Weekly Intelligence Brief

Classification: TLP:GREEN

June 28, 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 26, 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 2
ZeroFox Intelligence Flash Report - Tentative Israel-Iran Ceasefire Established 2
ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 12 2
ZeroFox Intelligence Flash Report - Israel-Iran: Cyber Threat Landscape 2
ZeroFox Intelligence Flash Report - Prominent Threat Actors Reportedly Arrested 3
| Cyber and Dark Web Intelligence Key Findings 5
Chinese State Hackers Suspected to be Behind Espionage Infrastructure "LapDogs" 5
Phishing Campaign Targets DMVs; Steals Financial Information 5
New Guidance Released for Reducing Memory-Related Vulnerabilities 6
| Exploit and Vulnerability Intelligence Key Findings 8
CVE-2025-49825 8
CVE-2025-5777 9
| Ransomware and Breach Intelligence Key Findings 11
Ransomware Roundup: Threat Actors, Industries, and Region 11
Major Data Breaches of the Week 14
| Physical and Geopolitical Intelligence Key Findings 17
Physical Security Intelligence: Global 17
Physical Security Intelligence: United States 18
| Appendix A: Traffic Light Protocol for Information Dissemination 20
| Appendix B: ZeroFox Intelligence Probability Scale 21

This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report - Tentative Israel-Iran Ceasefire Established

In the late evening of Monday, June 23, 2025, U.S. President Donald Trump announced on his social media platform, Truth Social, that Israel and Iran had fully agreed to a "complete and total ceasefire." Approximately two hours after the ceasefire was due to begin, Israel claimed to have detected a missile launch emanating from Iran—an action that would have been in violation of Iran's initial 12-hour ceasefire period. Despite initially bellicose statements from Israeli officials and explosions reported in Tehran, Prime Minister Benjamin Netanyahu claimed that Israel had refrained from retaliation. As of the writing of this report, the integrity of the ceasefire is unclear and fast-changing, though there is a very likely chance that the Iranian, Israeli, and U.S. governments perceive a bilateral ceasefire to be mutually beneficial. However, a likely chance remains that hostilities will resume within the coming weeks, exacerbated by the presence of numerous pro-Iranian parties in the region that have historically perceived Israeli and U.S. assets as viable targets. Meanwhile, ZeroFox published an advisory earlier this week, describing the attacks and the damages incurred by both sides.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 12

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

ZeroFox Intelligence Flash Report - Israel-Iran: Cyber Threat Landscape

During the recent conflict between Israel and Iran, ZeroFox observed an uptick in the attack tempo from both Israel- and Iran-aligned cyber threat groups. ZeroFox identified multiple examples of both pro-Israeli and pro-Iranian hacktivist collectives claiming to have targeted critical national infrastructure (CNI), which are very likely attempts to aid warfighting efforts. ZeroFox observed mis-, dis-, and malinformation associated with the conflict being shared on social media platforms, likely both intentionally (to fuel specific narratives) and unintentionally. Despite a ceasefire being announced on June 24, 2025, which resulted in the scaling down of conventional military action, adjacent offensive cyber activities are very likely to continue.

ZeroFox Intelligence Flash Report - Prominent Threat Actors Reportedly Arrested

Reporting on June 25, 2025, indicated that an individual thought to be behind the prominent deep and dark web (DDW) handle "IntelBroker" had been arrested by a law enforcement operation that occurred in France in February 2025. Earlier on the same day, separate reporting suggested that four key members of the popular hacking forum BreachForums, who are known by the aliases "ShinyHunters", "Hollow", "Noct", and "Depressed", had also been arrested on June 23, 2025. Both IntelBroker and ShinyHunters are prominent threat actors that are heavily associated with the popular deep web hacking forum BreachForums, which remains inactive as of the writing of this report. BreachForums is unlikely to make a successful comeback or relaunch, regardless of the presence of IntelBroker and ShinyHunters. Despite once being one of the most popular and prominent deep web hacking forums, there is a very likely chance that many members perceive a higher risk from using the forum, which is likely exacerbated significantly following the recent arrests.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Chinese State Hackers Suspected to be Behind Espionage Infrastructure "LapDogs"

What we know:

- Suspected Chinese state hackers have built a network of botnet-like operational relay boxes (ORBs) in targeted countries, reportedly for cyber espionage purposes.
- The targeted countries include the United States, Taiwan, Japan, Hong Kong, and South Korea.

Background:

- The infrastructure building has been dubbed "LapDogs" and is thought to have started in September 2023.
- So far, over 1,000 Linux-based small office/home office (SOHO) devices have been affected in the media, IT, networking, and real estate sectors.

What is next:

- The campaign is very likely building a botnet-like network to obfuscate malicious activity, such as carrying out anonymized browsing and command-and-control (C2) operations.
- The compromised devices are also likely to be used to gain further access into the internal network of the targeted organization.
- Once further access is gained, threat actors can likely branch out to conduct other cybercriminal activities, such as reconnaissance, C2, data exfiltration, and supply chain attacks.

Phishing Campaign Targets DMVs; Steals Financial Information

What we know:

- An ongoing SMS phishing campaign impersonating Departments of Motor Vehicles (DMVs) across the United States has tricked thousands of Americans into exposing their personal and financial data.

Background:

- The scam, suspected to be linked to a China-based group, targeted residents in several high-population U.S. states (Texas, Florida, New York, and others) using spoofed texts and fake websites about unpaid tolls and license suspensions.

Analyst note:

- Threat actors could use stolen credit card information collected through fake DMV sites for unauthorized purchases, sell it on the dark web, and use it in other fraud schemes, such as identity theft and financial account takeovers.

New Guidance Released for Reducing Memory-Related Vulnerabilities

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have released a joint guide highlighting the importance of adopting memory safe languages (MSLs) in improving software security and reducing the risk of security incidents.

Background:

- Memory safety vulnerabilities pose serious risks to national security and critical infrastructure. MSLs offer the most comprehensive mitigation against these vulnerabilities by providing built-in safeguards.

Analyst note:

- Threat actors are likely to exploit unaddressed memory safety vulnerabilities to gain unauthorized access, disrupt critical operations, and compromise sensitive data. The guide addresses key challenges in adopting MSLs and offers recommendations to help secure critical infrastructure systems.

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. CISA added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue. CISA has also released eight Industrial Control Systems (ICS) vulnerabilities. A remotely exploitable vulnerability in Cisco Meraki devices enables unauthenticated attackers to disrupt Virtual Private Network (VPN) services by sending crafted HTTPS requests. Citrix has issued security patches for a critical NetScaler ADC flaw (CVE-2025-6543) that is being exploited in the wild. CVE-2025-6474 is an SQL injection flaw that enables remote attackers to manipulate the user_id parameter and access or alter databases. Chrome 138 has released fixes for 11 security bugs. CVE-2024-51978 is a critical security vulnerability that affects hundreds of Brother printers. Pterodactyl has a vulnerability (prior to version 1.11.11) that enables unauthenticated attackers to execute arbitrary code. Mattermost versions 9.11.15 and below, 10.5.5 and below, 10.6.5 and below, 10.7.2 and below, and 10.8.0 and below have a vulnerability in archive extraction that enables authenticated users to perform path traversal, potentially leading to remote code execution. D-Link DPH-400S/SE VoIP Phone version 1.01 has hardcoded provisioning variables, including "PROVIS_USER_PASSWORD," which could lead to the exposure of sensitive user credentials.

CRITICAL

CVE-2025-49825

What happened: A critical vulnerability has been discovered in the open-source platform Teleport, which facilitates secure access to servers, cloud apps, Kubernetes clusters, and databases. The vulnerability could enable remote attackers to bypass standard Secure Shell (SSH) authentication. The flaw is present in Teleport Community Edition versions up to 17.5.1 and has been patched in subsequent updates across multiple versions. Teleport has urged users to update immediately.

- **What this means:** The flaw could enable unauthorized access to systems managed by Teleport, undermining security policies and potentially exposing sensitive infrastructure. While cloud customers received automatic patches, self-hosted environments remain at risk unless manually updated. Although vulnerable Teleport agents have also been auto-locked to prevent exploitation, prompt action is still required to restore secure access and prevent potential breaches.
- **Affected products:**
  - Teleport Community Edition versions up to 17.5.1

CRITICAL

CVE-2025-5777

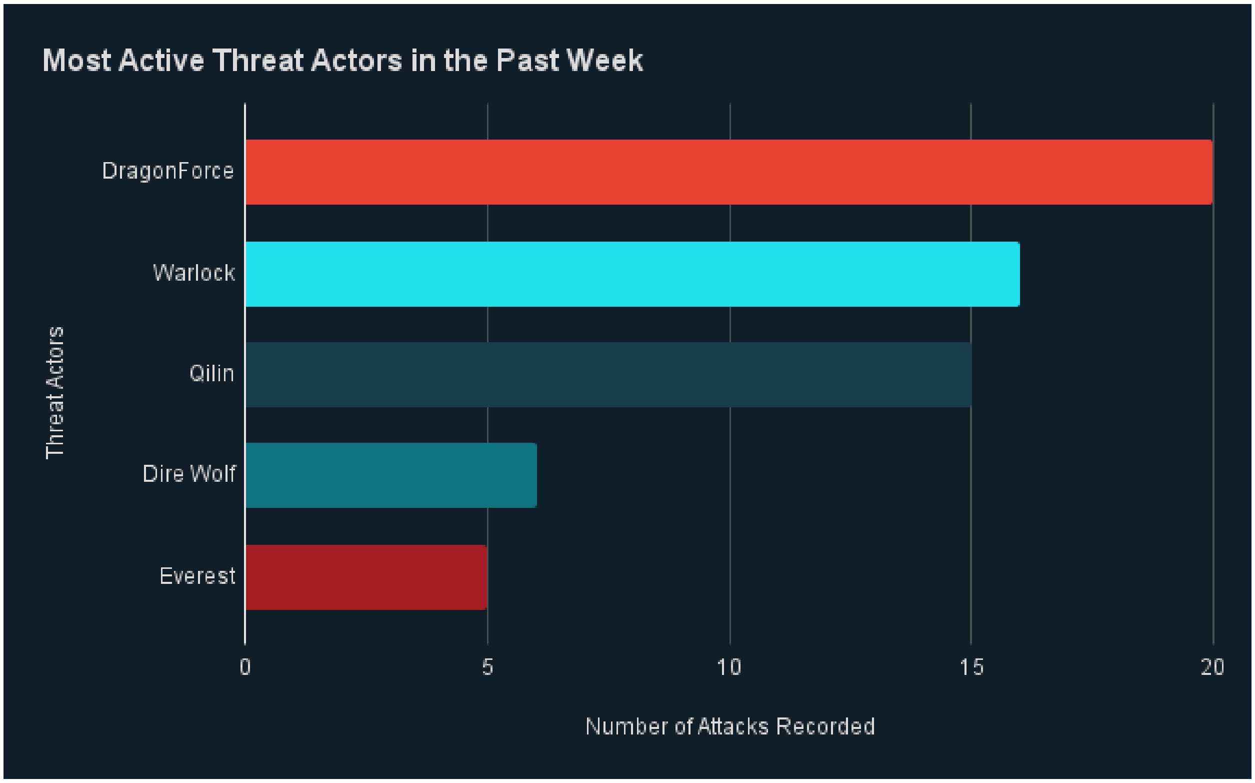
What happened: Citrix has patched a critical vulnerability in NetScaler ADC and NetScaler Gateway. The flaw is caused by insufficient input validation leading to an out-of-bounds read, which could be exploited remotely.

- **What this means:** This vulnerability is being compared to the infamous CitrixBleed flaw due to its severity and potential for widespread exploitation. If left unpatched, it could enable attackers to access sensitive data or compromise systems, putting enterprises at risk of data leakage, session hijacking, or even full system compromise.
- **Affected products:**
  - The affected products are listed in this advisory.

Ransomware and Breach Intelligence

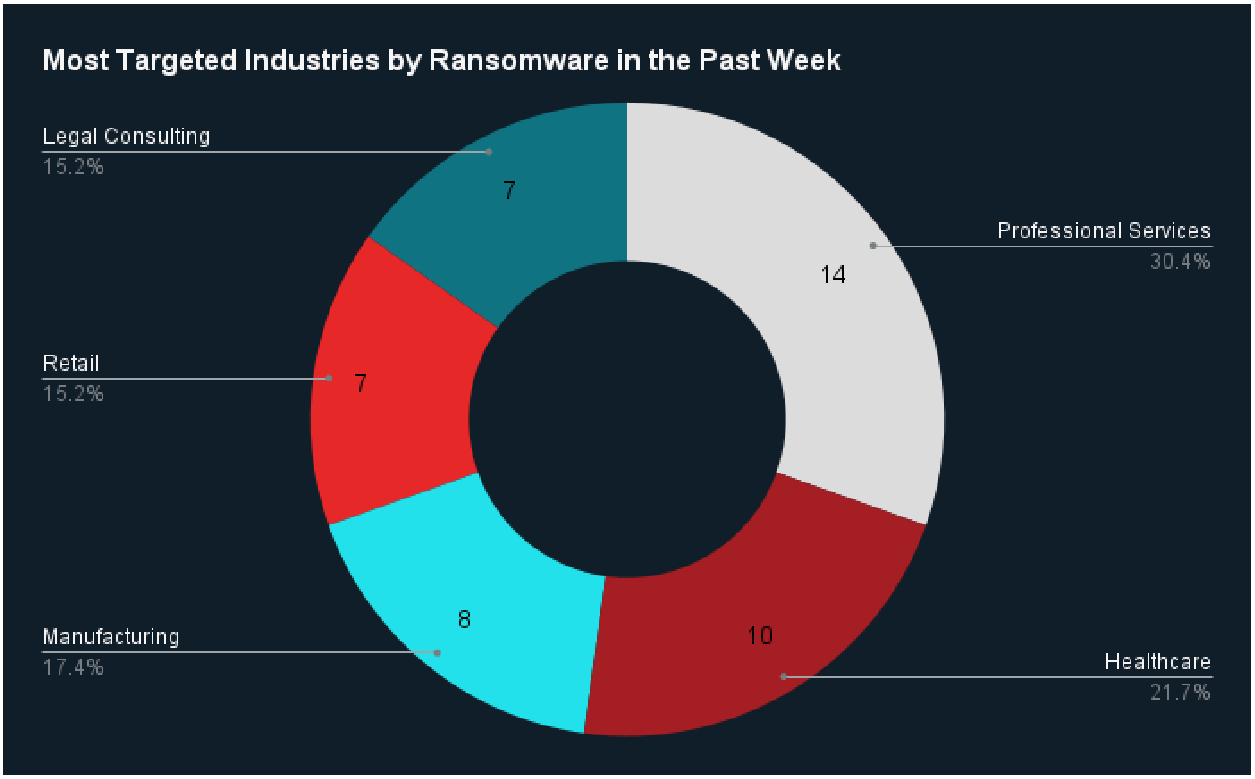
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup: Threat Actors, Industries, and Region



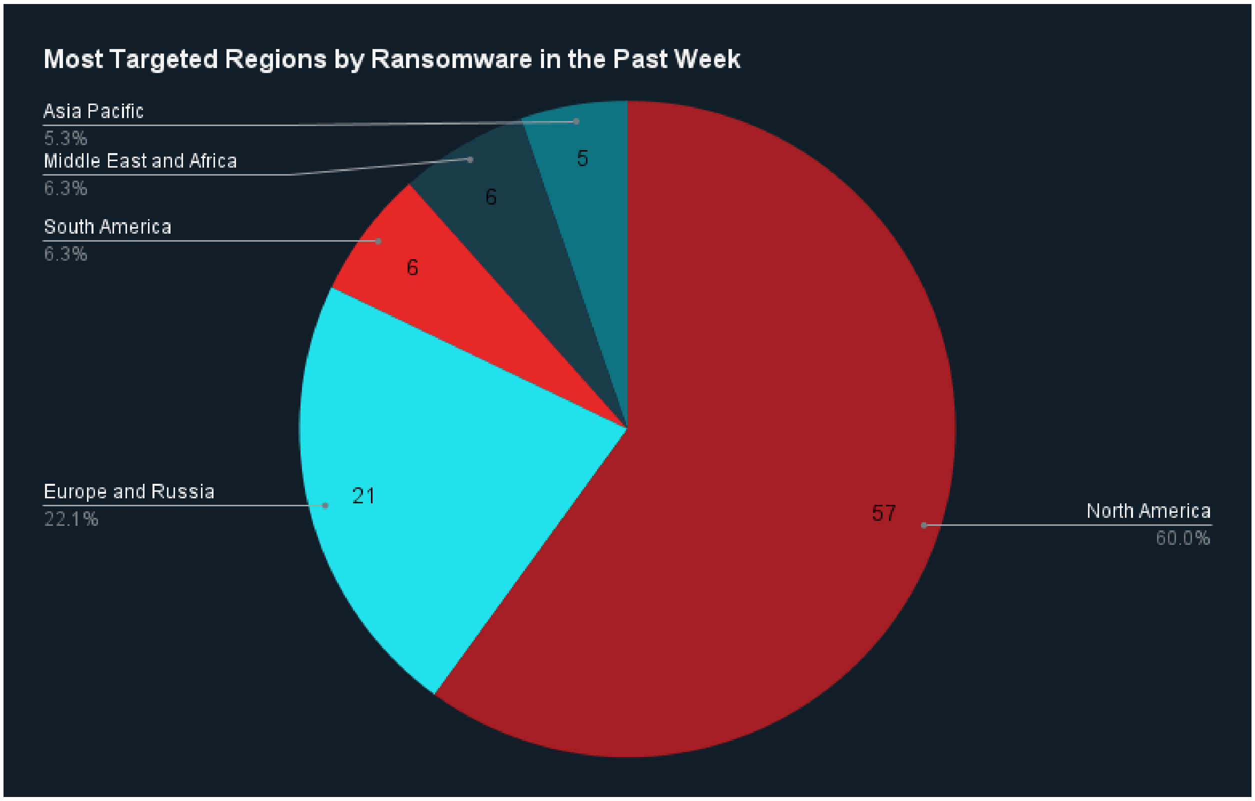
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, DragonForce, Warlock, Qilin, Dire Wolf, and Everest were the most active ransomware groups. ZeroFox observed at least 83 ransomware victims disclosed, most of whom were located in North America. The DragonForce ransomware group accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that professional services was the most targeted industry, with 14 attacks identified. Healthcare, manufacturing, retail, and legal consulting industries comprised the other most-targeted industries.



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 saw 57 counts of ransomware attacks, while Europe-Russia accounted for 21. Additionally, South America and the Middle East and Africa regions were targeted six times, while the Asia-Pacific region accounted for five attacks.

Major Data Breaches of the Week

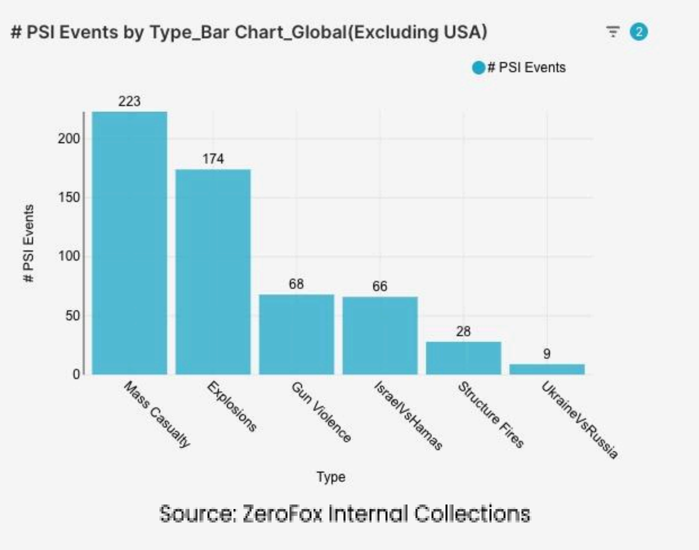
Targeted Entity	Saudi Games	Israel "Shelter" Locations	Liberty Township
Compromised Entities	Visitors and athletes from previous Saudi Games	Reportedly, 1,046 coordinates of fallout shelters in Israel (civilian safe zones during conflict)	48 GB of data, including employee login credentials
Compromised Data Fields	Personally identifiable information (PII) of visitors and athletes, including passport details, International Bank Account Numbers (IBANs), and medical certificates; IT staff credentials, including hashed passwords; and details of government officials on the site	Coordinates of locations reportedly serving as fallout shelters during Iranian airstrikes targeting Israel	Login credentials to multiple sites, including secure portals and township utilities
Suspected Threat Actor	Cyber Fattah or DarkForums user "ZeroDayX"	Handala Hack Team	Safepay ransomware group
Country/Region	Saudi Arabia	Israel	United States
Industry	Entertainment	Government and Security	Government
Possible Repercussions	Identity theft, fraud, phishing, and social engineering attacks, as well as ransomware attacks using credentials and encryption of critical data	Psychological impact triggering distrust in shelters and other safe zones; in cases of legitimate data, crowding at shelters and targeting of shelters by adversarial entities	Unauthorized login, data theft, and encryption leading to ransom demands and data leaks

Three major breaches observed in the past week

Recap of major data breaches observed in the past week: North American steel giant Nucor confirmed that threat actors stole data from the company's network following the May 2025 cyber incident. A major U.S. insurance company, Aflac, disclosed that hackers stole customers' personal information, including Social Security numbers (SSNs), during a cyberattack reported earlier in June 2025. At least 11 class action lawsuits have been filed against Aflac over the data breach. The Oxford City Council in the United Kingdom disclosed that some historic data on legacy systems was stolen during a cyberattack. The data stolen contained information on those who worked in the council-administered elections between 2001 and 2022.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

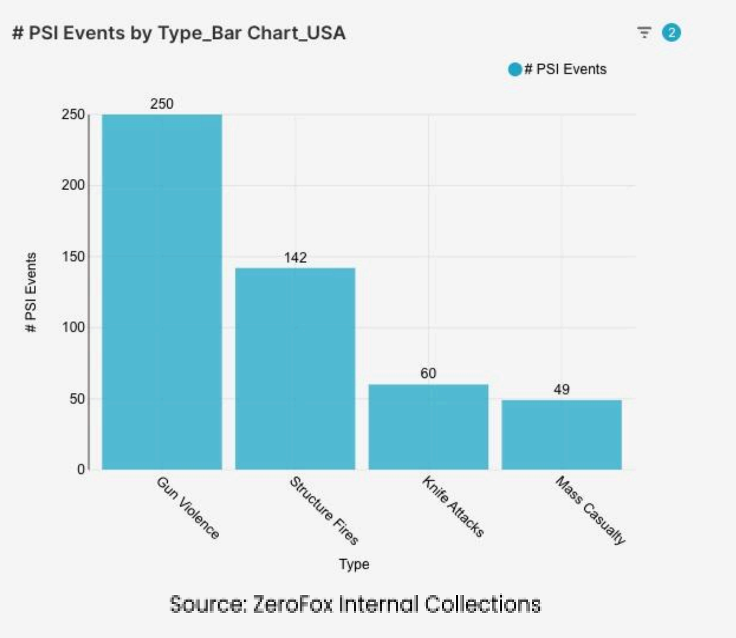


Source: ZeroFox Internal Collections

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, Israel, and the Palestinian territories, in that order. Approximately 78 percent of these events were explosions, and the aforementioned countries and territories accounted for approximately 49 percent of all mass casualty alerts. General alerts related to the Israel-Hamas war (including protests, raids, and attacks) decreased by 33 percent from the previous week. Events related to Russia's war in Ukraine increased by 80 percent. The top three most-alerted subtypes were explosions, which saw a 12 percent decrease from the previous week; gun violence, which increased by 39 percent; and structure fires, which increased by 8 percent. Meanwhile, global protest activity decreased by 11 percent.

- **What this means:** The primary contributors to mass casualty alerts this week, accounting for nearly half of all such events, were Iran, Israel, and the Palestinian territories; however, both mass casualty alerts and explosions saw decreased numbers this week compared to the week prior. This localized reduction within the volatile region, where a 12-day war saw intensive strikes resulting in multiple casualties, may be attributable to ongoing attempts at de-escalation and a recently announced, though fragile, ceasefire between Israel and Iran. Despite this, significant incidents continue, such as a recent missile barrage from Iran killing four people in Beersheba, Israel, on June 24. Conversely, data reveals a sharp increase in events linked to Russia's ongoing war in Ukraine, exemplified by a Russian missile attack on Dnipro, Ukraine, on June 24 that killed at least 17 and injured nearly 280 and a mass drone and missile attack on Kyiv, Ukraine, on June 23 that killed at least nine and injured 33. Gun violence also showed a significant increase, with Kenya being the top contributing country; 16 anti-government protesters were killed and at least 400 others were wounded on June 25 in Nairobi. All of these conflicts collectively underscore the precarious state of global physical security.



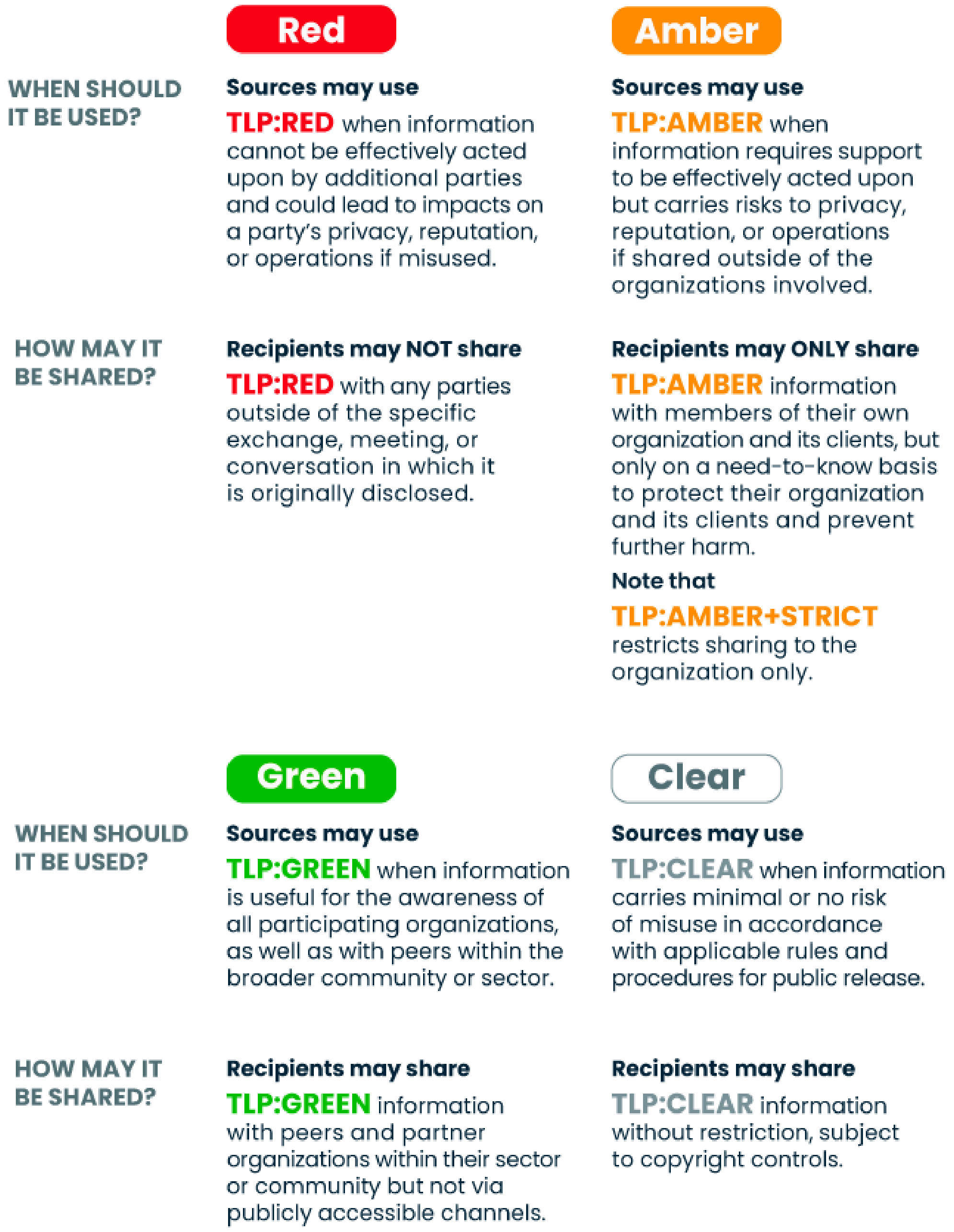
Source: ZeroFox Internal Collections

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, structure fires are fires that affect man-made buildings, and knife attacks involve a confirmed slashed or stabbed victim. The top two states with the most gun violence alerts were Illinois and Ohio, which together made up 19 percent of this week's nationwide total. Gun violence across the United States overall increased by 6 percent from the week prior. Structure fires increased by 12 percent, with the top two states for this subtype being New York and California. Knife attacks increased by 11 percent, and the top contributing states were also New York and California. Notably, 20 mass shootings occurred in the United States within the last seven days, and mass casualty alerts increased by 26 percent this week.

- **What this means:** In the United States, the past week has seen an increase in various incident types, with a notable rise in mass casualty alerts and 20 mass shootings; for instance, in Pittsburgh, Pennsylvania, gunfire at a basketball court injured 15 people on June 22 and a mass shooting in Anderson County, South Carolina, left one dead and at least nine injured during Juneteenth celebrations. Structure fires also increased, with New York and California being the top contributors; for instance, in New York, a five-alarm Bronx fire injured 15 people—including a child and 13 first responders on June 22—and Los Angeles Fire Department alerts showed multiple structure fires across the city this week. Knife attacks also increased this week, also most prominently in New York and California. In New York City, two people were stabbed on the subway at Grand Central Terminal on June 18. The increase in gun violence, knife attacks, and aggravated crime in general during summer months may be linked to factors such as increased social interaction and outdoor activity providing more opportunities for conflict, hotter temperatures potentially exacerbating aggression, and the lack of structured activities for youth when schools are not in session.

Appendix A: Traffic Light Protocol for Information Dissemination

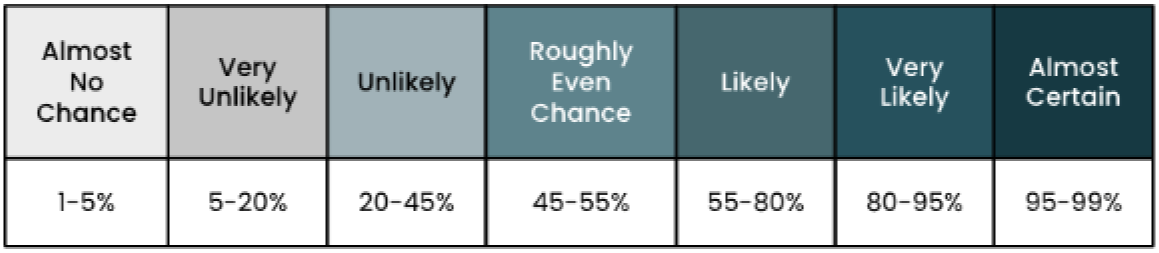


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively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