



*Weekly Intelligence Brief*

Classification: TLP:GREEN

April 15, 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 April 12, 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: Business Email Compromise                   | 2         |
| ZeroFox Intelligence Flash Report – Cybersecurity Risk Ahead of South Korea Elections               | 2         |
| <b>  Cyber Intelligence Key Findings</b>                                                            | <b>4</b>  |
| Social Engineering Attacks Targeting IT Help Desks in the Health Sector                             | 4         |
| U.S. Government Consulting Firm Discloses Data Breach Exposing over 340,000 Social Security Numbers | 4         |
| GHC–SCW Ransomware Attack Affects over 533,000 People                                               | 5         |
| <b>  Deep and Dark Web Intelligence Key Findings</b>                                                | <b>7</b>  |
| Untested Threat Actor Advertised Zero-Day Exploit on Dark Web Forums                                | 7         |
| Actor Advertised Access to Snapchat Employee Accounts                                               | 7         |
| Actor “USDoD” Leaked Data Allegedly from a U.S. Federal Agency                                      | 8         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                                        | <b>10</b> |
| CVE-2023-45590                                                                                      | 10        |
| CVE-2024-24576                                                                                      | 10        |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                                            | <b>13</b> |
| Change Healthcare Asked to Pay Second Ransom                                                        | 13        |
| Breach Intelligence: Sisense Breach Endangers Critical Infrastructure                               | 13        |
| <b>  Physical and Geopolitical Intelligence  </b>                                                   | <b>15</b> |
| <b>  Physical and Geopolitical Intelligence Key Findings</b>                                        | <b>16</b> |
| Physical Security Intelligence: Global                                                              | 16        |
| Physical Security Intelligence: United States                                                       | 17        |
| <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: Business Email Compromise](#)**

ZeroFox's Social Engineering series breaks down aspects of the threat into digestible reports and outlines defensive actions that can be taken to combat it. Part Five of this series takes a deep dive into Business Email Compromise (BEC), why and how threat actors do it, and how the threat can best be mitigated.

### **[ZeroFox Intelligence Flash Report – Cybersecurity Risk Ahead of South Korea Elections](#)**

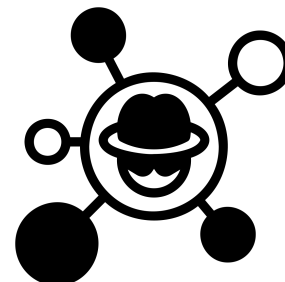
ZeroFox has not identified any evidence of a coordinated cyber campaign targeting South Korea's National Assembly elections. ZeroFox anticipates that threats to South Korean firms will continue irrespective of the elections, likely due to the country's growing ties with the United States and Japan. South Korea has developed closer economic ties with the United States to restrict sales of advanced technology to China, while it has deepened ties with Japan over shared concerns about the military threat posed by China and North Korea. The North Korean security threat is largely a secondary concern for South Korean voters, who are more focused on domestic issues such as the cost of living, low fertility rates, and party corruption. The likelihood of a positive electoral outcome for South Korea's adversaries is possibly behind the lack of coordinated nation-state cyber campaigns targeting the April 10 elections.

# | Cyber Intelligence |

## Cyber Intelligence Key Findings

### Social Engineering Attacks Targeting IT Help Desks in the Health Sector

**What happened:** Reports confirm that IT help desks in the health sector are the recent target of threat actors who seek to gain unauthorized access to organizations through advanced social engineering tactics. Threat actors first approach IT help desks with phone calls from the target organization's local area codes, posing as employees in financial roles such as revenue cycle or administrator positions. To further strengthen their disguise, the threat actors mimic high-level personnel through domain spoofing, amplifying the risk. Claiming their phone is broken and they are unable to receive multi-factor authentication (MFA) tokens, the threat actors convince the help desk to enroll a new device in MFA, thus gaining access to corporate resources.



- **What this means:** In September 2023, a high-profile social engineering cyberattack conducted by the threat actor Scattered Spider (UNC3944) hit the hospitality and entertainment industry, deploying ALPHV ransomware. Recent health industry campaigns, including the September 2023 incident, exploit spear phishing voice techniques (such as impersonating employees) to gain access. Threat actors have been increasingly using AI voice-cloning for social engineering, complicating remote identity verification. One of the mitigations noted in the report involves healthcare organizations conducting more thorough verification of callers when registering a new device and password resets. Other recommended steps include monitoring Automated Clearing House (ACH changes) and user training.

### U.S. Government Consulting Firm Discloses Data Breach Exposing over 340,000 Social Security Numbers



**What happened:** Greylock McKinnon Associates (GMA), a consulting firm known for assisting businesses and government agencies such as the U.S. Department of Justice (DOJ) in litigation support, has disclosed a data breach exposing 341,650 Social Security numbers. GMA stated it suffered a cyberattack in May 2023, promptly initiating mitigation measures. It has also notified law enforcement and the DOJ. In its notification email to the victims, GMA mentioned that the breach does not affect their current Medicare

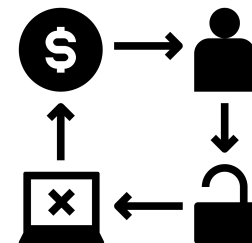
benefits or coverage and that the victims are not "the subject of this investigation or the associated litigation matters."

- **What this means:** GMA detected unusual activity in its internal network on May 30, 2023. The company took immediate steps to contain the attack. It consulted with third-party cybersecurity specialists and confirmed the individuals impacted by the cyberattack. Even though the breach does not affect the victims' Medicare benefits or coverage, the information exposed includes names, dates of birth, addresses, Social Security numbers, and some medical or health insurance information. GMA has further confirmed that it deleted all DOJ data from its systems after discovering the breach. As a part of its mitigation efforts, GMA is providing free proactive fraud assistance to the impacted individuals.

## **GHC-SCW Ransomware Attack Affects over 533,000 People**

**What happened:** Group Health Cooperative of South Central Wisconsin (GHC-SCW) has disclosed that a ransomware gang breached its network access and stole data that included protected health information (PHI) of over 533,000 individuals. On March 11, ZeroFox observed an update on the Black Suit Ransomware leak site [targeting](#) GHC-SCW.

- **What this means:** The attacker attempted to encrypt GHC-SCW's system, but the organization's IT department successfully secured the network. Investigators discovered that the attacker had copied some of GHC-SCW's data, which included PHI such as names, addresses, telephone numbers, e-mail addresses, dates of birth and/or death, Social Security numbers, member numbers, and Medicare and/or Medicaid numbers. GHC-SCW has been working with the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to mitigate the risks associated with the breach and has implemented enhanced security measures. The Impacted individuals are advised to monitor all communications from healthcare providers.



# | Deep and Dark Web Intelligence |

## | Deep and Dark Web Intelligence Key Findings

### Untested Threat Actor Advertised Zero-Day Exploit on Dark Web Forums



**What happened:** On April 10, 2024, untested threat actor "snowcat" (also known as "nightcat") advertised a zero-day Microsoft Outlook Remote Code Execution (RCE) exploit on predominantly Russian-language dark web forums Exploit and xss. According to snowcat, the exploit supports all versions of MS Outlook software. Snowcat is charging USD 300,000 for the exploit and has stated that the buyer will get exclusive rights to the exploit, its source code, and documentation on how the exploit works.

➤ **What this means:** As snowcat is untested, their credibility cannot be confirmed. Threat actors typically purchase zero-day exploits, as they target a vulnerability that is unknown to the vendor and does not have a patch. This allows attackers to compromise systems, run malicious code, and steal data. Ransomware groups have targeted zero-day vulnerabilities to conduct large-scale attacks. As this vulnerability affects a commonly used product, the exploitation of it could have a major impact.

### Actor Advertised Access to Snapchat Employee Accounts

**What happened:** On April 8, 2024, untested threat actor "hvc" advertised web access to two Snapchat employee accounts on xss. According to the threat actor, who is charging USD 20,000, the access includes the ability to request user information, make changes to user accounts, and review and modify spotlight posts. Additionally, a threat actor with this access can approve or deny reported accounts—meaning that the actor could report an account and then effectively ban it.



➤ **What this means:** As hvc is untested, ZeroFox cannot confirm the actor's credibility at this time. However, if the access sale proves to be credible, the buyer could acquire a significant amount of personal information from the large victim pool of Snapchat's 800 million users. The exact type of user information a buyer can obtain via this access was not disclosed in hvc's post; however, a 2019 breach of Snapchat user data by legitimate Snapchat employees provided access to information such as private messages, phone numbers, email addresses, and location data. ZeroFox assesses that this is likely the same type of information that would be available to the buyer.

## Actor “USDoD” Leaked Data Allegedly from a U.S. Federal Agency



**What happened:** On April 7, 2024, known threat actor “USDoD” leaked a database allegedly associated with a U.S. federal government agency on dark web forum BreachForums. USDoD claimed the leak contained over 15 million records in an uncompressed, 3 GB CSV format file. According to the forum post, the leaked data set included an unspecified contact list associated with “Critical Infra.” The post also included two samples of the data, which was divided into two fields in the CSV.

- > **What this means:** USDoD has a positive reputation on BreachForums, which typically indicates a number of successful transactions such as sales of leaked data or access to networks. It is unclear if USDoD received valid U.S. government data and, if they did, whether it is private or publicly available. Additionally, it is unclear if the association between the alleged contact list and “Critical Infra” (critical infrastructure) is derived from the raw data or an association the threat actor made on their own. U.S. federal agencies are often targeted by threat actors for data theft and extortion. As such, a number of threat actors on the dark web also make false claims to this information in an attempt to bolster their credentials or otherwise garner attention. ZeroFox will continue to monitor for indications this leak contains valid information.

# | Exploit and Vulnerability Intelligence |

## | Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies in the software solutions, asset management, and network security domains. Palo Alto Networks has [disclosed](#) a critical command injection vulnerability (CVE-2024-3400; CVSS score: 10) present in the GlobalProtect feature of its PAN-OS software for specific PAN-OS versions. Adobe has [released](#) security updates to address multiple vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. Fortinet has also [released](#) security updates to address vulnerabilities in multiple products, including OS and FortiProxy. Exploitation of some of these vulnerabilities could lead to unauthorized control over affected systems. Cybersecurity researchers have [discovered](#) a security flaw (CVE-2024-24576; CVSS score: 10) in the Rust standard library that could be exploited to target Windows users and stage command injection attacks. D-Link has [disclosed](#) a couple of vulnerabilities with critical and high ratings, respectively. These bugs affect approximately 92,000 internet-exposed D-Link network-attached storage (NAS) devices. Microsoft [released](#) the April 2024 Patch Tuesday notes this week, in which it addressed more than 140 vulnerabilities, including two actively exploited zero-day bugs (CVE-2024-26234 and CVE-2024-29988).

### Notable vulnerabilities:

#### [CVE-2023-45590](#)

**What happened:** Fortinet has released security patches for a **CRITICAL** FortiClientLinux vulnerability (CVE-2023-45590) assigned a CVSS score of 9.4.

➤ **What this means:** Users are advised to upgrade to the fixed versions listed in the advisory. The vulnerability can allow threat actors to execute unauthorized code or commands by tricking users into visiting malicious sites.

• **Affected products:**

- FortiClientLinux 7.2.0
- FortiClientLinux 7.0.6 through 7.0.10
- FortiClientLinux 7.0.3 through 7.0.4



#### [CVE-2024-24576](#)



**What happened:** A serious flaw (CVE-2024-24576) dubbed BatBadBut in the Rust standard library can be exploited to target Windows users and stage command injection attacks. This **CRITICAL** vulnerability has been assigned a CVSS score of 10.

➤ **What this means:** This vulnerability is due to OS command and argument injection weaknesses that can let attackers execute unexpected and potentially malicious commands on the operating system. The flaw impacts all versions of Rust before 1.77.2 on Windows. To mitigate this, it is recommended that users move batch files to a directory that is not included in the PATH environment variable.

● **Affected products:**

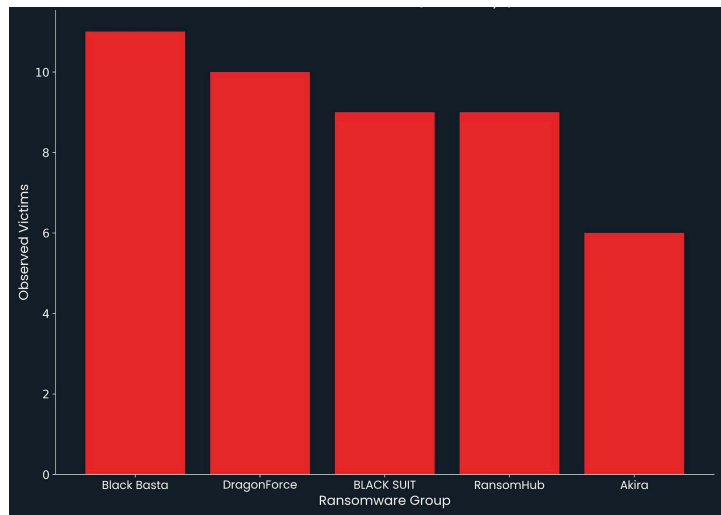
- Rust standard library

# | Ransomware and Breach Intelligence |

## **Ransomware and Breach Intelligence Key Findings**

### **Change Healthcare Asked to Pay Second Ransom**

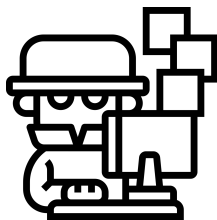
**What happened:** ZeroFox has observed BlackBasta record the highest ransomware-related activity for this week, closely followed by DragonForce. RansomHub has also upped its activity compared to last week; it has demanded a ransom from Change Healthcare and United Healthcare in exchange for a database that ALPHV previously claimed to have stolen. Meanwhile, Tarrant County Appraisal District has now confirmed that a cyberattack targeting its systems in March was a ransomware attack. On April 8, ZeroFox observed threat actor MedusaLocker claim responsibility for this attack.



Source: ZeroFox Internal Collections

- **What this means:** In the past week, the BlackBasta ransomware gang has targeted victims in the United States, the United Kingdom, and Switzerland. RansomHub, speculated to be associated with ALPHV, has threatened to leak 4 TB of stolen data from Change Healthcare in exchange for a ransom amount. This development came after ALPHV claimed responsibility for the cyberattack and had already received a ransom sum from Change Healthcare. MedusaLocker has threatened to leak 218 GB of stolen data of nearly 300 Fort Worth property owners unless a USD 100,000 ransom is paid. The impacted individuals must be wary of suspicious activities, as threat actors are likely to use the exposed credentials and information for further spear phishing attacks.

### **Breach Intelligence: Sisense Breach Endangers Critical Infrastructure**



**What happened:** CISA announced that Sisense, a data analytics company, has recently experienced a data breach. The agency is currently investigating this cyber incident and claims that it can affect critical infrastructure organizations. As a mitigation measure, customers are urged to reset any credentials connected with the company's platform and services.

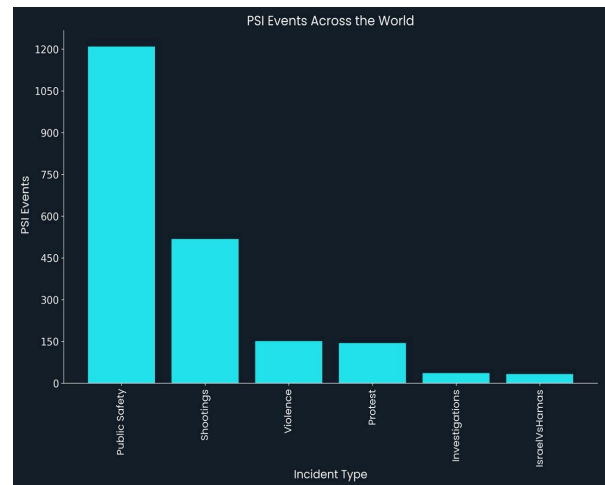
- **What this means:** Sisense confirmed that it has experienced a data breach and that certain information has been released on a “restricted access server.” According to the company, the data breach has not affected any business operations, and it is working towards securing its customers. At the time of writing, investigations have yet to reveal conclusive details about this breach.

# | Physical and Geopolitical Intelligence |

## | Physical and Geopolitical Intelligence Key Findings

### Physical Security Intelligence: Global

**What happened:** Israel has scaled back its ground troops in southern Gaza six months into the conflict. The military has reduced the number of soldiers, stating the need for “recuperation” and readiness for “future operations.” Meanwhile in Asia, a committee investigating the February 21 death of Shubh Karan Singh, a 21-year-old farm protester at the Khanauri border of Punjab, has requested six weeks to submit an interim report and six months to complete the death investigation. South Korea recently held elections amid pressing domestic issues like the cost of living, declining birth rates, and political corruption. Traditional concerns like North Korean nuclear threats and U.S. security commitments were reportedly overshadowed by more immediate worries about the country’s economic shortfalls. A cholera outbreak disinformation campaign in Mozambique has caused the deaths of nearly 100 individuals following the sinking of an overcrowded ferry off the Mozambique coast.

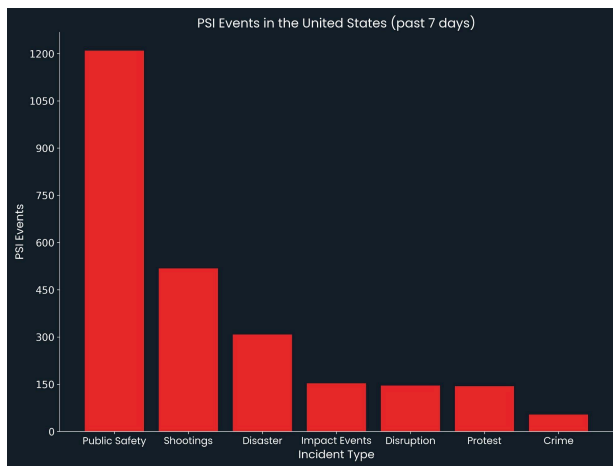


Source: ZeroFox Internal Collections

- **What this means:** The recent pause in the Israel-Hamas war involves only a fraction of the initial deployment remaining in the territory. Israel has not revealed any plans for a cease fire despite the famine, malnutrition, and increasing death toll in Gaza. Farmer protests in India have seen the High Court order a judicial probe into Singh's death amid various petitions, some of which sought restraining orders on farmers' marches and others aimed at removing barricades and restrictions imposed by the government to prevent the marches. Authorities on the South Korea elections view the divide between conservative and liberal candidates to be stark, as many voters lean towards party affiliation rather than individual candidates. In Mozambique, officials reported that the ferry vessel was overloaded with passengers attempting to escape the mainland due to false reports of a cholera outbreak. However, authorities have not provided further details on the source of the disinformation. ZeroFox observed a 40 percent reduction in protests in India compared to last week. After Israel's withdrawal of troops from Gaza, ZeroFox also observed a more than 50 percent drop in Israel/Hamas incident counts.

## Physical Security Intelligence: United States

**What happened:** In the past week, ZeroFox Intelligence observed that Illinois, California, and New York accounted for the highest numbers of U.S. public safety events. Illinois, Pennsylvania, and New York recorded the highest numbers of shooting incident alerts. While California saw a 27 percent increase in public safety alerts, Nevada witnessed shooting alerts six times more than the last week; Pennsylvania recorded a 50 percent increase in shooting incidents. Additionally, New York saw an increase in disaster alerts. There was a significant increase in protest activity in Illinois, but, overall, protest activity remained the same as last week across the United States..



Source: ZeroFox Internal Collections

➤ **What this means:** A shooting incident in the Summerlin neighborhood of Las Vegas, Nevada, left three dead, including the shooter. Meanwhile, a shooting at an Eid al-Fitr celebration attended by almost 1000 people in Philadelphia, Pennsylvania, left at least three people wounded. In Chicago, protesters urged Mayor Johnson to let them march nearer to the Democratic National Convention in August. New York witnessed a 4.8 magnitude earthquake on April 5, and researchers warned that California is likely to face earthquakes this year as well.

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%         |