



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

February 17, 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 14, 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 Flash Report Resumption of Israel-Hamas War	2
ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 3	2
 Cyber and Dark Web Intelligence Key Findings	4
8Base Leak Site Seized	4
United States and Others Sanction Key Infrastructure Enabling Ransomware Attacks	4
FTC Orders "World's First Robot Lawyer" to Stop Deceiving Users via Its AI Chatbot	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2025-23359	8
CVE-2025-24865	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Incidents Across Sectors	11
Data Breaches Target Large Swaths of Victims	12
 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

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Flash Report Resumption of Israel-Hamas War](#)

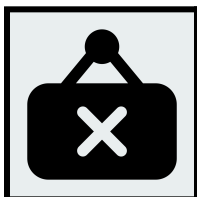
President Donald Trump's February 2025 statements that the United States will take possession of the Gaza Strip very likely signals that the Trump administration is not interested in pursuing the third phase of the Israel-Hamas ceasefire. A resumption in fighting very likely increases the risk of regional instability, with Houthi rebels very likely to resume attacks in the Red Sea if the ceasefire collapses. ZeroFox has observed an uptick in activity from pro-Palestinian cyber threat actors, who will likely increase their targeting of U.S. and Israeli entities in the event the ceasefire collapses.

[ZeroFox Intelligence Brief – Underground Economist: Volume 5, Issue 3](#)

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



8Base Leak Site Seized

What happened: An international law enforcement (LE) operation has successfully dismantled the 8Base ransomware group, which had been operating on the dark web since 2022. The operation, spanning the United States, Europe, and Asia, led to the seizure of the [group's dark web leak site](#) and the arrest of four European suspects. These individuals are accused of stealing USD 16 million from over 1,000 victims worldwide. Authorities in Bavaria seized the group's dark web portal, while Thai police conducted coordinated raids in Phuket, resulting in the capture of the European suspects.

- **What this means:** The 8Base ransomware group initially has kept a low profile before emerging as a major double extortion player in June 2023. Believed to be composed of experienced hackers, possibly from different ransomware groups, 8Base reportedly targets small and medium-sized businesses with weak cybersecurity defenses. It uses phishing, exploit kits, and drive-by downloads for access. The group has also been linked to Phobos ransomware, with researchers discovering Phobos samples using a ".8base" file extension on encrypted files. LE recovered over 40 pieces of critical evidence, including phones, cryptocurrency wallets, and laptops, which are likely to aid in further investigations. The seizure of the group's infrastructure and the arrest of its members disrupt a major ransomware operation, potentially preventing further financial losses for victims. The evidence gathered, including digital devices, could likely lead to additional arrests and help authorities trace the full extent of the group's illicit activities. Although the site has been seized, it is likely that the unapprehended members of 8Base will reemerge under a different name or affiliate with existing threat groups to continue their operations.

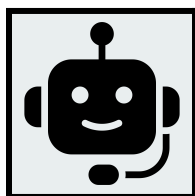


United States and Others Sanction Key Infrastructure Enabling Ransomware Attacks

What happened: Law enforcement bodies from the United States, Australia, and the United Kingdom are jointly sanctioning Zservers, a Russia-based bulletproof hosting (BPH) services

provider, for supporting LockBit ransomware attacks. The sanctions also designate two key administrators of Zservers for having materially assisted, sponsored, and supported LockBit ransomware in other ways to enable ransomware attacks and other criminal activities.

- **What this means:** Ransomware actors and other cybercriminals often rely on third-party network service providers like Zservers to enable their attacks on U.S. and international critical infrastructure. Zservers has materially assisted threat actors to evade detection, while also providing services including leasing numerous IP addresses to LockBit affiliates to conduct ransomware attacks. Disrupting Zservers is likely to hinder ransomware operations by cutting off a key infrastructure provider. However, cybercriminals could seek alternative BPH services to maintain their activities. The actions of the designated individuals are likely to have resulted in, or contributed to, the threat to national security, foreign policy, economic health or financial stability of the United States. This has very likely caused a misappropriation of funds, stolen intellectual property, proprietary information, personal identifiers, and financial information for financial gain.



FTC Orders “World’s First Robot Lawyer” to Stop Deceiving Users via Its AI Chatbot

What happened: The Federal Trade Commission has finalized an order requiring DoNotPay, a company that promoted its online subscription service as “the world’s first robot lawyer,” to stop making deceptive claims about the abilities of its AI chatbot. In a complaint announced in September 2024, the FTC charged that DoNotPay’s so-called robot lawyer failed to live up to claims that it was an adequate substitute for the expertise of a human lawyer. The final order requires DoNotPay to pay USD 193,000 in monetary relief. The order also prohibits DoNotPay from advertising that its service performs like a real lawyer unless it has sufficient evidence to back it up.

- **What this means:** DoNotPay did not test whether its “AI lawyer” operated to the level of a human lawyer when generating legal documents and giving advice, and the company did not hire or retain attorneys to test the quality and accuracy of the law-related features. Therefore, its deceptive claims about the chatbot giving reliable legal advice could have misled users to forgo qualified legal counsel, likely resulting in poor legal outcomes or harm in legal proceedings. Moreover, users relying on these unsubstantiated and unverified information could face financial and legal repercussions. Unchecked AI practices and regulations, especially when used in systems like law services that directly impact users, could have real-time practical repercussions. AI is increasingly used in

various sectors, sometimes with harmful consequences—such as biased hiring algorithms, misinformation spread by chatbots, and AI-generated financial scams.

| **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. CISA released [22 Industrial Control Systems \(ICS\) advisories](#) and added [six vulnerabilities](#) to its Known Exploited Vulnerabilities ([KEV](#)) catalog last week. CVE-2025-0994 is a deserialization [vulnerability in Trimble Cityworks](#). CVE-2024-53704 is a [vulnerability in certain versions of the SonicOS SSLVPN application](#) that enables authentication bypass. CVE-2025-25064 is a [bug in Zimbra's Collaboration software](#) that could enable threat actors to access information under certain conditions. CVE-2025-23359 is a [Time-of-Check Time-of-Use \(TOCTOU\) vulnerability in the NVIDIA Container Toolkit for Linux](#), which, when used with the default configuration, allows a crafted container image to gain access to the host file system. [Apple has released an emergency patch](#) for a vulnerability, CVE-2025-24200, that threat actors are exploiting in a targeted and "extremely sophisticated attack." CVE-2024-57968 is [an unrestricted upload of files with a dangerous type vulnerability](#) that allows remote authenticated users to upload files to unintended folders. This month's [Microsoft Patch Tuesday updates](#) comprise security fixes for 55 flaws, including four zero-day vulnerabilities, with two actively exploited in attacks. CVE-2024-55591 is an [authentication bypass vulnerability](#) affecting FortiOS and FortiProxy. Ivanti has released [security updates](#) for Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), and Ivanti Secure Access Client (ISAC) to fix multiple vulnerabilities, including three critical flaws.

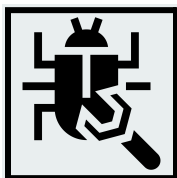


HIGH

CVE-2025-23359

What happened: NVIDIA Container Toolkit for Linux contains a time-of-check time-of-use (TOCTOU) vulnerability when used with default configuration, where a crafted container image could gain access to the host file system. This vulnerability is fixed in versions 1.17.4 and 24.9.2.

- **What this means:** A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.
- **Affected products:**
 - NVIDIA Container Toolkit for Linux: All versions up to and including 1.17.3
 - NVIDIA GPU Operator for Linux: All versions up to and including 24.9.1

**CRITICAL****CVE-2025-24865**

What happened: CVE-2025-24865 can enable unauthorized threat actors to access the administrative web interface without authentication, which could let the attackers retrieve sensitive information and upload files without the associated password. This bug has received the highest CVSS score of 10.0/10.0.

- **What this means:** CISA has released an ICS advisory addressing this vulnerability along with three others affecting the same product. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary OS commands, upload files, and obtain sensitive information without providing associated credentials.

Affected products:

- myPRO Manager: Versions prior to 1.4

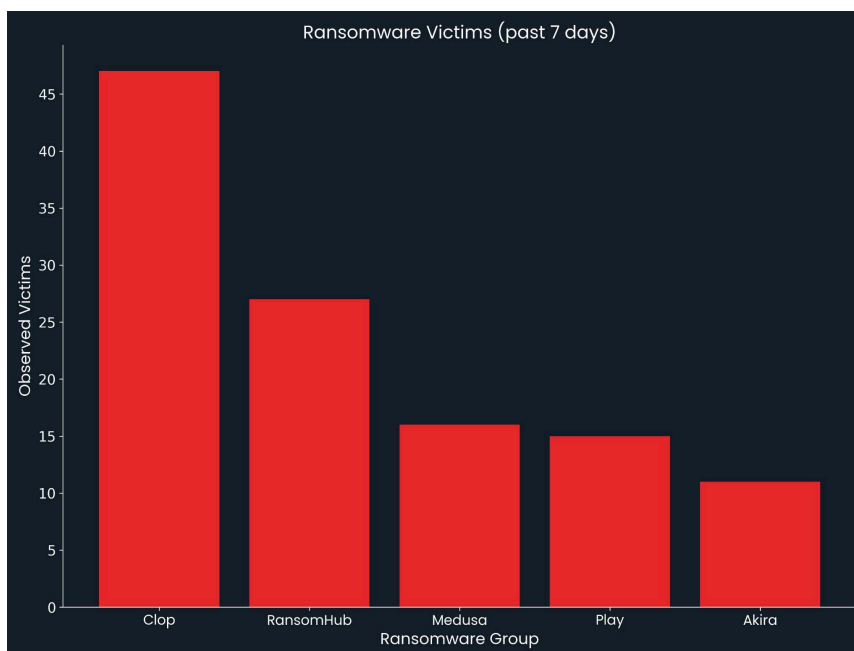
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Incidents Across Sectors

What happened: In the past week, ZeroFox observed close to 180 ransomware attacks, most of which were detected in North America. The most affected sector was manufacturing (followed by retail), while the most active group was the Cl0p ransomware group. Cl0p has yet again made headlines by [revealing all the names from the third victims list](#), which comprises around 50 entities. On

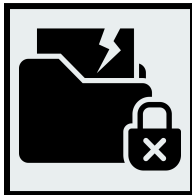


Source: ZeroFox Internal Collections

February 10, ZeroFox observed a new leak site, called "[Kraken leak blog \(hellokitty\)](#)," that listed five victims at the time of reporting and is [associated with the HelloKitty ransomware group](#). A China-based cybercriminal group, known as Emperor Dragonfly, has been spotted using [espionage-linked tools in a ransomware attack](#). Ransomware group "Sarcoma" has [taken credit for hacking Unimicron](#), a Taiwan-based company that designs, manufactures, and sells printed circuit boards (PCB).

- **What this means:** Cl0p continues to wreak havoc with its list of victims, all of whom are likely victims of the same Cleo vulnerability exploit attack. The threat group is likely leveraging the attention and anxiety around the attack to demonstrate its capabilities and the scale of the attack by releasing the names of its victims not in one go, but in batches. The association between Kraken leak blog and HelloKitty indicates that HelloKitty is likely looking to rebrand itself owing to a myriad of reasons, including change of its ransomware infrastructure and to avoid law enforcement detection and hindering. Ransomware groups

are constantly upgrading their cyber armada to conduct more impactful attacks while staying under the radar. Emperor Dragonfly's tactic of using espionage-linked tools in ransomware attacks is further evidence of this trend. The threat actor very likely aims to maintain undetected persistent access to a compromised system to leverage it for double and even triple extortion. Sarcoma's targeting of Unimicron is likely because of the company's capital strength, being one of the biggest PCB manufacturers in the world. The firm has confirmed that the attack has had [limited impact on its data](#).



Data Breaches Target Large Swaths of Victims

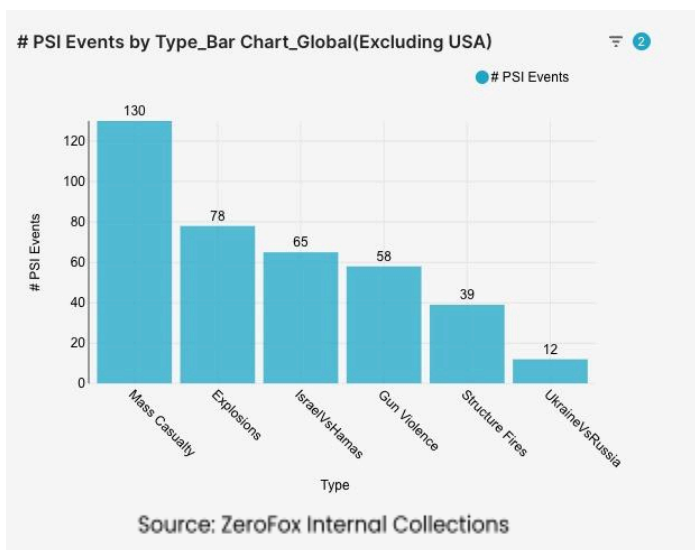
What happened: A [1.17 TB data leak](#) from Chinese IoT grow light company Mars Hydro exposed billions of records, including Wi-Fi passwords, IP addresses, and device IDs. When the compromise was observed, the company secured the database within hours. The exposed data included logging and error records of IoT devices, as well as API details linked to Mars Hydro and related companies. Hospital Sisters Health System (HSHS) has [notified over 882,000 patients](#) that a data breach in August 2023 exposed their personal and health information. Zacks Investment Research suffered a data breach [exposing sensitive information from 12 million accounts](#). A threat actor claimed access to the company's active directory as a domain admin, stealing source code for zacks[.]com and 16 other websites. The leaked database contained email addresses, names, hashed passwords, phone numbers, and physical addresses.

- **What this means:** The Mars Hydro data breach exposed data involving critical IoT infrastructure likely leading to unauthorized access, botnet deployment, and network infiltration. The swift database lockdown may have limited immediate damage, but the scale of exposed credentials and API details increases long-term security risks for affected users and systems. The healthcare sector is increasingly targeted by threat groups because it holds valuable, sensitive data that is often easier to monetize than other sectors. The HSHS breach compromised sensitive patient information, including names, addresses, medical records, Social Security numbers, and health insurance details. This exposure could lead to identity theft, financial fraud, insurance fraud, phishing attacks, targeted scams, and more. The breach at Zacks compromises user privacy and increases risks of identity theft, phishing, and credential stuffing attacks. The exposure of source code and admin-level access poses significant risks, including potential backdoor implantation, website manipulation, and replication of proprietary algorithms.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

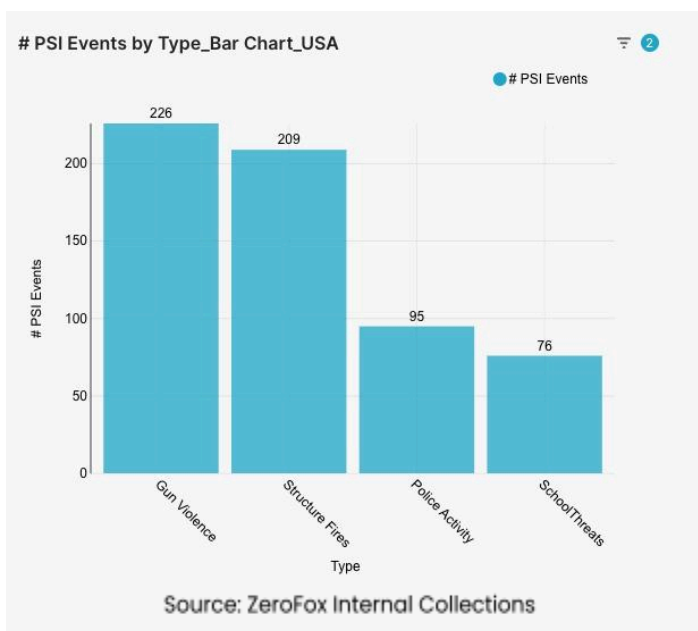


What happened: Excluding the United States, there was a 7 percent increase in mass casualty events this week from the previous week, with the top contributing countries being India and Palestine. Approximately 60 percent of these events were explosions, and the two aforementioned countries accounted for about 34 percent of all mass casualty alerts. General alerts related to the Israel-Hamas War (including protests, raids, and involvement in neighboring countries) increased by 25 percent from the

previous week. Events related to Russia's war in Ukraine increased by 20 percent. The top three most-alerted subtypes were explosions, which saw a 5 percent increase from the previous week; gun violence, which decreased by 18 percent; and structure fires, which increased by 34 percent. Global protest activity increased by 18 percent.

- **What this means:** Alerts related to the Israel-Hamas conflict, explosions, and mass casualty events in general all saw increases this week, with Palestine being one of the top contributing countries to mass casualty incidents; this is likely due to current [ceasefire](#) becoming more and more fragile as US President Donald Trump threatened to end the deal altogether if Hamas does not release all its hostages by Saturday. Additionally, Yemen's Houthis have [announced](#) they are ready to attack Israel if it reneges on its ceasefire deal with Hamas and resumes its assault on Gaza. Meanwhile, in Ukraine, while Ukrainian President Zelenskyy and President Trump are discussing a deal in which Ukrainian [rare earths](#) would be exchanged for further assistance from the US, the attacks from Russia have continued, including a bomb dropped on [Kramatorsk](#) on the 13th which killed one person and injured five. In India, the wave of [hoax bomb threats](#) has continued, as this week there were threats against various airports, railway stations, hotels, and other public places. Most of the threats were sent via Facebook messenger or email to police stations, and have all turned out to be false.

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

across the United States overall decreased by 14 percent from the week prior. Police activity alerts also decreased by 14 percent, and the top contributing states were Georgia and California. Structure fires increased by 5 percent, and the top two states for this subtype were California and New York. Notably, school-related threats decreased by 30 percent.

- What this means:** Gun violence, police activity, and school-related threats all saw decreases this week, which may correlate with recent weather patterns; a [winter storm](#) recently unleashed severe weather across parts of the South, Midwest and mid-Atlantic regions, leading to school closures and general disruption of criminal activity. These numbers are expected to remain low going forward, as next week, almost every U.S. state is forecast to experience [windchills](#) of 20 degrees or below. As for structure fires, since heating equipment usage inevitably causes fire hazards, we have seen this number increase, and expect it to continue to do so in the upcoming week. California had the highest number of gun violence instances, with one such event being a [mass shooting](#) which killed one person and injured six on February 9th in Los Angeles. In political updates, [protests](#) against President Donald Trump's immigration crackdown measures, Project 2025, Elon Musk, and the displacement of Palestinians from Gaza have continued to sweep the country, with several taking place at US state capitols on Wednesday. With the [ceasefire](#) deal between Israel and Hamas possibly coming to an end this weekend, more such demonstrations could arise.

| 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%