



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

July 22, 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 19, 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
ZeroFox Intelligence Flash Report – U.S.-Led Trade Restrictions Likely to Increase Espionage Threat	2
 Cyber Intelligence Key Findings	5
WazirX Cryptocurrency Exchange Loses USD 230 Million in Major Security Breach	5
IDF Computer Chief: Three Billion Cyberattacks Against Israel Since Beginning of War	5
Iranian Hackers Deploy New BugSleep Backdoor in Middle East Cyberattacks	6
 Deep and Dark Web Intelligence Key Findings	8
U.S.-Based IT Consulting Firm Target of Ransomware Attack	8
NullBulge Leak Site Targets the Walt Disney Company	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-39911	11
CVE-2024-20419	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: Ransomware Attacks Continue Amid Changes in the Landscape	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

The Olympic Games Paris 2024 (also referred to as the Olympics, Paris 2024, and the Games) is a highly visible, worldwide event that could be targeted by a variety of actors, both domestic and international, to bring attention to their causes. Physical disruption via strikes or protests are the major on-the-ground threat to the Games; cyberattacks sponsored by Russia are the major cybersecurity threat. Domestically, multiple unions have threatened strikes, anticipating that their local and national governments will feel sufficient pressure to hold a successful Paris 2024 that they will quickly give in to demands. The unions' resolve is reinforced by the recent French elections, in which a left-leaning coalition known to be supportive of workers won a plurality in the National Assembly. Local protest groups have also called for action ahead of and during the Games. These include organized campaigns by activists during events and disorganized Paris-area opposition to the Games. The polarization in French society—heightened by recent elections and protest movements—creates fertile ground for further social unrest during the Games and makes it very likely there will be disruptions. Internationally, both the war in Ukraine and the Israel-Hamas conflict have the potential to inspire protests and disruptions by nation-state-level actors. In particular, the Russian Federation has a history of targeting the Olympics with cyberattacks as revenge for its formal exclusion from the Games (such as in the Pyeongchang Winter Olympics). With Russian athletes once again slated to compete under the "Olympic Athletes from Russia" banner and the added factor of France's continued support for Ukraine, Kremlin-aligned hackers are likely to take aim at the cyber infrastructure of Paris 2024. Lastly, pure financial crimes—including internet scams and street-level petty crime—will very likely operate on a heightened level during the Games. Tourists in Paris should be wary of their surroundings and conduct due diligence on websites and applications they use related to the Games.

ZeroFox Intelligence Flash Report – U.S.-Led Trade Restrictions Likely to Increase Espionage Threat

Some of the world's largest technology companies and global stock markets plummeted in value on July 18, likely because the United States is seeking to enforce a rarely-used rule allowing it to prohibit sales of any foreign-made product with at least some U.S.-made materials to China. Restricting access to advanced technologies will likely put China at a competitive disadvantage when it comes to producing emerging technologies vital to its trade-based economy, as well as weapons systems needed for national security. China is very likely to retaliate with its own trade restrictions against companies and states that comply with the U.S. restrictions. Chinese-backed cyber threat actors are

very likely to increase cyber espionage against entities that produce the withheld technology with the goal of China creating its own endogenous industries.

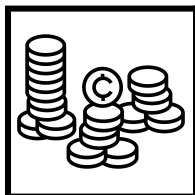
ZeroFox Intelligence Flash Report – Global IT Outages Causing Significant Disruption to Multiple Industries

On July 18, 2024, a global Information Technology (IT) outage caused significant disruption to industries around the world, with thousands of Windows workstations and servers displaying a fatal system error message commonly referred to as the “blue screen of death.” The incident reportedly impacts Windows hosts that have installed CrowdStrike’s Falcon Sensor service; it does not affect all Windows devices. At the time of writing, the cause of the outage is not being treated as a cyberattack and is instead most likely to be a faulty or incorrectly deployed security update or a faulty channel file. The outage is known to have affected Windows devices across the world, with a significant impact across multiple industries—including, but not limited to—Energy, Finance, Healthcare, Media, Retail, and Travel. The current workaround provided by the vendor requires a physical presence at each device and almost certainly cannot be deployed remotely.

| Cyber Intelligence |

Cyber Intelligence Key Findings

WazirX Cryptocurrency Exchange Loses USD 230 Million in Major Security Breach

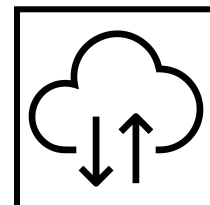


What happened: WazirX, one of India's leading cryptocurrency exchanges (owned by Binance), experienced a security breach involving one of its multi-signature (multisig) wallets. This breach led to the temporary suspension of both Indian rupee and cryptocurrency withdrawals. Approximately USD 230 million worth of assets were transferred suspiciously from the affected wallet.

➤ **What this means:** Cryptocurrency regulations in India are still evolving, and security incidents like this could attract increased regulatory scrutiny. Regulators may impose new requirements on exchanges to enhance security measures, potentially impacting how exchanges operate and users engage with cryptocurrencies. As one of India's largest crypto exchanges, disruptions at WazirX can potentially impact market stability and investor sentiment. Price volatility and trading volumes could be influenced as traders react to the news and adjust their positions. Despite WazirX utilizing features like multisig (technology designed to require multiple keys or signatures to authorize transactions) for security, threat actors could conduct an attack in one of its wallets. The threat actors might have compromised one of the signing keys through phishing attacks or social engineering, gaining enough control to authorize transactions. Initial investigations suggest the incident may be linked to North Korean threat actors, which adds a geopolitical dimension to the cyberattack. These actors leverage cyberattacks to circumvent international sanctions and acquire funds for illicit purposes. This dual threat of financial crime and geopolitical instability underscores the complexity and global impact of cybersecurity breaches in the cryptocurrency sector.

IDF Computer Chief: Three Billion Cyberattacks Against Israel Since Beginning of War

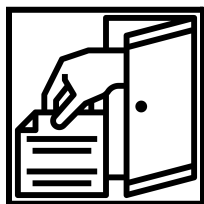
What happened: The Israel Defense Forces' (IDF) cloud-computing network experienced over three billion cyberattacks following the outbreak of war between Israel and Hamas on October 7, 2023, but all of the attacks were successfully intercepted and reportedly did not result in significant damage. These attacks targeted operational cloud systems used by troops during combat, aiming to disrupt information-sharing and reveal the location of forces. Despite the intensity and volume of these attacks, IDF's defenses remained uncompromised. The IDF had to manage system overloads due to increased usage from reservists and the need for additional



computing resources, leading to the establishment of an extra data center.

- > **What this means:** The Israel-Hamas conflict is not only physical but also extends to cyberspace, impacting civilians more than combatants. Cyber warfare scholars have [found](#) that cyberattacks primarily harm civilians by causing psychological distress and fueling violence. Even though strong cybersecurity measures enabled interception of the attacks, the volume of attacks reflects the volatile cyber threat environment during wartime—particularly from adversaries like Iran, whose cyber operations have become more aggressive. On the other hand, Hamas’ cyber activities range from espionage to disruptive attacks on Israeli systems, which are supported by Iran and hacktivists worldwide. These attacks aim to terrorize rather than achieve military objectives. During the Oct. 7, 2023, attack, Hamas used cyber techniques like phishing and false alerts to assist its operations. However, its cyber effectiveness has since waned, and Hamas has pivoted to misinformation campaigns and distributed denial-of-service (DDoS) attacks.

Iranian Hackers Deploy New BugSleep Backdoor in Middle East Cyberattacks



What happened: Iran-linked “MuddyWater” has been observed deploying a new backdoor dubbed BugSleep in its recent campaigns. The group conducts phishing campaigns and establishes persistence by deploying legitimate remote monitoring and management (RMM) software. The use of legitimate software has now reportedly been replaced by a new backdoor that can help threat actors evade detection by “blending in with legitimate network traffic.”

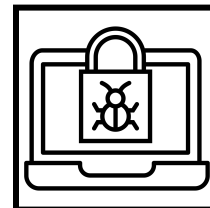
- > **What this means:** According to researchers, attackers using this new strain of malware focus on a wide range of targets globally, including Israel and some in Turkey, Saudi Arabia, India, and Portugal. MuddyWaters has also been observed targeting entities like government organizations, airlines, media outlets, telecommunications, and oil industry organizations. The threat group is reportedly shifting its attack tactics to better evade detection since the RMM software it uses is legitimate and subject to regular monitoring. These precautions reflect MuddyWater’s persistence in its phishing campaigns, making future campaigns likely to be more dangerous given the group’s attack sphere and methodologies.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

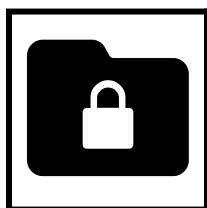
[U.S.-Based IT Consulting Firm Target of Ransomware Attack](#)

What happened: On July 15, 2024, ZeroFox observed an update on the “BianLian” ransomware leak site targeting Preferred IT Group, a U.S.-based information technology (IT) consulting and managed services firm. ZeroFox has detected close to 100 victims of ransomware and digital extortion in the technology sector in the past year, close to 50 percent of which are in the U.S.-Canada region.



- **What this means:** The leak—which exposed sensitive databases, technical data, customer information, and business correspondence—highlights the severe repercussions of cyberattacks on data integrity and confidentiality. For a technology service provider, the breach not only jeopardizes operational continuity but also triggers potential regulatory violations, depending on the nature of compromised data. The incident threatens such providers’ reputation and client trust, necessitating swift response measures including thorough investigation, notification of affected parties, and bolstering of cybersecurity defenses. When managed services are attacked through ransomware, it highlights the risks associated with third-party risk management.

[Texas Alcohol and Drug Testing Service Attacked by BianLian](#)



What happened: On July 15, 2024, ZeroFox observed an update on the BianLian ransomware leak site targeting Texas Alcohol and Drug Testing Service (TADTS), a U.S.-based drug testing company that provides workplace testing and individual testing services. ZeroFox has detected close to 110 victims of ransomware and digital extortion in the healthcare sector in the past year, close to 75 percent of which are in the U.S.-Canada region.

- **What this means:** The BianLian ransomware attack on TADTS represents a critical cybersecurity incident for those in the healthcare and drug testing sectors. The breach is alarming for several reasons. Hackers claim to have accessed a vast amount of TADTS’s data, including sensitive information such as financial records, human resources data, personally identifiable information (PII), protected health information (PHI), drug test results, and email correspondence. TADTS’s compromised integrity could undermine trust in drug-testing services and jeopardize workplace safety programs across various industries. Moreover, the exposure of PII and PHI raises serious regulatory concerns under laws like HIPAA, potentially subjecting TADTS to significant fines and legal repercussions. The incident threatens severe damage to TADTS’s reputation—critical for an organization

handling sensitive health data. It also illustrates the evolving sophistication of ransomware threats, highlighting vulnerabilities in supply chains and the broader implications for data security practices.

[NullBulge Leak Site Targets the Walt Disney Company](#)

What happened: On July 16, 2024, ZeroFox observed an update on the “NullBulge” leak site targeting The Walt Disney Company, a U.S.-based mass media and entertainment company. The threat actor alleges that it has obtained 1.1 terabytes (TiBs) of data from Disney’s internal Slack account, including messages and files from nearly 10,000 channels. This data purportedly includes unreleased projects, raw images and code, login credentials, and links to internal APIs and web pages. Additionally, the post also mentions that NullBulge had an “insider man” at Disney aiding in the threat actor’s compromise of the company; however, according to the post, the individual backed out and kicked the threat actor out of the system. NullBulge has now threatened to doxx the individual online.



- **What this means:** The breach of Disney’s IT systems by NullBulge highlights the dual threat of external cyberattacks and insider risks. The mention of a Disney employee offering assistance and then backing out underscores how insiders with access can exploit vulnerabilities, compromising sensitive data like internal communications and personal information. This incident not only jeopardizes data security and integrity but also disrupts business operations, potentially exposing strategic plans and damaging trust with partners. It serves as a clear reminder of the need for organizations to bolster cybersecurity measures against both external threats and insider risks through robust defenses, vigilant monitoring, and a culture of cybersecurity awareness.

| 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. SolarWinds has [fixed](#) eight critical vulnerabilities in its Access Rights Manager (ARM) software, six of which could allow attackers to [conduct](#) remote code execution (RCE) on vulnerable devices. Meanwhile, the [CVE-2024-20419](#) vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) poses a significant risk, as it enables unauthenticated, remote attackers to change passwords of any users—including administrative ones. Another critical flaw, CVE-2024-39841, affects [Centreon](#), allowing remote attackers to execute arbitrary code after authentication due to improper validation of user-supplied strings in the testServiceExistence function. Additionally, the [CVE-2022-21587](#) vulnerability in Oracle Web Applications Desktop Integrator of Oracle E-Business Suite permits unauthenticated network attackers to compromise the system via HTTP, potentially leading to a full takeover. Some threat actors have been [exploiting](#) available proof-of-concept (PoC) vulnerabilities rapidly, often within 22 minutes of public release, with notable targets including vulnerabilities in Apache products, ColdFusion, and MobileIron. Furthermore, the [CVE-2024-37381](#) vulnerability in Endpoint Manager (EPM) 2024 flat's Core server can be exploited by authenticated attackers with network access to execute arbitrary code through SQL injection, posing a severe security risk. The Cybersecurity and Infrastructure Security Agency (CISA) has also [added](#) some vulnerabilities—including CVE-2024-34102 [Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability] and CVE-2022-22948 (VMware vCenter Server Incorrect Default File Permissions Vulnerability)—to its Known Exploits and Vulnerability (KEV) catalog.

Notable vulnerabilities:

[CVE-2024-39911](#)



What happened: IPanel, a web-based Linux server management control panel, contains an unspecified SQL injection via User-Agent handling. This **CRITICAL** vulnerability has a CVSS score of 10. This issue has been addressed in version 1.10.12-Its.

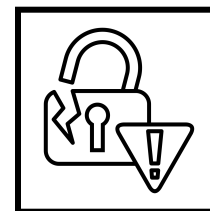
➤ **What this means:** The vulnerability in IPanel allows attackers to execute SQL injection attacks through the handling of User-Agent data. This critical flaw potentially allows attackers to gain unauthorized access, manipulate databases, and compromise sensitive information. Users are urged to update to version 1.10.12-Its immediately to mitigate these risks and secure their systems against exploitation.

➤ **Affected product:**

- v1.10.10-Its

CVE-2024-20419

What happened: This flaw is exploitable through crafted HTTP requests and requires no privileges or user interaction, significantly impacting system integrity, availability, and confidentiality. Affected products include SSM On-Prem and SSM Satellite. The flaw has been rated **CRITICAL** (CVSS score of 10.0).



- **What this means:** The vulnerability's severity, marked by its maximum CVSS score, necessitates immediate patching to prevent potential exploitation by malicious actors targeting network infrastructure vulnerabilities. Organizations using SSM On-Prem—especially in the financial, utility, service, and government sectors—should prioritize this update to prevent potential exploitation and since no workaround is available.
- **Affected products:**
 - Cisco SSM On-Prem
 - Cisco Smart Software Manager Satellite (SSM Satellite)

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

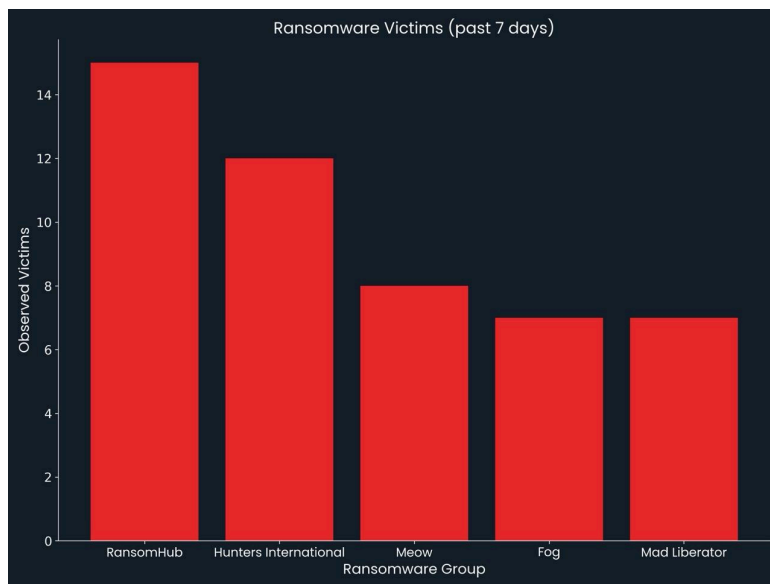
Ransomware Intelligence: Ransomware Attacks Continue amid Changes in the Landscape

What happened: In the healthcare industry,

Rite Aid is [investigating](#) a recent cyberattack, which was claimed by the “RansomHub” ransomware group. The company confirms that no “Social Security numbers, financial information, or patient information” were affected by the cyberattack. Meanwhile, boat dealer MarineMax has started [notifying](#) more than 123,000 individuals about a data breach that resulted from a ransomware attack earlier this year. The French government’s cybersecurity agency has [stated](#) that ransomware attacks will be “inevitable” during the upcoming Paris Olympics. The ransomware threat landscape has witnessed some significant changes in the

past week. Cybersecurity researchers have [observed](#) threat actor group “Scattered Spider” (known for targeting Las Vegas casinos last year) adopting RansomHub and Qilin ransomware variants. The “SEXi” ransomware group, notorious for attacking VMware ESXi servers, has [rebranded](#) itself as “APT INC” and has launched numerous attacks on organizations recently. Beginning in February 2024, these threat actors have used the leaked Babuk encryptor to attack VMware ESXi servers and the leaked LockBit 3 encryptor to target Windows systems. In other news, a report has [stated](#) ransomware attacks on oil and gas companies and utilities have not decreased over the past year, even though there has been a general decline in the number of such attacks globally. Not only has the frequency of attacks on critical infrastructure in these sectors remained steady, but the consequences for the affected companies have also worsened.

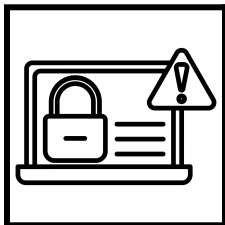
- **What this means:** A dark web post by the RansomHub group [claims](#) it stole 10 gigabytes of data from Rite Aid, including customer ID numbers and rewards numbers. RansomHub appears to focus on data-theft-based extortion rather than encrypting files to demand ransom payments. Rite Aid reportedly ended negotiations with the threat group, prompting RansomHub to threaten to leak the data in two weeks. MarineMax is one of the world’s largest recreational boat sellers. A data breach of a significantly large scale, affecting more than 123,000 customers and employees, creates opportunities for identity theft and



Source: ZeroFox Internal Collections

fraud, potentially causing financial harm to affected individuals. Additionally, the stolen data can be leveraged for future cyberattacks, including phishing scams and targeted malware distribution, exploiting the compromised information to gain unauthorized access to accounts or perpetuate further breaches. The Paris Olympics stands as a viable target for threat actors with a myriad of motives, including political and financial. Besides the identified Russian hacktivist threat, ransomware attacks are probable during the event; threat actors are likely to target victims in ticketing, extortion, and double extortion scams. APT INC's rebranding denotes a persistent ransomware operation targeting enterprise environments with secure encryption methods, leading to potentially significant financial and operational impacts for victims. The use of leaked encryptors highlights a broader issue within the cybersecurity landscape, where disseminating such tools can facilitate the rise of new and dangerous ransomware groups—thereby signaling a shift in the ransomware scene. The shift has become more evident after law enforcement took down "ALPHV/BlackCat" and the standing ransomware-as-a-service (RaaS) groups initiated a recruiting drive for the best affiliates. Last month, RansomHub [recruited](#) Scattered Spider into its ranks. As a result, Scattered Spider is actively using RansomHub's artillery, signifying RansomHub's growing popularity in the cybercrime landscape. Moreover, this shift reflects the increasing sophistication and effectiveness of these new ransomware families, which are now favored over older variants like ALPHV/BlackCat.

Breach Intelligence: Data Security Incidents Across the Globe



What happened: This week, there have been multiple data breach incidents reported from the United States and other countries around the globe. AT&T has [alerted](#) its customers and partners of a data breach, wherein adversaries illegally accessed customer data from its workspace and downloaded it onto a third-party cloud platform. The breached data included phone call and text message records of "nearly all" AT&T cellular customers from May 2022 to October 2022 and January 2023. Rite Aid is conducting an [investigation](#) into a recent cyberattack that was claimed by the RansomHub ransomware group. A dark web post by the group claims they stole 10 GB of data, including customer ID numbers and rewards numbers. ZeroFox intelligence has observed threat actor "888" claiming to have leaked a database allegedly associated with [BMW](#) customers located in Hong Kong on BreachForums. The leaked data supposedly includes salutations, surnames, first names, mobile numbers, and opt-out SMS preferences. Threat actor NullBulge claimed to have leaked a database associated with [Disney](#) on dark web forum BreachForums. The threat actor allegedly gained access to Disney's internal Slack, which exposed 1.1 TB of data—including almost 10,000 channels, messages and files, unreleased projects, raw images and code, some logins, and links to internal APIs/web pages. Hacktivists have reportedly stolen and leaked more than 300 GB of data from spyware maker [mSpy](#). The breached data includes 142 GB of user data and support tickets, 176 GB of attachments, and 2.4 million

unique email addresses. The data leak reportedly occurred as a result of a breach in a specific account linked to a customer-support system. A threat actor known as "emo" accessed over 15 million Trello (a web-based project management tool owned by Atlassian) account email addresses using an unsecure API in January. The adversary has also been observed to have claimed to leak a database allegedly containing personal information of over half a million users of [Life360](#), a family safety and location-sharing app, on the dark web. [MarineMax](#), one of world's largest retailers of recreational boats and yachts, has begun informing more than 123,000 individuals that their personal information was compromised in a [March](#) cyberattack reportedly claimed by the "Rhysida" ransomware group. Fractal ID, a blockchain identity [platform](#), disclosed a possible data breach detected on July 14. An unauthorized third party gained access to an operator's account and executed an API script to retrieve personal data of users.

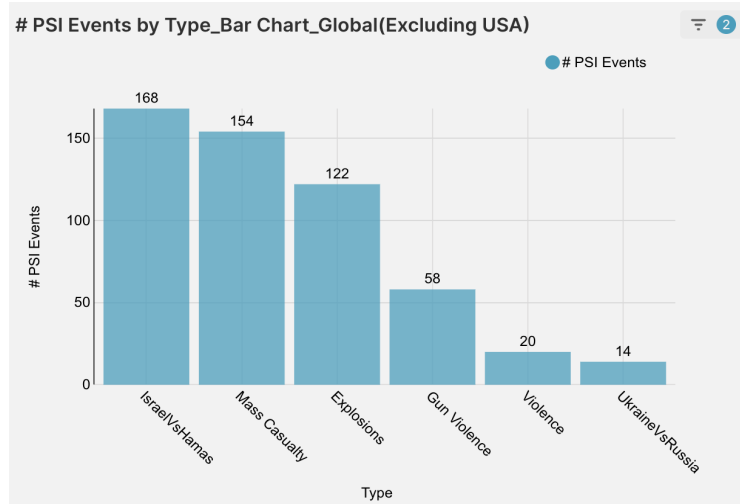
- **What this means:** The recent series of data breaches reported this week highlights a pervasive and concerning trend in cybersecurity. Companies like AT&T, Rite Aid, BMW, Disney, mSpy, and others have faced unauthorized access to sensitive customer data ranging from phone call records and internal communication messages to internal project details and user support information. For these companies, the breaches represent more than just a compromise of data—they erode trust and their reputations. Breaches like these can lead to financial losses, legal consequences, and lasting damage to the goodwill associated with their brands. Users affected by these breaches might face potential risks such as identity theft, phishing attacks, and unauthorized use of their personal information. Threat actors and hacking groups can leverage this stolen data to perpetrate further credential-stuffing attacks, sell sensitive information on dark web forums, or conduct targeted phishing campaigns. They can further exploit personal information to impersonate individuals, gain unauthorized access to accounts, manipulate communication channels, or re-sell the stolen financial details on the dark web, potentially causing further financial harm to victims beyond the initial fraudulent transactions.

| 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 Mass Casualty incidents across the globe compared to the previous week, with Palestine, Lebanon, and Israel being the largest contributors to the incident type; 74 percent of these events were explosions. General alerts pertaining to the Israel-Hamas conflict (including protests, raids and involvement in the neighboring countries) increased by 8 percent compared to last week. Palestine and Israel accounted for 52 percent of the all international explosions alerted this week. Additionally, the alerts pertaining to Ukraine and Russia showed a 35 percent decrease. Protests, Gun Violence, and Explosions were the most alerted subtypes and increased by 15 percent, 24 percent, and 8 percent, respectively.

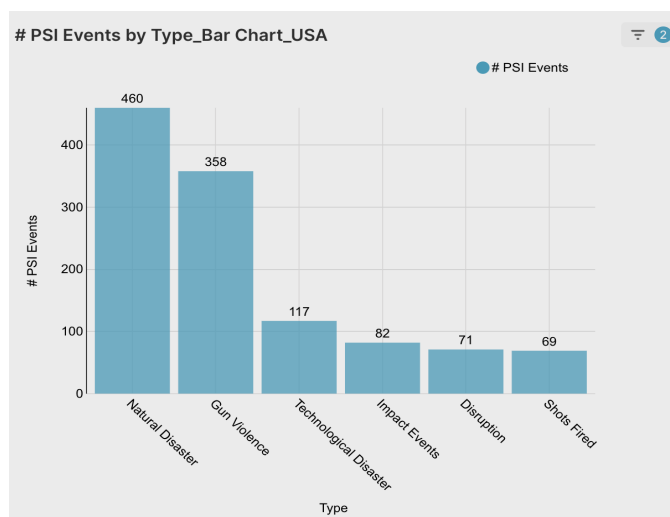


Source: ZeroFox Internal Collections

- **What this means:** This week saw a relative decrease in Violence-related alerts across the globe, but the conflict between Israel and Hamas continued. In the ongoing Russia-Ukraine war, cross-border shelling and deployment of unmanned aerial vehicles (UAVs) occurred. Attacks on critical infrastructures like [airports](#), railway stations, and [power stations](#) were reported, along with a few civilian casualties this week due to the conflict. The protests across Bangladesh contributed to the increase in Protest numbers compared with last week. Nineteen people have died and multiple others have been injured in the protest against *quotas* (reservations) in the country. The system, abolished in 2018, was reinstated by and set for appeal in the Supreme Court on August 7. But the students have begun protests, demanding the removal of all categories of reservation (excluding that for people with disabilities and indigenous communities). Additionally, the Explosion incidents were reported mainly in the Middle East and Asia region, with some reports of explosions coming in from Africa. Similarly, a large number of Gun Violence incidents were due to localized shooting reported from countries in South America.

Physical Security Intelligence: United States

What happened: In the past week across the United States, the most alerted incident subtypes were Natural Disaster, Gun Violence, and Technological Disaster. Illinois and California had the highest number of Gun Violence alerts (65 and 27 alerts, respectively), which together accounted for 25 percent of this week's nationwide total. Gun violence across the country showed a 16 percent decrease compared to the previous week. The top two states contributing to the Natural Disaster alerts were California and Florida, and U.S. Natural Disaster alerts have increased by 28 percent in comparison to last week. There were 26 alerts relating to schools, excluding Protests—an increase of 52 percent. Finally, the top contributing states to Technological Disaster alerts were Florida, California, and Maryland.



Source: ZeroFox Internal Collections

- **What this means:** This week across the United States, Natural Disaster was the highest alerted subtype and showed an 18 percent increase from last week. Tornadoes were alerted from Iowa, Nebraska, Indiana, all the way to the EastCoast of New York. Most of the hurricanes that these states experienced this week can be attributed to the remnants of Hurricane Beryl; New York alone saw a year's worth of tornadoes in a [month](#) due to that storm. Along with tornadoes, both wildfires and private structure fires were alerted in large numbers. Between the two, fires in the urban area have increased exponentially compared the previous few weeks. The United States reported a 16 percent decrease in gun violence cases this week but witnessed an [assassination attempt](#) on Former President Donald Trump. The assassination attempt was carried out when the former president was addressing a campaign rally in Butler, Pennsylvania. Trump survived the attempt with a minor graze wound, and the Secret Service were able to neutralize the attacker. Days after the assassination attempt, the Republican National Conference (RNC) went ahead as planned in Milwaukee, Wisconsin. Outside the venue an individual was fatally shot by an off-duty officer, leading to protests. However the situation was controlled, and the RNC

continued with the official selection of its presidential and [vice presidential](#) candidates for the upcoming November elections.

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

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%