



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

January 22, 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 19, 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 – Critical Microsoft SharePoint Vulnerability Actively Exploited	2
Flash Report – Disclosure of Critical Atlassian Confluence Vulnerability	2
Flash Report – Mass Access Sale to Retail eCommerce System	2
Flash Report – Citrix Vulnerabilities Continue to Be Exploited	2
Flash Report – Dark Web Actors Promoting Maritime Data	2
Cyber Intelligence Key Findings	4
U.S. Court Docs Expose Fake Antivirus Renewal Phishing Tactics	4
Hacker Spins Up 1 Million Virtual Servers to Illegally Mine Crypto	4
Chrome Addresses Four Vulnerabilities Including an Actively Exploited Zero-Day	4
Deep and Dark Web Intelligence Key Findings	7
'MyFlaw' Zero-Day RCE Vulnerability Uncovered in Opera Browser	7
Threat Actor "IntelBroker" Leaked Data from UK-Based Auto Manufacturer Vauxhall Motors	7
Actor KernelMode Advertised Malware for Sale Designed to Kill Most AV and EDR Products	8
Exploit and Vulnerability Intelligence Key Findings	10
CVE-2024-0552	10
CVE-2024-0538	10
Ransomware and Breach Intelligence Key Findings	12
LockBit Ransomware Gang Most Active	12
Breach Disclosure: JoinPiggy	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

[Flash Report - Critical Microsoft SharePoint Vulnerability Actively Exploited](#)

In this flash report, ZeroFox researchers report on a critical severity Microsoft SharePoint privilege escalation vulnerability currently being actively exploited in the wild.

[Flash Report - Disclosure of Critical Atlassian Confluence Vulnerability](#)

In this flash report, ZeroFox researchers provide updates on a critical Atlassian Confluence vulnerability which involves a critical remote code execution flaw in Confluence Data Center and Confluence Server.

[Flash Report - Mass Access Sale to Retail eCommerce System](#)

In this flash report, ZeroFox researchers report on the announcement of the sale of the source code, business operations data, and documentation of an unspecified eCommerce Content Management System (CMS) services vendor.

[Flash Report - Citrix Vulnerabilities Continue to Be Exploited](#)

In this flash report, ZeroFox researchers report on the ongoing exploitation of three separate Citrix vulnerabilities relating to Netscaler Application Delivery Controller (ADC) and Gateway appliances.

[Flash Report - Dark Web Actors Promoting Maritime Data](#)

In this flash report, ZeroFox researchers report on observations that threat actors are selling data related to maritime vessels and their infrastructure, which comes on the heels of commercial vessels being targeted in the Red Sea during the Israel-Hamas War.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

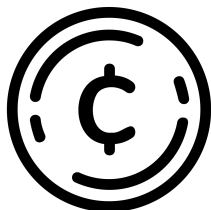
[U.S. Court Docs Expose Fake Antivirus Renewal Phishing Tactics](#)

What happened: U.S. Secret Service uncovered threat actors using fake antivirus renewal subscription notifications to gain access to a victim's PC and bank account and scam victims of USD 34,000. The threat actors redirected the victim to a site where they were tricked into downloading remote access software on their computer, among other actions, including entering their payment information. The threat actors now face charges for wire fraud, involvement in a phishing scam, money laundering, and bank fraud, among other transgressions.



- **What this means:** The tactics displayed by the scammers were not new – these types of scams have going on for years. However, authorities have indicated that they have recently observed a significant increase in the volume of these scams.

[Hacker Spins Up 1 Million Virtual Servers to Illegally Mine Crypto](#)



What happened: A cybercriminal in Ukraine orchestrated a large-scale cryptojacking attack by using hacked accounts to create 1 million virtual servers dedicated to mining approximately USD 2 million worth of cryptocurrency. The attack involved the exploitation of compromised accounts to gain administrative privileges. The suspect had reportedly been active since 2021 and used TON cryptocurrency wallets for illegal transactions.

- **What this means:** The attack wore out the CPU and GPU performance of compromised organizations, leading to increased power costs and other damages. The arrested individual now faces criminal charges for unauthorized interference in accordance with the Criminal Code of Ukraine.

[Chrome Addresses Four Vulnerabilities Including an Actively Exploited Zero-Day](#)

What happened: Google Chrome recently addressed four vulnerabilities, including an actively exploited zero-day flaw observed in the wild through now published updates. CVE-2024-0519 is a high-severity vulnerability that



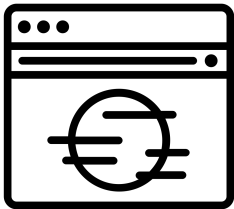
allows threat actors to exploit its out-of-bounds memory access in the V8 JavaScript and WebAssembly engine to trigger a crash.

- **What this means:** By exploiting out-of-bounds memory access, an attacker could obtain secret values, including memory addresses. This could allow them to bypass security measures like address space layout randomization (ASLR), enhancing the likelihood of exploiting another vulnerability for unauthorized code execution instead of just causing a denial of service.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

'MyFlaw' Zero-Day RCE Vulnerability Uncovered in Opera Browser



What happened: On January 15, Guardio Labs disclosed that it discovered a critical zero-day Remote Code Execution (RCE) vulnerability in Opera web browser for Microsoft Windows and Apple macOS that would allow for the execution of malicious files on the operating systems. The now patched vulnerability, dubbed 'MyFlaw' due to its exploitation of Opera's browser-to-mobile file and message-sharing extension My Flow, granted potential threat actors the ability to bypass the browser's sandbox and subsequently create a fraudulent extension that imitated a mobile device to pair with the target computer. Once the fraudulent extension is downloaded, an encrypted payload could be sent via a JavaScript file and executed once the user clicks on the screen. Evidence to suggest active exploitation of this vulnerability in the wild has not yet been found. Additionally, while ZeroFox has not yet observed any dark web chatter from threat actors regarding this vulnerability, it will continue to monitor for such.

- **What this means:** The rising number of vectors through which threat actors can attack web browser infrastructure, particularly as browsers increasingly include more advanced features, highlights the balance that is needed between employing ever-evolving technology for user convenience and maintaining cyber security best practices. Additionally, this type of vulnerability, which requires minimal victim interaction to successfully compromise a system, is highly sought after among threat actors. While there is no documented evidence of the exploitation of this vulnerability in the wild, it does not mean it has not occurred. My Flow users should continue to practice caution, and security entities should continue to monitor for relevant threat actor activity.

Threat Actor "IntelBroker" Leaked Data from UK-Based Auto Manufacturer Vauxhall Motors

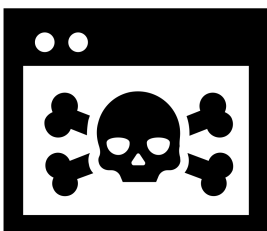
What happened: On January 17, 2024, threat actor IntelBroker claimed to have leaked a set of internal data associated with Vauxhall Motors, a United Kingdom (UK)-based automobile manufacturing and distribution company. The dataset, leaked on the English-language dark web forum "BreachedForums," was derived from the actor's access to user IDs, site IDs, call dates, and phone numbers derived from approximately 5.5



million call logs between Vauxhall Motors and their customers. It is unclear how IntelBroker accessed the internal information or if the actor released the complete set of data at their disposal..

- **What this means:** ZeroFox assesses IntelBroker to be a well-regarded and established threat actor with a history of releasing sensitive information. IntelBroker, who claims to be located in Serbia, was first identified on October 22, 2022, on BreachedForums where they claimed to be a developer of Endurance Ransomware. Endurance Ransomware was subsequently seized in mid-2023, but IntelBroker has maintained an active presence on multiple dark web forums where they primarily operate as an initial access and data broker. IntelBroker has targeted a broad cross-section of sectors and geographic locations, highlighting the threat posed by this and other access brokers.

Actor KernelMode Advertised Malware for Sale Designed to Kill Most AV and EDR Products



What happened: On January 17, 2024, the actor KernelMode advertised a malware for sale that can kill most antivirus and EDR products on the Exploit forum. The actor claimed the malware was successfully tested on Microsoft Windows 7-11 operating systems to terminate processes for several AV and EDR products. The malware was priced at USD 5000 a month with a limit of five clients.

- **What this means:** As KernelMode has minimal postings on this forum, it is unknown if their claim is credible. However, if a couple of actors purchase this malware and successfully terminate AV and EDR products on target machines, it will give them an advantage. It will make getting past a company's defenses easier to launch their attacks. If the actors are successful in their attacks, KernelMode may expand their limitation of clients as they would have more clients to vouch for them.

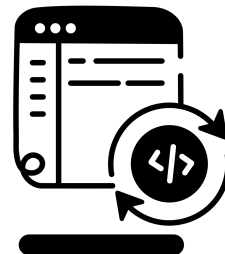
Exploit and Vulnerability Intelligence

| Exploit and Vulnerability Intelligence Key Findings

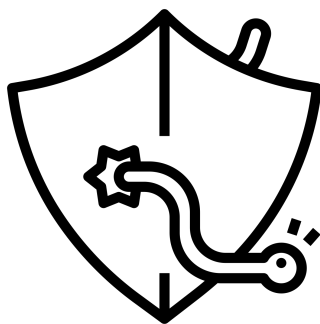
CVE-2024-0552

What happened: Intuit inc. SmartRobot's web framework has a remote code execution vulnerability classified as **CRITICAL**.

- **What this means:** An unauthorized remote attacker can exploit this vulnerability to execute arbitrary commands on the remote server.



CVE-2024-0538



What happened: A vulnerability has been found in Tenda W9 1.0.0.7(4456) and is classified as **CRITICAL**. This vulnerability affects the function `formQosManage_auto` of the component `httpd`. The manipulation of the argument `ssidIndex` leads to a stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250708.

- **What this means:** A public exploit for this vulnerability is known, and at this time, no known fix exists.

| Ransomware and Breach Intelligence |

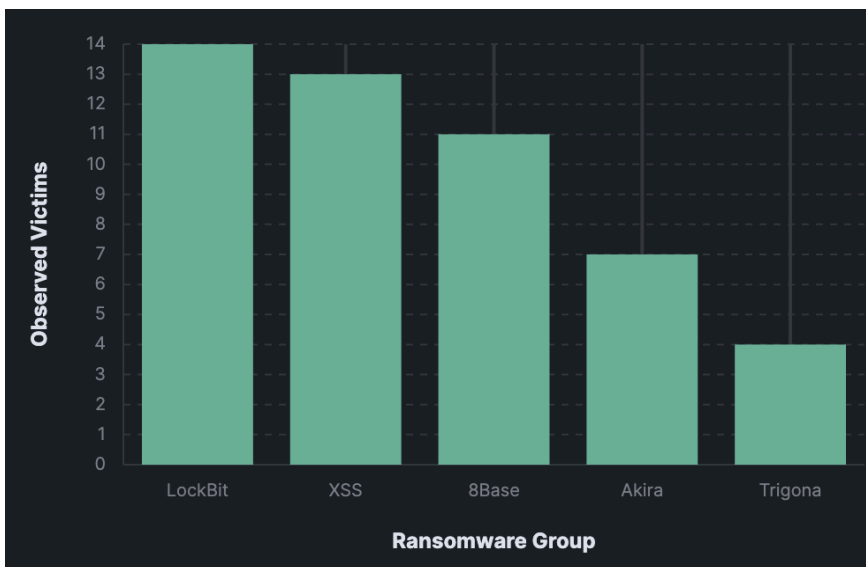
Ransomware and Breach Intelligence Key Findings

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 14 victims identified during that time. The LockBit group has targeted organizations in the legal, manufacturing, retail, and government sectors, along with other industries located in the United States and Europe.

➤ **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: JoinPiggy



What happened: JoinPiggy, a U.S.-based automatic coupon and cashback application, had 1,546,415 email addresses shared on a deep web platform. Other notable data fields observed in this package include name, physical address, phone number, gender, 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:** Impacted users should update their passwords immediately and remain vigilant against phishing attempts.

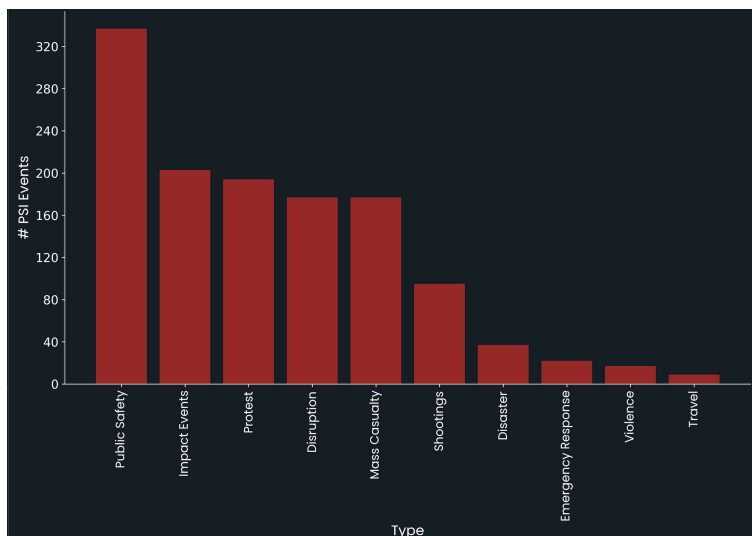
Physical and Geopolitical Intelligence

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

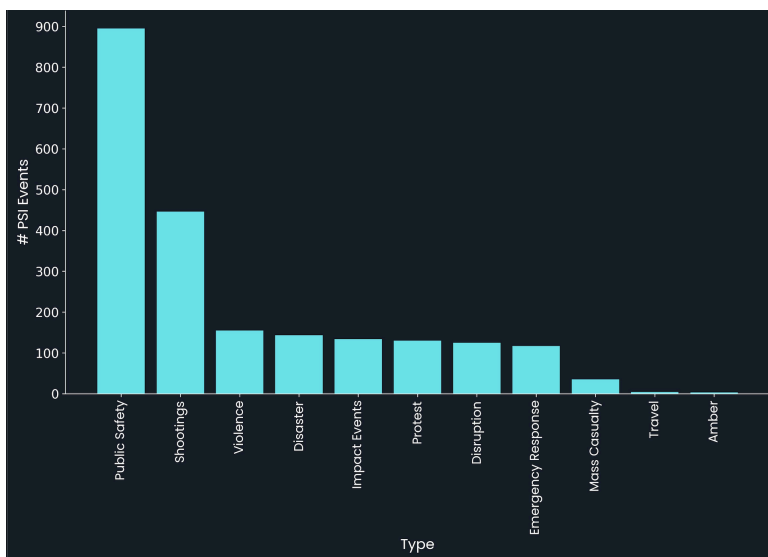
What happened: ZeroFox observed over 300 public safety issues in the past week worldwide, with these events involving some sort of considerable law enforcement presence. Countries in the Middle East impacted by the Israel-Hamas War unsurprisingly had the most physical security events occurring, along with significant protest activity taking place in the United Kingdom.

- **What this means:** Continued escalations in the Israel-Hamas 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 California and Maryland, with protest activity most commonly occurring in New York, Texas, and Florida.

- **What this means:** There was an observed 58 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%