



Weekly Intelligence Brief

Classification: TLP:GREEN

September 16, 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 13, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence Flash Report – New Exploitation of Existing Vulnerability Announced for Sale	2
 Cyber Intelligence Key Findings	4
Polish Security Neutralizes Sabotage Attempts Linked to Russia and Belarus	4
Two Terrorgram Leaders Charged for Inciting Hate Crimes	5
Russian Media Outlet Accused of Using U.S. and Other Personalities to Sway 2024 Election	6
 Deep and Dark Web Intelligence Key Findings	9
Divulge Stealer Targets 25 Cryptocurrency Wallets	9
Free Russia Foundation Investigates Data Breach After Internal Documents are Leaked	9
Patient Data of Confidant Health, a Mental Health and Addiction Treatment Provider, Exposed Online	10
 Exploit and Vulnerability Intelligence Key Findings	12
CVE-2024-29847	12
CVE-2024-45824	13
 Ransomware and Breach Intelligence Key Findings	15
Ransomware Attacks and Developments	15
Data Breaches and Data Leaks Across Sectors	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 Flash Report – New Exploitation of Existing Vulnerability Announced for Sale](#)

On September 6, 2024, an actor known as “skng” posted in the dark web forum xss advertising a new malicious script that is allegedly designed to target Fortinet software solutions. The product allegedly enables the exploitation of an existing critical vulnerability known as CVE-2022-40684, which was discovered in early October 2022. The vast majority of network exploitation leverages old or existing vulnerabilities that have since been remedied by software manufacturers. Threat actors are able to capitalize on the users that have not conducted the appropriate software updates and gain initial network access.

| Cyber Intelligence |

Cyber Intelligence Key Findings

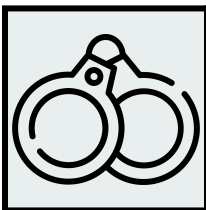


Polish Security Neutralizes Sabotage Attempts Linked to Russia and Belarus

What happened: Polish security services have successfully neutralized a cyber sabotage mission originating in Russia and Belarus reportedly aimed at destabilizing Poland. Saboteurs—allegedly based in Belarus and collaborating with Russia—infiltrated local and central government institutions, including state-owned companies that handle military contracts. The development comes amidst an increase in cyberattacks targeting states and entities supporting Ukraine in the Russia-Ukraine war. This particular sabotage effort is part of a broader surge in cyberattacks against Poland, a key aid supplier to Ukraine. Additionally, in the past week, German domestic intelligence agency Bundesamt für Verfassungsschutz (BfV) [warned](#) about military cyber group “UNC2589”, which is linked to Russian military intelligence (GRU) Unit 29155. The group, also referred to as “Cadet Blizzard” or “Ember Bear”, has conducted cyberattacks on NATO and European Union (EU) countries. The warning was a collaborative effort with international partners, including the Federal Bureau of Investigation, the Cybersecurity & Infrastructure Agency (CISA), and the National Security Agency. BfV highlighted the group’s activities involving espionage, website defacement, and data theft. UNC2589 is also linked to the 2018 Skripal poisoning, raising questions about Russian cyber aggression amid ongoing geopolitical tensions.

- **What this means:** Russian state-sponsored cyberattacks targeting its adversarial states have increased amid heightened concerns about the ongoing Russia-Ukraine war, likely as an alternative response strategy to traditional warfare involving direct military conflict. The sabotage operation, as well as the BfV’s warning, signals that the cyber war is intensifying alongside the physical hostilities. Attacks allegedly originating in Russia and targeting Poland—including the sabotage operation—are also very likely linked to Poland’s role in supplying aid to Ukraine; however, Russia has repeatedly denied having orchestrated these attacks. Reports suggest that the sabotage operation was designed to extort information, blackmail individuals or companies, and “wage a de facto cyberwar.” In June, Poland [earmarked](#) over 3 billion zlotys (USD 760 million) in funds to strengthen its cybersecurity following a suspected Russian cyberattack on the state news agency PAP. Russia-linked attacks against EU allies of Ukraine are not uncommon. Moreover, the penetration into governmental and military-contracting organizations suggests that these cyberattacks are not merely disruptive but strategic, aimed at gathering intelligence on military logistics and exerting psychological pressure on crucial actors supporting Ukraine.

The thwarted cyberattack against Poland and the warnings issued by Germany also reveal the scope of the Russian cyber warfare playbook, which includes tactics such as data extortion, blackmail, and the potential to disrupt essential services. The intensifying cyber conflict shows that Russia is increasingly relying on digital warfare as a means of retaliating against states supporting Ukraine. Poland's experience also mirrors broader concerns across the EU, with Germany and other NATO allies facing similar threats. Russian cyber espionage and sabotage will likely remain a persistent threat as geopolitical tensions remain high in the region.



Two Terrorgram Leaders Charged for Inciting Hate Crimes

What happened: Two leaders of the white supremacist group Terrorgram Collective were indicted for using Telegram to promote violence and hate crimes. The U.S. Department of Justice (DOJ) stated that the group's leaders used the platform to share ideologies, plan attacks on critical infrastructure, and call for assassinations of government officials. The DOJ asserted that Terrorgram Collective's influence extends internationally, with individuals obtaining its guidance to carry out violent acts that have included shootings and stabbings in Slovakia and Turkey targeting LGBTQ+ and Muslim communities. The indictment charges that the defendants used Telegram to promote white supremacist "accelerationism" and solicit hate crimes targeting Black, immigrant, LGBT, and Jewish people, as well as government and corporate leaders. Their goal was to incite a race war and accelerate the collapse of the government to establish a white ethnostate. The defendants encouraged followers to identify and kill targets, providing instructions on how to commit attacks. They celebrated past mass shooters as "saints," inspiring future violence.

- > **What this means:** The terrorists accused and others in the Terrorgram network abuse the privacy that platforms like Telegram seemingly offer its users. The activities of the Terrorgram Collective uncover risks posed by encrypted messaging platforms like Telegram, which can be exploited by extremist groups to coordinate and spread malicious ideologies without detection. These platforms enable anonymous, secure communication, allowing groups to evade law enforcement and intelligence agencies. The dissemination of hate-filled propaganda through secure platforms encourages and radicalizes more individuals to commit hate crimes, extending the reach of groups like Terrorgram Collective globally with minimal oversight. The individuals were accused of targeting Black, immigrant, LGBTQ+, and Jewish people, urging other members to engage in hate crimes

and terrorist attacks against them. Since the platform is known to host other cybercriminal collective other cybercriminals, it is likely that hacktivists and other malicious actors with similar ideological stances may feel validated and seek to expand their targeting of these communities. Individuals may get doxxed, harassed, deepfaked, and have their data stolen; institutions that are led by the members of these at-risk communities are also likely to be vulnerable to further espionage, sabotage, distributed denial of-service (DDoS) attacks, or coordinated cyberattacks by groups of cybercriminals that share similar ideologies.



Russian Media Outlet Accused of Using U.S. and Other Personalities to Sway 2024 Election

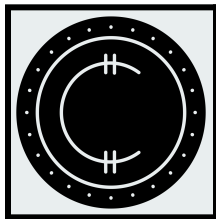
What happened: Russian state media outlet RT is reportedly engaging American and other influencers to sway U.S. voters in favor of Republican presidential candidate Donald Trump over his Democratic rival, Kamala Harris. This information emerged during a briefing on foreign meddling in the upcoming presidential election as part of a wider U.S. government initiative to combat such interference. Recently, the DOJ charged two RT employees with money laundering, accusing them of being involved in a scheme to hire an American company to create online content aimed at influencing voter opinion. U.S. officials highlighted that Russia is the most aggressive foreign player in these efforts, while China is allegedly concentrating on influencing local elections. Meanwhile, Iran has ramped up its activities to impact U.S. voters as compared to previous election cycles. The DOJ disclosed that the RT employees used shell companies and fake identities to channel USD 10 million to a Tennessee firm that produced videos designed to exacerbate U.S. political divisions.

- **What this means:** Russian state media's involvement in attempting to influence U.S. elections illustrates a significant and ongoing threat from foreign entities aiming to affect the political landscape. By employing influencers and funding online content aimed at endorsing specific candidates, Russia seeks to exploit and deepen existing domestic divisions as part of a broader strategy to covertly support its preferred electoral outcomes. As the U.S. elections draw nearer, foreign influence campaigns targeting political divides to sway voter opinions are anticipated to increase. The increased activity from Iran and the specific focus of China on local races contribute to a complex and multi-dimensional foreign influence environment. RT's alleged efforts involve a mix of state and private actors, as well as networks of American and other personalities, all aimed at persuading voters to

back former President Trump over Vice President Harris. The sophisticated tactics employed in this operation pose a risk of destabilizing electoral processes and undermining public trust in election integrity. In response, the U.S. intelligence community's increased use of private warnings and recent legal measures against RT employees reflect a concerted effort to counteract these foreign interference tactics. Concurrently, Russia has [threatened](#) to impose restrictions on U.S. media outlets in response to the allegations against RT.

| Deep and Dark Web Intelligence |

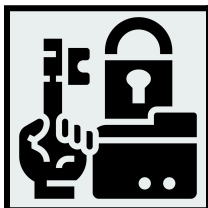
| Deep and Dark Web Intelligence Key Findings



Divulge Stealer Targets 25 Cryptocurrency Wallets

What happened: On September 7, 2024, threat actor "Py_Dev" unveiled on an underground forum a sophisticated infostealer dubbed "Divulge Stealer" with advanced capabilities to target cryptocurrency wallets. The stealer allegedly supports 25 major wallets, including Bitcoin, Ethereum, and Monero. Key features include anti-virtual machine detection, admin privilege management, and comprehensive data extraction capabilities such as browser passwords and wallet data. The malware utilizes stealth tactics like blocking security sites and deleting itself after execution, making detection challenging.

- **What this means:** The introduction of Divulge Stealer significantly impacts the threat landscape by offering cybercriminals a powerful tool for targeting cryptocurrency assets. Its ability to bypass virtual machine analysis, coupled with advanced evasion techniques, makes it particularly appealing to sophisticated actors looking to target high-value victims in the financial sector. The focus on cryptocurrency wallets suggests attackers are increasingly prioritizing digital assets, and the malware's modular nature could enable rapid adaptation to new security measures or wallet platforms. This development highlights the ongoing evolution of infostealers, with threat actors increasingly targeting sensitive financial data while enhancing their operational stealth.

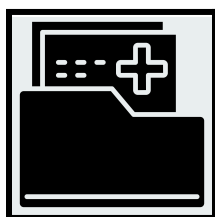


Free Russia Foundation Investigates Data Breach After Internal Documents are Leaked

What happened: On September 5, 2024, the Free Russia Foundation, a pro-democracy organization based in the United States, began investigating a significant data breach following the online publication of over 13 GB of its internal documents and more than 2,500 email chains. The breach exposed sensitive communications, including grant reports, internal documents, and salary records. The organization suspects that Kremlin-linked hacker group "Coldriver" may be responsible for the attack. This threat actor appears to target entities supporting opposition to Russia's government—including the operations of an online anti-Putin project reportedly located in

the Eastern European city of Tbilisi, Georgia, dubbed the “elf factory.” The timing and nature of the breach suggest that it could be used as justification for further repression of pro-democracy movements within Russia.

- **What this means:** This breach illustrates the growing capabilities of Kremlin-aligned threat actors like Coldriver, who leverage cyber operations to weaken opposition efforts both domestically and abroad. By targeting organizations like the Free Russia Foundation, which supports Russian activists and democratic reforms, these actors aim to undermine confidence in opposition groups while accessing sensitive intelligence on their operations and global connections. The exposure of internal documents and communications, especially related to foreign grants and funding, could be weaponized by Russian authorities to fuel anti-Western rhetoric and justify new crackdowns on organizations deemed “extremist.” Moreover, the breach serves as a warning to other pro-democracy groups, showing that they are under continuous cyber surveillance—particularly those assisting in information warfare efforts.



Patient Data of Confidant Health, a Mental Health and Addiction Treatment Provider, Exposed Online

What happened: On September 6, 2024, a cybersecurity researcher discovered an unsecured database belonging to Confidant Health, an artificial intelligence-powered mental health platform. The exposed data included over 126,000 sensitive files, such as psychosocial assessments, drug test results, and health insurance documents. The database, totaling 5.3 TB, also contained audio and video files from therapy sessions. Although the breach was addressed, it remains unclear how long the data was exposed or whether any unauthorized access occurred.

- **What this means:** This exposure presents significant risks to affected individuals and the broader cyber landscape. Sensitive mental health and substance abuse information can be exploited by threat actors for identity theft, extortion, and social engineering attacks. The availability of detailed personal records and therapy sessions increases the potential for targeted attacks, especially in extortion scenarios similar to previous breaches in healthcare. Additionally, the healthcare sector remains an attractive target for criminals due to the high value of health data on the dark web, emphasizing the need for robust security measures in telehealth services.

| 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, industrial control systems (ICS), and cybersecurity domains. Microsoft's September 2024 Patch Tuesday [addressed](#) 79 security vulnerabilities, including three actively exploited and one publicly disclosed zero-day flaws. Seven of the vulnerabilities were classified as critical, involving remote code execution and privilege escalation. CISA has [released](#) 25 advisories to provide information about current security issues, vulnerabilities, and exploits surrounding ICS. Ivanti [addressed](#) a critical-security advisory for CVE-2024-29847 affecting Ivanti EPM versions prior to 2022 SU6 and EPM version 2024. This flaw arises from the deserialization of untrusted data in the agent portal, enabling an unauthenticated attacker to execute arbitrary code remotely. This critical vulnerability has been patched. CVE-2024-41869 is a [critical](#) "use after free" vulnerability in Adobe Acrobat Reader, which, if exploited, allows attackers to execute malicious code by tricking victims into opening a malicious PDF document and eventually gaining full control of the targeted system. An improper access control vulnerability has been [identified](#) in the SonicWall SonicOS management access that potentially leads to unauthorized resource access and, in specific conditions, causes the firewall to crash. The "Akira" ransomware group is [suspected](#) of exploiting CVE-2024-40766 to target SonicWall SSLVPN devices. GitHub [released](#) an advisory to address several vulnerabilities, one of which ([CVE-2024-6678](#)) is a critical-severity bug that allows an attacker to trigger a pipeline as an arbitrary user under certain circumstances.



Critical

CVE-2024-29847

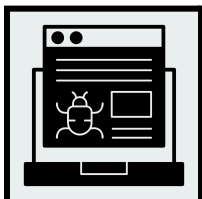
What happened: CVE-2024-29847 is a security vulnerability (CVSS score 10) affecting Ivanti EPM versions prior to 2022 SU6 and EPM version 2024. This flaw arises from the deserialization of untrusted data in the agent portal that enables an unauthenticated attacker to execute arbitrary code remotely. This critical vulnerability has been patched.

- **What this means:** This critical vulnerability enables remote, unauthenticated attackers to execute arbitrary code on affected systems, which can lead to complete system compromise. Without the patch, attackers could exploit this flaw to gain unauthorized access, steal sensitive data, or disrupt operations. The CVSS score of 10 highlights the extreme risk associated with this issue. Failure to update to the patched version leaves systems exposed to severe security breaches, including potential data theft and

operational disruptions. Applying the patch is crucial to protect against these significant risks and prevent potential financial and reputational damage.

➤ **Affected products:**

- Ivanti Endpoint Manager versions 2024 and 2022 SU5 and earlier



Critical

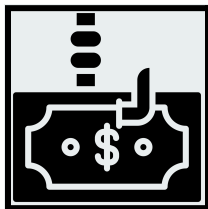
CVE-2024-45824

What happened: In the past week, CISA has [released](#) 25 ICS advisories, among which CVE-2024-45824 is a critical (CVSS score: 9.2/10.0) vulnerability in the Rockwell Automation FactoryTalk View Site. It is a command injection remote code execution bug.

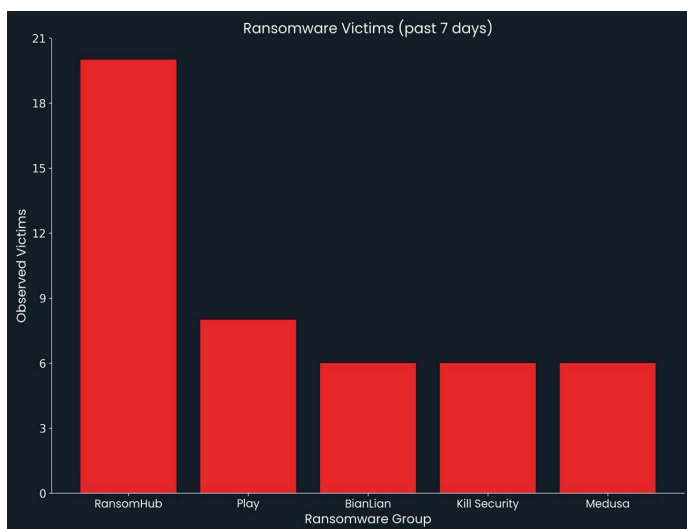
- **What this means:** The vulnerability occurs when chained with path traversal, command injection, and XSS vulnerabilities and allows for unauthenticated remote code execution. Successful exploitation of this vulnerability can let an attacker perform unauthenticated remote code execution.
- **Affected products:**
- FactoryTalk View Site Edition V12.0
 - FactoryTalk View Site Edition V13.0
 - FactoryTalk View Site Edition V14.0

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Attacks and Developments



Source: ZeroFox Internal Collections

What happened: In the past week, ZeroFox has observed over 45 ransomware attacks primarily conducted by the “RansomHub” ransomware group, continuing its streak as the one of the most prolific ransomware threat actors in the current cyber landscape. Recent activities of the “NoName” ransomware gang (also known as “CosmicBeetle”) suggest a possible affiliation with RansomHub. In a recent attack, the group [leveraged](#) RansomHub’s endpoint detection and response (EDR) killer to sabotage security measures on a

compromised machine following a failed deployment of ScRansom (a Delphi-based file-encrypting malware). Shortly after, the group deployed the RansomHub ransomware on the same system. Meanwhile, researchers have found that RansomHub has also [abused](#) the Kaspersky TDSSKiller tool to disable EDR services on targeted systems. After disabling defenses, RansomHub deployed the LaZagne tool to harvest credentials from various databases, allowing lateral movement within the network. The group evaded detection during the attack using TDSSKiller, a legitimate tool with a valid certificate. “Hunters International” ransomware gang has [claimed](#) to have stolen 6.6 TB of data (over 5.2 million files) from the London branch of the Industrial and Commercial Bank of China (ICBC). The group threatened to release the stolen data unless the bank met its demands by September 13. ICBC has not yet responded, and the claim is still unverified. Among the physical repercussions of ransomware attacks, a “BlackSuit” ransomware attack [forced](#) Charles Darwin School in Bromley, United Kingdom, to shut down between September 9 and 11. The attack compromised IT systems, including email and the internet, with expected outages lasting up to three weeks. The group claims to have stolen 200 GB of sensitive data, including student, staff, and financial information. The “Meow” ransomware group has surged in prominence, now ranking as one of the most active ransomware groups on the dark web. Its activity spiked in August, [accounting](#) for 9 percent of

global ransomware attacks. After beginning as a typical ransomware-as-a-service (RaaS), Meow has shifted to data theft and resale, offering stolen data at varying prices. On September 11, it [offered](#) “an exclusive opportunity” to access allegedly sensitive data, including 177 passports of Israeli Defense Forces (IDF) officials and operatives from Israeli intelligence agency Mossad.

- **What this means:** The evolution of the NoName toolset reflects a strategic move to enhance effectiveness and reputation in the ransomware landscape. Combining the RansomHub EDR killer tool with new tactics demonstrates adaptability and determination to overcome security defenses. The potential affiliation with RansomHub and the ongoing development of ScRansom indicate that NoName continues to be a significant and evolving threat to businesses. It could enhance their combined capabilities, resulting in more severe and disruptive attacks on organizations and considerable financial damage. Additionally, RansomHub abusing TDSSKiller is a likely indication that the group is expanding its cyber artillery, along with its list of associates. Additionally, abusing legitimate security tools like TDSSKiller erodes trust in a legitimate tool signed with a valid certificate. It allows attackers to bypass sophisticated security defenses like EDR without raising alarms. Attackers can freely harvest sensitive credentials with tools like LaZagne by disabling key security features. The alleged breach of 6.6 TB of ICBC data can potentially expose the sensitive financial data of millions of ICBC customers, severely damaging consumer trust in the bank. Given its reputation, consumer base, and immense financial assets, ICBC is a lucrative target for financially motivated threat actors like ransomware groups. Hunters International is escalating its global cybercriminal activity, despite being fairly nascent to the deep and dark underworld. The ransomware attack on Charles Darwin School reflects the threat ransomware and other cyberattacks pose to educational operations and student data security. With systems down for up to three weeks, the impact on teaching and administrative functions will be significant. The stolen data, which includes sensitive personal and financial information, raises serious concerns about data privacy and the potential for identity theft. The impact of the breach could also expose minors to a myriad of cybercrimes, including extortion and blackmail. Meow pivoting to data sales instead of ransomware extortion marks a significant shift in tactics. By offering data for auction rather than demanding a ransom, Meow seeks to differentiate itself and apply more pressure on victims. However, the success of this approach is uncertain, as it may not be as profitable or effective as traditional ransomware methods. Meanwhile, disclosing sensitive information allegedly belonging to the IDF is a likely indication that the actor is either politically motivated or trying to engage politically motivated actors. With the current geopolitical scenario, Middle Eastern countries—especially Israel and Iran—are in the spotlight as prime targets for malicious cyberattackers. Therefore, any data associated with any of these countries will very likely intrigue adversarial state-aligned

actors, who might use the sensitive data in myriad attacks—including spear phishing, extortion, blackmail, doxxing, and intimidation.



Data Breaches and Data Leaks Across Sectors

What happened: On September 12, 2024, threat actor “[Fortibitch](#)” claimed to have leaked a database from Fortinet, a U.S.-based cybersecurity company, on the predominantly English-language dark web forum BreachForums. Allegedly, the actor obtained 440 GB of data when Fortinet’s Azure and SharePoint were leaked. Fortibitch claims that the leaked data is in its S3 bucket and has provided the login and password details. According to the actor, the data was posted after Fortinet refused to negotiate or pay the ransom. Slim CD, a payment gateway provider, experienced a data breach affecting 1.7 million individuals. In its [notification](#) to affected clients, the company revealed that its network had been compromised by hackers for nearly a year, spanning from August 2023 to June 2024. A healthcare provider, Lehigh Valley Health Network (LVHN), is [paying](#) a settlement of USD 65 million for a breach it suffered in 2023. The “ALPHV / BlackCat” ransomware gang was reportedly responsible for this breach, which accessed personally identifiable information like health insurance data, phone numbers, medical and treatment information, and more. A China-linked threat actor group called “Mustang Panda” mostly conducts cyber espionage attacks against government entities. The group was [observed](#) changing the malware strain that it usually deploys in its attacks to PTSOCKET in order to download payloads and steal information from breached networks.

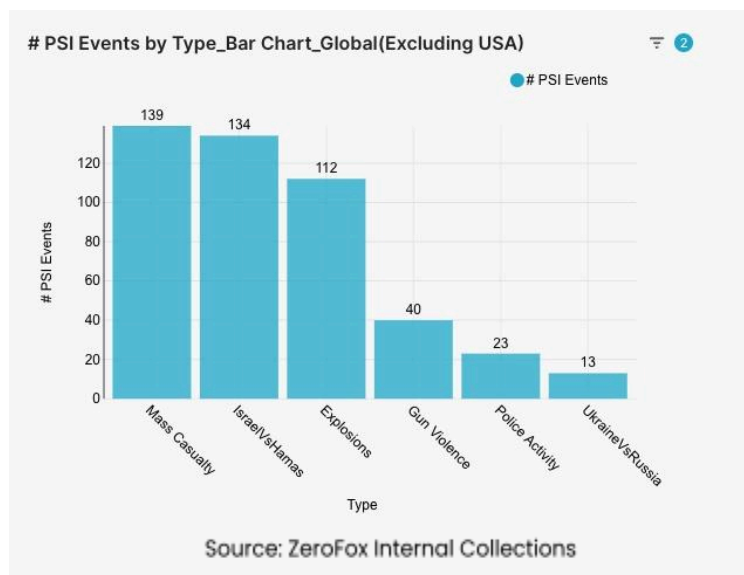
- **What this means:** Fortinet confirmed that customer data was stolen from a “third-party cloud-based shared file drive.” While the company did not disclose the number of affected customers or the specific type of compromised data, it stated that it “communicated directly with customers as appropriate.” While the threat actor claimed to have stolen 440 GB of data, Fortinet confirmed that the breach affected less than 0.3 percent of its customer base and has not led to any reported malicious activity targeting those customers. Additionally, Fortinet clarified that the breach did not involve data encryption, ransomware, or access to its corporate network. Fortibitch reportedly attempted to extort Fortinet by demanding a ransom to prevent the publication of the stolen data, but the company refused to pay. Slim CD has determined that the breach may have impacted personal information such as names, addresses, credit card numbers, and card expiration dates. While the credit card verification values (CVVs) were not exposed, there remains a risk of credit card fraud and identity theft. As payment gateway providers like Slim CD are increasingly relied upon for online transactions, this breach could lead to a higher

likelihood of fraudulent transactions and potential financial losses for users. Individuals affected, who likely interacted with businesses using Slim CD's payment services rather than the company directly, should stay alert for any signs of suspicious activity and are urged to promptly report any suspicious charges to their card issuers. In the LVHN incident, over 130,000 patients and employees were reportedly affected by the data breach. Additionally, the healthcare organization failed to specify that sensitive photos of patients were also stolen and that some of them were leaked on the threat actor's leak site. Such data breaches highlight the importance of healthcare organizations better securing sensitive patient resources to prevent data breaches—or at least minimizing their impact by segmenting their networks, for example. Threat actors are often emboldened to conduct brazen attacks on healthcare institutions as patients, healthcare organizations, and their third-party service providers are often willing to pay ransoms to avoid breaches like this one. Mustang Panda shifting its attack strategy and the malware strain it usually deploys likely shows that the group is expanding its attack sphere. It is possibly indicative that the group might be interested in stealing information to hold for blackmail, conduct phishing attacks to steal more information, or even hold the stolen information to demand ransoms from its high profile targets.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global



What happened: Excluding the United States, there was a 31 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Israel, and Lebanon. Approximately 81 percent of these events were explosions, and the three aforementioned countries accounted for about 48 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by

22 percent from the previous week. Additionally, events related to Russia's war in Ukraine decreased by 48 percent. The top three most-alerted subtypes were explosions, which saw a 28 percent decrease from the previous week; gun violence, which decreased by 26 percent; and police activity, which is used when there is significant law enforcement presence for unknown reasons or a generalized threat towards an institution that may cause a lockdown or evacuation.

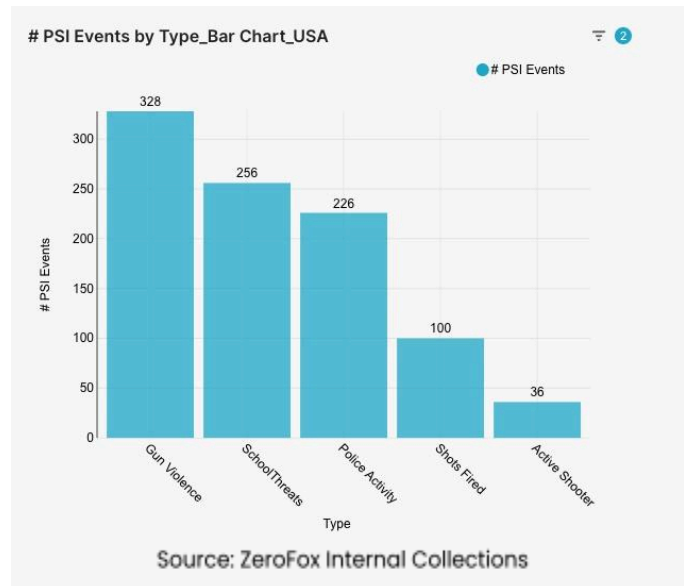
- **What this means:** This week, overall alerts were on a downward trend, but the top three countries of Palestine, Israel, and Lebanon nonetheless accounted for one half of all explosions. Earlier this week, Israeli [airstrikes](#) across Gaza hit a UN school sheltering displaced Palestinian families as well as two homes, killing at least 34 people. International efforts to mediate a cease-fire between Israel and Hamas have repeatedly stalled, as both sides have been accusing each other of making unacceptable demands. As for gun violence, besides the recurring South American statistics, Canada had the second highest number of instances this week. In one instance, a teenager was [shot](#) on Monday at Scarborough High School, prompting lockdowns at six nearby schools; Canada also had the highest number of police activity alerts, which are often used to alert law enforcement presence at schools due to lockdowns or evacuations.

Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, police activity, and shots fired. Gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim, police activity involves law enforcement presence for generalized threats or for unknown reasons, and shots fired are shootings without victims. The top two states that had the most gun violence alerts were Illinois and New York, which together made up 28 percent of this week's nationwide total. Gun violence across the United States overall

decreased by 11 percent from the week prior. Police activity alerts increased by 88 percent, and the top contributing states were California and Georgia. Illinois and Ohio had the highest number of shots fired alerts, and nationwide this subtype did not show a significant increase or decrease from the week prior. Notably, all alerts across the country (excluding protests) involving schools increased by 123 percent, and alert numbers with the active shooter tag increased by 38 percent.

- **What this means:** Both police activity alerts as well as school-related threats showed the most dramatic increases this week, as the two are often alerted together in the instance of generalized threats made towards schools, firearms found on campus, lockdowns due to nearby incidents, and evacuations. Following last week's Apalachee High School shooting, Georgia has continued to wrestle with an onslaught of threats; on Monday, several schools in the state were targets of social media [hoaxes](#) that either threatened a school shooting or claimed that there was an active bomb threat. Active shooter alerts saw an increase as well, with the highest number coming out of Kentucky; over the weekend, a man [shot](#) five people along I-75, which fueled a manhunt for the suspect that is still ongoing. As for shots fired, Illinois and Ohio saw the highest alert numbers, with Ohio experiencing a shots fired [incident](#) near a high school football game that prompted an evacuation; no one was injured in this event.



| 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%