



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

February 10, 2025

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 February 7, 2025**; 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 5, Issue 2	2
 Cyber and Dark Web Intelligence Key Findings	4
Phishing Campaign Hijacks High-Profile Users' X Accounts	4
CISA Releases Guidance on Edge Devices	4
WhatsApp Flags Zero-Click Attack Attributed to Spyware Firm	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2025-24891	8
CVE-2025-0960	9
 Ransomware and Breach Intelligence Key Findings	11
ZeroFox Observes Ransomware Activities with High Victim Numbers	11
Notable Breaches of the Past Week	13
 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

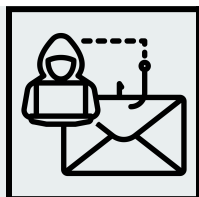
| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 2](#)

The Underground Economist is an intelligence-focused series illuminating dark web findings from our ZeroFox Dark Ops intelligence team.

| **Cyber and Dark Web Intelligence** |

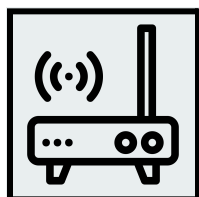
| Cyber and Dark Web Intelligence Key Findings



Phishing Campaign Hijacks High-Profile Users' X Accounts

What happened: An ongoing phishing campaign is targeting high-profile X accounts (formerly, Twitter), including political figures, journalists, and tech organizations, in an attempt to hijack them for fraudulent purposes. While primarily focused on X, the attackers also target other social media platforms to achieve financial gain. Phishing lures include fake login alerts that trick users into clicking malicious links in order to steal their credentials. Other tactics involve copyright violation scams, prompting victims to enter their X credentials on fraudulent sites. The attackers were observed stealing credentials, locking out the owner, and then posting fraudulent crypto schemes to target more victims.

- **What this means:** This campaign exploits the trust that users have in high-profile accounts, making it easier for attackers to deceive them into falling for cryptocurrency scams. Additionally, the campaign's tools can bypass email security filters, allowing the attackers to target even cautious users. This indicates that, in addition to being vigilant about opening suspicious emails, it is important to also verify URLs and not rely on platform security alone. Since the campaign is not limited to X, attackers are likely using credential stuffing, phishing kits, or malware to compromise accounts on multiple social media and crypto-related platforms. High-profile X accounts are prime targets, and hijacking them provides immediate access to large audiences. Once compromised, these accounts are used to promote fraudulent crypto schemes, tricking a large scale of followers into financial scams. This tactic likely allows attackers to rapidly maximize their profits before detection and takedown.



CISA Releases Guidance on Edge Devices

What happened: Cybersecurity and Infrastructure Security Agency (CISA)—in partnership with international and U.S. organizations—released guidance to help organizations protect their network [edge devices and appliances](#), such as firewalls, routers, Virtual Private Network (VPN)

gateways, Internet of Things (IoT) devices, internet-facing servers, and internet-facing operational technology (OT) systems. Edge devices are network hardware or software components that bridge internally managed networks and external, untrusted networks such as the internet. These devices can connect corporate networks to the internet and provide controlled connectivity to protected internal networks, as well as enable traffic flow.

- **What this means:** Edge devices like firewalls, routers, VPN gateways, and internet-facing servers are an important part of many enterprise computing systems. They allow connection across various devices that aid in productivity. However, as with many technologies, they are not without their vulnerabilities. Edge devices require attention and diligence to keep data safe and secure, as they are prime targets for attackers. Strengthening their security reduces the risk of unauthorized access and lateral movement within networks. CISA's focus on firewalls, VPN gateways, IoT, OT, and internet-facing servers is likely an attempt to fortify the attack vectors foreign adversaries and cybercriminals typically exploit to infiltrate networks. Implementing these security measures is likely to prevent costly breaches, minimize legal liabilities, and protect organizations' reputations from damage due to cyber incidents.



WhatsApp Flags Zero-Click Attack Attributed to Spyware Firm

What happened: WhatsApp recently revealed that a targeted spyware campaign affected approximately 90 individuals, including journalists and members of civil society organizations. The attack was traced back to Paragon Solutions, an Israeli spyware firm, which reportedly used a zero-click exploit to compromise users without requiring them to click any malicious links. The attack was carried out by sending infected PDF files through WhatsApp groups. WhatsApp has taken immediate steps to address the issue, notifying the affected users and rolling out a security update to patch the vulnerability. The company has not disclosed the specific locations or identities of the targeted individuals, including whether any were based in the United States.

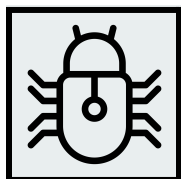
- **What this means:** This attack affected 90 individuals, including journalists and civil society members, posing a direct threat to press freedom by targeting those who rely on secure, encrypted communication for their work. As WhatsApp is a key platform for sharing sensitive information and documents and coordinating activities, such vulnerabilities can put journalists and activists at risk of surveillance, harassment, or even censorship. The spyware exploiting a vulnerability within WhatsApp suggests that even widely trusted communication tools are susceptible to targeted attacks. The "zero-click" nature of the

attack—where users do not have to interact with the malicious content for their devices to be compromised—makes it particularly dangerous, allowing attackers to exploit vulnerabilities without any action from the target, making it harder to detect and defend against. The campaign has likely exposed sensitive communication data, contributing to concerns about the potential use of commercial spyware to gather government intelligence. If such data falls into the wrong hands, it could be used for espionage, influencing policy decisions, manipulating political outcomes, or even fueling cyberattacks on critical infrastructure, putting both national security and international relations at serious risk. Similar to the NSO Group responsible for the infamous Pegasus spyware campaign, Paragon Solutions will likely face increased scrutiny if the allegations against it are proven true.

| **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 critical infrastructure. On February 6, 2025, CISA [released six Industrial Control Systems \(ICS\) advisories](#) providing information about current security issues, vulnerabilities, and exploits. Successful exploitation of these vulnerabilities allows for local privilege escalation, remote code execution (RCE), and machine-in-the-middle (MITM) attacks. CISA also added [five other vulnerabilities](#) addressing improper input validation and buffer overflow, among other things. On February 4, 2025, CISA added [nine more additional ICS advisories](#) and [four known exploited vulnerabilities](#) to the Known Exploited Vulnerabilities (KEV) catalog. In one of the web manager WeGIA's endpoints, an [SQL Injection vulnerability](#) could enable an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. CISA added [an information disclosure vulnerability](#) to its KEV catalog based on evidence of active exploitation. An attacker who successfully exploits this vulnerability could conduct RCE. [CVE-2024-53104](#) is a Linux Kernel out-of-bounds write vulnerability, which is a likely frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise. [CVE-2024-48510](#) is a vulnerability in drive composer that could enable attackers unauthorized access to the file system on the host machine. An attacker could exploit this flaw to run malicious code to compromise the affected system.



CRITICAL

CVE-2025-24891

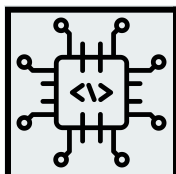
What happened: Dumb Drop is a file upload application that contains a path traversal vulnerability, allowing users with upload permissions to overwrite arbitrary system files. Since the container operates with root privileges by default, there are no restrictions on the files that can be modified. This vulnerability makes it possible to inject malicious payloads into files that are executed on a schedule or triggered by specific service actions. Additionally, because the service can run without authentication, it may grant root access to unauthenticated users or anyone who knows the PIN.

- **What this means:** The vulnerability in Dumb Drop allows users to overwrite critical system files and inject malicious code. Since the container runs with root privileges by default, attackers can modify or replace essential files without restrictions, potentially compromising the entire system. This could lead to the execution of unauthorized actions,

such as running malware or altering system processes. The lack of authentication further increases the risk, as unprivileged users or anyone with access to the PIN could gain root access, making the system vulnerable to exploitation.

➤ **Affected products:**

- Dumb Drop



CRITICAL

CVE-2025-0960

What happened: AutomationDirect C-more EA9 HMI contains a function with bounds checks that can be skipped, which could result in an attacker abusing the function to cause a denial-of-service (DoS) condition or achieving RCE on the affected device. AutomationDirect recommends that users update C-More EA9 HMI software and firmware to V6.80.

- **What this means:** Successful exploitation of this vulnerability could allow an attacker to cause a DoS condition or achieve RCE on the affected device. In case the patched version is not available, firms should deploy mitigations, like using more secure methods (such as VPNs). However, it is important to note that VPNs could also have vulnerabilities and should be updated to the most current version available.

Affected products:

- C-more EA9 HMI EA9-T6CL: v6.79 and prior
- C-more EA9 HMI EA9-T7CL-R: v6.79 and prior
- C-more EA9 HMI EA9-T7CL: v6.79 and prior
- C-more EA9 HMI EA9-T8CL: v6.79 and prior
- C-more EA9 HMI EA9-T10CL: v6.79 and prior
- C-more EA9 HMI EA9-T10WCL: v6.79 and prior
- C-more EA9 HMI EA9-T12CL: v6.79 and prior
- C-more EA9 HMI EA9-T15CL-R: v6.79 and prior
- C-more EA9 HMI EA9-T15CL: v6.79 and prior
- C-more EA9 HMI EA9-RHMI: v6.79 and prior

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

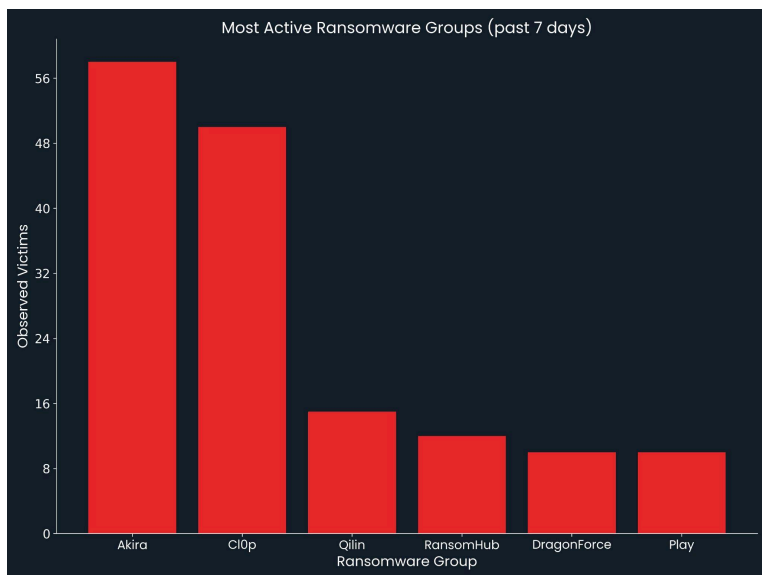


ZeroFox Observes Ransomware Activities with High Victim Numbers

What happened: In the past week, ZeroFox observed close to 200 ransomware attacks, a majority of which were detected in North America. The most affected sector was manufacturing, followed by retail, while the most active ransomware group was Akira. On February 5, 2025, ZeroFox observed Russia-based ransomware collective CI0p [releasing a third list of 50 undisclosed victims](#). The group has asked the companies included in the list to reach out, likely for ransom negotiations. On February 3, 2025, [Akira posted more than 30 new victims](#) on its leak site.

ZeroFox observed 26 new Akira victims on February 5, bringing the total number of target victims to 60. Meanwhile, [Tata Technologies](#) Ltd., one of India's key tech developers and state project contractors, suffered a ransomware attack that temporarily impacted its IT services. Ransomware groups like Sarcoma and DoNex are now embedding [ads in their ransom notes](#) to recruit insiders for company access. These notes promise financial rewards for employees willing to leak credentials or install malware. The ransomware group [LockBit is making a comeback](#) after last year's takedown by launching LockBit 4.0. The group has set up five onion links hosting login pages with registration options via Bitcoin or Monero.

- **What this means:** The group is revealing the victim names in alphabetical order; the second list had victim names beginning with A and B, while the current list includes victims with names starting with C and D. ZeroFox assesses that CI0p is likely following this approach to showcase the extensive list of victims in order to highlight the scale of its cyberattack. Operating under a ransomware-as-a-service (RaaS) model, Akira continues



Source: ZeroFox Internal Collections

to employ a double-extortion strategy, stealing and encrypting sensitive data before demanding ransom. The group's data leak site is divided into two sections: "leaks" (for victims who refused to pay) and "news" (for those still negotiating). All 60 victims are currently listed in the "news" section. Akira shows no signs of slowing down, and there will likely be more updates on its leak site in the coming days. This surge in activity highlights a significant increase in the group's operations and continued expansion. If the attackers managed to gain access to Tata Technologies' sensitive information, they could sell or exploit the company's intellectual property, use client data for fraud, or leak confidential project details, likely leading to both financial losses and legal consequences. Moreover, the company's involvement in state projects increases national security risks if sensitive data is compromised, potentially exposing critical infrastructure or defense systems to espionage, sabotage, or manipulation by hostile actors. Even though no ransomware group has taken responsibility for the attack yet, it is likely that the attackers are financially motivated, given Tata Technologies' status and the potential value of its intellectual property and sensitive data. Ransomware actors typically focus on financial extortion, demanding payment to decrypt systems. However, a change in traditional ransomware tactics (as seen with this new approach to recruiting affiliates) likely indicates a shift in objective, which is securing insider data that could enable deeper infiltration into company networks. Ransomware groups are now soliciting employees for insider access by asking for credentials such as remote desktop protocol (RDP) logins, VPN passwords, and corporate email accounts, which could broaden the affected company's attack surface to expose interconnected third-party services. LockBit's resurgence—despite law enforcement action—highlights the likely proliferation of ransomware groups on the dark web. As ransomware activity continues to increase, maintaining strong operational security and other cybersecurity best practices is essential for businesses and individuals in order to safeguard their information and assets.



Notable Breaches of the Past Week

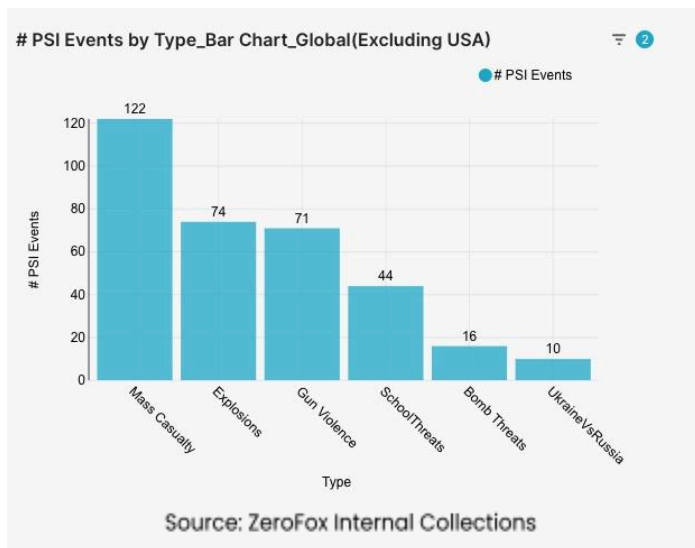
What happened: Hackers [compromised Casio UK's e-shop](#) (casio[.]co[.]uk) between January 14–24, 2025, injecting malicious scripts that stole customer credit card and personal information. Globe Life has concluded its investigation into a June 2024 [data breach](#) and revealed that the incident may have compromised the personal data of up to 850,000 customers. The healthcare industry continues to experience large-scale data breaches. Community Health Center (CHC)—a nonprofit healthcare provider in Middletown, Connecticut—is [notifying over one million patients](#) about a January 2 data breach in which a "skilled criminal hacker" accessed and stole sensitive patient information. Meanwhile, Moses-Weitzman Health System has [confirmed employee data was compromised](#), and the Chicago Department of Public Health (CDPH) disclosed exposure of patient data through a public health dashboard.

- **What this means:** Customers who made purchases from casio[.]co[.]uk between January 14–24, 2025, are likely to face risks of financial fraud and identity theft, while Casio faces increased scrutiny over its ability to protect sensitive customer data. The Globe Life breach exposed sensitive personal information, including Social Security numbers and health data; affected individuals are at risk of identity theft and fraud. Though CHC claims no operational disruptions or immediate misuse of data, the theft of detailed personal and medical information could expose affected patients to identity theft and insurance fraud. The healthcare sector is a lucrative target for data breaches because of the vast amounts of sensitive personal, medical, and financial information it holds. Such information could be exploited for identity theft, insurance fraud, and sold on black markets. Healthcare firms have a critical need to maintain uninterrupted operations, making them more likely to agree to hackers' demands to avoid disruptions. The CDPH's incident is an indication of how unsecured dashboards in public data sharing systems could expose medical details and other sensitive details.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

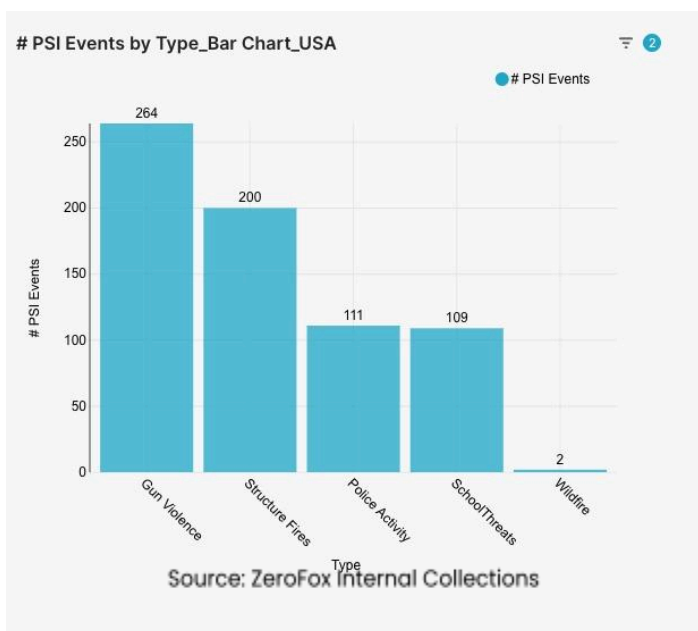


What happened: Excluding the United States, there was a 17 percent decrease in mass casualty events this week from the previous week, with the top contributing countries being Mexico, Palestine, and India (in that order). Approximately 61 percent of these events were explosions, with the three aforementioned countries accounting for about 37 percent of all mass casualty alerts. General alerts related to the Israel-Hamas conflict (including protests, raids, and involvement in neighboring countries) decreased by 21

percent from the previous week. Events related to the Russia-Ukraine war increased by 67 percent. The top three most-alerted subtypes were explosions, which saw a 20 percent decrease from the previous week; gun violence, which increased by 9 percent; and structure fires, which decreased by 6 percent. Global protest activity decreased by 13 percent. Notably, threats related to schools—excluding protest activity—increased by 33 percent.

- **What this means:** The Russia-Ukraine war saw the largest increase in events this week, with attacks ramping up while U.S. President Donald Trump and Ukrainian President Volodymyr Zelenskyy discuss potential [resolution](#) plans. The plans reportedly entail Ukraine supplying the United States with rare-earths in return for financially supporting Kyiv's war effort against Russia. On February 1, 2025, Russia launched an attack in which a missile hit an apartment building in [Poltava](#), killing 14 people and injuring 22. In India, bomb threats towards schools continue, this time in [Noida](#). In Mexico, gunfights on February 3, 2025, in [Nuevo Laredo](#) following the arrest of an alleged local cartel leader forced the suspension of flights at the local airport. This comes as Mexico has deployed the first of 10,000 National Guard troops to the U.S. border after Trump's tariff [threat](#), with the promise of stopping illegal migration and fentanyl trafficking.

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 Pennsylvania and California, which together made up 20 percent of this week's nationwide total. Gun

violence across the United States overall decreased by 1 percent from the week prior. Police activity alerts increased by 10 percent, with the top contributing states being California and Texas. Structure fires decreased by 24 percent, with the top two states for this subtype being California and New York. National protest activity increased by 159 percent from the week prior.

- **What this means:** Protest activity increased drastically this week; on February 5, 2025, there was a nationwide anti-Trump [demonstration](#), with protesters denouncing his comments on a U.S. takeover of Gaza, his immigration crackdown, his anti-trans orders, and Elon Musk's unofficial role in the White House. Protesters gathered in front of state capitols across all 50 states; a demonstrator at one such protest held an [AK-47](#) outside of the capitol building in Madison, Wisconsin. Pennsylvania was one of the top contributors to the gun violence numbers this week, with one instance being a mass shooting in [Allentown](#); one person was killed, and three people were injured after a fight between two groups. Structure fire alerts decreased significantly this week, as weather across the country is getting warmer, and hazardous heating equipment is not being used as regularly. Additionally, both the Palisades and the Eaton [wildfires](#) in California have been 100 percent contained after being active for approximately one month.

| 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%