



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

March 4, 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 1, 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 – Hunters International Increases Ransomware Activity	2
ZeroFox Intelligence Brief – iSoon Data Breach and China's Geopolitical Strategy	2
ZeroFox Intelligence Flash Report – Increased Demand for X Accounts in Dark Web Forum	2
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 5	3
 Cyber Intelligence Key Findings	5
CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors Targeting Cloud Infrastructure	5
The White House Issues Executive Order to Protect Americans' Sensitive Personal Data	5
Iran-Linked UNC1549 Hackers Target Middle East Aerospace & Defense Sectors	6
 Deep and Dark Web Intelligence Key Findings	8
Actor Yuril33T Advertising Microsoft Outlook and Jenkins Remote Code Exploits	8
Actor Medusa Recruiting for Ransomware-as-a-Service Project on Multiple Forums	8
Threat Group Anonymous Sudan Carries Out DDoS Attacks Against Targets in Israel and Chad	9
 Exploit and Vulnerability Intelligence 	10
 Exploit and Vulnerability Intelligence Key Findings	11
CVE-2024-1597	11
CVE-2024-1981	11
 Ransomware and Breach Intelligence Key Findings	13
Ransomware Intelligence: LockBit Resurfaces with New Leak Site	13
Breach Intelligence: Threat Actor Leaks Data from Los Angeles International Airport	13
 Physical and Geopolitical Intelligence Key Findings	16
Physical Security Intelligence: Global	16
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	18
 Appendix B: ZeroFox Intelligence Probability Scale	19

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Flash Report – Hunters International Increases Ransomware Activity

Ransomware and digital extortion (R&DE) collective Hunters International has significantly increased its operational tempo, having so far conducted at least 29 attacks in February 2024. Hunters International is a ransomware-as-a-service (Raas) operation that was first observed in October 2023. Over the following quarter, affiliates leveraged the ransomware against a diverse set of global targets from an array of industries. Since Q4 2023, over 60 percent of R&DE attacks leveraging Hunters International ransomware targeted organizations based in North America. The most targeted industries are manufacturing, construction, and healthcare.

ZeroFox Intelligence Brief – iSoon Data Breach and China's Geopolitical Strategy

The iSoon data breach provides meaningful evidence that the Chinese Communist Party (CCP) leverages the Chinese private sector to achieve its geopolitical goals and illustrates the role the CCP has on priority-setting in the Chinese technology sector. The breach shows that contractors are used to target China's adversaries with cyberattacks designed to exfiltrate data in line with CCP's geopolitical priorities, which is then sold to Chinese state bodies. There is evidence from the breach to suggest China has deployed this strategy against targets with which it has geopolitical disputes. While the targeting of entities in these locations may be in line with CCP's geopolitical aims, it is unknown if these efforts are at the direction of the CCP.

ZeroFox Intelligence Flash Report – Increased Demand for X Accounts in Dark Web Forum

A new shop with exceptionally high numbers of social media accounts for sale, which first began trading under the name fireaccs[.]biz on dark web forum xss on January 4, is gaining momentum amongst threat actors. On the store, X (formerly Twitter) accounts are significantly more numerous and in demand compared to other social media platforms. This is very likely indicative of their favor amongst a wide array of threat actors, given the perceived benefits of operating on X to advertise, brag, or disseminate content to a wider audience than on other platforms.

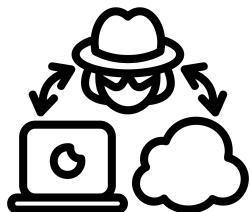
ZeroFox Intelligence Brief – Underground Economist: Volume 4, Issue 5

As of February 29, 2024, LockBit administrators remain committed to projecting the appearance of a fully-functioning and resilient R&DE operation. On February 16, 2024, well-regarded threat actor “skid_raper” announced in the English-speaking dark web community Omniforums that they are selling a zero-day vulnerability that affects the Go Programming Language’s (Golang) networking stack module. On February 14, 2024, untested English-speaking threat actor “authpress” announced the sale of a WordPress administrator authentication bypass zero-day exploit on the predominantly Russian-language dark web forum exploit[.]in. Despite many corporate websites having been built leveraging the tool, WordPress vulnerabilities are very commonly disclosed in open sources, with it widely regarded as one of the more vulnerable website building services. X accounts are significantly more numerous and in demand compared to other social media. This is very likely indicative of their favor amongst a wide array of threat actors, given the perceived benefits of operating on X versus other platforms. X accounts are almost certainly being increasingly implicated in various types of cybercrime that targets individuals and organizations.

| Cyber Intelligence |

| Cyber Intelligence Key Findings

CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors Targeting Cloud Infrastructure

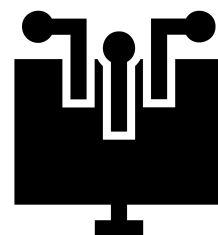


What happened: CISA and other international cybersecurity organizations have issued a joint advisory that provides an overview of recent tactics, techniques, and procedures (TTPs) deployed by Russian Foreign Intelligence Service (SVR) cyber actors, also known as APT29, the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard. In addition to outlining the TTPs used to gain initial access into the cloud environment, the advisory also includes advice to detect and mitigate such activities. The authoring agencies urged network defenders and organizations to review the joint advisory for recommended mitigations.

- **What this means:** As organizations continue to modernize their systems and move to cloud-based infrastructure, the SVR has adapted to these changes in the operating environment. The first line of defense against these actors should be to protect against their typical TTPs used for initial access. The advisory suggests organizations incorporate multi-factor authentication and ensure device enrollment policies are configured to only permit authorized devices. Organizations should also consider using various information sources (like application events and host-based logs) to help prevent, detect, and investigate potential malicious behavior.

The White House Issues Executive Order to Protect Americans' Sensitive Personal Data

What happened: The White House has issued an Executive Order to protect Americans' sensitive personal details including genomic, biometric, personal health, geolocation, and financial data and certain kinds of personally identifiable information—from exploitation by countries of concern. The Department of Justice (DOJ) and the Department of Homeland Security (DHS) are to work together to set high security standards to prevent access by countries of concern to Americans' data through other commercial means, such as data available via investment, vendor, and employment relationships.



- **What this means:** President Biden's Executive Order aims to safeguard Americans' sensitive personal data by enhancing collaboration between government departments. The DOJ and DHS will work together to establish stringent security standards, preventing countries of concern from accessing American data through various commercial channels. Additionally, the Departments of Health and Human Services, Defense, and

Veterans Affairs will ensure that federal grants, contracts, and awards do not facilitate access to sensitive health data by countries of concern, even through U.S.-based companies.

Iran-Linked UNC1549 Hackers Target Middle East Aerospace & Defense Sectors

What happened: A cyber espionage campaign targeting aerospace, aviation, and defense industries in the Middle East, including Israel and the United Arab Emirates (UAE), has been attributed to Iran-nexus threat actor “UNC1549.” Sources indicate other targets of the cyber



espionage activities likely include Turkey, India, and Albania. The attacks use Microsoft Azure cloud infrastructure for command-and-control (C2) and social engineering to disseminate two backdoors: MINIBIKE and MINIBUS. The spear phishing emails contain links to fake websites or phony job offers to deploy a malicious payload. The custom backdoors, upon establishing C2 access, act as a conduit for intelligence collection and further access into the targeted network.

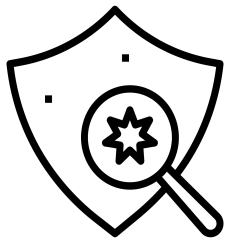
Tunneling software called LIGHTRAIL is also deployed to communicate with Azure cloud infrastructure.

- **What this means:** Security researchers suspect that the attackers are linked to Iran’s Islamic Revolutionary Guard Corps (IRGC). Moreover, the use of pro-Israel themed phishing messages (“Bring Them Home Now,” referring to the release of Israeli hostages) to deploy the backdoors suggest that the targets are primarily Israel’s allies.

| Deep and Dark Web Intelligence |

| Deep and Dark Web Intelligence Key Findings

Actor YuriL33T Advertising Microsoft Outlook and Jenkins Remote Code Exploits



What happened: On February 27, 2024, untested threat actor “YuriL33T” advertised Microsoft Outlook (CVE-2024-21413) and Jenkins (CVE-2024-23897) remote code execution (RCE) exploits on predominantly Russian-language dark web forum RAMP. The actor claims to be selling the Outlook exploit and the zero-day version of the Jenkins exploit to a single user through a guarantor for USD 150,000 and provides a link to a Proof-of-Concept (POC) for the Outlook exploit. The post—written in Russian and English—includes comments from other users questioning why YuriL33T is selling these exploits, as both are publicly available on GitHub.

- **What this means:** Since both exploits are publicly available—and the Jenkins exploit is no longer a zero-day despite YuriL33T selling it as such—the advertisement is not credible, and the actor is likely attempting to scam other users. However, it is also possible that YuriL33T was not aware that the exploits were public at the time of the original post. ZeroFox previously tracked YuriL33T’s activity in September 2023, which included posts about the sale of a Windows backdoor one-click exploit, access to a VT enterprise account, and the actor’s supposed private ransomware code. During this timeframe, YuriL33T also advertised a private tool that generates weaponized PDF files sold by ransomware developer SELENIUMCORE. Besides these instances, YuriL33T’s activity has not been consistent enough to confidently determine the trajectory of the actor’s future activity, but ZeroFox will continue to monitor for any updates.

Actor Medusa Recruiting for Ransomware-as-a-Service Project on Multiple Forums

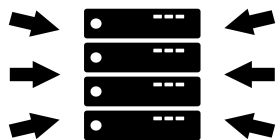
What happened: On February 24, 2024, threat actor “Medusa” (also known as Medusa_Official) was recruiting affiliates for their RaaS project called Medusa on the predominantly Russian-language dark web forum RAMP. Medusa advertised several features of the ransomware project. This actor has also posted on other dark web forums, including Exploit and xss, this year related to network access partnerships.



- **What this means:** Medusa ransomware was first observed in 2021 and started ramping up activity in 2023, when the group launched a data leak site. From December 2023 to present, Medusa ransomware has been one of the top 10 active

ransomware groups, with over 30 victims posted to their data leak site. The group actively recruiting more affiliates and partnering with network access brokers suggests that its activity could increase over the next few months as well.

Threat Group Anonymous Sudan Carries Out DDoS Attacks Against Targets in Israel and Chad



What happened: On February 28, 2024, threat actor group Anonymous Sudan carried out distributed denial of service (DDoS) attacks against targets in Israel and Chad. According to a post on the group’s Telegram site, the attacks against Israel reportedly affected seven universities and were carried out by “InfraShutdown,” a DDoS partner-for-hire. The attacks against Chad reportedly targeted the nation’s telecommunications and internet infrastructure.

- **What this means:** Anonymous Sudan has operated as a collective for multiple aligned hacktivist groups since early 2023. The group conducts attacks, typically DDoS, against nations for what it claims are “anti-Muslim” activities. Israel has been a primary target of the group since the onset of the Israel-Hamas war. Chad, a central African nation that borders Sudan, was reportedly targeted for allowing the presence of Rapid Support Forces (RSF) soldiers. RSF are paramilitary forces that Sudan’s government formerly operated. Anonymous Sudan is likely to continue DDoS attacks with an emphasis on Israel.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

[CVE-2024-1597](#)

What happened: CVE-2024-1597 is an SQL injection vulnerability in the PostgreSQL JDBC Driver under certain configurations. This **CRITICAL** vulnerability has the highest severity CVSS base score of 10. The affected versions are before 42.7.2, 42.6.1, 42.5.5, 42.4.4, 42.3.9, and 42.2.8 used with PreferQueryMode=SIMPLE.

- **What this means:** An attacker can exploit this flaw by crafting two user-controlled inputs: price and description. SQL injection attacks can allow threat actors to expose, manipulate, or gain complete control over databases.



[CVE-2024-1981](#)



What happened: The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to SQL Injection via the “table_prefix” parameter in version 0.9.68 due to insufficient escaping on the user-supplied parameter and lack of sufficient preparation on the existing SQL query. This **CRITICAL** vulnerability has a base score of 9.8.

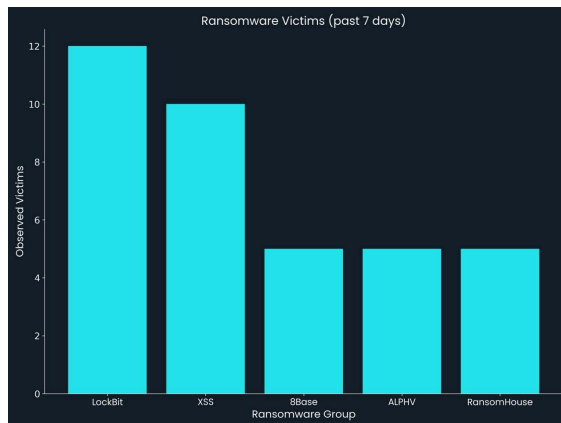
- **What this means:** This flaw makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

| Ransomware and Breach Intelligence |

Ransomware and Breach Intelligence Key Findings

Ransomware Intelligence: LockBit Resurfaces with New Leak Site

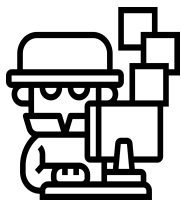
What happened: Despite recent law enforcement actions seizing their servers, the LockBit ransomware group has reemerged on the dark web with new infrastructure, including new mirror sites. A new shop with exceptionally high numbers of social media accounts for sale, which first began trading under the name fireaccs[.]biz on the dark web forum xss on January 4, is gaining momentum amongst threat actors. The FBI, CISA, and the Multi-State Information Sharing and Analysis Center have released a joint cybersecurity advisory on TTPs and IOCs associated with the Phobos ransomware variants.



Source: ZeroFox Internal Collections

- **What this means:** LockBit has shifted its data leak portal to a new .onion address on the TOR network and has listed more than 12 new victims, including a prominent U.S. federal agency. Threat actors are increasingly using X accounts to advertise, brag, or disseminate content to a wider audience than on other platforms. The Phobos ransomware group has frequently targeted municipal and county governments, emergency services, education, public healthcare, and other critical infrastructure entities.

Breach Intelligence: Threat Actor Leaks Data from Los Angeles International Airport



What happened: ZeroFox observed well-regarded and established threat actor “IntelBroker” claiming to leak a database associated with Los Angeles International Airport on the predominantly English-language dark web forum BreachForums. The threat actor claims the leaked database comprises 2.5 million records.

- **What this means:** IntelBroker has noted the data leak is from an alleged February 2024 data breach by user “kwilsy.” The sample data posted by Intelbroker indicates that the data includes company names, plane model numbers, CPA numbers, and personally identifiable information (PII) like full names and email addresses. Affected individuals and companies should be wary of unsolicited communication involving

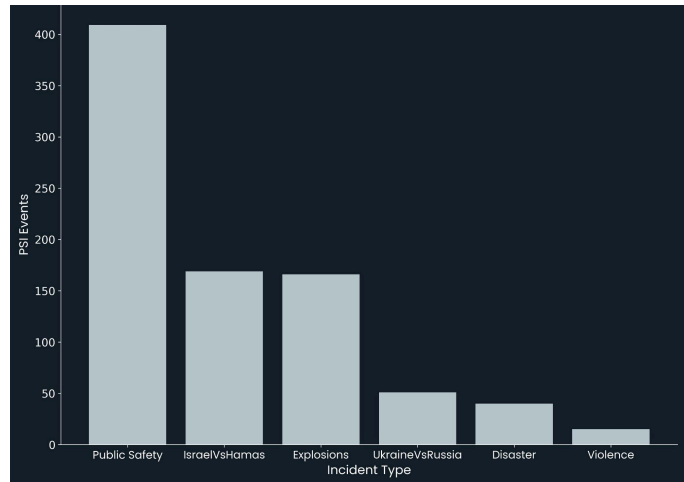
targeted emails or calls from unknown sources, as threat actors might use the leaked information for spear phishing attacks.

| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

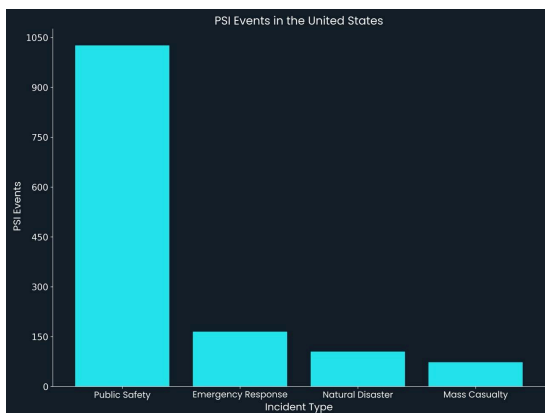
What happened: A Russian rocket has launched one Iranian satellite and 18 Russian satellites into space. Space experts have detected changes in the orbit of North Korea's first spy satellite, indicating that Pyongyang is successfully controlling it. North Korea launched Malligyong-1 in November 2023 after two failed attempts. Meanwhile, the Houthis have yet again struck the Red Sea, this time damaging four undersea communication cables between Djibouti and the Saudi Arabian city of Jeddah. As a result, internet connections were disrupted in the Gulf countries and India.



Source: ZeroFox Internal Collections

- **What this means:** Russia's launch of an Iranian satellite is likely a testimony to the increasing military cooperation between Russia and Iran in recent years. The North Korean Malligyong-1 has reportedly not shown any signs of performing other tasks or reconnaissance activities. As for Houthi-related actions, the attack on the underwater communication cables highlights continued Houthi willingness to find new ways to disrupt global operations in response to the Israel-Hamas war.

Physical Security Intelligence: United States



Source: ZeroFox Internal Collections

What happened: Some parts of the United States witnessed a series of weather events. Texas suffered wildfires which prompted an evacuation of 2,200 residents, who had to move to a safe space with their belongings and cattle. Other parts of the country experienced tornadoes and winter storms.

- **What this means:** A news source reported that the Texan wildfire on February 28 was the second largest recorded and spread across 850,000 acres. As the weather worsened on February 27, three million people across Ohio and Kentucky were placed under a tornado watch for February 28.

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%