ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

June 7, 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 5, 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: Web Page Shares Personally Identifiable Information of CEOs

A person or group with an affinity for the suspect alleged to have murdered a United Health Care CEO promoted an online database containing personally identifiable information (PII) on at least 1,061 corporate executives. Although the site has been taken offline as of this writing, an archived version remains, which could still enable a motivated, internet-literate person or group to gain access to an executive's PII. The database consolidates already publicly available contact information in one place—including executive names, job titles, company affiliations, LinkedIn profiles, and, in many cases, mobile phone numbers—raising concerns about its potential misuse for harassment or targeted intimidation.

ZeroFox Intelligence Flash Report: U.S. Property Data Advertised for Sale on Dark Web Forum

On May 27, 2025, an actor using the alias “Sentap” posted on the predominantly Russian-speaking dark web forum xss advertising the sale of 1.02 terabytes of property data. Sentap claimed to have obtained "unprecedented" access to this data from the cloud infrastructure of a U.S.-based title company that specializes in property record search services. Sentap also claimed that the data encompasses “strategic” regions of Illinois, Indiana, Wisconsin, Minnesota, Iowa, Colorado, and Kansas but offered no further context. If the data is as-advertised, its diverse nature would almost certainly appeal to a wide array of mostly financially motivated threat actors seeking to exploit PII.

ZeroFox Intelligence Flash Report: BreachForums and Notorious Actors Announce Re-emergence

On June 3, 2025, an actor using the alias “darked321” posted in the deep web forum DarkForums claiming its counterpart-BreachForums, another popular deep web hacking forum, has been relaunched. Darked321’s DarkForums post quoted a longer message from actor “ShinyHunters”, who provides an alleged explanation as to the status of the original BreachForums domain, and plans for the new one. ZeroFox also observed activity from “IntelBroker”. Given the presence of ShinyHunters and IntelBroker, there is a likely chance that breach-forums[.]st represents a relaunch effort led by actors in possession of digital infrastructure associated with the original domain. There is a very likely chance that breach-forums[.]st will quickly gain traction and restore functionality, though it is also likely that many users will remain active within peer domain DarkForums-where many actors migrated upon BreachForum's disruption.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

International Law Enforcement Seizes AVCheck, Disrupting Malware Testing Service

What we know:

- An international law enforcement operation took down AVCheck, a service used by cybercriminals for testing malware against antivirus software.
- Investigators found evidence that AVCheck's administrators were connected to crypting services such as Cryptor[.]biz and Crypt[.]guru, both of which help obfuscate malware to bypass detection.

Background:

- AVCheck was one of the largest counter antivirus (CAV) services, allowing cybercriminals to test the stealth and evasion of their malware before launching it in the wild.
- The takedown was part of Operation Endgame, which also led to the seizure of 300 servers and 650 domains involved in facilitating ransomware attacks.

What is next:

- AVCheck provided cybercriminals with an environment to test and improve their malware's ability to evade antivirus detection before deployment—likely helping them carry out stealthier attacks.
- It is likely that more domains or services connected to the CAV ecosystem may be identified and targeted for seizure by authorities.

Cybercriminals Defraud Hedera Hashgraph Wallet Users Through NFT Airdrops

What we know:

- The Federal Bureau of Investigation (FBI) has announced that cybercriminals are exploiting the nonfungible token (NFT) airdrop feature in non-custodial wallets to target Hedera Hashgraph users. These fake airdrops appear as free rewards but are designed to steal user data and cryptocurrency.

Background:

- The Hedera Hashgraph is Hedera’s distributed ledger. The airdrop feature was originally created by the non-custodial wallet companies for marketing purposes.

Analyst note:

- Exploiting the NFT airdrop feature enables cybercriminals to trick users into exposing sensitive data and granting access to their wallets—leading to theft of cryptocurrency, causing financial loss. The stolen user data can be used for further targeted attacks, like fraud and identity theft.

CISA and Partners Issue Updated Advisory on Play Ransomware

What we know:

- The Cybersecurity and Infrastructure Security Agency (CISA) and its partners have issued an updated advisory on Play ransomware (aka Playcrypt), highlighting new tactics, techniques, and procedures (TTPs) and updated indicators of compromise (IOCs) to enhance threat detection.

Background:

- Since June 2022, ZeroFox has observed Play ransomware group carrying out at least 850 attacks targeting diverse businesses and critical infrastructure across North America, South America, and Europe.

Analyst note:

- To mitigate Play ransomware threats, organizations are advised to prioritize fixing known vulnerabilities, enable multifactor authentication (MFA) for key services, and regularly update software while conducting vulnerability assessments.

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. CISA added five vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog and released eight Industrial Control Systems (ICS) vulnerabilities on May 29 and June 3. Meanwhile, Cisco has released a patch for a static credential vulnerability in its Identity Services Engine (ISE) caused by improper credential generation. Google has issued out-of-band patches to a flaw that enables a remote attacker to potentially trigger heap corruption by leveraging out-of-bounds read and write errors via a maliciously crafted HTML page—likely leading to unauthorized code execution or browser crashes and posing security risks to users. CVE-2025-48827 and CVE-2025-48828 are two vulnerabilities in vBulletin that could enable attackers to execute arbitrary code remotely, taking full control of affected vBulletin servers, stealing user data, and deploying malware. Qualcomm has issued security patches for CVE-2025-21479, CVE-2025-21480, and CVE-2025-27038—three zero-day vulnerabilities in its Adreno Graphics Processing Unit (GPU) driver. If left unpatched, they could enable attackers to execute arbitrary code or gain unauthorized access, potentially compromising affected devices and sensitive data.

HIGH

CVE-2025-37089

What happened: A command injection remote code execution vulnerability exists in HPE StoreOnce Software.

- **What this means:** This vulnerability is among eight recently patched by Hewlett Packard Enterprises. If affected devices are left unpatched, this vulnerability could enable threat actors to conduct unauthorized modifications of system configurations and service disruptions.
- **Affected products:**
    - HPE StoreOnce Software from 0 before 4.3.11

MEDIUM

CVE-2025-5610

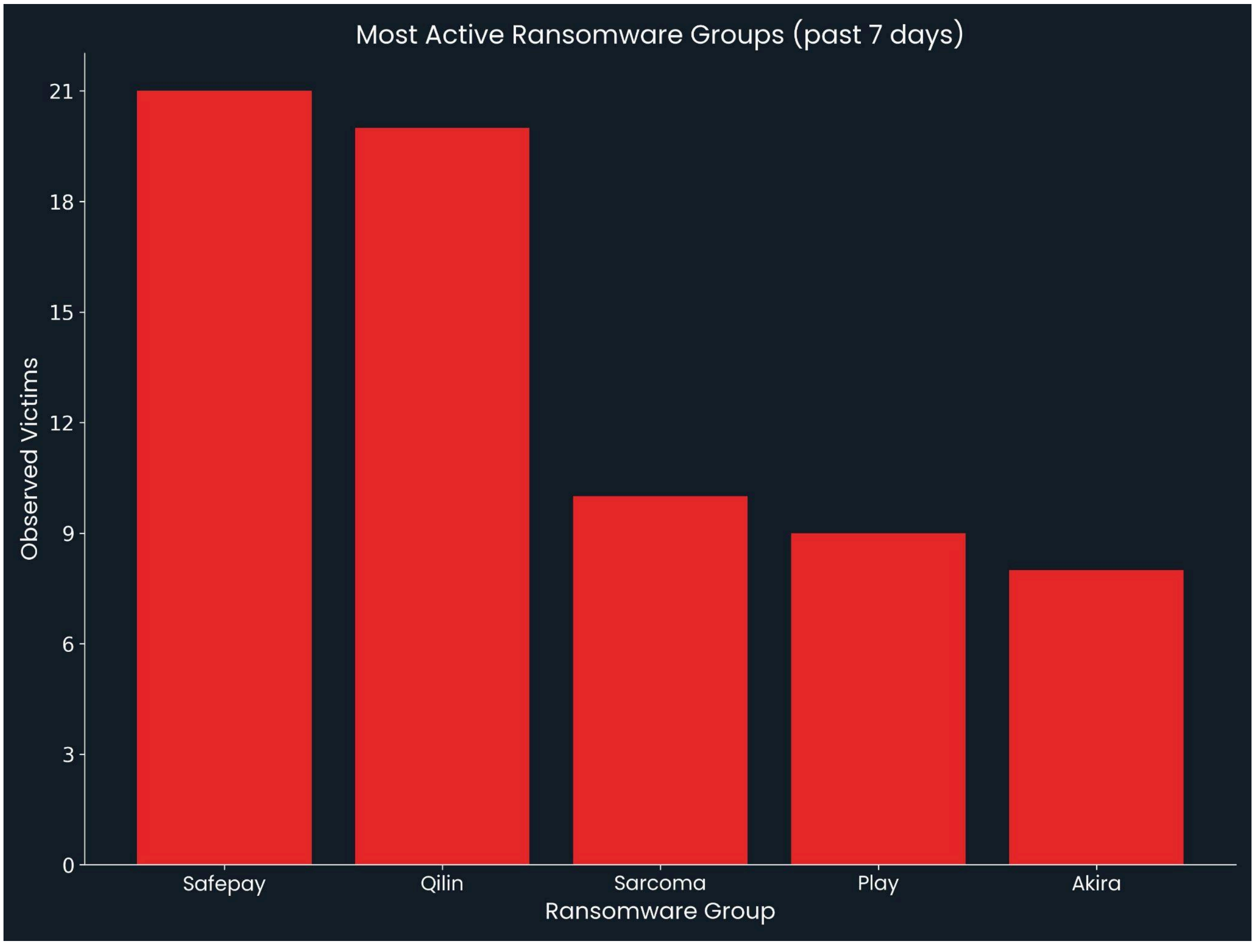
What happened: This SQL injection flaw, specifically observed in the /submitpropertydelete.php file via the ID parameter, can be exploited remotely.

- **What this means:** A public proof-of-concept is reportedly available for this vulnerability, increasing the risk of active exploitation.
- **Affected products:**
    - CodeAstro Real Estate Management System 1.0

Ransomware and Breach Intelligence

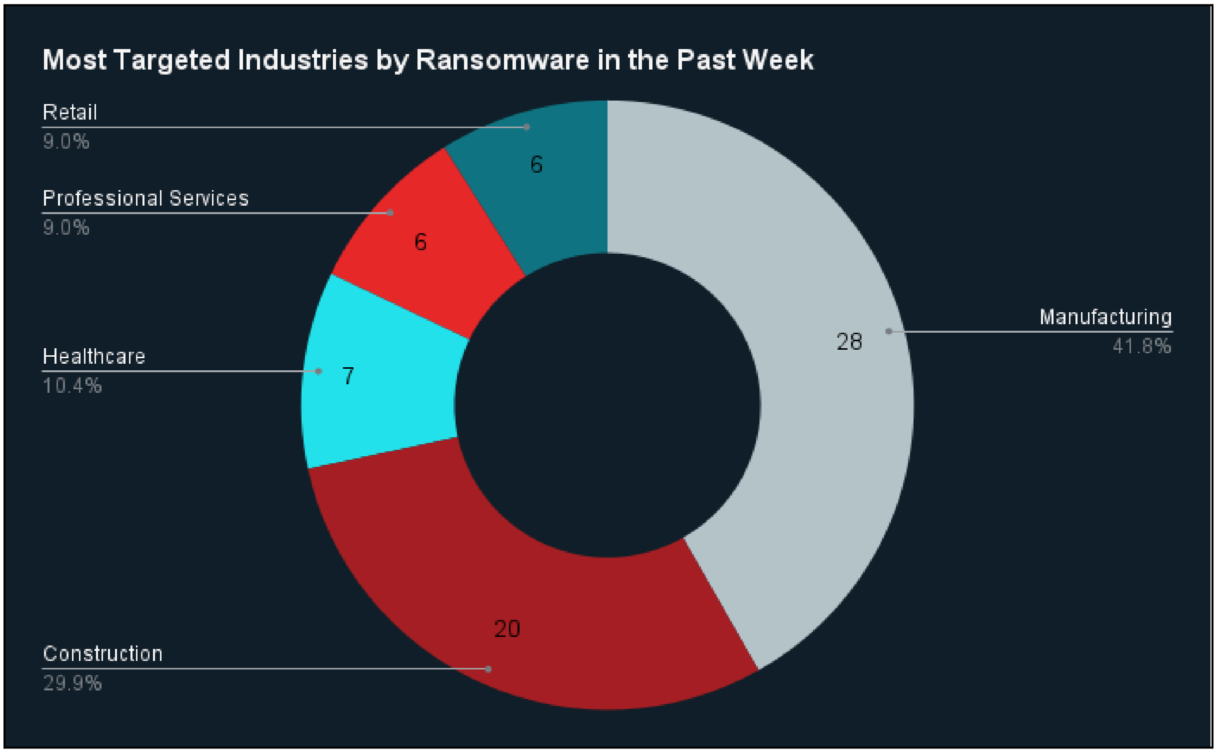
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup of the Week



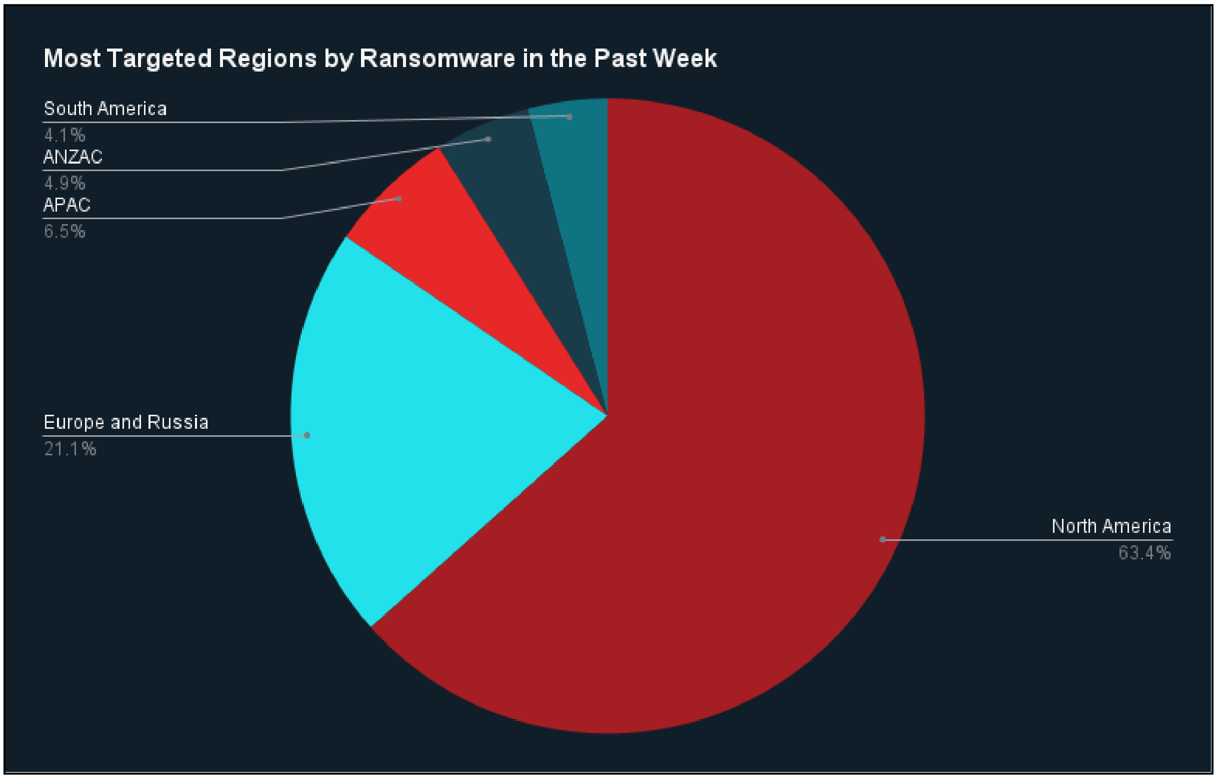
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Safepay, Qilin, Sarcoma, Play, and Akira were the most active ransomware groups. ZeroFox observed that at least 118 ransomware victims were disclosed, mostly located in North America. Safepay and Qilin accounted for the largest number of attacks.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing and construction were the most targeted industries by ransomware attacks, followed by healthcare, professional services, and retail.



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 and Russia.

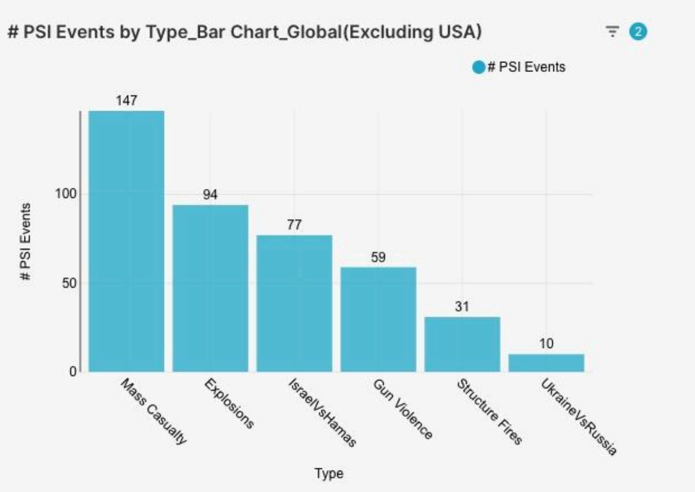
Notable Data Breaches of the Week

Targeted Entity	Cartier	The North Face	Lee Enterprises
Number of Firms/Victims Affected	N/A	2,800 online customers	39,779 readers
Compromised Data Fields	Name, email address, and shipping address	Full name, purchase history, shipping address, email address, date of birth, and telephone number	PII that includes first and last name and Social Security number
Suspected Threat Actor	N/A	N/A	Qilin ransomware group claimed responsibility.
Country/Region	France	United States	United States
Industry	Retail	Retail	Media and Entertainment
Possible Repercussions	Phishing and social engineering attacks, credential stuffing, identity theft, fraud, and ransomware	Identity theft, fraud, phishing attacks, physical threats, social engineering attacks, credential stuffing, and ransomware	Phishing attacks, extortion, politically motivated targeting, and identity theft

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings



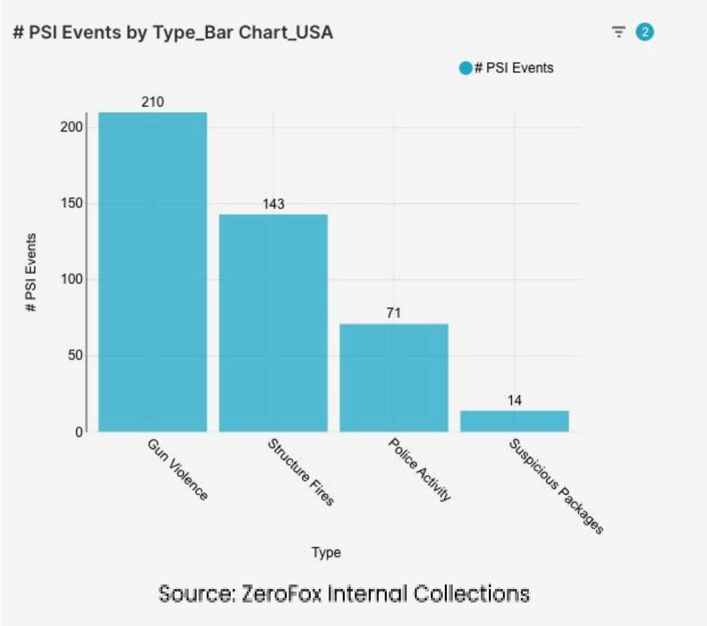
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 13 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, India, and Russia, in that order. Approximately 64 percent of these events were explosions, and the three aforementioned countries accounted for about 33 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 14 percent from the previous week. Events related to Russia's war in Ukraine increased by 11 percent. The top three most-alerted subtypes were explosions, which saw an increase of 13 percent from the previous week; gun violence, which did not increase or decrease; and structure fires, which decreased by 21 percent. Global protest activity increased by 1 percent.

- **What this means:** This week, both mass casualty events and explosions increased at the same rate, with Palestine being the highest contributing region for both incident types. Ongoing reports of strikes and aid distribution incidents in Gaza, where many casualties have been reported this week, have likely contributed to this increase, despite the decline of overall alerts related to the Israel-Hamas War. Concurrently, events tied to Russia's war in Ukraine escalated this week, with reports of continued shelling and drone attacks—including a recent Russian strike on Sumy that killed four people and injured 28. Additionally, Ukraine completed its biggest long-range attack since the beginning of the conflict on June 1, launching a series of major strikes at four military bases in Russia, for which Russian President Putin has vowed to retaliate. Despite these concerning trends in specific regions, global protest activity experienced a marginal 1 percent increase, suggesting that, while conflict zones are seeing heightened violence, broader civil unrest has remained relatively stable this week.

Physical Security Intelligence: United States

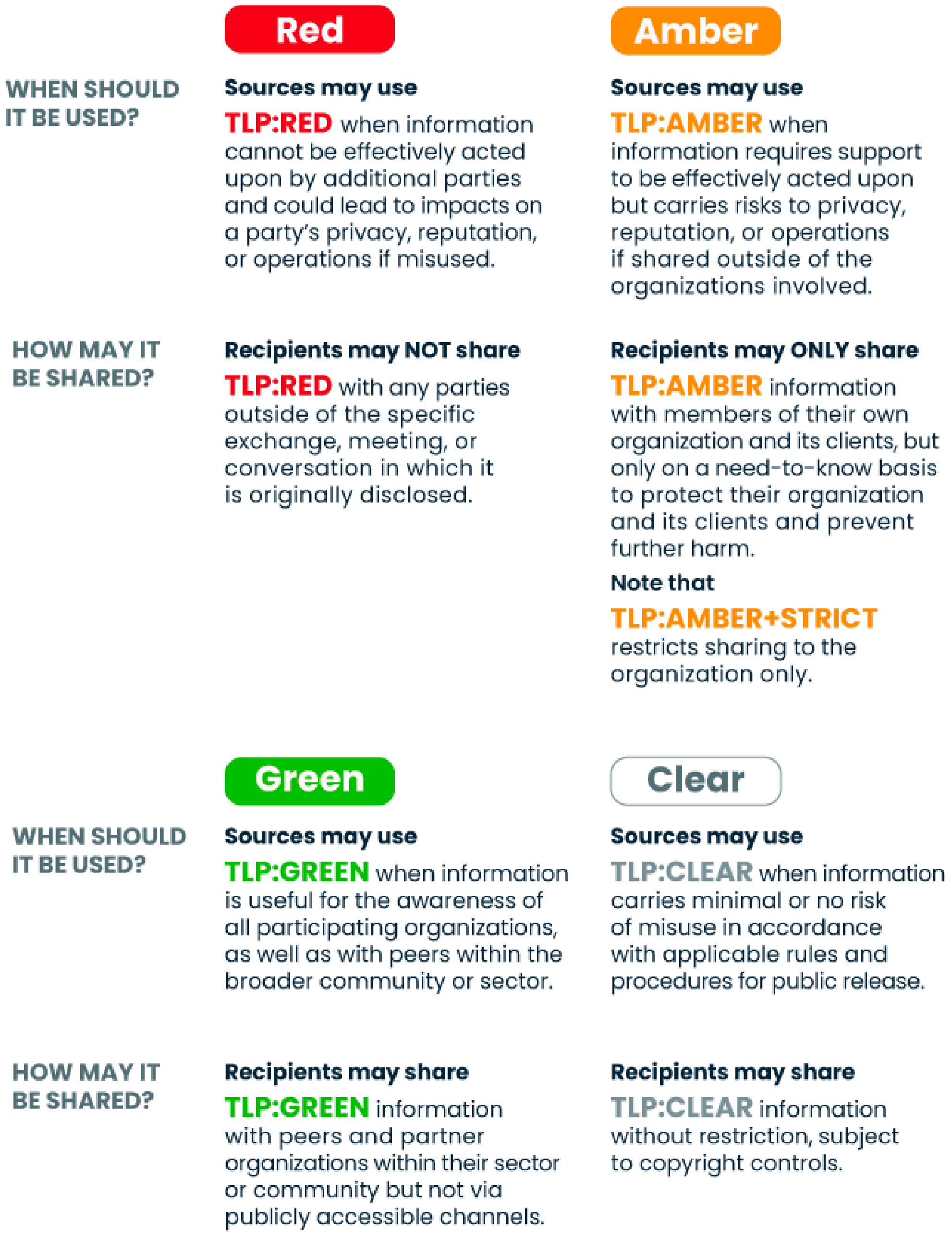


Source: ZeroFox Internal Collections

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 for unknown reasons, and structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were California and New York, which together made up 23 percent of this week's nationwide total. Gun violence across the United States overall decreased by 14 percent from the week prior. Police activity alerts increased by 16 percent, and the top contributing states were California and Michigan. Structure fires decreased by 1 percent, and the top two states for this subtype were New York and California. Notably, suspicious package incidents increased by 180 percent.

- **What this means:** Police activity had a significant increase this week, with Michigan being one of the top two contributing states, which is unusual. One such incident involved a standoff on June 3 in which a suspect was apprehended after an hours-long barricade in Northfield Township, MI. Structure fires experienced a slight decrease this week, with New York and California again being the top states for this subtype. For example, a large three-alarm fire in Bedford–Stuyvesant,, Brooklyn, on June 4 damaged several buildings and displaced residents. Gun violence decreased this week, which aligns with a recent report by the New York City Police Department that cited a historic low in shootings and murders in the city for the first five months of 2025. A particularly noteworthy trend was the sharp increase in suspicious package incidents. A recent example includes the investigation of a suspicious package near the Neal Smith Federal Building in Des Moines, Iowa, on June 4, which was later deemed safe. This significant rise suggests a heightened level of caution and vigilance regarding unattended or unusual items across the country.

Appendix A: Traffic Light Protocol for Information Dissemination

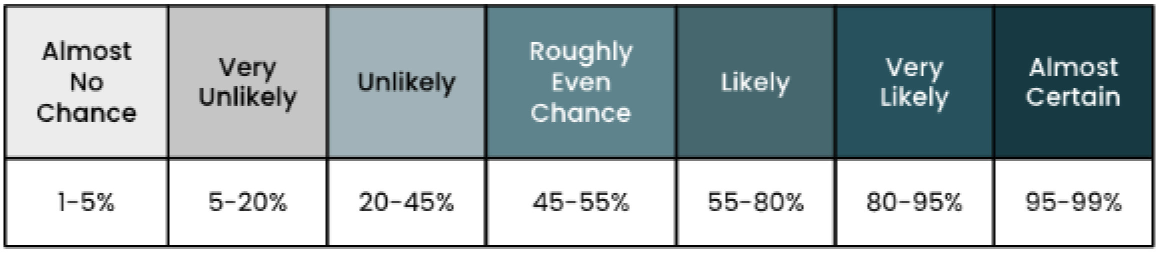


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively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