



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

July 29, 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 July 26, 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 Assessment – Physical and Cyber Threats to Olympic Games Paris 2024	2
 Cyber Intelligence Key Findings	4
CrowdStrike-Related Outage Causes Global Chaos	4
NCA Infiltrates World's Most Prolific DDoS-for-Hire Service	5
New ICS Malware Targeting Critical Infrastructure	5
 Deep and Dark Web Intelligence Key Findings	8
Threat Actor Uses CrowdStrike Impersonations for Phishing Campaign	8
Rhysida Ransomware Targets LawDepot	8
INC Ransomware Targets Association Management Strategies	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-6802	11
CVE-2024-41110	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: Ransomware Attacks Target Key Industries and Critical Infrastructure	14
Breach Intelligence: Data Security Incidents Across the Globe	15
 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

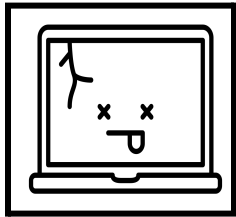
ZeroFox Intelligence Assessment – Physical and Cyber Threats to Olympic Games Paris 2024

France has a long history of civil unrest, and it is very likely that protests, boycotts, and other forms of disruptive activity will impact the Olympic Games Paris 2024. Interest groups could seek to leverage the visibility of the Olympics to garner more attention for their causes. Due to the significant social polarization and discontent extant in France, there are a number of activist groups potentially interested in this publicity. Authorities will begin enforcing movement restrictions and vehicle limitations. There will be 25 fan zone locations, where there will be parties and interactions with guests. Fan locations in zones designated as red or gray will need to download a "Pass Jeux" QR code in advance using their name, address, and a form of identification; these areas will have capacity restrictions and security checks. There will also be limitations on metro and rail services in and around Olympic venues, particularly around the opening ceremony. The most likely source of disruption to the Olympic Games Paris 2024 is physical protests in recent years, France has experienced many instances of unrest related to key political issues.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

CrowdStrike-Related Outage Causes Global Chaos

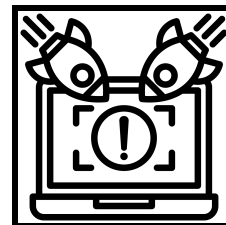


What happened: On July 19, 2024, CrowdStrike released a Rapid Response Content update for Windows sensors, which caused system crashes and the blue screen of death (BSOD) on systems running sensor version 7.11 and above. This update was meant to gather telemetry on new threat techniques but contained an undetected error. The problematic content was mistakenly validated and deployed due to a bug in the Content Validator. Upon loading, it [caused](#) an out-of-bounds memory read, leading to crashes. In an alert posted for customers soon after the outage, CrowdStrike said it was aware of “reports of crashes.” CrowdStrike’s engineering team identified the content deployment related to this issue and reverted those changes. ZeroFox [notes](#) that threat actors may seek to exploit the ongoing outages, including by taking advantage of stretched security infrastructure and performing attacks against targets that may otherwise draw quick attention and be identified. Scammers may also leverage the outage as a lure in social-engineering attacks. Attackers may continue targeting high-profile victims who have removed their endpoint detection and response (EDR) suite in response to the outage, thereby leaving them vulnerable. Meanwhile, ZeroFox Intelligence has [observed](#) threat actor “USDod” claiming to leak a database associated with CrowdStrike’s “entire threat actor list” on the predominantly English-language dark web forum BreachForums. The list allegedly contains 250 million scrapped Indicators of Compromise (IOCs) and will be released in two parts. The data includes aliases, target industries, target countries, and more.

- **What this means:** Windows has a large and global user base, which is why the outage has affected organizations and entities worldwide—including banks, news sites, healthcare institutions, and telecommunication companies. The impact extended to key airports, including Narita, Delhi, Edinburgh, and Sydney, with airlines calling for a “global ground stop” and issuing notices of potential disruptions. Additionally, threat actors abused this global outage by reportedly exploiting companies via data wipers (masquerading as an update from CrowdStrike) and remote access tools. The absence of a centralized workaround to address the outage prompted those affected to look for solutions online. Such panic-induced searches, as well as phishing emails promising mitigation measures, led victims to malicious websites that attempted to [steal](#) user credentials and infect systems with malware such as Lumma malware, which steals sensitive data like login details and browser histories. Cybercriminals will likely use the highly sensitive stolen info to access bank accounts, cryptocurrency wallets, emails, and other services. CrowdStrike has also [reported](#) an unidentified threat actor taking advantage of the update fiasco via a spear-phishing campaign targeting German customers. The campaign distributes fake installers through a website impersonating a German entity.

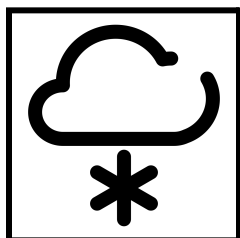
NCA Infiltrates World's Most Prolific DDoS-for-Hire Service

What happened: The UK National Crime Agency (NCA), along with other law enforcement (LE) agencies, infiltrated and disabled digitalstress[.]su, a major DDoS-for-hire service responsible for numerous global attacks. The agency disabled the actual site and created a mirror site, which directed users to a page that announced that their data had been collected by law enforcement.



- **What this means:** Distributed denial-of-service (DDoS) attacks are favored by hackers for their ability to disrupt and draw attention to social or political causes. DDoS-for-hire services operate by allowing users to purchase attacks, typically using online platforms or forums. These attacks flood a target's server with overwhelming traffic, rendering it inaccessible to legitimate users. The use of obscure domains like [.]su may have been an attempt to evade LE scrutiny, complicating efforts to track and mitigate such criminal activities. The operation led by the NCA and other LE agencies is crucial because DDoS-for-hire services pose significant threats to businesses and critical infrastructure worldwide. By dismantling digitalstress[.]su, LE agencies demonstrated the ability to penetrate sophisticated criminal networks, challenging the perceived anonymity of domains like [.]su. This takedown could hinder hackers' ability to launch large-scale DDoS attacks, potentially prompting them to seek alternative, less impactful methods to advocate for their causes.

New ICS Malware Targeting Critical Infrastructure



What happened: An energy company in Lviv, Ukraine, experienced a disruptive cyberattack early this year that used a new type of Industrial Control Systems (ICS)-focused malware dubbed "FrostyGoop." This malware is notable for being the first to employ Modbus TCP communications to target operational technology (OT) networks. FrostyGoop can manipulate ICS devices by reading and writing to their registers, affecting inputs, outputs, and configuration data.

- **What this means:** The discovery of FrostyGoop marks the emergence of the ninth known ICS-focused malware, underscoring a growing critical infrastructure threat landscape worldwide. Developing ICS-focused malware like FrostyGoop is exceptionally rare and difficult due to the specialized nature of ICSes and their stringent security measures. Crafting malware that can effectively interact with protocols like Modbus TCP requires deep technical expertise in both cybersecurity and industrial automation. By leveraging Modbus TCP, a widely used protocol in industrial environments, FrostyGoop malware poses a direct risk to the reliability and safety of ICS networks. Its ability to manipulate ICS devices

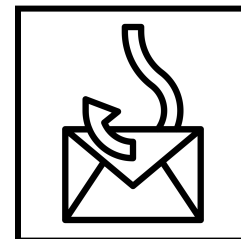
remotely underscores the potential for the type of severe operational disruptions in Lviv, where heating services to over 600 apartment buildings were disrupted for nearly two days. Furthermore, FrostyGoop's attribution to an unknown threat actor highlights the evolving landscape of cyber threats, where sophisticated tools like this can be deployed with strategic intent but without clear identification. In the underground world of cybercrime, access to new and sophisticated malware samples such as FrostyGoop is highly coveted. Malware developers and malicious actors seek these samples to study their mechanisms, adapt them for new attacks, or simply to gain prestige within their communities.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

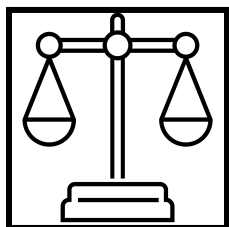
Threat Actor Uses CrowdStrike Impersonations for Phishing Campaign

What happened: On July 21, 2024, the Iran-based, pro-Palestinian threat actor group “Handala” claimed to have impersonated American cybersecurity company CrowdStrike in an email phishing campaign targeting several undisclosed Israeli companies. These emails contain a link for a malicious ZIP archive that, when executed, triggers a data-wiping attack against targeted devices' files. So far, Handala has allegedly extracted several terabytes of data from the victim organizations. Handala has also stated that if the Israel National Cyber Directorate (INCD) does not publish the list of affected organizations, the threat actor group will.



- **What this means:** This recent campaign targeting CrowdStrike users in Israel is a critical cybersecurity concern for organizations worldwide. This attack exploits the widespread disruption caused by CrowdStrike's recent faulty update, which affected millions of Windows systems globally. By impersonating CrowdStrike and offering fake fixes, the attackers are distributing malicious payloads, including data wipers and remote access tools. This incident highlights the importance of heightened vigilance during software-related crises, as cybercriminals often exploit such situations to target vulnerable organizations.

Rhysida Ransomware Targets LawDepot



What happened: On July 23, 2024, ZeroFox observed an update on the “Rhysida” ransomware leak site targeting LawDepot, an online service in which users can create and download personalized legal documents. Rhysida allegedly exfiltrated 5.5 terabytes of sensitive data from LawDepot, including SQL database backups; confidential customer information from multiple countries including credit card data, PayPal data, and legal documents; and full dumps of all associated LawDepot websites, internal passwords, and database certificates. The attack also allegedly compromised the internal LawDepot-wiki knowledge base and the company's full internal GitLab. Rhysida appears to be auctioning off the data to those looking to set up a similar business. It is asking 30 Bitcoin (approximately USD 2,000,000) for the data in addition to assistance with setting up the databases.

- **What this means:** This attack on LawDepot by Rhysida ransomware is a significant concern due to the massive amount of data compromised and the high ransom demand. These claims by Rhysida—a positive-reputation actor known for its sophisticated

techniques and double extortion tactics—are likely true, thus placing an alarming amount of customer financial and personal information at risk. The threat actor or user who wins the bid on the data will be able to utilize it to commit further malicious activity, to include phishing campaigns, Business Email Compromise (BEC), and potentially identity theft. Additionally, exposing the data specific to LawDepot’s internal operations will likely run the risk of corporate financial loss and reputational decline.

INC Ransomware Targets Association Management Strategies

What happened: On July 24, 2024, ZeroFox observed an update on the “INC” ransomware leak site targeting Association Management Strategies (AMS), a U.S.-based management company providing management expertise and administrative services. The post suggests that the ransomware group has at least 15 folders worth of compromised data, including HR files, engineering drawings, and potentially confidential client information. However, the exact amount of data is not specified. Additionally, while the post does not list a ransom demand amount, it lists AMS’s revenue as USD 5.5 million.



- **What this means:** This incident highlights the ongoing threat of ransomware attacks targeting businesses across various sectors. The breach exposes the vulnerability of service-oriented businesses that handle data for multiple clients, potentially leading to widespread impacts beyond the initial target. This attack serves as a stark reminder for organizations to prioritize cybersecurity measures, implement robust data protection strategies, and maintain up-to-date incident response plans. It also underscores the importance of secure data storage and access controls—especially for companies managing sensitive information for multiple clients or industry associations.

| 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, networking, and government security domains. Chip giant Nvidia has [released](#) patches for four vulnerabilities affecting many of its artificial intelligence (AI) and networking products. CVE-2024-0108 (CVSS score: 8.7/10.0) is a high-severity flaw in Jetson products [used](#) in robotics and embedded edge AI applications. CVE-2024-0101 (CVSS score: 7.5/10.0) can be [leveraged](#) in denial-of-service attacks, and CVE-2024-0104 (CVSS score: 4.2/10.0) can lead to improper access. Siemens has [addressed](#) two vulnerabilities in its Sicam power grid products: CVE-2024-37998 (CVSS score: 9.8/10.0), which lets attackers reset admin account passwords, and CVE-2024-39601 (CVSS score: 6.5/10.0), which allows unauthenticated attackers with physical access to downgrade the device firmware to a vulnerable version. Google has [released](#) Chrome 127, which introduces patches for 24 vulnerabilities. A vulnerability named PKFail can [allow](#) cybercriminals to run malicious codes while booting a system, which can further compromise the entire security chain, from firmware to the operating system. Digital workspace management platform ServiceNow has [fixed](#) CVE-2024-4879 (CVSS score: 9.3/10.0), which lets attackers conduct remote code execution on multiple versions of the Now Platform. Researchers have also observed other flaws affecting the platform, and threat actors are [using](#) publicly available exploits in attacks targeting government agencies and private firms in data-exfiltration attacks. CVE-2024-41110 (CVSS score: 10.0) is a critical issue that [enables](#) an attacker to exploit the Docker daemon by sending a specially crafted API request with a Content of 0, causing it to forward the request to the AuthZ plugin. CVE-2024-6802 (CVSS v3.1 score: 9.8/10.0), a vulnerability [found](#) in SourceCodester Computer Laboratory Management System 1.0., affects an unknown function of the file `/lms/classes/Master[.]php?f=save_record` and can allow SQL injection through the manipulation of the "id" argument. The Cybersecurity & Infrastructure Security Agency (CISA) has [added](#) two vulnerabilities in its Known Exploited Vulnerabilities (KEV) catalog. CVE-2012-4792 (CVSS score: 9.3/10.0) is a use-after-free bug affecting Microsoft Internet Explorer that [lets](#) remote attackers execute arbitrary code via a crafted website. CVE-2024-39891 is an information disclosure vulnerability in Twilio Authy API that [allows](#) an unauthenticated endpoint to accept a request containing a phone number and respond with information about whether the phone number was registered with Authy.

Notable vulnerabilities:

[CVE-2024-6802](#)

What happened: A vulnerability, which was classified as **CRITICAL**, was found in SourceCodester Computer Laboratory Management System 1.0. It affects an unknown function of the file `/lms/classes/Master.php?f=save_record`. The manipulation of the argument id leads to

SQLInjection. It is possible to launch the attack remotely. The exploit has been disclosed to the public.



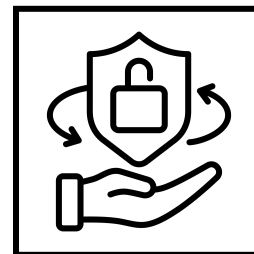
- **What this means:** The product [constructs](#) all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks or to insert additional statements that modify the back-end database, possibly including execution of system commands.

- **Affected product:**

- SourceCodester Computer Laboratory Management System 1.0

[CVE-2024-41110](#)

What happened: Docker issued critical security updates for a vulnerability reintroduced in later versions after being fixed in v18.09.1 (Jan 2019). The fix was reportedly not carried forward in some later versions, thus leading to the bug [resurfacing](#) in April 2024. The flaw (CVE-2024-41110) could let attackers bypass AuthZ plugins. Patches were released recently for all supported versions, addressing a potential five-year exposure period.



- **What this means:** This security lapse allowed attackers a significant window of five years to potentially exploit Docker instances by manipulating API requests. CVE-2024-41110 is a **CRITICAL**-severity vulnerability (CVSS score: 10.0) in Docker Engine. It enables attackers to exploit a flaw by sending API requests with a Content-Length of 0, deceiving the Docker daemon into mishandling requests forwarded to the AuthZ plugin. Normally, API requests contain essential data within their bodies that AuthZ plugins analyze to enforce access controls, making this oversight particularly risky. An attacker can potentially bypass authorization controls, gaining unauthorized access to Docker instances and compromising sensitive data or deploying malicious containers.
- **Affected products:**
 - Docker-ce versions v19.03.15 and lower, v20.10.27 and lower, v23.0.14 and lower, v24.0.9 and lower, v25.0.5 and lower, v26.0.2 and lower, v26.1.4 and lower, v27.0.3 and lower, and v27.1.0 and lower.

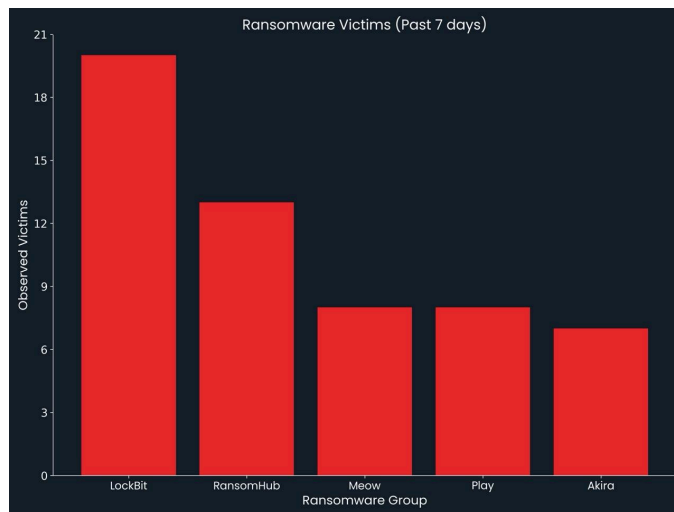
| Ransomware and Breach Intelligence |

| Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: Ransomware Attacks Target Key Industries and Critical Infrastructure

What happened: A recent ransomware attack on [MediSecure](#), an Australian electronic prescription service provider, has resulted in the theft of 6.5 terabytes of sensitive data, impacting up to 12.9 million Australians (about half of Australia's population). Efforts to reconstruct the affected server from a backup were successful, but the identification process is ongoing due to the sheer volume of data. A North Korean individual [linked](#) with several ransomware attacks against American healthcare providers, NASA, U.S. military bases, and international entities was recently indicted. A joint cybersecurity [advisory](#) highlights the activities of this state-sponsored group, targets, and tactics. Meanwhile, in the United (UK), researchers have [observed](#) that there is an upward trend in ransomware and phishing attacks against critical national infrastructure. A large number of organizations in the central government, civil aviation, energy, transport, and finance departments are being affected by data compromise and loss arising from ransomware attacks. Additionally, security researchers [discovered](#) that the North Korea-linked threat group dubbed "APT45" has now moved on to more financially motivated cybercrimes by deploying ransomware families like SHATTEREDGLASS and Maui targeting entities in South Korea, Japan, and the United States.

- **What this means:** In the Australia prescription provider attack, researchers have observed that a sample of the stolen data was posted on the dark web by the threat actor behind the attack. Initially priced at USD 50,000, the data was marked as sold and has since been re-listed by the buyer at a discounted price of USD 25,000. This indicates that the stolen information is actively being traded and potentially misused. The Australian National Cyber Security Coordinator has issued a warning to all affected individuals about the increased risk of scams and misuse of their data. The indictment of the North-Korea linked individual may lead to sanctions that could deter future ransom-based cyberattacks, especially on vital services like hospitals. However, the attacks, driven by North Korea's need to fund military and nuclear ambitions amidst international sanctions, indicate that such politically



Source: ZeroFox Internal Collections

motivated threat actors pose a significant risk to American critical infrastructure. Research delving into the UK's critical infrastructure security reveals ransomware incidents that have had implications for the nation and its civilians' safety, such as disrupting transportation facilities, slowing down financial services operations, and exposing civilian personally identifiable information (PII). Research also highlights threats from nation-state hackers were exacerbated by the relatively slow response time in de-escalating ransomware incidents.

Breach Intelligence: Data Security Incidents Across the Globe



What happened: A data breach from 2022 [exposed](#) private member information from the BreachForums v1 hacking forum. This leak allowed both threat actors and researchers to access details about its users. The complete database has [reportedly](#) been released on Telegram, exposing a vast amount of data. This includes members' information, private messages, cryptocurrency addresses, and every post made on the forum. Although the database had been shared with sources previously, it was not publicly

released until recently. Leidos Holdings Inc., one of the largest IT services providers of at least three U.S. government entities, has [suffered](#) a breach in which actors stole some internal documents. University of Michigan Medicine recently [informed](#) over 56,000 people that their protected health information was exposed. The breach involved unauthorized access to three employee email accounts between May 23 and May 29, 2024. Red Art Games, a well-known publisher and distributor of limited-edition [video games](#), experienced a cyberattack that exposed sensitive customer information. The company publicly announced the breach on July 25, 2024, through its official social media channels. On July 25, the threat actor USDoD claimed to have [leaked](#) data associated with two Mexican political parties on the predominantly English-language dark web forum BreachForums. The leaked data includes full names, voter IDs, addresses, dates of birth, and more. The Land Registry agency in Greece [experienced](#) a data breach after a series of 400 cyberattacks targeting its IT infrastructure. Hackers accessed employee terminals and stole 1.2 gigabytes of data. The stolen data mainly includes administrative documents and does not contain personal information about citizens. The agency expects that the breach will not affect its operations.

- **What this means:** Threat actors exploit stolen information in various ways, including identity theft, financial fraud, and unauthorized access to sensitive accounts. They may sell the data on dark web markets, use it to craft targeted phishing attacks, or commit further cybercrimes. Stolen personal and financial details can lead to significant financial losses and reputational damage for both individuals and organizations. Additionally, the high value of personal data on the black market also incentivizes hackers to persist in their attacks, making data breaches a constant and evolving threat in the digital age. Data

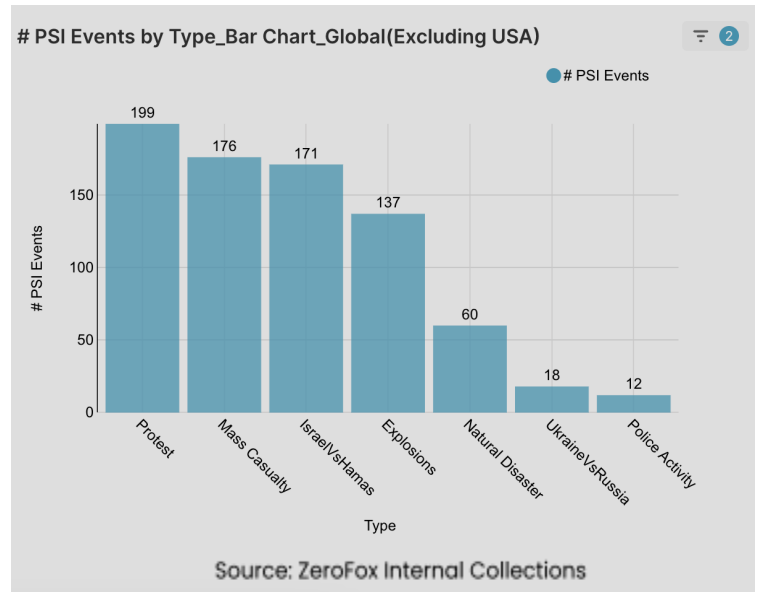
breaches have become increasingly common due to the growing sophistication of threat actors and the expanding digital landscape. As more personal and sensitive information is stored online, attackers find more opportunities to exploit vulnerabilities in systems and networks. Advanced hacking tools, social engineering techniques, and the proliferation of malware make it easier for cybercriminals to target organizations.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

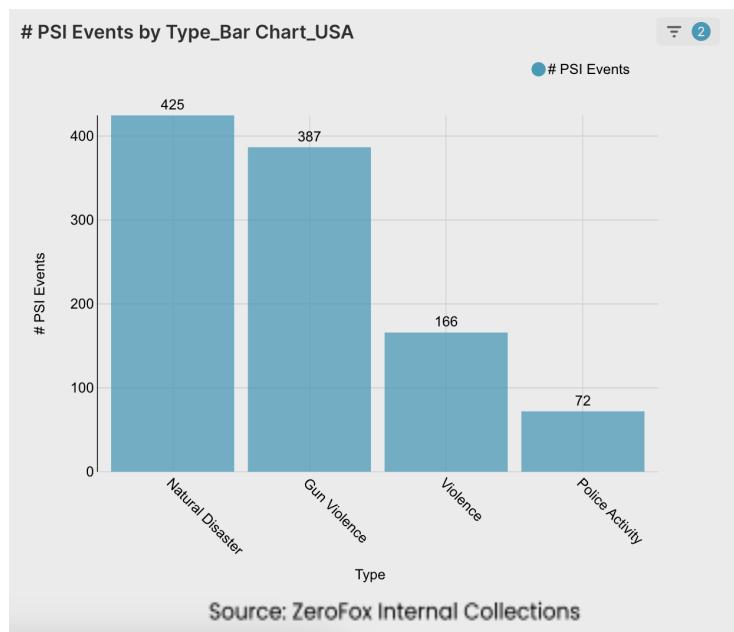
What happened: Excluding the United States, there was a 25 percent increase in Mass Casualty incidents compared with the previous week, with the top three contributing regions being Israel, Palestine, and Lebanon respectively; 82 percent of these events were Explosions. General alerts pertaining to the Israel-Hamas war (including protests, raids, and involvement in neighboring countries) increased by 6 percent this week. Palestine and Israel accounted for 72 percent of all international Explosions alerts. Additionally, events related to Russia's war in Ukraine showed an uptick of 46 percent. The top three most-alerted subtypes this week were Protest, Explosions, and Natural Disaster. Protest and Explosions increased by 9 percent and 24 percent this week, while Natural Disasters decreased by 20 percent.



- **What this means:** The world this week saw a heightened increase in mass-casualty incidents perpetrated by elements across the globe. Bombings in warring regions persisted and lives continued to be lost as the wars continued, with the latest being an explosion using a home-made bomb at the [Qalandia Checkpoint](#). This week we also witnessed an alleged attack by the Israeli Army on the Yemen Petroleum Company in the [Hodeidah port](#). The strike destroyed the oil storage units and also endangered the Yemeni aid ships in the harbor. The fire was ablaze for two days, and six people were killed in the incident. Russia's war against Ukraine continued with cross-border bombings and artillery shellings. Multiple infrastructure collapses and human lives were lost this week, similar to the previous week. Along with the usual targets, a Ukrainian grain silo near the [Romanian border](#) was targeted by *Shaheed* drones on July 24. The United States has issued a statement indicating it will help its NATO ally, Romania, to [investigate](#) the crash of the drone. Violent protests in Dhaka against the reservation system have calmed down after the apex court ordered to [modify the verdict](#) in accordance with the demand of the protestors. Nearly 100 people lost their lives in the deadly protest. Among heightened [security measures](#), the Paris Olympics will be held for 17 days across 35 different venues starting July 26. In a video post, [Hamas](#) has issued threats promising violence during the Games. Even though not as huge during its peak, the [ISIS K's atrocities](#) in Russia have also

sparked considerable concern regarding possible attacks during the Games. Additionally, many state-sponsored elements may also resort to violence during the Games this year. The Olympics is no stranger to terror attacks; it has dealt with them before in the 1972 Munich Olympics attack and the 1996 bombing at the Atlanta Olympics. However, considering the geopolitical state of the world at the moment, it is possible that many actors will be looking to make the Paris Olympic Games into a venue to imprint their own personal agendas.

Physical Security Intelligence: United States



What happened: In the past week, the most alerted subtype was Natural Disaster, Gun Violence, and Individual Violence. Illinois and California once again reported the highest number of Gun Violence incidents, with 52 and 39 alerts, which accounted for nearly a quarter of the alerts. The number of Gun Violence alerts this week was the same as last week. The top two states contributing to Natural Disasters were California and Florida, with 91 and 43 alerts, respectively. Natural Disasters this week have shown a 6 percent decrease compared with the previous week. Illinois and California were the

top two contributing states for police activity this week, and Police Activity across the country as a whole remained the same as last week. There were 22 alerts relating to schools, excluding protests, a 15 percent decrease from last week.

- **What this means:** Similar to last week, this week saw Natural Disasters remaining the top alerted subtype. A decrease in tornadoes across the United States was seen compared with last week. Most of the alerts pertaining to this subtype have been wildfires, house fires and commercial fires; all three have been on the rise, as seen last week. This week has been comparatively calm for the United States. Most of the subtypes have stayed the same or have decreased compared with the previous week. A majority of the important developments in the country this week occurred on the political front. President Joe Biden [dropped out](#) of the presidential race and endorsed Vice President Kamala Harris to run on

the Democratic ticket for the role. This announcement comes weeks before the [Democratic National Convention](#), which is scheduled to take place in the latter half of August. In addition, on July 24, Israeli Prime Minister Benjamin Netanyahu addressed a [joint meeting](#) of the U.S. Congress, during which a large gathering protested the Israel-Hamas war outside the Capitol. Prime Minister Netanyahu is expected to meet with President Biden and Vice President Harris on Thursday and former President Donald Trump on Friday as a part of his visit to the United States.

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%