



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 15, 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 12, 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
Flash Report – Alleged Sale of Three Exploits, Including Two Zero-Days	2
Flash Report – LockBit Ends 2023 with Record Number of Attacks	2
Profile – APT28 Distributes New Malware Strains OCEANMAP, MASEPIE, and STEELHOOK	2
Flash Report – Rise in Digital Extortion Attacks Against Healthcare in North America	2
Cyber Intelligence Key Findings	4
After Injecting Cancer Hospital with Ransomware, Criminals Threaten to Swat Patients	4
Ukraine Claims Revenge Hack Against Moscow Internet Provider	4
Turkish APT Targets Private and Public Entities in the Netherlands for Espionage	4
Deep and Dark Web Intelligence Key Findings	7
Threat Actor 'sandocan' Continues to Promote Remote Desktop Access to Companies Across the Globe	7
Akira Ransomware Updated their Leak Site with a Semiconductor Technology Manufacturing Firm	7
Snatch Ransomware Group Claims to Dox U.S. Officials on Their Telegram Channel	8
Exploit and Vulnerability Intelligence Key Findings	10
CVE-2024-0296	10
CVE-2004-0458	10
Ransomware and Breach Intelligence Key Findings	12
LockBit Ransomware Gang Most Active	12
Breach Disclosure: RaidForums	12
Appendix A: Traffic Light Protocol for Information Dissemination	13
Appendix B: ZeroFox Intelligence Probability Scale	14

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Flash Report - Alleged Sale of Three Exploits, Including Two Zero-Days](#)

In this flash report, ZeroFox researchers report on the announcement on the dark web of the sale of three exploits: two zero-day vulnerabilities impacting SonicWall Virtual Private Networks and Microsoft Windows, and a third one-day vulnerability in an undisclosed JetBrains product.

[ZeroFox Intelligence Flash Report – LockBit Ends 2023 with Record Number of Attacks](#)

In this flash report, ZeroFox researchers report on the Ransomware & Digital Extortion threat collective LockBit's record number of attacks in Q4 2023 (October–December).

[ZeroFox Intelligence Profile - APT28 Distributes New Malware Strains OCEANMAP, MASEPIE, and STEELHOOK](#)

In this Intelligence Profile, ZeroFox researchers provide an overview of APT28 and its background after it has been observed distributing new strains of malware.

[ZeroFox Intelligence Flash Report - Rise in Digital Extortion Attacks Against Healthcare in North America](#)

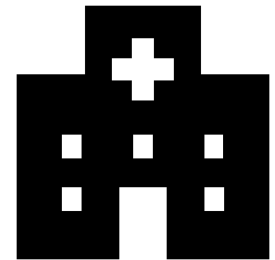
In this flash report, ZeroFox researchers report on the record number of Ransomware & Digital Extortion (R&DE) attacks against the North American healthcare sector in Q4 2023 (October–December) following a sustained rise throughout the year.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

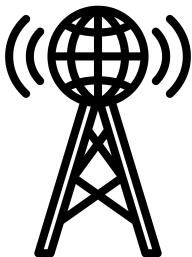
After Injecting Cancer Hospital with Ransomware, Criminals Threaten to Swat Patients

What happened: Cybercriminals are turning their attention to patients in an attempt to have their ransomware demand fulfilled by threatening them with bogus police reports if medical centers do not pay their ransomware. These reports have the potential to bring swat teams to patients' homes and elicit potentially dangerous outcomes. After a cyberattack on Fred Hutchinson Cancer Center, where medical records were stolen, criminals threatened to make bomb threats or false reports to law enforcement about patients. Similar threats were reported by Integris Health in Oklahoma.



- **What this means:** With this tactic, the threat actors aim to pressure hospitals to pay ransoms to prevent harm to patients and avoid negative publicity.

Ukraine Claims Revenge Hack Against Moscow Internet Provider

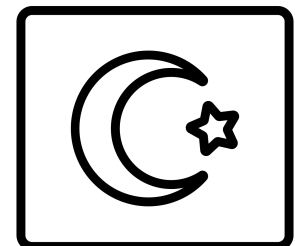


What happened: The Ukrainian Blackjack hacker group conducted a cyberattack on Moscow-based Internet provider M9 Telecom. The attack resulted in the destruction of M9 Telecom's servers, wiping off approximately 20 terabytes of data, including the company's official website, branch sites, mail server, and cyber protection services. Following the cyberattack, some residents in Moscow experienced disruptions in internet and television services. The hackers have reportedly warned that this attack is the start of a larger attack, which will be "serious revenge for Kyivstar."

- **What this means:** Expect similar attacks to occur back-and-forth between Russia and Ukraine as the war in Ukraine heads into its third year.

Turkish APT Targets Private and Public Entities in the Netherlands for Espionage

What happened: Turkey-associated Advanced Persistent Threat (APT) group, tracked as Sea Turtle, Cosmic Wolf, Marbled Dust, Silicon, and Teal Kurma, has targeted critical public and private infrastructures in the Netherlands over the past year as a part of cyberespionage efforts. Sea Turtle has been exploiting systems in the target infrastructures, vulnerable to supply-chain and island-hopping attacks, to steal crucial data.



- **What this means:** The stolen information includes politically motivated information that the APT has presumably used for intelligence gathering or surveillance.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor 'sandocan' Continues to Promote Remote Desktop Access to Companies Across the Globe

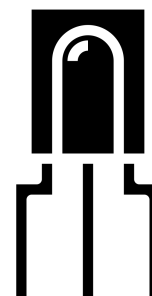


What happened: On January 9, 2024, esteemed threat actor 'sandocan' advertised an auction for RDWeb access with domain user rights to an unnamed U.S.-based insurance company on the predominantly Russian language dark web forum, Exploit. According to 'sandocan', the targeted insurance company generates USD 10 million in revenue. Just a day earlier, on January 8, 2024, the threat actor advertised an auction for RDWeb access with domain user rights to an unnamed Brazilian non-profit organization with a stated worth of USD 247 million.

➤ **What this means:** These recent posts are the latest in a seemingly broader campaign by 'sandocan'. ZeroFox has tracked similar activity from 'sandocan' since July 2023, in which the threat actor has advertised remote desktop access to various companies across the globe via Exploit. Previous victims include a French insurance company, a U.S.-based plastic surgery company, an Australian dental insurance company, a German agricultural company, and a U.K.-based law firm. While these auctions have not yet led to reports of significant data breaches, ZeroFox will continue to monitor the actor's activity and posts for any escalation.

Akira Ransomware Updated their Leak Site with a Semiconductor Technology Manufacturing Firm

What happened: On January 9, 2024, ZeroFox observed an update on the Akira ransomware leak site targeting Heller Industries, a U.S.-based industrial machinery manufacturer. Heller Industries specializes in reflow oven technology, fluxless reflow technology, and curing oven technology, providing solutions to electronics manufacturers and semiconductor advanced packagers around the world. The group claims that almost 300 GB of data will be available soon. The files allegedly contain numerous non-disclosure agreements with names of widely known corporations, personal documents, finance files and so on.



- **What this means:** The manufacturing sector is one of the 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are deemed so critical to the U.S. that their incapacity or destruction would have a crippling effect on security, national economic security, national public health or safety, or any combination of these, according to [CISA](#). Specifically, the manufacturing of semiconductor technology is critical to national security because it provides the development of semiconductors, which is a core technology to many other sectors, such as healthcare, defense, information technology, etc. Semiconductors are also essential components in devices ranging from smartphones to advanced military systems. The leaked data from this manufacturing firm may also contain highly confidential and

sensitive information, such as semiconductor technology plans, designs, algorithms, intellectual property, patents, research and development data, and more. Threat actors may take advantage of this leaked data to sell them to competitors, counterfeit manufacturers, or state-sponsored entities, who may exploit them for various purposes. This could include reverse engineering semiconductor technology, producing counterfeits, gaining a competitive advantage, compromising product security, examining it for zero-day vulnerabilities, and more. If the leaked data contains critical information regarding semiconductor technology development, this could have an impact on national security, especially if the leaked data contains sensitive plans for defense-related technology manufacturing.

Snatch Ransomware Group Claims to Dox U.S. Officials on Their Telegram Channel



What happened: On January 10, 2024, the ransomware and hacktivist group Snatch claimed to dox U.S. officials on their Telegram channel. They claim to have the personal data of top U.S. leadership that they began sharing. The group also claimed this is only the beginning, suggesting they have the personal details of additional officials.

➤ **What this means:** While government entities are a common target for threat actors in general, it is not as common to see specific government officials targeted. As the elections draw closer, additional government officials will likely be targeted by other actors/groups. The impact of U.S. leadership's personal details being shared with threat actors could result in various types of attacks against these officials, especially regarding varying

political stances.

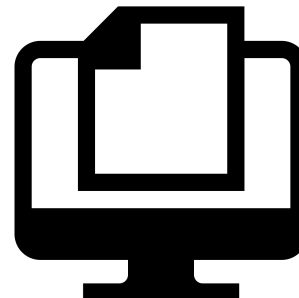
| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

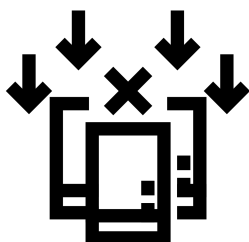
CVE-2024-0296

What happened: A vulnerability has been found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as **CRITICAL**. This vulnerability affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249862 is the identifier assigned to this vulnerability. NOTE:

- **What this means:** The vendor was contacted early about this disclosure but has not yet responded.



CVE-2004-0458



What happened: A vulnerability marked as **HIGH** was identified in mah-jong versions before 1.6.2, which allows remote attackers to cause a denial of service (server crash) via a missing argument, which triggers a null pointer dereference.

- **What this means:** Upgrading to the latest version of mah-jong is recommended in order to avoid running into this issue.

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 nine victims identified during that time. The LockBit group has targeted organizations in the retail, non-profit, and manufacturing sectors along with other industries, which are located all over the world. In addition, the ransomware group ALPHV was almost as active, with six observed victims.

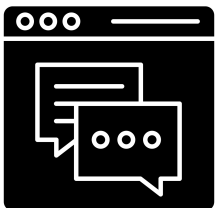
➤ **What this means:**

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: RaidForums



What happened: RaidForums had 478,516 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%