ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

November 8, 2025

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 (EST) on November 6, 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 Brief - Underground Economist: Volume 5, Issue 22

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

.

ZEROFOX®
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

278 Million Location Points Reveal EU Officials' Movements

What we know:

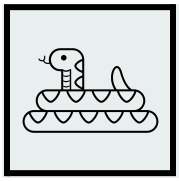
- Some European reporters have acquired a free sample from a commercial data broker containing 278 million location points from millions of Belgian mobile devices.
- This exposed data has reportedly made it "easy" to track top EU officials despite General Data Protection Regulation (GDPR) protections.

Background:

- GDPR is supposed to regulate how companies collect, store, and share personal data; mandate consent; and limit misuse. However, data brokers were still able to gather location data from apps on people's phones, package it, and distribute it commercially.
- Reporters reviewing the data found 2,000 location markers tied to 264 devices used around sensitive EU Commission areas and 5,800 markers linked to over 750 devices near the European Parliament.

What is next:

- This incident likely indicates that, despite GDPR protections, enforcement against data brokers remains limited, enabling perpetrators to compromise data.
- Criminals are likely to purchase such data, as it provides foreign intelligence that can be used to monitor diplomatic activity and exploit behavioral patterns, routines, and vulnerabilities to manipulate officials and conduct espionage.
- Affected individuals could face increased coercion, blackmail, and physical threats.



New Hacker Group UNK_SmudgedSerpent Linked to Iran Targeting U.S. Policy Experts

What we know:

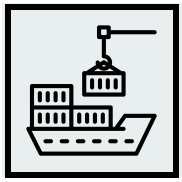
- A new Iran-linked threat activity cluster called UNK_SmudgedSerpent has been uncovered targeting Western academics and foreign policy experts between June and August 2025, coinciding with heightened geopolitical tensions between Iran and Israel.

Background:

- UNK_SmudgedSerpent impersonated prominent figures in Western foreign policy think tanks and used political lures, such as societal change in Iran, to phish over 20 Iran-focused U.S.-based think tank experts.
- Subsequently, they attempted to steal credentials or trick targets into installing legitimate remote monitoring and management (RMM) tools.

Analyst note:

- UNK_SmudgedSerpent's tactics closely resemble the activity of Iranian hacker groups such as Smoke Sandstorm, very likely indicating state-sponsored cyber espionage campaigns aimed at intelligence-gathering on foreign policy discussions.
- The activity also likely indicates growing collaboration between Iran's intelligence entities and cyber units.



Cyber Threat Actors Facilitating Physical Cargo Theft by Targeting Logistics Industry

What we know:

- Cybercriminals are collaborating with organized crime networks to steal cargo freight from trucking and logistics companies.
- The activity has been observed to be active since at least June 2025, with food and beverage products being the most targeted commodity.

Background:

- Threat actors reportedly use spear phishing emails to deploy legitimate RMM tools to infiltrate deeper into the corporate network.
- After gaining access, threat actors manipulate existing bookings and book loads under a compromised carrier's name to coordinate the physical theft of goods.

Analyst note:

- The activity very likely indicates that cybercriminals pose a physical risk to the surface transportation industry and interconnected supply chain providers.
- Threat actors are very likely to increasingly use other legitimate tools—such as RMM software—instead of malware to ensure obfuscation of activity.

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 nine industrial control systems (ICS) advisories on November 4 and November 6. CISA also added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog. Apple has rolled out updates for iOS, macOS, and other platforms, fixing over 100 security vulnerabilities. The Android November 2025 security update delivers patches for two flaws (CVE-2025-4859 and CVE-2025-48581), including a critical System component vulnerability that could enable remote code execution without user interaction. Hackers are exploiting a critical vulnerability (CVE-2025-11833) in the Post SMTP WordPress plugin to hijack administrator accounts. A recent security update from Microsoft addressing a flaw (CVE-2025-59287) in the Windows Server Update Services (WSUS) inadvertently disrupted hotpatching on some Windows Server 2025 systems. China-linked threat actors exploited a zero-day vulnerability (CVE-2025-61932) in Motex Lanscope Endpoint Manager to gain SYSTEM privileges and deploy the Gokcpdoor backdoor. Hackers are reportedly exploiting the critical CVE-2023-20198 flaw in unpatched Cisco IOS XE devices to deploy the "BadCandy" web shell. A China-linked hacking group is exploiting a Windows zero-day vulnerability (CVE-2025-9491) via malicious .LNK shortcut files to spy on European diplomatic targets. Researchers have disclosed four security bugs in Microsoft Teams that enabled attackers to impersonate colleagues, edit messages undetected, fake notifications, and caller IDs. Researchers have disclosed seven vulnerabilities in ChatGPT (including its GPT-4o and GPT-5 models) that enable attackers to trick AI into leaking private user data from chats and memory. CVE-2025-52665 is an improper authentication vulnerability in the Ubiquiti UniFi Access Application.

CRITICAL

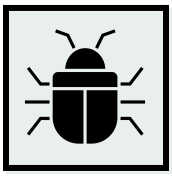
CVE-2025-5397

What happened: Hackers are exploiting a critical authentication bypass flaw in the JobMonster WordPress theme that allows them to log in as administrators without valid credentials if the site's social login feature is enabled. A patch has been released in version 4.8.2.

- **What this means:** The flaw enables attackers to gain full control over vulnerable job listing websites, modify content, inject malicious code, or create new admin users. This could lead to data theft, malware distribution, and potential compromise of hosting environments.

Unpatched sites face a high risk of takeover and further exploitation across connected systems.

- **Affected products:**
  - All versions of the theme up to 4.8.1



CRITICAL

CVE-2025-11953

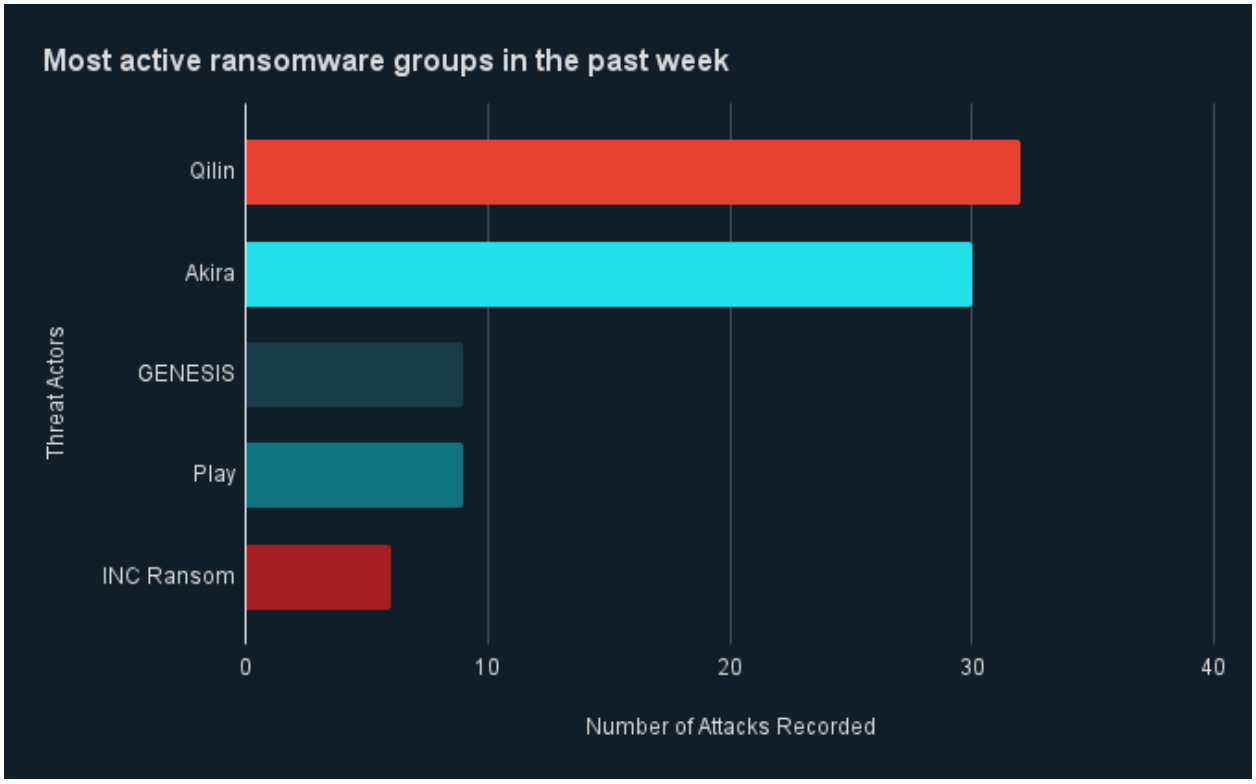
What happened: A critical flaw in the React Native Metro development server enables unauthenticated attackers to send crafted POST requests to the "/open-url" endpoint and execute arbitrary OS commands, with full impact on Windows and limited code execution on macOS and Linux. The development server binds to external interfaces by default, making it remotely exploitable rather than limited to local access.

- **What this means:** Attackers could remotely compromise developer machines, inject malicious code, or steal sensitive credentials and source files. Since development servers often run in shared or cloud environments, exploitation could also lead to tampered mobile app builds or lateral movement into continuous integration and continuous delivery (CI/CD) systems. This expands the threat surface beyond production systems to the development pipeline itself.
- **Affected products:**
  - @react-native-community/cli and @react-native-community/cli-server-api package, versions 4.8.0 to 20.0.0-alpha.2

Ransomware and Breach Intelligence

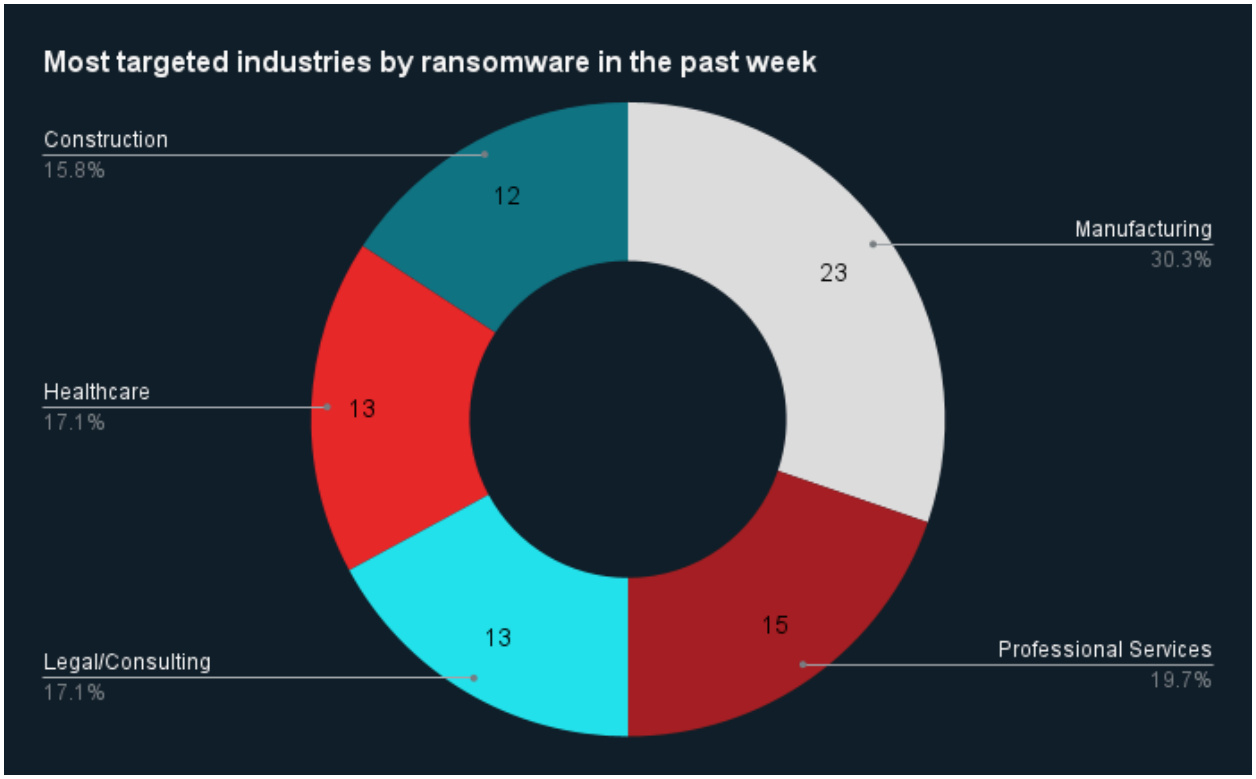
Ransomware and Breach Intelligence Key Findings

Ransomware Trends Observed This Week



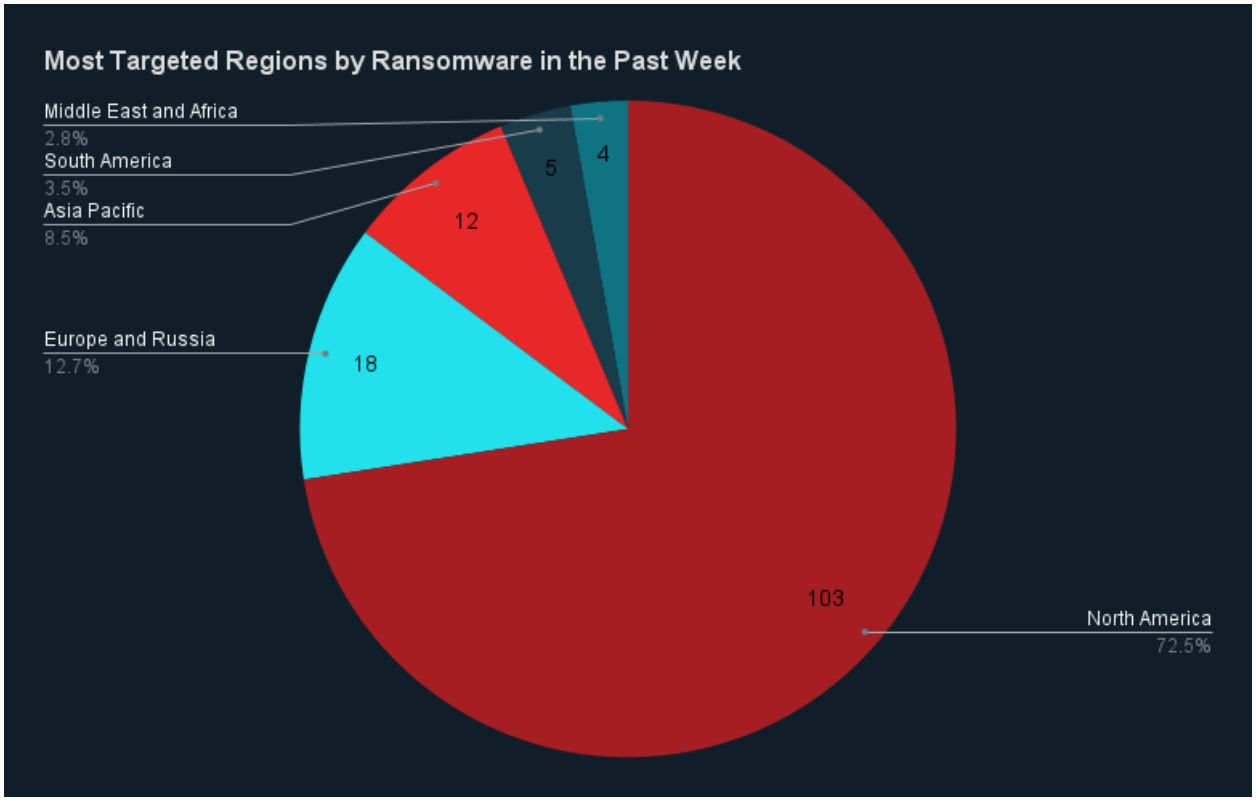
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Akira, GENESIS, Play, and INC Ransom were the most active ransomware groups. ZeroFox observed close to 133 ransomware victims disclosed, most of whom were located in North America. The Qilin ransomware group accounted for the largest number of attacks, followed by Akira.



Source: ZeroFox Internal Collections

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



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 103 ransomware attacks observed in North America, while Europe and Russia accounted for 18, Asia-Pacific (APAC) for 12, South America for five, and Middle East and Africa for four.

Recap of major ransomware events observed in the past week: The Apache Software Foundation has denied reports of an Akira ransomware attack on its OpenOffice project despite hackers claiming to have stolen 23 GB of data. Three former employees of cybersecurity firms DigitalMint and Sygnia were indicted for allegedly conducting BlackCat (ALPHV) ransomware attacks on five U.S. companies between May and November 2023. A free decryptor for the Midnight ransomware strain is now available, after researchers discovered a major vulnerability in its code that enables victims of the ransomware to restore affected files without paying the ransom.

Significant Data Breaches Reported This Week

Targeted Entity	Nikkei	Oglethorpe, Inc.	SOAS University of London
Compromised Entities/victims	17,368 employees and business partners	92,332 patients	N/A
Compromised Data Fields	Names, email addresses, and chat histories on the Slack messaging platform	First and last names, birth dates, Social Security numbers (SSNs), driver's license numbers, and medical information	Database containing login, password, email addresses, and other user information
Suspected Threat Actor	N/A	N/A	Exploit user BIG-BROTHER
Country/Region	Japan	United States	United Kingdom
Industry	Media/Entertainment	Healthcare	Education
Possible Repercussions	Extortion attempts in exchange for not exposing or selling confidential business information. Exposed individuals could be targeted by phishing and social engineering attacks	Blackmail, phishing, and social engineering attacks. Targeted individuals are likely to be especially vulnerable due to their mental health and addiction issues.	Account takeover, data theft, tampering of digital records, and operational disruptions

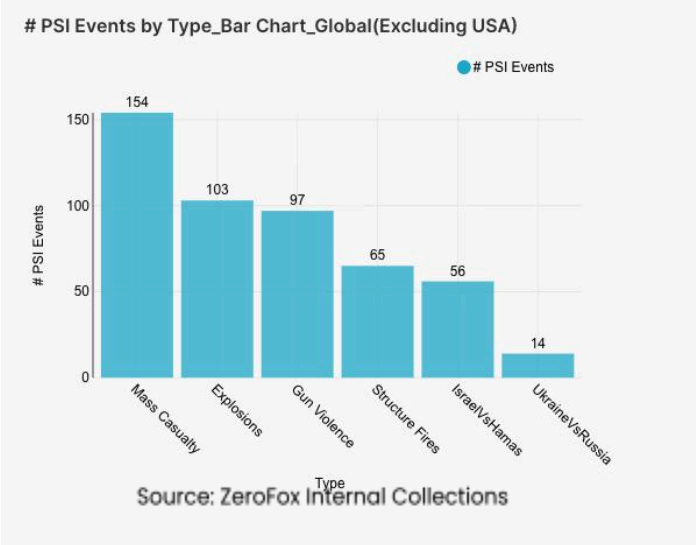
Three major breaches observed in the past week

Other major data breaches observed in the past week: A threat actor has claimed responsibility for breaching the University of Pennsylvania's systems in late October 2025, which allegedly compromised the data of 1.2 million donors, students, and alumni. The Swedish Authority for Privacy Protection is investigating a cyberattack on IT systems supplier Miljödata that exposed sensitive data of 1.5 million people on the darknet. Hyundai AutoEver America (HAEA) disclosed a data breach that has exposed sensitive personal data, including names, SSNs, and driver's license

details of unknown victims. An external software developer working for the Australian government accidentally exposed private government documents online; the incident has been classified as a Notifiable Data Breach due to its potential to cause serious harm to Australians.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

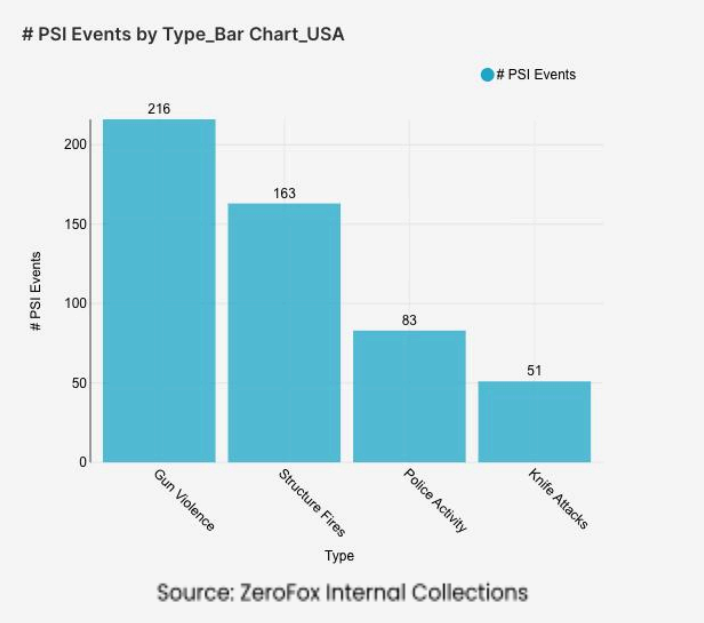


Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 1 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being India, Pakistan, and Mexico, in that order. Approximately 67 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 24 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including raids and attacks) decreased by 8 percent from the previous week. Events related to Russia's war in Ukraine increased by 250 percent. The top three most-alerted subtypes were explosions, which saw a 3 percent decrease from the previous week; gun violence, which increased by 10 percent; and structure fires, which increased by 7 percent.

- **What this means:** Despite a slight overall decrease in mass casualty events, activity remains highly concentrated in certain hot spots this week. The most significant shift in conflict reporting was the spike in events related to Russia's war in Ukraine, exemplified by recent major Russian missile strikes targeting Ukrainian military and infrastructure. For instance, a reported strike on a Ukrainian military award ceremony on November 1 has since sparked an official negligence probe and resulted in several casualties. Finally, gun violence showed an increase as well, with the Palestinian Territories being the highest contributor to these numbers despite the ceasefire; for instance, on November 3, Israeli forces killed two Palestinians and detained at least 15 using live ammunition against militants and demonstrators. Overall, global physical security this week is defined by a fractured threat landscape, marked by a surge in conflict intensity.

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 with the most gun violence alerts were Illinois and Ohio, which together made up 23 percent of this week's nationwide total. Gun violence across the United States overall increased by 2 percent from the week prior. Police activity alerts decreased by 8 percent, and the top contributing states were California and Texas. Structure fires decreased by 5 percent, and the top two states for this subtype were New York and California. Notably, knife attacks increased by 31 percent from the week prior.

- **What this means:** The domestic physical security environment this week stayed mostly within its typical range, with the exception of an uptick in knife attacks. For instance, a suspect armed with a knife and screwdriver broke into a home in Murrieta, California, killing a man and hospitalizing a woman on November 5. Meanwhile, while the number of alerts concerning structure fires decreased somewhat, California and New York remained the most active states in this category. For instance, there was a major emergency commercial fire in the Fashion District of downtown Los Angeles on November 3 that required over 100 firefighters to contain. Despite only a slight increase in overall gun violence alerts, there were 12 mass shootings within the last seven days across the country, with six of these occurring on November 2; for example, a shooting at a party in Bath Township, Ohio, on November 2 resulted in nine injured. Overall, the domestic security environment remains highly strained by persistent gun violence and a sharp rise in close-quarters attacks, requiring sustained law enforcement presence across key urban centers.

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%