



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 6, 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 3, 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 January 2025 Geopolitical Brief	2
 Cyber and Dark Web Intelligence Key Findings	4
U.S. Imposes Sanctions on Entities in Iran and Russia over Election Interference	4
Suspect Accused of Hacking Trump's AT&T Call Records Arrested	5
Final Rule Issued to Address Threats Posed by Foreign Adversary Access to Americans' Data	5
 Exploit and Vulnerability Intelligence Key Findings	8
CVE-2024-56116	8
CVE-2022-23227	8
 Ransomware and Breach Intelligence Key Findings	11
ZeroFox Observes Several High-Profile Ransomware Incidents	11
Breaches Affect Several Entities	12
 Appendix A: Traffic Light Protocol for Information Dissemination	14
 Appendix B: ZeroFox Intelligence Probability Scale	15

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence January 2025 Geopolitical Brief

Political and social unrest is very likely across Europe in the early part of 2025. Both France and Germany are struggling with minority-led governments unable to address key issues surrounding immigration and the cost of living. Simultaneously, several Eastern European states are likely to experience energy shortages. There will likely be a years-long battle for control of Syria, which will likely result in a deeply fractured society, with some parts of the country influenced by Türkiye, other parts by Iran and Iraq, and still others controlled by jihadist groups like the Islamic State. After decades of geopolitical tensions and military neutrality, Japan and South Korea agreed to mend ties in order to become military powerhouses. However, the two presidents who pushed through policies aimed at focusing on greater enemies in China and North Korea were suddenly removed from office, risking wider political instability in East Asia. Unrest in Mozambique is part of a wider political shift across Africa, where political parties who have ruled since independence are losing support.

| **Cyber and Dark Web Intelligence** |

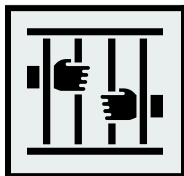
| Cyber and Dark Web Intelligence Key Findings



U.S. Imposes Sanctions on Entities in Iran and Russia over Election Interference

What happened: The United States imposed sanctions on entities from Iran and Russia accused of attempting to interfere in the 2024 U.S. election. According to the U.S. Treasury Department, the entities linked to Iran's Revolutionary Guard Corps (IRGC) and Russia's military intelligence agency (GRU) were engaged in activities aimed at stoking political divisions and influencing the voters through disinformation campaigns.

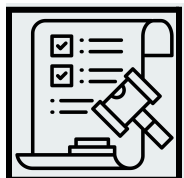
- **What this means:** The sanctions imposed are a significant response to ongoing foreign interference aimed at destabilizing the electoral processes. Ahead of the 2024 U.S. elections, Russian and Iranian state-backed actors significantly ramped up their cyberattacks, as detailed by multiple sources (including a [ZeroFox advisory](#) that highlighted these adversary activities). Russia used AI-generated [deepfake](#) videos to spread false narratives about Vice President Kamala Harris, while [bomb threats](#) targeting polling locations were traced back to Russian email domains. Additionally, Russian state-backed actors also launched a massive [disinformation](#) campaign, flooding the American media ecosystem with fake news disguised as credible sources. Meanwhile, Iranian operatives contributed by leaking hacked emails from Trump's campaign, further fueling political division. Numerous incidents on the deep and dark web (DDW) saw actors monetizing the election by selling malicious services designed to target the voter base, as well as illicitly obtained personally identifiable information (PII) and personal financial information (PFI). Federal agencies such as the Federal Bureau of Investigation (FBI), Cybersecurity & Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI) have also observed a rise in [influence campaigns](#) from Russia aimed at undermining public confidence in the integrity of U.S. elections. Meanwhile, Russia's embassy in Washington denied any interference, insisting that Russia has never and will never engage in meddling with the internal affairs of other countries, including the United States.



Suspect Accused of Hacking Trump's AT&T Call Records Arrested

What happened: An individual in Texas has been arrested for allegedly transferring confidential phone records unlawfully. Authorities suspect the individual is the cybercriminal known as “Kiberphant0m”, who is accused of breaching at least 15 telecommunications firms. The attackers reportedly targeted a select group of users from major U.S. telecom companies, such as AT&T and Verizon. Although the networks have since been secured, the hackers previously gained full access to record calls and steal call data. This prompted CISA to [recommend](#) encrypted communication for high-profile individuals to mitigate future risks.

- **What this means:** The [charges](#) suggest Kiberphant0m knowingly sold and shared sensitive phone records without permission, which can likely lead to identity theft, extortion, and other crimes. Kiberphant0m even bragged on BreachForums about stealing AT&T call logs for President-elect Donald Trump and Vice President Kamala Harris. The individual is suspected to be connected to a larger group of cybercriminals working together to profit from stolen data. The threat actors targeted a few individuals of “foreign intelligence interest.” Although a small number of users have been targeted, such breaches can likely enable nation-state actors to geolocate individuals, intercept sensitive communications, and compromise national security. Even with mitigations in place, the risks of undetected persistence or future attacks likely remain a threat.



Final Rule Issued to Address Threats Posed by Foreign Adversary Access to Americans' Data

What happened: The U.S. Department of Justice (DOJ) has issued a comprehensive [final rule](#) carrying out Executive Order (E.O.) 14117 “Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.” The E.O. charged the DOJ with establishing and implementing a new regulatory program to address the urgent and extraordinary national security threat posed by the continuing efforts of countries of concern—and covered persons that they can leverage—to access and exploit Americans’ bulk sensitive personal data and U.S. government-related data.

- **What this means:** The final rule lays down generally applicable rules for certain categories of data transactions that pose an unacceptable risk to U.S. national security. Adversarial nation-states and covered persons can use their access to this data to engage in malicious cyber-enabled activities and malign foreign influence activities, bolster their

military capabilities, and track and build profiles on U.S. persons. This includes members of the military and U.S. Intelligence Community, as well as other federal employees and contractors for illicit purposes such as blackmail, coercion, and espionage. These entities are also likely to exploit this data to collect information on activists, academics, journalists, dissidents, political opponents, and members of nongovernmental organizations or marginalized communities in order to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. Another concern addressed by the final rule is the use of artificial intelligence (AI) in conjunction with multiple unrelated data sets (for example, to identify U.S. persons whose links to the federal government would be otherwise obscured in a single dataset and who can then be targeted in espionage or blackmail).

| **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. A remote command injection vulnerability in Four-Faith router models F3x24 and F3x36, tracked as [CVE-2024-12856](#), is being exploited by threat actors to open reverse shells to the attackers. Another vulnerability found in D-Link DIR-823G 1.0.2B05_20181207 ([CVE-2024-13030](#)) affects a function of the component Web Management Interface, which can enable threat actors to remotely manipulate leads to access controls. Two more bugs in D-Link routers, CVE-2022-37056 and CVE-2024-33112, were used by two botnets tracked as “Ficora” and “Capsaicin” for [initial access](#). A threat actor has allegedly leaked a zero-day [exploit](#) that enables attackers to execute arbitrary code on a victim’s machine when opened or extracted with the latest version of 7-Zip. In the past week, CISA added [CVE-2024-3393](#), a Palo Alto Networks PAN-OS malformed DNS packet bug, to its KEV Catalog.



HIGH

CVE-2024-56116

What happened: A cross-site request forgery vulnerability in Amiro.CMS before 7.8.4 allows remote attackers to create an administrator account.

- **What this means:** This vulnerability allows attackers to trick authenticated users into performing unintended actions. An attacker can gain full control of the content management system, enabling them to modify content, add malicious scripts, or delete important data.
- **Affected products:**
 - Amiro.CMS versions 7.8.4 and earlier



CRITICAL

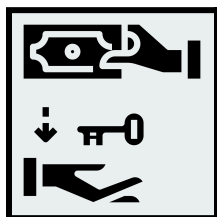
CVE-2022-23227

What happened: NUUO NVRmini2 through 3.11 allows an unauthenticated attacker to upload an encrypted TAR archive, which can be abused to add arbitrary users because of the lack of `handle_import_user.php` authentication. When combined with another flaw (CVE-2011-5325), it is possible to overwrite arbitrary files under the web root and achieve code execution as root.

- **What this means:** This vulnerability enables an unauthenticated attacker to gain unauthorized access to the NUUO NVRmini2 system, potentially leading to full control of the device. By exploiting the flawed authentication mechanism and combining it with the ability to overwrite critical system files, an attacker can likely execute arbitrary code with root privileges. This can result in the compromise of sensitive surveillance data, disruption of security operations, and broader network exposure, making it a severe threat to both system and organizational security.
- **Affected products:**
 - NUUO NVRmini2 versions through 3.11

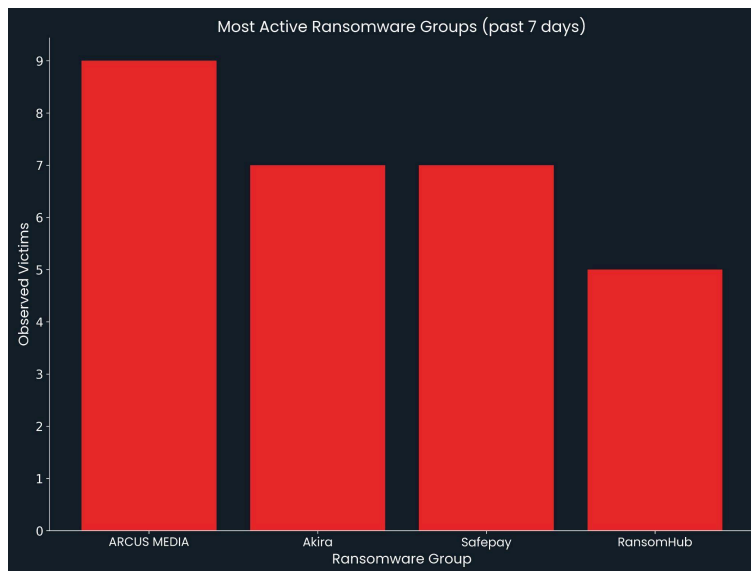
| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings



ZeroFox Observes Several High-Profile Ransomware Incidents

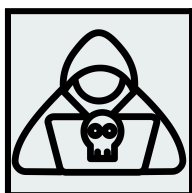
What happened: In the past seven days, ZeroFox has observed over 110 ransomware attacks primarily targeting the technology sector, with the Arcus Media ransomware group accounting for the highest number. Over 45 percent of these targeted entities are located in North America. ZeroFox observed an [update](#) on the Space Bears ransomware leak site targeting Atos, a France-based IT company. Atos has recently [confirmed](#) that the Space Bears ransomware group did not directly compromise the company's infrastructure, stating no evidence of a breach or ransom demand has



Source: ZeroFox Internal Collections

been found so far. However a third-party vendor did get compromised. On December 27, 2024, ZeroFox observed threat actor "Rey" [claiming](#) to have access to servers belonging to the Ministry of National Defense of Turkey on the predominantly English-language dark web forum BreachForums. ZeroFox observed an [update](#) on the RansomHub ransomware leak site targeting MetLife, a U.S.-based company that provides insurance benefits, annuities, and asset management services. MetLife [reportedly](#) denies the attack, stating there is no known incident impacting its Latin American operations. The ransomware group has set an 11-day countdown for payment, showcasing Spanish-language documents as proof of their claims. The U.S. Department of Health and Human Services (HHS) [proposed](#) updates to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to bolster healthcare cybersecurity and protect sensitive patient data from increasing ransomware threats. The Brain Cipher ransomware gang has been [leaking](#) data stolen from Rhode Island's "RIBridges" social services platform, which manages programs like healthcare and food assistance. Leaked files reportedly include databases, backups, and other sensitive data, raising concerns about the privacy of affected individuals.

- **What this means:** Cybercriminals often use third-party breaches as stepping stones to attack their primary targets. If the affected third-party company has access to Ato's systems, this could lead to further compromise. If the third-party company provides critical services such as cloud storage, software development, or IT support, the ransomware attack can likely disrupt operations for the tech company. If threat actor Rey's claims are true, access to Turkey's Ministry of National Defense's servers could mean exposure of sensitive military or governmental information, which adversaries could exploit for espionage, operational disruptions, or strategic advantages. Such data can likely lead to targeted campaigns against individuals or institutions in Turkey. A ransomware attack on MetLife can likely compromise sensitive information such as PII, financial records, and health-related data. Threat actors often target healthcare companies knowing that a ransom demand is highly likely to be met. If it is not, the resulting leak could expose millions of customers to identity theft, financial fraud, or phishing attacks. Hospitals are often forced to meet the demands since encrypted systems could halt operations, delay claims processing, and disrupt critical services to policyholders. As a response to ransomware attacks plaguing the healthcare industry, HIPAA aims to strengthen the Security Rule by requiring all implementation specifications to be mandatory, standardizing compliance timeframes, and mandating detailed documentation and risk assessments. Key proposals include developing an annual technology asset inventory, encrypting ePHI, implementing multi-factor authentication, conducting regular vulnerability scans and penetration tests, and ensuring network segmentation.



Breaches Affect Several Entities

What happened: In the past week, several healthcare entities notified thousands of patients about data breaches impacting sensitive [patient data](#), including medical records and PII. Threat actor "888" targeted American motorcycle manufacturer Harley-Davidson in an alleged data breach, claiming to leak a database with sensitive personal details of over [66,700](#) customers. Improper configuration of two IT applications of Cariad, Volkswagen's automotive software company, compromised the data collected from around [800,000](#) electric vehicles. The data, stored on a widely used cloud platform, included sensitive personal information, including precise geolocation details that could pinpoint vehicle locations down to a few centimeters. Another data breach impacting consumer electronics accessories manufacturer ZAGG Inc. exposed customer [credit](#)

[card data](#) to unauthorized threat actors. Meanwhile, ZeroFox observed a threat actor advertising some allegedly sensitive and confidential documents, claiming they belonged to the Russian Federal Security Service ([FSB](#)). The actor posted the leaked sample data along with a password.

- **What this means:** The data breaches affecting several healthcare firms involved sensitive patient data, which is likely to expose patients to identity theft, fraud, and privacy risks, with stolen data potentially misused for unauthorized medical services. Meanwhile, in response to a surge in healthcare data breaches, the HHS proposes strengthening [HIPAA](#) to secure patients' health data. The Harley-Davidson breach exposed personal data like names, addresses, and emails, risking identity theft. At the time of writing, Harley-Davidson has yet to confirm the breach officially. The Cariatid data breach exposed terabytes of sensitive customer data from major Volkswagen brands, including Audi, threatening customer privacy and security. Malicious actors will likely exploit leaked location data to track movements, steal information, plan targeted attacks, and conduct identity theft. The ZAGG Inc. breach compromised customer credit card data, which puts customers at risk of financial fraud, extortion, and blackmail. Finally, if the alleged FSB document leak is legitimate, it will likely expose Russia's sensitive security details to other threat actors. This data will likely attract financially and politically motivated groups, enabling blackmail, extortion, or strategic state advantages.

| 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%