



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 1, 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 December 29, 2023*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber Intelligence Key Findings	3
Infamous Carbanak Malware Reemerges in Ransomware Attacks	3
Cyberattack Disrupts Emergency Care at German Hospitals	3
Poorly Secured Linux SSH Servers Under Attack for Cryptocurrency Mining	3
 Deep and Dark Web Intelligence Key Findings	6
Hacktivist Group “Cyber Toufan” Targets Critical Infrastructure in Israel	6
Anonymous Sudan Claims DDoS Attack Against Microsoft OneDrive	6
Ddarknotevil Claims Leak of 940,000 Records of Voter Data	7
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2023-51385	9
CVE-2023-48107	9
 Ransomware and Breach Intelligence Key Findings	11
LockBit Ransomware Gang Most Active	11
Breach Disclosure: NGS	11
 Appendix A: Traffic Light Protocol for Information Dissemination	12
 Appendix B: ZeroFox Intelligence Probability Scale	13

| Cyber Intelligence |

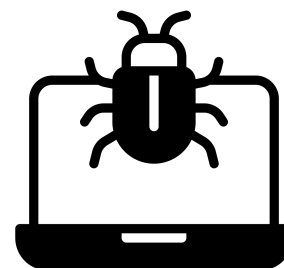
Cyber Intelligence Key Findings

Infamous Carbanak Malware Reemerges in Ransomware

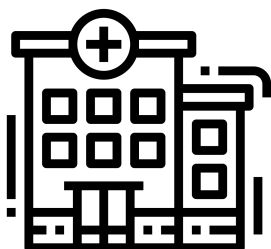
Attacks

What happened: Cybersecurity agencies have observed the infamous banking malware strain Carbanak in ransomware attacks with renovated strategies. Last month, the return of Carbanak was marked with its distribution through compromised websites while masquerading as different business-related software systems.

- **What this means:** The malware strain can now modify itself to assimilate attack vendors and improve its effectiveness, and in the most recent documented attack, the compromised websites were hosting malicious installer files disguised as genuine utilities to facilitate Carbanak's deployment.



Cyberattack Disrupts Emergency Care at German Hospitals



What happened: German hospital network Katholische Hospitalvereinigung Ostwestfalen (KHO) has been the target of recent service disruptions reportedly by an unknown threat actor, suspected to be the Lockbit ransomware group. The attack affected the IT systems supporting three hospitals in Bielefeld, Rheda-Wiedenbrück, and Herford. The threat actors gained access to the hospital network and encrypted data. Reportedly, all systems were shut down, and necessary parties and institutions were informed.

- **What this means:** Although essential patient information is accessible through backups, emergency care in the three hospitals is unavailable, leading to the redirection of patients to other facilities and potential delays in medical care.

Poorly Secured Linux SSH Servers Under Attack for

Cryptocurrency Mining

What happened: Recent research finds that a new multi-platform threat called NKAbuse is leveraging a decentralized, peer-to-peer network



connectivity protocol called New Kind of Network (NKN) as a communications channel for DDoS attacks to single out Linux devices.

- **What this means:** Cyber attackers are focusing on poorly secured Linux SSH servers, aiming to install port scanners and dictionary attack tools. Reportedly, the threat actors aim to compromise other vulnerable servers, forming a system for cryptocurrency mining and distributed denial-of-service (DDoS) attacks.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Hacktivist Group “Cyber Toufan” Targets Critical Infrastructure in Israel



What happened: On December 26, 2023, pro-Palestine hacktivist group Cyber Toufan Operations claimed to leak data packages against Israel Securities Authority, ICL Group, a chemical company, Carolina Lemke, an online sunglasses and eyeglasses retailer, ARI, a manufacturer of various water supply tools, and Palram Industries, a manufacturer of thermoplastic solutions.

➤ **What this means:** These data breaches imply that hacktivist groups supporting Palestine during the current war are escalating their attacks against Israel-based organizations by focusing on critical infrastructure sectors that provide essential necessities, such as water and chemical solutions.

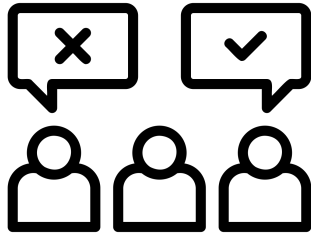
Anonymous Sudan Claims DDoS Attack Against Microsoft OneDrive

What happened: On December 28, 2023, threat actor group Anonymous Sudan claimed on its Telegram channel to have carried out a Distributed Denial-of-Service (DDoS) attack against Microsoft OneDrive. The group's stated reasoning for the attack was to draw attention to "the tragic situation in Sudan." This attack is the latest in an active string of DDoS attacks throughout the last month by Anonymous Sudan, with victims including Blizzard Entertainment, Reddit, Discord, Spotify, and several government entities across the globe.



➤ **What this means:** When Anonymous Sudan began conducting operations in January 2023, it primarily focused on targeting a variety of organizations in Sweden. Yet, these recent alleged attacks demonstrate how the group has easily expanded its targeting to organizations and governments around the globe. While these attacks have not resulted in any publicly reported significant or lasting damage, the consistency of the alleged attacks against a variety of high-profile targets in such a short time frame reflects the group's likely growing confidence in its operational capacity.

Ddarknotevil Claims Leak of 940,000 Records of Voter Data



What happened: On December 28, 2023, well-regarded and established threat actor “Ddarknotevil” advertised an alleged data breach of USA voter data from Didit, an internet marketing service on the predominantly English-language dark web forum “BreachForums.” The threat actor claims to have leaked 940,000 records, including full name, email, phone number, address, and more.

➤ **What this means:** Leaks of voter data are a recurring problem in cyberspace. When this occurs around general elections, it can become a more serious issue. These breaches show election infrastructure vulnerability. If threat actors can access voter databases, they have the potential to access other critical election infrastructure, which could allow them to manipulate voting results, threaten the democratic process, and possibly leak other highly confidential info.

Exploit and Vulnerability Intelligence

| Exploit and Vulnerability Intelligence Key Findings

[CVE-2023-51385](#)

What happened: A vulnerability classified as **CRITICAL** has been found in OpenSSH before 9.6, where an OS command injection might occur if a user name or hostname has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or hostname.



- **What this means:** While the vulnerability itself is novel, the expected impacts are likely limited on session secrecy or integrity.

[CVE-2023-48107](#)



What happened: A **HIGH** CVE identified this week was a Buffer Overflow vulnerability in zlib-ng minizip-ng v.4.0.2, which allows an attacker to execute arbitrary code via a crafted file to the mz_path_has_slash function in the mz_os.c file.

- **What this means:** An update is available for this vulnerability and recommended immediately.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

LockBit Ransomware Gang Most Active

What happened: The LockBit ransomware group was once again observed by ZeroFox Intelligence as the most active over the past week, with eight victims identified during that time. The LockBit group has targeted organizations in the financial services, healthcare, and education industries, along with other industries, which are located in the United States and Australia. In addition, the ransomware group ALPHV was almost as active with seven observed victims.



Source: ZeroFox Internal Collections

➤ **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.

Breach Disclosure: NGS



What happened: Russia-based news and media publishers NGS had 9,756,438 email addresses and/or usernames exposed, which were subsequently shared on a deep web platform. Of these, an assessed 7,210,754 records were successfully linked to hashed passwords. Other notable data fields observed in this package include name, and user activity. 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%