ADVERSARIALLY

weekly report

Feb 1 -8 , 2024

by

XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Feb 1 - 8, 2024

XG3 UNIT

Adversary of the Week

Azure Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Healthcare

Activity: Cybercrime

TTPs: Leak of confidential information

TA866

Type: Group

Countries:

Maturity:

Sectors: All

Activity: Information theft and espionage

TTPs: **Phishing**

LockBit 3.0

Type: APT

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: **41**

ADVERSARIALLY
weekly report
Feb 1 - 8, 2024

XG3 UNIT

Global

- A new variant of the **FritzFrog botnet** has been detected with new features such as **exploiting the Log4Shell vulnerability** to spread internally within an already compromised network. It also **exploits the CVE-2021-4034** vulnerability to achieve local privilege escalation.

- Threat actor **TA866** has **returned** after a period of inactivity with a **phishing campaign** in which it is **deploying the WasabiSeed and Screenshotter** malware. It is primarily targeting North American users.

- Actor **Ruby Cosmos Taurus** sells valid login **credentials of AnyDesk** users for $15k on a private Russian forum. It is estimated that around **18,000 accounts** have been compromised.

- **Private data,** such as parts of the source code, internal passwords or technical diagrams **of Binance, were available** to everyone for several months **in a GitHub repository**. The extent of the leak and the actor or group that carried out the attack are not yet known.

- Vietnam-based threat group **Lion Security Team** has announced on its Telegram channel that it **is part of Killnet 2.0** as of 31 January.

- A new threat group called **"ResumeLooters"** has **compromised 65 legitimate websites** and **stolen data** from more than **2 million people** using **SQL injection and XSS attacks**. It targets Australia, Taiwan, China, Thailand, India, and Vietnam and steals private information such as names, phone numbers, and more.

- A new website called **OnlyFake** claims to use neural networks to **generate realistic photos of fake IDs for $15**, disrupting the fake identity and cybersecurity market. This technology generates fake IDs, non-existent faces with AI and random signatures, which **could be used for bank fraud**, account verification by document **or laundering stolen funds**.

ADVERSARIALLY
weekly report
Feb 1 - 8 , 2024

XG3 UNIT

Spain & Portugal

- New denial-of-service attacks by the **NoName057** group against Spanish companies have been reported from 5 February to the present. The victims are Moncloa, the Constitutional Court, the Ministry of Economy, the Tax Agency, the company S2Group, transport websites of several autonomous communities, the websites of the navy and the air force and several autonomous city councils such as Murcia or Navarra.

- The **town hall of Sant Antoni** has been the **victim of a ransomware attack** by an as yet unknown actor, which has paralysed all activity in the computer systems.

- Actor **Beluga Cosmos Taurus** sells on a well-known forum on the darkweb, **access via Fortinet Master** of the Spanish company **Telefónica.** The price is only communicated privately via Telegram or TOX.

- Actor **Mimosa Cosmos Taurus** sells the **database** of the Spanish company **FootDistrict** on a well-known dark web forum. It consists of 943k lines of private customer information from all over Europe.

- Actor **Chive Cosmos Taurus** sells on a well-known dark web forum the **database** of an unknown **Spanish telecommunications company**. It includes information such as phone numbers and passwords.

- Actor **Crimson Rigel Taurus** sells on a dark web forum the **database** of a Spanish occupational health and safety agency **and FTP access**.

- Actor **Illuminating Cosmos Taurus** sells on a private Russian forum access via SQLI and the database of an unknown Spanish energy company with a revenue of 1$ billion.

- The **Foundation for the Development of Nursing (FUDEN)** acknowledged having **suffered a security breach** in which data of 50,000 Spanish nurses has been exposed. The ransom demanded and whether it is an individual actor or a ransomware group is unknown.

- A **new phishing campaign impersonating Correos** has been detected. This is because the entity **didn't have a DMARC registration** in its official domain for communications.

ADVERSARIALLY
weekly report
Feb 1 - 8 , 2024

XG3 UNIT

LATAM

- Actor **Saffron Cosmos Taurus** offers in a well-known private forum administrator access to the website of the Ministry of Justice of Argentina.
- Actor **Saffron Cosmos Taurus** offers access credentials from the Buenos Aires Ministry of Security in a well-known private forum.
- Actor **Azure Cosmos Taurus** sells access to a $23 million revenue health organisation in Brazil for $500 on a popular forum.
- Actor **Azure Cosmos Taurus** sells access to a $20 million revenue health organisation in Brazil for $300on a popular forum.on a popular forum.
- Actor **Amberglow Cosmos Taurus** markets access to the internal network of a casino in Peru for USD2,200.
- A new **phishing campaign** has been detected in Mexico **offering a modified** version of an open-source **remote access Trojan called AllaKore RAT**. Targets include the retail, agriculture, public sector, manufacturing, transportation, business services, capital goods and banking sectors.

ADVERSARIALLY
weekly report
Feb 1 - 8 , 2024

XG3 UNIT

Vulnerabilities & Exploits

- Four vulnerabilities cataloged with **CVE-2024-21626, CVE-2024-23651, CVE-2024-23652 and CVE-2024-23653** have been detected, affecting **runc, BuildKit, Moby and Docker Desktop components**. These vulnerabilities could lead to unauthorized access to the host file system, in addition to compromising the build cache.

- Has been resolved the critical vulnerability cataloged as **CVE-2024-23832** that affected **Mastodon** and with which attackers could impersonate users and hijack their accounts. This was due to **insufficient source validation**.

- Two new critical vulnerabilities have been detected in **FortiSIEM** catalogued as **CVE-2024-23108 and CVE-2024-23109** which allow unauthenticated attackers to execute commands via specially crafted API requests. They are currently under investigation as they **are related to a primary vulnerability listed as CVE-2023-34992.**

- **Update:** In connection with the **CVE-2023-46805** vulnerability and the significant risk of security breaches posed by compromised Ivanti VPN devices, **CISA has required** all federal agencies to "**disconnect all instances of the Ivanti Connect Secure and Ivanti Policy Secure solution** products from agency networks" as soon as possible.

- It has been detected that a **vulnerability in the BitcoinJS library**, which although already fixed, could be **causing wallets created between 2010 and 2015 to be vulnerable to real attacks**. The vulnerability consists in the **low security of the passwords** of the wallets generated with this library.

ADVERSARIALLY
weekly report
Feb 1 - 8, 2024

XG3 UNIT

⚠ Warning of the week

- FritzFrog's Sneaky Comeback: **Watch out for Log4Shell** making a comeback! Patch up those vulnerable assets pronto to stop its internal party. Keep those peepers peeled on Log4Shell – patching game is strong.

- FortiSIEM Alert: **Urgent Action Required**! Two new vulnerabilities, CVE-2024-23108 and CVE-2024-23109, in FortiSIEM's backyard. Unauthenticated attackers playing command games! Under investigation related to CVE-2023-34992. Remember to apply the patches!

- CISA demands federal agencies disconnect Ivanti Connect Secure and Ivanti Policy Secure solutions ASAP. Significant security risks at play! **Check if your Ivanti products are affected!** Don't say we didn't warn you...

- TA866 Phishing Encore: Guess who's back? TA866, hitting North America with a fresh phishing campaign. Brush up those defenses against **WasabiSeed and Screenshotter** – they're up to mischief.

- Ruby Cosmos Taurus' Credential Carnival: **Hold up, AnyDesk users**! Credentials up for grabs at a mere $15k. Time for a **credential check** and a watchful eye on those accounts.

- Binance's Oops Moment: Sensitive data out in the open on GitHub! It's review time – check those **security protocols** and keep an eye out for anything fishy.

- ResumeLooters' Web Extravaganza: 65 websites compromised – not your usual Tuesday. **Strengthen those web defenses**, especially if you're chilling in Australia, Taiwan, China, Thailand, India, or Vietnam.

- NoName057's Spanish Serenade: DDoS attacks on Spanish companies – not the salsa we were expecting. **Check and fortify those defenses**, and keep an eye on network vibes.

- Correos' Phishing Fiesta: Hold the phone – Correos impersonators in town. Watch out for suspicious Correos messages and **double-check their authenticity**.

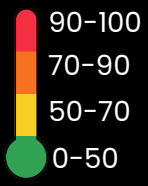
ADVERSARIALLY
weekly report
Feb 1 - 8, 2024

XG3 UNIT

Detections by Risk

Top 5 Weekly Rules Added/Updated by Adversary Rule Risk:

- Download detected using different Powershell methods **(68.5)**
- Potential Linux webshell execution **(68.5)**
- Potential Rose Flamingo loader filename **(66.5)**
- External connections to internal RDP services **(65)**
- WMI executing suspicious commands **(61.5)**



Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores
Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores
Rules with all or some of these features: Medium attack techniques, risky adversaries, trending (or not) Mitre TTPs, medium CVE scores
Rules with all or some of these features: Low attack techniques, not related to any adversaries, trending (or not) Mitre TTPs, low CVE scores

Top MITRE Covered

- Exploitation for Client Execution
- Command and Scripting Interpreter
- Server Software Component
- External Remote Services
- Proxy

Adversary Trends

Actors

Volt Typhoon
UNC2452
APT29
UTA0178
Strom-1567

Set Tools

COATHANGER
KrustyLoader
QUIETBOARD
NSPX30
Kasseika

Vulnerabilities

Jetbrains / CVE-2024-23917
Ivanti / CVE-2024-21893
Oracle / CVE-2024-20931
Google / CVE-2024-1283
Php / CVE-2023-46914

ADVERSARIALLY
weekly report
Feb 1 - 8, 2024

XG3 UNIT

Ransomware

Total Victims = 90 (+13)

- Spain - **3** (+1)
- Latam - **7** (+4)
  WorldWide - **80** (+5)

The king is...

Data of the week

Top Countries

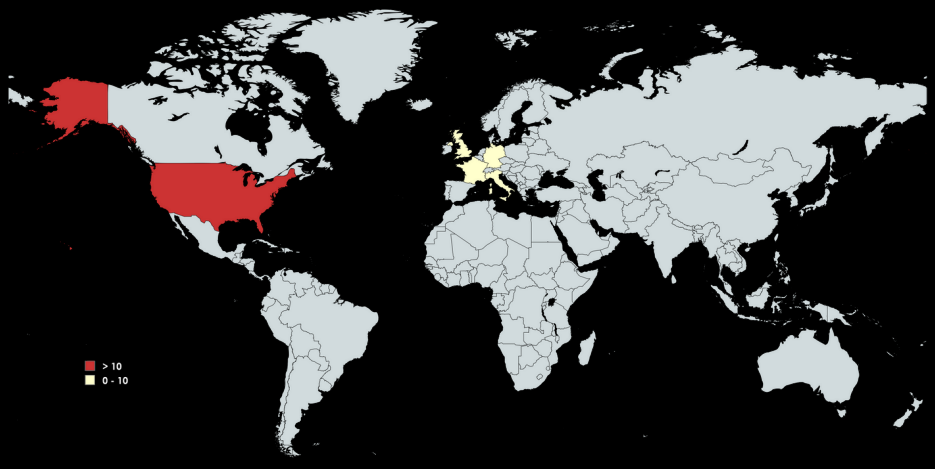
- USA - **43** (+3)
- GBR - **9** (+3)
- FRA - **4** ☆
- DEU - **3** ☆
- ITL - **3**

Top Sectors

- Services - **20** (+11)
- Manufacturing - **13** ☆
- Health - **7** (+1)
- Financial - **6**
- Telecom - **5** ☆

Top Groups

- Lockbit - **26** (+18)
- Play - **14** ☆
- 8Base - **10** (+1)
- BianLian - **7** (+1)
- Knight - **5** ☆



Victims

- **Ransom Victim:** Portline | Group: LockBit | Sector: Logistic | Country: Portugal
- **Ransom victim:** CNPC Peru | Group: Rhysida | Sector: Energy | Country: Peru
- **Ransom victim:** Derrama Magisterial | Group: Lockbit | Sector: Services | Country: Peru
- **Ransom victim:** Lex Caribbean | Group: Lockbit | Sector: Services | Country: Barbados
- **Ransom victim:** Digitel | Group: Medusa | Sector: Telecoms | Country: Venezuela
- **Ransom victim:** TGestiona | Group: Lockbit | Sector: Logistic | Country: Brazil
- **Ransom victim:** FEPCO Zona Franca | Group: Knight | Sector: Industrial | Country: Colombia
- **Ransom victim:** Abel Santos & Asociados | Group: Knight | Sector: Healtcare | Country: Argentina
- **Ransom victim:** SPB | Group: Cactus | Sector: Manufacturing | Country: Spain
- **Ransom victim:** Gocco | Group: Cactus | Sector: Retail | Country: Spain
- **Ransom victim:** San Antoni town council | Group: Unkwon | Sector: Government | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Feb 1-8, 2024

cipher

a Prosegur company