



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

April 8, 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 5, 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 - New "Wolf's Den" Platform Comes with Uncensored AI Text Generation	2
ZeroFox Intelligence Flash Report - Actor Seeks Access to Government and Critical Infrastructure Networks	2
ZeroFox Intelligence April 2024 Geopolitical Brief	2
 Cyber Intelligence Key Findings	5
Indian Government Rescues 250 Citizens Forced into Cybercrime in Cambodia	5
Massive Phishing Campaign Strikes Latin America; Venom RAT Targeting Multiple Sectors	5
Missouri County Hit by Ransomware	6
 Deep and Dark Web Intelligence Key Findings	8
Threat Actor Claims DDoS Attack Against Maryland Aviation Administration	8
Threat Actor "BabyLock" Advertises Malware for Persistent Access on RAMP Forum	8
Threat Actor "ByAI2O3" Selling RDP Access Bundle to 40 U.S. and European Companies	9
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-25096	11
CVE-2024-3094	11
 Ransomware and Breach Intelligence Key Findings	14
LockBit Continues to Dominate Ransomware Numbers	14
Breach Intelligence: AT&T Confirms Data Breach	14
 Physical and Geopolitical Intelligence 	16
 Physical and Geopolitical Intelligence Key Findings	17
Physical Security Intelligence: Global	17
Physical Security Intelligence: United States	17
 Appendix A: Traffic Light Protocol for Information Dissemination	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – New “Wolf’s Den” Platform Comes with Uncensored AI Text Generation

On March 21, well-known threat actor and malware-developer “Poe” announced on the dark web forum Onniforums the launch of a new anti-censorship underground community dubbed “Wolf’s Den.” Access to the full version of Wolf’s Den is expected to only be available via manually issued invites. Poe claims Wolf’s Den features uncensored artificial intelligence (AI) text and image generation—including malware scripting—and allegedly contains a video showing a live demonstration of a generative model writing out ransomware code. The project is expected to gain significant traction within Russian and English-speaking threat actor communities, with actors attempting to get an invite to Wolf’s Den in order to freely create malware applications.

ZeroFox Intelligence Flash Report – Actor Seeks Access to Government and Critical Infrastructure Networks

On March 27, untested threat actor “Nikazon” posted in the deep and dark web (DDW) forum RAMP advertising its search for affiliates able to provide illicit access to the networks of industrial, military, justice, and political targets. ZeroFox observed an approximately 55 percent increase in the number of ransomware and digital extortion (R&DE) attacks targeting organizations within the defense, government, and critical infrastructure sectors between Q1 2023 and Q1 2024. This advertisement is likely supportive of an ongoing shift in DDW norms manifested by financially motivated R&DE threat actors punitively seeking victim organizations—the targeting of which would traditionally be frowned upon by other groups, affiliates, and platform moderators.

ZeroFox Intelligence April 2024 Geopolitical Brief

In this monthly intelligence brief, ZeroFox details the warnings issued by authorities across Europe (led by France, Germany, and Italy) that the Islamic State (IS) threat is at its highest level in years. This high level of IS threat will likely continue from Easter weekend through the Paris Olympics in August. April will see the start of a new and potentially dangerous operating environment for Western firms in Hong Kong; in late March, Hong Kong authorities enacted a new national security law that bears a similarity to laws in mainland China that limit access to data and severely penalize those who access it. A dangerous security environment is emerging in the Caribbean region. Haiti presents the biggest risks, but there are also security risks stemming from the near collapse of Cuba's economy and

Venezuela's crackdown on the opposition ahead of the July elections. In India, a six-week-long election cycle presents unique risks, although the political outcome is all but certain. Croatia, Ecuador, Slovakia, and South Korea will also hold elections and other votes in April.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

Indian Government Rescues 250 Citizens Forced into Cybercrime in Cambodia

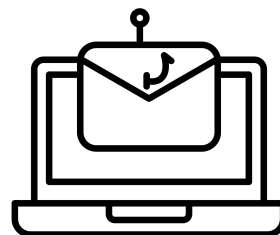


What happened: The Indian government has rescued and repatriated 250 citizens in Cambodia who were forced to conduct cybercrimes. According to sources, there are more than 5,000 Indians trapped in Cambodia who are being forced to launch extortion scams. The U.S. Department of State has called out China-based organized crime syndicates for posing as labor brokers to recruit people with English proficiency from Africa and Asia via social media with promises of lucrative jobs in Southeast Asia. An investigation to locate and repatriate more victims is ongoing.

- **What this means:** The rescue operation comes after a report from an Indian media outlet highlighted a meeting between the Ministry of Home Affairs (MHA) and other Indian federal agencies, including the Indian Cyber Crime Coordination Centre (I4C), to discuss strategy to rescue Indians held captive in Cambodia. The Indian nationals were lured with employment opportunities in Cambodia but were instead forced to undertake illegal cyber work. Sources have also stated that the Indians trapped in Cambodia conduct scams against their will targeting the Indian population. India has reportedly lost approximately USD 500 million (INR 500 crores) to Cambodian cyber fraud. The Indian Ministry of External Affairs (MEA) has said the Indian embassy is working with Cambodian authorities to crack down on such fraud schemes.

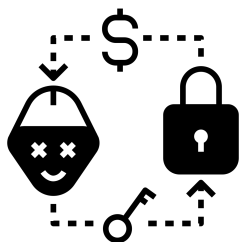
Massive Phishing Campaign Strikes Latin America; Venom RAT Targeting Multiple Sectors

What happened: The threat actor known as “TA558” has been connected to a new phishing campaign that targets a wide range of sectors in Latin America to deploy Venom RAT. The attacks primarily target hotel, travel, trading, financial, manufacturing, industrial, and government verticals in Spain, Mexico, the United States, Colombia, Portugal, Brazil, the Dominican Republic, and Argentina. Following the law enforcement takedown of QakBot last year, threat intelligence analysts have observed that threat actors have been increasingly using the DarkGate malware loader to target financial institutions in Europe and the United States.



- **What this means:** TA558 has been active since 2018 with a history of targeting victims in the Latin America region to deliver a variety of malware strains, including Loda RAT, Vjw0rm, and Revenge RAT. According to cybersecurity researchers, TA558 has been leveraging phishing emails as an initial access vector to deploy Venom RAT. This particular strain is a derivative of Quasar RAT and is capable of extracting sensitive data and controlling systems remotely. Researchers have stated that threat actors like TA558 aim to increase the number of infected devices and the volume of data extracted from a victim.

Missouri County Hit by Ransomware



What happened: Jackson County, Missouri, disclosed a cyber incident that caused major disruptions to its IT systems, possibly due to a ransomware attack. Although investigations are ongoing to confirm the cause, the county has reportedly taken steps to contain the attack and is working on restoring services. The disruption has impacted various services, including tax payments, online property, and inmate search systems. As a mitigation measure, Assessment, Collection, and Recorder of Deeds offices at physical locations are closed until the issue is resolved.

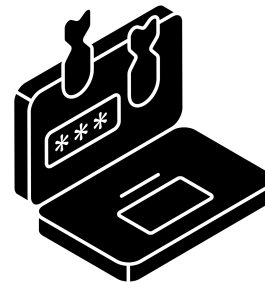
- **What this means:** Threat actors gained a foothold into Jackson County's network when a corrections officer reportedly clicked on a phishing email. The hack was contained, and municipal elections were not affected thanks to a private IT company working with the county at that time. An official confirmed that the attack did not affect core systems, taxpayer data, and the courts. At the time of writing, the county has entered a state of emergency in order to mitigate the situation.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Threat Actor Claims DDoS Attack Against Maryland Aviation Administration

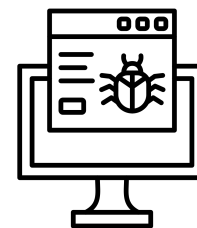
What happened: On March 31, 2024, pro-Russian hacktivist group “Server Killers” claimed on its Telegram channel to have conducted distributed denial-of-service (DDoS) attacks against two U.S.-based aviation administration websites: the Maryland Aviation Administration’s (MAA) site, marylandaviation[.]com, and the MAA’s Office of Regional Aviation Assistance site, marylandregionalaviation[.]aero. These attacks come less than a week after the group [claimed](#) to have conducted a DDoS attack against U.S.-based electric and natural gas utility company Energy East.



- **What this means:** ZeroFox [assessed](#) last week that Server Killers would very likely continue to post similar content claiming DDoS attacks against NATO member states, with a moderate chance that it would continue to focus on U.S. targets. The MAA is now the second U.S.-based victim of the group ZeroFox has tracked; both victims operate within major critical infrastructure sectors. As with Energy East, ZeroFox cannot currently confirm the validity of the claimed attack on MAA but can assess that it is highly likely that the group will continue to claim attacks against U.S. critical infrastructure entities. These entities should remain alert, and ZeroFox will continue to monitor for additional activity and/or escalated threats from the group.

Threat Actor “BabyLock” Advertises Malware for Persistent Access on RAMP Forum

What happened: On March 31, 2024 untested threat actor “BabyLock” posted an advertisement for a “private” malware on the RAMP forum. The malware, which BabyLock claims can bypass endpoint detection response (EDR) and extended detection response (XDR) systems, is reportedly capable of launching command lines on the target machine. The malware was being sold for USD 3,000. As of the latest reporting, it is unclear if the malware was sold.

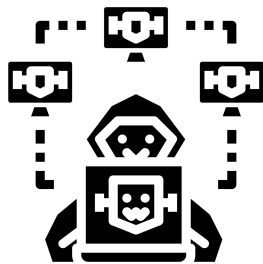


- **What this means:** It is noteworthy that an untested threat actor would ask for USD 3,000 for custom malware. BabyLock claims in the post that the malware is designed for persistence and to evade both EDR and XDR systems. The latter is designed to detect threats beyond the initial access vector and in multiple layers—a feature that, if bypassed, would allow for

the advertised network persistence. ZeroFox cannot assess with any confidence that the malware performs as advertised given the threat actor's lack of reputation but will continue to monitor for indications of a successful sale.

Threat Actor "ByAl2O3" Selling RDP Access Bundle to 40 U.S. and European Companies

What happened: On April 1, 2024, untested threat actor "ByAl2O3" advertised an auction for a remote desktop protocol access bundle to 40 separate U.S.-based and European companies on the predominantly Russian-language dark web forum Exploit. The starting bid for the access bundle was USD 400, with a minimum bid of USD 50 and an instant purchase price of USD 600.



➤ **What this means:** An actor could purchase all of these accesses and conduct a large number of attacks. This could also be beneficial for ransomware groups, as they could gain access to a potential victim company for a low cost compared to what they might receive for each ransom to increase their profit margin. Single access could also be purchased by lower-tier actors trying to evolve their capabilities by stealing a company's data and reselling it for a higher cost.

| 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 software solutions, asset management, and network security domains. Google [patched](#) two zero-day vulnerabilities in Google Pixel phones, which were exploited by forensic firms to bypass PIN protections and access stored data. Additionally, Ivanti released security [updates](#) to address four vulnerabilities affecting Connect Secure and Policy Secure Gateways. These flaws could lead to code execution and denial-of-service (DoS) attacks. Ubuntu fixed several security issues, including CVE-2024-31080, CVE-2024-31081, CVE-2024-31082, and CVE-2024-31083. Ubuntu also [fixed](#) other vulnerabilities affecting Firefox, including CVE-2024-29943 and CVE-2024-29944.

Notable vulnerabilities:

[CVE-2024-25096](#)



What happened: A remote code execution (RCE) vulnerability (CVE-2024-25096) in WordPress Canto Plugin allows a malicious actor to execute commands on the target website. This **CRITICAL** vulnerability has been assigned a CVSS score of 10.

- **What this means:** This vulnerability lets a threat actor gain backdoor access to take full control of the website. This vulnerability is not known to be fixed yet.
- **Affected products:**
 - WordPress Canto Plugin, up to version 3.0.7

[CVE-2024-3094](#)

What happened: CVE-2024-3094 is a vulnerability in the form of malicious code embedded in XZ Utils versions 5.6.0 and 5.6.1. XZ Utils is data compression software and may be present in Linux distributions. This **CRITICAL** vulnerability has been assigned a CVSS score of 10.

- **What this means:** Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library. Threat actors can leverage CVE-2024-3094 to gain unauthorized access to affected systems. CISA recommends developers and users to downgrade XZ Utils to an



uncompromised version—such as XZ Utils 5.4.6 Stable; they are also advised to look out for any malicious activity and report any positive findings to CISA. Researchers have released a free online scanner to detect Linux products infected with CVE-2024-3094.

- **Affected products:**

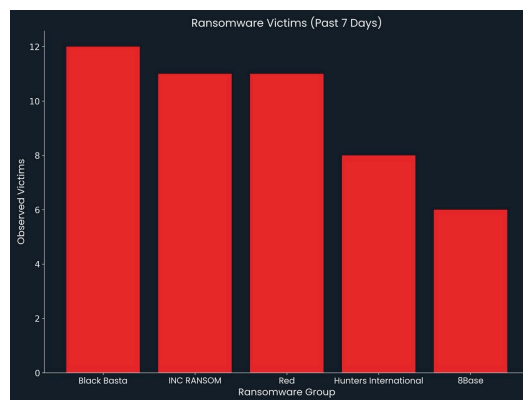
- XZ Utils version 5.6.0
- XZ Utils version 5.6.1

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings

LockBit Continues to Dominate Ransomware Numbers

What happened: ZeroFox reported an update on the [LockBit 3.0](#) ransomware leak site targeting Redwood Coast Regional Center (RDRC). The service provider's stolen data was uploaded on a DDW forum and RDRC was given until April 5 to pay the ransom. Jackson County, Missouri, has declared a state of emergency following a ransomware attack that disrupted several county services. The County Executive is reportedly mitigating the disruption caused by this attack by facilitating IT and emergency workers' requirements. At the time of writing, no ransom amount or threat actor communications have been disclosed. Additionally, Chilean data center and hosting provider IxMetro Powerhost fell victim to a cyberattack by a new ransomware gang called SEXi, which demanded a ransom of two bitcoins per victim (totaling USD 140 million for PowerHost). The ransomware adds the .SEXi extension to encrypted files and instructs victims to contact them via the Session messaging app. ZeroFox has observed more than 4,000 victims of ransomware in the past year.



Source: ZeroFox Internal Collections

- **What this means:** Healthcare providers are being increasingly targeted in ransomware attacks; threat actors take advantage of the fact that essential services cannot be indefinitely paused, which often leads healthcare victims to accede to ransomware demands. ZeroFox has observed the LockBit ransomware group successfully target over 50 organizations in the healthcare sector in the past year. As investigations proceed to determine the cause in the Jackson County ransomware attack, the county has taken steps to contain the attack and is working on restoring services. The disruption has impacted various services, including tax payments, online property records, and inmate search systems. In the Chilean data center attack, some customers' websites or services hosted on the company's VMware ESXi servers were inaccessible at the time of reporting.

Breach Intelligence: AT&T Confirms Data Breach

What happened: AT&T has confirmed that a data set released on a dark web forum comprises AT&T data-specific fields and affects 7.6 million current and 65.4 million former customers. The company

had initially denied that the leaked data set was associated with it, as reported in ZeroFox's Cyber Intelligence Daily Brief on March 18.



➤ **What this means:** The breach compromised sensitive personally identifiable information (PII), including full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, AT&T account numbers, and passcodes. The company has begun communicating proactively with impacted customers and is offering free credit monitoring. ZeroFox has also observed threat actor "MajorNelson" claiming to [leak](#) a database associated with AT&T on the predominantly English-language dark web forum BreachForums. AT&T has launched a robust investigation supported by internal and external cybersecurity experts.

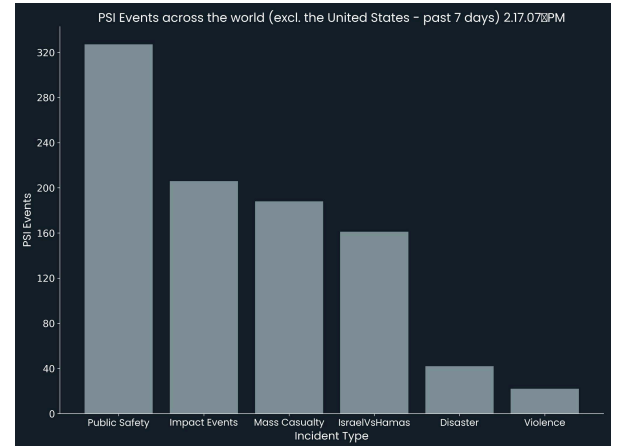
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

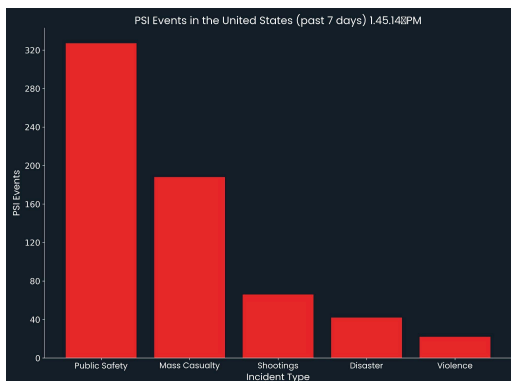
What happened: ZeroFox observed close to 1,400 instances of public safety alerts in the past week worldwide (excluding those in the United States, which have been analyzed separately below), with Europe being a major contributor to this number. Alerts relating to mass casualty events decreased to close to 250, indicating a decline of almost 38 percent in comparison to last week. Meanwhile, alerts for disaster-related events have spiked by almost 68 percent, with significant numbers from Asia. Incidents of violence have remained around 150.

- **What this means:** Natural disasters around the world have caught headlines this week. Taiwan witnessed its strongest earthquake in 25 years, with a recorded magnitude of 7.2. At least nine people were killed, and hundreds were injured. On April 3, Zimbabwe declared a state of disaster in response to a drought that has affected 80 percent of the country. Israeli Defense Forces (IDF) have canceled home leave for combat troops as a precaution against potential retaliation from Iran. The Indian government has reportedly assassinated individuals in Pakistan as part of a wider strategy to eliminate terrorists living in foreign territories.



Source: ZeroFox Internal Collections

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: ZeroFox Intelligence observed that Illinois, California, and New York accounted for the greatest number of public safety events, shooting instances/gun violence, and violent activity this week. In comparison to last week, Illinois recorded an almost 22 percent increase in shooting incidents, while California saw a 19 percent dip in public safety activity. In Pennsylvania, public safety incidents decreased by 34 percent, while shootings decreased by 45 percent from last week.

- **What this means:** A shooting incident in Crest Hill, Illinois, led to a short lockdown of Theodore Street. The suspects involved in the incident have been arrested. Meanwhile, a mass stabbing incident in the state left four people dead in about 20 minutes. The suspect claimed to be under the influence of marijuana following their arrest. Chicago also witnessed

shooting incidents over Easter weekend that claimed the lives of at least seven people and injured dozens.

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%