



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

June 3, 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 May 31, 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 Brief – Dark Web Competition Offers Insight into Threat Actor Focus	2
ZeroFox Intelligence Brief – Continuity Likely After Mexico Elections	2
ZeroFox Intelligence Flash Report – New One-Time Purchase Ransomware Announced in Dark Web Forum	2
ZeroFox Intelligence June 2024 Geopolitical Brief	3
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 11	3
 Cyber Intelligence Key Findings	5
U.S. Treasury Sanctions Individuals Behind Infamous 911 S5 Botnet	5
Bugged Minesweeper Clones Phish Financial Organizations	5
Free Piano Phish Targets American University Students, Staff	6
 Deep and Dark Web Intelligence Key Findings	8
Chatbot-Like Service Observed for Deep and Dark Web Activity	8
Threat Actor “moma” Advertised a 0-day Exploit on xss	8
Threat Actor Group “Hunt3r Kill3rs” Conducts Attacks Against Israeli Targets	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-23108	11
CVE-2024-24919	12
 Ransomware and Breach Intelligence Key Findings	14
Ransomware Intelligence: RansomHub Claims Christie's Data Breach	14
Breach Intelligence: Healthcare Services Breached	14
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	18
 Appendix A: Traffic Light Protocol for Information Dissemination	19
 Appendix B: ZeroFox Intelligence Probability Scale	20

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief – Dark Web Competition Offers Insight into Threat Actor Focus

The results of the competition “// XSSware” on the Russian-speaking dark web forum xss were announced on April 16, 2024. Projects focusing on obfuscation performed well, likely indicating a demand for accessible, free obfuscation tools within the threat actor community. While the direct impact is very likely limited, the competition and winning projects will likely contribute to increasing efficiency in attack vectors, particularly as the projects are free to access by members of the forum. The top three projects have predominantly been awarded due to their perceived potential rather than their immediate application—with the exception of the first-place PowerShell Stealer, which allegedly boasts immediate application. It is very likely that the total prize money of USD 20,000 awarded in the course of competition “//XSSware” will further fund threat actors in developing their malicious tools.

ZeroFox Intelligence Brief – Continuity Likely After Mexico Elections

Like the elections in India, South Africa, and now the United Kingdom (UK), there is a clear frontrunner in Mexico's June 2nd general election. Presidential candidate Claudia Sheinbaum of the ruling Movimiento de Regeneracion Nacional (Morena) party has maintained a 15–30 percent polling lead over her main opponent, Xochitl Galvez, for months and is very likely to be Mexico's next president. Morena will also likely win most of the other 20,000 posts for governor, congress, and local representatives. What matters is the margin of victory; a narrower-than-expected victory will make it difficult for the Morena party to achieve its overarching political reforms and goal of dominating Mexico's political institutions and economy. As with most major elections around the world, orchestrated disinformation campaigns are likely to pose a threat to informed voter behavior. As is normal during Mexican campaigning, violence by criminal groups—towards voters, candidates, and even third-party entities such as election observers and journalists—remains a significant threat to the integrity of the elections.

ZeroFox Intelligence Flash Report – New One-Time Purchase Ransomware Announced in Dark Web Forum

On May 26, 2024, well-regarded actor “phant0m” announced a new ransomware tool named “SpiderX” on the English-speaking dark web forum “OnniForums”. The software, which quickly gained traction amongst other forum users, is available for a one-time purchase of USD 150. The announcement of SpiderX contributes to a broader upward trajectory in the number of both English-speaking and one-time purchase ransomware offerings observed in deep and dark web

(DDW) marketplaces. While threat actors leveraging this ransomware almost certainly pose a threat to organizations across regions and industries, they are almost certainly unable to conduct attacks at the frequency or scale of larger ransomware-as-a-service RaaS groups.

ZeroFox Intelligence June 2024 Geopolitical Brief

The outcome of EU elections will likely see less legislation regarding climate change and human rights and more on improving the competitiveness of EU businesses. Mexico's leading presidential candidate does not have a detailed plan to combat rising insecurity which will likely continue following the elections. Haiti's security situation has stabilized as aid has arrived in the run-up to a foreign intervention. German authorities are on high alert for terrorist attacks during the month-long Euro 2024 soccer tournament. Georgia forced through an unpopular law that brings the country closer to Russia. Surprise UK elections will likely finish with a change in government. When G7 leaders meet in June, they will likely double down on efforts to fund Ukraine with frozen Russian assets and isolate China from the global economy. Outgoing Mexican president AMLO is likely to maintain influence over his successor Claudia Sheinbaum. Israeli Prime Minister Benjamin Netanyahu very likely sees the extension of the conflict as crucial to remaining in office. Russian troops are attempting to gain as much Ukrainian territory as possible before Western aid arrives and likely freeze battle lines until 2025.

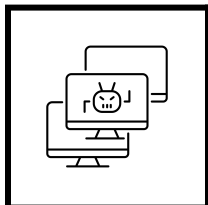
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 11

On May 26, 2024, well-regarded actor "phant0m" announced a new ransomware tool named "SpiderX" on the English-speaking dark web forum "OnniForums." On May 19, 2024, threat actor "Sumo" announced a data leak pertaining to a NATO school's e-learning platform on the Russian-speaking deep web forum "Cronos." On May 16, 2024, threat actor "USDoD" announced on X their intent to launch a new, open-source data breach forum named "Breach Nation". On May 15, 2024, "GhostSec" announced on its official Telegram channel its intention to abandon financially motivated cybercrime and resume hacktivism activities.

| Cyber Intelligence |

Cyber Intelligence Key Findings

U.S. Treasury Sanctions Individuals Behind Infamous 911 S5 Botnet

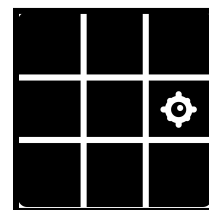


What happened: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned three individuals and three Thai companies for their association with the malicious botnet tied to the residential proxy service known as 911 S5. The sanctions mandate blocking and reporting the assets of designated individuals and entities within the U.S. or controlled by U.S. persons to OFAC. Regulations prohibit U.S. persons and those in the U.S. from dealing with blocked entities. Furthermore, those who engage in specific transactions with these entities risk being designated themselves. The accused individuals and entities used the 911 S5 botnet for fraudulent economic assistance applications and laundered proceeds through luxury real estate purchases.

- **What this means:** Cybercriminals use stolen residential IP addresses to hide malicious activities like credit card theft. They used the 911 S5 botnet to disguise their digital activities, to make it seem like the crimes originated from the victim's computer instead of their own. The IP masquerading process allows threat actors to bypass fraud detection systems, making it easier to commit crimes without being traced, thereby also hindering law enforcement efforts. The 911 S5 botnet compromised 19 million computers, enabling fraudsters to steal billions from the U.S. COVID-19 relief funds through thousands of counterfeit applications. Some of the IP addresses the botnet compromised were also involved in a series of bomb threats through the United States in April 2022.

Bugged Minesweeper Clones Phish Financial Organizations

What happened: Hackers are exploiting a Python clone of Microsoft's Minesweeper game to hide malicious scripts targeting financial institutions in Europe and the United States. Ukrainian cybersecurity agencies link these attacks to UAC-0188, which uses this code to install SuperOps RMM software, enabling remote access to compromised systems.



- **What this means:** SuperOps RMM allows attackers direct access to sensitive financial systems, including transactional details, personal information, credit card information, and more, which can further be used for spear phishing or pig butchering scams. Besides, this is not the first time threat actors have infected malicious codes in seemingly innocuous files. In a campaign researchers [discovered](#) in April, threat actor TA558 had targeted over

320 organizations globally via images infected with malicious code to deploy malware tools. The U.S. Securities and Exchange Commission (SEC) has [announced](#) new data breach reporting regulations for certain financial firms, aiming to address the evolving risks posed by technology and data breaches in the financial sector. Financial organizations are required to notify individuals of data breaches within 30 days.

Free Piano Phish Targets American University Students, Staff



What happened: A large-scale phishing campaign enticed recipients with a promise of a free Yamaha baby grand piano. The campaign targeted mainly North American university students and faculty, as well as healthcare and food and beverage service providers, and amassed over USD 900,000 through fraudulent shipping fees.

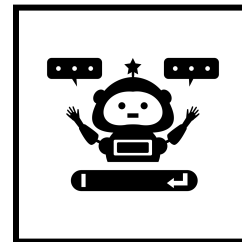
➤ **What this means:** The phishing scheme preys on recipients' trust with a seemingly generous offer of a free Yamaha baby grand piano, exploiting urgency and legitimacy to convince victims to pay substantial shipping fees via non-traceable methods. This phishing campaign's success highlights the effectiveness of leveraging unusual lures to deceive recipients and extract significant sums of money. Phishing emails can further target individuals by exploiting their trust in seemingly legitimate sources. This can impact individuals by deceiving them into providing personal information or making financial transactions, leading to identity theft, financial loss, and compromised cybersecurity.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Chatbot-Like Service Observed for Deep and Dark Web Activity

What happened: On May 29, 2024, ZeroFox observed a Chatbot-like service, dubbed FraudGPT, selling its services on the deep and dark web (DDW). The service reportedly includes generating phishing websites and emails, identifying malicious code, creating undetectable malware, and quickly uncovering leaks and vulnerabilities via the use of uncensored artificial intelligence (AI). Users are required to register and subscribe to use the service, with a monthly subscription selling for EUR 89 and a lifetime subscription selling for EUR 199 at the time of the post. FraudGPT PRO, a version of the service that includes a database of over 18,000 Critical Vulnerabilities and Exposures (CVEs), is also available to subscribers.



- **What this means:** AI technology continues to revolutionize the operations of legitimate industries across the globe, improving productivity and enhancing problem-solving capabilities. AI even has a positive impact on cyber security operations such as dark web monitoring, highlighted by ZeroFox in a November 2023 [blog post](#). However, AI technologies have also positively impacted the capabilities of those operating in illicit industries, particularly on the dark web. The automation of nefarious cybercriminal activity, such as malware generation, vulnerability identification, and code obfuscation, will likely increase the number of victims and quality of attacks globally if implemented. This includes allowing technologically unsophisticated users to potentially carry out high-level attacks more easily, as they can rely on AI to carry out operations the users may not have been able to successfully conduct manually.

Threat Actor “moma” Advertised a 0-day Exploit on xss



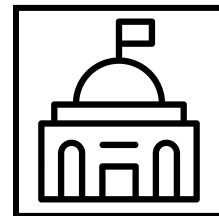
What happened: On May 26, 2024, the untested threat actor “moma” advertised a 0-day Pulse Connect Secure VPN remote code execution (RCE) exploit on the predominantly Russian language Dark Web forum “xss.” According to moma, there were 2,102 vulnerable devices from 2,685 tested IP addresses. The actor did not specify the charge for the exploit, instead asking interested buyers to communicate via TOX and Jabber messengers.

- **What this means:** As moma is untested, their credibility cannot be confirmed. It is likely that there will be interested buyers as threat actors frequently purchase 0-day exploits since they target a vulnerability that is unknown to the vendor and does not have a patch. This allows attackers to compromise systems, run malicious code, and steal data. Ransomware groups have also targeted zero-day vulnerabilities to

conduct large-scale attacks. The exploit will likely be sold privately as the actor asked to be contacted via TOX or Jabber, so it will be unknown if it is purchased. Due to the number of vulnerable devices, though, and how widely Pulse Connect Secure VPN is used, if the actor can provide proof of their claim, ZeroFox assesses that there is a high probability that the 0-day exploit will be purchased. It is important to ensure that Pulse Connect Secure is running on the most updated version of the product and to be on the lookout for a patch in the near future.

Threat Actor Group “Hunt3r Kill3rs” Conducts Attacks Against Israeli Targets

What happened: On May 30, 2024, threat actor group “Hunt3r Kill3rs” claimed to have initiated a wave of attacks against unspecified Israeli military and government infrastructure. The group posted the attack claim on their Telegram channel along with additional claims to have Israeli government data prepared for future leaks. This includes a claim that the group is in possession of 2000 documents and information on personnel at Unit 8200 (NFI). The group previously claimed an [attack against the Israeli Ministry of Foreign Affairs on May 27, 2024](#), and stated they were in possession of additional data related to the attack.



- **What this means:** Hunt3r Kill3rs is a relatively new threat actor group that appears to have begun operations this month. The group’s Telegram channel posts are in Russian and English, and their operations appear to align with those of a pro-Palestinian hacktivist group. While other hacktivist groups tend to conduct lower-risk distributed denial of service (DDoS) attacks, Hunt3r Kill3rs has conducted three separate attacks – two against Israeli targets and one against Germany’s video infrastructure – that included data theft and leaks. It is unclear if the group is in possession of sensitive material related to Unit 8200 or any other Israeli government entity. Unit 8200 is roughly equivalent to the U.S. National Security Agency (NSA) and is responsible for signals intelligence collection and reporting. Hunt3r Kill3rs appears to be big-game hunting and operating at an aggressive pace for a new group, indicating possible overlap with other established, Russian-based hacktivist groups.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent entities in software solutions, network security, and telecommunications sectors. The [vulnerabilities](#) (CVE-2024-2214, CVE-2024-2212 & CVE-2024-2452) in Eclipse ThreadX could lead to code execution. CISA has added security [flaws](#) (CVE-2024-1086 & CVE-2024-4978) to its Known Exploited Vulnerabilities (KEV) Catalog, indicating that there is evidence of active exploitation. [CVE-2024-24919](#) (CVSS score: 8.6) potentially allows an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote access VPN or Mobile Access Software Blades. The [flaw](#) on the TP-Link Archer C5400X tracked as CVE-2024-5035 has a critical CVSS v4 score of 10. The network service called "rftest" is vulnerable to unauthenticated command injection on ports TCP/8888, TCP/8889, and TCP/8890. By successfully exploiting this flaw, remote unauthenticated attackers can gain arbitrary command execution on the device with elevated privileges. [CatDDoS](#) threat actors are found to be leveraging vulnerabilities that are relatively old such as CVE-2010-2506, a nearly 14-year-old vulnerability in Linksys firmware; CVE-2013-1599 (CVSS score: 9.8), a more than decade-old flaw in D-Link IP cameras; and CVE-2011-5010 (CVSS version 2.0: 10), a remote code execution vulnerability in Ctek SkySouters from 2011. The Campbell Scientific CSI [Web Server](#) supports a command that will return the most recent file that matches a given expression. A specially crafted expression can lead to a path traversal vulnerability (CVE-2024-5433; CVSS score: 5.3).

Notable vulnerabilities:

[CVE-2024-23108](#)



What happened: Security researchers have disclosed a proof-of-concept exploit for CVE-2024-23108 (patched in February 2024), a **CRITICAL** vulnerability (CVSS score: 9.8) in Fortinet's SIEM solution, allowing remote command execution without authentication, affecting versions 6.4.0 and above.

➤ **What this means:** This newly disclosed vulnerability in Fortinet's SIEM solution is critical due to its potential for remote command execution without

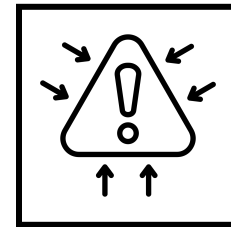
authentication, posing a severe security risk to organizations using FortiSIEM. Given Fortinet's widespread adoption in enterprise environments, this vulnerability has the potential to affect a large number of systems, increasing the urgency for organizations to apply the patch released in February. Failure to do so could leave these systems vulnerable to exploitation, potentially leading to unauthorized access, data breaches, and other security incidents with significant consequences.

Affected products:

- Fortinet FortiSIEM version 7.1.0 through 7.1.1; 7.0.0 through 7.0.2; 6.7.0 through 6.7.8; 6.6.0 through 6.6.3; 6.5.0 through 6.5.2; 6.4.0 through 6.4.2.

CVE-2024-24919

What happened: Check Point has warned about an ongoing campaign targeting its customers' remote-access VPN environments. Attackers are exploiting old local accounts with weak password-only authentication to gain unauthorized access to enterprise environments. The vulnerability (CVE-2024-24919) has been rated **HIGH** with a CVSS score of 7.5. The company has released emergency fixes to address the bug.



➤ **What this means:** CVE-2024-24919 allows attackers to access data on Internet-connected Gateways with remote or mobile access enabled. Attacks target outdated local accounts with weak password-only authentication. Customers should apply the released patches to avoid being targeted in cyberattacks.

Affected products:

- CloudGuard Network versions R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.
- Quantum Maestro versions R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.
- Quantum Scalable Chassis versions R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.
- Quantum Security Gateways versions R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.
- Quantum Spark Appliances versions R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20.



ZEROFOX®

Weekly Intelligence Brief

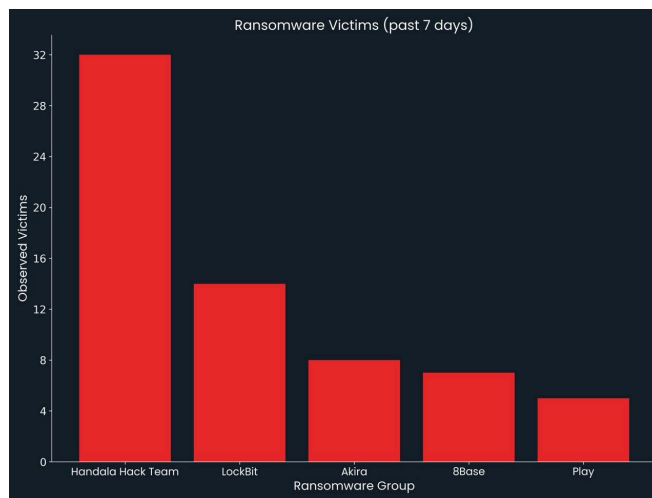
TLP:GREEN

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: RansomHub Claims Christie's Data Breach

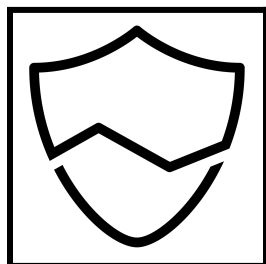
What happened: In the past week, ZeroFox Intelligence has observed the highest ransomware / digital extortion activity associated with the Handala Hack Team and LockBit. ZeroFox has also observed an update on the RansomHub ransomware leak site targeting Christie's, a prominent U.K.-based fine art, luxury, and antiques auction company. The threat actor claims to hold the information of 500,000 of Christie's private clients. Meanwhile, the Handala Hack Team has targeted a group of "fake news companies" in Israel.



Source: ZeroFox Internal Collections

- **What this means:** Retail, financial services, and construction are the industries most affected. Christie's has confirmed that it has suffered a technology security incident, adding that investigations revealed "unauthorized access by a third party to parts of Christie's network." Handala Hack Team has upped its attacks targeting Israeli institutions, seemingly aligned with the team's support for Palestine. The list of victims also includes news sites that the team accuses of propagating "fake news."

Breach Intelligence: Healthcare Services Breached



What happened: Prescription management company Sav-Rx has notified over 2.8 million people in the United States of a data breach that occurred in October 2023. The breach reportedly exposed the personal data of 2,812,336 individuals. The company identified an interruption in its computer network on October 8, 2023, and promptly secured its systems with the help of third-party cybersecurity experts. Investigations revealed that hackers first accessed customer data on October 3, 2023, obtaining files containing personally identifiable information like full name, date of birth, Social Security Number (SSN), phone numbers, and insurance identification number. Healthcare services are often a major target for data breaches. [Cencora](#), a drug distributor, has also confirmed that some of its systems

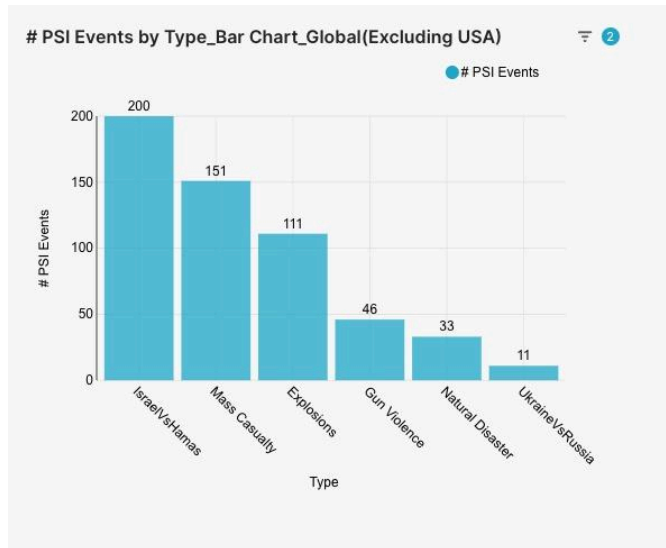
suffered a breach where personal and sensitive medical information was stolen from its information systems.

- **What this means:** Sav-Rx's data breach illustrates the pervasive threat to personal data within healthcare systems. With sensitive information like Social Security Numbers compromised, affected individuals are at risk of identity theft and other forms of cyberattacks. The healthcare company had engaged third-party cybersecurity experts to secure its systems and conduct a comprehensive investigation, ensuring minimal disruption to business operations. Some of the major drug companies in the industry have disclosed data breaches due to the cyberattack at Cencora, whom they partner with for pharmaceutical and business services. Threat actors often target healthcare services, exfiltrating sensitive data to demand ransom. Cencora confirmed that patient data was stolen but did not observe any sale or misuse of said data at the time of writing.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



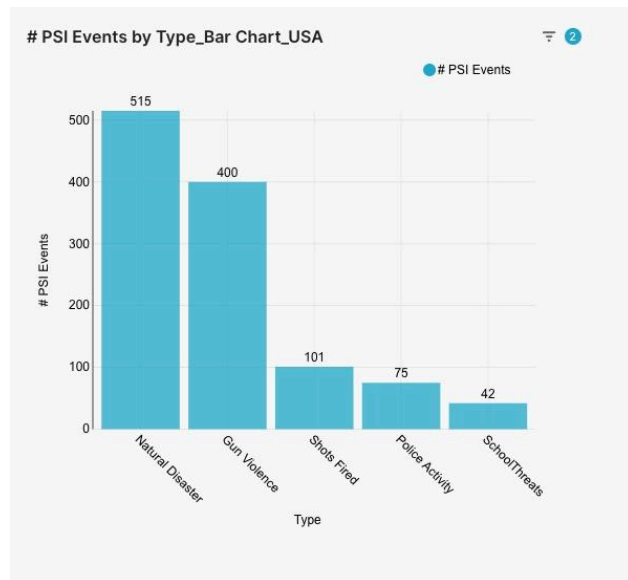
Source: ZeroFox Internal Collections

What happened: Excluding the United States, there was an 8 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Lebanon, and Israel (in that order); approximately 74 percent of these events were explosions. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 9 percent from the previous week; notably, Palestine, Israel, and Lebanon accounted for over half of all international explosions alerted (58

percent). Additionally, events related to Russia's war in Ukraine decreased by 45 percent. The top three most-alerted subtypes were explosions, which saw a 12 percent decrease from the previous week; gun violence, which decreased by 8 percent; and natural disasters, which decreased by 15 percent.

- **What this means:** This week, Lebanon rejoined the top three countries with the most mass casualties, likely due to a rekindled effort by Israel to [target](#) Hezbollah; this week was one of the deadliest periods since hostilities broke out between Israel and Hezbollah on the Lebanese border in October. While there were fewer overall events and explosions related to the Israel-Hamas War, the strikes have been more lethal this week, with Israel continuing its Rafah [offensive](#). As many civilians have been killed throughout this process, this week saw an especially large amount of [criticism](#) against the war in the media, with an "All Eyes on Rafah" post being shared over 46 million times. In regards to Ukraine, pressure is growing on U.S. President Joe Biden to allow Ukraine to use West-supplied weapons to strike Russian territory, with several other U.S. allies supporting the decision; Russian President Vladimir Putin, however, has [warned](#) that doing so will result in dangerous escalations, adding that the responsibility for any strikes inside his country's territory would lie with Western arms suppliers, even if Ukraine's forces carried out the strikes.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed victim, whereas shots fired alerts encompass shootings that did not result in a victim. The top two states that had the most gun violence alerts were Illinois and California, which together made up approximately one-quarter of this week's nationwide total (24 percent). Gun violence across the United States decreased by 7 percent from the week prior.

The top two contributors to natural disaster alerts this week were Texas and Ohio, and natural disaster alerts across the country increased by 26 percent. Alerts related to schools, excluding protests, decreased by 64 percent.

- **What this means:** This week marks the first time in several months that shots fired have replaced police activity as the third most alerted subtype. As the police activity subtype encompasses lockdowns, threats, finding of firearms on premises (not used), and general officer presence for unknown reasons, several of these are events related to schools; since school threat alerts saw a very significant decrease this week, it is understandable that police activity alerts declined as well. At this point, many schools in the United States have begun or are beginning their summer holiday. Natural disasters replaced gun violence as the top most alerted subtype this week, likely due to an uptick of severe storms and hurricane-force winds that have taken place across the country; in [Texas](#) alone, several hundreds of thousands of people have been left without power, and the storms have even resulted in fatalities. There are concerns that, without working air conditioning, the summer heat could increase that number.

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%