



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

November 6, 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 3, 2023*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 Cyber Intelligence Key Findings	3
Hackers Use Citrix Bleed Flaw in Attacks on Government Networks Worldwide	3
Atlassian Warns of New Critical Confluence Vulnerability Threatening Data Loss	3
BlackCat Ransomware Claims Breach of Healthcare Giant Henry Schein	4
 Deep and Dark Web Intelligence Key Findings	6
RansomedSupport Ransomware Project Being Sold	6
Boeing Listed on LockBit Ransomware Group Leak Site	6
European Travel Sector Targeted by Iranian APT Group Watering Hole Attacks	7
 Exploit and Vulnerability Intelligence Key Findings	9
CVE-2023-45018	9
CVE-2023-2979	9
 Ransomware and Breach Intelligence Key Findings	11
8Base and Play Ransomware Gangs Most Active	11
Zipmex Breach Disclosure	11
 Appendix A: Traffic Light Protocol for Information Dissemination	12
 Appendix B: ZeroFox Intelligence Probability Scale	13

| Cyber Intelligence |

| Cyber Intelligence Key Findings

Hackers Use Citrix Bleed Flaw in Attacks on Government Networks Worldwide

What happened: Security researchers have observed at least four ongoing campaigns exploiting “Citrix Bleed,” a critical severity flaw (CVE-2023-4966) affecting Citrix NetScaler ADC and NetScaler Gateway (which was disclosed on October 10, 2023). While these attacks have been significantly stealthy and left behind sparse forensic evidence, researchers have observed post-exploitation activity that indicates credential theft and lateral movement. Tens of thousands of exploited servers have been reportedly observed, with attacks originating from over a hundred individual IP addresses.



Source: [hXXps://www.citrix\[.\]com/](https://www.citrix.com/)

Moreover, ongoing attacks would require a full incident response, as deploying the available patches will not secure already breached systems.

- **What this means:** At this time, organizations should consider all NetScaler devices to be potentially vulnerable, and any unpatched devices should be patched immediately. In addition, credentials should be updated to ensure that previous ones are invalidated, and devices should be analyzed for potential compromise.

Atlassian Warns of New Critical Confluence Vulnerability Threatening Data Loss

What happened: Atlassian has warned users of a critical security flaw (CVE-2023-22518; CVSS score of 9.1) in Confluence Data Center and Server that could lead to significant data loss in the event of a successful attack. Atlassian stated that the “improper authorization vulnerability” would not affect confidentiality as an attacker cannot exfiltrate any instance data.



[hXXps://www.atlassian\[.\]com/](https://www.atlassian.com/)

- **What this means:** Customers should immediately secure their instances and upgrade to the latest (patched) versions; Atlassian recommends disconnecting publicly accessible instances until the patch has been applied. Atlassian Cloud sites are not affected by the issue.

BlackCat Ransomware Claims Breach of Healthcare Giant Henry Schein

What happened: Multinational healthcare solutions provider Henry Schein has reportedly suffered a ransomware attack that forced it to take some systems offline and disrupted business operations. Russia-linked BlackCat/ALPHV ransomware group listed Henry Schein on its dark web leak site and claimed to have stolen 35 TB of sensitive files (including payroll data and shareholder information) after breaching the company's networks. In a cybersecurity advisory earlier this year, the U.S. Health Sector Cybersecurity Coordination Center (H3C) had named ALPHV/ as one of the most prolific groups targeting critical infrastructure, including healthcare, in the past year.



hXXps://www.henryschein[.]com/

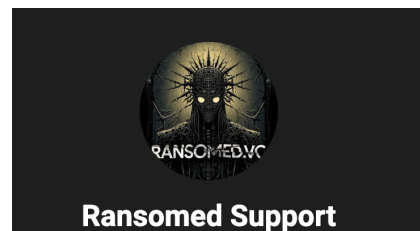
- **What this means:** This follows the high-profile breach of MGM Resorts, which BlackCat affiliate Scattered Spider claimed responsibility for, and also appears to be the first publicly disclosed instance of a medtech company falling victim to a ransomware attack since the SEC launched new regulations requiring publicly traded companies to promptly disclose cybersecurity incidents that have a material impact.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

RansomedSupport Ransomware Project Being Sold

What happened: The actor RansomedSupport announced that they were selling their ransomware project Ransomed[.]vc. The actor claimed they were selling because they did not want to be monitored by federal agencies but wanted the project to continue. The package includes domains for the project, the ransomware builder, source code, administrative panel access, access to affiliate groups, access to social media accounts, VPN access to 11 different companies internal networks, and stolen databases impacting 37 companies that have not been released. There is no price listed, as the actor suggested that buyers contact them on Telegram.



Source: ZeroFox Internal Collections

- **What this means:** This ransomware project was fairly new, having launched in August 2023 and released 44 victims in September 2023, then launched their own forum as well. As the actor is selling databases that have yet to be released and actors continuously want to start their own ransomware group, there will likely be interest in buying from lower-level actors since there is already a foundation built. There is a chance that another ransomware group will also want to buy this to obtain the unreleased databases and affiliate groups, as well as have one less ransomware competitor.

Boeing Listed on LockBit Ransomware Group Leak Site

What happened: The LockBit ransomware group listed Boeing, a U.S. aerospace and defense company, on their data leak site. The group claimed to have exfiltrated a large amount of sensitive data, and Boeing has since confirmed a cyber incident occurred since the post was made but has not specified if it is correlated to LockBit's alleged ransomware attack. The listing on the ransomware data leak site has also now been deleted which may mean the claim was not legitimate or that the company has decided to partake in negotiations for now.



hXXps://www.boeing[.]com/

- **What this means:** LockBit ransomware has been the most prolific ransomware group since the Conti shutdown in May 2022. The targeting of Boeing shows that ransomware groups are willing to target critical infrastructure sectors and that they are not solely focused on small to medium-sized businesses. It is likely that ransomware groups will continue to target larger companies due to the higher payout they could receive for selling the data or in ransom payments. The fact that there was a cyber incident at Boeing further highlights

the importance of keeping systems up-to-date, patching vulnerabilities, and practicing strong cyber hygiene across the board to lessen the chance of an attacker gaining access.

European Travel Sector Targeted by Iranian APT Group Watering Hole Attacks

What happened: An Iranian APT group targeted the European travel sector with a series of watering hole attacks. Beginning in 2022 and continuing through 2023, Tortoiseshell deployed a malware termed IMAPLoader to conduct credential harvesting and follow-on attacks against European targets. Tortoiseshell, an Iranian Islamic Republican Guard Corps (IRGC)-aligned APT group, has a history of targeting logistics and transportation-related entities in Israel and elsewhere.

- **What this means:** Iranian government cyber actors frequently gather PII to aid in their counterintelligence and targeting mission. This mission is likely a primary goal in the campaign above and puts at risk any traveler who has used those companies. Iranian APT groups target multiple sectors upstream from the government or military, putting those sectors at risk from Iranian cyber activity.



[hXXps://thehackernews\[.\]com/2023/10/iranian-group-tortoiseshell-launches.html](https://thehackernews.com/2023/10/iranian-group-tortoiseshell-launches.html)

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

CVE-2023-45018

What happened: One of the most critical Common Vulnerabilities and Exposure (CVE) identified this week was CVE-2023-45018, which is ranked **CRITICAL** and involves the Online Bus Booking System v1.0 being vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the includes/login.php resource does not validate the characters received, and they are sent unfiltered to the database.

- **What this means:** Currently, there is no available exploit for CVE-2023-45018; however, technical details of the vulnerability are known.

CVE-2023-2979

What happened: Another **CRITICAL** CVE identified this week was a vulnerability that has been found in Abstrium Pydio Cells 4.2.0. This affects an unknown part of the component User Creation Handler. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-230211.

- **What this means:** The exploit has been disclosed to the public and may be used. Upgrading to version 4.2.1 can address this issue.

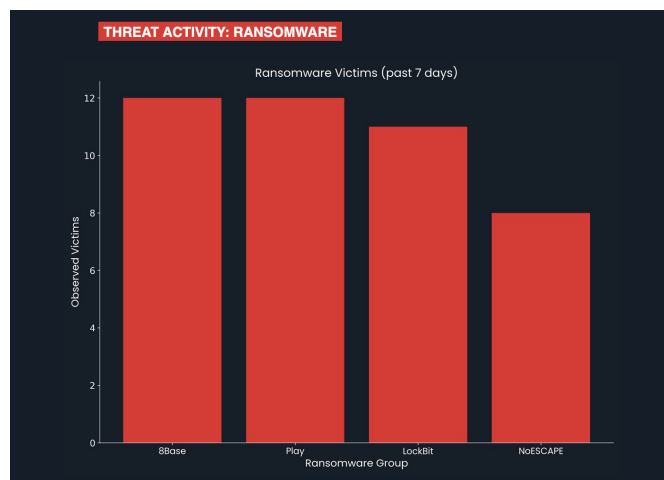
Ransomware and Breach Intelligence

| Ransomware and Breach Intelligence Key Findings

8Base and Play Ransomware Gangs Most Active

What happened: ZeroFox Intelligence has observed the 8Base and Play ransomware gangs as the most active over the past week. 8Base, identified as early as May 2023, has victims who are predominantly small-medium size businesses that are dispersed geographically and are primarily from the finance, manufacturing, and technology sectors. The Play ransomware group also set new records for the highest number of victims in a given month earlier this year.

- **What this means:** Newly-formed ransomware groups such as 8Base and Play are expected to demonstrate proficiency faster than ever before due to a number of proliferating as-a-service tools that continue to lower entry barriers to would-be threat actors.



Source: ZeroFox Internal Collections

Zipmex Breach Disclosure

What happened: Zipmex, a Singapore-based digital assets exchange platform, in which 1,458,606 email addresses were exposed and subsequently shared on a deep web platform. No passwords were found in this breach. Other notable data fields observed in this package include browser user agent, date of birth, name, phone number, physical address, 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.

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%