



**ZEROFOX<sup>®</sup>**

*Weekly Intelligence Brief*

**Classification: TLP:GREEN**

**February 12, 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 (EST) on February 9, 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 Assessment – Super Bowl LVIII Event Assessment                         | 2         |
| ZeroFox Intelligence Brief – Threat Actors Exacerbate Divisions Ahead of Pakistan Elections | 2         |
| ZeroFox Intelligence Flash Report – Innovative Loader-as-a-Service Announced                | 2         |
| ZeroFox Intelligence Flash Report – Second New RaaS of 2024 Announced in Dark Web Forum     | 3         |
| <b>  Cyber Intelligence Key Findings</b>                                                    | <b>5</b>  |
| Hong Kong Company Loses USD 25 Million to Deepfake Scam Targeting an Employee               | 5         |
| Millions of User Records Stolen from 65 Websites via SQL Injection Attacks                  | 5         |
| Verizon Insider Data Breach Hits Over 63,000 Employees                                      | 6         |
| <b>  Deep and Dark Web Intelligence Key Findings</b>                                        | <b>8</b>  |
| ALPHV Ransomware Site Leaks Stolen Data from U.S.-based Healthcare Center                   | 8         |
| RansomHub Ransomware Group Emerges and Launches Data Leak Site                              | 8         |
| U.S. Government-Associated Contractors' Data Leaked on "Donut Leaks" Leak Site              | 9         |
| <b>  Exploit and Vulnerability Intelligence Key Findings</b>                                | <b>11</b> |
| CVE-2023-45025                                                                              | 11        |
| CVE-2001-1125                                                                               | 11        |
| <b>  Ransomware and Breach Intelligence Key Findings</b>                                    | <b>13</b> |
| Feud Between xss Admins and LockBit                                                         | 13        |
| "Mother of All Breaches" (MOAB)                                                             | 13        |
| <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>17</b> |
| <b>  Appendix B: ZeroFox Intelligence Probability Scale</b>                                 | <b>18</b> |

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

### **ZeroFox Intelligence Assessment - Super Bowl LVIII Event Assessment**

Super Bowl LVIII is scheduled to take place on February 11, 2024, at the Allegiant Stadium in Paradise, Nevada. Taking place just outside Las Vegas, the local area is anticipated to be saturated with attendees and visitors from February 9–13, 2024. Super Bowl LVIII is categorized by the U.S. Department of Homeland Security (DHS) as having a high-risk security rating with regards to public safety, and security is expected to be heavy around the stadium and across the Las Vegas region. At the time of this report, there were no credible threats associated with the Super Bowl; however, attendees and locals need to be aware of possible physical security and cyber-related concerns surrounding the event.

### **ZeroFox Intelligence Brief - Threat Actors Exacerbate Divisions Ahead of Pakistan Elections**

What was originally going to be a tight November 2023 general election now looks settled in February 2024. During the delay, the government of Prime Minister Shehbaz Sharif managed to nullify the electoral threat posed by former Prime Minister Imran Khan, initially looked to be the most likely winner. Backed by the powerful military, the government launched a crackdown on Khan and his supporters, which has left Khan isolated in jail while his party has languished politically. With both the political status quo and the military on the same side, expect a more predictable economic and foreign policy position from Pakistan. However, these well-laid plans could unravel because of the dual threat of social unrest posed by Khan as well as the elevated risk of terrorism inside Pakistan. If either of those issues is worse than anticipated, Pakistan could become even more unstable. Cyber threat actors appear to be working diligently to exacerbate these risks.

### **ZeroFox Intelligence Flash Report – Innovative Loader-as-a-Service Announced**

Since its announcement on January 25, 2024, by untested actor “Null14”, an innovative malware loader-as-a-service offering has been gaining traction on the predominantly Russian-speaking dark web community exploit[.]in. The currently unnamed loader allegedly targets Windows operating systems and is signed using valid certificates, enabling its deployment to remain undetected by various Windows systems as well as VirusTotal. Although ZeroFox can neither confirm nor disconfirm the credibility of the service, positive indicators add credence to the legitimacy of this loader service as an innovative malware-spreading technique. Malware distribution based on emulating credible software is likely on an upward trajectory, and this trend is expected to continue in the first half of 2024.

## **ZeroFox Intelligence Flash Report – Second New RaaS of 2024 Announced in Dark Web Forum**

On February 2, 2024, English-speaking threat actor “koley” announced the launch of a Ransomware-as-a-Service (RaaS) project named Ransomhub. The announcement, which was made in the Russian-speaking dark web forum RAMP, revealed that affiliates are now being sought. Ransomhub allegedly offers affiliates a host of new features, such as daily re-encryption and access to a control panel comprising a unique .onion domain address. The announcement about Ransomhub in English aligns with the recently-observed trend of English-speaking actors being willing to enter the traditionally Russian-dominated ransomware scene, as well as post in Russian-speaking dark web forums. The latest increase in new RaaS operations observed by ZeroFox is likely contributed to by the recent disruption of several prolific ransomware and digital extortion (R&DE) threat collectives.

# | Cyber Intelligence |

## **Cyber Intelligence Key Findings**

### **Hong Kong Company Loses USD 25 Million to Deepfake Scam Targeting an Employee**

**What happened:** The Hong Kong branch of a multi-national company suffered a loss of USD 25 million after scammers used deepfake technology to trick one of its employees. The targeted finance department employee reportedly received a message from an individual claiming to be the company's UK-based chief financial officer (CFO). They then attended a video conference with deepfake versions of the company's CFO and other company employees. Acting on instructions received on the video call, the employee then reportedly made 15 transactions to various Hong Kong bank accounts, transferring USD 25.6 million in total. No arrests have been made at the time of reporting.



- **What this means:** The Hong Kong police has classified the case as “obtaining property by deception” after an initial investigation conducted by its cybercrime unit. Deepfakes have been agitating the online community, claiming notable names as victims. Recently, social media platform X was forced to suspend Taylor Swift-related searches for a month after deepfake images of the popular celebrity were released on the platform. A deepfake version of President Joe Biden’s voice was used earlier this month in New Hampshire to deter voters from voting. It is imperative to be wary of deepfakes and AI technology, especially while sharing personal information over the internet.

### **Millions of User Records Stolen from 65 Websites via SQL Injection Attacks**

**What happened:** A hacking group known as “ResumeLooters” carried out a cyberattack, stealing over two million email addresses and other personal information from at least 65 websites in November and December 2023. The group reportedly used SQL injection attacks and sold the stolen data on Chinese-speaking, hacking-themed Telegram groups. Their targets were mainly in India, Taiwan, Thailand, Vietnam, and China, but ResumeLooters also hit sites in other countries, including Australia, the Philippines, South Korea, Japan, the United States, Brazil, Russia, and Italy. The group focused on compromising retail and recruitment websites, although victims in various other sectors were also identified.



- **What this means:** An SQL injection attack involves a threat actor injecting malicious SQL queries to trick databases into handing over information. ResumeLooters' methodologies are similar to those used by previously-identified threat actor "GambleForce."

## Verizon Insider Data Breach Hits Over 63,000 Employees

**What happened:** Over 63,000 employees from Verizon Communications have been affected by an insider data breach that exposed their sensitive information. The exposed data varies per employee and includes full name, physical address, social security number, national ID, gender, union affiliation, date of birth, and compensation information.

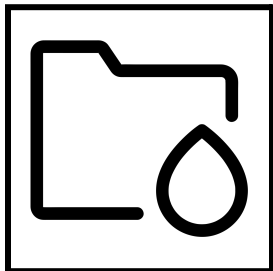
- **What this means:** Verizon has disclosed that it found no indication of malicious intent and does not believe that the information was shared externally. To avoid similar incidents, Verizon is reportedly working towards strengthening its internal security and has advised the exposed employees to enroll in a two-year identity theft protection and credit monitoring service.



# | Deep and Dark Web Intelligence |

## | Deep and Dark Web Intelligence Key Findings

### ALPHV Ransomware Site Leaks Stolen Data from U.S.-based Healthcare Center



**What happened:** On February 6, 2024, ZeroFox observed an update to the ALPHV ransomware leak site containing stolen data from the U.S.-based healthcare center Vail-Summit Orthopaedics and Neurosurgery (VSON). Published on the leak site on February 5, the post claims that the ransomware group stole 150 GB of internal data from the company's file server (including employees' personal data, financial statements, and accounting data) and customer documentation (including drivers'

licenses, Social Security numbers, and credit card information). The post also claims that ALPHV possesses the company's full network map, including credentials for local and remote services.

- **What this means:** After the FBI's seizure of ALPHV's former ransom site in December 2023, the group vowed to retaliate against U.S. targets in addition to removing all rules from its affiliate program that previously barred users from targeting hospital networks and emergency services. Despite several disruptions to the group's operations (even prior to the December 2023 seizure) that led to a downturn in associated attacks, ZeroFox has tracked a steady stream of recent claimed attacks against U.S. entities. While ZeroFox cannot confirm the authenticity of these—and despite ALPHV's current relatively-degraded operational capacity—the group's abilities should not be completely disregarded. ZeroFox will continue to monitor the group's activities— including those targeting the healthcare sector, which continues to experience an uptick in ransomware attacks.

### RansomHub Ransomware Group Emerges and Launches Data Leak Site

**What happened:** On February 2, 2024, threat actor koley announced the RansomHub RaaS affiliate program on dark web forum RAMP. The actor claimed that the locker is written in Golang and C++ and has a very fast encryption speed. This week, a data leak site was launched for RansomHub ransomware as well. The group claims to be hackers from different countries and will not target Commonwealth of Independent States (CIS) countries, Cuba, North Korea, China, and Romania. It also claims that RansomHub ransomware affiliates cannot



target non-profit organizations or re-attack victims after the ransom payment is received. At the time of reporting, no victims are listed on the data leak site.

- **What this means:** Ransomware continues to be a major threat to companies worldwide, and new groups are consistently emerging. Koley claims to have considered the pros and cons of past ransomware affiliate groups and created the next generation of ransomware. As these new groups emerge, they appear to build on past ransomware programs and make their own unique enhancements to them. This suggests that ransomware will continue to become harder to detect and have more security functions, benefitting the affiliates using RaaS services. ZeroFox will continue to monitor this new ransomware group and its data leak site.

## **U.S. Government-Associated Contractors' Data Leaked on "Donut Leaks" Leak Site**



**What happened:** On February 6, 2024, the "Donut Leaks" leak site claimed to have information derived from multiple companies that are U.S. government contractors. The post claimed to have an unspecified set of documents from three separate U.S. government contractors. The leak site provided alleged samples of documents from each of the three companies, some of which were marked "proprietary," and stated the data was valued at USD 20,000 by the victim organizations. Furthermore, the group claimed in the post to have an asking price of "at least" USD 500,000.

- **What this means:** The Donut Leaks leak site (aka D0nut Leaks) is associated with the Donut Leaks ransomware group and has been active since August 2022. The group likely has overlap with other ransomware groups, such as Ragnar Locker and Hive. The alleged sample documents appear to be engineering-related documents for specific projects and have the companies' names in an attempt to prove authenticity. At least one of the sample documents contains a commercial and government entity (CAGE) code, an identifier used by companies that have a contractual relationship with the U.S. government. ZeroFox is unable to verify the leak site's claims to have valid, proprietary data from the listed companies but will continue to monitor for indications authenticity and further data leaks.

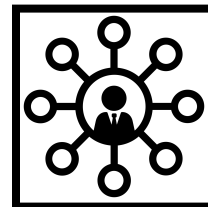
# | Exploit and Vulnerability Intelligence |

## | Exploit and Vulnerability Intelligence Key Findings

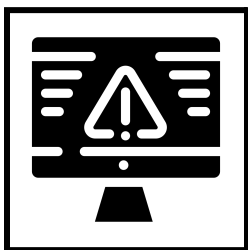
### [CVE-2023-45025](#)

**What happened:** An operating system (OS) command-injection vulnerability affects several versions of QNAP OS. This **CRITICAL** vulnerability has a CVSS base score of 9.8.

- **What this means:** The vulnerability could allow a successful attacker to execute commands via a network when the system is in a certain configuration. Users of the affected versions of the OS should update their systems to the latest versions containing patches for the bug.



### [CVE-2001-1125](#)



**What happened:** Symantec LiveUpdate before 1.6 does not use cryptography to ensure the integrity of download files, which allows remote attackers to execute arbitrary code via DNS spoofing of the update.symantec[.]com site. This **CRITICAL** vulnerability has a CVSS base score of 9.8.

- **What this means:** Cybersecurity researchers have reported that Symantec LiveUpdate for Norton Antivirus does not use cryptography when updating virus definitions. This potentially allows a remote attacker to dupe unsuspecting clients into installing malicious LiveUpdates, which may contain malicious programs.

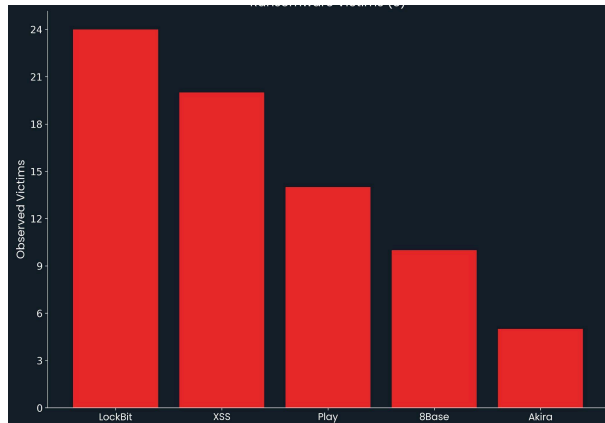
# Ransomware and Breach Intelligence

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

### **Feud Between xss Admins and LockBit**

**What happened:** Underground forum xss continues to feature the highest number of relevant (cybersecurity-related) posts tracked by ZeroFox. 8Base, BianLian, and Akira were among the most active ransomware groups for the past three weeks, while LockBit remains the most prolific.

- **What this means:** Manufacturing, professional services, and construction were the industries most widely-targeted by ransomware groups this week. ZeroFox also reported on an [ongoing feud](#) (involving death threats) between LockBit and the admins of the xss forum over LockBit's alleged non-payment for a purchase.



### **"Mother of All Breaches" (MOAB)**

**What happened:** Security researchers have discovered one of the largest-ever data breach packages, dubbed "Mother of All Breaches" (MOAB), which contains over 26 billion records.

**What this means:** The package is a combination of several individual breach packages, some of which were already publicly available. The meticulously-arranged data package was sourced from major social media and other platforms across the world. The leaked fields include email address, password, name, username, date of birth, and physical address.

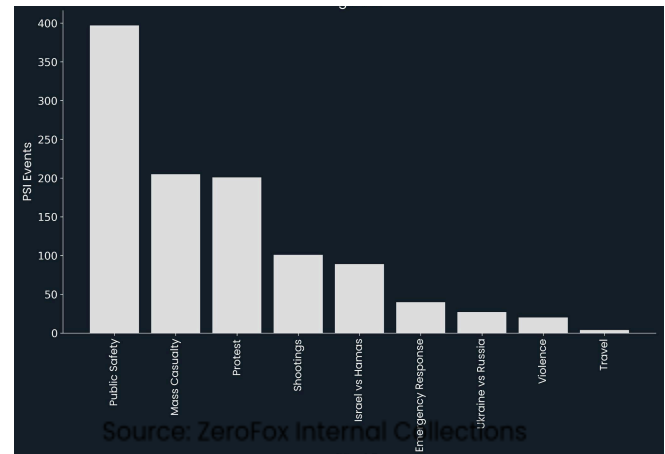
# Physical and Geopolitical Intelligence

## Physical and Geopolitical Intelligence Key Findings

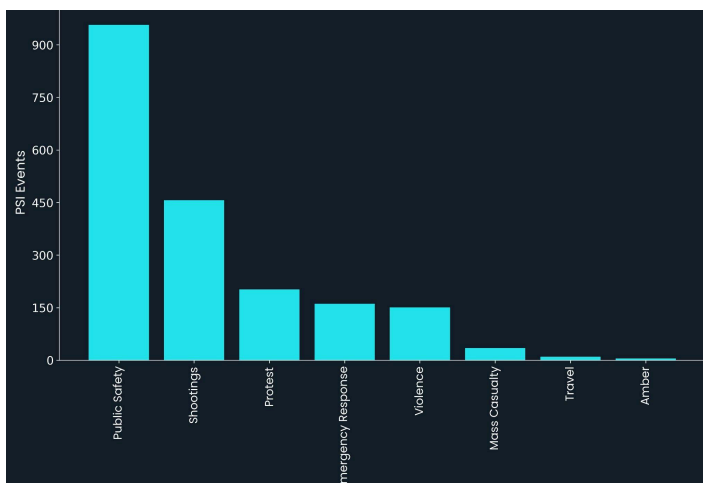
### Physical Security Intelligence: Global

**What happened:** In a controversial interview with Tucker Carlson, Russian president Vladimir Putin indicated that the ongoing Russia-Ukraine war could end via a deal with the West negotiated by the United States. Additionally, protest activity continues to dominate the news, with farmer protests of varying degrees of significance occurring in Europe and Asia.

- **What this means:** The European farmers' protests are escalating and are now spreading to Spain. Meanwhile, India is witnessing farmers' protests demanding agricultural concessions, including a law to guarantee a minimum support price for crops. Such activity is very likely to continue in the run-up to the Indian general elections, which are likely to be conducted in April and May this year.



### Physical Security Intelligence: United States



**What happened:** ZeroFox Intelligence observed that California, Illinois, and New York accounted for the greatest number of public safety, shooting, and gun violence events in the past week. Additionally, as highlighted in a [ZeroFox advisory](#), attendees and locals need to remain aware of possible physical security concerns surrounding the upcoming Super Bowl LVIII.

- **What this means:** Super Bowl LVIII is categorized by the U.S. Department of Homeland Security (DHS) as having a high-risk security rating with regards to public safety. At the time of this report, there were no credible threats associated with the Super Bowl.

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

### WHEN SHOULD IT BE USED?

#### Red

##### 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.

#### Amber

##### 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

### 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.

#### Clear

##### 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%         |