



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

October 21, 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 9:00 AM (EDT) on October 18, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber and Dark Web Intelligence Key Findings	3
Pro-Palestine Actor RipperSec Explains Motives Behind Attacks on Various Nations	3
Reports Suggest Uptick in Russia, China, and Iran-Linked Attacks Against Adversaries	4
DOJ Indicts Two Anonymous Sudan Operators	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-8963	7
CVE-2024-9486	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Attacks Target Healthcare, Governments, Manufacturing, and More	10
From Financial Institutions to Healthcare: The Rising Tide of Data Breaches	11
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	15
 Appendix A: Traffic Light Protocol for Information Dissemination	16
 Appendix B: ZeroFox Intelligence Probability Scale	17

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



Pro-Palestine Actor RipperSec Explains Motives Behind Attacks on Various Nations

What happened: In a Telegram post, pro-Palestine threat group RipperSec explained the motives behind its cyberattacks on different nations, including Thailand, Israel, Taiwan, the United States, the United Kingdom, France, India, and Australia. Thailand was targeted due to alleged killings of innocent Muslims in Pattani and accusations of land theft. Israel was attacked in response to its actions in Palestine and Lebanon. Taiwan's assault was linked to claims of aiding Israel and insulting Russia. The United States was targeted for allegedly funding actions against innocent people in Palestine and Lebanon, while the United Kingdom and France were attacked for providing support and weaponry to Israel. India faced breaches for its alleged mistreatment of Muslims and backing of Israel, and Australia was attacked due to its perceived support of Israel through financial and military assistance.

- **What this means:** The cyberattacks carried out by RipperSec reflect a growing trend in which hacktivist groups target nations based on ideological motivations and perceived injustices. By explicitly linking their actions to specific grievances—such as alleged human rights abuses or military support for contentious actions—these groups aim to draw attention to their causes and mobilize public sentiment against the targeted countries. This method of attack demonstrates how cyber warfare is increasingly becoming a tool for expressing political dissent and advancing ideological agendas in the digital age. These attacks not only disrupt national security and critical infrastructure but also contribute to geopolitical tensions. When nations are targeted based on controversial actions or policies, it can escalate conflicts and foster an environment of mistrust between countries. It is crucial for governments and organizations to understand this phenomenon in order to develop effective strategies to counteract cyber threats while addressing the underlying issues that fuel these motivations. Meanwhile, after the arrest of Anonymous Sudan's leaders, ZeroFox has observed a [surge](#) in solidarity among pro-Palestine hacktivist groups.



Reports Suggest Uptick in Russia, China, and Iran-Linked Attacks Against Adversaries

What happened: A cybersecurity report suggests that the governments of Russia, China, and Iran increasingly rely on hackers to conduct cyber espionage, intelligence gathering, and disinformation campaigns targeting the United States and its allies. The partnerships help each state expand its cyber operations without direct involvement, leveraging hackers motivated by financial gain or political objectives. For instance, an Iran-linked hacking group breached an Israeli dating site to both profit, while Russian-affiliated hackers targeted Ukrainian military devices to aid Russia's war effort. The report found no evidence of collaboration among these states but noted each country's cyber activities are intensifying. Russia and Iran are focusing on spreading disinformation and launching cyberattacks related to the 2024 U.S. elections. China, while avoiding direct interference in the presidential race, has shifted its focus to regional targets and down-ballot elections in the United States.

- **What this means:** The growing alliance between authoritarian governments and criminal hackers has been increasingly blurring the lines between state and criminal activities in cyberspace, complicating attribution and response efforts. Adversarial states like Russia and Iran benefit by outsourcing cyber operations to criminals. It enables them to amplify disinformation campaigns, disrupt military operations, and manipulate foreign elections at low risk. As election season approaches, the United States is facing and will very likely continue to face disruptions or disinformation that can undermine voter trust and election integrity. Meanwhile, China's focus on regional influence and local U.S. races is a likely indication that cyber interference is not limited to presidential elections— it extends to various layers of democratic governance. Additionally, ZeroFox has [observed](#) a very likely uptick in espionage-focused, state-actor operations in the U.S. pre-election period, as the opposing states seek to understand the implications of potential leadership outcomes.



DOJ Indicts Two Anonymous Sudan Operators

What happened: The U.S. Department of Justice (DOJ) charged two Sudanese nationals that operated Anonymous Sudan, an online cybercriminal group responsible for tens of thousands of distributed denial-of-service (DDoS) attacks against critical infrastructure, corporate networks, and government agencies in the United States and around the world. Anonymous Sudan's attacks have caused more than USD 10 million in damages to U.S. victims. These law enforcement actions were taken as part of Operation PowerOFF, an ongoing, coordinated effort among international law enforcement agencies aimed at dismantling criminal DDoS-for-hire infrastructure worldwide.

- > **What this means:** The Anonymous Sudan group posed a significant threat to critical infrastructure, healthcare systems, corporate networks, and government agencies worldwide. According to the indictment and a criminal complaint, Anonymous Sudan actors and their customers have used the group's Distributed Cloud Attack Tool (DCAT) to conduct destructive DDoS attacks and publicly claim credit for them since early 2023. In approximately one year of operation, Anonymous Sudan's DCATtool was used to launch over 35,000 DDoS attacks, including at least 70 targeting computers in the greater Los Angeles area. The group's attacks on critical infrastructure, including government networks and corporate systems, caused millions in financial damages and service outages, impacting thousands—likely to neutralize their capabilities. These arrests are likely to discourage any immediate emergence of similar groups and the potential rise of new actors to fill the void.

| 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 technology, software development, and government services. [CVE-2024-30088](#) is an elevation of privilege vulnerability that can let an attacker gain system privileges. Iranian advanced persistent threat group OilRig, or APT34, has been exploiting this bug to target government and critical infrastructure entities in the United Arab Emirates and the Gulf region. Additionally, over 86,000 Fortinet instances are [vulnerable](#) to CVE-2024-23113, a critical flaw affecting FortiOS and related products (primarily in Asia, North America, and Europe), posing risks of unauthorized access and potential data breaches. [VMware's HCX](#) also faces an authenticated SQL injection vulnerability (CVE-2024-38814), enabling malicious users to execute unauthorized SQL queries. Meanwhile, [Oracle](#) has released its quarterly Critical Patch Update to address vulnerabilities that could allow cyber actors to gain control of affected systems. [CVE-2024-44133](#) permits bypassing macOS's Transparency, Consent, and Control (TCC) technology, allowing unauthorized access to users' data and device features, with fixes available in macOS Sequoia 15. On October 15, 2024, Cybersecurity and Infrastructure Security Agency (CISA) released two Industrial Control Systems (ICS) advisories to provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. These [advisories](#) include the vulnerabilities CVE-2024-3506, CVE-2024-8530, and CVE-2024-8531. CISA also [added](#) three new vulnerabilities—CVE-2024-9680, CVE-2024-28987, and CVE-2024-30088—to its Known Exploited Vulnerabilities (KEV) Catalog based on evidence of active exploitation. On October 17, CISA [released](#) seven ICS advisories, and also added [one](#) new vulnerability to its KEV Catalog.



CRITICAL

CVE-2024-8963

What happened: A suspected nation-state threat actor exploited multiple zero-day vulnerabilities in Ivanti Cloud Service Appliance (CSA), including CVE-2024-8963, to infiltrate enterprise networks. The nation-state actor gained unauthenticated access, enumerated users, stole credentials, and dropped a web shell for further exploitation. [CVE-2024-8963](#) is a path traversal bug in the Ivanti CSA before 4.6 Patch 519 enabling a remote unauthenticated attacker to access restricted functionality. Additionally, the actor abused another Ivanti Endpoint Manager (EPM) flaw to enable remote code execution, conducted reconnaissance via DNS tunneling, and installed a rootkit for persistent access.

- **What this means:** After the attack, the actor patched the exploited vulnerabilities to block others from interfering. The actor exploited Ivanti CSA to breach networks and then took additional steps to secure their foothold by patching vulnerabilities—a sophisticated tactic ensuring uninterrupted control. The use of DNS tunneling and kernel-level rootkits is a likely indication of a long-term espionage intent.
- **Affected products:**
 - Ivanti CSA version 4.6 (all versions before Patch 519)



CRITICAL

CVE-2024-9486

What happened: A security vulnerability has been identified in Kubernetes Image Builder versions up to v0.1.37 in which default credentials are enabled during the image build process. This issue specifically affects virtual machine images built using the Proxmox provider, as these images do not disable the default credentials. Consequently, nodes running on these images may be exposed and accessible through the default credentials, allowing unauthorized users to gain root access to the systems.

- **What this means:** The flaw poses a critical security risk to Kubernetes clusters that utilize VM images created with the Image Builder project and the Proxmox provider. If attackers exploit this vulnerability, they can potentially gain full control over the affected nodes, leading to unauthorized access, data breaches, and disruptions in service. Ensuring that default credentials are disabled is essential for maintaining the integrity and security of Kubernetes environments, especially those supporting critical infrastructure and sensitive applications. It is crucial to update to the patched version to mitigate the risks associated with this flaw and ensure the security and integrity of Kubernetes environments, especially those supporting critical infrastructure and sensitive applications. The flaw has been addressed in version 0.1.38.
- **Affected product:**
 - Kubernetes Image Builder version v0.1.37 or earlier

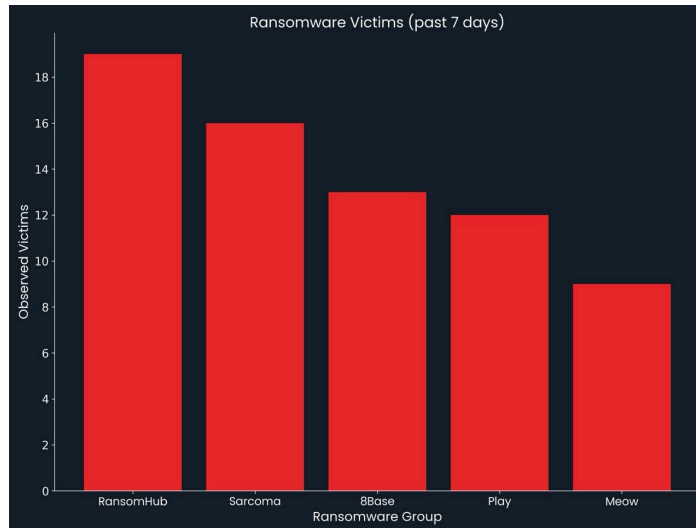
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Attacks Target Healthcare, Governments, Manufacturing, and More

What happened: In the past week, ZeroFox has observed more than 100 ransomware attacks, primarily targeting the manufacturing sector. The highest number of ransomware attacks were detected in North America, while RansomHub emerged as the most active group. The BianLian ransomware group [claimed](#) responsibility for a cyberattack on Boston Children's Health Physicians (BCHP). The attackers compromised an IT vendor on September 6, and BCHP discovered unauthorized access on its network four days later. On



Source: ZeroFox Internal Collections

October 16, 2024, ZeroFox [observed](#) an update on the Kill Security ransomware group's leak site listing the Ministry of Interior of Libya as a target. The threat actors likely accessed and exfiltrated sensitive data. On October 16, 2024, pro-Russia threat actor group CyberVolk [threatened](#) to launch a series of cyberattacks on Japan, including ransomware, DDoS attacks, data breaches, and website defacements. These attacks are part of its campaigns labeled #OpJP and #31D.

- > **What this means:** BianLian has [exfiltrated](#) sensitive data, including Social Security numbers, medical information, and billing records, from BCHP. Although electronic medical records were unaffected, the group is now threatening to leak files unless a ransom is paid. Even if BCHP pays the ransom, it is likely that BianLian will use the stolen sensitive information to target customers in triple extortion attacks. The stolen data is also likely to be used for identity theft or insurance fraud, which may not be detected as quickly by the victims since it involves children's information. Kill Security's alleged attack on the Libyan ministry is likely to expose confidential internal government operations and create leverage for threat actors to demand ransoms or further destabilize Libya's political environment. CyberVolk's targeting of Japan is a likely indication of growing geopolitical tensions, suggesting that hostile groups are leveraging cyber warfare to disrupt nations aligned with Ukraine or the West. Japanese entities in key sectors like government, finance,

and infrastructure are likely to face disruptions, the scale of which will depend on the severity and type of attack. Meanwhile, cybersecurity researchers have [released](#) a report revealing that ransomware attacks have surged nearly 300 percent compared with last year, but encryption-stage successes have dropped threefold over two years due to automated defenses.



From Financial Institutions to Healthcare: The Rising Tide of Data Breaches

What happened: Data breaches are increasingly affecting individuals and organizations across diverse sectors globally, leading to an increased risk of cyberattacks via methods such as phishing, ransomware, and exploitation of vulnerabilities, as well as potential service disruptions. Several noteworthy data breaches were reported in the last seven days. Intesa Sanpaolo, a leading banking group in Europe, [reported](#) a data breach involving one of its employees that affected thousands of account holders, including Prime Minister Giorgia Meloni. The developer behind the Pokémon game series “Game Freak” [confirmed](#) that an August 2024 cyberattack compromised personal information belonging to employees, contractors, and retirees, including names and email addresses. In a dark web forum post, a threat actor using the alias @Satanic claimed [responsibility](#) for breaching MiPC Mexico, a Mexican electronics retailer. The breach reportedly exposed sensitive customer and order information, with the actor announcing the availability of a “MiPC Mexico Database” that allegedly contains details of over 194,000 orders and 79,000 customers. A collective of family healthcare centers, drawing on nearly 180 years of combined service to their communities, is among the recent healthcare groups to [report](#) significant data theft incidents to regulators. Omni Family Health, Tri-City Medical Center, and New York Plastic Surgery have all experienced major breaches that collectively impact nearly 740,000 patients and employees. Intel Broker claims to have conducted a major data breach [involving](#) the theft of source codes, confidential documents, and credentials from global firms, including prominent telecommunications companies like Verizon, AT&T, and other major industry players. The stolen data is reportedly now for sale on BreachForums.

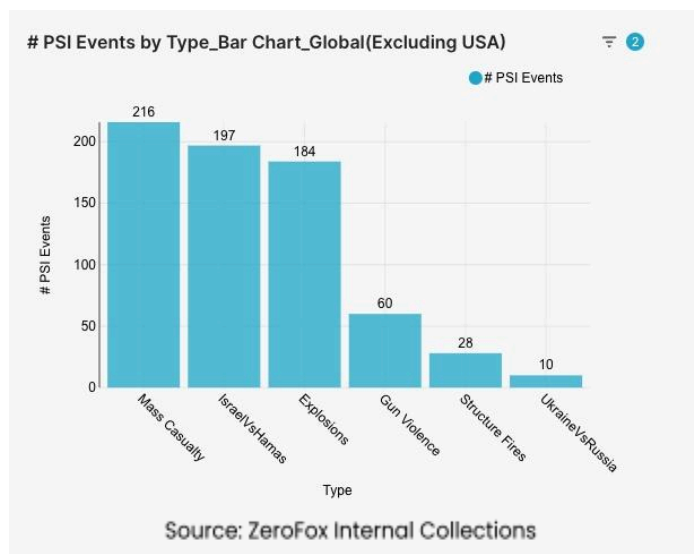
- **What this means:** These recent data breaches reveal the growing vulnerability of individuals and organizations across various sectors to cyberattacks, which can lead to significant financial losses and reputational damage. The exposure of sensitive personal and financial information increases the risk of identity theft and fraud, as seen in the Intesa Sanpaolo breach affecting thousands of account holders, including Prime Minister Giorgia Meloni. This incident not only jeopardizes personal information but also raises questions

about the bank's internal security practices. The compromised Game Freak personal information can expose affected individuals to targeted phishing attacks, extortion attempts, and financial scams, with a roughly equal chance of malicious actors doxxing these individuals on social media. The MiPC Mexico breach not only exposes customer information but also jeopardizes the retailer's reputation and customer loyalty. Meanwhile, the collective breaches among family healthcare centers put nearly 740,000 patients' data at risk, potentially disrupting critical healthcare functions and raising alarms about the security of healthcare information. As cybercriminals exploit weaknesses, the impact on operations and customer confidence underscores the necessity for enhanced strategies to prevent future breaches. In a related development, Brazilian authorities have recently [apprehended](#) the hacker known as USDoD, who is linked to high-profile breaches (including the FBI's InfraGard and the National Public Data breach) that exposed the personal information of billions.

| 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 Israel, Lebanon, and Palestine (in that order). Approximately 85 percent of these events were explosions, and the three aforementioned countries accounted for about 64 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) decreased by 7 percent from

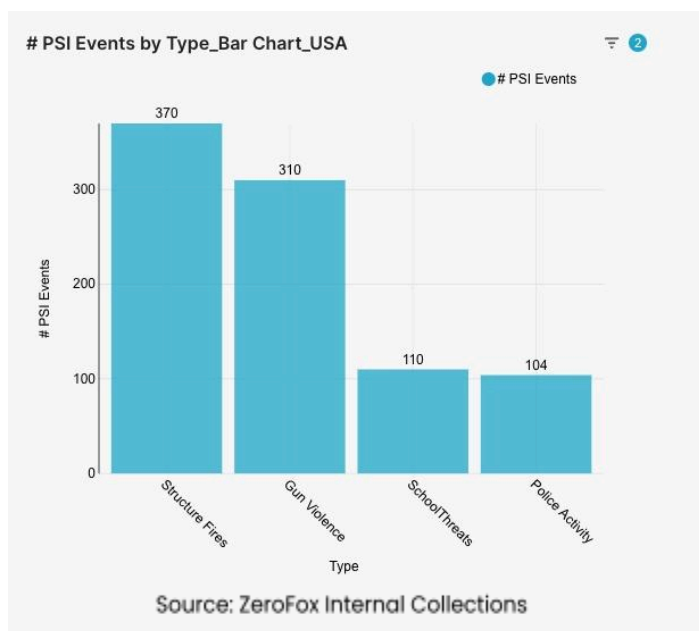
the previous week, and events related to Russia's war in Ukraine decreased by 41 percent. The top three most-alerted subtypes were explosions, which saw a 6 percent increase from the previous week; gun violence, which increased by 46 percent; and structure fires, which increased by 47 percent. Lastly, global protest activity decreased by 4 percent.

- **What this means:** All three top incident types increased this week, despite the small decrease in overall mass casualty events as well as the decreases in alerts related to the Israeli and Ukrainian conflicts. Notably, Hamas leader Yahya Sinwar, the architect of the October 7 massacre in Israel, has been [killed](#), according to the Israeli military. This comes after U.S. President Joe Biden threatened to cut off weapons [shipments](#) to Israel should it not resume humanitarian aid to Gaza. Whether or not this warning will come to fruition will depend on which administration takes over the White House in January 2025. U.S. officials have speculated that Sinwar's [death](#) could be one of the best chances of bringing the Israel-Hamas war to an end, but the situation remains volatile; Hamas could choose to retaliate, and Hezbollah may continue its offensive as well. As for the Ukrainian conflict, officials have confirmed that North Korea is [deploying](#) both weapons and soldiers to the Russian front lines, suggesting that Pyongyang is forming a close military alliance with the Kremlin. How this will affect the overall conflict is yet to be seen, and both President Zelenskyy and the U.S. government are keeping a watchful eye.

Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were gun violence, structure fires, and police activity. 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 structure fires are fires that affect man-made buildings. The top two states that had the most gun violence alerts were Illinois and Tennessee, which together made up 24 percent of this week's nationwide total. Gun violence across the United States overall

decreased by 21 percent from the week prior. Police activity alerts decreased by 17 percent, and the top contributing states were Illinois, Texas, and Maryland. Structure fires increased by 10 percent, and the top two states for this subtype were Texas and New York.



- **What this means:** As mentioned in the previous week's analysis, temperatures are beginning to drop, which correlates with an increase in structure fires as people begin to use various heating systems in their homes. For instance, five homes were set ablaze in [Irvington](#), NJ, this week due to the dry air and wind gusts spreading the fire from one home to several. For gun violence, Tennessee had the second highest number of shooting alerts for the first time in several weeks. This is likely due to the mass [shooting](#) earlier this week at Tennessee State University in which one person died and nine people were injured. Of the nine injured, three were juveniles ranging in age from 12-14 years old. Despite this, gun violence and police activity alerts decreased quite significantly overall; this is to be expected as people are spending more time indoors, and less crime is committed in public view. A [study](#) published by the John Jay College of Criminal Justice found that rising temperatures are associated with increases in robbery and homicide, while temperature declines are associated with decreases of those crimes. As temperatures continue to drop, continued decreases in alerts regarding these types of events are likely.

| 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%