



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

December 30, 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 27, 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 Flash Report – EU Energy Risks in Early 2025	2
 Cyber and Dark Web Intelligence Key Findings	4
After Exploiting Cleo's File Transfer Platforms, CIOp Ransomware Claims 66 Victims	4
Lazarus Group Targets Nuclear Industry with CookiePlus Malware	4
U.S. Law Enforcement Officials Release Final "Don't Click December" PSA	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-45387	7
CVE-2021-44207	8
 Ransomware and Breach Intelligence Key Findings	10
Ransomware Attacks Across Various Sectors	10
From Health Records to Payment Data: Notable Data Breaches in the Past Week	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

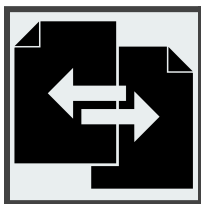
| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – EU Energy Risks in Early 2025

European energy prices have reached their highest level since the start of Russia's war in Ukraine in early 2022, just as Ukraine plans to halt the transit of Russian gas through the Druzhba pipeline on January 1, 2025. While price increases are steepest in eastern Europe, there will very likely be inflationary costs across the European Union (EU) without the replacement of Russian gas supplies. Energy insecurity and rising costs have been a key source of political unrest in Europe since the Russia-Ukraine war began. Additional gas price increases will likely continue to foment social tensions.

| Cyber and Dark Web Intelligence |

| Cyber and Dark Web Intelligence Key Findings



After Exploiting Cleo's File Transfer Platforms, CI0p Ransomware Claims 66 Victims

What happened: ZeroFox Intelligence has observed Russia-based criminal ransomware collective CI0p claiming responsibility for exploiting alleged zero-day vulnerabilities (CVE-2024-55956 and CVE-2024-50623) in Cleo file transfer tools to target 66 organizations in data theft attacks. In the leak site post, the group further warned that it would publicize the names of the companies if they failed to meet its demands within 48 hours from the initial posting. CI0p was also responsible for the May 2023 exploitation of CVE-2023-34362, a zero-day vulnerability in the MOVEit file transfer software that affected at least 2,600 organizations. Although CI0p operates primarily as a ransomware group, it also uses the ransomware-as-a-servicem (RaaS) model, selling access to its brand of malware.

- **What this means:** The initial victim list likely marks the beginning of a campaign to extort and leak data in the coming weeks and months. CI0p is also likely to expose some of the exfiltrated databases—regardless of how its ransom demands are met—which will likely interest other financially motivated adversarial threat actors. For example, on December 25, 2024, ZeroFox observed popular and well-regarded threat actor “Nam3L3ss” had [posted](#) more than 230 victims involved in the MOVEit breach on BreachForums. The Cleo attack will also likely inspire such activities on the deep and dark web. Meanwhile, CI0p will likely continue exploiting the two Cleo vulnerabilities, CVE-2024-55956 and CVE-2024-50623, in unpatched systems. These bugs impact some versions of Cleo Harmony, VLTrader, and LexiCom. All Cleo customers should upgrade the affected tools to the latest release versions and continue to follow the guidelines provided by their internal security teams and the software provider to avoid being targeted by CI0p.



Lazarus Group Targets Nuclear Industry with CookiePlus Malware

What happened: The North Korea-linked Lazarus Group has escalated its cyberattacks by targeting the nuclear industry, shifting away from previous focuses on defense, aerospace, and cryptocurrency. Over the course of a month, the group sent malicious files to at least two employees of a nuclear organization through fake job postings, a tactic known as the “DeathNote

campaign" or "Operation DreamJob." Victims were lured by fraudulent job offers and tricked into opening files disguised as job assessments. These files, often appearing as legitimate tools like VNC viewers or ZIP archives, contained malicious payloads that, when executed, granted the attackers unauthorized access to the victims' systems.

- > **What this means:** By using fake job postings as a delivery method for malicious files, the group is exploiting common tactics to deceive individuals and infiltrate sensitive networks. The attackers' ability to gain unauthorized access to systems through seemingly legitimate job assessments puts sensitive data and infrastructure at risk, with potential consequences that include stolen intellectual property, compromised operations, or large-scale disruptions. Additionally, the introduction of a novel malware tool called CookiePlus marked a significant evolution in the group's tactics. CookiePlus is a plugin-based malware strain that operates primarily in memory, making it more difficult for traditional security systems to detect and counter. This evasive technique allows the Lazarus Group to bypass conventional detection methods and maintain a persistent presence within targeted networks.



U.S. Law Enforcement Officials Release Final "Don't Click December" PSA

What happened: U.S. law enforcement authorities have released a fourth public service announcement ([PSA](#)) as part of their joint "Don't Click December" Consumer Protection Campaign. The PSA warns residents about the surge in online scams and fraud schemes during the holiday season. With additional support from the American Association of Retired Persons (AARP), the initiative aims to raise awareness and help consumers avoid falling victim to phishing emails, fake websites, and other common online scams.

- > **What this means:** The "Don't Click December" campaign warns the public about the growing threat of tech support scams, wherein criminals impersonate technology, banking, or government officials to trick victims into revealing personal information or granting remote access to their computers. The scam often begins with a fraudulent pop-up message claiming that an account has been hacked, prompting the victim to call a number that connects them to the scammer. Once in contact, the scammer manipulates the victim into providing access to their computer or financial accounts, ultimately stealing money or sensitive data. The campaign emphasizes that legitimate businesses and government agencies will never contact individuals unsolicited in this way, urging consumers to remain skeptical and avoid engaging with suspicious messages by simply following the advice "Don't Click It."

| **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, known exploited vulnerabilities (KEV), and government services. [CVE-2024-11349](#) is a vulnerability in the AdForest theme for WordPress present in all versions up to and including 5.1.6. This flaw allows attackers to bypass authentication, potentially granting unauthorized access to the site. [CVE-2024-1015](#) is a remote command execution (RCE) vulnerability in SE-elektronik GmbH E-DDC3.3 affecting versions 03.07.03 and higher, allowing attackers to send commands from the operating system to the device via its web configuration interface. [CVE-2021-44207](#) allows a threat actor with knowledge of the validationKey and decryptionKey for a web application to craft a malicious ViewState that bypasses the MAC check and is deserialized by the server. The Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its KEV catalog. [CVE-2024-43441](#) is a vulnerability in Apache HugeGraph-Server that allows attackers to bypass authentication due to improper handling of authentication mechanisms and assumed immutable data structures. [CVE-2024-45387](#) is an SQL injection vulnerability in Traffic Ops in Apache Traffic Control that allows a privileged user with the roles of "admin", "federation", "operations", "portal", or "steering" to execute arbitrary SQL commands against the database by sending a specially-crafted PUT request. [CVE-2024-52046](#) is a vulnerability that allows attackers to exploit the deserialization process by sending specially crafted malicious serialized data, potentially leading to RCE attacks. [CVE-2024-3393](#) is a vulnerability in PAN-OS that affects its next-gen firewalls; it allows unauthenticated attackers to exploit the DNS Security feature, triggering a denial-of-service (DoS) and causing affected firewalls to reboot or enter maintenance mode.



CRITICAL

CVE-2024-45387

What happened: The Apache Software Foundation (ASF) released a patch for a critical SQL injection vulnerability (CVE-2024-45387; CVSS score: 9.9/10.0) in Apache Traffic Control. It allows privileged users to execute arbitrary SQL commands in the database via crafted PUT requests.

- **What this means:** Threat actors are likely to exploit this bug to alter Content Delivery Network (CDN) configurations or steal sensitive operational data, leading to service disruptions, compromised website integrity, or targeted delivery of malicious content. It could also have far-reaching consequences impacting businesses relying on CDN services, including e-commerce, streaming platforms, and financial institutions.
- **Affected products:**

- Traffic Ops in Apache Traffic Control versions 8.0.1 and lower
- Traffic Ops in Apache Traffic Control versions 8.0.0 and higher

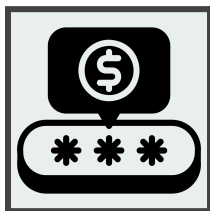
**HIGH****CVE-2021-44207**

What happened: A threat actor with knowledge of the validationKey and decryptionKey for a web application can construct a malicious ViewState that passes the MAC check and will be deserialized by the server. This deserialization can result in the remote execution of code on the server. CISA has [added](#) CVE-2021-44207 to its KEVs catalog.

- **What this means:** The bug was used as a zero-day by China-linked APT41 in 2021 as part of attacks targeting six U.S. state government networks. New evidence of the bug being exploited in the wild is a likely indication of similar state-sponsored attacks.
- **Affected products:**
 - Acclaim USAHERDS web application versions 7.4.0.1 and earlier

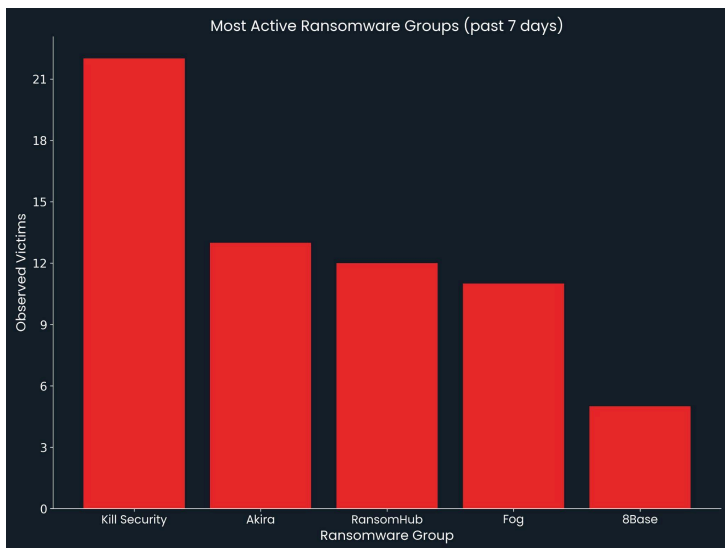
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



Ransomware Attacks Across Various Sectors

What happened: In the past week, ZeroFox observed close to 120 ransomware attacks, most of which targeted entities in North America. The most affected sectors were retail and manufacturing, while the most active group was the Kill Security ransomware group. A new criminal [complaint](#) has been filed in New Jersey charging a dual-national individual for their role as a developer in the LockBit ransomware group. The accused was arrested in Israel in August under a U.S. provisional arrest request and is awaiting extradition to the United States. The individual charged for their involvement in the NetWalker ransomware attacks will [serve](#) a 20-year imprisonment sentence. A May 2024 ransomware attack targeting U.S. healthcare giant Ascension has [impacted](#) nearly 5.6 million patients. Ascension [says](#) it will begin notifying individuals whose personal information was involved in this incident and providing them with complimentary credit monitoring and identity protection services. The Play ransomware group has [claimed](#) responsibility for the attack targeting donut chain Krispy Kreme in November. Pittsburgh Regional Transit (PRT) [suffered](#) a ransomware attack, which caused temporary disruptions in the city's transport network.



Source: ZeroFox Internal Collections

- > **What this means:** The charges against the accused LockBit developer come on the heels of an [announcement](#) about the release of a new version of LockBit ransomware, LockBit 4.0, set for February 3, 2025. Actions against key members of the group are likely to disrupt LockBit's near-future activities, while also giving law enforcement time to dismantle other disruptive networks in the group's infrastructure. The large number of individuals impacted by the Ascension attack are likely to face further cybercrime-related threats, including extortion, blackmail, doxxing, and other malicious attacks. Healthcare organizations are repeatedly targeted in ransomware attacks, as threat actors know that hospitals store

large amounts of sensitive and valuable patient data. Healthcare organizations are also known to pay ransomware demands to protect their patients and restore services immediately. Even though the cyberattack targeting Krispy Kreme did not affect in-store sales and deliveries, the company saw a share [drop](#) of about 2 percent in premarket trading. The costs the company will bear due to the incident [are](#) reasonably likely to have a [material impact](#) on the company's results of operations and financial condition. The cyberattack, conducted at the start of the busy holiday season, was likely a targeted attack aimed at harming the company's reputation, finances, and customer trust in the institution. Similarly, the attack on PRT also had significant, albeit temporary, tangible implications, [including](#) delays in the city's T rail cars and rendering several of the transit authority's systems offline.



From Health Records to Payment Data: Notable Data Breaches in the Past Week

What happened: In the past week, several notable data breaches have been reported, revealing ongoing vulnerabilities in various sectors. These incidents range from unauthorized access to sensitive personal and health information to cyberattacks targeting government and private organizations. One significant breach was discovered on December 20, 2024, that occurred in April, when a phishing attack targeted the [Illinois Department of Human Services](#) (IDHS). Multiple employee email accounts were compromised, exposing sensitive data—including public assistance records for over 1.1 million customers and the Social Security numbers of 4,701 individuals. In a separate incident, the [European Space Agency's](#) (ESA) official web shop was hacked, with a malicious JavaScript script injected into the checkout process. This script redirected customers to a fake Stripe payment page, where their payment card details were stolen. The data was exfiltrated to a domain mimicking the legitimate ESA shop but with a different top-level domain (.pics instead of .com). Meanwhile, a dark web criminal group was discovered running an operation designed to bypass [Know Your Customer](#) (KYC) verification processes commonly used in banking and financial institutions. In the United States, a major cybersecurity incident from March 2020 recently came to light involving the hack of a New Jersey-based company's [network](#). The attacker stole confidential data from approximately 300,000 customers and then extorted the company, demanding 300 BTC (around USD 3.2 million) in exchange for not releasing or selling the stolen information. The accused has now been charged. Lastly, the [Douglas County Department of Health and Human Services](#) in Wisconsin notified patients that their protected health information had been accessed without authorization by a former employee

over a period of 21 months.

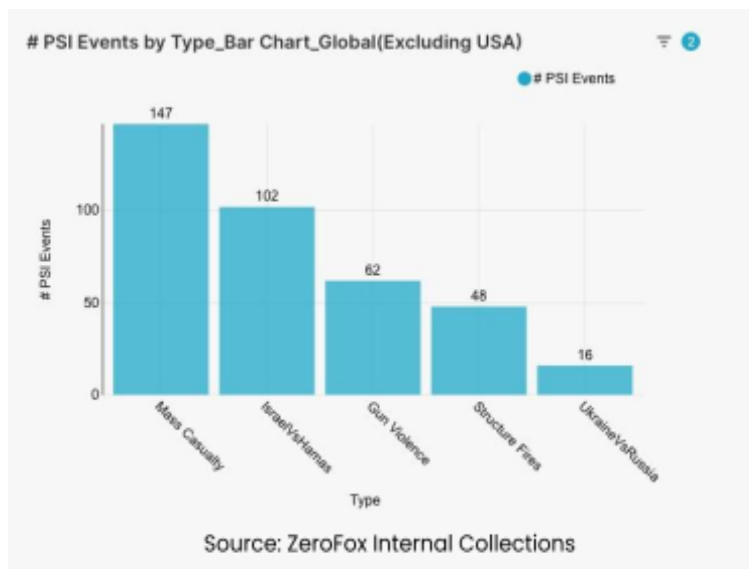
- **What this means:** These incidents collectively demonstrate the persistent and evolving nature of cyber threats. The breach at the IDHS exposed personal information for over 1.1 million customers, including Social Security numbers, which may potentially lead to identity theft, fraud, and long-term security concerns for the affected individuals. The cyberattack compromised ESA customers' payment information, putting them at risk of identity theft and financial loss. The use of a fraudulent domain likely misled shoppers, and ESA's lack of control over the third-party store exposes the risks of outsourcing sensitive data management. The criminal group used authentic identity documents paired with corresponding facial biometric data to bypass KYC verification processes, making it more difficult to identify the perpetrators through conventional security checks. If successful, this operation can likely facilitate widespread identity fraud, allowing criminals to impersonate individuals in financial and banking systems, leading to potential financial losses and regulatory concerns. The stolen data affected 300,000 customers from the New Jersey-based company. The hacker exploited vulnerabilities in the company's network, affecting a large number of customers and violating their privacy. If the accused had successfully released or sold the stolen data, it likely would have led to widespread identity theft, financial fraud, and significant harm to the affected customers. The unauthorized access of sensitive health data at Douglas County Department of Health and Human Services by a former employee highlights the risks posed by insider threats, even from trusted personnel. Over 21 months, the breach compromised protected health information, putting patients at risk of identity theft, privacy violations, and potential misuse of sensitive health data for malicious purposes.

| Physical and Geopolitical Intelligence |

| Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 4 percent increase in mass casualty incidents this week across the globe, with Palestine, Russia, and Mexico contributing the highest alerts in the category; almost 56 percent of the alerts were explosions. General alerts pertaining to the Israel-Hamas conflict (including protest, raids, and involvements in the neighboring countries), showed a 10 percent decrease. Notably, Israel and Palestine accounted for 41 percent of all explosion alerts. Additionally, alerts



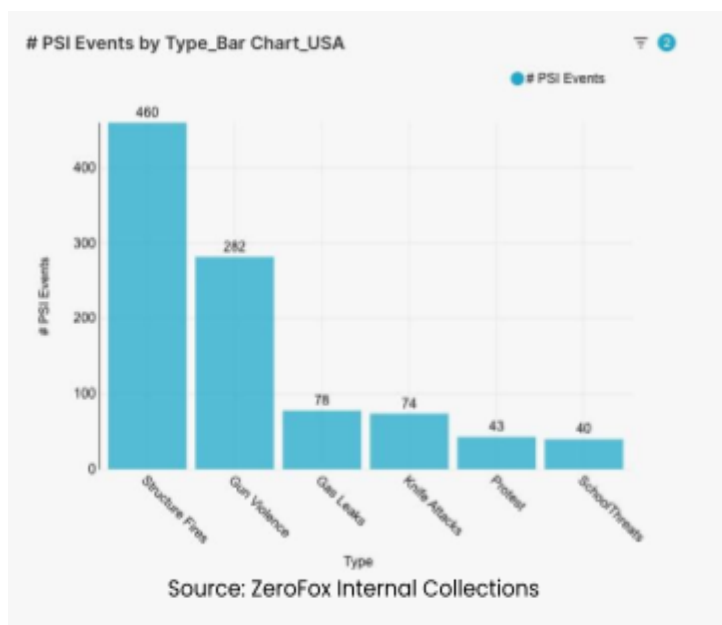
pertaining to the ongoing Russia-Ukraine war increased by 14 percent. The three most alerted subtypes were explosions, gun violence, and structure fires. This week, all subtypes showed a decrease in alerts compared to the last. Explosions decreased by 17 percent, gun violence decreased by 3 percent, and structure fires decreased by 2 percent. Both school threats and bomb threats decreased by 32 percent compared to last week.

- **What this means:** The Israel-Hamas conflict continued this week and accounted for multiple mass casualty incidents. Attacks on Nuseirat increased, with more than 15 casualties over the week. Armed shelling of the [Kamal Adwan Hospital](#) in the Beit Lahiya city in Palestine also increased, with the military justifying the attack on the hospital by calling it a designated regrouping spot for Hamas members. Shelling on Thursday near the hospital resulted in [five casualties](#). Attacks increased this week, with cities like Deir al Balah, Jabalia, Nuseirat, and Beit Lahiya reporting heightened cases of violence compared to the last. Additionally, cross-border shellings continued in the ongoing Russia-Ukraine war. This week, the town of [Rylsk](#) was hit, killing six people and injuring 10 others. This strike was considered retaliation for an attack on Ukraine's capital that resulted in one casualty. In another attack on Christmas Eve, a building in [Kryvyi Rih](#) was targeted in a shelling incident. Fourteen people were injured, and one person was killed. Structure fires continued to increase; cold winter brings with it heaters and flammable decor, leading to fires in residential dwellings. Alerts relating to this subtype will likely go up in the upcoming weeks. On December 20, 2024, a Christmas market in [Magdeburg](#), Germany, became a site of

mass casualty after an individual drove into the crowd, resulting in five deaths and over 200 injuries.

Physical Security Intelligence: United States

What happened: This week, the most alerted subtypes were structure fires, gun violence, and gas leaks. California and New York recorded the highest number of alerts in the structure fires category, with 62 and 66, respectively. The top contributors made up 28 percent of the total structure fires alert. Gun violence this week decreased by one alert. Illinois and Texas were the top contributors to this category, with both states making up 23 percent of the total alerts. Gas leaks were the third most-alerted category, increasing by 3 percent compared to the last week with Maryland and New Hampshire being the top two contributors. This week saw a 13 percent increase in protest-related activities and a 17 percent increase in knife attacks across the United States. However, school threats decreased by 56 percent compared to last week.



- > **What this means:** Similar to the previous week, structure fire remained the highest alerted subtype due to the increased use of heaters and other festive decor. In the upcoming days as cold nights increase, this subtype is likely to increase as well. Gun violence stayed the same as last week, with no major incidents reported over the past week. However, [localized shootings](#) across the country continued. On December 25, 2024, three people were shot and another was found stabbed at the [Phoenix Sky](#) Harbour International Airport. Domestic alerts saw a decline compared to the previous week. [Protest activities](#) calling for ceasefires in various active war zones were seen this week, leading to an increase in alerts; knife attack alerts also increased. School threats decreased by 56 percent this week, as many U.S. schools are closed for the holidays.

| 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%