ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

September 27, 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 September 25, 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 - Cyberattacks on European Airports Reveal Contagion Risk

Over the weekend of September 19–21, 2025, a cyberattack caused widespread operational disruption at major European airports, resulting in a host of flight cancellations and delays. As of writing, no threat actor has claimed responsibility for the attack. The attribution details—such as the ransomware strain or the threat actor responsible—have not yet been made public, and it remains unclear whether a third-party vendor or Collins Aerospace itself was targeted. This attack highlights a critical vulnerability in the IT infrastructure used in the aviation industry, especially where third-party systems support multiple airports and airlines. The airline industry likely faces significant pressure to quickly meet ransomware demands, as customer satisfaction and maintaining scheduled flight times are crucial to its business model.

ZeroFox Intelligence Flash Report - Drone Sightings Disrupt Airport Operations in Europe

Between September 22 and September 25, 2025, drone sightings near airports in Denmark and Norway resulted in the closure of multiple airports, including two of the major international hubs in Copenhagen and Oslo. While the incidents have not been linked to a suspect or motive to date, the possibility of Russian involvement cannot be ruled out. The drone sightings come on the heels of Polish airports being temporarily closed due to Russian drone intrusions on September 10, 2025. They also coincide with a cyberattack that caused disruptions at several major airports in Europe, stirring concerns for the European civil aviation sector. The recent airspace violations in Europe—all with a marked proximity to the Russia-Ukraine conflict—very likely signal a rise in drone and other airspace intrusions across northern and eastern Europe. In the wake of these disruptions, air carriers are likely to adopt longer routes; proceed with contingency planning, including higher insurance premiums; and experience elevated operational costs for passenger and cargo sectors.

ZeroFox Intelligence Brief - Underground Economist: Volume 5, Issue 19

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

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

Europe’s Airlines and Critical Sectors Hit by Cyberattacks This Week

What we know:

- A ransomware attack disrupted operations at major European airports, including at Heathrow, Brussels, Berlin, Dublin, and Cork, affecting electronic check-in and baggage drop systems.
- The UK National Crime Agency (NCA) has arrested a suspect linked to the airport ransomware attack; the suspect was later released on conditional bail.
- Separately, Iranian hacker group Nimbus Manticore (also referred to as UNC1549 or Smoke Sandstorm) is targeting European defense, aerospace, and telecommunication companies for espionage purposes.
- Nimbus Manticore campaigns use phishing emails disguised as job applications that direct victims to fake career websites to deliver malware.

Background:

- The ransomware attack occurred over the weekend of September 19–21, 2025, resulting in a host of flight cancellations and delays.
- On September 22, 2025, the European Union Agency for Cybersecurity (ENISA) confirmed that the disruption was due to a ransomware attack.
- The attacker managed to impact aviation operations despite reportedly using a basic ransomware strain.
- Nimbus Manticore has been active since early 2025 and has previously run campaigns such as the Iranian Dream Job campaign.
- The fake websites in Nimbus Manticore’s campaigns use React templates and Cloudflare protections to hide the attackers’ infrastructure.

What is next:

- Airport and airline operations will likely continue to experience delays and service interruptions as systems are fully restored.
- It is very likely that law enforcement will interrogate the suspect to gather more information about the attack and identify possible additional suspects or accomplices connected to the ransomware operation.
- The Nimbus Manticore operation could provide attackers with long-term access to sensitive corporate systems.

- State-associated threat actors could use the stolen information to fuel espionage campaigns, compromise supply chains, and gain geopolitical leverage for Iran.
- These attacks are likely to push critical sectors in Europe to urgently review their cybersecurity measures, update systems and software, and test backup and recovery plans to prevent similar disruptions in the future.

Threat Actors Are Spoofing FBI's IC3 Website

What we know:

- The Federal Bureau of Investigation (FBI) has warned the public about fake Internet Crime Complaint Center (IC3) government websites.
- Threat actors are reportedly spoofing legitimate government websites to carry out illegal acts, such as stealing personal information and attempting financial scams.

Background:

- Spoofed websites look like legitimate sites but have slightly different characteristics, such as alternative spellings of words.
- The public can unknowingly visit these fake websites while attempting to find the FBI's IC3 website.

Analyst note:

- Data gathered through the fake websites is very likely to be used in phishing and social engineering attacks by financially motivated threat actors.
- Visitors to the fake websites are also likely to unknowingly download malware into their systems, risking system compromise and credential theft.

Secret Service Uncovers SIM Card Farm near the U.N. Headquarters

What we know:

- The U.S. Secret Service has dismantled an illegal communications network in New York involving 100,000 SIM cards and 300 servers capable of sending 30 million texts per minute.
- The network was reportedly spread across facilities within a 35-mile radius of the U.N. headquarters.

Background:

- The evidence found points toward a large-scale SIM card farm, a setup where devices packed with thousands of SIMs can be used to flood phones with spam calls and texts.
- Officials are currently investigating whether the network's location near the U.N. headquarters points to possible foreign surveillance or criminal activity.

Analyst note:

- The network's concentration near the U.N. headquarters suggests that it was likely built for espionage during the U.N. General Assembly summit.
- Additionally, its scale could have strained telecom infrastructure, overwhelming cell towers and hindering emergency response and secure channels.

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) released seven Industrial Control System (ICS) advisories on September 23 and September 25. CISA has also added one vulnerability to its Known Exploited Vulnerabilities (KEV) catalog on September 23. Additionally, it has disclosed that attackers breached a federal civilian executive branch (FCEB) agency last year by exploiting an unpatched GeoServer instance with a critical remote code execution (RCE) vulnerability (CVE-2024-36401). The U.S. national agency and SonicWall are warning SonicWall customers that attackers have brute-forced MySonicWall portal, exposing some of their cloud backup files. SonicWall has also released a firmware update for SMA 100 series devices that can detect and remove OVERSTEP rootkit malware used by threat actor UNC6148. A privilege escalation flaw (CVE-2025-55241), caused by legacy Azure AD Graph API validation errors, allowed cross-tenant token abuse. CVE-2025-10035 is a deserialization bug in GoAnywhere MFT's License Servlet that enables threat actors to carry out command injection attacks in affected products. CVE-2025-20352 is a stack-based buffer overflow in Cisco's Simple Network Management Protocol (SNMP) subsystem that could enable denial-of-service or full system compromise. Cisco has also released advisories in response to active exploitation of zero-day vulnerabilities (CVE-2025-20333 advisory and CVE-2025-20362 advisory) in its ASA and Firepower devices. CVE-2025-10643 and CVE-2025-10644 are authentication bypass flaws in Wondershare RepairIt that reportedly exposed sensitive cloud storage data and AI models. SolarWinds has released a hotfix for CVE-2025-26399, an unauthenticated RCE flaw in Web Help Desk caused by unsafe deserialization in the AjaxProxy component. The issue is a patch bypass of earlier CVEs and affects WHD 12.8.7, making immediate updates essential.

MEDIUM

CVE-2025-7937 and CVE-2025-6198

What happened: Researchers have disclosed two Baseboard Management Controller (BMC) firmware vulnerabilities in Supermicro devices that enable crafted firmware images to redirect validation tables (fwmap / sig_table) into unsigned regions, causing the signature verification process to be bypassed.

- **What this means:** An attacker could exploit these flaws to load malicious firmware that passes validation and bypasses the Root of Trust, enabling persistent, low-level control of the BMC and host OS, risking full server compromise, supply-chain tampering if signing keys or images are abused.

- **Affected products:**
    - Supermicro BMC in select motherboards

HIGH

CVE-2025-10184

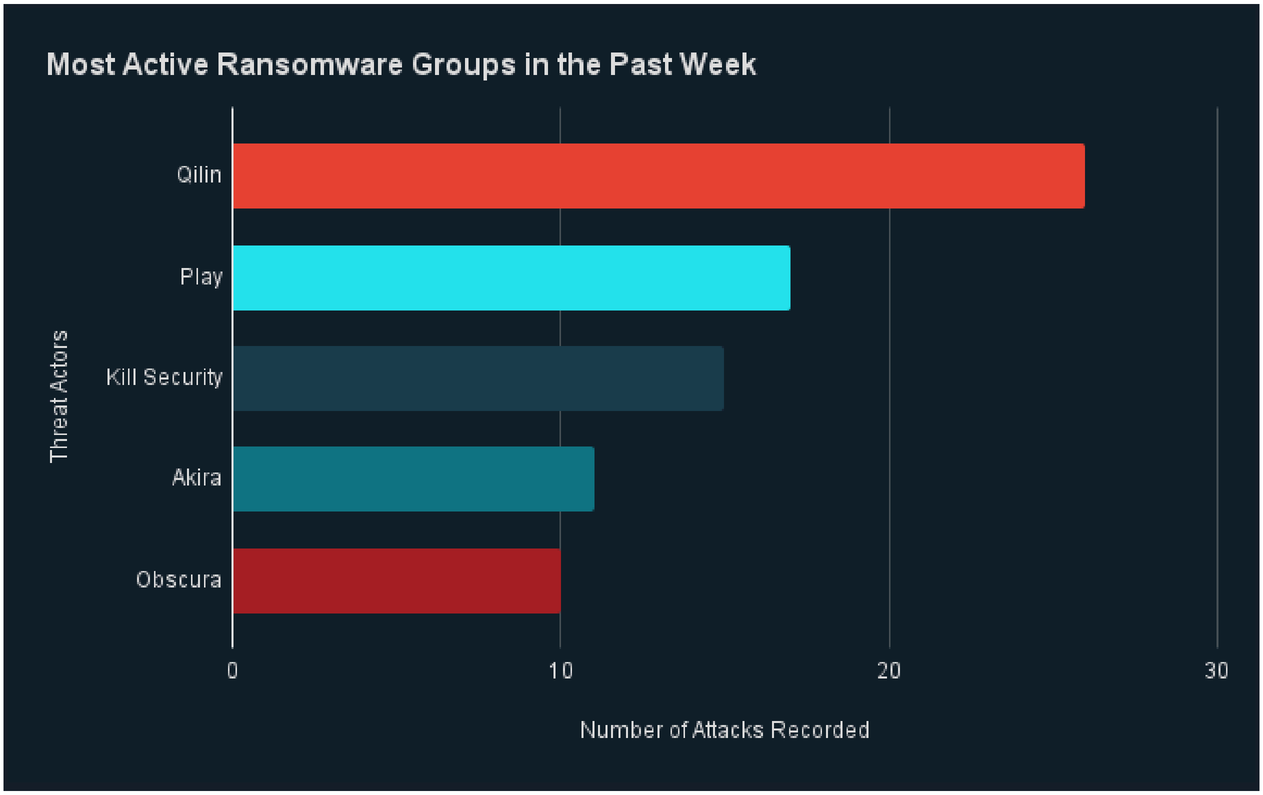
What happened: This flaw in OxygenOS enables any installed app to silently read SMS or MMS data and metadata without permissions or user awareness. The flaw reportedly stems from missing permission checks and a blind SQL injection bug in Telephony providers.

- **What this means:** This bug could weaken account security and potentially enable account takeovers in affected devices. The root cause creates a severe privacy and security risk, as attackers are likely to extract message content and metadata successfully without triggering alerts or permissions prompts.
- **Affected products:**
    - OnePlus OxygenOS versions 12 to 15

Ransomware and Breach Intelligence

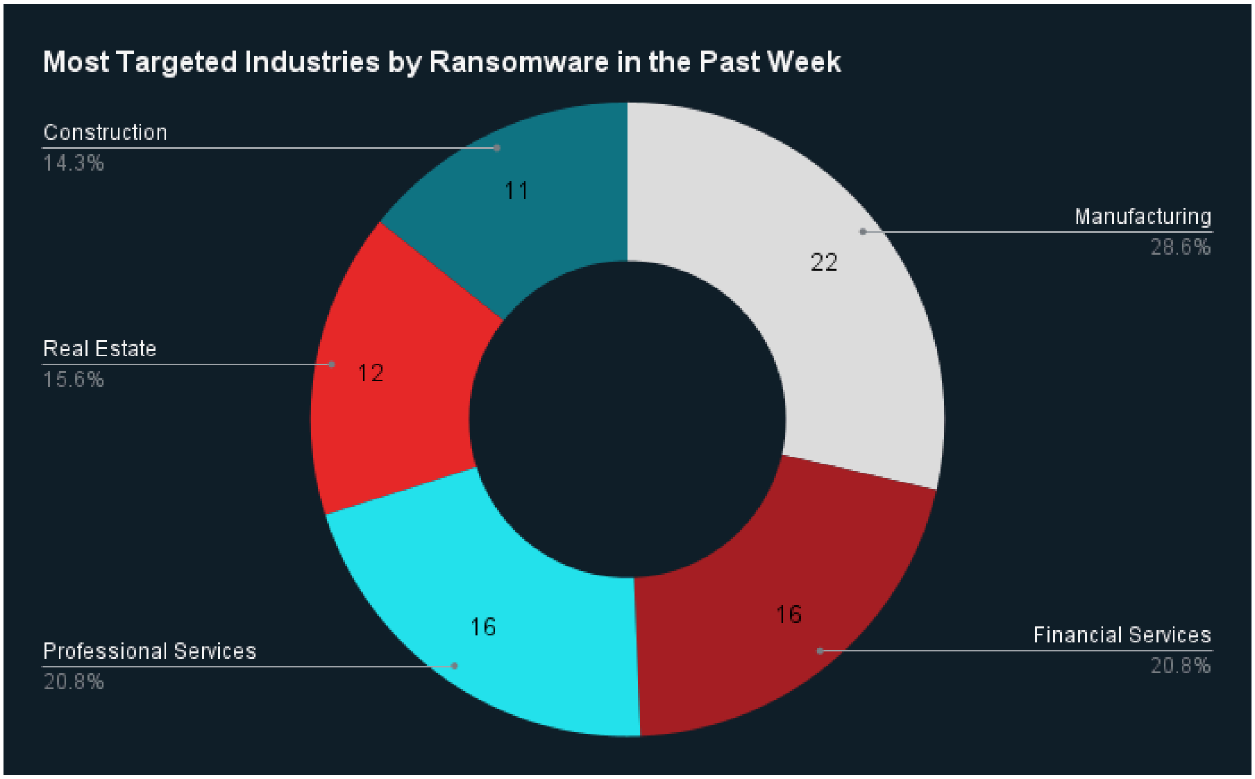
Ransomware and Breach Intelligence Key Findings

Ransomware Roundup: Most Active Groups, Regions, and Industries



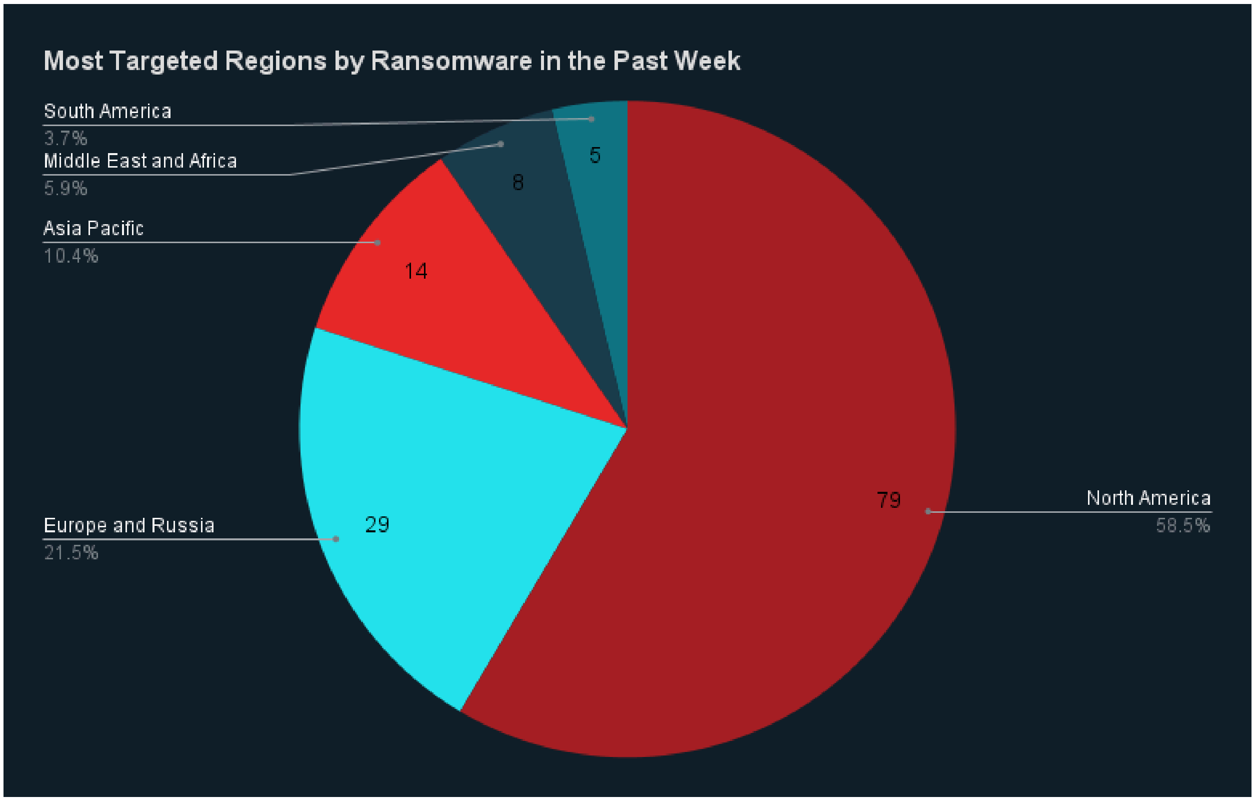
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Play, Kill Security, Akira, and Obscura were the most active ransomware groups. ZeroFox observed at least 120 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Play.



Source: ZeroFox Internal Collections

Industry ransomware trend: In the past week, ZeroFox observed that manufacturing was the most targeted industry by ransomware attacks, followed by financial and professional services, real estate, and construction.



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. There were at least 79 ransomware attacks observed in North America, while Europe and Russia accounted for 29, Asia-Pacific (APAC) for 14, Middle East and Africa for eight, and South America for five.

Significant Data Breaches Detected in the Past Week

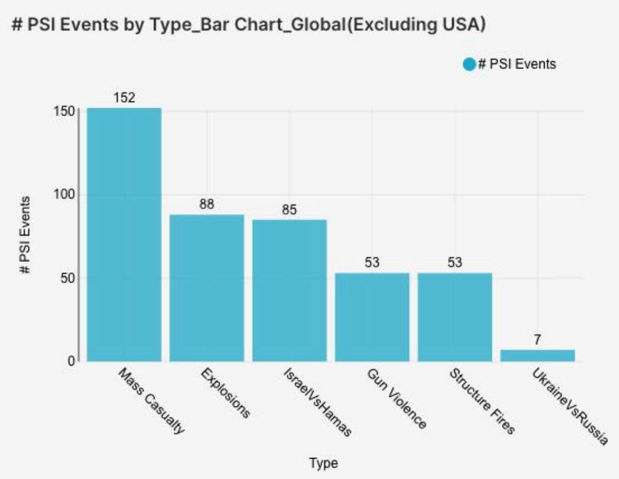
Targeted Entity	**Stellantis N.V.**	**Boyd Gaming**	**Volvo Group North America LLC**
Compromised Entities/victims	Customers' data	Employee information and information of other unspecified individuals	Current and former employees
Compromised Data Fields	Personally identifiable information (PII), including contact details	N/A	PII, including first and last names and Social Security numbers
Suspected Threat Actor	ShinyHunters extortion group	N/A	N/A
Country/Region	North America	United States	North America
Industry	Transportation	Hospitality	Transportation
Possible Repercussions	Phishing attempts targeting exposed customers, with the aim of monetary extortion	Exposed individuals are likely to face phishing and extortion attempts	Identity theft and fraud

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

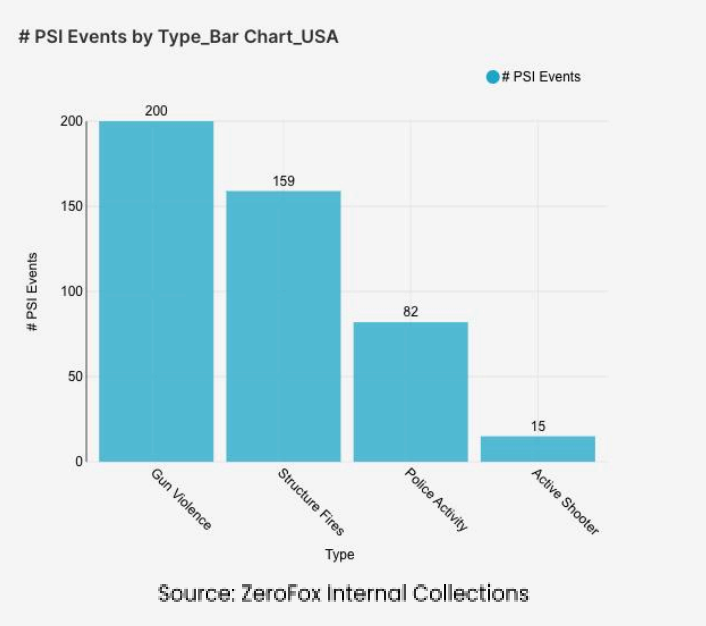


Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was a 9 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian Territories, India, and Ukraine, in that order. Approximately 58 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 32 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 20 percent from the previous week. Events related to Russia's war in Ukraine increased by 17 percent. The top three most-alerted subtypes were explosions, which saw a 5 percent decrease from the previous week; gun violence, which increased by 2 percent; and structure fires, which increased by 13 percent. Global protest activity increased by 21 percent.

- **What this means:** Despite a decrease in overall mass casualty alerts, volatility increased in localized conflict zones, driven largely by explosions. As for the Israel-Hamas conflict, which showed a significant increase in alerts, recent updates have included Israeli tanks pushing deeper into Gaza City, as well as forces continuing intensified assaults against targets, including the destruction of an evacuated health center on September 23. Mirroring the conflict escalation, global protest activity simultaneously rose this week, as evidenced by large-scale, pro-Palestinian demonstrations in major European cities such as Milan on September 22. Events related to Russia's war in Ukraine also surged, with ongoing cross-border attacks and drone strikes; 1,495 Ukrainian troops were killed in the past 24 hours of fighting as of September 25, according to Russian news agencies. Meanwhile, the ongoing 80th United Nations General Assembly (UNGA) in New York City has become an arena for world leaders to call for immediate ceasefires related to both of the aforementioned conflicts, as well as to discuss other global issues. It is yet to be determined whether these conversations will lead to actionable changes.

Physical Security Intelligence: United States

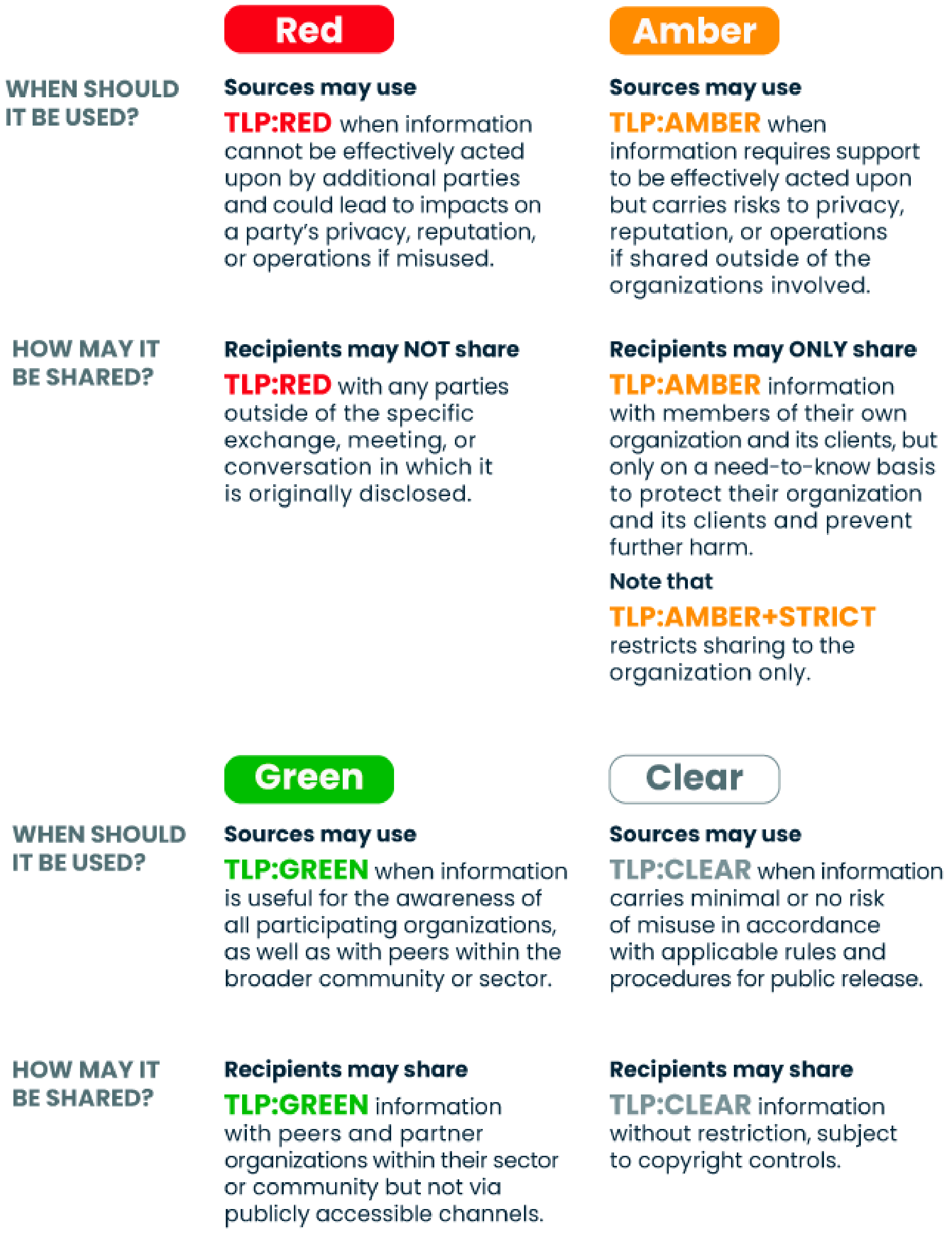


Source: ZeroFox Internal Collections

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 Ohio and Illinois, which together made up 20 percent of this week's nationwide total. Gun violence across the United States overall did not increase or decrease from the week prior. Police activity alerts decreased by 35 percent, and the top contributing states were California and North Carolina. Structure fires increased by 3 percent, and the top two states for this subtype were New York and California. Notably, active shooter alerts increased by 50 percent.

- **What this means:** This week's data reveals a complex landscape of crime and man-made disasters across the United States. While gun violence did not increase or decrease overall, this week saw a spike in active shooter events, with 12 mass shootings (that is, shootings in which there are four or more victims) occurring within the last seven days; for instance, a mass shooting in Shreveport, Louisiana left two dead and six injured after a fight broke out at a large gathering. While this event was seemingly random, there were other ideologically motivated attacks as well; for instance, a shooting outside of the U.S. Immigration and Customs Enforcement (ICE) facility in Dallas, Texas, resulted in four victims (including the shooter, who had "Anti-ICE" written on a bullet found at the scene). Structure fire alerts saw only a small increase, as there has been progress in containment efforts for both the Dillon Fire and Blue Fire in California this week. The steep rise in active shooter alerts—alongside persistently high rates of gun violence (particularly ideologically motivated attacks)—and geographically concentrated structure fires demonstrate the ever-evolving nature of national physical security.

Appendix A: Traffic Light Protocol for Information Dissemination

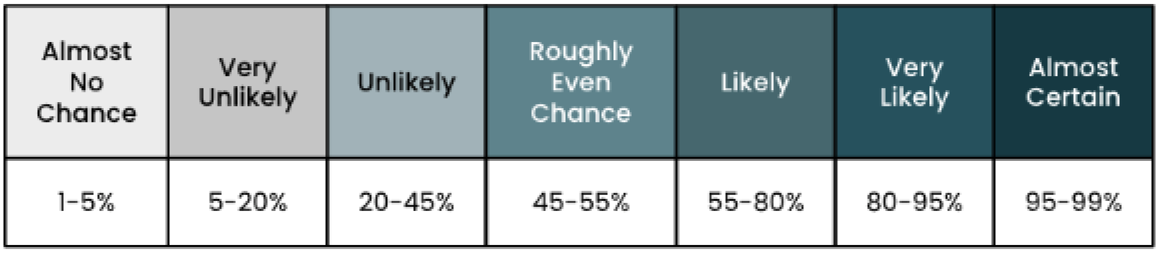


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively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