



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 9, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EST) on December 6, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 20	2
 Cyber and Dark Web Intelligence Key Findings	4
FTC Takes Action Against Illegal Sale of Sensitive Location Data	4
Poland Probes Illegal Spyware Deployment by Former Leaders	5
North Korean Hackers Leverage Russian-Sourced Emails for Credential Theft	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-42448	8
CVE-2024-20397	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Attacks Target Football Clubs and Energy Sector Entities	11
High-Profile Data Breaches with Severe Implications	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 20](#)

The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

| **Cyber and Dark Web Intelligence** |

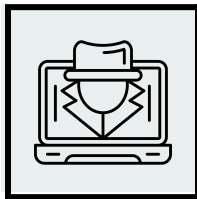
| Cyber and Dark Web Intelligence Key Findings



FTC Takes Action Against Illegal Sale of Sensitive Location Data

What happened: The Federal Trade Commission (FTC) has accused data brokers Mobilewalla, Inc. and Gravy Analytics of unlawfully tracking and selling sensitive location data. Mobilewalla allegedly [collected](#) private addresses and sold the information without taking reasonable steps to verify consumers' consent. Under the FTC's proposed settlement order, Mobilewalla will also be banned from collecting consumer data from online advertising auctions for purposes other than participating in those auctions. Meanwhile, Gravy Analytics and its subsidiary, Venntel, illegally [tracked](#) and sold sensitive location data from users—including sensitive private data about consumers. As per the FTC, Gravy Analytics and Venntel will be prohibited from selling, disclosing, or using sensitive location data in any product or service and must establish a sensitive data location program.

- **What this means:** Gravy Analytics and Venntel—via suppliers and apps—collected precise location data from mobile devices tied to Mobile Advertising IDs (MAIDs), amassing over 17 billion daily signals. They sold this data to commercial and government clients, revealing sensitive details like medical conditions, political activities, and religious beliefs. Additionally, Mobilewalla sourced consumer location data and personal information indirectly from real-time bidding (RTB) exchanges and data brokers, without consumers' knowledge. It collected data, including MAIDs and app usage details, to build detailed profiles for purposes of advertising, political campaigns, and even tracking union organizers. Unchecked data brokering practices enables invasive surveillance, profiling, and potential misuse for targeted manipulation, discrimination, or physical tracking. In the wrong hands, confidential, sensitive data of individuals is likely to be weaponized against the data owner, whether for influencing political decisions, suppressing union activities, or violating personal privacy and security.



Poland Probes Illegal Spyware Deployment by Former Leaders

What happened: Poland's current government, led by Donald Tusk, is investigating alleged abuses of Pegasus spyware by the previous Law and Justice (PiS) administration. The former internal security chief was arrested after ignoring three summons to testify before a parliamentary committee. Reports indicate that Pegasus was used against three government critics, including a senator targeted multiple times before the 2019 elections. Amnesty International and other institutions confirmed these findings, and a 2023 Polish Senate report [deemed](#) the spyware's use unlawful.

- **What this means:** The final report by Poland's Senate Special Commission on Illegal Surveillance reveals systemic abuse of Pegasus spyware by the previous government under the PiS party, targeting critics without legal justification. High-profile figures such as members of the parliament and others were spied on, violating constitutional standards and undermining the fairness of the 2019 elections. The report confirms the illegal procurement and use of Pegasus, describing it as a "cyber weapon" that manipulated political processes. Advocacy groups—including Amnesty International—have, in the past, [emphasized](#) the urgent need to regulate spyware like Pegasus to prevent its misuse. Authorities allegedly used Pegasus against opposition figures, including a [member](#) of the Polish Senate, potentially undermining the integrity of Poland's 2019 parliamentary elections and democratic processes. Poland's ruling party reportedly misused public funds—meant to be set aside to aid crime victims and rehabilitate offenders—to purchase Pegasus and deploy it against political critics, indicating abuse of power.



North Korean Hackers Leverage Russian-Sourced Emails for Credential Theft

What happened: North Korea's advanced persistent threat (APT) group Kimsuky has been orchestrating a series of sophisticated phishing campaigns to steal user credentials in Japan and South Korea. These attacks typically involve emails that appear to come from Russian sender addresses, using domains associated with VK's Mail[.]ru service—including trusted email domains like mail[.]ru, internet[.]ru, bk[.]ru, inbox[.]ru, and list[.]ru. Kimsuky exploits these domains to impersonate trusted entities, such as financial institutions and popular internet services like Naver

(South Korea's search engine and online platform). One of the group's common tactics involves phishing emails masquerading as notifications from Naver's MYBOX cloud storage, falsely alerting users to the presence of malicious files in their accounts and urging them to click on links to delete these supposed threats. Often crafted to invoke a sense of urgency, these emails aim to deceive recipients into disclosing sensitive information or downloading malware.

- > **What this means:** The use of these phishing techniques suggests that Kimsuky is relying heavily on social engineering to bypass security defenses. By sending emails that appear to come from trusted sources, the group manipulates victims into taking immediate actions, such as providing sensitive login credentials or downloading malicious files. Once credentials are harvested, the threat actors can access personal and business accounts, launching further attacks that likely lead to data theft, espionage, or corporate network infiltration. Such attacks can also be leveraged for politically motivated operations to extract sensitive government, military, and diplomatic information. The group uses legitimate tools like PHPMailer and Russian email services, which allow it to maintain operational secrecy and evade detection for longer periods. Furthermore, the use of compromised accounts not only threatens individual and organizational security but also weakens trust in email and cloud-based 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 technology, software development, industrial control systems (ICS), and government services. Japan's computer emergency response team (CERT) has [issued](#) an alert about zero-day vulnerabilities in I-O Data router devices that threat actors are exploiting to modify device settings, execute commands, or even turn off the firewall. A proof-of-concept (PoC) exploit for a critical remote code execution flaw (CVE-2024-8785) in Progress WhatsUp Gold has been [released](#). It allows unauthenticated attackers to modify Windows registry keys remotely, enabling the execution of malicious code. [CVE-2024-41713](#) is a path traversal vulnerability in the NuPoint Unified Messaging (NPM) component of Mitel MiCollab that could allow an unauthenticated attacker to conduct a path traversal attack due to insufficient input validation. This vulnerability is exploitable without authentication. In the past week, CISA [added](#) a total of four vulnerabilities to its Known Exploited Vulnerabilities [catalog](#). CISA also [released](#) 10 ICS [advisories](#) to provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

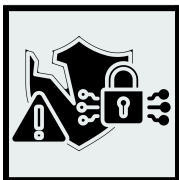


CRITICAL

CVE-2024-42448

What happened: Veeam has released security updates to address two vulnerabilities in its Service Provider Console (VSPC), a platform used by service providers to manage Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS). CVE-2024-42448 allows attackers to execute arbitrary code on unpatched servers by exploiting the VSPC management agent machine.

- **What this means:** This vulnerability was discovered during Veeam's internal testing and could be exploited if an attacker gained access to the management agent's machine, which has authorized access to the VSPC server. If successfully exploited, the attacker could likely execute arbitrary code on the VSPC server, potentially gaining full control of the system. This could lead to disruptions in backup and recovery operations or theft of sensitive data. To prevent exploitation and protect their systems from remote attacks, organizations using Veeam's platform are advised to apply the patches urgently.
- **Affected products:**
 - VPSC 8.1.0.21377 and all earlier versions 8 and 7 builds

**MEDIUM****CVE-2024-20397**

What happened: A vulnerability in the bootloader of Cisco NX-OS Software could allow an unauthenticated attacker with physical access to an affected device (or an authenticated, local attacker with administrative credentials) to bypass NX-OS image signature verification. Cisco has released software updates that address this vulnerability.

- **What this means:** This vulnerability is due to insecure bootloader settings. An attacker could exploit this vulnerability by executing a series of bootloader commands. A successful exploit could take advantage of this vulnerability and load unverified software.
- **Affected products:**
 - MDS 9000 Series Multilayer Switches (CSCwh76163)
 - Nexus 3000 Series Switches (CSCwm47438)
 - Nexus 7000 Series Switches (CSCwh76166)
 - Nexus 9000 Series Fabric Switches in ACI mode (CSCwn11901)
 - Nexus 9000 Series Switches in standalone NX-OS mode (CSCwm47438)
 - UCS 6400 Series Fabric Interconnects (CSCwj35846)
 - UCS 6500 Series Fabric Interconnects (CSCwj35846)

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



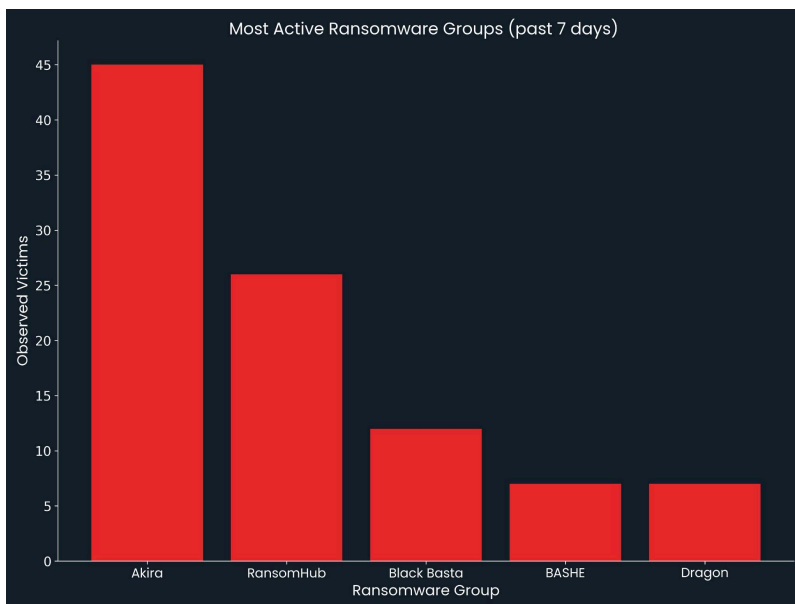
Ransomware Attacks Target Football Clubs and Energy Sector Entities

What happened: In the past seven days, ZeroFox has observed more than 150 ransomware attacks, most of which were detected in North America. The most affected sector was Manufacturing, followed by Healthcare, with the most active ransomware group being Akira. RansomHub ransomware group [claimed](#) responsibility for targeting Italian professional football club Bologna Football Club 1909 S.p.A. and leaked samples of the

allegedly stolen data, including contracts, medical data, information on young players, commercial strategies, and

business plans. McLeod Russel India [confirmed](#) a ransomware attack that affected its IT systems; the company's management initiated measures to minimize the impact. ENGlobal Corporation, a U.S. engineering services firm serving the Energy and Defense sectors, [experienced](#) a ransomware attack, where threat actors disrupted operations and encrypted files. While no group has claimed responsibility, ENGlobal has restricted employee IT access to essential functions and is investigating the incident. A Russian cybercriminal linked to the LockBit and Hive ransomware groups has reportedly been [arrested](#). They have allegedly conducted significant attacks against entities in the United States, global businesses, and critical infrastructure. INTERPOL has [launched](#) the "Think Twice" campaign to raise awareness about the rising threat of cyber and financial crimes targeting vulnerable individuals and organizations. The campaign highlights five growing online threats, including ransomware.

- **What this means:** Bologna Football Club 1909 S.p.A. [confirmed](#) its security systems were affected in the ransomware attack, affecting both a cloud server and its internal network. If the leaked confidential data—including medical records and contract details—is



Source: ZeroFox Internal Collections

legitimate, it is likely to expose owners to cyber threats like extortion, scams, blackmail, and doxxing. Even though the ransomware attack on McLeod Russel had no material impact on its internal systems, it is yet another example of how financially motivated actors pose a significant threat to businesses globally. ENGlobal Corporation confirmed that threat actors gained unauthorized access to its IT systems and encrypted some data files. This attack closely follows other ransomware incidents targeting entities in the energy sector, including those targeting Costa Rica's state-owned energy provider [RECOPE](#) and Texas-based oilfield supplier [Newpark Resources](#). The arrest of the LockBit and Hive operative resulted from law enforcement targeting of an extensive cybercrime network and exposed the scale of the damage caused. It could help prevent further financial losses and reputational harm from LockBit and Hive's ransomware campaigns. The "Think Twice" campaign aims to reduce online scam risks by educating users on being more cautious about unsolicited digital interactions, verifying identities, and pausing before engaging with suspicious content.



High-Profile Data Breaches with Severe Implications

What happened: Russian APT group "Turla" has [exploited](#) access to the Pakistan-based Storm-0156 hacking group's command-and-control (C2) servers since 2022 to launch its own cyber operations. The campaign primarily targets Afghan government entities with custom malware. In [Romania](#), declassified documents show "aggressive hybrid Russian attacks" and campaigns that targeted consecutive elections, including leaking access data for election websites on Russian cybercrime platforms. Romania's intelligence agency also identified over 85,000 cyberattacks aiming to target system vulnerabilities. The group allegedly exfiltrated over 1 terabyte of compressed sensitive data. ZeroFox also [observed](#) threat actor "Ciph3r" claiming to have hacked a database associated with Malaysian Nuclear Agency on predominantly English-language dark web forum BreachForums. According to Ciph3r, they have accessed 180 CSV files that contain 1,650,000 rows of data. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

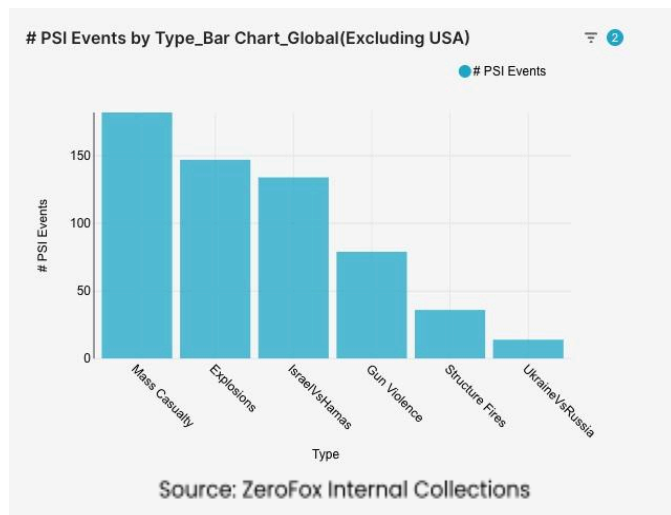
- **What this means:** Turla has been operating using malware strains like TwoDash (a downloader) and Statuezy (a clipboard-monitoring trojan) for targeted espionage. This persistent and stealthy campaign can potentially breach sensitive networks, compromising diplomatic and military operations while allowing long-term data exfiltration. The use of compromised C2 servers further complicates detection and

attribution, increasing the risk of broader exploitation by other threat actors. In the Malaysian Nuclear Agency breach, Ciph3r clarified that the database is not currently for sale and that they are in negotiations with the system administrator. In the event an agreement is not reached, the actor has threatened to sell the data within “a few days.” This organization focuses on research and development in the field of nuclear science and technology in Malaysia. If the breached data is leaked, confidential information regarding controls and other functions that keep nuclear facilities safe may be exposed. Additionally, the leaked data is likely of interest to Malaysia’s geopolitical rivals, who can leverage such information in further targeted and coordinated attacks.

Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

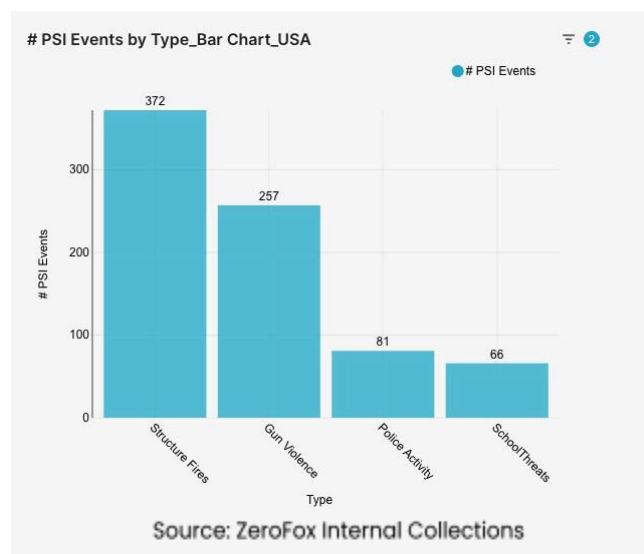


What happened: Excluding the United States, there was a 9 percent increase in mass casualty events this week from the previous week, with the top contributing countries being Palestine, Syria, and Lebanon, in that order. Approximately 81 percent of these events were explosions, and the three aforementioned countries accounted for about 45 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. Events related to Russia's war in Ukraine decreased by 13 percent. The top three most-alerted subtypes were explosions, which saw a 12 percent increase from the previous week; gun violence, which increased by 114 percent; and structure fires, which increased by 9 percent. Global protest activity decreased by 3 percent.

- **What this means:** This week's data saw a notable shift, with Syria replacing Israel as the country with the second-highest mass casualty instances. Typically, explosions and alerts related to the conflict in Israel will trend in the same direction (i.e., if one increases, so does the other); however, this week, explosions increased despite the significant decrease of Israel-Hamas alerts. This is due to Syrian opposition group Hayat Tahrir al-Sham (HTS) launching a large-scale [attack](#) on Syrian government forces, which resulted in the [capture](#) of Aleppo as well as Hama. The Syrian government, which relies heavily on Iranian and Russian backing to stay in power, has weakened due to Russia's primary focus being on Ukraine and the death of several Iran-allied Hezbollah leaders. HTS is now pushing further south to capture [Homs](#). As for Israel, the [ceasefire](#) between it and Lebanon is still in place, although both sides have accused the other of violating the agreement. On Monday night, Israeli strikes on two southern Lebanese villages killed at least 10 people, which was supposedly a response to a Hezbollah attack on Israeli military positions in the Shebaa Farms. Whether the ceasefire will last the full 60 days remains unclear at this point.

Physical Security Intelligence: United States



What happened: In the past week, the top three most-alerted incident subtypes were structure fires, police activity, and gun violence. Structure fire alerts are for fires that affect man-made buildings, police activity alerts involve law enforcement presence for generalized threats or for unknown reasons, and gun violence alerts are instances in which there is a confirmed or likely confirmed shooting victim. . The top two states that had the most gun violence alerts were Illinois and California, which together made up 21 percent of this week's nationwide total. Gun violence across the United States decreased by 13

percent from the week prior. Police activity alerts decreased by 25 percent, and the top contributing states were California and Florida. Structure fires increased by 12 percent, and the top two states for this subtype were New York and Texas.

- > **What this means:** This week, structure fires were the most alerted subtype, which is unsurprising due to [Thanksgiving](#) Day typically having the highest number of cooking fires throughout the year. Ideologically motivated crimes and killings may still happen. UnitedHealthcare CEO Brian Thompson was fatally [shot](#) on Wednesday, and the manhunt for the suspect is still underway at this time. The words on the three bullets used to kill Thompson said "deny," "defend", and "depose," which echo the title of the 2010 book *Delay, Deny, Defend: Why Insurance Companies Don't Pay Claims and What You Can Do About It*. In light of this, police are investigating whether anger at the insurance industry is a possible motive in this attack.

| 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%