



**ZEROFOX<sup>®</sup>**

*Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**October 14, 2024**

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 9:00 AM (EDT) on October 11, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# | Weekly Intelligence Brief |

|                                                                                     |           |
|-------------------------------------------------------------------------------------|-----------|
| <b>  This Week's ZeroFox Intelligence Reports</b>                                   | <b>2</b>  |
| ZeroFox Intelligence Brief October 7 Anniversary Report                             | 2         |
| <b>  Cyber and Dark Web Intelligence Key Findings</b>                               | <b>4</b>  |
| U.S. Utility Company Forced to Take Systems Offline After Cyber Incident            | 4         |
| Salt Typhoon's Targeted Campaigns Against U.S. Entities                             | 4         |
| Pro-Palestine Hackers Target Israel and Pro-Israel Nations on October 7 Anniversary | 5         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                        | <b>8</b>  |
| CVE-2023-33246                                                                      | 8         |
| CVE-2024-9463                                                                       | 9         |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                            | <b>11</b> |
| Emerging Ransomware Threats Across Sectors                                          | 11        |
| Data Breaches and Nation-State Actors                                               | 12        |
| <b>  Physical and Geopolitical Intelligence Key Findings</b>                        | <b>15</b> |
| Physical Security Intelligence: Global                                              | 15        |
| Physical Security Intelligence: United States                                       | 16        |
| <b>  Appendix A: Traffic Light Protocol for Information Dissemination</b>           | <b>17</b> |
| <b>  Appendix B: ZeroFox Intelligence Probability Scale</b>                         | <b>18</b> |

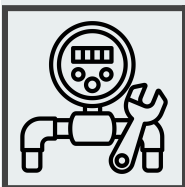
## **| This Week's ZeroFox Intelligence Reports**

### **ZeroFox Intelligence Brief October 7 Anniversary Report**

October 7, 2024, marks the one-year anniversary of Hamas' attack on Israel, wherein thousands of Palestinian militants breached the Gaza-Israel border in an unprecedented attack that resulted in the deaths of 1,180 Israelis and foreign nationals. In the weeks running up to this date, Israel has used years of successful intelligence-gathering to severely weaken Hezbollah, Israel's longtime nemesis that entered the conflict to support Hamas. This intelligence allowed Israel to execute high-profile, booby-trapped communication device attacks and precision airstrikes that wiped out Hezbollah's leadership and degraded its weapons supplies.

# | Cyber and Dark Web Intelligence |

## | Cyber and Dark Web Intelligence Key Findings



### U.S. Utility Company Forced to Take Systems Offline After Cyber Incident

**What happened:** American Water faced a cyberattack that disrupted its customer portal and billing operations, though water and wastewater services remain unaffected. The company is working with cybersecurity experts to manage the incident and ensure a swift recovery. While the full impact of the attack is still being assessed, American Water does not [anticipate](#) any material adverse effect on its financial condition or operations. Customers may experience disruptions in account management, but critical services continue to operate without issue.

- **What this means:** American Water is a major regulated U.S. water and wastewater utility. Since water and wastewater facilities are [classified](#) as critical infrastructure in the United States, a cyberattack on such a critical provider highlights the vulnerability of essential infrastructure to digital threats. Water and wastewater facilities are increasingly integrating information technology (IT) and operational technology (OT) systems into their operations to enhance them. The integration of IT/OT systems has created new vectors through which adversaries can exploit vulnerabilities in assets, networks, systems, and devices. Given the scale of American Water's operations, any successful breach could have far-reaching consequences, impacting public health, safety, and continuity in essential services.



### Salt Typhoon's Targeted Campaigns Against U.S. Entities

**What happened:** Chinese state-backed advanced persistent threat (APT) group Salt Typhoon has breached multiple critical U.S. infrastructure networks, specifically targeting major telecommunications providers—including Verizon, AT&T, and Lumen. Notably, the hackers infiltrated networks used by the U.S. government for court-authorized wiretaps, which facilitate criminal and national security investigations. The group focused on gaining long-term, deep, and stealthy access, remaining undetected for months or potentially longer by targeting a small number of broadband and cable networks. Additionally, researchers have stated that this campaign aimed to steal sensitive data and potentially prepare the group for future disruptive

attacks. The nature and extent of the breach have alarmed government officials, with experts describing the incident as one of the most severe cyber espionage events in recent years.

- **What this means:** As Chinese state-sponsored hackers continue to target sensitive data-rich systems in the United States for espionage and intel-gathering purposes, they also keep diversifying their cyber arsenal to evade detection for a considerable time. Cybersecurity researchers have observed Chinese state-sponsored activity in other parts of the world as well, where hackers have deployed unique channels to conduct cyber espionage. For instance, researchers [observed](#) Chinese spies using CCTV cameras in Taiwan and South Korea as indirect channels to communicate with malware in the Indian power grid. There has also been a notable shift in Chinese cyber tactics, from previously conspicuous data thefts to highly sophisticated and covert intrusions. The Salt Typhoon campaign compromised critical U.S. government communication networks, potentially accessing sensitive and classified information that could be crucial to national security. By gaining access to court-authorized wiretap networks, the actor will likely monitor active U.S. counterintelligence operations, undermining efforts to track Chinese spies and hampering national security investigations. The stealthiness and complexity of Salt Typhoon's approach is a further indication that China is evolving its cyber capabilities to conduct long-term espionage and establish footholds in vital infrastructure for potential sabotage.



## Pro-Palestine Hackers Target Israel and Pro-Israel Nations on October 7 Anniversary

**What happened:** October 7, 2024, marks the first anniversary of Hamas' attack on Israel, during which thousands of Palestinian militants breached the Gaza-Israel border in an unprecedented assault that resulted in the deaths of 1,180 Israelis and foreign nationals. In the lead-up to this anniversary, ZeroFox observed pro-Palestine threat actors launching multiple cyber campaigns against Israel and its allies under the #OpIsrael banner. Key actions include attacks by the Anonymous Collective and KromSec; these groups targeted an Israeli electricity company and leaked data from the Israeli Association for Ecology and Environmental Sciences, while also spreading misinformation, disinformation, and malinformation against nations and companies connected to Israel. The Sylhet Gang attacked the marketing site Perniagaan Viral, and Actor Nusantara leaked information from Indian companies in response to India's support for Israel. Hunt3r Kill3rs claimed a data leak involving 130 Israeli defense firms, and LulzSec Black (in collaboration with Moroccan Soldiers) accessed a database containing over 20,000 sensitive records. Additionally, Blackhun73r, Cyber Toufan, and Ghosts of Palestine have expressed gratitude for their collaborations on cyberattacks and vowed to continue targeting pro-Israel entities. Nearly

200 hacktivist groups are now [engaged](#) in cyberwarfare related to the conflict, with distributed denial-of-service (DDoS) attacks being the most prevalent method. Many pro-Russian hacktivists are also joining these efforts to disrupt daily life and influence the information landscape. ZeroFox has also [identified](#) cyber threat actors on Telegram forming alliances with both Israel and Iran in October and November 2023. Throughout the conflict, cyberattacks against Israel have intensified in tandem with escalations in ground fighting. While pro-Israel cyber actors are also active, they are likely operating to a lesser degree, primarily targeting Iran.

- > **What this means:** Pro-Palestine threat actors are actively leveraging cyber campaigns to target Israel and its allies, demonstrating a coordinated effort among various hacktivist groups. This includes a range of attacks, from data leaks to disinformation campaigns, indicating a strategic move to influence public perception and create disruption. The involvement of nearly 200 hacktivist groups reflects a broader mobilization in the cyber domain, with pro-Russian elements adding to the complexity. Meanwhile, pro-Israel cyber actors are responding, albeit to a lesser extent, mainly focusing their efforts on Iran. Overall, the situation represents a dynamic and evolving battleground where digital and physical confrontations are increasingly intertwined.

# | Exploit and Vulnerability Intelligence |

## | Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, industrial control systems (ICS), and government services. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) announced the addition of a total of six vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog across two advisories. The first advisory [addressed](#) CVE-2024-43047, CVE-2024-43572, and CVE-2024-43573. Qualcomm has [released](#) security patches for CVE-2024-43047, a high-severity use-after-free vulnerability. This month's Microsoft Patch Tuesday [addressed](#) 117 security vulnerabilities, including five publicly disclosed zero-days, among which CVE-2024-43572 and CVE-2024-43573 have been added to the KEV. [CVE-2024-43572](#) is a remote code execution flaw in Microsoft Management Console (MMC), and [CVE-2024-43573](#) is a Windows MSHTML Platform Spoofing vulnerability. The second CISA KEV advisory [addressed](#) CVE-2024-23113, CVE-2024-9379, and CVE-2024-9380.

CVE-2024-23113 is an externally controlled format string use vulnerability [CWE-134] in FortiOS fgfmnd daemon that may [allow](#) a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests. CVE-2024-9379 and CVE-2024-9380 are bugs in the Ivanti Cloud Services Appliance (CSA). Ivanti has [released](#) updates to address these two high-severity vulnerabilities and a third CSA bug (CVE-2024-8963). CISA also [released](#) 21 ICS advisories in the past week addressing bugs in Siemens, Schneider Electric, Rockwell Automation, and Delta Electronics products. Adobe [released](#) security updates to address multiple vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. Palo Alto Networks has [released](#) patches for several critical vulnerabilities in its Expedition customer migration tool. One significant flaw, identified as [CVE-2024-9463](#), is an OS command injection vulnerability with a CVSS score of 9.9. Researchers have [discovered](#) the perftcl malware strain targeting Linux servers by exploiting CVE-2023-33246 in Apache RocketMQ and privilege escalation bug CVE-2021-4043. [CVE-2024-9680](#) is a use-after-free issue in the Animation timeline affecting Mozilla Firefox and Firefox ESR. [CVE-2024-9441](#) is an unpatched vulnerability in Nice Linear eMerge E3 access controller systems that could allow arbitrary OS commands to be executed.



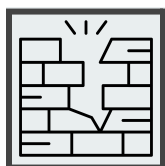
**CRITICAL**

**CVE-2023-33246**

**What happened:** Reportedly, the perftcl malware strain has been targeting Linux servers over the past three to four years. This malware is observed to be persistent and sophisticated and evades

detection. Perfctl exploits misconfigurations to install itself onto devices. It exploits system misconfigurations and the critical vulnerability CVE-2023-33246 in Apache RocketMQ, a messaging and streaming platform. The malware strain reportedly achieves root system rights by exploiting [CVE-2021-4043](#), which is a privilege-escalation vulnerability.

- **What this means:** Perfctl's ability to reportedly disguise itself with legitimate-looking names makes it difficult for users and security teams to identify the infection. Its versatility in performing various malicious activities, from data exfiltration to deploying additional payloads, makes perfctl a destructive tool that can disrupt organizational and individual systems, leading to financial loss, compromised security, and operational instability.
- **Affected products:**
  - RocketMQ versions 5.1.0 and below



## **CRITICAL** **CVE-2024-9463**

**What happened:** Palo Alto Networks has released patches for several critical vulnerabilities in its Expedition customer migration tool, cautioning that attackers could easily exploit these flaws to gain control of firewall administrator accounts. One notable vulnerability, CVE-2024-9463 (CVSS score 9.9), is classified as an OS command injection flaw. This vulnerability enables an unauthenticated attacker to execute arbitrary OS commands with root privileges, potentially exposing usernames, plaintext passwords, device configurations, and API keys from PAN-OS firewalls.

- **What this means:** The vulnerabilities in Palo Alto Networks' Expedition tool present significant cybersecurity challenges, especially concerning unauthorized access to firewall administrator accounts. Attackers' capability to execute commands with root privileges creates a critical risk of exposing sensitive information, which can have serious consequences for organizations that depend on these firewalls. This exposure could include usernames, plaintext passwords, device configurations, and API keys, compromising overall security. Therefore, promptly addressing these vulnerabilities through patches is essential to fortify defenses and mitigate the risk of exploitation.
- **Affected product:**
  - The affected products and versions have been listed by Palo Alto Networks in [this](#) security update.

# **Ransomware and Breach Intelligence**

## Ransomware and Breach Intelligence Key Findings



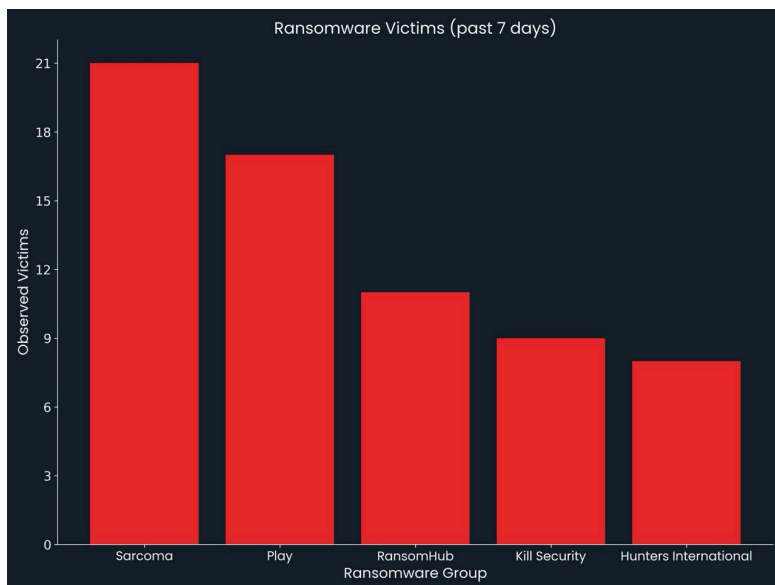
### Emerging Ransomware Threats Across Sectors

**What happened:** In the past seven days, ZeroFox has observed over 100 ransomware attacks primarily targeting the manufacturing sector, with the Sarcoma ransomware group accounting for the highest number. Over 60 percent of these targeted entities are located in North America. On October 10, 2024, ZeroFox [discovered](#) Sarcoma Group's new ransomware leak site, which listed 30 victims at the time of reporting. Sarcoma Group emphasized that companies storing sensitive information on their servers must adopt a responsible

approach to security and that its mission is to highlight the critical importance of data protection. Meanwhile, Japanese

tech giant Casio recently [suffered](#) a significant cyberattack that resulted in unauthorized access to its network and widespread system disruptions. The company is collaborating with cybersecurity experts to investigate the breach and has confirmed that a third party illegally accessed its network, causing a system failure that affected Casio's ability to provide various services. The Underground ransomware gang has [claimed](#) responsibility for the attack and has released a substantial amount of sensitive data on its dark web extortion portal. Axis Health System, a nonprofit healthcare provider located in Colorado, has [reportedly](#) been targeted by a cyberattack from the Rhysida ransomware group. The group has warned that it will release sensitive information in six to seven days if its demands are not met.

- **What this means:** In the ever-evolving landscape of cybercrime, the emergence of new ransomware groups poses a significant threat to organizations worldwide. The recent discovery of the Sarcoma Group, with 30 victims already listed on its leak site (at the time of writing), underscores the alarming pace at which these groups proliferate. As cybercriminals refine their tactics and expand their operations, the potential for



Source: ZeroFox Internal Collections

devastating data breaches and financial losses increases. In light of this growing threat, the ramifications of the Casio breach are significant; it jeopardizes both the privacy of Casio's workforce and the security of its intellectual property. The leaked data—which includes confidential documents, employee personal information, legal files, financial records, patents, project information, and incident reports—raises serious concerns about the security of the company. This exposure could lead to identity theft for employees and compromise sensitive company information, ultimately harming Casio's reputation and operational capabilities. In addition to threatening employee privacy and the integrity of confidential data, the leaked information could also be used by threat actors to conduct further attacks or manipulate market conditions.



## Data Breaches and Nation-State Actors

**What happened:** ZeroFox recently observed an [update](#) on the Handala Hack Team's leak site, where the group claims to have targeted Israel's internal security agency (Shin Bet), a former prime minister's [emails](#), and the Soreq Nuclear Research [Center](#). The threat actor alleges that they breached the security systems of phones belonging to Shin Bet officers, leaking over 7 TB of sensitive data that is allegedly connected to more than 30,000 officers. Handala Hack Team also claims to have leaked over 11,000 emails from former Israeli Prime Minister Ehud Barak. Leading up to the first anniversary of the October 7 attacks, ZeroFox observed [several](#) cyber campaigns claimed by pro-Palestine threat actors against Israel and pro-Israel nations. The #Oplsrail campaign involved web defacements, DDoS attacks, data leaks, and more. The national Dutch police confirmed that a recent data breach of its systems was likely [caused](#) by a state actor; investigations continue to probe the attack, which affected police office contact details, names, email addresses, and more. [ADI](#) disclosed a breach in which threat actors accessed its systems using stolen credentials from a third-party partner. The attackers reportedly exfiltrated encrypted employee account data before ADT terminated the unauthorized access. In other news, Fidelity is notifying 77,000 of its customers about an August data breach that [compromised](#) their personal information. Additionally, the Internet Archive's "Wayback Machine" [experienced](#) a data breach in which a hacker compromised the site and stole a user authentication database containing 31 million records.

- **What this means:** Threat actor Handala's leak of "secret emails" pertaining to Israel's security agency, former prime minister, and research facility can provide proponents of Palestine with leverage against Israel in the Israel-Hamas war. ZeroFox has detected close

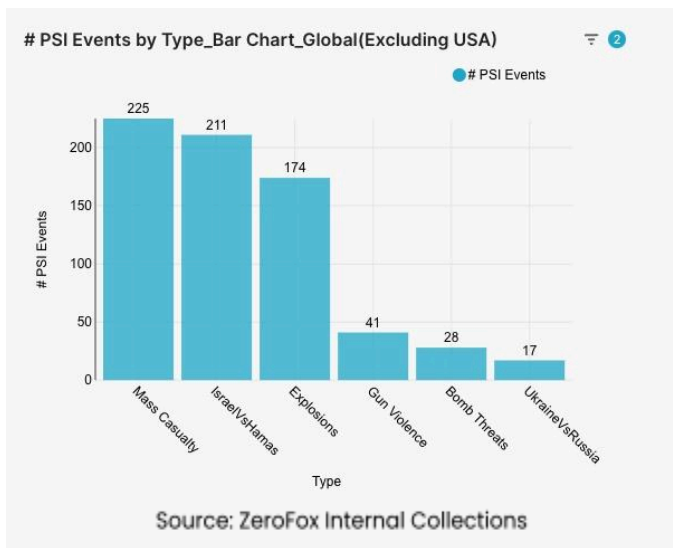
to 300 ransomware and digital extortion victims in the Middle East–Africa region in the past year, of which over 25 percent were targeted by the Handala Hack Team. The #OpsIsrael cyber campaigns are targeting Israeli infrastructure and expanding to nations supporting Israel. Attacks on sectors such as electricity and defense are likely to have serious implications for national security and economic stability. The data leak at the national Dutch police is likely to have negative implications for the security of sensitive information instrumental in keeping civilians safe. The stolen data includes information from criminal databases, arrest numbers, and suspects and is likely to be used by threat actors to encourage further criminal activities. As the police focus on assessing the nature and scope of the leak, they have also implemented enhanced security measures to protect sensitive data. ADT is likely to be exposed to potential internal security risks, as sensitive employee account data was exfiltrated, even though customer data remains unaffected. The use of stolen credentials from a third-party partner highlights the risks of supply chain vulnerabilities in cybersecurity. Additionally, the disruption caused by containment efforts impacts ADT's operations, which could hinder its ability to provide security services and raise concerns about the company's preparedness and resilience in the face of such attacks. The breach at Internet Archive exposes sensitive authentication data for registered members, including email addresses, screen names, password change timestamps, hashed passwords, and other internal data, putting millions of users at risk of identity theft and account compromise. With the potential for further attacks from hacker groups, the integrity of the Internet Archive—an essential resource for historical web content—could be jeopardized, affecting countless users and researchers who rely on its services.

# | Physical and Geopolitical Intelligence |

## | Physical and Geopolitical Intelligence Key Findings

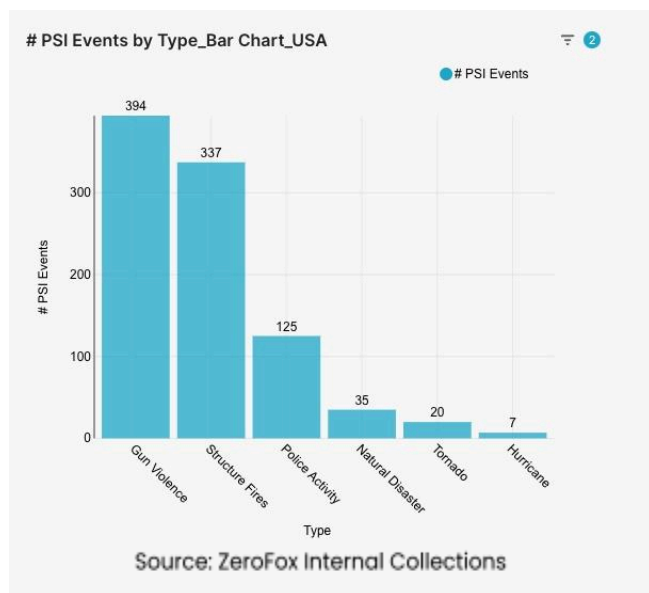
### Physical Security Intelligence: Global

**What happened:** Excluding the United States, there was a 7 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Lebanon, Israel, and Palestine (in that order). Approximately 77 percent of these events were explosions, and the three aforementioned countries accounted for about 66 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 13 percent from the previous week. However, events related to Russia's war in Ukraine increased by 42 percent. The top three most-alerted subtypes were explosions, which saw an 11 percent decrease from the previous week; gun violence, which decreased by 40 percent; and bomb threats, which increased by 22 percent. Lastly, global protest activity decreased by 19 percent.



- **What this means:** This week, the most notable increase in alerts was seen with the Russian and Ukrainian conflict, triggered by several new events within the war. For instance, on October 11, Ukraine successfully detonated 400 Iranian-made Shahed attack [drones](#) in southern Russia, which may reduce the ability of Russian occupiers to target Ukrainian civilians. As for the conflict in Israel, there has been a recent shift from Palestine having the most mass casualty alerts to Lebanon now claiming this title, as Israeli Defense Forces and Hezbollah militants continue to clash at the Lebanese border. Israeli President Benjamin Netanyahu has [threatened](#) that Lebanon faces "destruction and suffering" similar to what has been seen in Gaza, despite the White House urging the countries to reach a diplomatic agreement. Bomb threats were the third most-alerted subtype this week, with Austria contributing to the majority of these instances. Over a period of several days, multiple [train](#) stations in the country have received hoax bomb threats, causing evacuations and disruptions in transportation. Police are currently carrying out an investigation to find the culprit, as they believe the same suspect is responsible for all of these threats.

## Physical Security Intelligence: United States



**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 California, which together made up 26 percent of this week's nationwide total. Gun violence across the United States overall increased by 14 percent from the week prior.

Police activity alerts decreased by 13 percent, and the top contributing states were California and Texas. Structure fires increased by 4 percent, and the top three states for this subtype were California, New York, and Florida. Notably, natural disaster alerts increased by 13 percent, with one-fifth of those alerts falling under the hurricane category. Florida accounted for all hurricane alerts, as well as all tornado alerts.

- **What this means:** After attempting to recuperate from Hurricane Helene, Floridians were hit with Hurricane [Milton](#) this week, which has caused four deaths, mass power outages, and widespread damage. The hurricane also brought several tornadoes, which are said to have caused the Milton fatalities. President Joe Biden deployed thousands of federal personnel to areas affected by the storm, including more than 1,000 Coast Guard members, as rescue and clean-up efforts begin to take place. Gun violence across the country increased from the week prior, with three mass [shootings](#) being recorded by the Gun Violence Archive. California, which continues to be in the top two states for gun violence alerts, accounted for one of these events; five people were shot in [Redding](#) on October 4. As for structure fires, the increase in numbers this week was expected, as the weather begins to cool down and people are starting to use various heating systems to keep warm. This number is likely to increase as temperatures continue to drop across the country.

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> 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?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |