



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

September 9, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on September 6, 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 September 2024 Geopolitical Brief	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 17	2
 Cyber Intelligence Key Findings	4
Chinese Influence Operation Targeting Political Divides Escalates Ahead of U.S. Presidential Election	4
Global Malware Campaign “Voldemort” Mimics Tax Authorities to Spread Malware	5
FBI Seizes Russian-Led Disinformation Network Ahead of U.S. Elections	6
 Deep and Dark Web Intelligence Key Findings	8
Threat Actor “@888” Allegedly Leaks Additional Data from August 2024 BMW Hong Kong Breach	8
New Pro-Russian Threat Actor Group “DoubleFace” Claims Alliance with “Cyber Army of Russia”	8
Threat Actor “agreindex” Allegedly Leaks Database from EnglishCentral	9
 Exploit and Vulnerability Intelligence Key Findings	12
CVE-2024-7261	12
CVE-2024-45623	13
 Ransomware and Breach Intelligence Key Findings	15
Global Ransomware Attacks Disrupt Operations Across Multiple Sectors	15
Data Breaches Affecting Several Industries	17
 Physical and Geopolitical Intelligence Key Findings	20
Physical Security Intelligence: Global	20
Physical Security Intelligence: United States	21
 Appendix A: Traffic Light Protocol for Information Dissemination	22
 Appendix B: ZeroFox Intelligence Probability Scale	23

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence September 2024 Geopolitical Brief](#)

Although possible, a ceasefire agreement between Israel and Hamas in the next several weeks is unlikely, which means international shipping and oil prices will remain volatile. Social unrest linked to France's government formation is very likely in September 2024. Germany's ruling political parties are likely to be defeated by a wide margin in a series of September state elections. Despite immigration being the primary campaign issue, Germany's sluggish economy is the bigger long-term threat to the country. Ukraine's unprecedented incursion into Russia will likely heavily influence its wartime strategy. Russian retaliation encompassing a range of hybrid measures is likely in the coming weeks.

[ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 17](#)

The Underground Economist is an intelligence-focused series illuminating Dark Web findings from the ZeroFox team.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

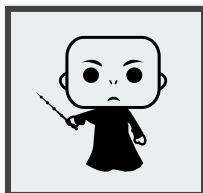


Chinese Influence Operation Targeting Political Divides Escalates Ahead of U.S. Presidential Election

What happened: A Chinese state-linked influence operation known as "Spamouflage" or "Dragonbridge" is impersonating U.S. voters and spreading divisive content targeting both major political parties ahead of the November 5 U.S. presidential election. The operation, active since 2017, has recently intensified and is using thousands of accounts across over 50 platforms to push propaganda and incite political tensions. Earlier this year, researchers [discovered](#) the same operation using artificial intelligence (AI) and social media to amplify chaos narratives, such as "civil war" or the collapse of democracy, and depicting both President Biden and former President Trump in negative, aggressive lights. The posts lack clear partisan bias but criticize both leaders regarding the same parameters. The long-running campaign likely aims to sow deep distrust among the voter community by portraying the United States as beset by social issues like urban decay, homelessness, drug abuse, and gun violence.

- > **What this means:** Networks like Spamouflage have evolved to focus on U.S. elections. Initially, they [promoted](#) pro-China content and attacked critics of the Chinese Communist Party. Now, they are spreading divisive messages within the United States. Spamouflage is a testimony to evolving foreign efforts designed to interfere with the U.S. elections, wherein operations directly abuse and deepen existing political and societal divisions in the country. Experts have argued that, despite its large-scale efforts, Spamouflage's past operations have been ineffective due to poor cultural understanding, lack of coordination, and engagement mostly from fake accounts. However, it has become increasingly successful at engaging American citizens, not just people from other countries discussing U.S. politics—especially supporters of former President Trump. Additionally, operations like Spamouflage make it harder for voters to discern truth from misinformation. The dissemination of misleading content, the reach of the campaigns, and the deceptive strategies employed—including impersonation and viral video manipulation—are likely to delude voters and influence public opinion. Such operations are also likely to complicate efforts to maintain a fair and transparent electoral system and potentially sway outcomes. From observing its AI-driven operation earlier this year, it is evident that—unlike traditional disinformation efforts—the Spamouflage campaign does not promote one candidate over the other but instead seeks to exacerbate existing divisions, sow distrust, and erode faith in

electoral processes. The campaign also demonstrates how foreign influence operations are turning to AI tools to produce more realistic content with sensational information, making the posts more likely to resonate with a specific populace.



Global Malware Campaign “Voldemort” Mimics Tax Authorities to Spread Malware

What happened: A global malware campaign named “Voldemort” has been targeting organizations with phishing emails that primarily impersonate tax authorities across Europe, Asia, and the United States. This custom C backdoor malware is designed for data exfiltration and deploying additional malicious payloads. This malicious campaign has reportedly impacted numerous organizations globally, with over 20,000 phishing messages documented since it first emerged on August 5.

- **What this means:** The campaign experienced a notable surge in activity in August 2024, with nearly 6,000 phishing emails sent in a single day impersonating various tax agencies such as the U.S. Internal Revenue Service (IRS), the United Kingdom’s HM Revenue & Customs, and France’s General Directorate of Public Finances (DGFiP). These phishing emails were meticulously crafted in the native language of the targeted tax authority and used both compromised and legitimate domain names to boost their credibility. This sophisticated and localized strategy greatly enhances the chances of deceiving recipients and compromising security. Additionally, the campaign uses a spreadsheet application for command-and-control (C2) communications and leverages legitimate software to maintain stealth. The scale and complexity of the operation suggest an intent to conduct espionage, aiming to access sensitive organizational data and posing serious security and operational threats. Companies can defend against personalized phishing attacks by improving email filtering systems, training employees to spot and report suspicious emails, using strong multi-factor authentication (MFA), and regularly updating publicly available information to minimize exposure. Additionally, implementing email authentication protocols like DMARC, SPF, and DKIM, along with S/MIME certificates, can help prevent impersonation and verify email sender identities.



FBI Seizes Russian-Led Disinformation Network Ahead of U.S. Elections

What happened: The U.S. Department of Justice recently announced that the Federal Bureau of Investigation (FBI) seized 32 web domains used by the “Doppelgänger” network, a Russian-linked influence operation that was running a disinformation campaign targeting the American public ahead of this year’s presidential election. According to court documents, the Doppelgänger network is connected to Russian companies like Social Design Agency (SDA), Structura National Technology (Structura), and ANO Dialog, which are all believed to be under the control of the Russian presidential administration. The network used these domains (managed via the Vesta open-source hosting control panel) to spread Russian government propaganda aimed at promoting pro-Russian policies. This included attempts to reduce international support for Ukraine and influence elections not only in the United States but also in Germany, Mexico, Israel, and other nations. This operation highlights the continued threat of foreign interference in democratic processes and the spread of disinformation.

- **What this means:** This operation, conducted by Russian state-affiliated entities such as SDA and Structura National Technology, highlights the sophisticated nature of Russia’s disinformation tactics, including cybersquatting and AI-generated content. These domains, designed to mimic legitimate news sources, served as platforms to spread propaganda aimed at influencing public opinion (particularly ahead of the U.S. presidential election), while also targeting other nations like Germany, Mexico, and Israel. This demonstrates how foreign threat actors are increasingly leveraging the digital ecosystem to manipulate public discourse on a global scale, making the detection and dismantling of such covert networks a critical priority. The operation’s focus on reducing international support for Ukraine and shaping geopolitical narratives underscores the far-reaching consequences of these disinformation campaigns—not only for the upcoming U.S. elections but also for future electoral stability. The FBI’s actions in seizing these domains reflect the growing challenge in defending democratic institutions against such threats, which continue to increase in both frequency and sophistication.

| Deep and Dark Web Intelligence |

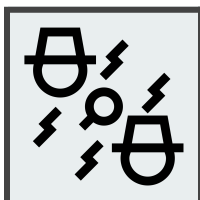
| Deep and Dark Web Intelligence Key Findings



Threat Actor “@888” Allegedly Leaks Additional Data from August 2024 BMW Hong Kong Breach

What happened: On September 3, 2024, a threat actor known as “@888” (also tracked as “888”) allegedly uploaded the complete breach package from an attack on BMW Hong Kong, which it claimed responsibility for on BreachForums in August 2024. The breach purportedly exposed 14,057 rows of customer data, including sensitive information such as chassis numbers, registration details, and customers’ personal data (names, contact preferences, and more). This breach appears to be more significant compared with @888’s earlier [claimed breach](#) of BMW Hong Kong customer data on July 15, 2024, heightening concerns about the company’s security practices. The actor shared samples of the newly leaked data to prove authenticity, but full verification of the breach is pending. BMW Hong Kong, part of a global enterprise with substantial revenue, now faces scrutiny over its data protection strategies.

- **What this means:** This incident underscores a broader trend in automotive industry breaches whereby threat actors target personal and vehicle information to exploit customer identities. The exposure of personal data like names, contact details, and vehicle information provides opportunities for threat actors to launch targeted phishing attacks or resell the data on dark web marketplaces. Companies handling extensive customer databases, especially those associated with high-value brands like BMW, remain lucrative targets. ZeroFox assesses that this breach will likely encourage similar threat actors to exploit vulnerabilities in corporate databases, fueling further dark web activity and possibly ransomware or extortion attempts.



New Pro-Russian Threat Actor Group “DoubleFace” Claims Alliance with “Cyber Army of Russia”

What happened: On September 2, 2024, ZeroFox observed the pro-Russian threat actor group “DoubleFace” claim in a post on the group’s Telegram channel to have formed an alliance with

prominent hacktivist group “Cyber Army of Russia” (aka “Cyber Army of Russia Reborn” and “People’s Cyber Army”). The post also claimed that the alliance would cause “destruction to the entirety of the cyber world”, but did not provide further information on upcoming attacks.

- **What this means:** DoubleFace appears to be a relatively new threat actor on the deep and dark web (DDW), with the group’s only other public activity being the release of its custom ransomware strain on August 5, 2024. While ZeroFox has not identified any victims of this ransomware strain as of the time of reporting, DoubleFace claims the strain maintains a Fully UnDetectable (FUD) structure against major anti-virus software and has anti-virtual machine, anti-debugging, and anti-sandboxing capabilities. Cyber Army of Russia is a notorious pro-Russian hacktivist group known for large-scale distributed denial of service (DDoS) attacks and for targeting industrial control systems (ICS). A possible alliance between these two groups could mean an increase in the efficiency, frequency, and combination of the types of attacks these two groups use against common adversaries (i.e., those they perceive as holding anti-Russian ideologies). It is also likely that DoubleFace—as a new and unknown threat actor—sought an alliance with Cyber Army of Russia to bolster its reputation in DDW communities. ZeroFox will continue to monitor for additional activity from this alleged alliance, including the emergence of new tactics, techniques, and procedures (TTPs).



Threat Actor “agreindex” Allegedly Leaks Database from EnglishCentral

What happened: On September 3, 2024, threat actor “agreindex” claimed on the dark web forum BreachForums to be selling the personally identifiable information (PII) of over 3.8 million customers associated with EnglishCentral, a U.S.-based online English language learning platform. Although the threat actor did not specify the methods it used to conduct the hack, it did disclose the information contained in the leaked database: names, account IDs, email addresses, registration dates, phone numbers, last visits, expiration dates, and contact statuses—all of which allegedly span from 2021 to the present. The post also states that agreindex is accepting payment via the cryptocurrency Monero (XMR), though it does not specify a specific amount for which the actor is selling the data. This incident is still being verified, as the threat actor has not posted definitive proof of the hack.

- **What this means:** This is the first and only instance of activity by agreindex tracked by ZeroFox. As such, ZeroFox cannot definitively confirm the veracity of this claim—particularly since the threat actor has not posted proof of the hack. However, if true, this alleged

breach highlights the importance of companies maintaining strict security protocols, including simulation training for employees and updated virus protection for the companies themselves and their clientele. This breach further demonstrates that selling PII on the dark web is continuous and lucrative, which leads to the potential for additional breaches, identity theft, financial loss, and reputational damage to the targeted company. ZeroFox will continue to monitor both this alleged breach for any fallout and aggregate for future activity.

| 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, recruitment platforms, operating systems, and government security domains. The Cybersecurity & Infrastructure Security Agency (CISA) has [added](#) three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. [CVE-2021-20123](#) is a local file inclusion vulnerability that exists in Draytek VigorConnect 1.6.0-B3 in the file download functionality of the DownloadFileServlet endpoint. [CVE-2021-20124](#) is a local file inclusion vulnerability that exists in Draytek VigorConnect 1.6.0-B3 in the file download functionality of the WebServlet endpoint. [CVE-2024-7262](#) is an improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.16412 (exclusive) on Windows that allows an attacker to load an arbitrary Windows library. LOYTEC LINX-212 firmware 6.2.4, LVIS-3MEI2-A1 firmware 6.2.2, and LIOB-586 firmware 6.2.3 devices send password-change requests via cleartext HTTP. Successful exploitation of this vulnerability (CVE-2023-46380) could [allow](#) an attacker to disclose sensitive information or make modifications to an affected device. The critical [vulnerability](#) (CVSS score: 9.8) in the WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to Local File Inclusion, Arbitrary Settings Update, and User Creation in all versions up to, and including, 2.1.6 via several functions called by the “checkFormRequest” function. The flaw (CVE-2022-46025; CVSS score: 9.1) in Totolink N200RE_V5 V9.3.5u.6255_B20211224 is vulnerable to Incorrect Access Control. The device allows remote attackers to obtain Wi-Fi system information, such as Wi-Fi SSID and Wi-Fi password, without logging into the management page. A high-severity (CVSS score: 8.8) code execution [vulnerability](#) exists in FactoryTalk View Site Edition. An improper access control vulnerability has been [identified](#) in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and, in specific conditions, causing the firewall to crash. D-Link DAP-2310 Hardware A Firmware 1.16RC028 [allows](#) remote attackers to execute arbitrary code via a stack-based buffer overflow in the ATP binary that handles PHP HTTP GET requests for the Apache HTTP Server (httpd). Zyxel has [issued](#) patches to fix an operating system (OS) command injection vulnerability (CVSS v3 score of 9.8) found in certain versions of their access points and security router versions. [CVE-2024-45623](#) is a vulnerability that affects only products that are no longer supported by the maintainer. This shows that end-of-life products are particularly vulnerable to being exploited in the wild.



Critical

CVE-2024-7261

What happened: Zyxel released updates to fix this critical OS command injection vulnerability affecting access points and security routers. This bug carries a CVSS score of 9.8. In addition to this, Zyxel [patched](#) eight vulnerabilities, including high-severity ones that could lead to OS command execution, denial-of-service (DoS) attacks, or browser-based information access. These flaws affect Zyxel routers and firewalls, posing risks to both authenticated and unauthenticated users.

- **What this means:** CVE-2024-7261 allows unauthenticated attackers to execute commands via a specially crafted cookie. Vulnerabilities like these can pose severe risks, like unauthorized control of network devices, exposing organizations to attacks.
- **Affected products:**
 - Zyxel has provided a list of the Zyxel access point and security router versions impacted by CVE-2024-7261 in [this](#) advisory.



Critical **CVE-2024-45623**

What happened: D-Link DAP-2310 Hardware A Firmware 1.16RC028 allows remote attackers to execute arbitrary code via a stack-based buffer overflow in the ATP binary that handles PHP HTTP GET requests for the Apache HTTP Server (httpd).

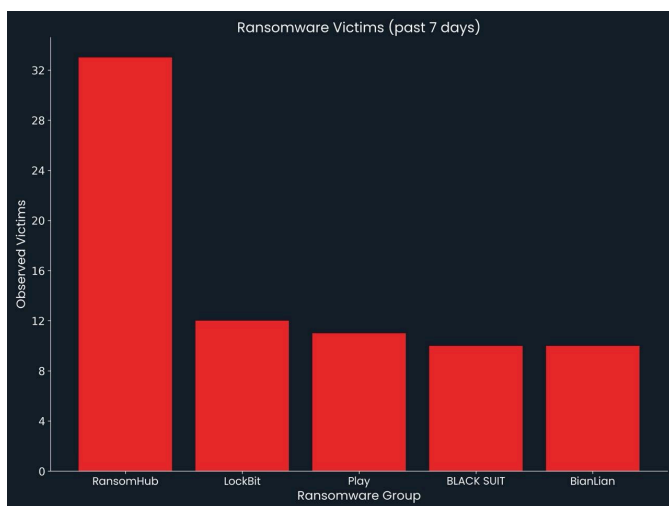
- **What this means:** This critical vulnerability only affects products that are no longer supported by the maintainer. This vulnerability can compromise PII, organization data, client information, and other confidential business dealings.
- **Affected products:**
 - D-Link DAP-2310 Hardware Revision A, Firmware v 1.16RC028

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Global Ransomware Attacks Disrupt Operations Across Multiple Sectors



Source: ZeroFox Internal Collections

What happened: ZeroFox has observed close to 80 ransomware attacks in the past seven days, mostly on the manufacturing sector and primarily conducted by the “RansomHub” ransomware group. Over 60 percent of these targeted industries are located in North America. Since its inception, RansomHub has targeted major global organizations across various sectors. Originally known as “Cyclops” and “Knight,” RansomHub is a ransomware-as-a-service (RaaS) variant that has become well-established due to its efficient and

successful service model. The group is notorious for using the double extortion tactic, which involves both exfiltrating data and encrypting systems to maximize their leverage over victims. RansomHub has been observed targeting organizations in different countries, with a few notable incidents outlined here. Planned Parenthood was a [recent](#) victim of this group’s attacks; the organization has enlisted federal law enforcement to assist with the investigation. The RansomHub ransomware group has [claimed](#) responsibility for the attack, alleging they stole 93 GB of data from the organization. ZeroFox also observed RansomHub targeting [Bennett Currie](#), [Park’N Fly](#), [Nissan](#), and several other organizations. Among other news, a newly [surfaced](#) RaaS operation known as “Cicada3301” has been targeting companies across the world. The operation, which ZeroFox intelligence has been [tracking](#) since June 2024, is believed to be a rebranding of the infamous “ALPHV” group. Cicada3301, like many ransomware gangs, uses double-extortion tactics—encrypting and stealing data—to coerce victims into paying a ransom.

- **What this means:** Ransomware is a global threat, with cybercriminals targeting organizations worldwide. If data from Planned Parenthood is leaked, the organization could face serious risks due to the exposure of sensitive information. Such breaches can expose individuals who seek confidential services, making them vulnerable to blackmail, harassment, or even violence from hacktivist groups or individuals opposed to abortion.

The leaked data could lead to targeted extortion campaigns, threatening both personal safety and privacy. The attack on Bennett Currie, a New Zealand-based accounting firm, can potentially disrupt financial operations and compromise sensitive client data. It can have profound effects on both the organization and its clients. For accounting firms, the encryption of financial records and client data can halt accounting processes, delay tax filings, and disrupt audits, leading to significant financial losses and damaging the firm's reputation for reliability. Clients may face delays in their financial reporting and tax preparation, potentially leading to missed deadlines and compliance issues. The attack on Park'N Fly, a major Canadian off-airport parking provider, could lead to significant repercussions for both the organization and its users. For the company, if operational data and payment information are stolen, it could lead to business disruptions and damage its reputation, while leaked payment information might result in financial fraud and loss of customer trust. Customers may face direct risks such as identity theft and financial fraud if personal and financial information are stolen. A ransomware attack on an automobile company like Nissan could disrupt manufacturing operations, halt vehicle production, and compromise internal systems. This can lead to delays in vehicle availability and potential breaches of customer data. For customers, the impact may include delayed deliveries and potential exposure of their personal and financial information. ZeroFox intelligence [observed](#) the Cicada3301 group announce its ransomware malware on the predominantly Russia- language dark web forum RAMP in July 2024. This malware has overlapping features with the one ALPHV (AKA "BlackCat/Noberus") used, including the ChaCha20 algorithm for encryption and identical virtual machine shutdown and snapshot-wiping commands. Cicada3301's focus on VMware ESXi environments is a likely indication of its intent to specifically target enterprise networks, which are crucial to modern infrastructure. Additionally, the group is reportedly aiming to collaborate with the "Brutus" botnet to gain initial access to corporate networks. The botnet has previously conducted large-scale VPN brute-forcing attacks targeting several popular appliances. The potential collaboration will likely facilitate such attacks and cause large-scale disruptions in crucial networks. Organizations can protect themselves from ransomware attacks by keeping their software up to date and fixing security vulnerabilities promptly. Implementing advanced systems to detect and respond to threats, training staff to recognize phishing attempts, and regularly backing up important data are crucial steps. Additionally, having a detailed plan for responding to security incidents can help minimize the impact and speed up recovery in case of an attack.



Data Breaches Affecting Several Industries

What happened: This week witnessed data breaches in several key sectors and industries, including business, government, oil and gas, financial services, and more. ZeroFox [observed](#) threat actor group “CyberVolk” claiming on Telegram to have leaked a database of the U.S. National Oceanic and Atmospheric Administration (NOAA). The group is asking for a ransom in exchange for not releasing the data—while announcing the release of 5 percent of the allegedly stolen data as proof that CyberVolk is not making false claims for clout and attention. CBIZ Benefits & Insurance Services [disclosed](#) a data breach involving unauthorized access to client information in specific databases between June 2 and June 21. The breach was reportedly caused by an exploited vulnerability on one of CBIZ's web pages, allowing an unauthorized party to acquire sensitive data. The company, which provides actuarial, administration, and investment advisory solutions services for organizations, has not yet determined if the data has been misused. A major oil and gas company, Halliburton, [confirmed](#) recently that it was a victim of a data breach reportedly linked to RansomHub. The company is conducting investigations to determine the impact of this data breach. Young Consulting, a software solution provider for medical stop-loss organizations, is notifying over 950,000 individuals of a [data breach](#) in which attackers accessed its network between April 10 and April 13, compromising personal information. The stolen data includes names, dates of birth, Social Security numbers, insurance details, prescriptions, and healthcare provider names. Hacker “Hikki-Chan” [reportedly](#) targeted the data of 390 million users of a Russian social network. The data included city, country, full names, and profile image URLs. However, the social media platform company claims that the threat actor did not, in fact, breach its infrastructure and that the data was collected from publicly available sources.

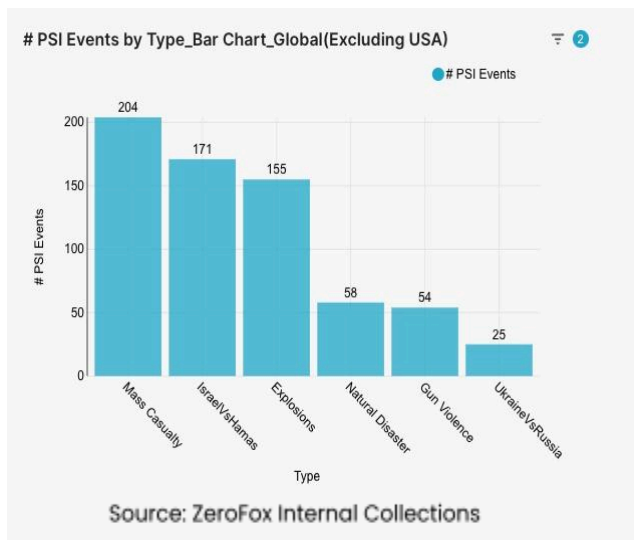
- **What this means:** Data breaches at entities like NOAA pose significant dangers, especially as they manage critical infrastructure during extreme weather events. If NOAA systems are compromised, malicious actors could disrupt the accuracy of weather forecasting, leading to misinformed disaster responses and endangering lives. Additionally, cyberattacks timed with extreme weather events could amplify the disruption of emergency services and other critical systems, causing widespread chaos. The integration of information communication and control (ICC) technologies into infrastructure operations further heightens the vulnerability of these systems to cyberattacks, particularly during high-stress periods like natural disasters. The breach at CBIZ is responsible for the potential exposure of close to 36,000 individuals’ data—including names, contact details, Social Security numbers, dates of birth and deaths, retiree health information, and welfare plan information. This data, if leaked, may be valuable to other bad actors, as it may provide valuable insights into the

company's business dealings. Threat actors can possibly leverage such data to use as blackmail; for identity theft, fraud and phishing; and more. Critical infrastructure entities such as the oil and gas company have been highly susceptible to such attacks given the significant connectivity between operational technology and networks. Such companies provide critical services to people and, therefore, have more often been observed paying ransom demands so that they can store operations immediately. The breach at Young Consulting potentially could also impact the data from a health insurer and other covered entities, posing significant risks of identity theft and fraud for affected individuals. There are risks to profile picture URLs being leaked as seen in the Russian social media data breach incident. The profile picture URLs, if acquired by threat actors, can [become](#) a gateway for various cyberattacks, including Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks. A malicious actor could manipulate a seemingly harmless URL to execute unauthorized actions on behalf of the user, such as deleting data or compromising accounts. Additionally, attackers can stage sophisticated schemes, such as initially displaying a legitimate image and later redirecting users to malicious content. In a busy platform, these vulnerabilities could also be exploited to launch DDoS attacks, overwhelming servers and disrupting services.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

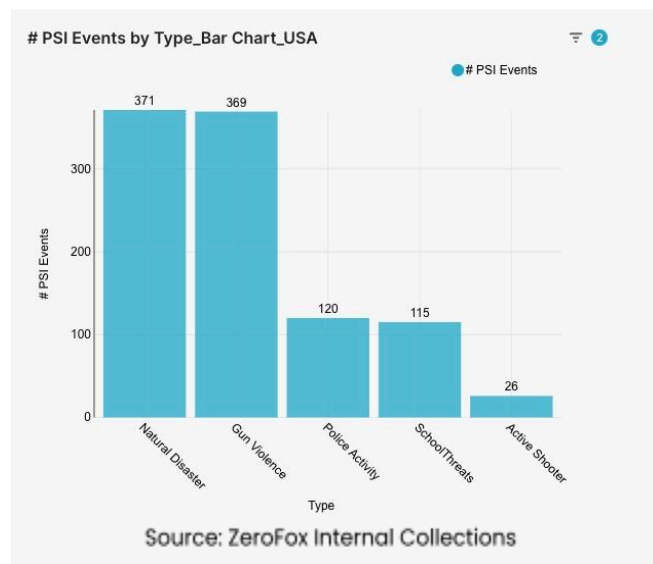


What happened: Excluding the United States, there was a 4 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Ukraine. Approximately 76 percent of these events were explosions, and the three aforementioned countries accounted for approximately 50 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 10 percent from the previous week. Additionally, events related to Russia's war

in Ukraine increased by 4 percent. The top three most-alerted subtypes were explosions, which saw a 10 percent decrease from the previous week; gun violence, which decreased by 2 percent; and natural disasters, which did not show any increase or decrease from the previous week.

- What this means:** Generally speaking, there were small decreases or no significant changes in alert numbers for many of the top subtypes. However, this merely shows a continuation of conflicts that are already happening, rather than a movement towards resolution. For instance, Hezbollah fired more than 100 [rockets](#) from Lebanon at northern Israel on Wednesday, sparking fires and causing damage (no people were injured). During the entirety of this conflict, many rockets were able to be intercepted by air defenses, which may have contributed to the slight decrease in alert numbers this week. In Ukraine, which replaced Lebanon as the country with the third-most mass casualty alerts, there was a large Russian ballistic missile [attack](#) on Tuesday, killing more than 50 people and wounding more than 200 others in one of the deadliest strikes since the war began. Russian President Vladimir Putin has recently said that his government is ready to [negotiate](#) peace talks with Kyiv, a change from his prior statement that such discussions would be impossible following the Kursk incursion.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and police activity. Natural disaster alerts typically involve fires and severe weather; gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim; and police activity involves law enforcement presence for generalized threats or for unknown reasons. The top two states that had the most gun violence alerts were Illinois and Pennsylvania, which together made up 25 percent of this week's nationwide total. Gun violence across the

United States overall increased by 12 percent from the week prior. The top two contributors to natural disaster alerts this week were California and Texas, and natural disaster alerts across the country decreased by 8 percent. Police activity alerts decreased by 8 percent, and the top contributing states were California and Texas as well. Notably, all alerts across the country (excluding protests) involving schools increased by 10 percent, and alert numbers with the active shooter tag increased by 117 percent.

- > **What this means:** Unfortunately, both active shooter threats and school-related threats increased this week, with the most notorious event being the [Apalachee](#) High School shooting in which four people were killed and nine others were injured. This event marks the 45th school shooting in 2024 and is the deadliest so far; the United States has had 385 mass shootings so far this year, according to the Gun Violence [Archive](#), which defines mass shootings as those with four or more victims. Besides Apalachee, several schools nationwide have experienced generalized threats, which have caused lockdowns, evacuations, and school cancellations. These events fall under the police activity subtype and explain why it is the third most-alerted subtype this week. As for natural disasters, wildfires continue to spread across California, with the [Bear](#) fire reaching 3,000 acres and causing mass evacuations and road closures. The combination of warm temperatures and strong winds intensify these fires, making them difficult to contain.

| 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%