



| Brief |

The Underground Economist: Volume 4, Issue 2

B-2024-01-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Vulnerability Exploitation, Botnets, Access
Sales, Geopolitical Threats

January 19, 2024

Scope Note

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 9:00 AM (EST) on January 19, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 2

| Citrix Vulnerabilities Continue to Be Exploited

On January 16, 2024, Citrix released a security bulletin urging consumers to update Netscaler ADC and Gateway appliances to mitigate against actively-exploited zero-day vulnerabilities CVE-2023-6548 and CVE-2023-6549, which impact the Netscaler management interface.

- If unpatched, the former enables an attacker to conduct remote code execution, and the latter can be leveraged in denial-of-service (DoS) attacks.

According to Citrix, the following versions of Netscaler ADC (formerly Citrix ADC) and Netscaler Gateway (formerly Citrix Gateway) are affected by the vulnerabilities:

- Netscaler ADC and Netscaler Gateway 14.1 before 14.1-12.35
- Netscaler ADC and Netscaler Gateway 13.1 before 13.1-51.15
- Netscaler ADC and Netscaler Gateway 13.0 before 13.0-92.21
- Netscaler ADC 13.1-FIPS before 13.1-37.176
- Netscaler ADC 12.1-FIPS before 12.1-55.302
- Netscaler ADC 12.1-NDcPP before 12.1-55.302

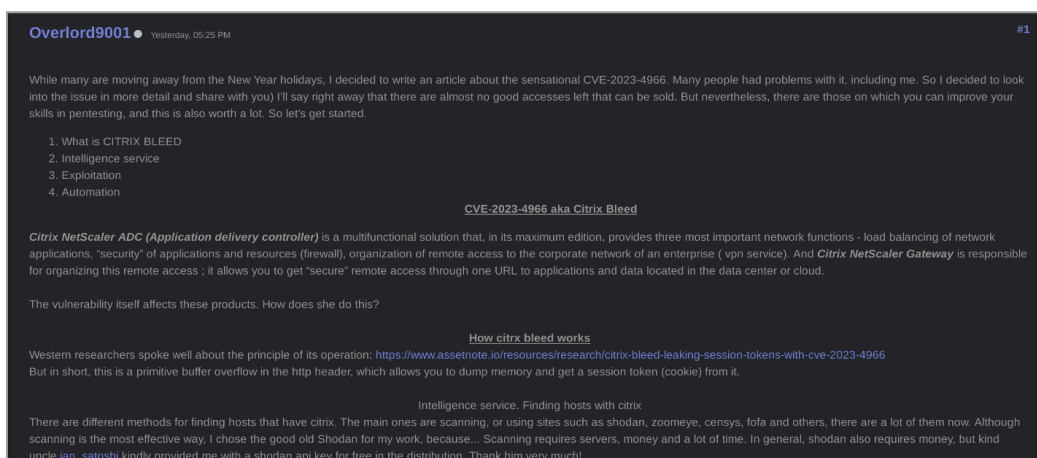
CVE-2023-4966, also known as “Citrix Bleed,” is also very likely still being targeted by threat actors. An article published as early as January 14, 2024, in primarily Russian-language dark and dark web forum xss is very likely indicative of a significant number of networks comprising Citrix Netscaler and Gateway appliances remaining unpatched and susceptible to the critical vulnerability.

The article is translated from an existing Russian publication and advises readers on:

- Finding and studying potential targets via open source search engine Shodan;
- Subsequently exploiting them via the use of “Choccapikk”—a tool readily available on developer platform GitHub; and
- Automating and replicating the attack process in order to exploit as many targets as possible.

The article was posted by a well-regarded threat actor in xss known as “Overlord9001” and received significant acclaim from both English and Russian-speaking actors.

- The notably positive reception of this article very likely indicates that threat actors still seek to exploit CVE-2023-4966.
- Despite its prominent reputation within deep and dark web (DDW) forums, many threat actors likely experience difficulties in leveraging the vulnerability to conduct subsequent attacks, such as gaining access to data centers associated with Citrix Netscaler appliances.



Screenshot of the article's introductory paragraphs

Source: ZeroFox Intelligence

CVE-2023-4966 is a critical-severity, remotely-exploitable security flaw that enables attackers to retrieve authentication session cookies from vulnerable Citrix Netscaler ADC and Gateway appliances. This can lead to the bypass of multi-factor authentication protocols and session hijacking, allowing subsequent network attacks to take place.

It was discovered and patched by Citrix on October 10, 2023, though significant exploitation took place both before its discovery and in the months following the patch's release. The vulnerability almost certainly continues to appeal to a variety of threat actors, including:

- Initial access brokers (IABs);
- Advanced Persistent Threat (APT) groups, such as FIN8; and
- Financially-motivated ransomware collectives, such as LockBit, MedusaLocker, and ALPHV—all of which have almost certainly exploited CVE-2023-4966 to conduct digital extortion campaigns.

We automate the process

It turns out that driving in cookies is a very exhausting task. Yes, it's interesting, but switching all these tabs and copying back and forth... And when there's nothing on the target yet... Monkey's work in general.

But that's why we're hackers, to automate the routine, and then get access and get high null

Therefore, for these purposes, let's add an exploit from Chocapikk to additionally perform the following actions:

1. When a target with valid cookies is found, a browser window will open, in which a citrix session with our cookies will open. We will do this through the selenium library. Also, using the threading library, we will create a semaphore to synchronize our sessions. So that our virtual machine or vps does not fall short of the number of accesses)
2. All IP users that are vulnerable to citrix bleed will be recorded in the new txt. Regardless of whether the cookies are valid or not. This is necessary in order to re-use citrix bleed on these targets in the future, because our access depends on whether the corporate employee is working.

Here's the code:

```
# https://github.com/Chocapikk/CVE-2023-4966

import re
import sys
import hexdump
import argparse
import requests

from rich.console import Console
from urllib.parse import urlparse
from alive_progress import alive_bar
from typing import List, Tuple, Optional, TextIO
from concurrent.futures import ThreadPoolExecutor, as_completed

warnings = requests.packages.urllib3
warnings.disable_warnings(warnings.exceptions.InsecureRequestWarning)

class CitrixMemoryDumper:
```

Guidance on process automation

Source: ZeroFox Intelligence

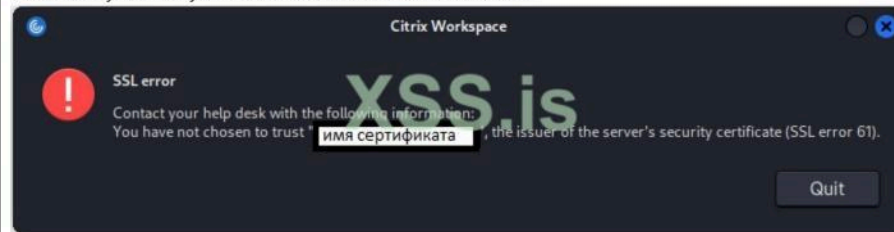
The article contains information that is likely intended to appeal particularly to ransomware collectives, due to the detail provided on delivering malicious payloads after gaining initial network access.

- This likely highlights continued interest in the Citrix Bleed vulnerability from ransomware and digital extortion (R&DE) collectives.
- There is a roughly even chance that newer, highly-active R&DE collectives observed during 2023, which are likely comprised of some less-experienced operatives of a lower technical sophistication, will benefit the most from guides such as these.

One aspect of the original article is not included in the translation. The missing section advises potential attackers on how to deal with an SSL error returned by Citrix Workspace upon attempting to connect to a remote desktop, which is noted as an effect of the successful implementation of the guide. The actor claims that, if the attack is conducted on operating system Linux, the process to circumvent this error is as follows:

- Obtain an SSL certificate in PEM format via an open source search engine;
- Change its extension to [.].crt;
- Copy it into a recognized/opt subfolder (i.e., the directory that contains non-default software packages); and
- Update the certificate store used by the Citrix client—a readily available and effective solution that could enable further attacks via Citrix Bleed.

After receiving valid sessions, search for remote desktops and connect to them. Odnako may not always be able to do this because of this error:



To solve it, you need to do the following:

1. Search Google for ssl certificate in PEM format
2. Save certificate with .crt extension
3. Copy the certificate from root to `/opt/Citrix/ICAClient/keystore/cacerts/`
4. Prescribe `sudo /opt/Citrix/ICAClient/util/ctx_rehash`
5. Reconnect

This method works under linux, I didn't look for a solution under Windows.

Guidance upon encountering SSL error

Source: ZeroFox Intelligence

The recent security bulletin from Citrix is very likely indicative of the continued targeting of Citrix Netscaler ADC and Netscaler Gateway appliances via the exploitation of CVE-2023-6548 and CVE-2023-6549. The publication is likely to prompt some consumers to install the latest security patches, but it is likely that additional attacks will continue.

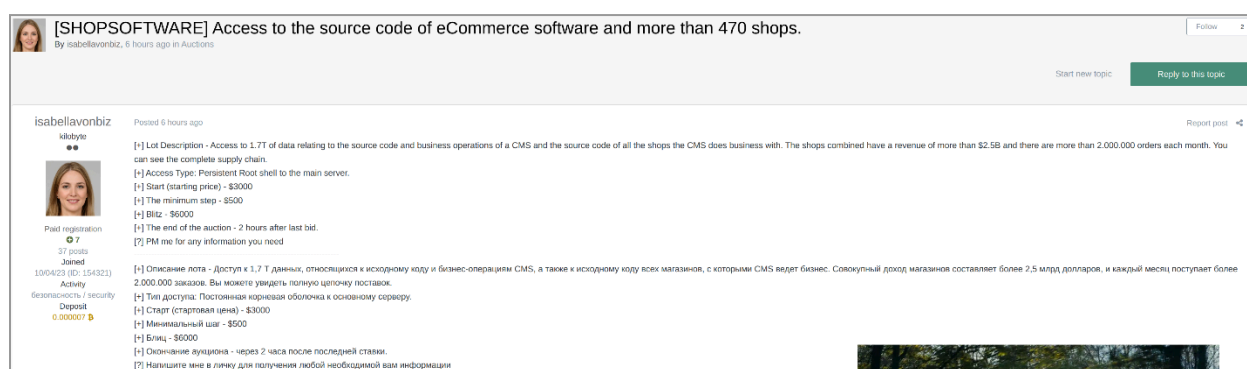
Should the article guiding the exploitation of CVE-2023-4966 prove intuitive and effective, it is likely that associated attacks will continue during the short term. Citrix Bleed is very likely to appeal to newer, financially-motivated R&DE collectives that previously lacked the technical expertise to exploit this vulnerability, as well as larger groups seeking to capitalize upon the likely sizable number of networks that have not been patched with the latest software.

Mass Access Sale to Retail eCommerce System

On January 15, 2024, well-regarded threat actor "isabellavonbiz" announced the sale of the source code, business operations data, and documentation of an unspecified eCommerce Content Management System (CMS) services vendor on the predominantly Russian-language dark web forum exploit[.]in. The actor claimed that the CMS is used by

470 vendors, totalling in excess of two million orders per month and a combined annual revenue of more than USD 2.5 billion. The package includes:

- The source code of all online retailers with which the CMS has business relationships;
- Approximately 1.7 terabytes of documentation; and
- Persistent root shell to the main server of the CMS. The threat actor claimed that the buyer would be able to observe the entire supply chain.



Exploit[.]in post advertising the CMS data and access sale

Source: ZeroFox Intelligence

The entire package was instantly purchased (or “blitzed”) by guru-level actor “s4l0_” for USD 6,000, leaving no chance for any competition. S4l0_ is a highly competent and popular threat actor, with additional intelligence indicating they are buying and potentially hoarding access to as many online shops as possible.

- In January 2024, ZeroFox observed a mass access sale featuring access to nearly a dozen U.S. WooCommerce online retailers.
- S4l0_ blitzed this deal as well, an hour after its announcement.

The access sale is likely indicative of an impending large-scale attack against the widely-used eCommerce CMS provider and may be part of a broader operation against retail targets. Since the start of 2024, ZeroFox has observed a continued high frequency of mass access sales targeting online retailers.

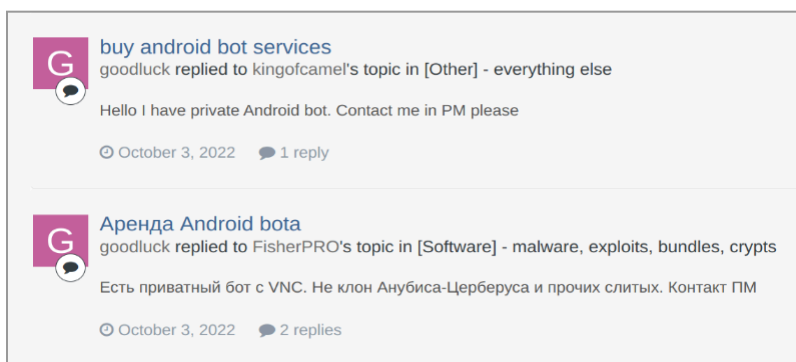
- Given the highly-specific targeting, it is likely the threat actor will seek to initiate a criminal financial scheme.
- This is most likely to take the form of a large-scale carding operation involving cashing out as many stolen credit and debit cards via the compromised shops' payment processors.
- It is also possible access will be leveraged by or sold to ransomware and digital extortion collectives for mass targeting of retailers.

| Likely Increased Threat from Android Malware Strain

On January 7, 2024, esteemed English-speaking threat actor "Red3vl" announced on DDW forum xss that they have obtained source code associated with an Android botnet called Octo Botnet, which first appeared as early as 2021 and was reported on by the information security industry by April 2022.

Access to Octo Botnet has previously been sold publicly in individual cases in which the developer—well-regarded Russian-speaking threat actor "goodluck" (aka "thearchitect")—responded to queries in the exploit[.]in DDW forum that were posted by those seeking Android botnet services.

- Such incidents were observed in October 2022, at which time the botnet was operational. Therefore, it is likely that Octo Botnet is currently between two and three years old and functioning semi-privately in order to prevent source code leaks and reverse engineering attempts.



Threat actor goodluck claiming to possess a private Android bot

Source: ZeroFox Intelligence

On November 24, 2023, goodluck announced in exploit[.]in that the Octo project would be canceled due to leaks of the source code by “entrepreneurs”, following the likely discovery of a vulnerability in the Octo admin panel. However, the actor claimed that production of Octo Botnet 2 had started, suggesting its expected appearance in January or February 2024.

- The actor also revealed information alluding to the functioning of “crypting services” on the DDW, which are able to steal privately-owned malware strains and reverse engineer them before exploiting any vulnerabilities discovered.

G

goodluck

byte

●

G

Paid registration

8

20 posts

Joined

08/07/20 (ID: 107085)

Activity

coding/coder

Android Octo bot official thread

By goodluck, November 24, 2023 in [Software] - malware, exploits, bundles, crypts

Posted November 24, 2023 (edited)

In connection with the emergence of “entrepreneurs” trying to sell the “leaked” Octo bot, I believe that the situation needs to be clarified.

<https://xss.is/threads/102527/> - they tried to sell the “leaked” Octo.

There was no leak, no one leaked the source. You can see the hucksters' panel - but it is available to any client, as it is installed on his server.
There is no such thing as a merged builder.

They only managed to replace the address of the panel in the finished apk file. This implies that the file is out of date. It can neither be fixed, updated, nor enhanced with new features.

What's more, **Octo doesn't really get the right to Android 13.** I'm discontinuing it and I'm working on the development of Octo 2.
Octo 2 will be released approximately in January-February 2024.

The official and only page of Octo <https://teletype.in/@thearchitect/101Tzn5v9G2-octobot>
(published December 2021)

The only contact is **Telegram @thearch001**
Either PM on exp or PM on XSS (nickname Architect)
<https://forum.exploit.in/profile/107085-goodluck/>
<https://xss.is/members/224534/>

I don't have resellers, support, publics, channels, jabber, or anything else.

It's all SCAM: <https://t.me/AndroidOctoBotnet>, <https://t.me/OctopusBotnet>, @octobot

Threat actor goodluck claiming to have started development of Octo 2

Source: ZeroFox Intelligence

Should the actor be credible, which is likely based upon their reputation and previous activity, this post is likely indicative of two separate threats:

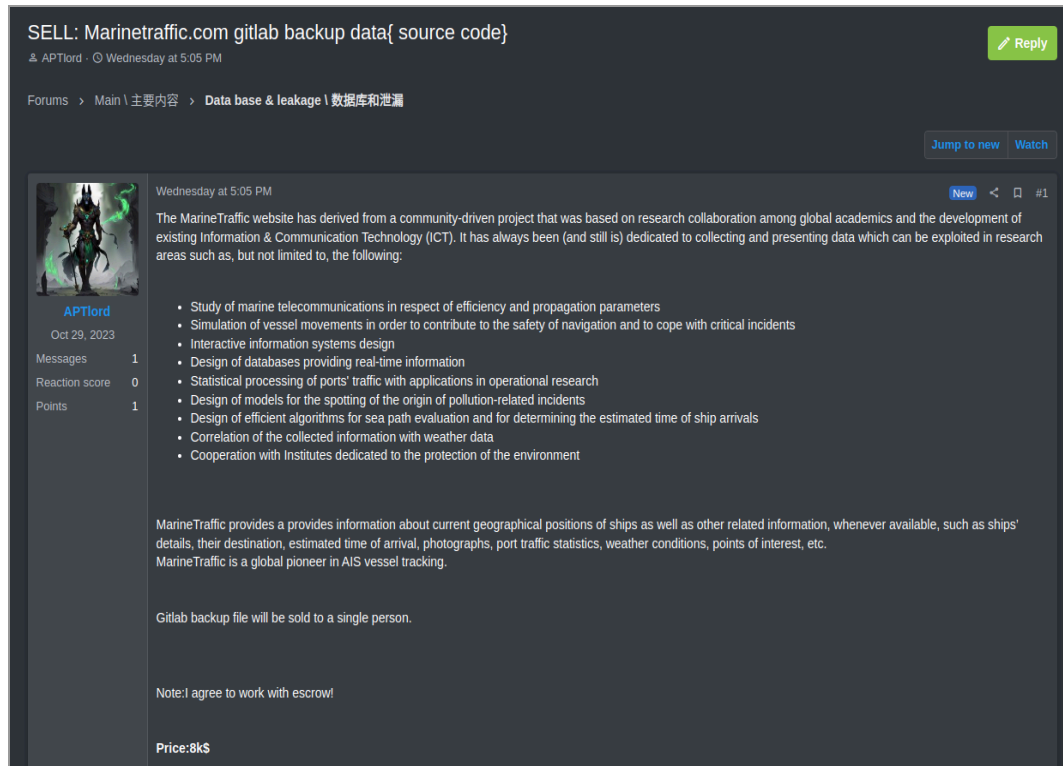
- It is likely that multiple, competent attackers now have access to a previously-private Android botnet following its source code leak. This poses an increased risk to global Android devices.

- Octo 2 is soon to be released in DDW marketplaces, as goodluck will likely be trying to compensate for losses created by the source code leak of its predecessor. Octo 2 will likely pose a severe risk to Android devices and consumers, particularly considering the significant demand for reliable Android botnet malware observed in DDW marketplaces.

| Dark Web Actors Promoting Maritime Data

On December 27, 2023, threat actor “APTlord” announced on dark web forum RAMP that they were selling source code and other information owned by marinetraffic[.]com, which was allegedly obtained by the theft of backup data from web-based Git repository GitLab. Marinetraffic[.]com is an open-source analytics platform that provides real-time information on maritime vessels and activity around the globe. Some of the information available includes:

- The geographic positions of vessels (accuracy and update frequencies vary between vessels);
- Vessel details (such as photographs, country of operation, speed, design, and other physical attributes);
- Journey details (such as originating locations, destinations, and expected arrival times); and
- Information relating to maritime infrastructure (such as port locations, capacity, traffic statistics, and weather conditions).

**RAMP post advertising the sale of source code owned by marinetrtraffic[.]com**

Source: ZeroFox Intelligence

Then, on January 13, 2024, threat actor “Drechsler” announced on the same RAMP forum that they had dumped the source code of Maritime Situation Inconsistency Analysis (ANAIS), a software used for the analysis of maritime space by the French Navy. ANAIS aims to aggregate and process maritime data more efficiently, especially in regards to suspicious or dangerous vessel behavior, in order to facilitate intervention decisions. ANAIS also allegedly features innovations in maritime research and intelligence pertaining to the development of maritime AI, among other things.

Problematic

The ANAIS project (for "Maritime Situation Inconsistency Analysis") aims to better aggregate maritime data to process it more efficiently. The objective is to better monitor the multiple activities at sea, and in particular detect suspicious or dangerous vessel behavior in order to decide more quickly and intervene more effectively. The idea is to start by working on the global flow of ship positions coming from the European Maritime Safety Agency, in collaboration with the Maritime Affairs Directorate. This basic data will be enriched throughout the project by other data sources and analyzed in greater detail.

Goals

Keep the agile team as close as possible to operational users Regularly secure developments to deploy more widely Make a lighter version of ANAIS available to the academic world to deepen the algorithm

Results

Concrete and recognized operational contribution
Testing of an innovative method and tool by the Navy.
Issues of digital sovereignty and development of maritime AI
ANAIS is accessible by invitation link

About the source code :

- Git history included, so you can see history
- about 50 MB of content (compressed)
- Estimated cost of creation of this software, for french military services, according to data leaked, is \$800/day for 2 developers since late 2018 = At least \$1m (lowest estimation)
- Software deployed to french aircraft carrier, according to another leak

RAMP post advertising the sale of source code for ANAIS software

Source: ZeroFox Intelligence

On the same day, Drechsler also published another French military-related leak of management software "Les alpps," which is used by the 27th Mountain Infantry Brigade. The software aims to facilitate mountain training operations and improve reaction time in the event of an accident during such operations.

[Free][Army related][France] Software that manage internship for 27th Mountain Infantry Brigade

▲ Drechsler · Saturday at 3:27 PM

Forums > Main \ 主要内容 > Data base & leakage \ 数据库和泄漏

[Jump to new](#) [Watch](#)

 Saturday at 3:27 PM [New](#) < > #1

As we want to proof our claim about accessing french military code bases, we're releasing here the source code of "Les alpps" for free, because estimated value is low.

Archive password : rampio

<https://ufile.io/kzn7qkuq>

mirror <https://file.io/gSaALP18ZEHg>

About the software, translated from french via deepl

Drechsler
Nov 21, 2023
Messages 2
Reaction score 0
Points 1

RAMP post advertising the sale of French Army training software Les alpps

Source: ZeroFox Intelligence

Making mountain outings safer for militaries**Context**

The EMHM (Ecole Militaire de Haute Montagne), part of the 27th Mountain Infantry Brigade, employs military and civilian mountain instructors, all experts in their field. These instructors focus primarily on two crucial activities: Training and assessing trainees. Mountain training, in both summer and winter, to ensure they remain seasoned in this dangerous and demanding environment. As part of these activities, not only instructors, but also all qualified people who need to train, must prepare their itinerary when they go into the mountains, and submit it to their corps leader for validation. This procedure, known as FACM (Fiche d'Activité à Caractère Montagne), enables them to be covered in the event of an accident, but also to inform their comrades of their itinerary and timetable, so as to facilitate the activation and intervention of emergency services in case of need.

Issues

The FACM application and validation procedure is based on a paper form requiring the approval and signature of several parties. This inflexible process can be laborious, and sometimes leads to people leaving without a FACM. The assessment of trainees, the planning of training courses and the processing of their results is also a lengthy process involving multiple players. To avoid a multiplication of tools, EMHM wanted a single tool on which its staff could manage their two main activities.

Objectives

Simplify the creation and processing of FACMs to optimize the responsiveness of sights and signatories, and reduce processing times.

Maximize FACM coverage for mountain outings

Manage courses and evaluate trainees according to given skill criteria

Have an application accessible via Milistore

RAMP post advertising the sale of French Army training software Les alpps

Source: ZeroFox Intelligence

In the first hack on December 13, 2023, APTlord asserts that some of the website's research areas—such as interactive information systems design, design of databases providing real-time information, and correlation of the collected information with weather data—can be exploited. However, the price requested for the data is USD 8,000, and the threat actor claims that the information will only be sold to a single buyer. This is at odds with most disclosures on the DDW, where profit-seeking is the primary motive.

In the two attacks on January 13, Drechsler does not mention a price but claims the ANAIS software itself is worth USD 1 million. However, ZeroFox assesses that the value of the leaked source code in terms of the ability of the purchaser to profit is close to zero. Rather, the value of these leaks may be ideological, and threat actors selling or purchasing the data may be inspired by other attacks on maritime targets.

It is unclear how this information could be directly leveraged to facilitate attacks against maritime targets—especially given the abundance of maritime data already publicly available. However, Houthi rebel attacks in the Red Sea region since mid-November have had significant impacts on international trade and demonstrate the vulnerability of international shipping.

- About half the vessels that normally transit the Red Sea have decided to take a longer and more expensive journey around southern Africa instead, adding 10 days to the journey and millions in additional costs.
- The cost to ship from Asia to Northern Europe has increased by 176 percent in one week ending January 11.¹ The cost of the Asia-to-U.S. East Coast route, which also traverses the Red Sea, has increased 50 percent in a week.
- There have also been cost increases on routes that avoid the area. The Asia-U.S. West Coast route has seen a 50 percent jump in costs due to more companies using it as an alternative supply chain.² There are also the added costs of delivering goods by truck or rail from the U.S. West Coast to their intended destination on the East Coast.

Threat actors may view the success the Houthis have had at disrupting global trade along a key supply chain that handles 12–15 percent of global trade³ and attempt to apply it elsewhere. Possible targets include the Malacca Strait between Indonesia and Malaysia, which handles 28 percent of global trade; the South China Sea, responsible for 30 percent; and the East China Sea, which handles 21 percent.⁴

Recent data leaks on the RAMP forum do not align with the typical profit-making schemes on the DDW. However, geopolitically-engaged threat actors may nevertheless see value in such leaks if they can be used to achieve their goals or harm their adversaries. The increasing regularity of these sorts of leaks could be tied to the growing convergence of geopolitical tensions and cyber threats.

¹ [hXXps://www.freightos.com/january-10-2024-update/](https://www.freightos.com/january-10-2024-update/)

²

[hXXps://www.supplychaindive.com/news/ocean-freight-rates-continue-climb-red-sea-crisis-Suez-Canal/704386/](https://www.supplychaindive.com/news/ocean-freight-rates-continue-climb-red-sea-crisis-Suez-Canal/704386/)

³ [hXXps://www.bbc.com/news/business-67980256](https://www.bbc.com/news/business-67980256)

⁴

[hXXps://www.bloomberg.com/opinion/articles/2024-01-14/supply-chains-canal-aren-t-the-biggest-shipping-chokepoints](https://www.bloomberg.com/opinion/articles/2024-01-14/supply-chains-canal-aren-t-the-biggest-shipping-chokepoints)

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%