



**ZEROFOX<sup>®</sup>**

*Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**August 19, 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 12:00 PM (EDT) on August 16, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# | Weekly Intelligence Brief |

|                                                                                            |           |
|--------------------------------------------------------------------------------------------|-----------|
| <b>  Cyber Intelligence Key Findings</b>                                                   | <b>3</b>  |
| Donald Trump's Campaign Alleges Email Hack, FBI Launches Investigation                     | 3         |
| Law Enforcement Operations Tackle Cybercriminals                                           | 4         |
| GPS Spoofers Target Commercial Airlines                                                    | 5         |
| <b>  Deep and Dark Web Intelligence Key Findings</b>                                       | <b>7</b>  |
| Rhysida Ransomware Targets Moser Wealth Advisors                                           | 7         |
| New HellDown Ransomware Group Targets Swiss Technology Company                             | 7         |
| LockBit 3.0 Ransomware Targets John L. Lowery & Associates                                 | 8         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                               | <b>10</b> |
| CVE-2024-39825                                                                             | 10        |
| CVE-2024-41940                                                                             | 11        |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                                   | <b>13</b> |
| Ransomware Intelligence: New Groups Emerge as Ransomware Attacks Plague Various Industries | 13        |
| Breach Disclosure: Global Data Security Breaches                                           | 14        |
| <b>  Physical and Geopolitical Intelligence Key Findings</b>                               | <b>18</b> |
| Physical Security Intelligence: Global                                                     | 18        |
| Physical Security Intelligence: United States                                              | 19        |
| <b>  Appendix A: Traffic Light Protocol for Information Dissemination</b>                  | <b>20</b> |
| <b>  Appendix B: ZeroFox Intelligence Probability Scale</b>                                | <b>21</b> |

# | Cyber Intelligence |

## | Cyber Intelligence Key Findings



### Donald Trump's Campaign Alleges Email Hack, FBI Launches Investigation

**What happened:** Former President Donald Trump's campaign has reported a hack, alleging that Iranian actors were responsible for the theft and dissemination of sensitive internal documents. The Trump campaign attributed the hack to "foreign sources hostile to the United States," suggesting Iranian involvement (which Iran has denied) and the FBI is [investigating](#) the matter. Meanwhile, a political media outlet reported receiving internal documents from Donald Trump's campaign via an anonymous AOL account named "Robert." Additionally, a recent threat intelligence [report](#) revealed that in June, Iranian government-linked hackers attempted to breach the account of a high-ranking U.S. presidential campaign official.

- **What this means:** As the U.S. presidential elections approach, cyberattackers are ramping up their efforts to disrupt the process, with foreign interference via hacking, mis/disinformation campaigns, and targeted spear-phishing attacks being a major threat. Foreign threat actors are anticipated to play a significant role in the upcoming election by exploiting societal divisions and eroding trust in democratic institutions to influence electoral outcomes. Iran, known for targeting its adversaries in the Middle East and beyond, has also threatened retaliation against former President Trump for the 2020 drone strike that killed a key Revolutionary Guard figure. Recent attacks on high-level campaign officials and government employees suggest a strategic effort to gather intelligence on political campaigns and potentially sway election results. Cybersecurity researchers have identified Iranian groups creating covert "news" sites using artificial intelligence (AI) to copy content from legitimate news sources and targeting U.S. voters across the political spectrum. This tactic is part of a broader strategy to create political discord and manipulate public opinion. Additionally, Russia-linked accounts have been [observed](#) spreading divisive content aimed at U.S. audiences. As Election Day approaches in November 2024, the threat of cyberattacks, leaks, and violent plots is increasing. The production and dissemination of information online are expected to reach unprecedented levels, driven by adversarial nation-states, politically motivated cyber actors, and individuals. This surge in misinformation, disinformation, and malinformation is likely to exacerbate social, political, and geopolitical tensions, making it increasingly challenging to distinguish fact from fiction. The FBI's investigation into the alleged hack of Trump's

campaign could enhance election security by prompting stronger protective measures against foreign interference.



## Law Enforcement Operations Tackle Cybercriminals

**What happened:** Over the past week, law enforcement (LE) operations have disrupted operations of ransomware group Disposessor (alias Radar), arrested the creator of Ransom Cartel and Reveton ransomware operations, and put out arrest warrants for two individuals from Florida involved in illicit Dark Web activities. Authorities [dismantled](#) three U.S. servers, three United Kingdom servers, 18 German servers, eight U.S.-based criminal domains, and one German-based criminal domain associated with the Disposessor ransomware operations. The creator of Ransom Cartel and Reveton ransomware operations is being [extradited](#) to the United States to face charges for creating the operation and a malvertising campaign. The operations ran their schemes across many years to distribute malware onto the computers of millions of internet users globally. The two individuals from Florida have been charged with conspiracy for trafficking in unauthorized access devices and the possession of 15 or more unauthorized access devices. Authorities have arrested one of the charged and are on the lookout for the other one.

- **What this means:** With the upcoming U.S. elections, U.S. officials are keeping a close eye on computer networks to thwart any possible cyber threat. The past week saw substantial LE actions against cybercriminals. Disposessor ransomware had developed into an impactful operation targeting small-to-mid-sized businesses and organizations from the production, development, education, healthcare, financial services, and transportation sectors. Investigations revealed 43 companies as victims of Disposessor, from around the globe, reflecting the scale of the operation. By taking down servers and domains across multiple countries, authorities have shut down the Disposessor operations, potentially preventing further attacks and protecting sensitive data. Meanwhile, the creator of Ransom Cartel and Reveton ransomware operations is also involved in transmitting the Angler Exploit Kit, other malware, and online scams. It indicates how one threat actor can maintain the capability of running various malicious operations. Ransomware has become one of the greatest cyber threats to the digital world, with alarming statistics. Ransomware attacks have also had tangible effects, including shutting down crucial systems and impacting critical infrastructure. For example, the Colonial Pipeline attack, the largest cyberattack to [impact](#) an oil infrastructure in the United States, resulted from a ransomware attack. Hence, ransomware attacks are a potential threat to the upcoming elections too, where threat actors might try to take over critical infrastructure or crucial

networks to coerce voters into paying substantial ransom sums. The recent takedowns of infamous ransomware groups LockBit and Blackcat, besides Dispossessor, indicate dedicated efforts to combat this threat. On the other hand, the two Florida individuals involved in the trafficking of unauthorized access devices had sought and gained asylum after they arrived in Florida. However, soon after gaining asylum, the duo started leading a lavish lifestyle, which prompted an FBI investigation. The investigation revealed that the duos' unusually high spendings were funded by illicit activities on Dark Web platforms like WWH Club and its related forums, Skynetzone, Opencard, and Center-Club. They were orchestrating a sophisticated operation trafficking in unauthorized access devices and financial data. The platforms they were operating in let cybercriminals buy, sell, and trade login credentials, malware, financial credentials, sensitive information, and more.



## GPS Spoofers Target Commercial Airlines

**What happened:** A recent surge in GPS spoofing has raised significant concerns about flight safety. Research indicates a 400 percent increase in GPS spoofing incidents affecting commercial airliners in recent months. Many of these incidents reportedly involve illicit ground-based GPS systems, particularly around conflict zones, where they broadcast incorrect positions to the surrounding airspace in an attempt to confuse incoming drones or missiles.

- **What this means:** GPS spoofing allows threat actors to trick people by manipulating (in this case aviation) an aircraft's location, effectively misdirecting navigation systems and other connected systems. As spoofing incidents become more frequent and complex, flight crews need to stay cautious and manage unpredictable situations while maintaining safety in increasingly challenging conditions. Adversaries have been observed secretly rerouting an aircraft's course to enter currently contentious regions. These events raise serious concerns about passenger safety and navigation.

# | Deep and Dark Web Intelligence |

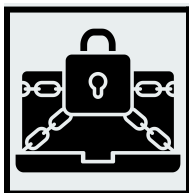
## | Deep and Dark Web Intelligence Key Findings



### **Rhysida Ransomware Targets Moser Wealth Advisors**

**What happened:** On August 12, 2024, ZeroFox observed an update on the Rhysida Ransomware leak site targeting Moser Wealth Advisors, a U.S.-based financial planning and wealth management firm. According to the post, the threat actors are selling the “exclusive, unique, and impressive” data to one person at the price of 2 BTC but do not disclose the specific types of data being sold. The post further states that Moser has seven days to comply with the ransom demand as of August 12, 2024.

- **What this means:** This attack underscores the significant cybersecurity risks faced by financial institutions and highlights the vulnerability of organizations that handle sensitive client information, particularly high-net-worth individuals and businesses. For professional organizations, this attack serves as a stark reminder of the necessity to bolster cybersecurity measures to protect against potential data breaches and financial losses, emphasizing the broader threat that ransomware poses to the financial sector.



### **New HellDown Ransomware Group Targets Swiss Technology Company**

**What happened:** On August 14, 2024, ZeroFox observed the emergence of a new ransomware group, HellDown Ransomware. Later in the same day, ZeroFox observed an update on the leak site targeting Hug-Witschi, a Switzerland-based company that provides technology solutions for hardware and software needs. The post claims that data totaling 67 GB have been stolen, and while it does not explicitly state the types of data stolen, screenshots of samples indicate that some may involve usernames, passwords, and company financial information.

- **What this means:** This attack comes only five days after the Switzerland-based plant manufacturing company Schlatter Industries was hit with a major cyberattack affecting its IT services. While limited information is currently available on the Schlatter Industries attack—including the threat actors behind it—some reporting indicates it may have been a ransomware attack. These attacks on a major IT services and payment technology provider, as well as a manufacturing plant, underscore the escalating threat of ransomware to crucial infrastructure. An attack on such an entity can have widespread

implications, affecting not only the companies themselves but also their clients and partners who rely on its services for critical operations.



## **LockBit 3.0 Ransomware Targets John L. Lowery & Associates**

**What happened:** On August 13, 2024, ZeroFox observed an update on the LockBit 3.0 Ransomware leak site targeting John L. Lowery & Associates, a U.S.-based employment agency. The post further states that the firm has until August 25, 2024, to comply with the ransom demand.

- **What this means:** This attack underscores critical risks for professional organizations. Although detailed information about the attack's impact is limited, it highlights the pervasive threat posed by LockBit Ransomware, even with its relatively limited capabilities following LE disruptions earlier this year. LockBit operates as a Ransomware-as-a-Service (RaaS) model and is notorious for utilizing a double extortion technique, increasing the severity of threats to its victims. Attacks on entities such as John L. Lowery & Associates can lead to significant operational disruptions, which in turn can lead to delays in providing employment resources and, ultimately, financial losses. While the repercussions of targeting an entity such as this may not be as high-profile or as far-reaching, the repercussions faced by those individuals it does affect can be harsh.

# | **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 software solutions, technology, and security domains. This week, several companies released their advisories addressing several security flaws. In this August's Microsoft's Patch Tuesday, the company [addressed](#) more than 80 flaws, including six actively exploited and three publicly disclosed zero-days. Adobe disclosed [fixes](#) for more than 70 security vulnerabilities, including those that make products vulnerable to code execution, memory leaks, and denial-of-service attacks. Software company, Ivanti [announced](#) patches for eight vulnerabilities which also include patches for two critical-severity vulnerabilities (CVE-2024-7569 and CVE-2024-7593). SolarWinds [disclosed](#) patches for a critical vulnerability (CVE-2024-28986) that could allow threat actors to execute arbitrary code and run commands on the host machine. Palo Alto, in an [advisory](#), highlighted a command injection issue (CVE-2024-5914), which allows an unauthenticated attacker to execute arbitrary commands within the context of an integration container. SAP's Security Patch Day [includes](#) 17 new Security Notes and eight other updates pertaining to previously released Notes. Fortinet [patched](#) several vulnerabilities, including one (CVE-2024-39825) that could allow threat actors to escalate privileges over a network.



**HIGH**

**CVE-2024-39825**

**What happened:** Buffer overflow in some Zoom Workplace Apps and Rooms Clients may allow an authenticated user to conduct an escalation of privilege via network access.

- **What this means:** This **HIGH**-severity bug impacts Zoom Workplace apps for desktop and mobile devices, and Rooms clients for Windows, macOS, and iPad. The flaw can allow threat attackers to exploit weaknesses in the software's privilege management, gaining higher levels of access than intended by the system's security protocols.
- **Affected products:**
  - Zoom Workplace Desktop App for Linux before version 6.0.0
  - Zoom Workplace Desktop App for Windows before version 6.0.0
  - Zoom Workplace Desktop App for macOS before version 6.0.0
  - Zoom Workplace VDI Client for Windows before version 5.17.13
  - Zoom Workplace App for iOS before version 6.0.0
  - Zoom Workplace App for Android before version 6.0.0

- Zoom Rooms App for Windows before version 6.0.0
- Zoom Rooms App for Mac before version 6.0.0



**CRITICAL**  
**CVE-2024-41940**

**What happened:** A **CRITICAL** vulnerability (CVSS score: 9.1) was found in SINEC NMS (all versions before V3.0), where the application fails to properly validate user input for a privileged command queue.

- **What this means:** This flaw allows an authenticated attacker to inject and execute OS commands with elevated privileges. Such unauthorized command execution could lead to severe security risks, including full system compromise, data breaches, and potential disruption of services. Given that the attack requires only authenticated access, it increases the risk for insiders or attackers with valid credentials to exploit the system. Siemens has issued a patched version of SINEC NMS and advises upgrading to the latest release.
- **Affected products:** SINEC NMS versions before V3.0

# **Ransomware and Breach Intelligence**

## Ransomware and Breach Intelligence Key Findings

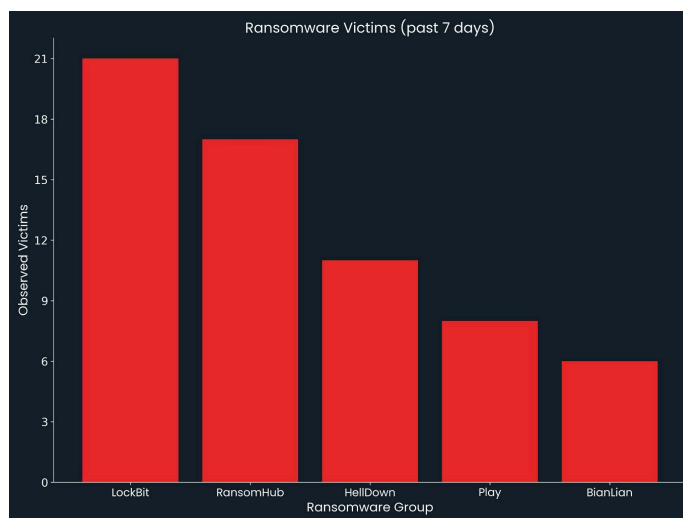


### Ransomware Intelligence: New Groups Emerge as Ransomware Attacks Plague Various Industries

**What happened:** A data breach at Kootenai Health [impacted](#) over 464,000 patients after their sensitive information was stolen and leaked by the 3AM ransomware group. The attack was detected in early March 2024, with unauthorized access occurring on February 22, 2024. On August 8, 2024, Evolution Mining, one of Australia's largest gold producers, [experienced](#) a

ransomware attack that disrupted its IT systems. The company has since contained the incident with the help of external

cybersecurity experts. In other news, despite a law enforcement takedown of LockBit 3.0 earlier this year, cybersecurity researchers [report](#) that it remains the most active ransomware gang in 2024, leading in victim counts. In the first half of 2024, LockBit 3.0 was responsible for 325 victim posts, dominating other ransomware groups. In the past week, ZeroFox has observed two new ransomware groups. On August 9, ZeroFox researchers [identified](#) HexaLocker on Telegram. This group, composed of experienced administrators from notorious organizations like LAPSUS\$ and Gloriamist, claims to collaborate with DoubleFace ransomware. On August 14, ZeroFox [identified](#) the second group named HellDown ransomware.



Source: ZeroFox Internal Collections

- **What this means:** The healthcare sector is a particularly lucrative target for ransomware groups, where the stakes are particularly high due to the sensitive nature of the data involved. The 3AM ransomware group's leak of a 22GB archive of personal and medical information poses significant risks, including identity theft and further cyberattacks. Moreover, the adversary's probable association with notorious ransomware groups like Conti and Royal indicates the possibility of further extortion attempts. Meanwhile, as a key name in the gold and copper markets, Evolution Mining's economically vital operations are likely also of strategic importance. Minerals like gold and copper are essential for a wide

range of industries, including electronics, aerospace, and defense—sectors that often come into play in geopolitics. Companies like Evolution Mining are thus attractive targets for cybercriminals, ransomware groups, and state-sponsored threat actors. A leading brand in plant engineering, Schlatter Industries is a lucrative target for financially motivated actors. The ransomware group likely aims to extract a hefty ransom from the company, using the stolen data as leverage. Even though the specific nature remains unclear, researchers are speculating common ransomware attack vectors behind the attack, including social engineering, unpatched software, or compromised credentials. In the meantime, the persistence of LockBit 3.0 as one of the leading ransomware groups, even after significant takedowns, demonstrates the adaptability of cybercriminal enterprises. Of the two new ransomware groups ZeroFox identified in the past week, HexaLocker maintains sophisticated capabilities, with data decryption without the proper key supposedly nearly impossible. With an encryption speed of 500 MB/s, it can quickly lock down vast amounts of data. The ransomware is also seemingly designed to evade detection by common tools, resist memory scans, and avoid analysis by refusing to run in virtual environments. This level of complexity suggests that HexaLocker can effectively bypass standard cybersecurity defenses and target the most valuable files.



## Breach Disclosure: Global Data Security Breaches

**What happened:** The People Power Party (PPP), South Korea's ruling party, has [reported](#) that North Korean hackers have reportedly stolen sensitive information concerning the K2 tanks, South Korea's primary battle tank, along with details about its "Baekdu" and "Geumgang" spy planes. The PPP is concerned that this stolen data could enable North Korea to evade military surveillance and gain a strategic advantage. In response, the party is advocating for the immediate implementation of enhanced measures to protect national security. About four months after a notorious hacking group [declared](#) that it had stolen a vast amount of sensitive personal information from a major data broker, a member of the group has reportedly released much of this data for free on an online marketplace dedicated to stolen personal information. According to a class-action lawsuit filed in the U.S. District Court in Fort Lauderdale, FL, the hacking group USDoD claimed in April to have stolen personal records of 2.9 billion individuals from National Public Data. The group had initially offered the stolen data, which includes records from the United States, Canada, and the United Kingdom, for USD 3.5 million on a hacker forum. The Computer Emergency Response Team of Ukraine (CERT-UA) [reported](#) a widespread phishing campaign where attackers,

masquerading as the Security Service of Ukraine (SSU), sent emails with a malicious link to download a file named "Documents[.]zip." This link triggers a process that finally installs ANONVNC malware, granting unauthorized access to the victim's computer. An unsecured backup blob [exposed](#) pre-employment background checks on approximately 200,000 people. The files contained various amounts of personal and occupational information, including SSN, name, address, driver's license, date of birth, education and employment history, and in some cases, criminal background checks. The blob was unsecured for at least six months and possibly much longer. Threat actor "dk0m" [claimed](#) to be selling access to TikTok's Law Enforcement (EDR) Panel and other accesses to various governments and ministries from the US, Argentina, Brazil, Serbia, Ukraine, Malaysia, and Egypt on the predominantly English-language dark web forum BreachForums. To discuss the cost of the access, the actor requested to communicate with it using their Telegram account. The moderately credible threat actor "blackfield" [advertised](#) a data breach impacting the Israel Defense Forces on the predominantly Russian language Dark Web forums RAMP and XSS. According to blackfield, the breached data contains information about Ex IDF "intelligence members," including real geolocation outside of Israel, names, phones, emails, names of companies, and private projects. The actor charged BTC 1 for the data breach.

- **What this means:** Data breaches by threat actors around the globe are rapidly rising, frequently culminating in ransomware attacks that further jeopardize organizational security and personal information. The PPP has called for a revision of existing criminal law to include foreign countries in the application of its espionage laws. Data leaked about the military units (including the spy planes) has a likely chance of North Korea strategically upgrading its arsenal to better evade military surveillance and improve its tactics against South Korea. The breach exposing 2.9 billion personal records presents a serious risk, potentially leading to widespread identity theft, fraud, and other criminal activities. Furthermore, this incident has escalated into a ransomware attack, with the stolen data being used as leverage to extort victims and further amplify the damage caused. The widespread phishing campaign posing as SSU shows a growing trend of attackers masquerading as LE officials and distributing malware via phishing emails to infiltrate government networks. The campaign affected more than 100 computers across central and local government agencies. The ANONVNC malware used in this attack enables covert and unauthorized access to sensitive systems. The sophistication of the breach suggests the involvement of foreign actors, potentially attempting to undermine Ukraine's security and destabilize its governmental operations. This exposure of pre-employment background checks puts the personal and occupational information of approximately 200,000 individuals at significant risk, potentially leading to identity theft, fraud, and other forms of exploitation. The compromised data, including SSNs and criminal background checks, can be used by threat actors to conduct various malicious activities, such as impersonation, financial fraud, and targeted phishing attacks. The prolonged period of

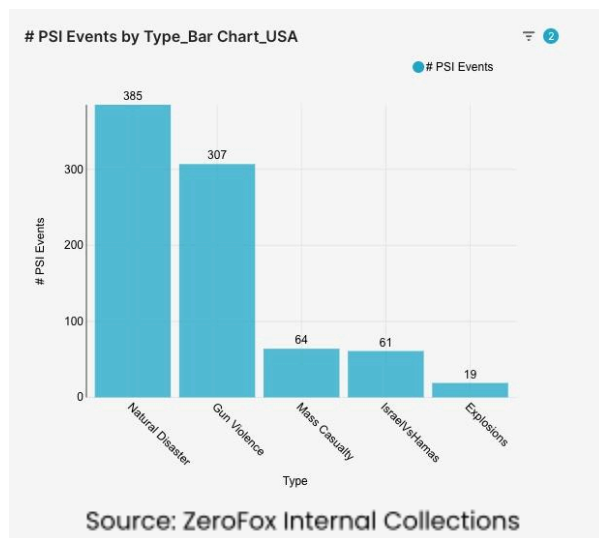
unsecured access exacerbates the risk, as it provides ample time for malicious actors to exploit the data for a range of criminal purposes. Threat actors are often targeting high-profile and sensitive information from government and military organizations. The sale of access to TikTok's Law Enforcement Panel and various government ministries on the dark web underscores a serious breach of security, potentially compromising LE operations and government data. Similarly, the exposure of data from the Israel Defense Forces, including geolocation and personal details of intelligence members, could have severe implications for national security and operational integrity. Threat actors can potentially use this stolen data to blackmail organizations, conduct espionage, or further exploit the information for financial gain or to disrupt national security efforts.

# | Physical and Geopolitical Intelligence |

## | Physical and Geopolitical Intelligence Key Findings

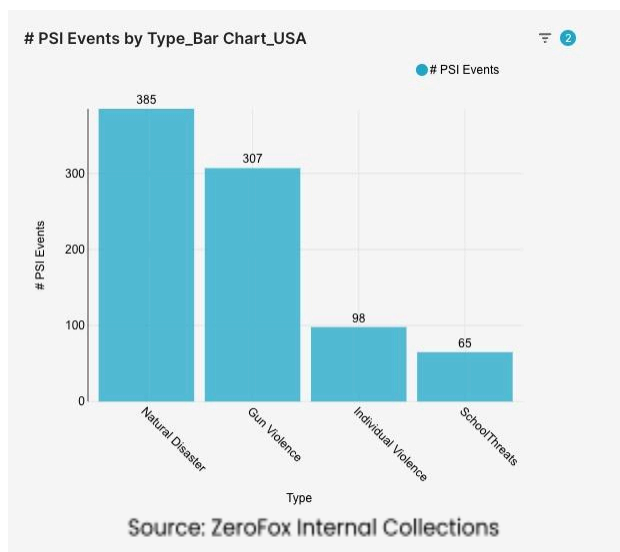
### Physical Security Intelligence: Global

**What happened:** Excluding the United States, there was no increase or decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon. Approximately 85 percent of these events were explosions, and the three aforementioned countries accounted for approximately 55 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 21 percent from the previous week. Additionally, events related to Russia's war in Ukraine increased by 155 percent. The top three most-alerted subtypes were explosions, which saw a 5 percent increase from the previous week; gun violence, which decreased by 13 percent; and natural disasters, which decreased by 16 percent.



- **What this means:** Once again, events related to the war in Ukraine have shown a dramatic increase as Ukrainian troops continue to work their way into Russian territory. For instance, on Wednesday night, Ukrainian drones hit four Russian airfields in the [Kursk](#) region; simultaneously, Russia has taken control of villages near [Pokrovsk](#), which hosts several important Ukrainian supply routes. These events are a contributing factor to the increase in explosion alerts as well. In the Israel-Hamas War, there was a decrease in alerts, potentially due to peace talks that are set to take place today. Officials from the U.S., Qatar, and Egypt will be meeting an Israeli delegation in [Doha](#), Qatar, in an effort to strike a peace deal between Israel and Hamas; however, Hamas will not be participating, and Iran has stated that they may not retaliate against Israel – only if a ceasefire deal is reached. Whether or not an agreement can be settled is yet to be determined.

## Physical Security Intelligence: United States



**What happened:** In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and individual violence. Natural disaster alerts typically involve fires and severe weather; gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim; and individual violence mainly refers to occurrences of stabbings. The top two states that had the most gun violence alerts were Illinois and Pennsylvania, which together made up almost one-quarter of this week's nationwide

total (23 percent). Gun violence across the United States overall decreased by 24 percent from the week prior. The top two contributors to natural disaster alerts this week were California and New York, and natural disaster alerts across the country decreased by 14 percent. Individual violence alerts increased by 5 percent, and the top contributing states were New York and California as well. Notably, all alerts (excluding protests) involving schools increased by 210 percent.

- **What this means:** The most drastic increase this week are alerts in relation to schools, as many students are beginning to return from summer break. In a [study](#) conducted by the Secret Service, it was noted that the most frequent incidents of school violence occurred at the start of the school year and that 41 percent of the observed attacks happened within the first week of the semester. These numbers are expected to increase as more and more students are returning from their holidays. Natural disaster alerts have decreased somewhat, and with California being a top contributor again, this correlates with recent containment efforts of the [Park](#) Wildfire, which has been 40 percent contained as of Wednesday. Even so, the fire remains the fourth largest in the state's history, and more than 5,400 firefighters are still assigned to combat the blaze. Generally, droughts and rising temperatures aggravated by climate change have increased the frequency and intensity of California wildfires in recent years. Wildfire season has only just begun, however, so the numbers are likely to increase even further.

## | 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%         |