



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 29, 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 26, 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
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 02	2
ZeroFox Intelligence Flash Report – New BEC Campaign Set to Target Western Countries	2
 Cyber Intelligence Key Findings	4
SIM Swapping Used to Breach SEC's X Account	4
CISA Issues Emergency Directive (ED) 24-01 on Ivanti Bugs	4
Mother of All Breaches Reveals 26 Billion Records	4
 Deep and Dark Web Intelligence Key Findings	7
Threat Actor 'thx4drugs' Announces Xehook Stealer	7
New Ransomware Group "My Data" Emerges	7
Hacktivist Group 'UserSec' Announces Recruitment for New Defacement Training Team	8
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2023-34048	10
CVE-2024-23222	10
 Ransomware and Breach Intelligence Key Findings	12
xss Forum Exposing Organizations Across the Globe	12
Breach Disclosure: Womplay	12
 Physical and Geopolitical Intelligence Key Findings	14
Physical Security Intelligence: Global	14
Physical Security Intelligence: United States	14
 Appendix A: Traffic Light Protocol for Information Dissemination	15
 Appendix B: ZeroFox Intelligence Probability Scale	16

| This Week's ZeroFox Intelligence Reports

[ZeroFox Intelligence Brief - Underground Economist: Volume 4, Issue 02](#)

The Underground Economist is an intelligence-focused series illuminating Dark Web findings in digestible tidbits from our ZeroFox Dark Ops intelligence team.

[ZeroFox Intelligence Flash Report - New BEC Campaign Set to Target Western Countries](#)

In this flash report, ZeroFox researchers report on the announcement of a new Business Email Compromise (BEC) campaign set to target Western states that promise affiliates substantial monetary profit.

[ZeroFox Intelligence Profile - IntelBroker](#)

In this Intelligence Profile, ZeroFox researchers provide an overview of IntelBroker, a well-regarded and established threat actor who is a hacker and malware developer who has recently increased its targeting of U.S. government entities.

[ZeroFox Intelligence Flash Report - Fortra Discloses Critical MFT Vulnerability](#)

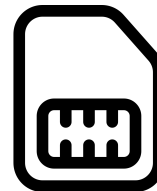
In this flash report, ZeroFox researchers report on Fortra's disclosure of a new critical vulnerability affecting its GoAnywhere Managed File Transfer Software.

| Cyber Intelligence |

Cyber Intelligence Key Findings

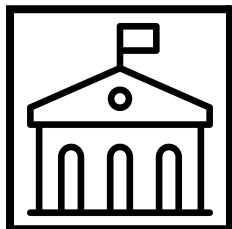
SIM Swapping Used to Breach SEC's X Account

What happened: The U.S. Securities and Exchange Commission (SEC) has confirmed unauthorized access and activity on its @SECGov X account, revealing that the breach resulted from a SIM swap attack on the associated cell phone number. In this attack, the unauthorized party gained control of the phone number through the telecom carrier, allowing them to receive voice and SMS communications. However, no evidence suggests access to SEC systems, data, devices, or other social media accounts.



- **What this means:** As explained in the SEC report, SIM swapping involves transferring a person's phone number to another device without authorization, allowing the unauthorized party to begin receiving voice and SMS communications associated with the number. Law enforcement is currently investigating how the unauthorized party convinced the carrier to change the SIM and how they identified the specific phone number associated with the SEC account.

CISA Issues Emergency Directive (ED) 24-01 on Ivanti Bugs



What happened: In its first emergency directive of 2024 (ED 24-01), CISA has directed all Federal Civilian Executive Branch (FCEB) agencies to immediately mitigate two actively exploited flaws in Ivanti Connect Secure and Ivanti Policy Secure (CVE-2023-46805 and CVE-2024-21887). CISA advises FCEB agencies to apply the updates to the products within 48 hours of Ivanti releasing the updates and implement the mitigations as detailed in the ED.

- **What this means:** After observing widespread and active exploitation of the bugs, CISA determined that they pose "an unacceptable risk" to FCEB agencies and require emergency action. As reported in ZeroFox's Cyber Intelligence Daily Brief on January 14, these bugs are being widely exploited by several threat actors, including Chinese state-linked hackers.

Mother of All Breaches Reveals 26 Billion Records

What happened: A massive data leak has been uncovered, containing a staggering 12 terabytes of data from numerous past breaches, totaling 26



billion records. This extensive leak encompasses user data from platforms like LinkedIn, Weibo, Tencent, and others. Reportedly, Tencent's data amounted to 1.5 billion records leaked, followed by the second largest, Weibo — 504 million records. This breach consolidates records from thousands of meticulously compiled and reindexed leaks and privately traded databases..

- **What this means:** The database contains both old and new, undisclosed information. This indicates that the unknown threat actor could be a data broker service or a malicious actor using this information for identity theft, sophisticated phishing schemes, targeted cyberattacks, and other forms of attacks.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor 'thx4drugs' Announces Xehook Stealer



What happened: On January 20, 2024, threat actor thx4drugs claimed to release a new info stealer named 'Xehook Stealer' on the predominantly Russian-language dark web forum, 'xss.' According to the threat actor, the stealer is written in the C# programming language and has a variety of functionalities, including panel integration with Telegram which allows it to send logs to the messaging platform with a single button. The stealer also purportedly collects passwords, cookie files, credit card information, and auto-filled data from all Chromium and Gecko-based

browsers, as well as supports over 110 cryptocurrency and two-factor authentication browser extensions. Xehook Stealer appears to be an updated, more sophisticated version of the info stealer 'Agniane Stealer,' which was released by the same threat actor in August 2023.

- **What this means:** While the release of these two info stealers is the only activity ZeroFox has observed from thx4drugs, the threat actor's persistence to evolve this malware product indicates the high payout that it hopes to achieve from it. As always, maintaining a heightened awareness of threat actor trends and a high standard of cyber hygiene is crucial to prevent compromise, particularly with auto-fill technology and browser extension usage.

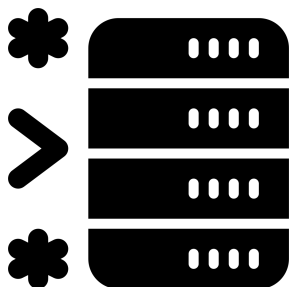
New Ransomware Group "My Data" Emerges

What happened: On January 25, 2024, ZeroFox came across a new ransomware site called MyData Ransomware aka Alpha Locker, which currently lists six victims.

- **What this means:** Recent developments have brought to light a ransomware group known as MyData / Alpha Locker. An examination of their data leak site reveals multiple companies victimized by the group. The data exfiltrated from these companies is relatively recent, dating back to 2023, suggesting that the group is likely still active.



Hacktivist Group 'UserSec' Announces Recruitment for New Defacement Training Team



What happened: On January 25, 2024, threat actor UserSec announced on its Telegram channel that it is recruiting candidates for a new defacement training team with the promise of becoming a permanent member of the defacement team if successful. In addition to reviewing “almost all methods of defacing a website,” UserSec offers to teach users how to obtain administrative panels of websites, search for subdomains, and how to look for XSS and SQL vulnerabilities. UserSec claims to be recruiting three users in total, with an entrance fee of USD 100 each.

- > **What this means:** UserSec is a highly active pro-Russian hacktivist group that routinely claims to carry out various cyber attacks on NATO member states, particularly Distributed Denial-of-Service (DDoS) attacks and website defacements. According to ZeroFox intelligence, the most recent claimed attack against a U.S. entity occurred on January 18, 2024, in which the group targeted the website of precious metals broker American Bullion. The Telegram post announcing the attack included the hashtag “#GloryToRussia.” This all follows UserSec’s announcement last month that it planned to recruit groups to conduct joint attacks against NATO countries and that it planned to form a DDoS squad. While ZeroFox has not tracked UserSec specifically targeting U.S. election-related websites as of yet, it is a significant possibility ZeroFox is monitoring for, particularly as the U.S. presidential race heats up and the group publicly seeks to expand.

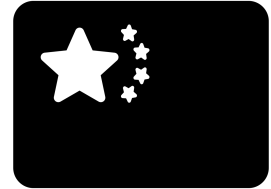
Exploit and Vulnerability Intelligence

| Exploit and Vulnerability Intelligence Key Findings

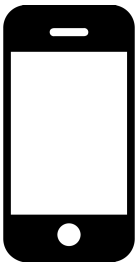
[CVE-2023-34048](#)

What happened: vCenter Server contains a **CRITICAL** out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write, potentially leading to remote code execution.

- **What this means:** No viable in-product workarounds are available. Updates are available for the affected VMware products to fix the vulnerability.



[CVE-2024-23222](#)



What happened: A type confusion issue was addressed with improved checks in this **CRITICAL** vulnerability. Processing maliciously crafted web content may lead to arbitrary code execution. This CVE is under active investigation, and a CVSS score has not been assigned at the time of writing this report.

- **What this means:** Apple is aware of a report that this issue may have been exploited. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3.

| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

xss Forum Exposing Organizations Across the Globe

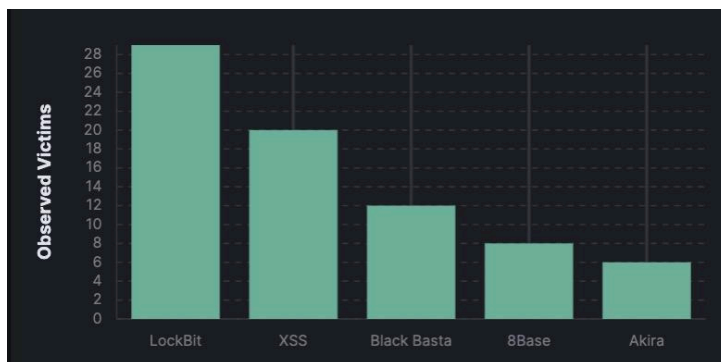
What happened: The LockBit

ransomware group retains its position as the most prolific ransomware group, with ZeroFox Intelligence recording close to 30 victims this week. Meanwhile, primarily Russian-language deep and dark web forum xss has been among the most active among the criminal

underground—with ZeroFox Intelligence recording 13 significant and relevant

posts on the forum this week. The posts involved

claims of network access to companies in Asia, Europe, and South America and the alleged sale of infostealers, as well as remote code execution (RCE) exploits.



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. Threat modeling to tackle internal threats and leaks is necessary to curb the sale of network and internal data on underground forums.

Breach Disclosure: Womplay



What happened: Womplay, a Germany-based earning platform for mobile gamers, allegedly suffered a data breach, after which 145,816 email addresses, names, usernames, and hashed passwords were 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:** Affected users should be wary of unsolicited communication involving targeted emails from unknown sources, as threat actors might use the leaked data for spear phishing attacks.

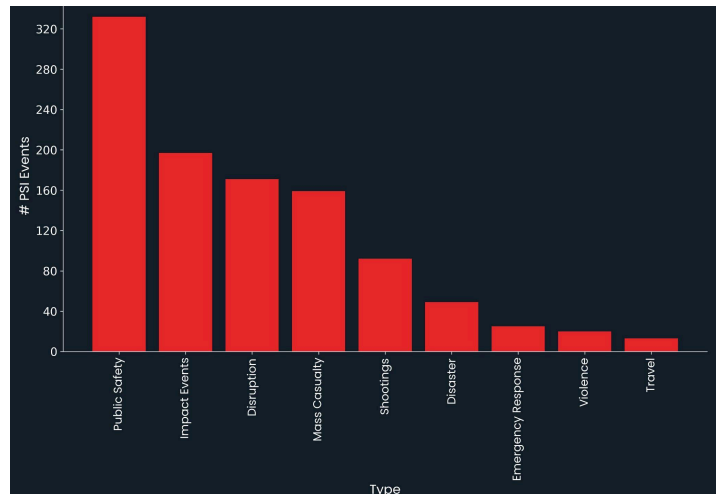
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

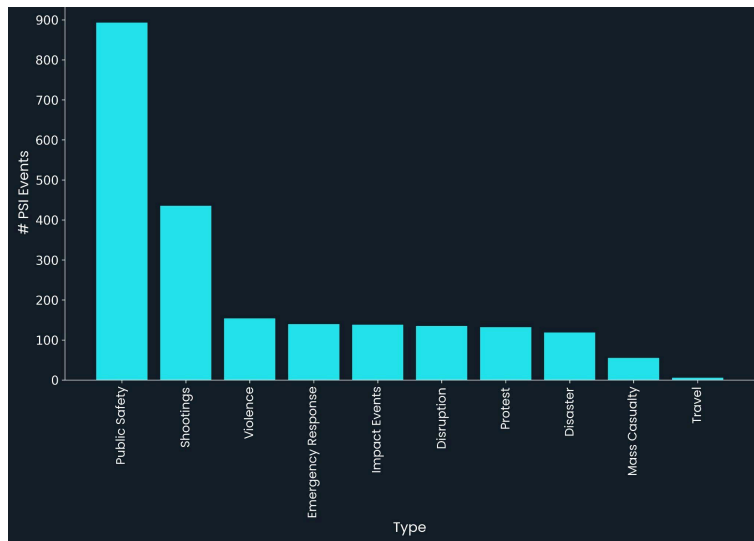
What happened: ZeroFox observed over 300 public safety issues in the past week worldwide (excluding those in the United States, which have been analyzed separately below). Significant protest activity has been observed in the United Kingdom, France, and Germany, while instances of violence continue to be persistent in the Middle East, Ukraine, and Russia.

- **What this means:** Continued escalations in the Israel-Hamas War as well Russia-Ukraine war are contributing to these numbers, and with no apparent immediate resolution, this region is expected to see continued disruptive activity.



Source: ZeroFox Internal Collections

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: New York, California, and Illinois were observed by ZeroFox Intelligence to have the most public safety and shooting activity occur over the past week. Disaster-type activity was most concentrated in Maryland, Texas, and Florida and protest activity most commonly occurring in New York, Texas, and California.

- **What this means:** There was an observed 3 percent increase in public safety events

week-over-week, with protest activity remaining nearly the same.

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%