ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

May 30, 2026

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 28, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Weekly Intelligence Brief

This Week's ZeroFox Intelligence Reports

Fragile Ceasefire – SITREP #38: May 28, 2026

The United States and Iran have likely reduced their negotiation gaps, making a memorandum of understanding (MOU) on ending the war more likely. Initial reports indicate that the latest draft MOU outlines a roadmap for a permanent end to the war and includes a 60-day window to implement a full peace deal and negotiate other issues. That window would almost certainly be extended. As predicted in ZeroFox's SITREP report dated April 23, 2026, the United States has likely adjusted its negotiating position to align closer with Iranian demands, led by moving away from an immediate mandate to denuclearize and instead pushing the topic until a later date. However, key differences remain, and a formal acknowledgement ending the war has yet to materialize, making a return to conflict unlikely but not improbable—especially if talks collapse or stall into June. Global markets are reacting positively, suggesting deal prospects outweigh escalatory risks. However, the relative lack of economic pressure on the United States is likely delaying full support for the MOU, as it is likely leading to internal concerns that the deal is overly favorable to Iran.

ZeroFox Intelligence Brief: The Role of Initial Access Brokers in Ransomware Operations

Initial Access Brokers (IABs) have become a key part of the ransomware ecosystem by obtaining and selling unauthorized network access to threat actors. Several ransomware affiliates, such as Akira, BlackBasta, and Conti, have been known to purchase access directly rather than conducting the initial intrusion themselves, accelerating attack timelines and reducing operational effort. The decline in publicly visible IAB listings between Q1 2025 and Q1 2026 likely reflects market maturation rather than reduced activity. High-value access is very likely being increasingly sold through private channels, while some ransomware groups appear to be internalizing access operations. Credential theft, infostealer malware, and exploitation of internet-facing infrastructure remain common access vectors, making early detection and monitoring increasingly critical.

ZEROFOX®

Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

FBI Warns of Spoofed FIFA Domains Targeting the 2026 World Cup

What we know:

- The Federal Bureau of Investigation (FBI) has warned that threat actors are using spoofed versions of the official Fédération Internationale de Football Association (FIFA) website for cybercriminal activity ahead of the 2026 FIFA World Cup.
- These spoofed sites are being used to sell fraudulent tickets and hospitality packages, conduct FIFA recruitment scams, and collect personally identifiable information (PII).

Background:

- The attackers register domains that closely imitate official FIFA branding, layouts, ticketing portals, and hiring pages through typosquatting, fake subdomains, and alternative top-level domains, such as .xyz, .live, .sale, and .org.
- Examples include misspelled domains like filfa[.]org and fake recruitment-themed domains such as jobs-fifa[.]com.

Analyst note:

- Operators of these scams have likely already collected some PII through spoofed websites.
- Additionally, these scams are likely enabling threat actors to build databases of fans, travelers, and job seekers for use in future phishing operations tied to major sporting events.

Los Angeles Transit Breach Tied to Pro-Iran Hacktivist Operation

What we know:

- Pro-Iran hacktivist group “Ababil of Minab” has been attributed to the March 16 breach of the Los Angeles County Metropolitan Transportation Authority (LACMTA).
- The attackers reportedly stole at least 700 GB of emails, backups, and internal files from LACMTA systems.

Background:

- Although train and bus operations continued, the breach reportedly disrupted LACMTA passenger services by disabling some arrival screens and preventing customers from adding funds to transit cards.

Analyst note:

- Given that Ababil of Minab presents itself as a geopolitically motivated hacktivist group, the decision to exfiltrate large volumes of LACMTA data rather than solely cause disruption suggests the operation also likely served intelligence-gathering purposes.
- The stolen data likely provides insight into how transit agencies structure networks and manage communications, supporting future disruption activity.

FBI Issues Alert on "Silent Ransom Group" Targeting U.S. Law Firms

What we know:

- The FBI has issued an advisory warning that the Silent Ransom Group (SRG) is targeting U.S. law firms using social engineering techniques.
- SRG actors pose as IT employees to establish access to victim systems to exfiltrate data without encryption, either using legitimate remote access tools or by visiting the target's location in-person.

Background:

- The threat actors exfiltrate data using tools such as Windows Secure Copy (WinSCP) or a version of Rclone to destinations that include cloud platforms and external drives.
- Victims are then extorted via ransom emails, direct calls to employees, or affected clients.
- Additionally, traditional antivirus products are unlikely to flag intrusion attempts since the group uses legitimate tools.

Analyst note:

- The group's focus on data theft over encryption suggests a specific interest in sensitive legal information that is likely to influence active cases.
- Notably, the tactic of conducting in-person intrusions very likely indicates that some members are locally based.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

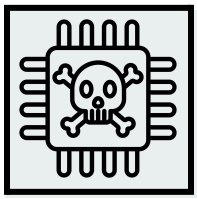
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on May 22 and May 26, 2026. It also included seven Industrial Control System (ICS) advisories on May 26. An SQL injection vulnerability affecting Drupal's database abstraction API due to Improper Neutralization of Special Elements is being actively exploited. Successful exploitation is likely to result in remote code execution (RCE), privilege escalation, and information disclosure. Threat actors are reportedly exploiting a zero-day vulnerability in learning management system (LMS) KnowledgeDeliver, which is widely used for enterprise and educational e-learning in Japan, to deploy web shells and backdoors. Ubiquiti has released security patches for three critical vulnerabilities (tracked as CVE-2026-34908, CVE-2026-34909, and CVE-2026-34910) in UniFi OS that can be exploited by remote attackers without privileges. Trend Micro has patched a directory traversal zero-day vulnerability in Apex One, tracked as CVE-2026-34926, which is being exploited in attacks targeting Windows systems. Threat actors are reportedly exploiting a now-mitigated type of attack variant called domain fronting in shared content delivery network (CDN) infrastructure to hide connections to malicious domains; the vulnerability has been dubbed "Underminr". A critical vulnerability, CVE-2026-48172, impacting LiteSpeed User-End cPanel Plugin is reportedly being actively exploited in the wild.

HIGH

CVE-2026-45659

What happened: Microsoft has patched an RCE vulnerability in Microsoft Office SharePoint due to deserialization of untrusted data. The flaw enables an authorized attacker, with a minimum of Site Member permissions (PR:L), to execute code over a network.

- **What this means:** Threat actors are likely to attempt exploitation of the flaw to steal sensitive information, internal communications, and confidential data often shared via the collaboration platform.
  - **Affected products:** Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, and Microsoft SharePoint Enterprise Server 2016



CRITICAL

CVE-2026-26980

What happened: This is an SQL injection vulnerability in Ghost CMS, an open-source content management system used by over 100,000 websites. The flaw exists in Ghost's Content API, enabling an unauthenticated attacker to extract the site's Admin API key from the database without authorization and subsequently modify published articles. Threat actors have actively exploited this vulnerability to inject malicious JavaScript loaders into compromised sites, triggering ClickFix attacks.

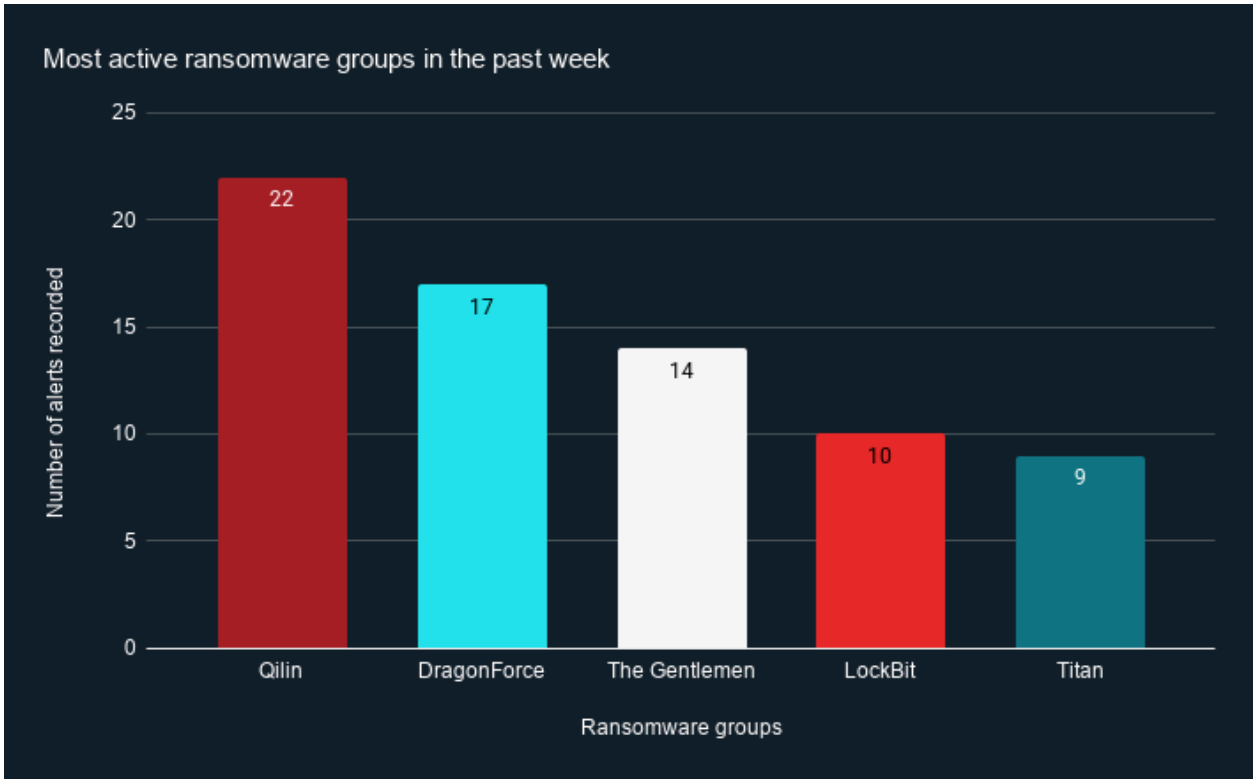
- **What this means:** Threat actors are likely to steal, delete, or modify data on compromised sites, resulting in operational disruptions.
  - **Affected products:** Ghost CMS versions prior to 6.19.1

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

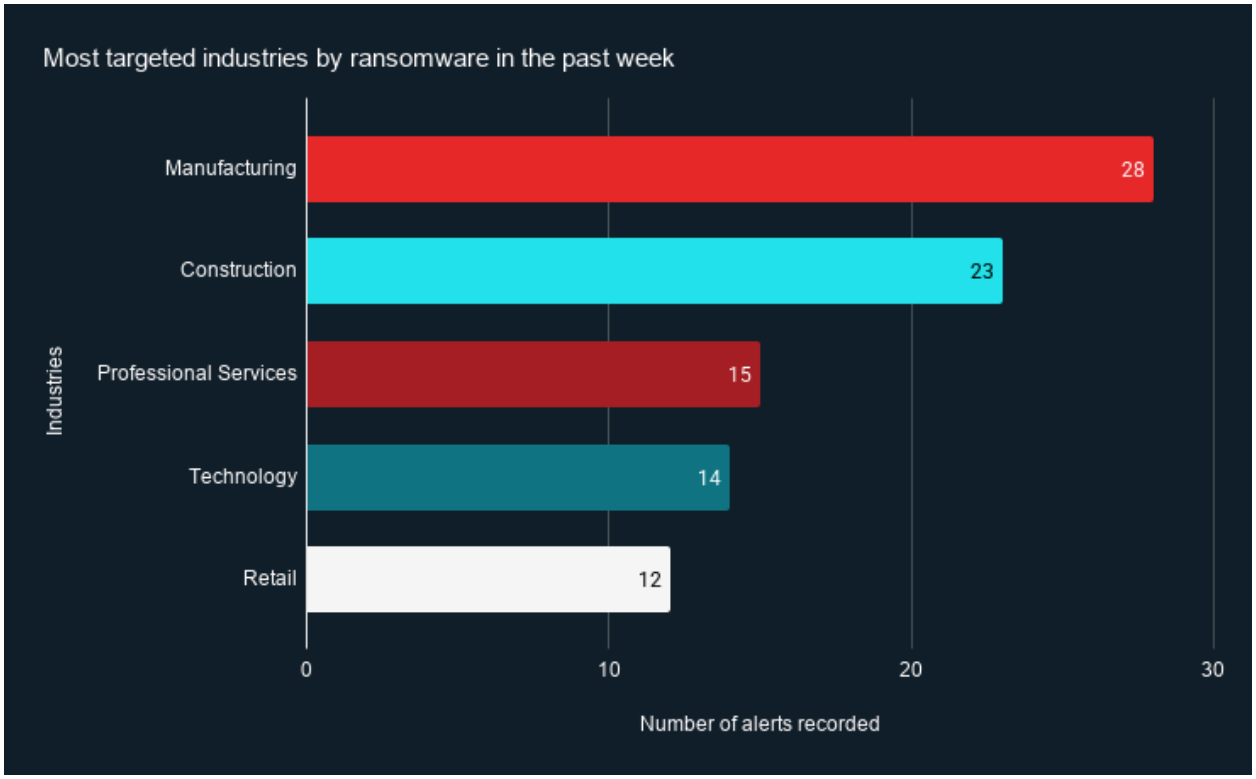
Ransomware Group, Industry, and Regional Trends

Last week in ransomware: In the past week, Qilin, DragonForce, The Gentlemen, LockBit, and Titan were the most active ransomware groups. ZeroFox observed close to 152 ransomware victims disclosed, most of whom are located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by DragonForce.



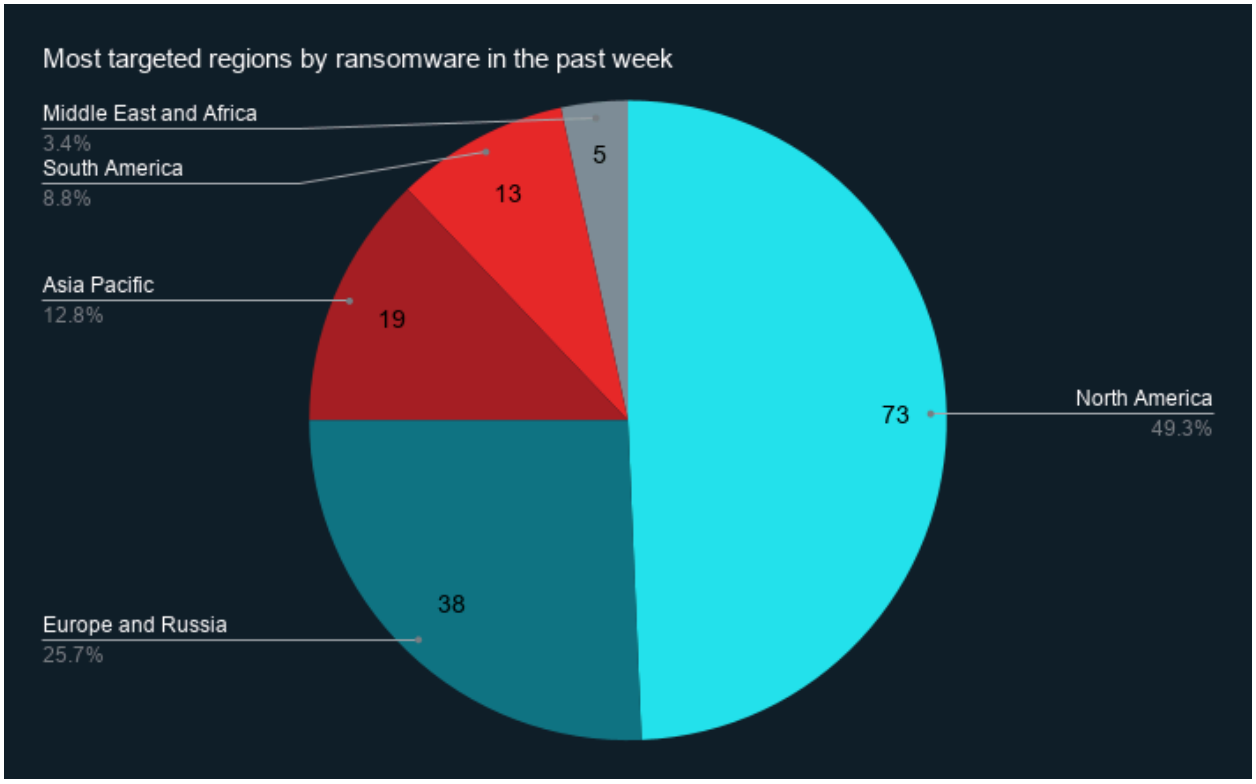
Source: ZeroFox Internal Collections

Industry ransomware trends: In the past week, ZeroFox observed that Manufacturing was the industry most targeted by ransomware attacks, followed by 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 73 ransomware attacks observed in North America, while Europe and Russia accounted for 38, Asia-Pacific for 19, South America for 13, and Middle East and Africa for five.



Source: ZeroFox Internal Collections

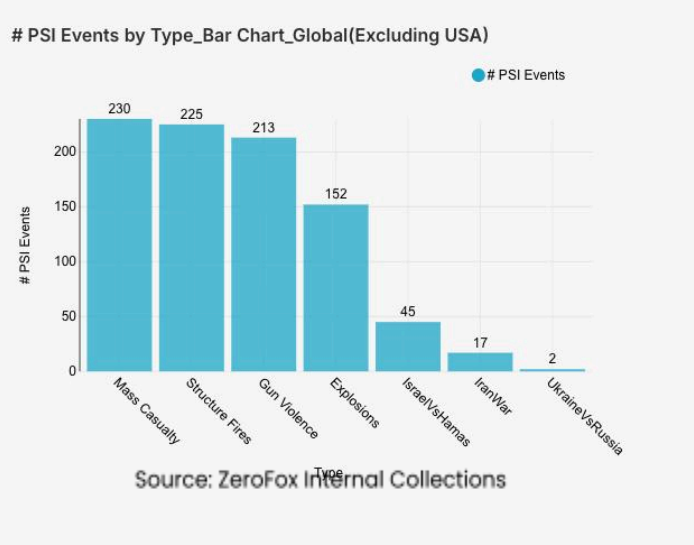
Significant Data Breaches Reported over the Past Week

Targeted Entity	7-Eleven	Lithuania	Radiology Associates of Richmond
Compromised Entities/Victims	Over 600,000 corporate data records	600,000 records managed by the Centre of Registers	266,000 individual's data
Compromised Data Fields	Unique email addresses, names, physical addresses, dates of birth, and phone numbers	Personal and property-related information	Protected health information (PHI), as well as data suspected to be names and Social Security numbers
Suspected Threat Actor	ShinyHunters	Unknown at this time	Unknown at this time
Country/Region	United States	Europe	United States
Industry	Retail/CPG	Government Ministries	Healthcare
Possible Repercussions	Identity theft, phishing attacks, credential stuffing, social engineering, financial fraud, and unauthorized access to corporate systems	Phishing attacks, financial fraud, targeted social engineering attacks, and identity theft	Identity theft, medical fraud, phishing attacks, and unauthorized access to sensitive patient records

Three major breaches observed in the past week

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

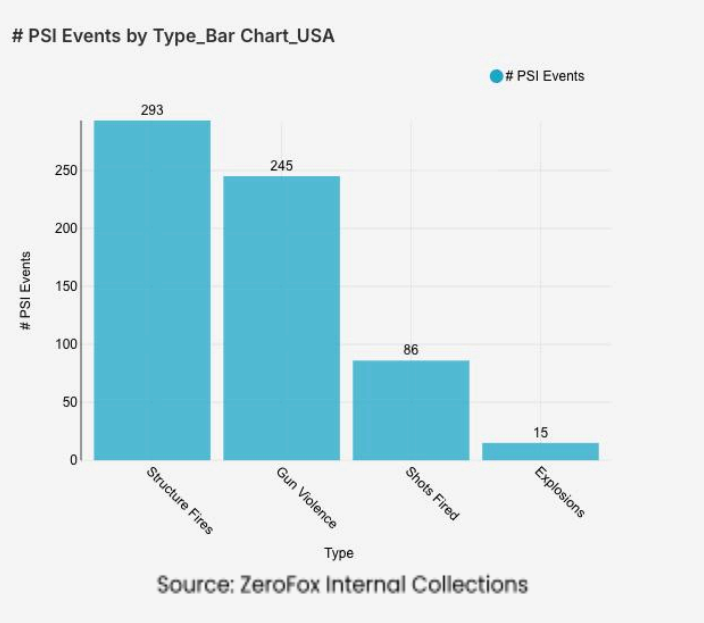


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 6 percent increase in mass casualty events this week from the previous week, with the top contributing countries or territories being Lebanon, the Palestinian territories, and Mexico (in that order). Approximately 66 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 27 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict decreased by 19 percent from the previous week, and alerts related to the war in Iran decreased by 29 percent. Events related to Russia's war in Ukraine decreased by 80 percent. The top three most-alerted subtypes were structure fires, which saw a 15 percent increase from the previous week; gun violence, which increased by 3 percent; and explosions, which increased by 28 percent.

- **What this means:** Global mass casualty events rose slightly this week, with Lebanon, the Palestinian territories, and Mexico collectively driving roughly one-third of all such alerts, a pattern consistent with the intensifying conflicts across each region. In Lebanon, Hezbollah claimed responsibility for over 130 attacks on Israel Defense Forces (IDF) and targets in northern Israel between May 18–25 alone. Israeli forces also launched a fresh wave of airstrikes on Lebanon in late May, killing at least 20 people and wounding dozens more, with raids striking buildings in and around the city of Tyre overnight on May 22–23. In the Palestinian territories, the IDF conducted continued strikes in Gaza as recently as May 27 targeting Hamas operatives, reportedly with at least seven killed and 18 wounded in a single strike. Meanwhile, alerts related to Russia's war in Ukraine dropped significantly, likely tied to a notable shift on the battlefield: Russian forces saw a net loss of 38 square miles of Ukrainian territory within the last week—its largest weekly territorial loss of 2026. All of the aforementioned data reflects an overall threat environment shaped by conflict zones in which aerial and ground-based explosions remain the primary instrument of harm.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, gun violence, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, shots fired includes shootings with no victims, and structure fires are fires that affect man-made buildings. The top two states with the most gun violence alerts were California and Illinois, which together made up 23 percent of this week's nationwide total. Gun violence across the United States overall increased by 7 percent from the week prior. Shots fired alerts decreased by 12 percent, and the top contributing states were Illinois and Pennsylvania. Structure fires decreased by 5 percent, and the top two states for this subtype were California and New York.

- **What this means:** This past week's alert trends reflect an ongoing pattern of gun violence, fires, and opportunistic crime that continues to affect communities across the United States. Illinois—one of the top-contributing states for both gun violence and shots fired alerts—saw 38 people wounded in shootings across Chicago over Memorial Day Weekend, including mass shooting incidents in the Austin and Little Village neighborhoods. There were nine mass shootings across the country within the last week, which is consistent with typically higher crime rates during holiday weekends. On May 23, a gunman fired roughly three shots toward the White House in Washington, D.C., before Secret Service agents returned fire and fatally struck the suspect, with a nearby civilian also wounded in the exchange. Structure fires also drove significant alert volume this week, with New York accounting for some of the most severe incidents. Most notably, a fire and explosion at a Staten Island shipyard on May 22 killed one civilian and injured more than 30 firefighters and first responders, with preliminary findings indicating the blaze was sparked by the ignition of flammable paint vapors inside a confined metal structure. Taken together, this week's data reflects a broad and persistent public safety threat landscape across the United States, from increased firearm usage to industrial disasters.

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%