



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 27, 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 January 24, 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 – CIOp Publishes Data of Cleo Compromise Victims	2
ZeroFox Intelligence Flash Report – Threat Actors Seeking to Exploit California Wildfire Recovery Funds	2
 Cyber and Dark Web Intelligence Key Findings	4
President Trump Issues Executive Order to Delay TikTok Ban	4
Philippine Authorities Arrest Three on Espionage Charges	4
Telegram CAPTCHATricks Users into Running Malicious PowerShell Scripts	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-47100	7
CVE-2024-11166	8
 Ransomware and Breach Intelligence Key Findings	10
CIOp Continues to Threaten Victims	10
Recent Data Breaches Expose Millions Across Key Sectors	11
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	15
 Appendix A: Traffic Light Protocol for Information Dissemination	16
 Appendix B: ZeroFox Intelligence Probability Scale	17

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – CI0p Publishes Data of Cleo Compromise Victims

Between January 17 and 18, 2025, the ransomware group CI0p published data allegedly belonging to three organizations that were targeted during the Q4 2024 compromise of Cleo's secure managed file transfer (MFT) solutions. Previously, in December 2024, CI0p added the obfuscated names of 66 alleged victim organizations to its leak site. The names of these organizations were unveiled on January 14 and 15, 2025, along with a blog post threatening to publish their data on January 18, 2025. There is a very likely chance that CI0p will publish data stolen from other named organizations in the coming weeks, beginning with those the group perceives to be impeding negotiations or unlikely to meet its demands. Also between January 17 and 18, 2025, CI0p posted a seemingly unrelated statement to its victim leaksite, alluding to the collective's "downloading" of data belonging to organizations that use the MOVEit MFT solution via a vulnerability. The meaning and intent behind CI0p's message to MOVEit customers is unclear.

ZeroFox Intelligence Flash Report – Threat Actors Seeking to Exploit California Wildfire Recovery Funds

ZeroFox has identified threat actors actively discussing methodologies to exploit California wildfire recovery funds for financial gain on the dark web. In a thread identified on the Dread forum, threat actors discussed methodologies for successful scams, stating that this is "free money", as well as the importance of exercising patience to avoid early scrutiny during the verification process. Based on previous behavior and attitudes towards disaster relief funds, it is very likely that a broader array of threat actors are interested in exploiting these funds than those identified to date. Although ZeroFox has identified no evidence that threat actors are actively—and successfully—leveraging wildfire recovery funds in financial scams, such activity could result in financial and reputational damage for state or local government authorities and reduce the availability of relief funds for those legitimately affected by the wildfires, as well as perpetuate the idea that these funds are a viable attack vector.

| **Cyber and Dark Web Intelligence** |

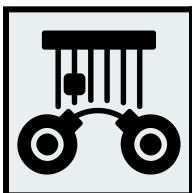
| Cyber and Dark Web Intelligence Key Findings



President Trump Issues Executive Order to Delay TikTok Ban

What happened: U.S. President Donald Trump has ordered a pause on the Protecting Americans from Foreign Adversary Controlled Applications Act (the “Act”) for 75 days to determine the appropriate course of action concerning TikTok. On January 19, TikTok [issued a statement on the X platform](#) that it was restoring its services after going “dark” for a brief period for its American customer base, comprising 170 million users. A previous [statement posted to TikTok’s website](#) on January 18 had asked for a “definitive statement to satisfy the most critical service providers, assuring non-enforcement” from the Biden administration.

- **What this means:** The Protecting Americans from Foreign Adversary Controlled Applications Act regulates “foreign adversary controlled applications,” specifically those operated by TikTok and any other subsidiary of its China-based parent company, ByteDance Ltd., on national security grounds. A temporary pause on the enforcement of the Act will enable the Trump administration to review and pursue a resolution that protects national security while saving a platform used by 170 million Americans, including those for whom the platform is the primary source of income. No action will be taken to enforce the Act or impose any penalties against any entity for any conduct during the 75 days while the Trump administration reviews the different possibilities of retaining TikTok in the United States. In the meantime, TikTok has been facing other different issues, including [a lawsuit filed by the Austrian non-profit None of Your Business \(noyb\)](#), which is suing several China-based companies for violating the European Union’s data protection regulations.

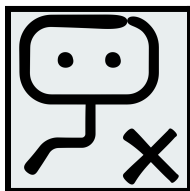


Philippine Authorities Arrest Three on Espionage Charges

What happened: Philippines authorities have arrested a Chinese national and two Filipino accomplices on suspicion of espionage. The Chinese individual, believed to be affiliated with the Army Engineering University of the People’s Liberation Army (PLA) in Nanjing, was found with equipment thought to be intended for spying on military facilities. The group had been under

surveillance by the Philippine National Bureau of Investigation (NBI) based on intelligence reports that indicated they had arrived in the country to monitor critical infrastructure—including military installations where U.S. forces have access under a mutual defense agreement.

- **What this means:** The seizure of espionage-related equipment from the accused with connections to the Chinese military indicates that China may be conducting covert operations to monitor and potentially disrupt Philippines military infrastructure. This operation seems aimed at identifying weaknesses in Philippines defense systems, which could then facilitate cyberattacks, compromise U.S. military access points, and strengthen China's influence in the South China Sea. The gathered intelligence is likely to strengthen China's strategic position in the region, while further complicating international shipping routes in the Asia-Pacific region. Given the overlapping territorial claims of the Philippines and China in the South China Sea, these actions are likely part of a Chinese effort to assert control over contested areas, especially as the U.S. military's presence continues to expand in accordance with mutual defense agreements.



Telegram CAPTCHA Tricks Users into Running Malicious PowerShell Scripts

What happened: Threat actors are exploiting the name of Ross Ulbricht (founder of the illicit online market place Silk Road) and recent news of his pardon to spread malware via fake verified accounts on X (formerly Twitter). Victims are lured to malicious Telegram channels, where they are tricked into running a PowerShell command disguised as a "verification process." This command downloads malware, likely a Cobalt Strike loader. The campaign mimics recent tactics where CAPTCHAs or fake verifications are used to deliver malware through PowerShell commands.

- **What this means:** Platforms like Telegram have become a hotbed for cybercriminals, offering a relatively unregulated space to distribute malware, coordinate attacks, and target users. The use of the "ClickFix" tactic has gained popularity among threat actors over the past year due to its effectiveness in distributing malware. In this scam, threat actors use fake-but-verified accounts on X to redirect users to malicious Telegram channels posing as official Ulbricht platforms. These channels employ a social engineering technique disguised as CAPTCHA verification, tricking users into running PowerShell commands. This stealthy tactic bypasses standard security measures and installs tools like Cobalt Strike, enabling attackers to escalate their operations. Likely consequences include network infiltration, credential theft, and ransomware attacks, showcasing how attackers exploit high-profile events to enhance their malicious campaigns.

| **Exploit and Vulnerability Intelligence** |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, and government services. Researchers have discovered over a dozen [vulnerabilities in a Mercedes-Benz infotainment system](#). The carmaker has assured customers that the bugs are not easily exploitable and the security gaps have been patched. [CVE-2025-23086](#) pertains to a feature in Brave Browser versions 1.70.x-1.73.x that, in combination with an open redirect vulnerability on a trusted site, could enable actors to make a malicious site look as though it originated from the trusted domain in the file selector dialog. Tracked as [CVE-2025-23184](#), a potential denial-of-service (DoS) vulnerability is present in versions of Apache CXF that could enable actors to overwhelm services. The Debian Long-Term Support (LTS) team has [addressed several bugs](#) in the 389-ds-base LDAP server, including CVE-2021-3652. [CVE-2021-3652](#) could authenticate attackers as users whose passwords have been disabled, bypassing account security entirely. [CVE-2024-13454](#) in Easy-RSA versions 3.0.5 through 3.1.7 could enable brute force attacks. Threat actors could exploit a buffer overflow vulnerability, [CVE-2024-54887](#), in TP-Link TL-WR940N routers to execute arbitrary code remotely. [CVE-2025-24014](#) in Vim before version 9.1.1043 could lead to an out-of-bounds write scenario. 7-Zip file archiver has a [high severity vulnerability](#) that threat actors could exploit to bypass Mark of the Web security features in popular operating systems and execute codes on targeted computers. CISA released three [Industrial Control Systems \(ICS\) advisories](#) last week. [CVE-2024-32555](#) is an incorrect privilege assignment vulnerability in Easy Real Estate that allows for privilege escalation via the social login.



HIGH

CVE-2024-47100

What happened: The web interface of devices with this bug is vulnerable to cross-site request forgery (CSRF) attacks. This vulnerability is one of three listed recently by CISA as part of its ICS advisories.

- **What this means:** This vulnerability likely allows an unauthenticated attacker to change the CPU mode by tricking a legitimate and authenticated user with sufficient permissions on the target CPU to click on a malicious link.
- **Affected products:**
 - The affected products and platforms are listed in this [CISA](#) advisory.

**HIGH****CVE-2024-11166**

What happened: CISA has released an ICS advisory addressing CVE-2024-11166 and two more vulnerabilities in Traffic Alert and Collision Avoidance System (TCAS) II. Older TCAS II systems, which rely on transponders that do not meet the latest standards (RTCA DO-181F), are vulnerable to being exploited in cyberattacks.

- **What this means:** This bug can enable an attacker to impersonate a ground station and issue a Comm-A Identity Request. This action can set the Sensitivity Level Control (SLC) to the lowest setting and disable the Resolution Advisory (RA), leading to a DoS condition.
- **Affected products:**
 - TCAS II: Versions 7.1 and prior

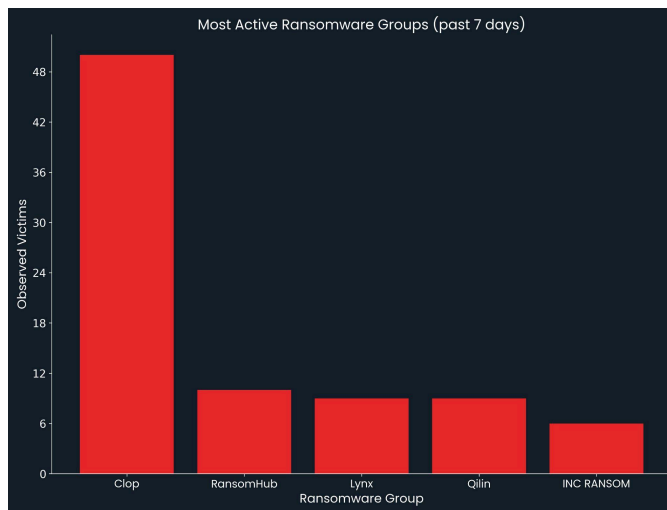
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



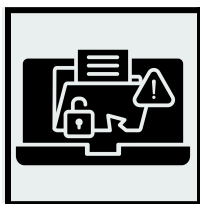
Cl0p Continues to Threaten Victims

What happened: In the past week, ZeroFox observed close to 100 ransomware attacks, most of which were detected in the North America region. The most affected sector was manufacturing (followed by professional services), while the most active group was the Russia-based criminal ransomware collective Cl0p. On January 22, 2025, ZeroFox observed that Cl0p [announced the disclosure](#) of 50 additional unrevealed victims. Between January 17 and 18, 2025, [Cl0p published data](#) allegedly belonging to three organizations that were targeted during the Q4 2024 compromise of secure MFT solutions.



Source: ZeroFox Internal Collections

- **What this means:** Also between January 17 and 18, 2025, Cl0p posted a seemingly unrelated statement to its victim leaksite alluding to the collective's "downloading" of data belonging to organizations that use the MFT solution via a vulnerability. To safeguard against potential threats, ZeroFox recommends that organizations consult official manufacturer guidance (such as the type provided on Cleo and Progress' support pages) and prioritize implementing the latest security patches. Establishing a comprehensive patch management process ensures IT assets are updated promptly. Adopting a Zero-Trust cybersecurity model with the principle of least privilege, network segmentation, and phishing-resistant multi-factor authentication (MFA) further strengthens defenses. Secure password policies and unique credentials should be enforced, and critical data must be backed up regularly to secure, off-site, or cloud-based servers.



Recent Data Breaches Expose Millions Across Key Sectors

What happened: Wolf Haldenstein Adler Freeman & Herz LLP, a [prominent New York City law firm](#), [experienced a significant data breach](#) that compromised the personal and protected health information of over 3.4 million individuals. The breach was first suspected on December 13, 2023, when the firm detected suspicious activity on its network. This led to immediate actions to contain the incident, including engaging a third-party digital forensics firm to investigate the breach's scope and nature. Though the firm worked to prevent further unauthorized access, the breach still impacted a vast number of individuals. Notifications have been sent to those for whom the firm had valid address information, but a subset of affected individuals could not be directly contacted because their address details were unavailable. Otelier, a [hotel management platform](#), [experienced a significant data breach](#) that compromised sensitive personal information and reservation details for millions of guests. The breach, which reportedly began in July 2024 and lasted until October 2024, involved threat actors gaining unauthorized access to Otelier's cloud storage systems. The attackers claimed to have stolen almost eight terabytes of data, including details from major hotel brands. This breach affected not only hotel chains but also their customers, whose personal and reservation data was potentially exposed to malicious actors. On January 17, 2025, threat actor "empathy" claimed on dark web forum BreachForums to have [leaked a database associated with Emirates Cancer Society](#), a UAE-based organization that provides support and assistance to cancer patients and their families. The leaked data comprises sensitive information, including email addresses, password hashes, names, and phone numbers and is formatted as a [.]txt file.

- **What this means:** The recent breach at Wolf Haldenstein Adler Freeman & Herz LLP exposed the sensitive personal and health information of over 3.4 million individuals, putting them at significant risk for identity theft, fraud, and other security threats. This breach is particularly concerning given the firm's involvement in complex litigation, including data breach cases; despite typically helping clients navigate and address such vulnerabilities, Wolf Haldenstein Adler Freeman & Herz LLP appears to have become a victim of the very risks it seeks to mitigate. The Otelier breach resulted in the theft of sensitive personal information (including names, contact details, payment methods, and reservation histories), exposing millions of guests to significant risks such as identity theft, financial fraud, and privacy violations. With such a massive volume of data compromised, the attackers now possess a trove of valuable information, which can be exploited or sold

on the criminal underground market. For the affected hotels, the impact is substantial in terms of reservation systems and customer databases. With guest information potentially in the wrong hands, hotels may face disruptions in their booking operations—including increased cancellations, fraudulent reservations, and difficulty verifying guest identities; further, the hotels must now handle customer inquiries and potential reimbursements due to the breach. As a charity supporting cancer patients, the Emirates Cancer Society deals with vulnerable individuals who may have shared their personal details in confidence, seeking assistance or treatment. The exposure of email addresses and phone numbers can lead to targeted phishing attacks or even harassment. The leaked password hashes, if not properly secured or encrypted, could potentially be cracked, giving malicious actors access to other accounts or services that victims use.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 2 percent decrease in global mass casualty incidents this week, with Palestine, Mexico, Ukraine, and India contributing the highest number of alerts in the category (almost 49 percent were explosions). General alerts pertaining to the Israel-Hamas conflict (including protest, raids, and involvement in the neighboring countries) showed an 11 percent decrease compared to the prior week. Notably, Israel and Palestine accounted for 14 percent of all explosion alerts this week. Additionally, alerts pertaining to the ongoing Russia-Ukraine were increased by 44 percent this week.

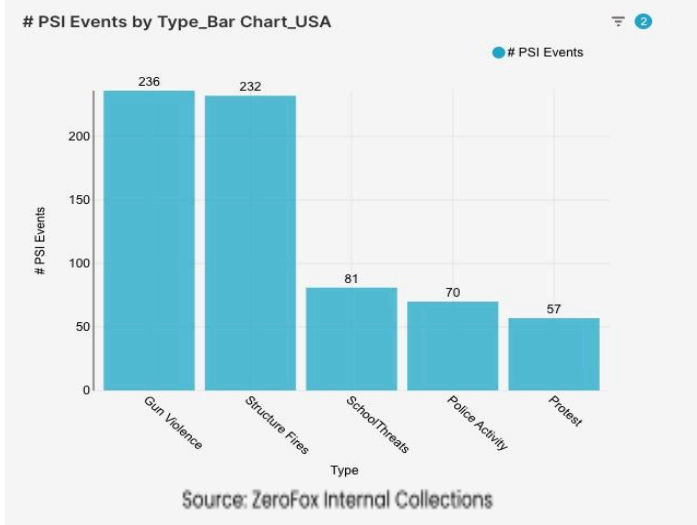
The three most-alerted subtypes were explosions, which showed a 1 percent increase; gun violence, which showed an 18 percent increase; and structure fires, which increased by 48 percent. Protest activity showed an increase of 18 percent this week compared to the last.



- **What this means:** With a ceasefire agreement currently in effect in the ongoing Israel-Hamas conflict, the incident alerts have dropped by 11 percent. The [ceasefire](#), which was mediated by the United States, Qatar, and Egypt, came into effect on January 19 with Hamas handing over the names of three female captives who would be released. This ceasefire is expected to last for 42 days; after the first 16 days, another round of negotiations will begin aimed at negotiating a permanent ceasefire. In this first phase of the ceasefire, Hamas is expected to hand over 33 hostages, while the Israeli army has agreed to fall back from the populated areas. Additionally, in the ongoing Russia-Ukraine war, this week saw increased artillery shelling compared to the last. [Drone attacks](#) targeting Tula, Kaluga, Smolensk, and Saratov in Russia were conducted by Ukraine. Counter-shelling by Russia in the [Bekhetry](#) region of Ukraine led to two deaths and 25 reported injuries. Structure fires increased this week by a large margin due to localized wildfires and apartment fires spread across South America and Canada.

Physical Security Intelligence: United States

What happened: In the past week, the most-alerted subtypes in the United States were gun violence, structure fires, and police activity. California (22 alerts) and Illinois (18 alerts) reported the highest amount of gun violence, contributing 17 percent of the total alerts in the category. Structure fires were a close second with 232 alerts, of which California (37 alerts) and New York (34 alerts) accounted for 31 percent of the total. Police activity was the third most-alerted subtype this week, with California (16 alerts) and Texas (eight alerts) comprising 34 percent of the total incidents.



- What this means:** In the United States this week, gun violence rose by 11 percent, becoming the most-alerted subtype. Over the weekend in Chicago, Illinois, one person was killed and 12 others were injured in [shooting-related incidents across the city](#). Alerts with the "SchoolThreats" tag saw a significant increase of 45 percent, with California being the largest contributor. The major SchoolThreats incident recorded this week occurred at Antioch High School, where a student fatally shot his fellow classmates and himself. Protest activities showed an uptick this week of 46 percent. Most of the protest activity was during the inauguration ceremony of President Donald Trump and was concentrated around Washington, DC. Contrasting climate conditions across the United States continued this week, with California having registered [a new wildfire named "Hughes"](#) that has burnt 9,400 acres of land, displaced almost 50,000 people, and threatened several structures in the area. Additionally, California State University was closed on Thursday due to the Laguna [wildfire spreading across Ventura County](#). However, in the southern United States, [snowstorm "Enzo"](#) has killed four people and disrupted public life. The snowstorm is expected to continue, with temperatures not beginning to rise until the end of the week. Both the intense wildfires and the extreme cold are reportedly consequences of climate change.

| 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%