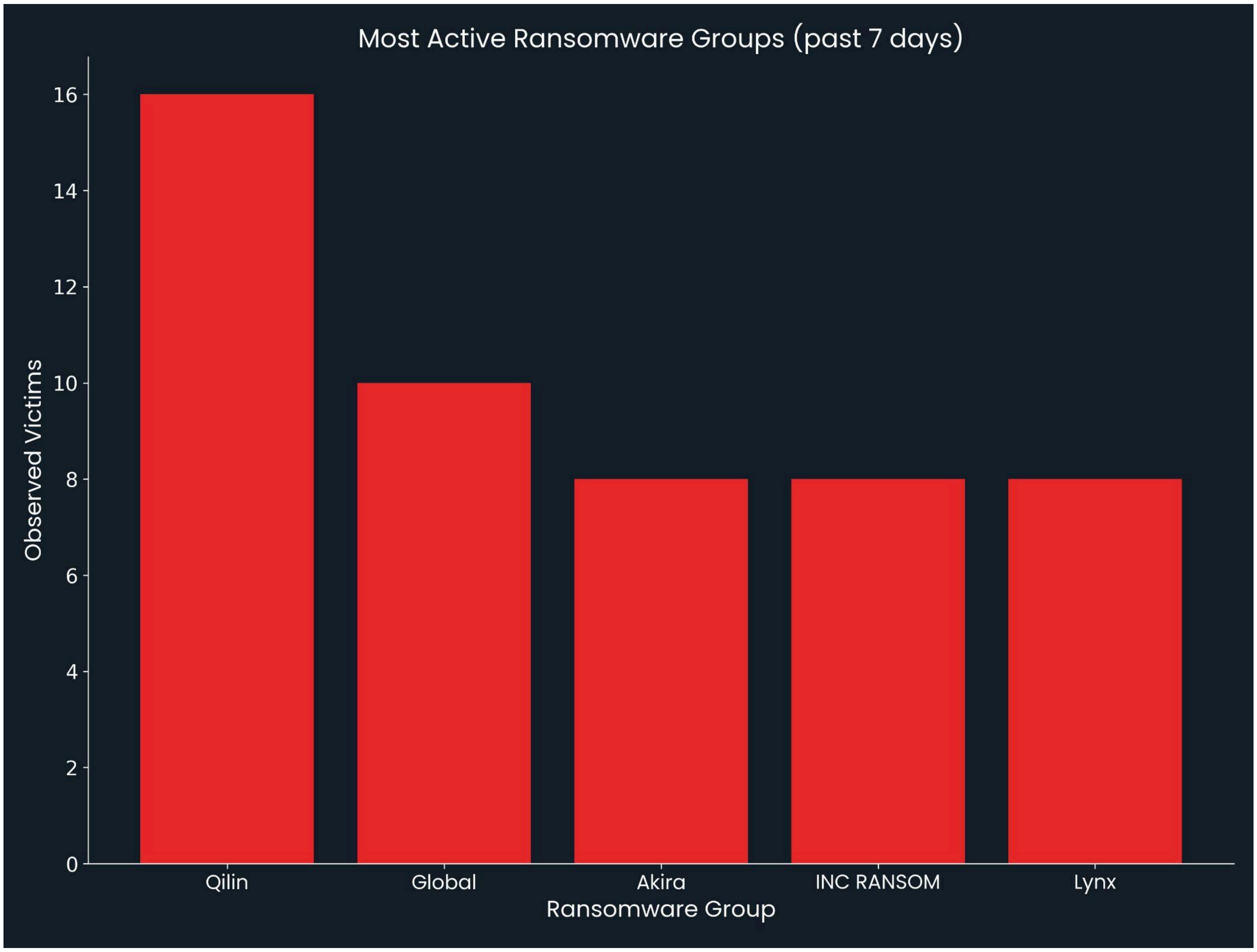
© 2025 ZeroFox, Inc. All rights reserved.

Ransomware and Breach Intelligence

© 2025 ZeroFox, Inc. All rights reserved.

Ransomware and Breach Intelligence Key Findings

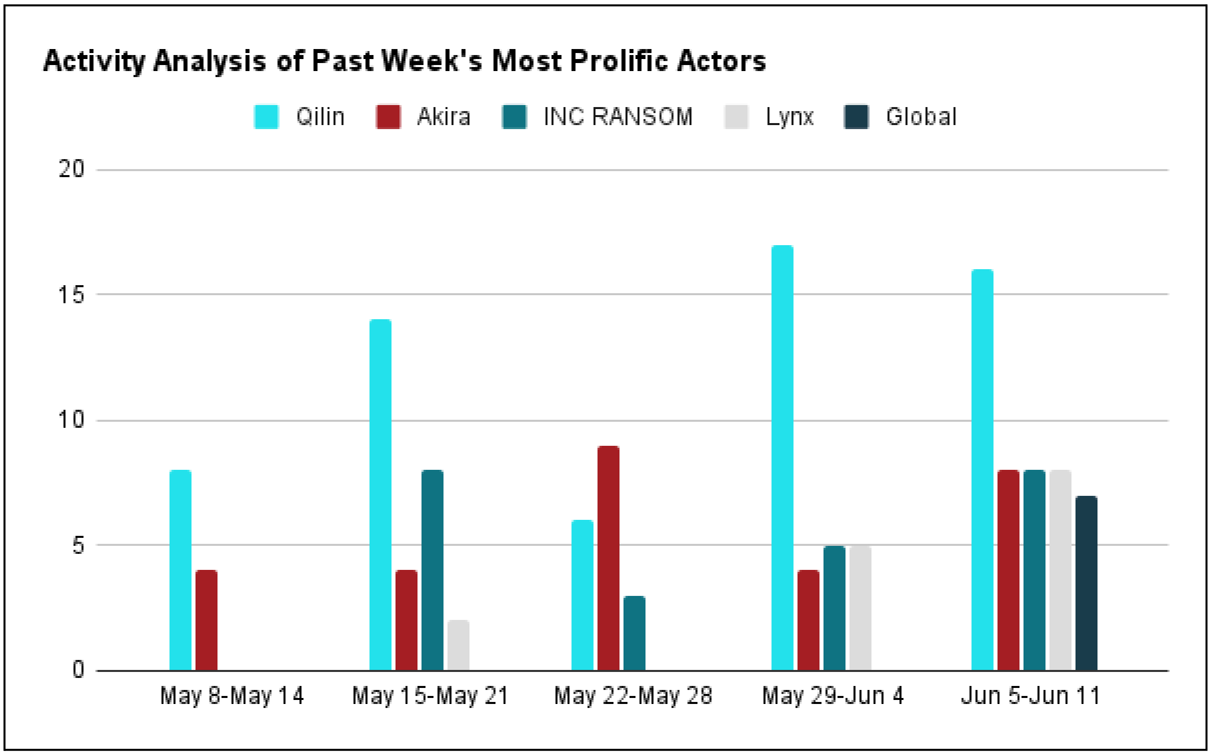
Ransomware Roundup: Most Active Groups, Affected Industries, Regions, and More



Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Global, Akira, INC RANSOM, and Lynx were the most active ransomware groups. ZeroFox observed at least 105 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks.

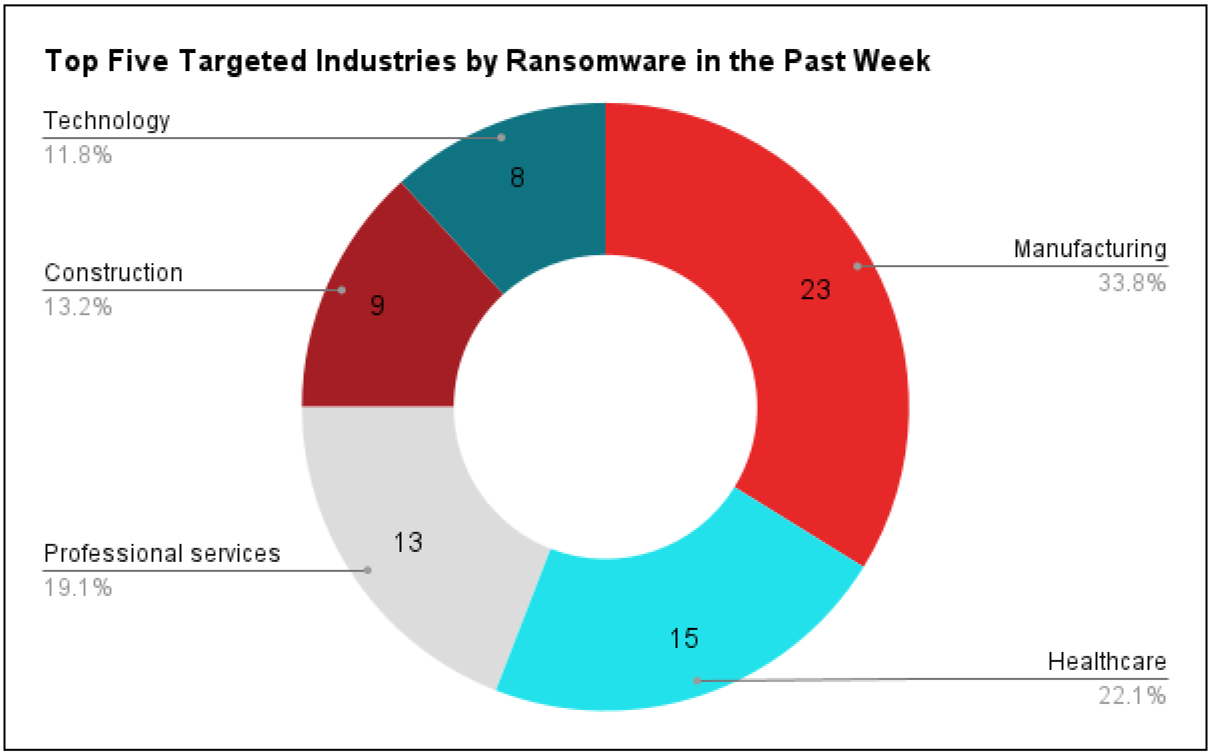
© 2025 ZeroFox, Inc. All rights reserved.



Source: ZeroFox Internal Collections

Threat group activity trend: In the past week, ZeroFox observed that Qilin, Global, Akira, INC RANSOM, and Lynx were the most prolific threat actor groups. The graph above shows their activities over the past five weeks. Qilin and Akira have been active throughout all five weeks, with Qilin conducting at least 61 attacks. ZeroFox observed activity by the ransomware group Global in Week 5, but none by this actor the previous four weeks.

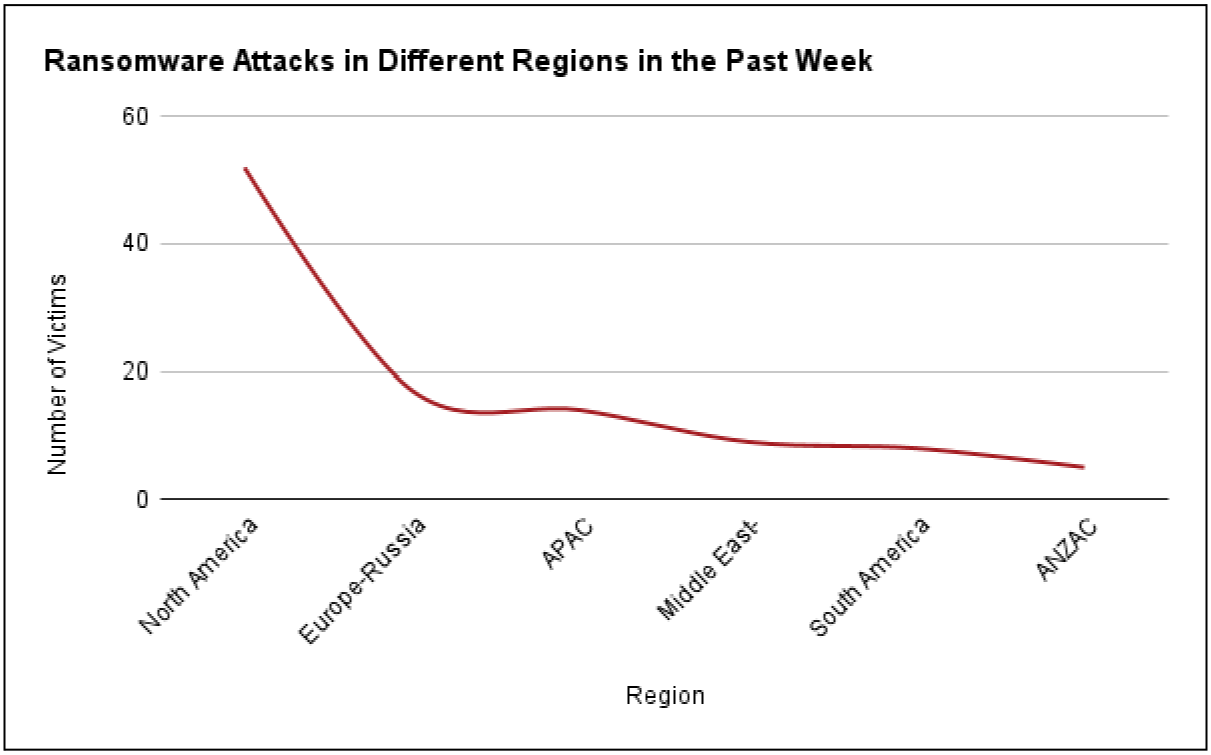
© 2025 ZeroFox, Inc. All rights reserved.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing, healthcare, professional services, construction, and technology were the industries most targeted by ransomware attacks. The manufacturing industry was the top target, with 23 attacks identified.

© 2025 ZeroFox, Inc. All rights reserved.



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.

Recap of major ransomware events observed in the past week: Over the past seven days, ZeroFox observed two new ransomware leaksites: "Warlock" and "WAlocker." ZeroFox has also observed an image and onion URL associated with Qilin ransomware group posted in the "About & Contact" section of Arkana ransomware group's dark web leak site. Additionally, a digital banner, which looks like a job posting for the role of pentesters for the Qilin group in Russian, is also present on the page. Meanwhile, Optima Tax Relief, a U.S.-based tax resolution firm, has fallen victim to a Chaos ransomware attack, with the attackers leaking data stolen from the company. Kettering Health, a major healthcare provider operating 14 medical centers in Ohio, has confirmed that the Interlock ransomware group breached its network and stole data during a cyberattack in May.

© 2025 ZeroFox, Inc. All rights reserved.

Significant Data Breaches Reported This Week

Targeted Entity	**Texas Department of Transportation**	**Sensata Technologies**	**Jackson Health System**
Number of Firms/Victims Affected	Approximately 300,000	N/A	Over 2,000 patients
Compromised Data Fields	Full name, physical address, license plate number, driver's license number, vehicle insurance policy details, and description of the crash and the injuries sustained	Social Security numbers (SSNs), government identity numbers, financial and medical information, and dates of birth	Names, birth dates, addresses, medical record numbers, and clinical information
Suspected Threat Actor	N/A	N/A	Insider leak
Country/Region	United States	United States	United States
Industry	Government	Industrial Technology	Healthcare
Possible Repercussions	Phishing, social engineering, and impersonation attacks. Delays in accessing insurance claims.	Phishing and social engineering attacks and identity theft. Operational disruptions across customer organizations.	Identity theft, phishing and social engineering attacks, as well as insurance fraud.

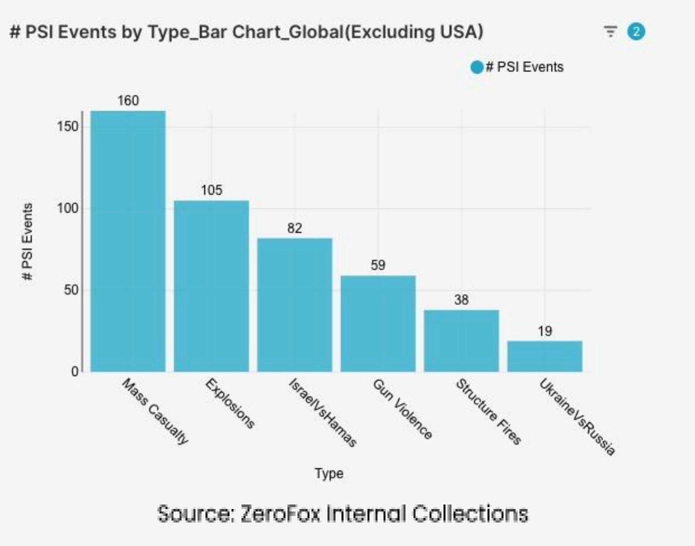
Three major breaches observed in the past week

© 2025 ZeroFox, Inc. All rights reserved.

Physical and Geopolitical Intelligence

© 2025 ZeroFox, Inc. All rights reserved.

Physical and Geopolitical Intelligence Key Findings



Source: ZeroFox Internal Collections

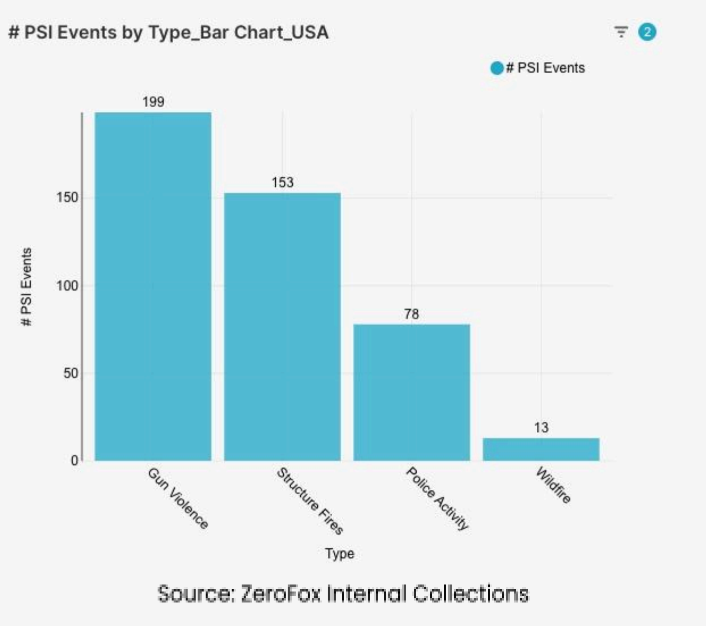
Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 9 percent increase in mass casualty events this week from the previous week, with the biggest contributions coming from the Middle East, India, and Ukraine. Approximately 66 percent of these events were explosions, and the three aforementioned countries accounted for approximately 38 percent of all mass casualty alerts. General alerts related to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries) increased by 6 percent from the previous week. Events related to Russia's war in Ukraine increased by 90 percent. The top three most-alerted subtypes were explosions, which saw a 12 percent increase from the previous week; gun violence, which did not increase or decrease from the week prior; and structure fires, which increased by 23 percent. Global protest activity increased by 8 percent.

- **What this means:** This week, explosions and mass casualty alerts in general saw increases alongside both the Israel-Hamas and Ukraine-Russia conflicts. In Gaza, an Israeli offensive against an aid site killed 36 people and wounded 207 on June 10, contributing to the increase in IsraelVsHamas alerts as well as explosions. According to the Gaza Health Ministry, over 55,000 Palestinians have been killed since the beginning of the war, and Israeli President Benjamin Netanyahu has vowed to continue the fight until all Israeli hostages are returned and Hamas is defeated. Ukraine had the third highest number of mass casualty events this week, and there was a sharp increase in alerts related to the Russia-Ukraine conflict in general. On June 10, swarms of Russian kamikaze drones were launched into Kyiv, Ukraine, in one of the largest wartime attacks to date. As of this writing, there have been no agreements on ceasefires between the two countries. Finally, structure fires saw a fairly significant increase as well, with Canada being one of the top contributing countries, as it is in the midst of its wildfire season. Some towns are being evacuated, with burned areas already exceeding year-to-date averages from recent years.

© 2025 ZeroFox, Inc. All rights reserved.

Physical Security Intelligence: United States



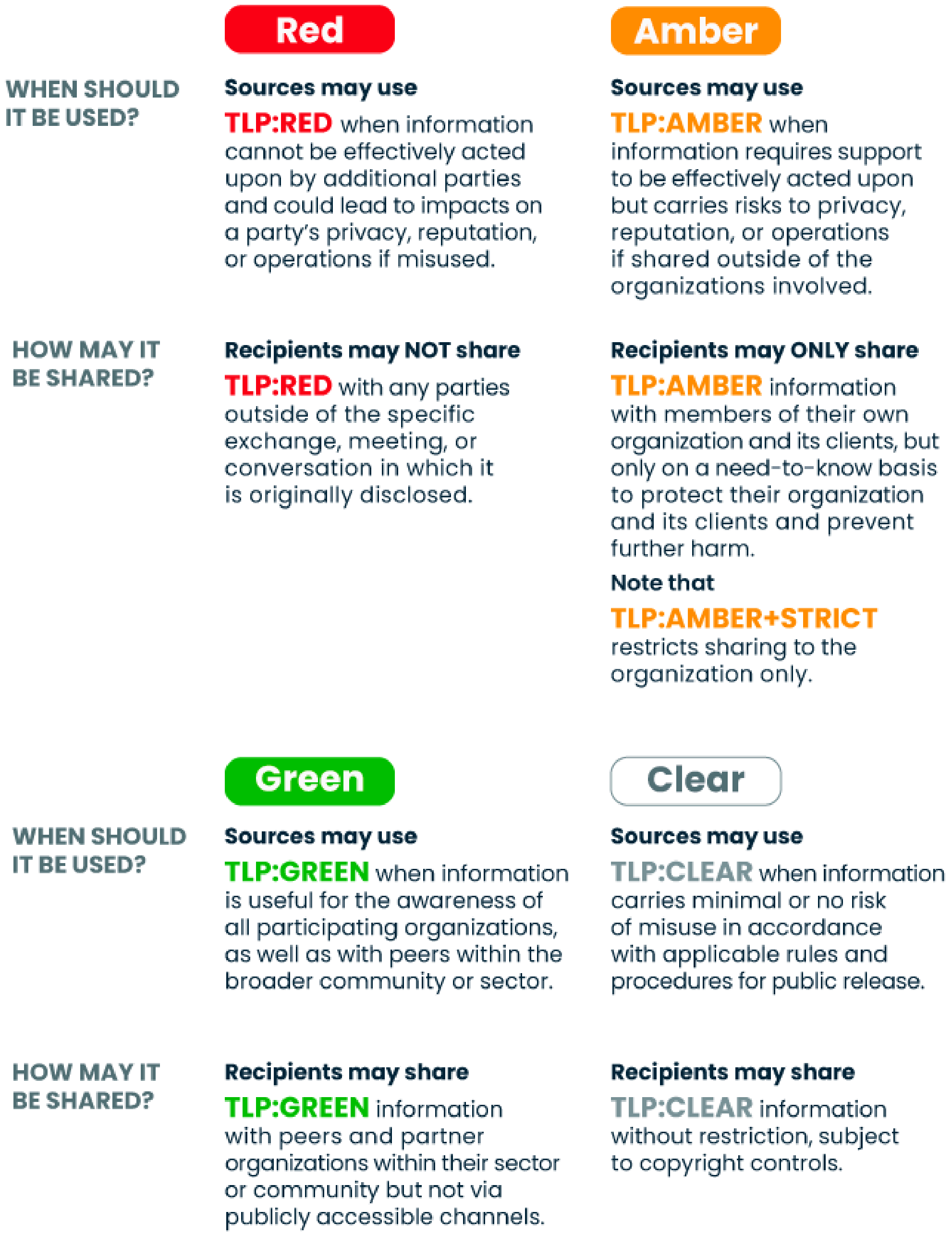
Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and police activity. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or unknown reasons, 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 20 percent of this week's nationwide total. Gun violence across the United States overall decreased by 5 percent from the previous week. Police activity alerts increased by 10 percent, and the top contributing states were California and New York. Structure fires increased by 7 percent, and the top two states for this subtype were also California and New York. National protest activity increased by 33 percent compared to the previous week.

- **What this means:** The most significant increase this week was seen in protest activity, as demonstrations against U.S. Immigration and Customs Enforcement (ICE) have recently surged across the United States. These protests—which began in Los Angeles and quickly spread to other major cities like New York, Austin, and San Francisco—aim to oppose the Trump administration's immigration enforcement policies. Protesters are demanding an end to raids and deportations, often clashing with law enforcement and resulting in arrests; this may also explain the increase in police activity alerts seen this week, as California was a top contributing state. These incidents are expected to continue into the weekend as several "No Kings" protests have been planned for June 14, coinciding with a Washington, D.C. military parade as well as President Trump's birthday. Structure fires also increased this week, as wildfires—such as the San Bernardino County Ranch Fire in California—have destroyed homes and caused evacuations. The rest of 2025 also poses severe wildfire risk in numerous states due to developing drought conditions and heat waves.

© 2025 ZeroFox, Inc. All rights reserved.

Appendix A: Traffic Light Protocol for Information Dissemination



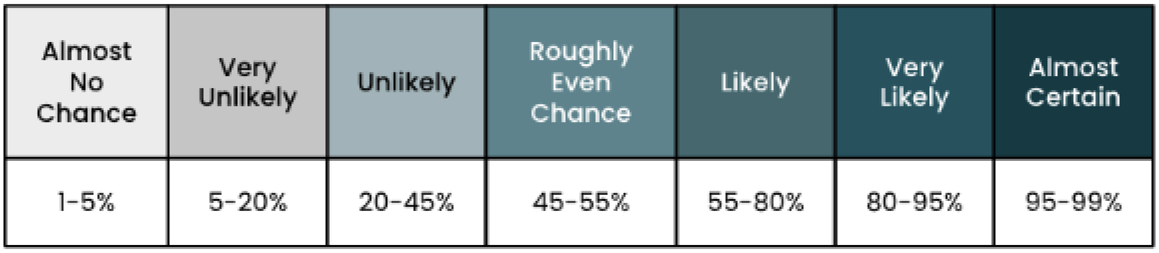
	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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.

© 2025 ZeroFox, Inc. All rights reserved.

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%