



**ZEROFOX<sup>®</sup>**

*Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**March 18, 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 March 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# | Weekly Intelligence Brief |

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| <b>  This Week's ZeroFox Intelligence Reports</b>                               | <b>2</b>  |
| ZeroFox Intelligence Brief – Social Engineering Series: MFA Bypass via Phishing | 2         |
| ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 6           | 2         |
| <b>  Cyber Intelligence Key Findings</b>                                        | <b>4</b>  |
| French Government Targeted in Denial-of-Service Attacks by Pro-Russian Hackers  | 4         |
| Fortinet Warns of Severe SQLi Vulnerability in FortiClientEMS Software          | 4         |
| New Banking Trojan CHAVECLOAK Targets Brazilian Users via Phishing Tactics      | 5         |
| <b>  Deep and Dark Web Intelligence Key Findings</b>                            | <b>7</b>  |
| BlackByte Ransomware Group Emerges with New Onion Site                          | 7         |
| Threat Actor Claims Cyberattack Against NATO Military Infrastructure            | 7         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                    | <b>10</b> |
| CVE-2024-21334                                                                  | 10        |
| CVE-2024-21899                                                                  | 10        |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                        | <b>12</b> |
| BianLian Targets Healthcare Facilities                                          | 12        |
| Nissan Oceania Breach Confirmed                                                 | 12        |
| <b>  Physical and Geopolitical Intelligence Key Findings</b>                    | <b>15</b> |
| Physical Security Intelligence: Global                                          | 15        |
| Physical Security Intelligence: United States                                   | 15        |
| <b>  Appendix A: Traffic Light Protocol for Information Dissemination</b>       | <b>18</b> |
| <b>  Appendix B: ZeroFox Intelligence Probability Scale</b>                     | <b>19</b> |

## **| This Week's ZeroFox Intelligence Reports**

### **[ZeroFox Intelligence Brief – Social Engineering Series: MFA Bypass via Phishing](#)**

Multi-factor authentication (MFA) uptake has been on a consistent upward trajectory since its inception; today its use is widely expected, considered best practice, and a part of basic cybersecurity hygiene. Despite improving security, some MFA protocols are still susceptible to bypass or circumvention by threat actors seeking to gain illicit network access. This type of activity is almost certainly on an upward trajectory as of 2024, as threat actors continuously evolve their techniques, tactics, and procedures (TTPs).

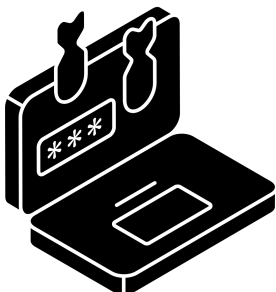
### **[ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 6](#)**

Nearly four years after its discovery, CVE-2020-1472 (ZeroLogon) is almost certainly still being exploited by malicious actors. On March 8, 2024, positive-reputation Russian-speaking threat actor “investimer” announced in deep and dark web (DDW) forum exploit[.]in that they are selling X accounts that include either USD 500 or EUR 500, which can be spent on promotional ads. ZeroFox has observed several new services specializing in the sale of illicitly-obtained social media accounts in 2024, indicating a very likely chance that they are growing in popularity. On March 3, 2024, hacktivist organization Handala boasted of successfully infiltrating the servers of DRS Rada Technologies (RADA), an Israeli defense company that manufactures radar solutions and legacy avionics systems, on dark web forum RAMP.

# | Cyber Intelligence |

## | Cyber Intelligence Key Findings

### French Government Targeted in Denial-of-Service Attacks by Pro-Russian Hackers



**What happened:** On March 11, the French government said that cyberattacks of “unprecedented intensity” had targeted several of its services, prompting it to activate a special crisis center to restore online services. A French official noted that it was a series of distributed denial-of-service (DDoS) attacks. A statement from Prime Minister Gabriel Attal’s office added that the attacks had impacted multiple French state bodies but that the government had been able to contain

the impact of the cyberattacks and restore access to its targeted websites.

- **What this means:** The incident comes after the Prime Minister’s office issued a warning last week regarding the Paris Olympics and the upcoming summer European Parliament elections being potential targets for cyberattacks. On March 11, ZeroFox observed threat actor group Anonymous Sudan take responsibility for [targeting](#) the French government in denial-of-service attacks, naming the French Interministerial Directorate of Digital Affairs as a victim.

### Fortinet Warns of Severe SQLi Vulnerability in FortiClientEMS Software

**What happened:** Fortinet has issued a warning about a critical security vulnerability affecting its FortiClientEMS software, potentially allowing attackers to undertake code execution on affected systems. The flaw (CVE-2023-48788) has a CVSS rating of 9.3 out of 10 and impacts several versions of FortiClientEMS. The vulnerability in FortiClientEMS involves an SQL injection flaw, which is categorized under CWE-89.

- **What this means:** CVE-2023-48788 allows attackers to execute unauthorized code or commands by exploiting special elements within SQL commands. It can be exploited by unauthenticated attackers via carefully crafted requests. While there is no evidence of active exploitation of these vulnerabilities yet, users are still strongly advised to promptly apply the updates to safeguard their systems.



## New Banking Trojan CHAVECLOAK Targets Brazilian Users via Phishing Tactics



**What happened:** A new banking trojan called CHAVECLOAK is targeting users in Brazil through phishing emails that contain PDF attachments. The phishing emails use DocuSign lures related to contracts to trick users into opening the PDF files, which contain a button to read and sign the documents. However, clicking the button triggers the retrieval of an installer file from a shortened remote link, which installs the CHAVECLOAK trojan on victims' systems.

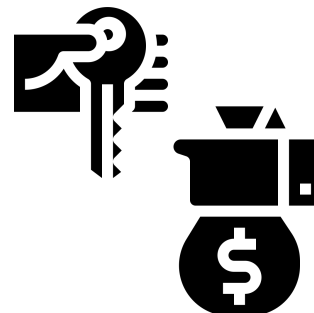
➤ **What this means:** This malware establishes a connection with a command-and-control (C2) server to exfiltrate different types of financial information from the victims to servers controlled by the attackers.

# | Deep and Dark Web Intelligence |

## | Deep and Dark Web Intelligence Key Findings

### [BlackByte Ransomware Group Emerges with New Onion Site](#)

**What happened:** On March 13, 2024, ZeroFox observed a new onion site for BlackByte ransomware. Reportedly, the group has emerged after five months of silence with a fresh look and a new download service in the data company list section. Additionally, on March 13, 2024, BlackByte appeared to have targeted an U.S.-based utility company.



- **What this means:** After five months of inactivity, BlackByte ransomware group has changed its appearance (they are now using shades of gray and a new font) and is offering a new download service in the data company list section. In addition to resurfacing, BlackByte also allegedly targeted Encina Wastewater Authority on March 13, 2024, exfiltrating data that includes invoices, contracts, payroll records, project details, HR documents, and employees' personal details. While BlackByte targets a multitude of countries, ZeroFox assesses the ransomware group will continue to primarily target the United States.

### [Threat Actor Claims Cyberattack Against NATO Military Infrastructure](#)



**What happened:** On March 11, 2024, threat actor "aaron\_bushnell" claimed to have carried out a cyberattack against the military infrastructure of NATO on predominantly English-language dark web forum BreachForums. The post stated that multiple hackers were involved in this attack, calling them the "Aaron Bushnell hackers" and claiming they are motivated by the Palestinian cause. These hackers allegedly stole 5GB of data, including 4,000 sensitive documents containing military maps, contracts, and information on employees and military personnel. The actor is offering to sell the data for USD 20,000 and claiming all proceeds will go towards "humanitarian purposes" in Palestine. The actor did not disclose the source or the methods of the breach but did allege to have made a previous sale of the same nature on an unidentified date.

- **What this means:** The February 25 self-immolation of U.S. airman Aaron Bushnell outside the Israeli embassy in Washington, DC, in response to U.S. diplomatic and military actions surrounding the ongoing Israel-Hamas war has garnered substantial media attention and

fueled extensive public discord online. However, this is the first instance tracked by ZeroFox of a dark web threat actor leveraging the incident to conduct cyberattacks in support of Palestine. While nefarious cyber activity in support of a pro-Palestine agenda is far from unusual, the targeting of NATO in response to this specific conflict has not been widely observed. With this unusual shift in targeting, it is possible that additional pro-Palestinian threat actors may follow suit and realign their focus on other Western entities involved in the military support of Israel. ZeroFox will continue to monitor for any such activity as the conflict continues.

## **Anonymous Sudan Claims Attack Against State of Alabama Infrastructure and Law Enforcement Agencies**

**What happened:** On March 13, 2024, hacktivist collective Anonymous Sudan claimed to have executed a “massive” cyberattack against the infrastructure of the U.S. state of Alabama. The group reportedly targeted the Alabama Law Enforcement Agency, the State of Alabama Office of Information Technology, and the Alabama Supercomputer Authority. Anonymous Sudan claimed to have carried out the attacks in response to the United States’ support of Israel in its conflict with Hamas. Additionally, the group claimed the attack was meant to draw attention to “the dire situation in Sudan.”



- **What this means:** Anonymous Sudan is a hacktivist collective made up of disparate groups and individuals with common enemies. This attack was reportedly carried out by distributed denial-of-service (DDoS) infrastructure operated by “@infrashutdown”, a group involved in recent attacks against other Western and Israeli infrastructure. Each of the institutions targeted in this attack is a state-level executive agency; the attack against the IT infrastructure entity is noteworthy, as it was likely selected due to its perceived disparate impact on state communications. ZeroFox assesses that Anonymous Sudan will almost certainly continue to carry out similar attacks against Western and Western-aligned nations, regardless of the status of the conflict in the Middle East.

# | Exploit and Vulnerability Intelligence |

## | Exploit and Vulnerability Intelligence Key Findings

### CVE-2024-21334



**What happened:** Microsoft's vulnerability (CVE-2024-21334) concerns a weakness in Open Management Infrastructure (OMI), a Linux-based cloud infrastructure in Microsoft Azure. This **CRITICAL** vulnerability has a CVSS base score of 9.8. Microsoft has graded it as "important" in accordance with its severity scale and has stated that it is less likely to be exploited.

➤ **What this means:** Malicious actors can exploit CVE-2024-21334 to access OMI instances from the internet without authentication and send specially crafted requests to gain remote code execution privileges on the host device. Customers running affected versions of System Center Operations Manager (SCOM) have been advised to update to OMI version 1.8.1-0 in order to mitigate the risks associated with this vulnerability.

### CVE-2024-21899

**What happened:** CVE-2024-21899 is an improper authentication vulnerability detected in several QNAP operating system versions and QTS, QuTS hero, and QuTScloud products. It exposes network-attached storage (NAS) devices to unauthenticated access. This **CRITICAL** vulnerability has been assigned a CVSS score of 9.8.

- **What this means:** Exploitation of CVE-2024-21899 could lead threat actors to gain unauthorized access to sensitive information or disrupt system operations, making it a notable risk. QNAP has already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later; QTS 4.5.4.2627 build 20231225 and later; QuTS hero h5.1.3.2578 build 20231110 and later; QuTS hero h4.5.4.2626 build 20231225 and later; and QuTScloud c5.1.5.2651 and later.



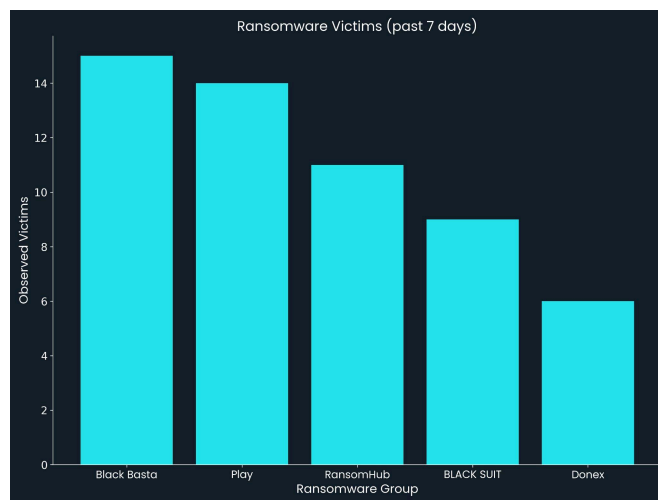
# Ransomware and Breach Intelligence

## Ransomware and Breach Intelligence Key Findings

### BianLian Targets Healthcare Facilities

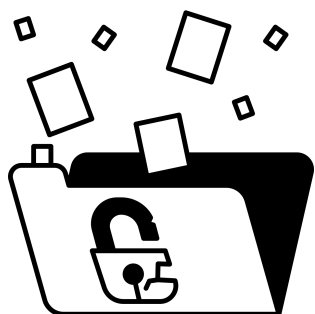
**What happened:** BlackBasta and Play ransomware groups have been the most active groups in the past week. Additionally, ZeroFox has observed the BianLian group targeting several victims in this same period. The targets have mostly been in North America, and two (Lindsay Municipal Hospital and New York Home Healthcare) are in the healthcare industry. BianLian has also been exploiting known bugs in JetBrains' TeamCity software development platform to gain initial access to victims' systems and eventually conduct ransomware attacks.

**What this means:** Cybersecurity analysts have observed BianLian attempting to install various malicious tools, including a newly developed PowerShell backdoor, after gaining access to a vulnerable system's TeamCity server. Moreover, BianLian's targeting of two healthcare facilities is likely connected to a larger campaign aimed at hospitals across the United States. Last month, UnitedHealth Group (UHG), a major U.S. health insurance giant, confirmed that its subsidiary Change Healthcare suffered a cyberattack, likely by government-backed hackers.



Source: ZeroFox Internal Collections

### Nissan Oceania Breach Confirmed



**What happened:** Nissan Oceania has provided an update on the December 2023 data breach, stating it has impacted approximately 100,000 individuals. The list of the affected individuals includes some of Nissan's customers, dealers, and a few current and former employees. Ten percent of the list had at least one form of government ID stolen. The remaining 90 percent lost other forms of personal information, such as copies of loan-related transaction statements, employment and salary information, and more general information like dates of birth.

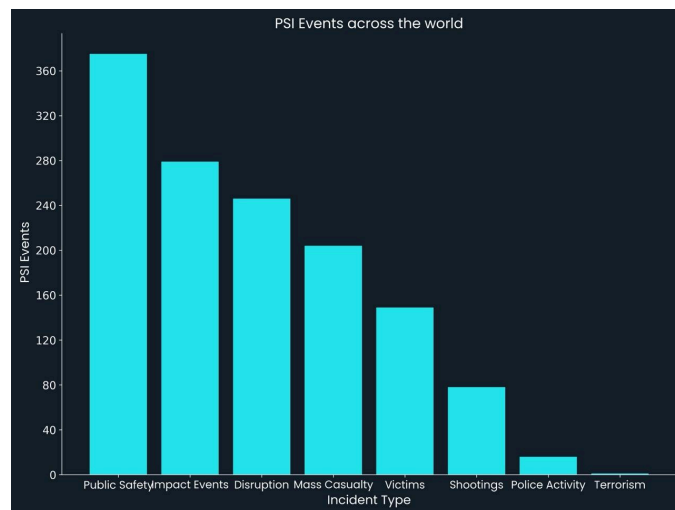
- **What this means:** Nissan has provided mitigation measures, including access to Australia and New Zealand's national identity and cyber support community service, free credit monitoring, and reimbursement in cases where government ID replacement is recommended by the relevant issuing authority.

# | Physical and Geopolitical Intelligence |

## | Physical and Geopolitical Intelligence Key Findings

### Physical Security Intelligence: Global

**What happened:** U.S. and European warships have shot down at least 30 Houthi drones following the largest Red Sea attack launched by the rebel group so far. In Haiti, Kenyan officials paused the deployment of 1,000 police officers, which was initially agreed upon between the two countries to help Haiti curb widespread gang violence, after Prime Minister Ariel Henry announced his resignation following the formation of a transitional council. On March 8, Indian authorities announced the discovery of a human-trafficking ring tricking young men into fighting in Ukraine for the Russian military. About 35 Indian men have so far been lured to Russia with promises of high-paying jobs or educational opportunities only to be pressed into combat roles as part of Russia's invasion.

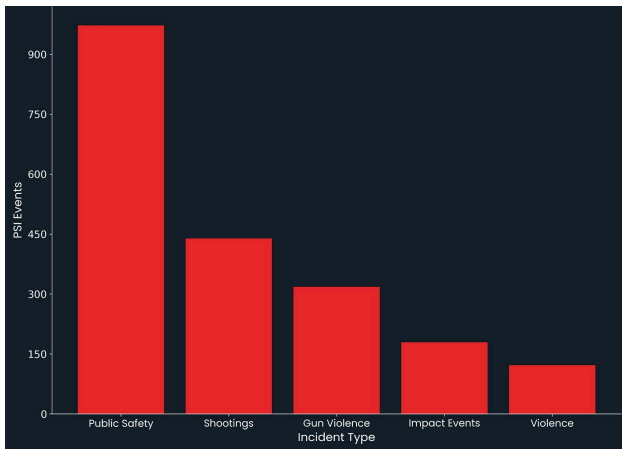


Source: ZeroFox Internal Collections

- **What this means:** Attacks by Houthi rebels have resulted in the sinking of one cargo ship and the deaths of at least three commercial sailors. Meanwhile in the Caribbean, violence has ensued throughout Haiti. Two major gangs, G9 Family (led by Jimmy "Barbecue" Cherizier) and GPep (led by Gabriel Jean-Pierre), are competing for territories around Port-Au-Prince. The gang violence has resulted in mass displacement of residents, scarcity in essential commodities, and closures of airports and major roads. In the context of the Russia-Ukraine war, Indian authorities conducted raids in seven cities to unravel the Russian human-trafficking network in India and have arrested multiple individuals in connection with the investigation.

### Physical Security Intelligence: United States

**What happened:** According to ZeroFox intelligence, in the past week, California reported the highest number of public safety incidents, while Illinois saw the highest number of shooting incidents. A mass shooting at a private party in Arkansas left at least four wounded and two dead. Officers have reported that the suspect is also dead, although the cause of death remains unknown. On March 10, authorities reported a small plane crashed into woods near Virginia's western border, bursting into flames and killing all five people onboard. The towns of Winchester and Selma in Indiana experienced a tornado on March 14 that left several people injured.



Source: ZeroFox Internal Collections

➤ **What this means:** The Arkansas shooting occurred during a private party at an abandoned building. Officials have described it as a domestic incident, stating that the shooter knew the victims who were killed and one of the victims who was injured. The police officers investigating the Virginia plane crash said that the plane had been “short on its approach to the runway, struck the trees and then the hillside.” The Indiana State Police Superintendent has said that some homes in the two towns affected by the tornado have been destroyed. No deaths have been reported.

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? | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> 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?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |