



Weekly Intelligence Brief

Classification: TLP:GREEN

August 12, 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 August 9, 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 August 2024 Geopolitical Brief	2
ZeroFox Intelligence Flash Report – Travel Alerts Ahead of Likely Iranian Strikes on Israel	2
ZeroFox Intelligence Assessment – Threats to the Democratic National Convention	2
ZeroFox Intelligence Flash Report – Malicious Stealer Log Marketplace Advertised for Sale	3
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 15	3
 Cyber Intelligence Key Findings	5
INTERPOL Recovers over USD 40 Million Stolen in a BEC Attack	5
U.S. Department of State Seeking Information on Hactivist-Led ICS Attack	6
French Police Probe Ransomware Attack on Grand Palais Olympic Venue	7
 Deep and Dark Web Intelligence Key Findings	9
New Pro-Russia Threat Actor Group Emerges, Targets NATO Member States	9
Canadian Financial Services Company Falls Victim to Lynx Ransomware	10
Threat Actor Publishes Breached Data from National Public Data	10
 Exploit and Vulnerability Intelligence Key Findings	13
CVE-2024-4885	13
CVE-2024-38856	14
 Ransomware and Breach Intelligence Key Findings	16
Ransomware Intelligence: Global Ransomware News	16
Breach Disclosure: Data Security Incidents and DDW Leaks	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 August 2024 Geopolitical Brief

Iran, Israel, and Hezbollah still do not wish to significantly widen the conflict. However, any escalation risks miscalculation and unintended consequences. The Paris Olympics has likely repelled countless security threats, with the most effective acts of sabotage occurring well outside the main event space. Key emerging markets like Kenya, Bangladesh, and, most recently, Nigeria are experiencing widespread protests organized primarily over social media. Venezuelan President Nicolas Maduro will very likely crack down on growing opposition protests, while the bulk of the international community will work on supporting the opposition and fraying Maduro's support among the armed forces.

ZeroFox Intelligence Flash Report – Travel Alerts Ahead of Likely Iranian Strikes on Israel

Travel alerts have been issued across the Middle East ahead of a likely Iranian attack on Israel. While Iran and Hezbollah are almost certain to retaliate for Israel's killing of two key Hamas and Hezbollah leaders, they will likely calibrate their retribution to avoid an all-out war, as they have done during previous escalation incidents in the nearly year-long war between Israel and Hamas. Like the April 2024 episode wherein both Iran and Israel launched direct attacks against each other, the negative economic, geopolitical, and supply chain effects will likely be muted as Iran has telegraphed its response. Supreme Leader Ali Khamenei vowed there would be a "harsh" direct attack against Israel for killing a guest on his country's soil. According to reports, this will be coordinated with Iran's proxies in Lebanon, Yemen, and Iraq.

ZeroFox Intelligence Assessment – Threats to the Democratic National Convention

The Democratic National Convention (DNC) will be held at the United Center and McCormick Place convention centers in Chicago, Illinois, from August 19–22, 2024. The two venues are approximately 5.7 miles apart. The United Center will host the event's official proceedings and primetime speeches, while McCormick Place will be the home for non-televised DNC business. According to party officials, approximately 5,000 delegates, 12,000 volunteers, 20,000 media members, and 50,000 other visitors are expected to enter the city for the event, in addition to thousands of protesters. The recent change in the Democratic nominee for president and the July 13 assassination attempt on former President Trump just days ahead of the Republican National Convention (RNC) have likely shifted the threat landscape significantly. Potential allies, such as international diplomats and business leaders, as well as adversarial protesters and foreign intelligence agencies, will likely be using the DNC to learn about a new slate of politicians, some of whom they may know little about. The event is very likely to attract

a wide array of foreign interests, which increases the likelihood of espionage attempts to discern the policy positions of the possible new administration and some of its leading actors, who will be in attendance at the DNC.

ZeroFox Intelligence Flash Report – Malicious Stealer Log Marketplace Advertised for Sale

On July 30, 2024, user “2Easy.Shop” (which is almost certainly synonymous with the official handle of the malicious marketplace 2EasyShop) announced in a deep and dark web (DDW) forum that the stealer log marketplace is available for purchase. 2EasyShop—described by the poster as a “ready-made, configured, highly profitable business”—is a DDW marketplace that specializes in advertising and selling stealer logs, which are compilations of information that have been stolen from devices and networks infected with malware. Given the very likely growing demand among various types of cyber threat actors for the information contained within stealer logs, it is likely that a sale will take place. If the auction fails, there is a roughly even chance that the site will remain closed until a sale occurs. A successful deal at the asking price would very likely reinvigorate 2EasyShop, resulting in more reliable service, an increased supply of logs, and a higher volume of sales that almost certainly pose a threat to individuals and organizations.

ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 15

On July 30, 2024, user “2Easy.Shop” posted in the primarily Russian-speaking dark web forum Exploit claiming that 2EasyShop, its digital infrastructure, and its domain will be auctioned and sold to the highest bidder. Only July 30, 2024, threat actor “Sp1d3rHunters” posted in the popular hacking forum BreachForums advertising a data breach that targeted a North America-based pharmaceutical company. On July 25, 2024, untested threat actor “Michelangelo” posted in Exploit advertising a new artificial intelligence (AI)-powered tool designed to facilitate “complex, sophisticated, and large-scale” attacks targeting cryptocurrency wallets. On July 23, 2024, positive-reputation, English-speaking actor “Mr_Stuxnot” announced their contribution to a dark web forum video creation contest.

| Cyber Intelligence |

| Cyber Intelligence Key Findings



INTERPOL Recovers over USD 40 Million Stolen in a BEC Attack

What happened: INTERPOL's global stop-payment mechanism, I-GRIP, enabled Singapore authorities to recover USD 42.3 million in the largest-ever business email compromise (BEC) scam recovery. A Singapore-based commodity firm fell victim to the scam after receiving a fraudulent email from a threat actor impersonating one of the firm's suppliers. The email requested that a pending payment be sent to a new bank account in Timor Leste. Four days later, the firm realized its mistake when the real supplier reported non-payment. The Singapore Police initiated INTERPOL's I-GRIP, coordinating with authorities to retrieve the stolen funds.

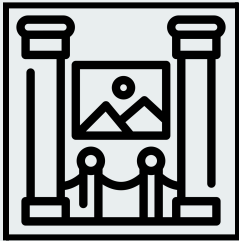
- **What this means:** According to INTERPOL, this is the largest recovery of funds stolen through a BEC scam. BEC is a high-effort phishing technique in which a threat actor targets the legitimate business email addresses of organizations and individuals, tricking users into providing sensitive information that can lead to monetary theft or enable further malicious activity. ZeroFox [observes](#) that BEC attacks are on a sharp upward trajectory, which is very likely due in part to their relatively high success rates and payoffs in comparison to other methods of cyberattack. INTERPOL is encouraging businesses and individuals to take preventative steps to avoid falling victim to BEC and other social engineering scams. According to the Federal Bureau of Investigation (FBI), BEC incurred the second-highest average cost for victim organizations amongst all types of cyberattacks during 2023. This cost has reportedly increased significantly over the past five years to an approximate median of USD 50,000 and remains on a steep upward trajectory. Although entities of all sizes are at risk of being victimized by BEC attacks, larger organizations very likely have the highest probability of being targeted. This is due, in part, to large organizations' higher number of potential threat vectors, often fragmented communications, and unclear employee-reporting procedures.



U.S. Department of State Seeking Information on Hacktivist-Led ICS Attack

What happened: The U.S. Department of State is offering a USD 10 million reward in exchange for information on senior officials of Iran's Islamic Revolutionary Guard Corps' Cyber-Electronic Command unit (IRGC-CEC), who are accused of being behind a hacker group named "Cyber Av3ngers" that has targeted industrial control systems (ICS). In November 2023, the Cybersecurity and Infrastructure Security Agency (CISA) [released](#) an advisory acknowledging the active exploitation of Unitronics programmable logic controllers (PLCs) used in the Water and Wastewater Systems (WWS) sector, including an identified Unitronics PLC at a U.S. water facility. In response to the attack, the affected municipality water authority had to take the system offline and switch to manual processes. In December, CISA released another advisory [attributing](#) the attack to self-proclaimed hacktivist group Cyber Av3ngers, which by then had also claimed responsibility. The IRGC-CEC-affiliated cyber actors had left a defacement image stating, "You have been hacked, down with Israel. Every equipment made in Israel is CyberAv3ngers legal target." On February 2, 2024, the U.S. Department of the Treasury announced sanctions against the six IRGC-CEC officials for their malicious cyber activities.

- **What this means:** According to CISA, these IRGC-CEC-affiliated cyber actors compromised default credentials in Unitronics devices in November 2023, targeting victims across multiple U.S. states. The attacks were particularly notorious because PLCs are commonly used in the WWS sector and other industries, including energy, food and beverage manufacturing, and healthcare. A CyberAv3ngers member is allegedly the head of the IRGC-CEC and has previously been [involved](#) in various IRGC cyber and intelligence operations. Additionally, Cyber Av3ngers also declared its pro-Palestinian political stance when it [claimed](#) to have conducted cyberattacks leading to mass power outages across Israel. IRGC-CEC has been [attributed](#) to several other malicious cyber activities targeting critical infrastructure and about a dozen U.S. organizations. These attacks are likely designed to gather intelligence and retaliate against sanctions, military actions, and the United States' relations with Israel. The cyberattacks also serve to project influence on regional dynamics and support Iranian geopolitical objectives by disrupting critical infrastructure, stealing sensitive data, and spreading propaganda. This cyber warfare is a key element of Iran's asymmetric warfare approach, allowing it to challenge stronger adversaries without direct military confrontation. As tensions in the Middle East grow, more IRGC-CEC cyber operations will likely target entities in the United States and Israel, as well as in countries that are politically opposed to Iran.



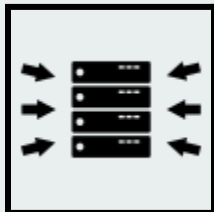
French Police Probe Ransomware Attack on Grand Palais Olympic Venue

What happened: French cybercrime police are probing a ransomware attack on the Grand Palais Réunion des musées nationaux (Rmn) in Paris, where Olympic events like fencing and Taekwondo are being held. The central computer system (which also oversees data for 40 smaller museums) was targeted, but no disruption to the Olympic events occurred.

- **What this means:** The Olympics have consistently been a prime target for cyberattacks and security threats due to its global visibility and high-profile status. While the attack did not disrupt the ongoing events, it underscores the broader risk of cyber threats during major international gatherings. The cybercriminals [demanded](#) a ransom and threatened to leak financial data, raising concerns about data security and the potential for broader impacts on affiliated museums. The data leak could result in significant financial losses for the museums, damage their reputation, and expose individuals to identity theft and fraud. With Paris hosting the Olympics, threat actors see an opportunity to exploit the global attention for financial gain or to cause operational chaos. As the Olympics attract global scrutiny, maintaining operational integrity and safeguarding sensitive data becomes crucial for organizers and affiliated institutions. Just ahead of the Paris Olympics, many threat actors have been [observed](#) collaborating to intensify distributed denial-of-service (DDoS) campaigns against France, leveraging their combined resources and expertise to disrupt the event. Meanwhile, "SN_Blackmeta" has reportedly launched an attack on La Poste, France's national postal service. La Poste's official website was allegedly inaccessible for some time. The original post can be found on the group's Telegram channel ([hXXps://t\[.\]me/SN_Darkmeta](https://t.me/SN_Darkmeta)). This breach can potentially cause significant disruptions in mail processing and delivery operations, compounding the challenges of managing logistics during the high-profile international event. The attack appears to exploit the heightened activity and increased data flow associated with the Olympics.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings



New Pro-Russia Threat Actor Group Emerges, Targets NATO Member States

What happened: On August 1, 2024, new pro-Russia threat actor group “KozSec” announced its presence on Telegram, claiming to be “a formidable hacktivist collective driven by a passion for democracy and human rights” that uses its “advanced cyber skills to challenge oppressive regimes worldwide.” According to the post, KozSec’s goal is to expose corruption, advocate for freedom of speech, and protect civil liberties as they relate to what the group perceives as violations of Russia’s physical and digital sovereignty by Western powers. According to the same post, KozSec’s operations range from disrupting censorship measures and leaking government data to sparking global debates and mobilizing online communities in protest. Elsewhere on its Telegram channel, the group claimed to have carried out a DDoS attack against the telecommunications company Vodafone in Ukraine. KozSec also reportedly plans to target NATO member states in the near future, as well as conduct a DDoS attack on Movistar, a Spain-based telecommunications company.

- **What this means:** Threat actors that rely on DDoS attacks as their main cyber operations technique are not necessarily considered technologically advanced. However, as KozSec has just emerged onto the cybercriminal scene, it is highly possible that they plan on leveraging other attack techniques in the near future. KozSec’s operations are notable due to their targets and the surrounding geopolitical climate that can exacerbate DDoS attacks. Attacking Vodafone, a leading telecommunications provider on the European continent, has the potential to cause significant operational disruption—particularly in Ukraine, where a range of military communications and functions occur continuously. While unlikely, possible disruptions to communications surrounding high-risk military operations could cause strategic losses or even fatalities. These strategic battleground losses could tilt the scale in Russia’s favor in its war with Ukraine, which would almost certainly flame the historically contentious relationship between Russia and NATO. ZeroFox will continue to monitor for additional and/or escalated actions by KozSec to better understand the threat level the group may pose to Western interests and NATO member-state security.



Canadian Financial Services Company Falls Victim to Lynx Ransomware

What happened: On August 6, 2024, ZeroFox observed an update on the Lynx Ransomware leak site targeting The Pyle Group, a Canada-based financial services company that specializes in portfolio management and financial planning. The post lists The Pyle Group's income as 5 million (no currency specified) but does not include a ransom demand or the amount of data the group has obtained. While the post also does not explicitly state the type of data the group is holding for ransom, samples of documents attached to the post indicate that financial data is involved. However, ZeroFox cannot confirm whether the financial data is company-specific or customer-specific.

- **What this means:** As a financial service provider, The Pyle Group holds sensitive client information—including financial records, personal details, and investment strategies—which could be compromised in this attack. This breach could not only expose sensitive data but also significantly damage the company's reputation and erode client trust. Additionally, financial services firms are bound by strict data protection regulations, and a breach could lead to regulatory scrutiny, fines, and legal consequences.



Threat Actor Publishes Breached Data from National Public Data

What happened: On August 6, 2024, threat actor "Fenice" posted a link on the dark web forum BreachForums that allows users to download a dataset related to a breach affecting National Public Data, a U.S.-based public records data provider and background check company. Earlier this year, on April 7, 2024, threat actor "USDoD" posted a sample of data associated with National Public Data on BreachForums. Sources reported that USDoD acted as the middleman for the initial post; both actors—Fenice and USDoD—credited actor "SXUL" for the breach. Fenice claims to possess a 277 GB uncompressed data package and has shared a password to access these files. The leaked data includes first, middle, and last names; dates of birth; addresses; phone numbers;

Social Security numbers (SSNs); and more. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

- **What this means:** This breach has reportedly compromised the personal information of approximately 2.9 billion individuals. Specifically, the exposure of SSNs significantly heightens the risk of identity theft and financial fraud, as SSNs can be exploited for various illicit activities such as opening fraudulent accounts or filing false tax returns. The enormity of this breach—potentially one of the largest in recent history—also puts National Public Data (also known as Jerico Pictures Inc.) in jeopardy of facing substantial legal consequences and lawsuits, amplifying the impact of this security failure on both individuals and the company itself.

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, technology, and security domains. Last week, CISA [added](#) three vulnerabilities to its Known Exploited Vulnerabilities Catalog. CVE-2018-0824 is a remote code execution (RCE) vulnerability and a frequent attack vector for malicious cyber actors that [poses](#) significant risks to federal enterprise. The second one, CVE-2024-36971, is a patched use-after-free (UAF) bug in the Linux kernel's network route management. The third, CVE-2024-32113, is a critical (CVSS score: 9.8/10.0) path traversal vulnerability in Apache OFBiz that could [allow](#) for RCE. With a CVSS score of 9.8, CVE-2024-38856 (another critical bug in the Apache OFBiz system) can let attackers [access](#) critical endpoints via specially crafted requests, raising the possibility of exfiltration. Threat actors are likely [exploiting](#) it to conduct arbitrary code execution without user interaction on unpatched devices. CISA has also [released](#) an ICS advisory addressing a high-severity vulnerability in Delta Electronics products (CVE-2024-7502). South Korea's National Cyber Security Center (NCSC) has [reported](#) that state-backed North Korean hackers exploited vulnerabilities in a VPN's software update to deploy malware and breach networks in South Korea; "Kimsuky (APT43)" and "Andariel (APT45)" have been identified as the threat groups involved. Google Chrome's new version 127.0.6533.99 has [addressed](#) six vulnerabilities, including a critical out-of-bounds memory access flaw (CVE-2024-7532) in the Angle component. Mozilla has [released](#) Firefox version 129, containing patches for 14 vulnerabilities. Among them, 11 are rated as "high severity," while two are classified as "moderate" and one as "low." Researchers have [discovered](#) a bug termed "GhostWrite" in T-Head XuanTie C910 and C920 RISC-V CPUs. The vulnerability lets unprivileged attackers read, write any memory, and control peripherals, bypassing security features. Fixing it requires disabling nearly half of the CPU's functionality.



CRITICAL

CVE-2024-4885

What happened: Cybersecurity researchers have observed threat actors exploiting this RCE bug in Progress WhatsUp Gold, targeting exposed servers for initial access to corporate networks. It has been rated **CRITICAL** (CVSS score: 9.8/10.0)

- **What this means:** Exploits for CVE-2024-4885 have been in use since August 1, with proof-of-concept code publicly available. Once exploited, the bug grants attackers elevated privileges, enabling them to run commands, access sensitive data, and

potentially take control of the entire system. It could lead to unauthorized access to corporate networks, data breaches, and persistent backdoors, such as webshells. Organizations using affected versions of WhatsUp Gold are at high risk if necessary updates or security measures are not applied to protect systems from these active exploits.

- **Affected products:** Progress WhatsUp Gold versions released before 2023.1.3



CRITICAL
CVE-2024-38856

What happened: This Critical (CVSS score: 9.8) RCE vulnerability was discovered in Apache OFBiz, an open-source enterprise resource planning (ERP) system. This flaw allows attackers to exploit the system via a crafted request due to an issue in the override view functionality.

- **What this means:** Exploiting this flaw could enable attackers to access sensitive endpoints, potentially leading to data theft and unauthorized lateral movement within an organization's network. This could compromise various business processes managed by OFBiz, including accounting and customer relationship management. Organizations should immediately upgrade to version 18.12.15 or newer to mitigate this risk.
- **Affected product:** Apache OFBiz version 18.12.14

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Intelligence: Global Ransomware News

What happened: ZeroFox has

observed around 70 ransomware attacks in the past seven days, mostly on the manufacturing sector and primarily conducted by the RansomHub ransomware group. Over 50 percent of these targeted industries are in North America.

Meanwhile, U.S. and German law enforcement (LE) [seized](#) the domain of Cryptonator, a cryptocurrency wallet platform, and indicted its operator on charges of money laundering and running an unlicensed money service

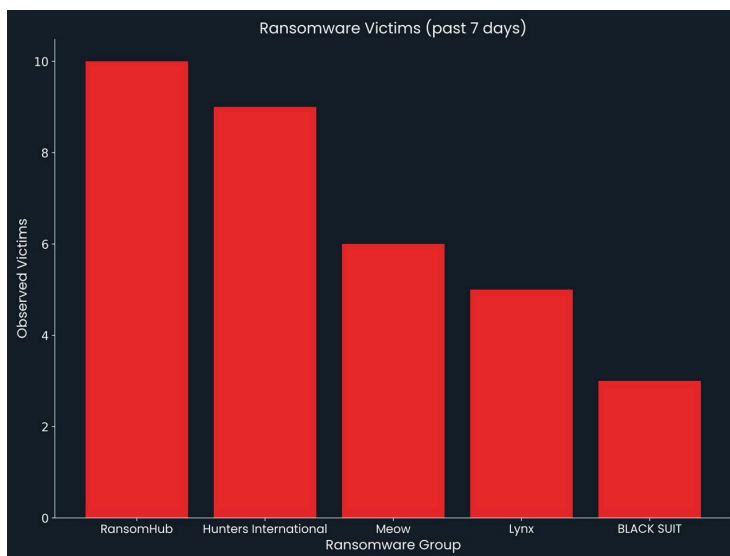
business. French cybercrime police are [probing](#) a

ransomware attack on the Grand Palais Rmn in Paris,

where Olympic events like fencing and Taekwondo are being held. CISA and the FBI [announced](#)

that the “Royal” ransomware group, which has been operating for over two years, has rebranded as “BlackSuit” and has demanded over USD 500 million from its victims. The United Kingdom’s Information Commissioner’s Office (ICO) has [issued](#) a provisional decision to levy a GBP 6.09 million (USD 7.74 million) fine on Advanced Computer Software Group Ltd (Advanced) for failing to protect the personal data of tens of thousands of individuals during a ransomware attack in 2022.

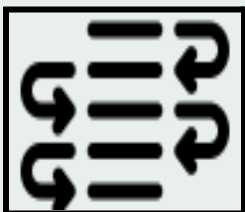
The “Hunters International” ransomware group is [targeting](#) IT professionals with a new C# remote access trojan (RAT) named SharpRhino. This malware allows the group to gain initial access, escalate privileges on infected systems, execute PowerShell commands, and ultimately deploy its ransomware payload. Keytronic, an electronic manufacturing services provider, has [disclosed](#) losses exceeding USD 17 million from a ransomware attack in May. According to a filing with the U.S. Securities and Exchange Commission (SEC), the company detected the breach on May 6,



Source: ZeroFox Internal Collections

following disruptions at its facilities in Mexico and the U.S. that affected business applications crucial to both operational and corporate functions.

- **What this means:** The Department of Justice (DOJ) alleges that the operator of Cryptonator allowed illicit activities on the platform and failed to comply with know-your-customer (KYC) regulations. The seizure of Cryptonator by LE and partners highlights the growing crackdown on platforms facilitating illegal activities in the cryptocurrency space. By targeting entities linked to ransomware, darknet markets, and other illicit services, authorities aim to disrupt financial networks supporting cybercrime and terrorism. The case emphasizes the importance of stringent KYC regulations and the need for compliance in financial transactions. Additionally, the indictment and potential penalties serve as a warning to other operators of unregulated cryptocurrency services. While the attack at Grand Palais did not disrupt the ongoing Olympic events, it underscores the broader risk of cyber threats during major international gatherings. The attackers [demanded](#) ransom and threatened to leak financial data, posing significant financial losses, reputational damage, and exposing individuals to identity theft and fraud. BlackSuit ransomware attacks have spread across numerous critical infrastructure sectors, including—but not limited to—commercial facilities, healthcare and public health, government facilities, and critical manufacturing. CISA has [released](#) a #StopRansomware: BlackSuit (Royal) Ransomware advisory, which provides network defenders with recent and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs) associated with BlackSuit and legacy Royal activity. The ICO's fine on Advanced Computer Software for failing to secure personal data during a ransomware attack reflects the rising scrutiny and penalties for data protection failures. Additionally, Hunters International's deployment of the SharpRhino RAT and Keytronic's significant financial loss from a ransomware attack underscore the severe and evolving nature of cyber threats. These developments highlight the urgent need for robust cybersecurity measures and regulatory oversight to protect against sophisticated cybercrime.



Breach Disclosure: Data Security Incidents and DDW Leaks

What happened: A data breach affecting Mobile Guardian, a globally used digital classroom management platform, has wiped data from over 13,000 students' systems. The company has [confirmed](#) that a hacker gained unauthorized access to the platform, impacting its instances in

North America, Europe, and Singapore. National Public Data, owned by Jerico Pictures, has [suffered](#) a massive breach; threat actor Fenice leaked people's personal details (including full names, addresses, and SSNs) in plain text on [BreachForums](#). The breach amounted to a total of 2.9 billion records, putting affected individuals at risk for identity theft and financial fraud. Earlier (on April 7, 2024), threat actor USDoD posted a sample associated with the National Public Data breach on BreachForums. It was reported that actor USDoD was a middle man for the initial posting. Both Fenice and USDoD credited threat actor SXUL for the breach. American building security giant ADT confirmed a data breach [wherein](#) threat actors accessed certain databases associated with ADT customer order information. The company reportedly took steps to shut down the unauthorized access and launched an investigation, collaborating with third-party cybersecurity experts. The attackers obtained some limited ADP customer information, including email addresses, phone numbers, and postal addresses.

- **What this means:** In response to the Mobile Guardian breach, the Singaporean Ministry of Education has announced the removal of the Mobile Guardian Device Management Application from all iPads and Chromebooks in the country. Among the affected users are students from secondary schools. Although investigations have yet to reveal the type of information exposed, it is likely to include sensitive information such as student names, addresses, grades, and behavioral records. The personal data of the users, including minors, can be exploited for identity theft, cyberbullying, and phishing attacks. Attacks that affect personally identifiable information (PII) can expose confidential data to malicious adversaries with geopolitical and financial motives to interfere or cause significant damage to a country's infrastructure. The National Public Data breach poses severe, long-term risks, such as fraudulent credit accounts, loans, and tax returns and has the potential to lead to significant financial losses and legal battles for both the victims and Jerico Pictures. In the ADT incident, ZeroFox observed that the threat actor "netnsher" reportedly [leaked](#) customer data associated with ADT. The threat actor claims that the leaked data includes more than 30,000 customer records, including email addresses, physical addresses, user IDs, and the products purchased.

| Physical and Geopolitical Intelligence |

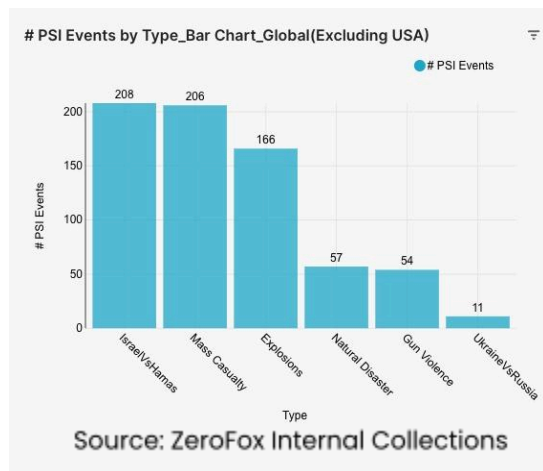
Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was an 18 percent increase 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 countries accounted for approximately one half of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 35 percent from the previous week.

Additionally, events related to Russia's war in

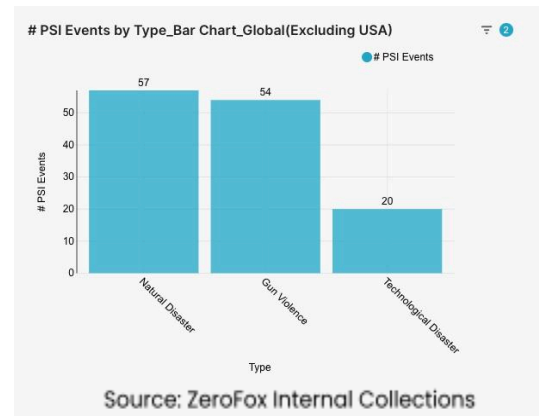
Ukraine increased by 38 percent. The top three most-alerted subtypes were explosions, which saw a 44 percent increase from the previous week; gun violence, which increased by 13 percent; and natural disasters, which decreased by 3 percent.



- **What this means:** This week, Ukrainian conflict-related alerts as well as explosions showed a significant increase, likely due to Ukraine's recent offensive efforts in the Kursk Oblast region. On Tuesday, at least 1,000 Ukrainian [forces](#) supported by tanks and armored vehicles crossed the Russian border and have been advancing ever since; there are speculations that this is an attempt to redirect Russian brigades away from Kyiv, but this has not been confirmed. As for the Israel-Hamas War, which also saw a significant increase in alerts, Israeli forces have stepped up attacks across the occupied West Bank, including an [attack](#) on a school over the weekend that killed at least 15 people. On Wednesday, Israeli forces raided the Balata refugee camp near the city of [Nablus](#) and carried out air raids in Jenin the day prior that killed at least 12 people. Gun violence alerts also saw an increase, with the top contributing country this week being Guatemala. Over the years, Guatemala has generally had a high level of firearm-related [homicides](#) due to ongoing gang violence and a weak judicial system, so this is not unexpected. Overall, this week saw an increase in mass casualty events across the board.

Physical Security Intelligence: United States

What happened: In the past week, the top three most-alerted incident subtypes were natural disasters, gun violence, and technological disasters. Natural disaster alerts typically involve fires and severe weather; gun violence alerts are instances in which there is a confirmed or likely confirmed victim; and technological disasters refer to instances of man-made disasters, such as building collapses, hazmat situations, and large-scale transportation accidents. The top two states that had the most gun violence alerts were Illinois and California, which together made up over one-quarter of this week's nationwide total (29 percent). Gun violence across the United States overall increased by 3 percent from the week prior. The top two contributors to natural disaster alerts this week were Florida and California, and natural disaster alerts across the country decreased by 3 percent. Technological disaster alerts increased by 54 percent, and the top contributing states were Ohio and Maryland.



- **What this means:** While natural disaster numbers as a whole saw a very slight decrease, Florida led the way as the top contributing state, accounting for approximately 20 percent of all natural disaster alerts this week. This is undoubtedly due to the arrival of tropical storm [Debby](#), which killed five people in Florida and left hundreds of thousands without power. It will likely continue to cause issues along the East Coast of the country, as the storm is continuing to move north to the Carolinas and Virginia. Technological disasters saw a very large increase this week, with the majority of these events being hazmat-related. For instance, in Ohio, there was a butane [leak](#) from a railcar that was carrying over 150,000 pounds of the chemical. Fortunately no one was injured, and the leak was successfully contained. Gun violence saw a slight increase, with Chicago and Los Angeles once again contributing to a significant number of these alerts. For example, in Chicago, 45 people were [shot](#) over the weekend, five of whom were killed.

| 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%