



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 11, 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 March 8, 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
ZeroFox Intelligence Flash Report – LockBit & ALPHV Activity Likely Consistent with Exit Scams	2
ZeroFox Intelligence Flash Report – Threat Actors Target Israel over Possible Rafah Incursion	2
ZeroFox Intelligence Assessment – How GenAI is Changing the Cyber Threat Landscape	2
 Cyber Intelligence Key Findings	5
North Korean Hackers Target South Korean Semiconductor Firms Using LoTL Tactics	5
Content Farm Impersonating over 60 Prominent English Media Outlets	5
BEC–Specialized Hackers Mimic U.S. Government Entities to Steal Sensitive Information	6
 Deep and Dark Web Intelligence Key Findings	8
ALPHV Reportedly Exit Scamming and Selling Source Code	8
New Python-Based Snake Info Stealer Spreading Through Facebook Messages	8
 Exploit and Vulnerability Intelligence 	9
 Exploit and Vulnerability Intelligence Key Findings	10
CVE-2024-27198	10
CVE-2024-23296 & CVE-2024-23225	10
 Ransomware and Breach Intelligence Key Findings	12
Ransomware Intelligence: ALPHV Pulls an Exit Scam	12
Breach Intelligence: IMS Systems Hack Exposes Victims' PII	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	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – LockBit & ALPHV Activity Likely Consistent with Exit Scams

Operators behind both the LockBit and ALPHV ransomware and digital extortion (R&DE) operations are exhibiting behavior likely consistent with imminent exit scams against their affiliates at the time of writing. Both groups have claimed to be continuing operations following recent law enforcement (LE) activities, consistently downplaying the impact of disruptive action despite a significant reduction in observed activity. While ZeroFox can neither confirm nor deny the veracity of claims of scamming made by alleged LockBit and ALPHV affiliates, similar activity has been conducted by other notable ransomware collectives in the days preceding the cessation of their operations. Victims of outstanding or ongoing extortion attacks by LockBit and ALPHV are unlikely able to assume their stolen data will be deleted following payment of ransom demands. Regardless of whether they choose to pay ransom demands, victims are at an increased risk of stolen data not being deleted and, instead, sold on the deep and dark web (DDW) to the highest bidders.

ZeroFox Intelligence Flash Report – Threat Actors Target Israel over Possible Rafah Incursion

Hacktivist group Handala claimed an attack against Israel's Iron Dome missile defense system and a radar system tracking Israeli aircraft. The effects of this attack could disrupt Israel's defense industry and military operations in Gaza if the leaked radar information is disclosed to Israel's adversaries. The finding indicates that Handala is more incentivized and capable than other threat actors who have emerged since the Israel-Hamas war began in October. The group seems to be intent on continuing attacks against Israel, as well as increasing the impact of these attacks. Handala warned that its hacks could escalate if Israel moves ahead with its final incursion into Rafah, the last remaining city in Gaza yet to face an offensive. A ceasefire proposal between both sides is proving elusive, and Israel has given the start of Ramadan on March 10 as a key date for beginning the offensive.

ZeroFox Intelligence Assessment – How GenAI is Changing the Cyber Threat Landscape

Generative Artificial Intelligence (GenAI) models offer vast potential in enabling mass automation, economic growth, scientific advances, and communication. However, there are also numerous security risks arising from its development and deployment, including ethical concerns, societal impacts, and use by nefarious cyber actors for malicious purposes. Adoption of GenAI-enabled technologies by corporate enterprises will also very likely introduce new vulnerabilities into

organizations' infrastructure and undermine secure-by-design principles. With emerging technologies and tools getting widespread and significant media and public attention, much of the discussion around the threat from GenAI is misleading, unclear, and unhelpful. At least in the short to medium term, GenAI will very likely serve as a force for both good and evil; the rapid development of new technologies will be added to the repository of tools used by threat actors to conduct their attacks as well as to the arsenals security personnel use to mitigate threats.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

North Korean Hackers Target South Korean Semiconductor Firms Using LoTL Tactics

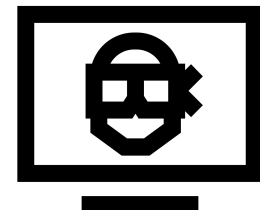


What happened: The National Intelligence Service (NIS) of South Korea has issued a press release highlighting its discovery of North Korean hackers targeting domestic semiconductor firms from the second half of 2023 until recently. The press release details cyberattacks that occurred in December 2023 and February 2024 targeting two companies that had their configuration management server and security policy server hacked. The attackers also stole product design drawings and facility site photos. They used Living off the Land (LoTL) techniques to conduct the attacks. These techniques minimize malicious code usage and target systems via programs already installed, making the attacks difficult to detect.

- **What this means:** NIS has urged all related industries to be wary of North Korean LoTL attacks. The agency believes North Korea is manufacturing its own semiconductor devices after sanctions against the country made it difficult to procure chips. NIS also associates North Korea's increase in demand for semiconductors with the development of weapons such as satellites and missiles. This likely also has geopolitical implications, as North Korea has accelerated weapons and military resource exchanges with Russia amid the ongoing Russia-Ukraine war. Moreover, earlier in February, United Nations sanctions reportedly targeted individuals behind suspected North Korean cyberattacks on cryptocurrency-related companies. These crypto thefts raked in USD 3 billion, which has reportedly helped nurture the country's nuclear weapons program.

Content Farm Impersonating over 60 Prominent English Media Outlets

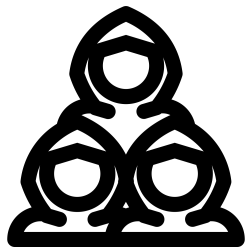
What happened: Cybersecurity researchers have analyzed a content farm impersonating over 60 prominent English-language media outlets based in the United States and the United Kingdom. The research has identified over 60 domains reposting articles from credible media and research organizations without proper attribution and traced the websites' proprietor in India. The proprietor has been observed spamming comments sections of various websites with backlinks to the domains to improve their credibility. Some of the comments also appear to be advertisements for



the sale of slots for press releases and product reviews; prices start at USD 50 per post and range to "bulk deal" pricing of USD 1,000.

- **What this means:** This discovery has highlighted the proliferation of deceptive online practices, raising concerns about the spread of disinformation and exploitation of legitimate media trademarks. Amid the election season across the world, numerous threat actors are targeting media outlets to spread propaganda and disseminate disinformation. Moreover, in the past year, ZeroFox has detected over 150 ransomware attacks on the media and entertainment industry primarily orchestrated by ClOp and LockBit, of which 80 percent of the targeted media outlets were based in North America and Europe.

BEC-Specialized Hackers Mimic U.S. Government Entities to Steal Sensitive Information



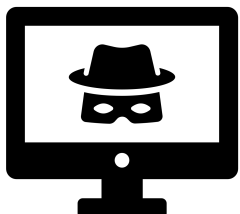
What happened: TA4903, a hacker group specializing in business email compromise (BEC) attacks, has been impersonating several U.S. government agencies to deliver files with malicious links that redirect targets to fake bidding processes. Cybersecurity researchers have observed the threat actor masquerading as the U.S. Department of Transportation, the U.S. Department of Agriculture, and other federal departments. From mid-2023 through 2024, researchers have also observed the actor spoofing small and medium-sized businesses (SMBs) in several industries, including construction, manufacturing, food and beverage, energy, and finance. TA4903 reportedly carries out these financially-motivated attacks to steal corporate credentials, infiltrate mailboxes, and conduct follow-on BEC activity.

- **What this means:** While TA4903's high-volume email campaigns mostly target organizations in the United States, researchers have observed the threat actor targeting global entities as well. Organizations must be vigilant in monitoring emails from suspicious accounts to prevent threat actors like TA4903 from accessing sensitive information. Additionally, incorporating a comprehensive, multi-layered security strategy is the most effective method of mitigating the risks of spoofing attacks.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

ALPHV Reportedly Exit Scamming and Selling Source Code



What happened: On March 4, 2024, ZeroFox published a [Flash Report](#) noting that ALPHV activity suggested the ransomware operator was likely about to perpetrate an exit scam. On March 5 and 6, 2024, ALPHV claimed to have its old and new leak sites seized by law enforcement agencies on dark web forums; however, there is speculation that the seizure notices are fake.

Affiliates have also taken to dark web forums with evidence that suggests ALPHV is conducting an exit scam. ALPHV updated its TOX status to an announcement that it is selling the ALPHV ransomware source code for USD 5,000,000 as well.

- **What this means:** These additional pieces of information further confirm ZeroFox's prediction about ALPHV exit scamming. It is possible that the actor is planning on rebranding after some time when attention from law enforcement reduces. ALPHV has been one of the most prominent ransomware groups (following LockBit), so overall ransomware activity may temporarily decline.

New Python-Based Snake Info Stealer Spreading Through Facebook Messages

What happened: Cybersecurity research revealed new methods by which threat actors are using Facebook messages to execute a Python-based information stealer dubbed Snake designed to capture credentials and other sensitive data.

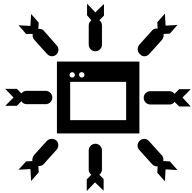
- **What this means:** Details about the campaign first emerged on the social media platform X (formerly Twitter) in August 2023. The attacks entail sending prospective users seemingly harmless RAR or ZIP archive files that, upon opening, activate the infection sequence. The intermediate stages involve two downloaders: a batch script and a cmd script, with the latter responsible for downloading and executing the information stealer from an actor-controlled GitLab repository. The credentials harvested from unsuspecting users are transmitted to different platforms such as Discord, GitHub, and Telegram.



| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

[CVE-2024-27198](#)

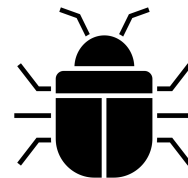


What happened: CVE-2024-27198 is an authentication bypass vulnerability in the TeamCity On-Premises CI/CD (continuous integration and continuous delivery/continuous deployment) solution from JetBrains. It can potentially allow threat actors to bypass authentication checks and gain administrative control of a vulnerable TeamCity On-Premises server. This **CRITICAL** vulnerability has been assigned a CVSS score of 9.8

- **What this means:** CVE-2024-27198 affects all versions of TeamCity On-Premises. Compromising a TeamCity On-Premises server can create conditions for a supply chain attack. Threat actors can also conduct denial-of-service (DoS) attacks or listen on client connections from an adversary-in-the-middle position. JetBrains has released a patch for this vulnerability in TeamCity 2023.11.4 and has urged all customers to upgrade to this version.

[CVE-2024-23296](#) & [CVE-2024-23225](#)

What happened: Apple has recently patched two iOS memory corruption zero-day vulnerabilities, CVE-2024-23296 and CVE-2024-23225. ZeroFox has assessed CVE-2024-23296 as **CRITICAL** (CVSS score 9.8) and CVE-2024-23225 as **HIGH** (CVSS score 8.4). The vulnerabilities allow cyberattackers to bypass kernel memory protections.



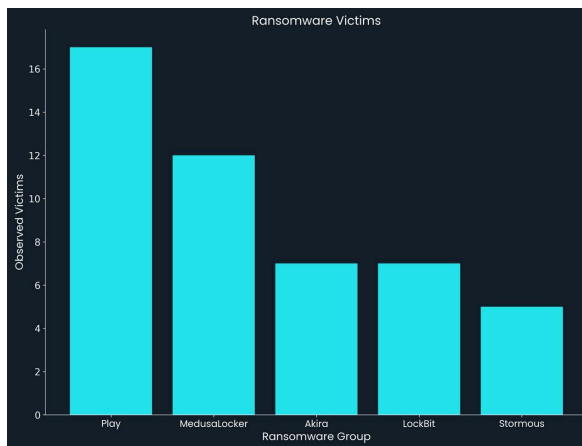
- **What this means:** Both the bugs allow threat actors with arbitrary kernel read and write capabilities to bypass kernel memory protections. Bypassing kernel protections essentially lets an attacker rootkit the device so that they can access everything, including access to location information, iPhone camera and mic, and messages. The company has rolled out urgent software updates (iOS 17.4, iPadOS 17.4, and iOS 16.7.6) to fix these security flaws.

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: ALPHV Pulls an Exit Scam

What happened: Notorious threat actor BlackCat/ALPHV has claimed that law enforcement agencies have seized its leak sites. However, law enforcement has reportedly denied involvement in disrupting BlackCat's operations. Meanwhile, as observed by ZeroFox intelligence, the Play ransomware gang has overtaken LockBit in the past week in terms of activities. Play ransomware has been in the news lately for reportedly leaking 65,000 Swiss government documents after it breached a software solutions provider for the Swiss government in May 2023.



Source: ZeroFox Internal Collections

- **What this means:** Law enforcement's reported denial of taking over ALPHV's leak sites indicates that the group is likely pulling an exit scam on its affiliates. This development comes after the adversary allegedly received USD 22 million in ransom payment from UnitedHealth's Change Healthcare unit (Optum). Meanwhile, Play ransomware has added around 10 victims to its leak site this week, with most of them based in the United States.

Breach Intelligence: IMS Systems Hack Exposes Victims' PII



What happened: A data breach at Infosys McCamish Systems (IMS) reportedly compromised financial information of over 28,000 people associated with a prominent insurance company. Another major bank reported a breach last month that exposed the data of over 57,000 customers, again via a breach at IMS. LockBit ransomware group had reportedly claimed IMS as a victim and posted a data-sale ad—purportedly of data stolen from over 2,000 compromised IMS systems—on its darknet site.

- **What this means:** The breaches compromised customers' names, Social Security numbers, states of residence, bank account and routing numbers, and dates of birth. Customers should remain vigilant for fraudulent activity or identity theft and beware of threat actors using the compromised data in follow-on attacks. In the past year, ZeroFox has observed 822 victims of LockBit, of which 48 belonged to the financial sector.

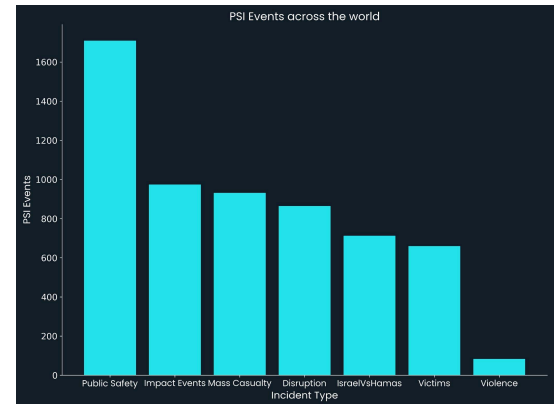
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

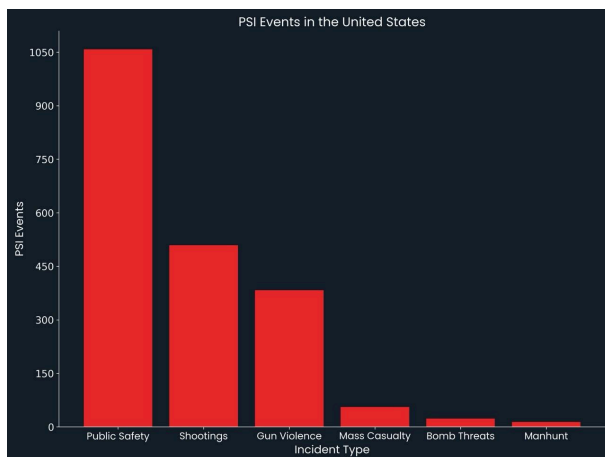
What happened: Yemen's Houthi rebels declared that ships entering Yemeni territorial waters would be required to obtain a permit from the Houthi-controlled Maritime Affairs Authority. Meanwhile, media sources reported that Yemen-based Houthi rebels had damaged four undersea communication cables in the Red Sea between Djibouti and the Saudi Arabian city of Jeddah. On March 7, 2024, sources reported that the anchor of the *MV Rubymar*, a cargo ship sunk by a Houthi strike, may have been responsible for severing submerged Red Sea data cables.

- **What this means:** It is unclear what the penalty would be for ships that do not obtain a permit; the Houthis have readily attacked cargo ships with drones and missiles since the Israel-Hamas war began in Gaza last year. Sources first began reporting damage to the undersea cables in late February, and it was speculated that Houthi agents were responsible as the group had previously suggested it may target them. Internet disruptions from the damage have mostly been reported in Gulf countries and India; disruptions seem serious but not critical because many other Red Sea cables remain functional.



Source: ZeroFox Internal Collections

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: Philadelphia has witnessed at least four shooting incidents in the past week (March 3-March 7), claiming two deaths and several injuries. Another shooting incident at a Mississippi nightclub claimed the life of a 20-year-old and injured at least 12 others. The FBI has accused a 42-year-old Iranian of being involved in plots to kill current and former U.S. government officials to avenge the killing of Iranian general Qasem Soleimani. Florida's governor has planned to deploy state troopers for crowd control during the spring break season to impede "lawlessness."

- **What this means:** The FBI has published a notice stating it wants the alleged Iranian spy to come in for questioning regarding the recruitment of individuals for operations in the

United States. Meanwhile, as thousands of college students travel to popular spring break destinations across Florida, 17 law enforcement agencies and around 140 state troopers will help curb chaos, direct traffic, and monitor DUI (driving under the influence) sobriety checkpoints.

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%