



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 8, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the cyber threat landscape. 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 (EDT) on January 5, 2024*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber Intelligence Key Findings	3
Hackers Attack U.K.'s Nuclear Waste Services Through LinkedIn	3
Russian Intelligence Hacks Webcams in Kyiv to Aid Missile Strikes	3
Researchers Develop New Black Basta Decryptor to Recover Files	3
 Deep and Dark Web Intelligence Key Findings	6
3 TB of Data Stolen from Popular Iranian Food Delivery Service Snappfood	6
Threat Actor "Zelda" Claims Leak of Iranian Nuclear Power Communication	6
Pro-Russian Hacktivist Group "UserSec" Claims Web Defacement Attack Against NATO Countries	7
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2023-7134	9
CVE-2023-7114	9
 Ransomware and Breach Intelligence Key Findings	11
LockBit Ransomware Gang Most Active	11
Breach Disclosure: Konga	11
 Appendix A: Traffic Light Protocol for Information Dissemination	12
 Appendix B: ZeroFox Intelligence Probability Scale	13

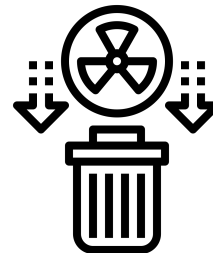
| Cyber Intelligence |

| Cyber Intelligence Key Findings

Hackers Attack United Kingdom's Nuclear Waste Services

Through LinkedIn

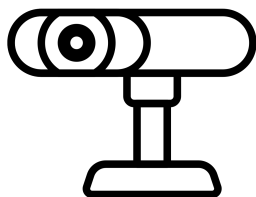
What happened: The United Kingdom's Radioactive Waste Management (RWM) company recently faced a cyberattack attempt that targeted the organization through LinkedIn. The RWM manages the 50 billion GBP Geological Disposal Facility (GDF) project, which aims to create an underground nuclear waste repository in the United Kingdom. Specific details, whether it involved phishing or an attempt to trick employees into installing malware, are unknown. The company's multi-layered defense systems detected and thwarted the attack, preventing unauthorized access.



- **What this means:** This is another example of threat actors leveraging the corporate and professional information that can be found on LinkedIn in order to craft targeted attacks against organizations, and organizations should remain vigilant against attacks looking to trick employees from information harvested online.

Russian Intelligence Hacks Webcams in Kyiv to Aid Missile

Strikes



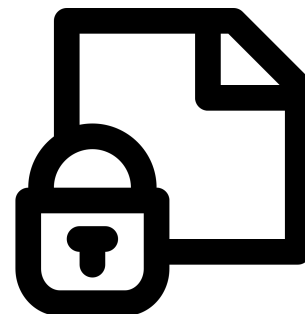
What happened: A recent missile strike on Kyiv, aided by two webcams in the Ukrainian capital city hacked by Russian agents, has evoked concerns among Ukraine's security agencies. The Security Service of Ukraine (SSU) has stated that Russian intelligence services gained operational control of the two webcams, both of which were situated in residential areas, to monitor the surroundings, collect data, and "adjust strikes on Kyiv."

- **What this means:** The SSU has also asked webcam owners and operators to restrict broadcasts from their devices to prevent Russian intelligence from further using the feeds for military surveillance against strategic targets.

Researchers Develop New Black Basta Decryptor to Recover Files

What happened: Cybersecurity researchers have developed a new decrypting tool that leverages a vulnerability in Black Basta Ransomware, letting victims recover their encrypted files for free. The decryptor Black Basta Buster exploits an encryption algorithm flaw in the ransomware's encryptor tools.

- **What this means:** This can recover files that are more than 5,000 bytes and were targeted by Black Basta from November 2022 to this month—full recovery is possible for files between 5,000 bytes and 1 GB in size. For files larger than 1 GB, the first 5,000 bytes of data will be lost.



Deep and Dark Web Intelligence

| Deep and Dark Web Intelligence Key Findings

3 TB of Data Stolen from Popular Iranian Food Delivery Service Snappfood



What happened: On December 30, 2023, a hacker or hacking group identified as “irleaks” disclosed via BreachForums and Telegram that it had allegedly stolen three terabytes of highly sensitive data from the popular online Iranian food delivery service Snappfood. The stolen data reportedly includes over 20 million customer profiles such as usernames, email addresses, and password hashes; payment details of over 600,000 customers; data from 180 million devices; and trip-related information such as addresses and GPS locations of customers and delivery drivers.

The initial compromise is presumed to have occurred via a Snappfood employee’s computer infected with the StealC info-stealer malware. This attack follows two previous dumps of stolen data by “irleaks” involving numerous Iranian insurance companies within the past year, the most recent of which on December 20 consisted of 23 companies and over 160 million pieces of personal data.

- **What this means:** Despite being an unknown threat actor with previously little to no reputation, the breaches of such high-profile companies and the amount of data obtained indicate a highly sophisticated and experienced actor. It is possible that “irleaks” is a new subset of another, more prominent, hacking group or is state-sponsored. ZeroFox will continue to monitor the dark web for continued activity by “irleaks” as well as additional information that could lead to the actor or actors’ attribution.

Threat Actor “Zelda” Claims Leak of Iranian Nuclear Power Communication

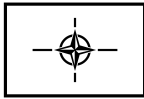
What happened: On January 3, 2024, threat actor “Zelda” claimed to have leaked the top secret messages from Iranian Nuclear power on the predominantly English-language dark web forum BreachForums.

- **What this means:** Iran continues to be targeted with cyberattacks. The more frequent attacks as of late are most likely due to Iran’s involvement in the regional conflict. However, more recent cyberattacks are bringing more focus on high-value Iranian institutions and infrastructure, highlighting more sophisticated attacks.



Pro-Russian Hacktivist Group “UserSec” Claims Web

Defacement Attack Against NATO Countries



What happened: On December 29, 2023, the pro-Russian hacktivist group UserSec announced that they were forming a DDoS squad to attack European and North Atlantic Treaty Organization (NATO) countries. The group planned to recruit those with specific requirements. On January 1, 2024, the group claimed to have defaced a few websites from NATO countries such as Romania, Canada, Poland, Holland, and Germany.

- **What this means:** This comes after Anonymous Russia also announced the targeting of NATO countries in December 2023. These two groups may join forces to work together in DDoS attacks. These DDoS attacks are unlikely to be highly disruptive campaigns against NATO targets of critical value. Any such attacks are likely to have limited operational impact as well.

Exploit and Vulnerability Intelligence

| Exploit and Vulnerability Intelligence Key Findings

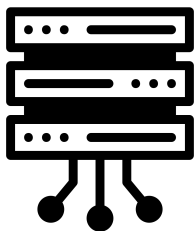
[CVE-2023-7134](#)

What happened: A vulnerability was found in SourceCodester Medicine Tracking System 1.0 that has been rated as **CRITICAL**. This issue affects some unknown processing. The manipulation of the argument page leads to path traversal: '../filedir'. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249137 was assigned to this vulnerability.



- **What this means:** Currently, this is in the proof-of-concept stage, and no countermeasures against it are known, so alternative options may be necessary.

[CVE-2023-7114](#)



What happened: Mattermost version 2.10.0 and earlier fails to sanitize deeplink paths, which allows an attacker to perform cross-site request forgery vulnerability (CSRF) attacks against the server.

- **What this means:** Exploiting this vulnerability successfully requires user interaction by the victim. It is recommended that users upgrade to version 2.10.1 to mitigate this risk.

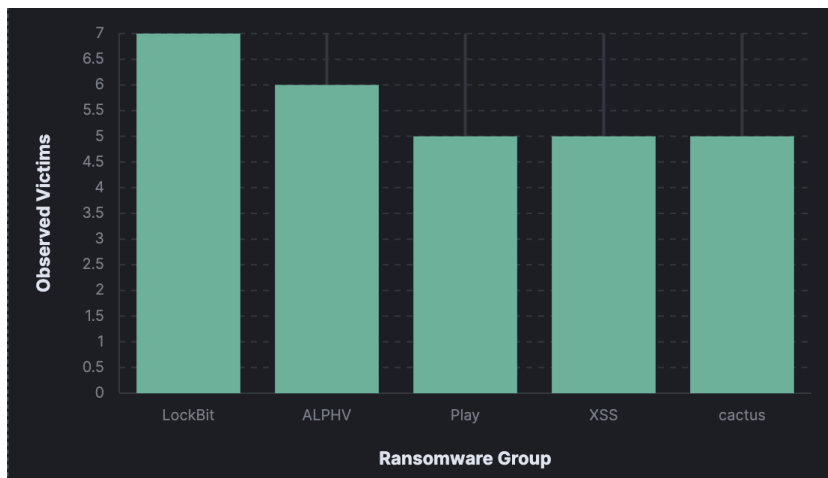
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

LockBit Ransomware Gang Most Active

What happened: Similar to last week, the LockBit ransomware group was once again observed by ZeroFox Intelligence as the most active over the past week, with seven victims identified during that time. The LockBit group has targeted organizations in the supply chain services, education, and manufacturing, along with other industries, which are located in the United States, Czech

Republic, France, Belgium, and, interestingly, Taiwan. In addition, the ransomware group ALPHV was almost as active, with six observed victims.



- **What this means:** Organizations should adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege, implement secure password policies with phishing-resistant MFA, complex passwords, and unique credentials, and deploy robust External Attack Surface Management solutions for ongoing Lockbit-targeted discovery.

Source: ZeroFox Internal Collections

Breach Disclosure: Konga



What happened: Konga, a Nigeria-based e-commerce company, had 2,112,029 records containing personally identifiable information exposed, which were subsequently shared on a deep web platform. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

- **What this means:** Impacted users should update their passwords immediately and remain vigilant against phishing attempts.

Interested in more ZeroFox Threat Intelligence? ZeroFox researchers produce timely, relevant, and actionable [intelligence reporting](#) regularly to keep your team informed on developments in the threat landscape.

| 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%