



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

August 5, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the cyber threat landscape. 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 2, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence Flash Report: Pro-Russia Actors Threaten Paris Olympics	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 14	2
ZeroFox Intelligence Flash Report – AI-Powered Tool to Target Cryptocurrency Wallets In Development	3
 Cyber Intelligence Key Findings	5
Paris Olympics Face Myriad Cyber Threats	5
FBI Warns About Crypto Scammers	6
China-Backed Phishing Attack Targets India Postal System Users	6
 Deep and Dark Web Intelligence Key Findings	9
Threat Actor Allegedly Leaks Database from French Olympic Games Website	9
Cicada3301 Ransomware Targets Three U.S.-Based Manufacturers	9
Pro-Palestine Hacktivist Group Claims DDoS Attacks on Israeli Olympic Teams' Websites	10
 Exploit and Vulnerability Intelligence Key Findings	12
CVE-2024-4879	12
CVE-2024-37085	13
 Ransomware and Breach Intelligence Key Findings	15
Ransomware Intelligence: Tangible Effects of Ransomware Attacks Felt Across Various Sectors	15
Breach Intelligence: HealthEquity Data Breach Exposes Patient Information	16
 Physical and Geopolitical Intelligence Key Findings	18
Physical Security Intelligence: Global	18
Physical Security Intelligence: United States	19
 Appendix A: Traffic Light Protocol for Information Dissemination	21
 Appendix B: ZeroFox Intelligence Probability Scale	22

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report: Pro-Russian Actors Threaten Paris Olympics

The 2024 Olympics, scheduled to be held from July 26 to August 11 in Paris, France, is facing and likely will continue to face cyberattacks—primarily from politically motivated actors. Pro-Russian hackers are likely to conduct low impact attacks targeting Olympics-related events and states that oppose Russia's participation in the Games. Russian-aligned actors will likely try to undermine the International Olympic Committee (IOC) via disinformation campaigns. These efforts may result in disruption to events, dissuade spectators, and create fear among attendees and athletes, leading to reputational damage to the host (France), the IOC, and, by extension, the West.

Malicious Pro-Russian cyber activities are likely part of a broader strategic initiative seeking to undermine both France and the IOC's security and credibility, as well as France's ability to host such a large-scale international event.

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 14

On July 18, 2024, an untested actor named "saltyyy" posted in the dark web forum Omniforums (to which they had recently registered), attempting to ascertain if their peers had interest in procuring physical access to commercial office spaces. On July 9, 2024, hacker collective "SiegedSec" announced its alleged success in breaching a network associated with The Heritage Foundation, claiming to have stolen over 200 GB of data that includes passwords and personally identifiable information (PII). On June 30, 2024, untested actor "enryu" advertised a new extended validation code-signing service on the primarily Russian-speaking dark web forum Exploit. On June 28, 2024, a positive reputation threat actor named "uroboros" advertised network access to two U.S.-based managed service providers in the primarily Russian-speaking dark web community RAMP. In June 2024, two ransomware and digital extortion collectives advertised their intent to attract additional affiliates with posts in the primarily Russian-speaking dark web forum RAMP. On June 26, 2024, untested actor "DragonForce" advertised collaboration opportunities to individuals, "teams," or other unspecified "specialists" able to carry out penetration testing.

ZeroFox Intelligence Flash Report – AI-Powered Tool to Target Cryptocurrency Wallets In Development

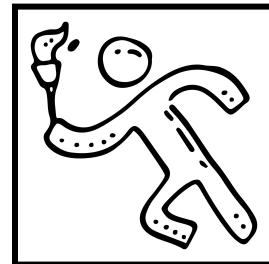
On July 25, 2024, untested threat actor “Michelangelo” posted in a dark web forum advertising a new artificial intelligence (AI)-powered malicious tool designed to facilitate attacks targeting cryptocurrency wallets. The tool lists an array of features that enable various methods of obtaining passwords associated with victims’ cryptocurrency wallets. An emphasis is also placed upon user convenience, flexibility, and management of attack processes. While tools with brute-forcing and password-mining capabilities are not new, this tool allegedly contains innovative features that reflect an appetite amongst cybercriminals to develop and commercialize malicious techniques able to target the growing cryptocurrency economy.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

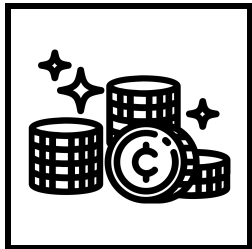
Paris Olympics Face Myriad Cyber Threats

What happened: The Paris Olympics has been facing and will continue to face various cyber threats—including data breaches and distributed denial-of-service (DDoS) attacks—from politically and financially motivated actors. An alleged doxing attack attributed to threat actor “Zeus” exposed some sensitive data belonging to Israeli athletes participating in the Paris Olympics on Telegram. The type of data exposed, which allegedly includes military statuses, blood test results, and login credentials, has prompted France's Anti-Cybercrime Office (OFAC) to intervene. On July 29, ZeroFox Intelligence observed pro-Palestine hacktivist group “Anonymous Collective” [claiming](#) to conduct a DDoS attack against the websites of the Israel Swimming Association and the Israel Pro Football Leagues under its ongoing operations #ParisOlympics2024 and #OplIsrael. On July 31, threat actor group “LulzSec Muslims” [claimed](#) to have leaked a database associated with the Paris Olympic Games. Additionally, French authorities have [stated](#) that they detected and thwarted 68 cyberattacks since July 22, two of which were directly related to the Olympics.



- **What this means:** The Olympics is a lucrative target for financially motivated actors and politically guided adversaries. Several pro-Palestine threat actors are targeting Israeli athletes due to geopolitical and military tensions involving Israel. The exposed personal and military information will likely invite other malicious actors to target the affected athletes with intimidation or fear-mongering campaigns or disrupt the athletes' participation in the Olympics. The leaked data from the doxing attack, such as blood test results and login credentials, could be used for identity theft, blackmail, or further cyberattacks. Additionally, disclosing military statuses could potentially endanger the athletes and their families. This attack not only impacts the individuals involved but also serves as a political statement, aiming to draw international attention to the ongoing conflicts involving Israel. Meanwhile, the Paris Olympics opening ceremony attracted the attention of several religious groups and elicited responses from different entities, including hackers like LulzSec Muslims. The group allegedly leaked an Olympics-related database “in response to the abuse they (the IOC) committed against our Lord Jesus.” Besides these attacks, hacktivist groups have also been highly active, aiming to disrupt the event by leveraging DDoS attacks or discrediting the IOC's reputation via disinformation campaigns. The media, public, and government attention to the Games also makes it an attractive target for malicious cyber actors intending to cause disruption and gain prominence—both for themselves and for their political cause.

FBI Warns About Crypto Scammers

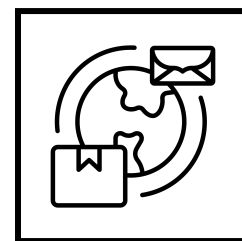


What happened: The Federal Bureau of Investigation (FBI) has warned that scammers are impersonating cryptocurrency exchange employees to steal funds. Scammers contact victims through unsolicited calls or messages, create a sense of urgency, and deceive victims into revealing login credentials. The scammers then access victims' accounts and steal their cryptocurrency.

➤ **What this means:** The federal law enforcement agency has detailed a new scam wherein fraudsters contact victims through phone calls or messages impersonating representatives of legitimate cryptocurrency exchanges. They often create a sense of urgency by claiming that someone is attempting to hack into the victims' accounts or that there are security issues needing immediate attention. Once contact is established, the scammers use various tactics to deceive victims into revealing sensitive information, such as login credentials. With this information, the scammers gain access to the victims' cryptocurrency accounts and transfer the assets to wallets they control, leaving victims with few or no options to recover their funds. To protect against these scams, the FBI advises never to provide login information in response to unsolicited calls or messages. Additionally, avoid clicking links, downloading messages, or opening attachments from unknown sources, as these could contain malicious payloads designed to steal information after infecting a system. Being aware of these tactics and practicing caution can help safeguard against this type of fraud.

China-Backed Phishing Attack Targets India Postal System Users

What happened: A China-based hacking group known as “Smishing Triad” targeted iPhone users in India with phishing attacks through text messages. The messages falsely claimed that a package was waiting at an India Post warehouse and contained URLs leading to fraudulent websites. Over 470 domains mimicking the India Post’s official domain were registered between January and July 2024, primarily through Chinese and American registrars. Phishing emails were also sent via iMessage using third-party email services.



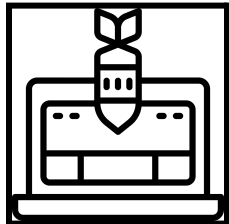
➤ **What this means:** By mimicking official communications and using convincing lures, the attackers increase the likelihood of their targets falling victim to the scam. If successful, threat actors could steal sensitive PII from victims, such as login credentials and financial details, potentially leading to identity theft, financial loss, or unauthorized access to other accounts. The involvement of both Chinese and American domain registrars in registering deceptive domains complicates the tracking and mitigation of the threat. Additionally, the use of iMessage and third-party email services broadens the attack vector, making mobile

devices a highly attractive target for such campaigns. During the 2023 holiday season, researchers detected a surge in DNS queries to "combosquatting" domains mimicking the United States Postal Service ([USPS](#)) and its services. Security researchers found that phishing campaigns targeting USPS generate traffic levels similar to the legitimate site, often peaking during holidays. By impersonating legitimate postal services like India Post and USPS, attackers leverage the inherent trust people place in these organizations to create a sense of legitimacy. These phishing attacks usually aim to steal sensitive information like account credentials and credit card details or trick users into making payments for fake fees or fraudulent charges. This tactic increases the likelihood that individuals will interact with malicious content or provide sensitive information, thereby enhancing the effectiveness of the phishing attacks.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor Allegedly Leaks Database from French Olympic Games Website

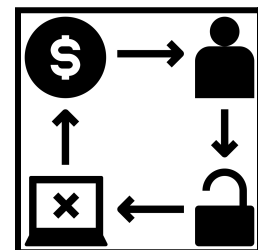


What happened: On July 31, 2024, threat actor group LulzSec Muslims claimed to have leaked a database associated with the French Olympic Games website in response to “abuse committed against Lord Jesus.” This is likely a reference to the controversial opening ceremony of the Paris Olympic Games held on July 26, 2024, during which some viewers believe imagery of Leonardo da Vinci’s “The Last Supper” was used inappropriately. The leaked database supposedly contains 3,000 lines of data, including first names, last names, addresses, email addresses, and user accounts.

- **What this means:** The LulzSec Muslims database leak is the first solo attack by the group tracked by ZeroFox, so the legitimacy of the claim—as well as the group’s capabilities—are currently unverifiable. However, the group is likely leveraging the widespread controversy over the topic in the media in order to gain notoriety within the online hacking community. Additionally, the group almost certainly targeted the French website as France is the host of this year’s Games; however, claims of attacks against websites of other participating countries are possible in the short term. ZeroFox will continue to monitor for updates on the veracity of the group’s claim as well as any significant fallout from the leak if proven true.

Cicada3301 Ransomware Targets Three U.S.-Based Manufacturers

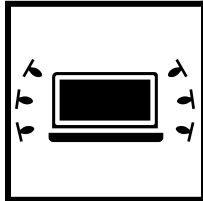
What happened: On July 26, 2024, ZeroFox observed several updates to the “Cicada3301” ransomware leak site targeting three U.S.-based manufacturing companies: [NARSTCO](#), which provides steel railroad ties and turnouts; [D&K Group](#), which provides laminating films and equipment; and [Voss Belting & Specialty](#), which provides designs and fabrications for conveyor belts and timing belts. Cicada3301 stole sizable volumes of data from each company: 80GB, 125GB, and 130GB, respectively. Additionally, the affected NARSTCO domain does not display content at the time of reporting.



- **What this means:** Assuming Cicada3301’s claims are true and it is in possession of the companies’ data, the release of such data has far-reaching implications. For NARSTCO, this could include the compromise of industrial designs and critical railroad infrastructure information. For D&K Group, this could include the exposure of sensitive manufacturing processes as well as client information. For Voss Belting & Specialty, this could include the

disclosure of proprietary designs and customer data. These targeted attacks demonstrate the vulnerability of diverse sectors to ransomware threats, including manufacturing, industrial services, and critical infrastructure.

Pro-Palestine Hacktivist Group Claims DDoS Attacks on Israeli Olympic Teams' Websites



What happened: On July 29, 2024, pro-Palestine hacktivist group Anonymous Collective conducted DDoS attacks against the websites of two national sports entities from Israel participating in the 2024 Paris Olympics: the Israel Swimming Association and the Israel Pro Football Leagues. These websites were attacked under Anonymous Collective's long-standing operation, #OplIsrael.

➤ **What this means:** #OplIsrael is an ongoing malicious cyber campaign carried out by various pro-Palestine threat actor groups against Israeli entities and those perceived as supporters of Israel, particularly after the outbreak of conflict between Israel and Hamas in October 2023. While the majority of attacks by Anonymous Collective under #OplIsrael are low-level DDoS attacks that do not result in lasting damage, some of its attacks have involved data leaks, demonstrating the need for companies to be vigilant about their cyber hygiene practices. Additionally, while these DDoS attacks against the Israeli Olympic teams are currently more of a nuisance than a serious threat, they illustrate how the collective is leveraging an event with a massive global audience to call attention to its pro-Palestine cause.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

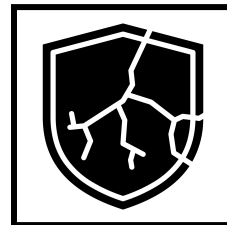
In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in software solutions, technology, and government security domains. In an [advisory](#), Carnegie Mellon University notes that two newly identified vulnerabilities (CVE-2024-7208 and CVE-2024-7209) could allow threat actors to abuse hosted email services to spoof the identity of the sender and bypass existing protections, and the researchers who found them claims millions of domains are affected. VMware [disclosed](#) a vulnerability that can allow a malicious actor with sufficient Active Directory (AD) permissions to gain full access to an ESXi host. Google [announced](#) security updates to resolve one critical vulnerability (CVE-2024-6990), which is an uninitialized use issue in Dawn; a high-severity out-of-bounds read in WebTransport (CVE-2024-7255); and insufficient data validation in Dawn (CVE-2024-7256). Apple [released](#) security updates to address vulnerabilities in Safari, iOS, iPadOS, macOS, watchOS, tvOS, and visionOS. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. Critical-severity [vulnerabilities](#) in ServiceNow's IT service management platform have reportedly exposed more than 100 organizations—including government agencies, data centers, energy providers, and software development firms. [CVE-2024-6980](#) in affected products can potentially expose organizations to server-side request forgery (SSRF) attacks. A verbose error-handling issue in the proxy service implemented in the GravityZone Update Server can allow an attacker to initiate SSRF attacks, potentially compromising the security of affected systems. The Cybersecurity and Infrastructure Security Agency (CISA) [released](#) nine Industrial Control Systems (ICS) advisories, six of which pertain to Johnson Controls.

Notable vulnerabilities:

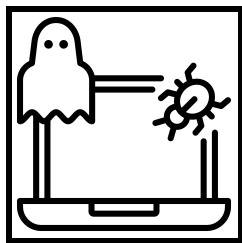
[CVE-2024-4879](#)

What happened: ServiceNow has addressed an input validation vulnerability that could enable an unauthenticated user to remotely execute code within the context of the Now Platform. ServiceNow applied an update to hosted instances and released the update to partners and self-hosted customers.

- **What this means:** This **CRITICAL**- severity vulnerability is being exploited by threat actors to steal email addresses, hashed passwords, and other sensitive data, potentially leading to compromise, data theft, and disruption of business operations.
- **Affected product:**
 - [ServiceNow](#) versions prior to the latest security patches released in July 2024



CVE-2024-37085



What happened: VMware ESXi contains an authentication bypass vulnerability. This bug has been marked **HIGH** and has a CVSS score of 7.2 out of 10. CISA added CVE-2024-37085 to its Known Exploited Vulnerabilities (KEV) Catalog on July 30.

➤ **What this means:** A malicious actor with sufficient AD permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group (“ESX Admins” by default) after it was deleted from AD. Researchers have [stated](#) that threat actors such as “Storm-0506,” “Storm-1175,” “Octo Tempest,” and “Manatee Tempest” have exploited this vulnerability. CISA has instructed the U.S. Federal Civilian Executive Branch (FCEB) agencies to protect their servers from this vulnerability, which has also been used in ransomware attacks.

➤ **Affected products:**

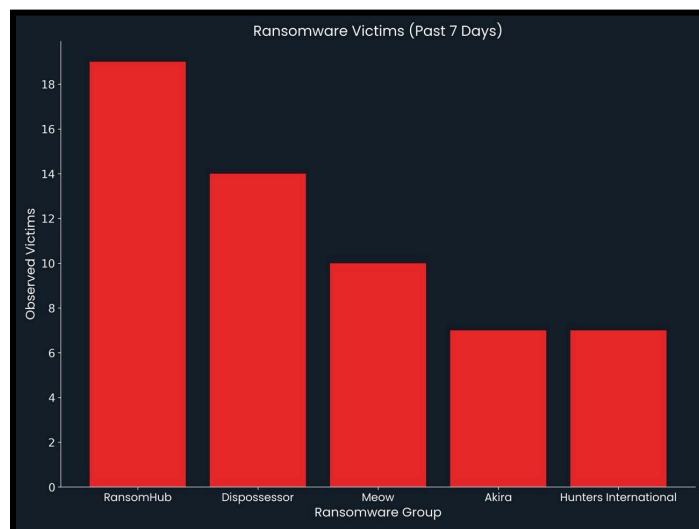
- VMware ESXi 8.0
- VMware ESXi 7.0
- VMware Cloud Foundation 5.x
- VMware Cloud Foundation 4.x

Ransomware and Breach Intelligence

| Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: Tangible Effects of Ransomware Attacks Felt Across Various Sectors

What happened: A ransomware attack reportedly [affected](#) the payment systems of about 300 small Indian banks, forcing them to shut down temporarily. The targeted company, C-Edge Technologies, is a banking technology solutions provider catering to the affected banks. OneBlood, a non-profit blood donation service, [confirmed](#) a ransomware attack that has forced the service to operate at a reduced capacity. Investigations have not concluded if any data was accessed or stolen. However, a spokesperson confirmed that one of the impacts of this attack could be that OneBlood's available inventory is affected. The City of Columbus, Ohio, is [investigating](#) the impact of a July ransomware attack that disrupted the city's services temporarily. Meanwhile, ransomware group "Dark Angels" reportedly [received](#) a record-breaking USD 75 million in ransom payments from a Fortune 50 company.

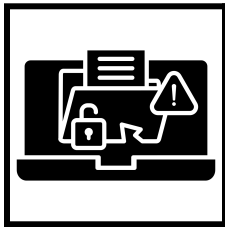


Source: ZeroFox Internal Collections

- **What this means:** Even though the ransomware attack targeted small banks in the country and affected only about 0.5 percent of India's payment system volumes, the effects on impacted customers can be significant. In such attacks, customers likely lose access to their accounts, face difficulties completing transactions, and experience delays in payroll deposits or bill payments. It can lead to financial distress, especially for those living paycheck to paycheck. Additionally, personal data might be compromised, increasing the risk of identity theft and fraud. Moreover, if the adversary successfully encrypts the exfiltrated data, it can use sensitive information, including PII, for further malicious attacks, like spear phishing, extortion, and financial scams. In June, the Reserve Bank of India (RBI), the Indian central bank, published an advisory regarding the cybersecurity of banks countrywide because of the increased risk of cyber threats to the Indian banking sector. "Banks should immediately put in place a cybersecurity policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board," RBI [said](#). According to an official [notification](#), the attack on OneBlood has affected the service's "software systems," causing it to rely on manual processes. OneBlood services around 250 hospitals;

switching to manual processes takes significantly longer and may also hinder many hospitals' capabilities in fulfilling emergency requirements. Although emergency procedures are in place, cyberattacks on healthcare facilities can have deadly consequences, as essential patient services like blood donations may place lives at risk. The ransomware attack on the city of Columbus paralyzed some of its public-facing services, including email services and IT connectivity between public agencies, which were rendered unavailable for some time. The attacks reflect how ransomware can have serious and tangible consequences on critical services, which can cause distress to the public.

Breach Intelligence: HealthEquity Data Breach Exposes Patient Information



What happened: HealthEquity, a Utah-based health savings account (HSA) provider, experienced a data breach affecting 4.5 million customers. The breach, originating from a third-party data repository, exposed various PII, including names, addresses, phone numbers, Social Security numbers, and dependent details. Initial access to the data occurred on March 9, but the breach was officially reported on June 26, with the attackers remaining undetected for just over two weeks. Additionally, Fresnillo PLC, a leading global [producer](#) of silver, gold, copper, and zinc, reported a recent cyberattack that compromised data on its systems. The company responded by initiating containment measures and is currently investigating the incident with the help of external forensic experts to assess the damage.

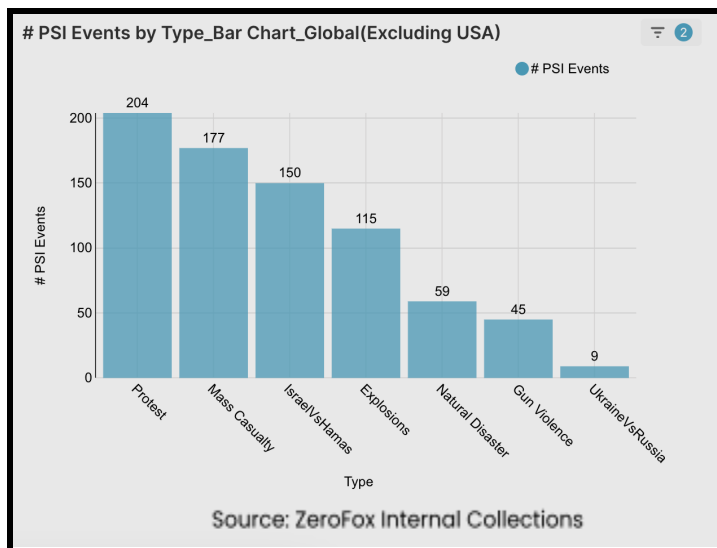
- **What this means:** HealthEquity's breach compromised a wide range of sensitive PII, which can facilitate identity theft and fraud. The attackers could leverage this data to open fraudulent accounts, apply for loans, or commit other forms of financial fraud. Additionally, the extensive personal details can be used for sophisticated social engineering attacks, deceiving individuals or organizations into divulging further sensitive information, potentially putting millions of individuals at risk. The delay in reporting the breach exploited a gap in monitoring or response protocols, potentially allowing the attackers to operate undetected during this critical period. The company cut down the adversary's dwell time by taking immediate action upon being alerted by a third-party vendor. With the healthcare industry under constant threat from hackers, CISA [released](#) a report last year highlighting various vulnerabilities in the healthcare sector that could be exploited by threat actors to breach systems and maintain persistent access. The HealthEquity attack comes at the heels of prominent ransomware attacks targeting the healthcare industry. Moreover, the technique of breaching companies via third-party vendors is gaining more traction among threat actors, as was [evident](#) from the Snowflake-related breaches.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 5 percent decrease in the Mass Casualty events this week, with the top three contributing countries being Israel, Palestine and Lebanon; approximately 74 percent of the events were Explosions. General alerts regarding the Israel-Hamas war (including protest, raids and involvement in neighboring countries) increased by 9 percent; notably, Israel and Palestine accounted for 37 percent of all the Explosions. Additionally, events related to Russia's war in

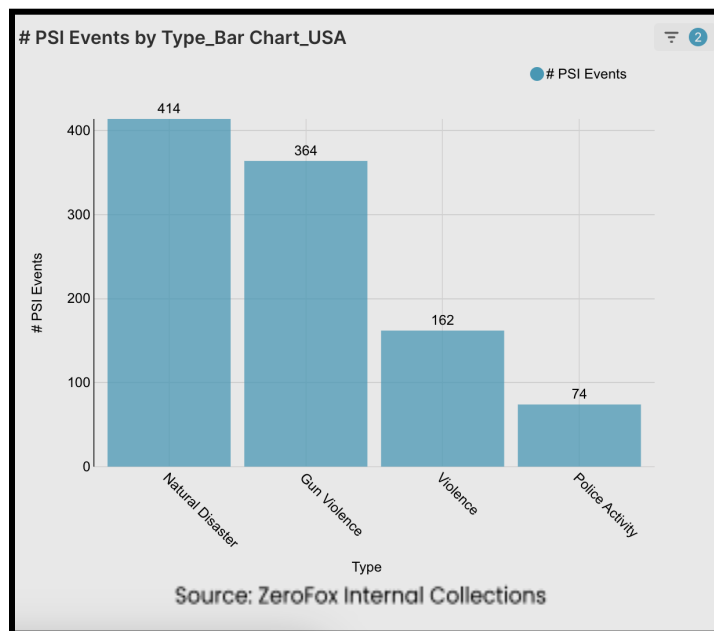


Ukraine decreased by a substantial 57 percent this week. The top three most alerted sub-types were Explosions, Gun Violence, and Natural Disaster; Explosions decreased by 18 percent, Gun Violence increased by 7 percent, and Natural Disaster also increased by 7 percent.

- **What this means:** Mass Casualty incidents decreased this weekend, as the two major contributors of the category—the Israel-Hamas and the Ukraine-Russia wars—both had fewer alerts pertaining to the subtype compared to last week. However, violence continued in both the conflicts. Israel reported multiple bombings over the week, killing and displacing a multitude of people on both the fronts. On Saturday, a missile struck the [Khadija School](#) in Deir Al-Balah, killing more than 30 people and injuring another 15 people. Over the course of the week, the two top commanders of Hamas and Hezbollah, backed by Iran, were killed in a span of 12 hours. Hamas chief [Ismail Haniyeh](#) was killed in Tehran, Iran, and Hezbollah commander [Faud Shukr](#) was killed following a large-scale attack on the capital city of Beirut in Lebanon. The Israeli Army took responsibility for Faud Shukr's death, along with several other casualties, and indicated it was in response to the targeted attack by Hezbollah in Golan Heights. The killing of Faud Shukr has plunged Lebanon into a state of proactive conflict and war; in light of this, multiple countries have now issued travel warnings cautioning their citizens to leave the country immediately. On the Eastern side of the world, Russia launched a large-scale drone attack targeting Kyiv on Wednesday. Ukrainian President Zelensky emphasized that the drone attack—the largest of its kind since the beginning of 2024—was successfully [thwarted](#) by Ukrainian forces without any

critical hits to infrastructure or loss of human life. The Paris Olympics began this week under security threats from multiple state and non-state actors. Hours before the beginning of the event, arsonists [attacked](#) France's high speed railway network by setting fire to cables that control the railway systems and disrupting the train services into the capital city. The attacks have been dubbed as a form of protest against the Paris Olympics. India has been witnessing torrential downpour this week in multiple parts of the country. The rains have caused a large landslide in [Wayanad](#), Kerala that killed approximately 150 people. In the northern part of India, cloud bursts have been reported that have caused flooding and infrastructural collapses. Gun violence this week showed an increase in the conflict-stricken areas and in parts of South America.

Physical Security Intelligence: United States



What happened: In the past week, the most alerted sub-types were Natural Disaster, Gun Violence, and Individual Violence. Illinois and California reported the highest number of Gun Violence incidents this week with 56 and 37 alerts, respectively, which comprised 24 percent of the alerts. The top two states contributing the highest number of alerts for Natural Disaster were California (75 alerts) and New York (44 alerts), and Natural Disaster incidents increased by 4 percent this week compared to last week. California and Texas reported the highest Police Activity incidents this week with 10 and

8 alerts respectively, decreasing the total percent from last week by 4 percent. Alerts relating to schools (excluding protests) decreased by 19 percent.

- **What this means:** Natural Disaster has become the most alerted subtype this week as well, with multiple [wildfires](#) and heat waves recorded over the past week. These wildfires have resulted in thousands being evacuated, as the fires have engulfed lands the size of some U.S. states. Wildfires are known to deteriorate air quality and trigger potential heat waves. A [heatwave](#) has been spreading from the central United States to the coasts on both sides; as per the advisories issued on Thursday, this heat wave is likely to worsen along the West Coast. These wildfires also have an economic [impact](#) on labor and productivity, as reports

have shown that increases in wildfires align with a proportionate increase in productivity losses. Gun Violence across the United States increased by 7 percent, and ZeroFox recorded 393 such alerts this month. Over the weekend, Chicago witnessed 21 incidents of shootings, and three people were killed in those shootings. A recent report [indicated](#) that Gun Violence has become the number one reason for the deaths of American teenagers—far more than diseases and car crashes. Despite being the number one murder weapon across the United States, guns still remain an integral part of U.S. culture. Individual Violence with 102 alerts showed a 2 percent increase compared to last week. Multiple instances of fatal stabbings were recorded in the past week; New York reported the largest number of stabbing incidents and accounted for almost half of the total share, especially in the boroughs of New York. Most of the remaining stabbing incidents are scattered across Los Angeles, Philadelphia, Minneapolis, and Tucson.

Interested in more ZeroFox Threat Intelligence? ZeroFox produces timely, relevant, and actionable [intelligence reporting](#) regularly to keep your team informed on developments in the threat landscape.

| 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%