ZEROFOX®

Weekly Intelligence Brief

Classification: TLP:GREEN

August 2, 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 July 31, 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 Assessment - Q2 2025 Ransomware Wrap-up

ZeroFox observed at least 1,366 separate ransomware and digital extortion (R&DE) incidents during Q2 2025, which is a drop of approximately 30 percent from the record-breaking 1,961 incidents observed during the first quarter of the year. North America-based organizations were the most targeted by a substantial margin, accounting for approximately 57 percent of all incidents. This is consistent with the 58 percent average observed throughout 2024 and a slight decrease from the 66 percent observed in Q1 2025. During Q2 2025, organizations in the manufacturing industry were targeted by more R&DE incidents than those in other industries, experiencing a total of at least 33 attacks. Approximately 19 percent of all R&DE incidents targeted entities in the manufacturing industry during Q2 2025, a slight decrease from the approximately 21 percent observed during Q1 2025. The five most active R&DE collectives ZeroFox observed during Q2 2025 were almost certainly Qilin, Play, Akira, SafePay, and INC Ransom. This is a notably different picture from the first quarter of 2025; only two (Qilin and Akira) of those same five collectives appear on both lists.

ZEROFOX
Weekly Intelligence Brief

Cyber and Dark Web Intelligence

Cyber and Dark Web Intelligence Key Findings

BreachForums Original Onion Address Seemingly Functional Again

What we know:

- ZeroFox has observed that dark web forum BreachForums (BF) has resurfaced on its original [.]onion domain after a long period of inactivity.
- BF has also returned on clearnet with a new domain (breachforums[.]hn).
- The dark web site has resurfaced with fully restored infrastructure and retains all the old leaked databases, breach listings, and forum posts.

Background:

- The administrators behind the relaunch claimed in a post that they voluntarily took the site offline due to a now-patched MyBB zero-day vulnerability.
- The admins of the forum also clarified that threat actor IntelBroker, arrested in late June 2025, was not an administrator of the forum and was a ploy to "divert attention" from the actual admins.
- The development comes on the heels of the Russian language dark web forum xss, being seized by law enforcement following the arrest of a suspected administrator in Ukraine.
- Moreover, domain registration details for both xss and BF were reportedly the same, including email, physical address, and contact details.

What is next:

- The reinstated BF domain is likely to be a law enforcement honeypot to track and trap other administrators of the forum and prominent threat actors.
- BF's return is likely linked to the law enforcement seizure of xss.
- Threat actors from xss are likely to be migrating to the newly reinstated BF.

Russian Airline Aeroflot Cancels Flights Following Cyberattack

What we know:

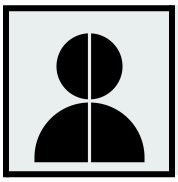
- Russia's national airline Aeroflot has been hit by a cyberattack, forcing it to cancel and delay several flights. Pro-Ukrainian hacker groups Silent Crow and Cyber Partisans—the latter of which is based out of Belarus—have claimed responsibility for the attack.

Background:

- An investigation is underway and Aeroflot has reportedly not ruled out the involvement of adversarial nations. It has canceled over 40 flights across the country, as well as to the Belarusian capital Minsk and the Armenian capital Yerevan.

Analyst note:

- The incident is very likely to spark a wave of cyberattacks by Russian hackers targeting Ukrainian, European, and American entities. Investigations are likely to lead to cross-border arrests of the responsible parties behind the attack.



FBI Warns of Rising Impersonation Scams

What we know:

- The Federal Bureau of Investigation (FBI) is warning of a surge in government impersonation phone scams across New England, United States. Scammers spoof caller IDs and pose as law enforcement to extort money or steal personal information.

Background:

- Scammers threaten victims with arrest and seizures unless they pay through prepaid cards, wire transfers, or cryptocurrency. These scams can also occur through email and include poor grammar and fake official imagery to appear legitimate.

Analyst note:

- As scammers threaten victims with arrests and asset seizure, victims are likely to feel increased pressure to comply with their demands. Additionally, the personal information stolen during these scams will likely be sold on carding forums and dark web marketplaces, which could result in identity theft, financial fraud, and further scams.

Exploit and Vulnerability Intelligence

Exploit and Vulnerability Intelligence Key Findings

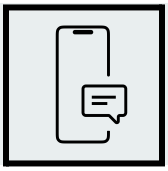
In the past week, ZeroFox observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) issued 11 industrial control system (ICS) advisories on July 24 and July 29, 2025. CISA also added three vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on July 28, 2025, including two Cisco Identity Services Engine Injection vulnerabilities. Researchers have uncovered several vulnerabilities in Tridium's Niagara Framework, a building automation platform. The most critical bugs enable privilege escalation, command injection, and unauthorized access, each rated CVSS 9.8. Vulnerabilities in Dahua smart camera firmware (CVE-2025-31700 and CVE-2025-31701) enable unauthenticated remote code execution via malicious ONVIF or file upload requests. CVE-2025-5394 is an unauthenticated arbitrary file upload flaw in the WordPress theme "Alone" that enables threat actors to execute code remotely and carry out complete site takeover. Apple has patched eight vulnerabilities across its products, including flaws that could expose passcodes via VoiceOver and lead to changes in restricted network settings.

CRITICAL

CVE-2025-40599

What happened: SonicWall has urged customers to patch a vulnerability in SMA 100 series appliances that enables authenticated attackers to upload arbitrary files and achieve remote code execution.

- **What this means:** As of this writing, threat actors are targeting affected devices using stolen credentials. If left unpatched, threat actors could upload malicious files, execute arbitrary code, and compromise systems.
- **Affected products:**
  - MA 100 Series (SMA 210, 410, 500v) 10.2.1.15-81sv and earlier versions



CRITICAL

CVE-2025-31324

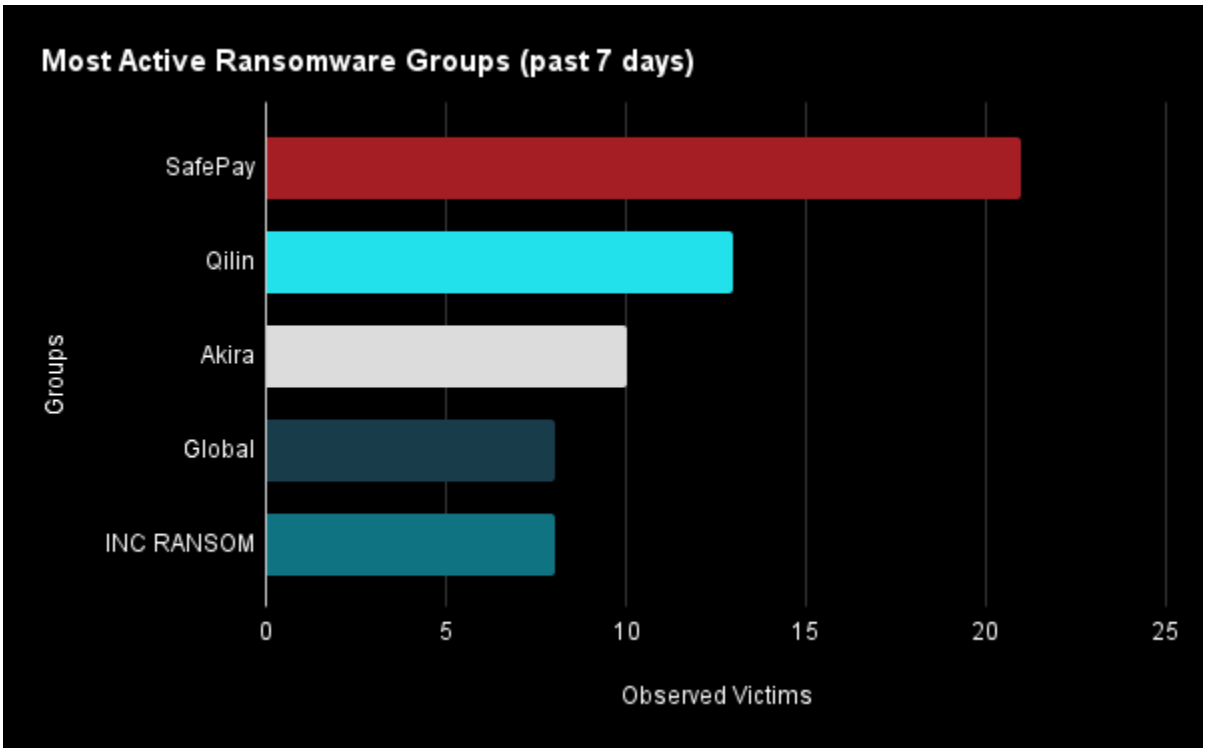
What happened: Threat actors have exploited CVE-2025-31324, a SAP NetWeaver flaw, to deploy the advanced Auto-Color Linux malware in an attack on a chemicals company.

- **What this means:** The malware enables remote code execution and uses stealthy persistence techniques, including rootkit functionality. Threat actors could maintain long-term access on affected devices, execute arbitrary commands, and exfiltrate data.
- **Affected products:**
  - VCFRAMEWORK 7.50

Ransomware and Breach Intelligence

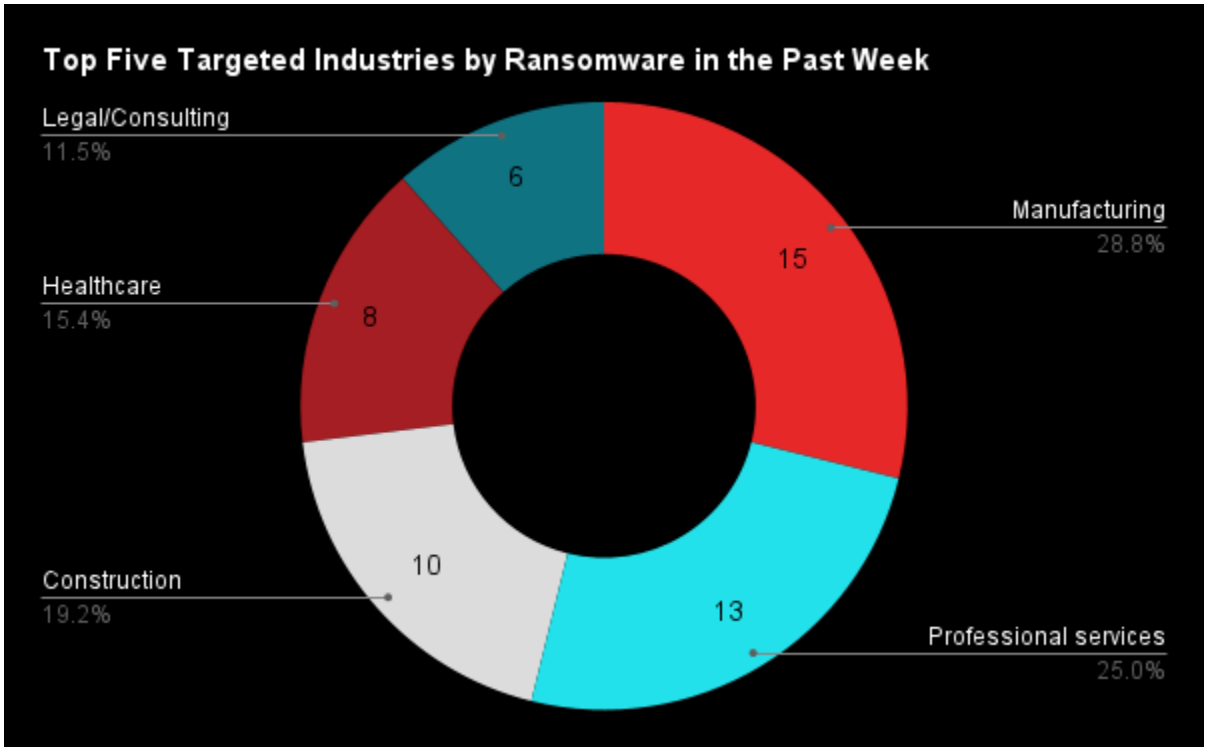
Ransomware and Breach Intelligence Key Findings

Ransomware Developments in the Past Week



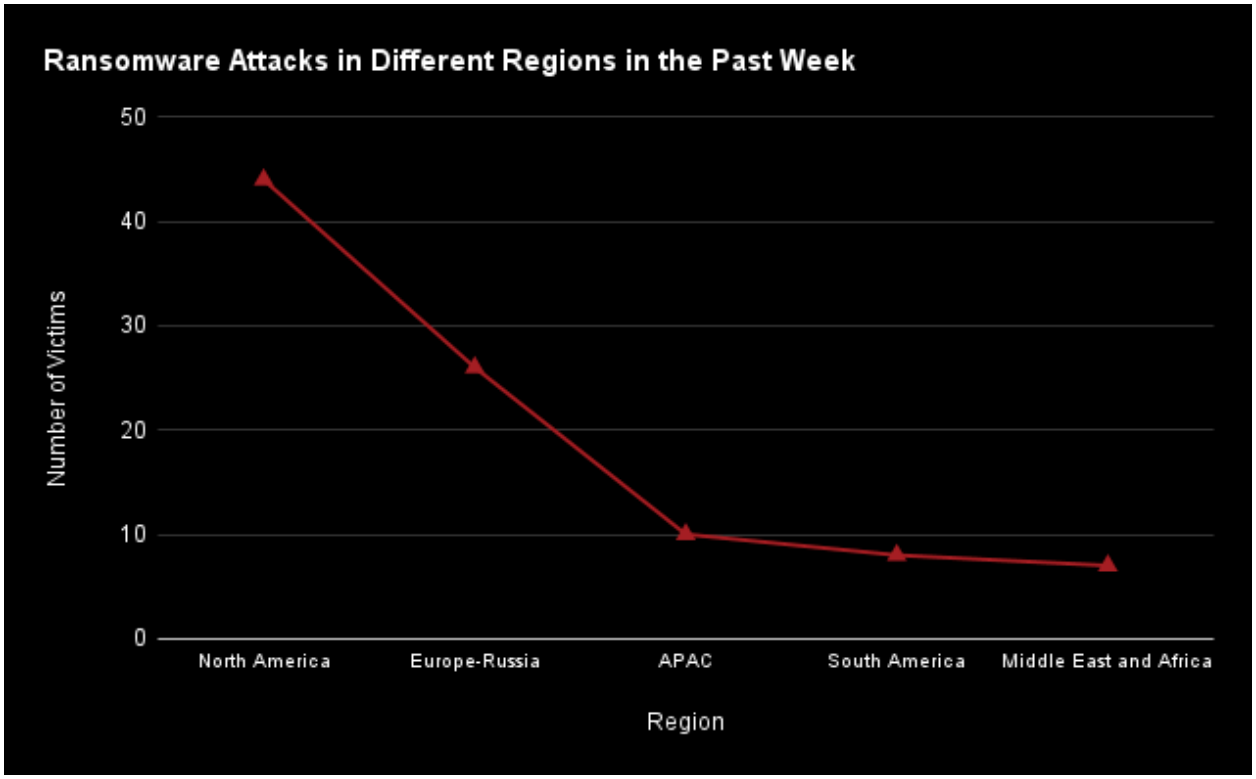
Source: ZeroFox Internal Collections

Last week in ransomware: In the past week, SafePay, Qilin, Akira, Global, and INC RANSOM were the most active ransomware groups. ZeroFox observed at least 88 ransomware victims disclosed, most of whom were located in North America. The SafePay ransomware group accounted for the largest number of attacks followed by Qilin.



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, construction, healthcare, and legal/consulting 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-Russia. North America witnessed 44 ransomware attacks, while Europe-Russia accounted for 26, Asia-Pacific (APAC) for 10, South America for eight, and Middle East and Africa for seven.

Recap of major ransomware events observed in the past week: Medusa ransomware group has claimed responsibility for a March 2025 cyberattack on NASCAR, which led to the theft of sensitive data including names and Social Security numbers (SSNs). The group demanded a ransom of USD 4 million. The SafePay ransomware group is threatening to release 3.5TB of data allegedly stolen from IT giant Ingram Micro following a system breach earlier this month. BlackSuit ransomware group's domains have been seized in an international operation, called Operation Checkmate, which also involved a U.S. law enforcement agency. Additionally, the U.S. law enforcement seized approximately USD 2.4 million worth of cryptocurrency reportedly associated with a member, named "Hors," of the Chaos ransomware group in April. The Scattered Spider ransomware group has been targeting U.S. organizations by attacking VMware ESXi hypervisors.

Notable Data Breaches in the Past Week

Targeted Entity	Naval Group	Tea Dating Advice	Wood River Health
Compromised Entities/Data Set	1 TB of sensitive data	59 GB of data	54,926 individuals
Compromised Data Fields	Classified CMS for military vessels, technical documents, development VMs with simulation data, and internal communications	72,000 images—including 13,000 verification selfies and 59,000 public images from posts, comments and direct messages—and 1.1 million private messages	Names and SSNs
Suspected Threat Actor	Neferpitou	Yet to be determined	Yet to be determined
Country/Region	France	United States	United States
Industry	Defense	Technology	Healthcare
Possible Repercussions	Espionage and intelligence gathering, supply chain attacks, sabotage and disruption, blackmail, extortion, and more targeted attacks	Sextortion, blackmail, identity theft, impersonation, doxxing and harassment, social engineering and phishing attacks, credential stuffing, deepfakes, and stalking or surveillance	Identity theft, synthetic identity creation, phishing and social engineering attacks, and account hijacking

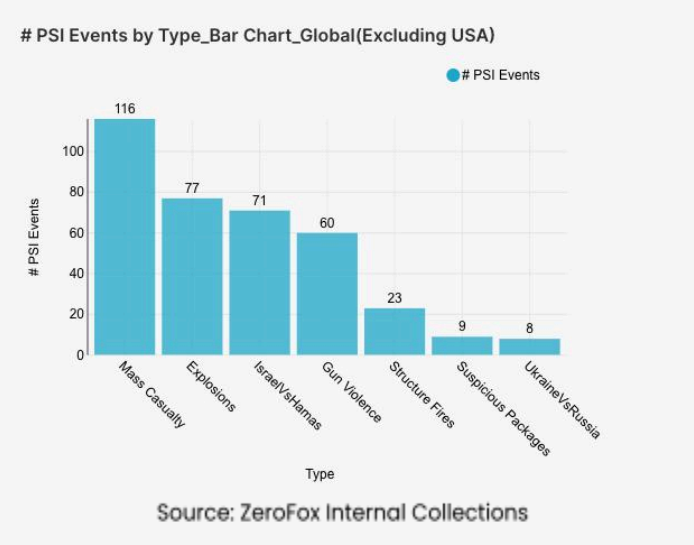
Three major breaches observed in the past week

Other major data breaches observed in the past week: A series of data breaches affecting companies such as Qantas, LVMH, and Adidas has been attributed to the ShinyHunters extortion group, which is leveraging voice phishing attacks to extract data from Salesforce CRM systems. Orange, a French telecommunications company, announced that it discovered a compromised system on its network late last week. Untested threat actor sultan2022 has advertised the sale of a

massive 18 billion-line mail:pass database on Russian language forum bhf[.]pro. The actor claimed the dataset was accumulated over three years from various sources, including logs, cloud breaches, and direct purchases.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings



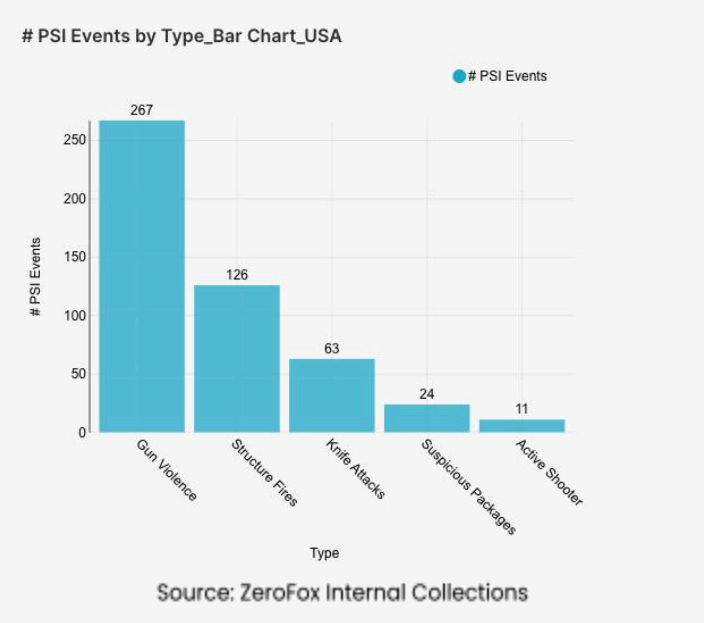
Source: ZeroFox Internal Collections

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 26 percent decrease in mass casualty events this week from the previous week, with the top contributing countries or territories being the Palestinian Territories, Syria, and Mexico in that order. Approximately 66 percent of these events were explosions, and the three aforementioned countries and territories accounted for about 37 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and attacks) increased by 6 percent from the previous week. Events related to Russia's war in Ukraine increased by 33 percent. The top three most-alerted subtypes were explosions, which saw a 19 percent decrease from the previous week; gun violence, which decreased by 24 percent; and structure fires, which decreased by 8 percent. Global protest activity increased by 61 percent. Notably, suspicious package incidents increased by 13 percent, and the United Kingdom accounted for 66 percent of these alerts.

- **What this means:** Despite an overall decrease in mass casualty events globally this week compared to the last, several ongoing conflicts continue to drive significant humanitarian crises and violence. For instance, recent days have seen continued Israeli attacks across Gaza; several Palestinians have been killed as the Israeli "tactical pause" to address the humanitarian situation has ended, and starvation has worsened. Protest activity surged as well; for example, on July 26, hundreds rallied in Santiago, Chile, protesting the famine in Gaza and urging their government to cut ties with Israel. Events related to Russia's war in Ukraine also saw a notable increase, with Russian forces launching recent attacks; on July 29, Russian bombs and missiles struck a Ukrainian prison and medical facility, killing at least 22 civilians across the country. Global suspicious package incidents rose, notably in the United Kingdom, including one at a Trump golf course in Aberdeenshire, Scotland, on July 29 during President Trump's visit, highlighting the progression from public discontent to tangible threats of violence.

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 knife attacks. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, structure fires are fires that affect man-made buildings, and knife attacks include confirmed stabbings or slashings. The top state that had the most gun violence alerts was Illinois, which made up 13 percent of this week's nationwide total. Gun violence across the United States overall showed no increase or decrease from the week prior. Knife attack alerts increased by 7 percent, and the top contributing states were California and Pennsylvania. Structure fires decreased by 7 percent, and the top two states for this subtype were New York and California. Notably, active shooter alerts increased by 267 percent, and suspicious packages increased by 26 percent.

- **What this means:** In the past week, domestic security concerns have seen notable shifts, particularly concerning violent incidents and suspicious activities. Active shooter alerts rose significantly; for instance, on July 28, a shooter killed four people, including an NYPD officer, at the NFL headquarters in Manhattan before dying by suicide. There have been 14 mass shootings in the United States since July 24, including one in Atlanta, Georgia, which saw 11 people shot. Knife attack alerts also increased; for instance, a man stabbed 11 people at a Walmart in Traverse City, Michigan, on July 27, leading to terrorism charges. Additionally, suspicious package incidents increased; for instance, a suspicious package was found near the White House in Washington, D.C. on July 28, prompting a lockdown and response from the bomb squad before it was deemed safe. The above examples collectively highlight an intensifying and evolving landscape of physical security threats in the United States, marked by a significant escalation in targeted violent acts like active shooter events and mass stabbings, alongside a persistent prevalence of gun violence.

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%