



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

November 13, 2023

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 November 10, 2023*; 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 2024 Key Forecast and 2023 Conclusions	2
Intelligence Brief – Executive Order Outlines U.S. Priorities on AI Governance, Risk Mitigation	2
Intelligence Flash Report – Ransomware and Digital Extortion Landscape Diversifying	2
Intelligence Flash Report – Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability	2
Intelligence Flash Report – Ransomed[.]vc Sunsets Operations, Auctions Off Infrastructure	2
 Cyber Intelligence Key Findings	4
Okta Shares Details on Unauthorized Access to Support Case Management System	4
HC3 Analyst Note: BlackSuit Ransomware	4
Ransomware Attack on The Industrial & Commercial Bank of China (ICBC) Disrupts U.S. Treasury Market Trades	4
 Deep and Dark Web Intelligence Key Findings	7
Iranian APT Group Targeting Middle Eastern Nations	7
Sandworm APT Group Targets Ukrainian Power Grid Once Again	7
Ransomed.vc Shutting Down Operations	7
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2023-35784	10
CVE-2023-21397	10
 Ransomware and Breach Intelligence Key Findings	12
LockBit Ransomware Gang Most Active	12
The Art Story Breach Disclosure	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 2024 Key Forecast and 2023 Conclusions](#)

In this ZeroFox Intelligence Assessment, ZeroFox researchers provide a forecast of anticipated cyber threats in 2024 while also including conclusions from observations in 2023.

[ZeroFox Intelligence Brief - Executive Order Outlines U.S. Priorities on AI Governance, Risk Mitigation](#)

In this intelligence brief, ZeroFox provides an overview of U.S. President Joe Biden's Executive Order, which outlines a policy roadmap for artificial intelligence (AI) including measures to safeguard against emerging risks and to orchestrate a framework for the responsible development and deployment of AI.

[ZeroFox Intelligence Flash Report - Ransomware and Digital Extortion Landscape Diversifying](#)

In this Intelligence Flash Report, ZeroFox researchers report on the diversifying ransomware and digital extortion threat landscape, with a fall in the operational tempo of attacks by major strains and new threat collectives demonstrating proficiency at pace.

[ZeroFox Intelligence Flash Report - Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability](#)

In this Intelligence Flash Report, ZeroFox researchers report on the SysAid zero-day vulnerability (tracked as CVE-2023-47246) being actively exploited by financially motivated threat actors to deploy ransomware.

[ZeroFox Intelligence Flash Report - Ransomed\[.\]vc Sunsets Operations, Auctions Off Infrastructure](#)

In this Intelligence Flash Report, ZeroFox researchers report on the ransomware and digital extortion collective known as Ransomed[.]vc announcing that it no longer wanted to continue running the project and was selling all aspects of its infrastructure.

| Cyber Intelligence |

Cyber Intelligence Key Findings

Okta Shares Details on Unauthorized Access to Support Case Management System

What happened: Identity and access management company Okta has revealed details of the October 2023 data breach in which a threat actor gained access to files inside Okta's customer support system relating to 134 customers (which the company stated is less than 1% of its customer base). The attacker was ultimately able to steal some session tokens to hijack the legitimate Okta sessions of five unnamed customers.



- **What this means:** To combat the threat of session token theft, Okta has released session token binding based on network location. Okta administrators are now forced to re-authenticate if a network change is detected.

HC3 Analyst Note: BlackSuit Ransomware

What happened: The U.S. Health Sector Cybersecurity Coordination Center (HC3) has published an advisory stating that the relatively new BlackSuit ransomware will likely be a credible threat to the public-health sector. The advisory notes how this double-extortion (data encryption and exfiltration) group shares similarities with Royal ransomware, which is believed to be a direct successor to the notorious Russia-based Conti operation.



<https://www.hhs.gov/sites/default/files/black-suit-ransomware-analyst-note-tlpclear.pdf>

- **What this means:** BlackSuit's impact on the sector, MITRE ATT&CK techniques, indicators of compromise, and possible defense and mitigation measures are also detailed in the document. ZeroFox Intelligence has detected more than 150 victims of this operation in the past year, nearly 75 percent of which are in the U.S.-Canada region.

Ransomware Attack on The Industrial & Commercial Bank of China (ICBC) Disrupts U.S. Treasury Market Trades

What happened: The Industrial and Commercial Bank of China (ICBC) is actively trying to restore affected systems after a ransomware attack disrupted some trades in the U.S. Treasury



<https://www.cnn.com/2023/11/10/investing/icbc-ransomware-attack-hnk-intl/index.html>

market on November 8. This, in turn, caused equities clearing issues, as reported by the Treasury Department. Because of this attack, the ICBC was unable to settle the U.S. Treasury trades for other market participants.

- **What this means:** A temporary fix supposedly suggested by the bank suggests some of its brokerage clients reroute their trades. At the time of reporting, there is no official statement from ICBC confirming the severity of the attack.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Iranian APT Group Targeting Middle Eastern Nations

What happened: An Iranian APT group is in the middle of a sophisticated cyber espionage campaign targeting multiple Middle Eastern nations. Scarred Manticore, an APT group that overlaps with APT34, targets critical sectors throughout the region, including the military, government, financial, and telecommunications sectors of numerous nations. The campaign leverages a proprietary framework dubbed "Liontail" to stealthily collect sensitive information.

- **What this means:** Iranian government cyber actors are growing increasingly sophisticated in their attacks. This group is reportedly affiliated with Iran's intelligence service, MOIS, and focused on collecting intelligence. Any organization that is active in the Middle East is at risk of being targeted for connection either directly or indirectly.



Source:
<https://www.britannica.com/topic/flag-of-iran>

Sandworm APT Group Targets Ukrainian Power Grid Once Again

What happened: A Russian state APT group successfully targeted a Ukrainian power grid for the third time. Sandworm, a prominent APT group with ties to Russia's military intelligence agency (GRU), conducted an attack that took an unnamed power grid offline. Of note, this attack coincided with a missile strike during a Russian military offensive.

- **What this means:** Russian cyber actors have taken aggressive action in targeting infrastructure in Ukraine. This particular attack showed the Russian military's willingness and ability to fuse cyber attacks with kinetic operations. The attack shows the lengths to which Russia will go in carrying out cyber attacks against infrastructure targets.



Source:
<https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/>

Ransomed.vc Shutting Down Operations

What happened: Ransomed.vc announced it was shutting down operations instead of selling its infrastructure due to several affiliates allegedly being arrested. The operator claimed the affiliates had a lack of operational security.

- **What this means:** There continues to be a crackdown on ransomware, with new groups forming and disbanding on a regular basis to avoid



Source:
https://twitter.com/CSIRT_KNF/status/1699752243778453569

detection. Low-level actors may not know the best operational security practices, which allow for greater insight into groups and easier takedown.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

[CVE-2023-35784](#)

What happened: One of the most critical Common Vulnerabilities and Exposure (CVE) identified this week was CVE-2023-35784, which is ranked **CRITICAL** and involves the double free or use after free could occur after SSL_clear in OpenBSD 7.2 before errata 026 and 7.3 before errata 004, and in LibreSSL before 3.6.3 and 3.7.x before 3.7.3. NOTE: OpenSSL is not affected.

- **What this means:** Currently, there is no available patch for CVE-2023-35784; however, technical details of the vulnerability are known.

[CVE-2023-21397](#)

What happened: A **HIGH** CVE identified this week was a vulnerability that has been found in Android In Setup Wizard, where there is a possible way to save a WiFi network due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

- **What this means:** Newer versions of Android are much more difficult to exploit, and so users are recommended to update to the latest version as much as possible.

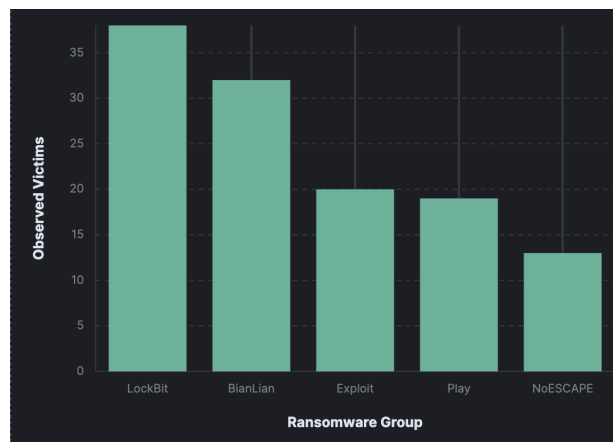
Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

LockBit Ransomware Gang Most Active

What happened: ZeroFox Intelligence has observed the LockBit 3.0 ransomware gang as the most active over the past week, with over 35 victims identified during that time. The group has targeted organizations in a wide variety of industries, including education, retail, logistics, energy, and education, which are located in the United States, Europe, Asia, and South America. In addition, the BianLian group has also been very active and targeting various industries.

- **What this means:** LockBit continues to be one of the most prolific ransomware groups in existence, with success against organizations of all sizes utilizing double-extortion techniques of deploying ransomware on an organization's systems in tandem with exfiltrating data from the organization.



Source: ZeroFox Internal Collections

The Art Story Breach Disclosure

What happened: The Art Story, a U.S.-based educational organization providing e-learning services, had 1,048,575 email addresses exposed, which were subsequently shared on a deep web platform. Of these, an assessed 761,040 records were successfully linked to hashed passwords. Other notable data fields observed in this package include name, IP address, and user activity. The threat actor did not disclose the ultimate source of the data breach or how it was exploited.

- **What this means:** Immediate password changes for affected accounts should be implemented, as well as enabling multi-factor authentication for all organizational accounts to help mitigate phishing and credential stuffing attacks.



Source: [hXXps://www.theartstory\[.\]org/](https://www.theartstory.org/)

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%