ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

October 4, 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 (EDT) on October 2, 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

Monthly Geopolitical Assessment: October 2025

Although Israeli Prime Minister Benjamin Netanyahu accepted a U.S.-backed, 20-point plan for ending the Israel-Hamas war, it remains unlikely that this development will lead to an end to the fighting in the near term. Russia's military activities in Ukraine will likely continue spilling over into NATO territory. Therefore, European leaders are increasingly discussing seizing Russian assets and more direct military engagement against Russia, which has threatened all-out war if they do so. Following Indonesia's protests and Nepal's "Generation Z" (Gen Z) uprising, protest movements around the world have aligned with these causes. Madagascar's government has since fallen, and further bouts of Gen Z protests are very likely across the globe. U.S. President Donald Trump confirmed that he and Chinese President Xi Jinping will meet on the sidelines of the 2025 Asia-Pacific Economic Cooperation (APEC) Economic Leaders' Meeting at the end of October. Some breakthroughs on bilateral issues like tariffs and TikTok are likely, but a complete resolution to trade issues is very unlikely. Elements from China's 2026-2030 Five-Year Plan released in October are more likely to dictate relations between the two countries. Key emerging markets in Latin America and Africa are due to hold elections in October.

ZeroFox Intelligence Brief: Increasing Violations of NATO Airspace Threaten Wider War

Over the past several weeks, NATO allies have reported an increase in Russian violations of their airspace, as well as suspicious Russian flight patterns in international territory close to Allied states. The majority of these incidents took place in the Baltic region. The airspace violations likely serve as reconnaissance missions (probing NATO defenses) and signal the possibility of direct conflict with Russia. NATO held emergency consultations under Article 4 twice in September and began work to integrate NATO air and ground defenses in eastern states that border Russia. European leaders have also increasingly discussed seizing Russian assets and possibly directing military support to Ukraine. Russian leaders have denied responsibility for any airspace violations and have warned NATO that asset seizures or direct military aid to Ukraine would constitute an act of war.

ZeroFox Intelligence Flash Report - Threat Collective Touts Red Hat Breach

On October 1, 2025, the threat collective known as "Crimson Collective" claimed via their Telegram channel to have breached Red Hat's private GitHub repositories, allegedly stealing around 570 GB of

data from nearly 28,000 internal repositories and approximately 800 Consulting Engagement Reports (CERs). Crimson Collective is an extortion threat collective that created their Telegram channel on September 24, 2025, amassing 393 subscribers as of the writing of this report. Crimson Collective posted screenshots of an alleged attempt to contact Red Hat regarding the incident, along with a file named git[.]tar[.]gz they assert represents only half of the total breached data—which they likely intend to release once the files have been compressed. Exposure of internal repositories will very likely reveal proprietary code and security controls across Red Hat's products and services, which would almost certainly enable threat actors to identify further exploitable weaknesses.

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

FIN11 Suspected of Being Behind Emails Claiming Oracle E-Business Suite Data Theft

What we know:

- Executives at multiple companies have reportedly received emails claiming their data from Oracle E-Business Suite systems was stolen.
- The extortion emails were sent from a large number of compromised email accounts with at least one account associated with financially-motivated threat actor FIN11.
- Associated email addresses have reportedly also appeared on Cl0p ransomware's data leak site, suggesting a potential connection.

Background:

- The extortion campaign reportedly began around September 29, 2025.
- The potential stolen data includes financial, operational, and business information stored within affected Oracle environments.

What is next:

- FIN11 likely has access to less sensitive information, such as names, job titles, or publicly available corporate details, but is threatening executives in order to coerce ransom payments.
- Investigations are still underway to determine if any real data theft occurred. It is likely this exfiltrated data was acquired through an old data breach.

Fake North Korean IT Workers Expand Targeting Beyond Tech Sector

What we know:

- Fake North Korean IT workers have been observed targeting companies beyond the tech sector in multiple different countries in order to funnel money back to Pyongyang.

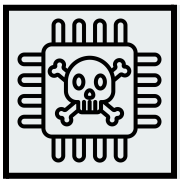
Background:

- The scammers are now targeting Big Tech and artificial intelligence (AI) firms for sensitive intellectual property (IP) and algorithms, as well as seeking roles in healthcare and med-tech to access personally identifiable information (PII) and medical data.

- They have also been pursuing positions in finance, banking, fintech, and crypto, including back-office roles, in order to exploit financial data and revenue streams.

Analyst note:

- This expansion likely suggests these threat actors are targeting both intellectual property and high-value data.
- Healthcare and med-tech roles provide access to PII, medical records, and hospital workflows, while public administration positions offer insights into government operations and policy, extending their intelligence value beyond software IP.



Japan's Brewer, Asahi, Suspends Operations Due to Cyberattack

What we know:

- Japan's major brewer, Asahi Group Holdings, has suspended its ordering and shipping operations due to a cyberattack.
- Call center operations, including customer service desks, are also suspended.

Background:

- The company, which operates globally, said the cyberattack has affected only its operations in Japan.
- Investigations are underway, but no threat actor has claimed responsibility for the incident yet.

Analyst note:

- The disruption to ordering and shipping operations suggests that customer data and order details are likely among the data that has been compromised.
- In the event this is a ransomware attack, it is likely that Asahi will not be able to access necessary data due to encryption.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

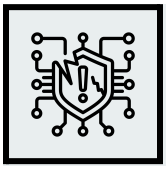
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) added 10 vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on September 29, 2025 and October 2. CISA also added 12 Industrial Control Systems (ICS) advisories on September 30 and October 2. A vulnerability in the Red Hat OpenShift AI service has been disclosed that can enable attackers to escalate privileges and take control of the complete infrastructure. NVIDIA released a patch for a vulnerability affecting the FrameviewSDK installation process, which enabled an attacker with local unprivileged access to modify files in the Frameview SDK directory. Under certain circumstances, a high-severity flaw in the One Identity OneLogin Identity and Access Management (IAM) solution could expose sensitive data stored in the OpenID Connect (OIDC) application. An SQL injection flaw in Project Monitoring System 1.0's /login[.]php (username/password parameter) enables an attacker to inject SQL remotely via the authentication input. The OpenSSL Project has patched three vulnerabilities in its latest versions of the open source SSL/TLS toolkit, including CVE-2025-9231, which could enable an attacker to recover the private key. Adobe fixed an ingestion flaw in its Analytics Edge data collection system, which caused data from certain organizations to appear in the reports of others for approximately one day.

HIGH

CVE-2025-43400

What happened: Apple has released an out-of-bounds patch for a vulnerability affecting the font parser in multiple products.

- **What this means:** The flaw can result in app termination or corrupt process memory due to a malicious font. While exploitation has not yet been observed in the wild, a successful attack is likely to result in operational disruption in the targeted device.
- **Affected products:**
  - The affected products are listed in this advisory.



HIGH

CVE-2025-41244

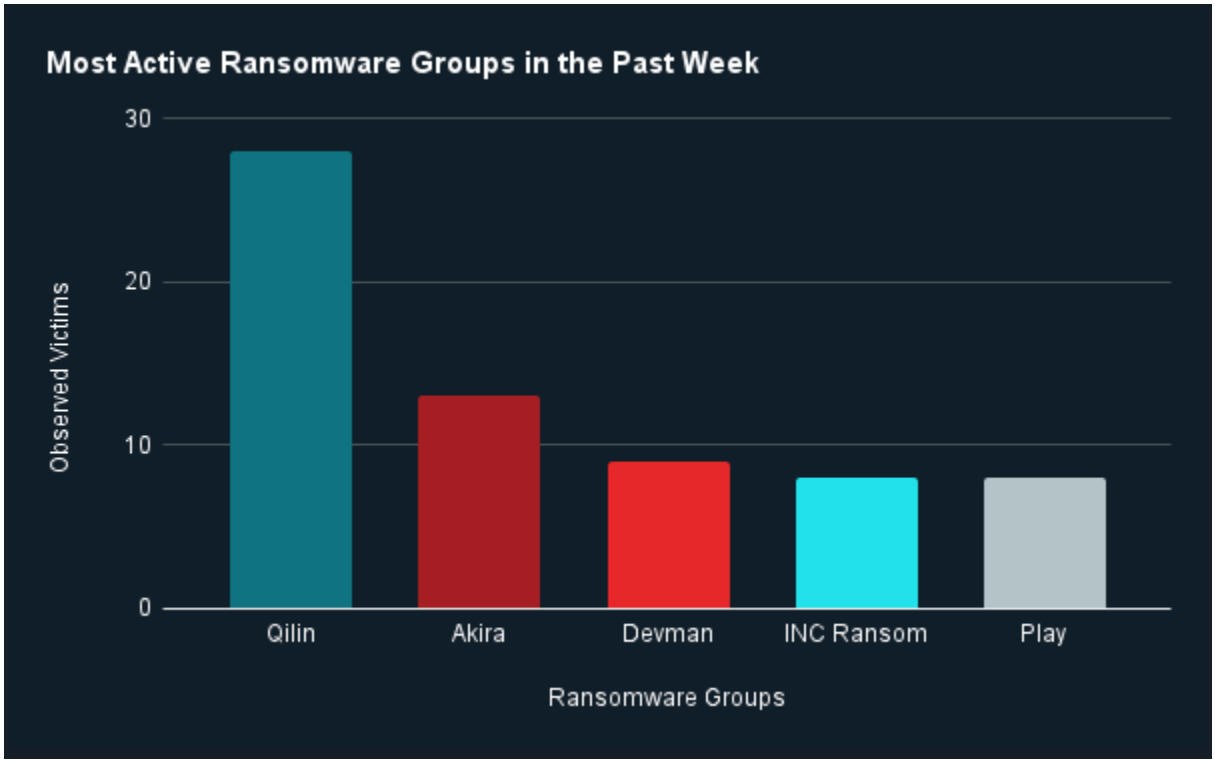
What happened: Broadcom has patched a high-severity vulnerability that Chinese hackers have reportedly been exploiting in zero-day attacks since October 2024.

- **What this means:** Threat actors are likely to exploit this local privilege escalation bug to gain complete system control, exfiltrate data, compromise infrastructure, and disrupt services. Unpatched systems are likely to be targeted in Chinese state-associated operations.
- **Affected products:**
  - VMware Aria Operations and VMware Tools

Ransomware and Breach Intelligence

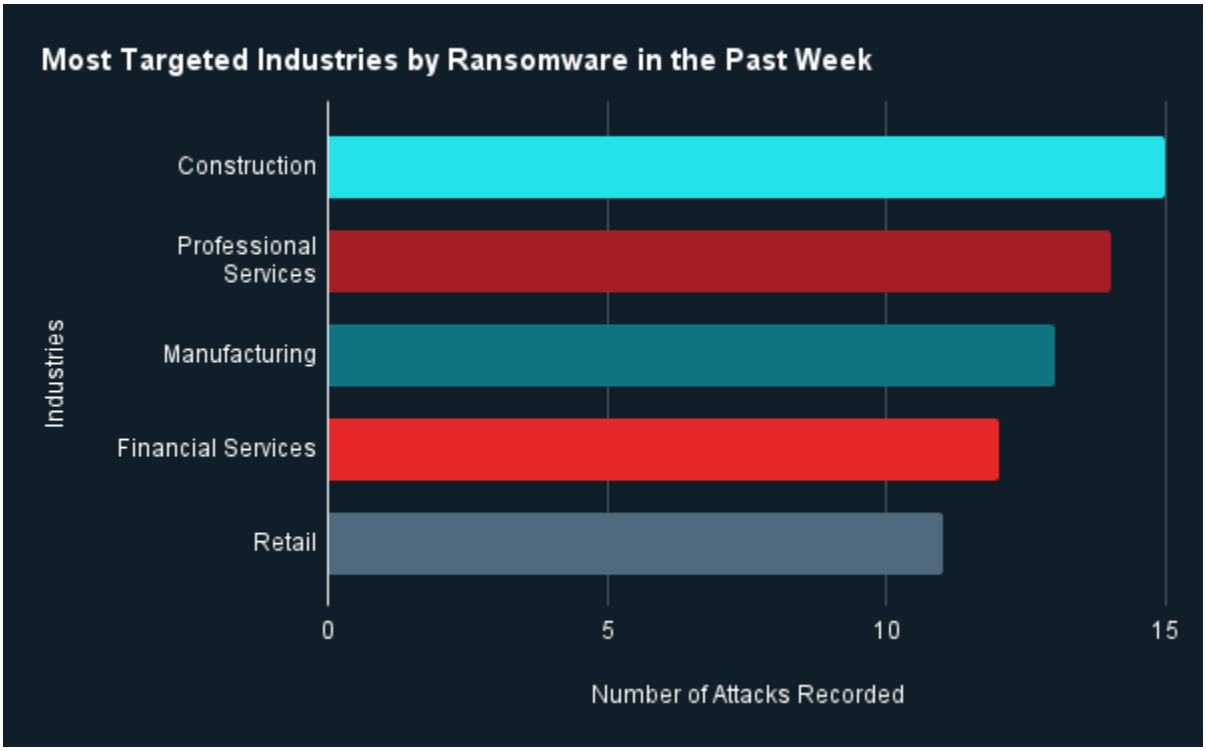
Ransomware and Breach Intelligence Key Findings

Ransomware Groups and Trends



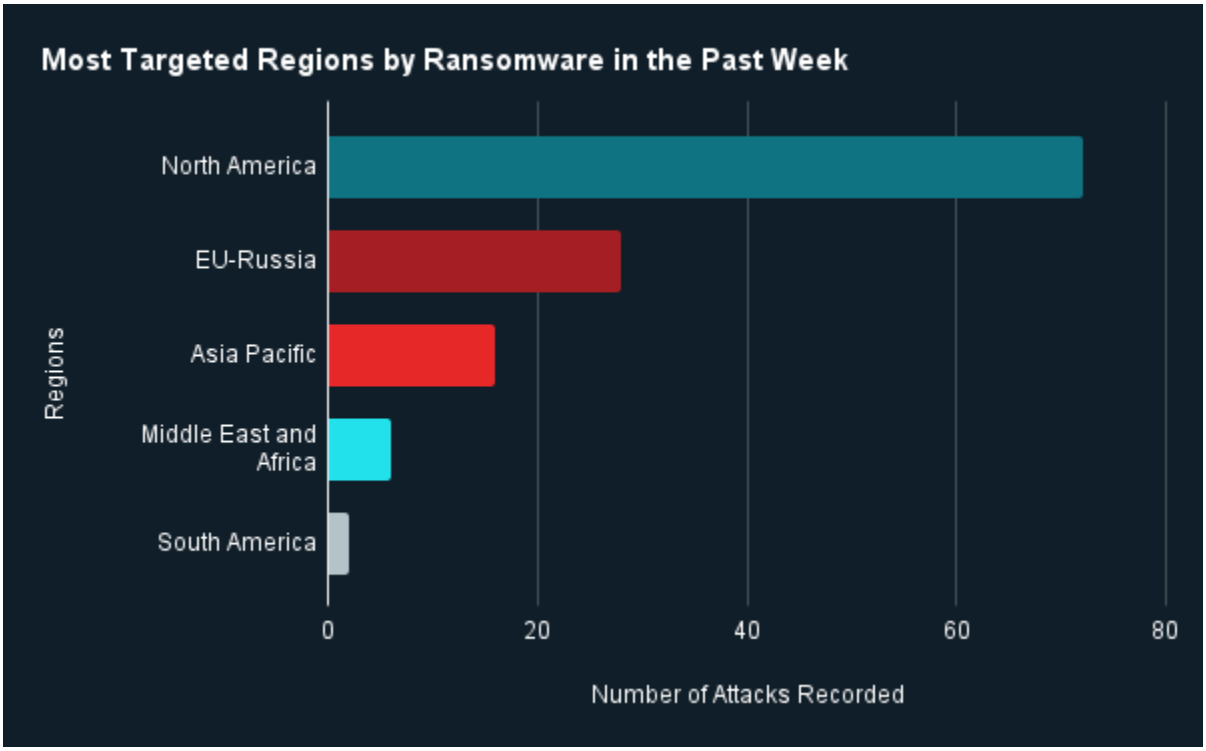
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, Qilin, Akira, Devman, INC Ransom, and Play were the most active ransomware groups. ZeroFox observed close to 113 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 construction was the most targeted industry 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 EU-Russia. There were at least 72 ransomware attacks observed in North America, while Europe and Russia accounted for 28, Asia Pacific (APAC) for 16, Middle East and Africa for six, and South America for two.

Data Breaches Affecting Multiple Industries

Targeted Entity	WestJet	Veradigm	ClaimPix
Compromised Entities/victims	1.2 million WestJet customers	70,000 Veradigm healthcare customers in Texas and South Carolina so far	Undisclosed number of ClaimPix customers
Compromised Data Fields	PII, including passports and ID documents, filed complaints, WestJet Rewards Member ID, points, WestJet RBC Mastercard, and other details	PII, including names and contact information, dates of birth, health records (diagnoses, medications, test results, and treatments), health insurance details, payment information, and Social Security Numbers (SSNs)	About 16,000 Powers of Attorney (POA) documents with electronic signatures and IP addresses, names, addresses, phone numbers, emails, vehicle registrations, VINs, license plates, and internal company files
Suspected Threat Actor	Unknown	Unknown	Unknown
Country/Region	Canada	United States	United States
Industry	Airlines	Healthcare	Insurance
Possible Repercussions	Identity theft and fraud, travel security risks, loyalty program abuse, and phishing and other social engineering attacks	Identity theft, fraud, medical identity theft, operational disruption, and phishing and other social engineering attacks	Identity theft, impersonation, and vehicle and insurance fraud

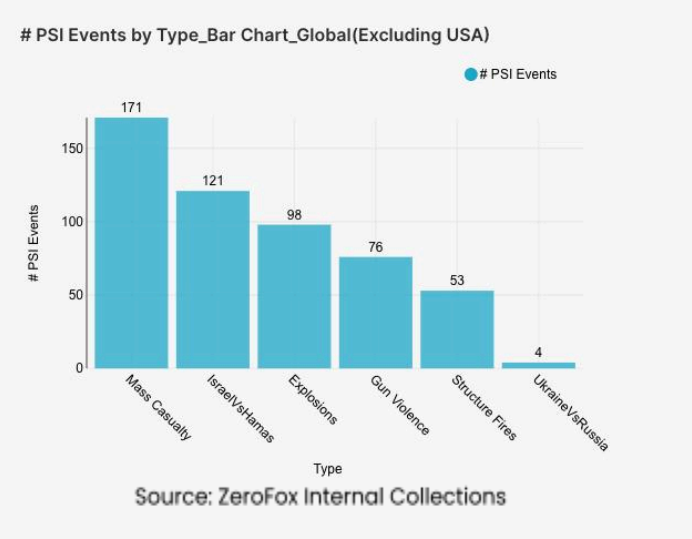
Three major breaches observed in the past week

Other major data breaches observed in the past week: A new extortion campaign—possibly linked to FIN11 and Cl0p ransomware—targeting Oracle E-Business Suite (EBS) customers has

emerged, with emails sent from compromised accounts alleging data theft and demanding up to USD 50 million in ransom. A threat actor has reportedly breached RemoteCOM, a U.S.-based provider of monitoring services for pretrial, probation, and parole clients. The leaked information allegedly includes personal details of nearly 14,000 monitored clients and records of almost 6,900 criminal justice employees across 49 U.S. states.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

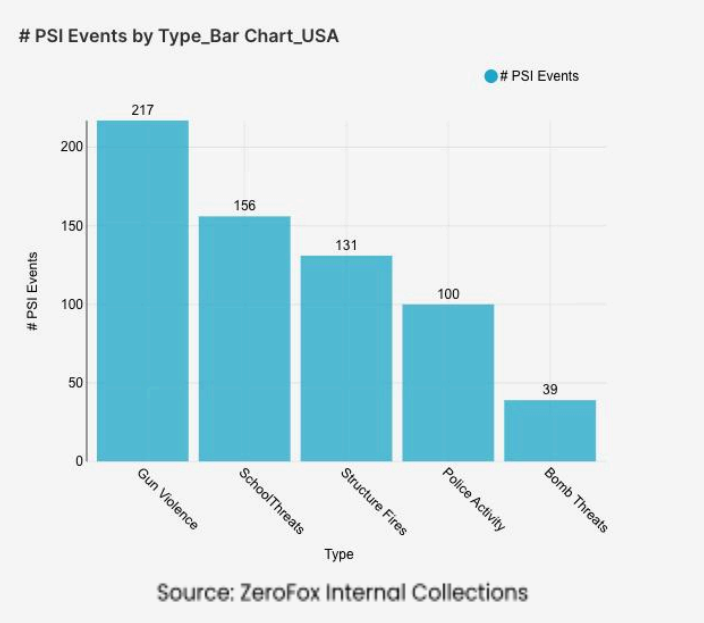


Physical Security Intelligence: Global

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 or territories being the Palestinian territories, India, and Pakistan, in that order. Approximately 57 percent of these events were explosions, and the three aforementioned territories and countries accounted for about 42 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 42 percent from the previous week. Events related to Russia's war in Ukraine decreased by 43 percent. The top three most-alerted subtypes were explosions, which saw an 11 percent increase from the previous week; gun violence, which increased by 43 percent; and structure fires, which did not increase or decrease from the week prior. Global protest activity increased by 19 percent.

- **What this means:** This week, mass casualty events and explosions saw a significant increase, with violence heavily concentrated in the Middle East and South Asia. This was particularly pronounced amid Israel's intensified offensive in Gaza City, which included strikes on a school sheltering displaced persons that killed at least 13 Palestinians overnight into October 2. Additionally, this week saw widespread protests after Israel intercepted and detained activists on the Global Sumud Flotilla near Gaza on October 1, with demonstrations erupting in cities that included Rome, Athens, Buenos Aires, and Berlin; the protesters condemned Israel's actions and demanded the activists' release. Meanwhile, both India and Pakistan remain high-alert zones due to ongoing terrorist activity. For example, Pakistan is grappling with a severe domestic security crisis after a September 30t suicide bombing that killed at least 10 people and wounded more than 30 others in Quetta was linked to Tehreek-e-Taliban Pakistan. These incidents confirm the volatile nature of global physical security, driven by escalating violence and terrorism.

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 Illinois and Ohio, which together made up 21 percent of this week's nationwide total. Gun violence across the United States overall increased by 9 percent from the week prior. Police activity alerts increased by 22 percent, and the top contributing states were California and Illinois. Structure fires decreased by 18 percent, and the top two states for this subtype were California and New York. Notably, threats related to schools (not including protest activity) increased by 53 percent, and bomb threats increased by 225 percent.

- **What this means:** The domestic U.S. security landscape this week is defined by escalating threats to public safety and a surge in targeted disruption, with sharp increases in both school-related activity and bomb threats that often overlap. For instance, there was a recent bomb threat that forced an evacuation at Prairie View A&M University in Texas on September 30, as well as a lockdown and evacuation at Monroe County Community College in Michigan, also due to a bomb threat that same day. There were 10 mass shootings (shootings with four or more victims) within the last week. These included a shooting at a bar in Southport, North Carolina, that resulted in 11 victims and a mass shooting and arson attack at the Church of Jesus Christ of Latter-day Saints in Grand Blanc, Michigan, that resulted in 12 victims. Both premeditated shootings were carried out by military veterans, whose significant mental health changes after overseas service highlight the urgent need for improved post-traumatic stress disorder (PTSD) treatment for veterans. The rise in targeted threats overall confirms a distinct and escalating crisis in domestic 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%