ADVERSARIALLY

weekly report

Feb 29 - Mar 7, 2024

by

XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

Adversary of the Week

ResolutionBlue Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Defense

Activity: Cybercrime

TTPs: Leak of confidential information

Saffron Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Government

Activity: Cybercrime

TTPs: Leak of confidential information

Play

Type: Group

Countries:

Maturity:

Sectors: Government, Finance, Media.

Activity: RaaS

TTPs: **32**

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

Global

- A new **phishing kit** named **CrypoChameleon** has been detected being used to target the cryptocurrency industry, mainly **targeting** employees of companies such as **Binance, CoinBase** and **users of cryptocurrency applications.** This phishing attack masquerades as login pages of various applications and combines it with phishing attacks via emails, SMS and voice messages to obtain users and passwords.

- A **new variant of the BIFROSE** or Bifrost RAT has been discovered **targeting Linux** systems. The malware is **used by** the Chinese state group **BlackTech** and has targeted organisations in Japan, Taiwan and the United States.

- **American Express credit cards exposed in vendor data breach**. The company said that the breach occurred at one of its service providers used by their travel services division, American Express Travel Related Services Company. led to **customers'** American Express Card **account numbers, names, and card expiration data** being accessed by the hackers.y the hackers.

- **Pepco** employees have fallen **victim to a sophisticated phishing attack** in which threat actors gained unauthorised access to financial systems and **stole approximately $15 million**.

- Actor **USC Gold Cosmos Taurus** sells private data such as full names, numbers, telephone numbers, confidential documents, photographs, etc. about the FBI on a well-known English forum for $499.

- A possible **attack by the STORMOUS ransomware group on the Tox** service has been detected. This is a widely used messaging service in the cybercriminal ecosystem, so depending on what **data** the group may have had access to and what Tox actually holds, it could be **highly confidential and coveted.**

- **Anonymous Sudan** claims credit for the **DDoS attack launched against Facebook and Instagram.** There is strong speculation that the group leaked hundreds of thousands of login credentials for both platforms. At the moment the group has only announced information regarding the DDoS on its usual channels.

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

Spain & Portugal

- Database of a **Spanish notary's office** is up for sale on the Dark Web. The threat actor claims to have **150GB of sensitive documents**, including 400 passports and contracts. The starting price is $1000.

- The company **Enplast** has been **compromised by the 8Base ransomware** group. The compromised data reportedly included invoices, receipts, accounting documents, personal data, certificates, employment contracts, confidentiality agreements and personal files.

- Actor **ResolutionBlue Cosmos Taurus X** offers on a well-known English forum **180MB of private data** such as full names, numbers, telephone numbers of the **Association of Official Tourist Guides of Madrid.**

- Actor **ResolutionBlue Cosmos Taurus X** offers on a well-known English forum 80MB of information from the software development company **Sof Pro XE.**

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

LATAM

- Actor **Coral Blue Cosmos Taurus** offers on a well-known Dark Web forum, 7GB of documents, files and source codes from the **Subsecretaría de Telecomunicaciones (SUBTEL)**.

- Actor **Saffron Cosmos Taurus** offers on a well-known English DarkWeb forum a **database** with private personal information of 325 agents of the **National Police of Peru**.

- Actor **RaspberryPink Cosmos Taurus** shared a database from APROA (Asociación Propietarios de Automotores y Mandatarios del Automotor) with almost 1.200.000 rows.

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XGB UNIT

Vulnerabilities & Exploits

- An alleged **remote code execution (RCE) exploit** for Microsoft Office has been detected being sold by an unknown actor. This actor claims to possess an **exploit capable of executing commands via cmd/powershell.**

- Researcher **Samip Aryal discovered a zero-click flaw** that could allow an attacker to **take control of any Facebook account by forcing a specific type of nonce**. He described the flaw as a rate-limiting problem at a specific endpoint in Facebook's password reset flow.

- The **Lazarus Group** have **exploited** a vulnerability listed as **CVE-2024-21338**, which allowed threat actors to gain kernel-level access and disable security software on compromised hosts.

- A critical vulnerability listed as **CVE-2024-21413** has been detected in **Microsoft Outlook**. This vulnerability allows an attacker to **remotely execute code (RCE)** when opening an email. It **also allows circumventing Office Protected View, opening malicious files in edit mode** instead of protected mode and infecting computers without taking any action on the email.

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

⚠️ Warning of the week

- Cryptocurrency lover! Guard against **CryptoChameleon phishing**. Verify URLs, avoid random links and **enable two-factor authentication**. Keep apps and **systems updated**🛡️

- The name **BIFROSE** rings a bell! It's **against your Linux system**! Update it regularly and use reliable security software. Beware of unknown downloads or links and activate firewalls. Keep your digital door locked! 🔒

- Stay vigilant with your American Express! 💳 Monitor statements regularly and report suspicious activity ASAP. Enable transaction alerts and two-factor authentication. Use unique passwords and be cautious with third-party services

- Alert ⚠ a **RCE exploit for Microsoft Office** has been detected! **Update immediately**. Avoid sketchy files or links. Keep a tidy digital space, and be wary of unexpected messages.

- You've heard about the **Facebook** mess 🌐 ! **Strengthen passwords**, enable **multi-factor authentication** and keep everything up to date. **Beware of suspicious links**, check your Facebook privacy settings and keep an eye out for suspicious messages.

- It appears that Microsoft Outlook 💻 has a vulnerability (**CVE-2024-21413**)! **Update your Outlook**, keep your defences in "safe festival" mode and remember, never invite that suspicious attachment to the dance floor!

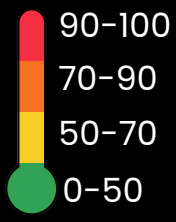
ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

Detections by Risk

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

- Cobalt Strike malleable (OCSP) profile **(74)**
- Cobalt Strike malleable OneDrive browsing traffic profile **(74)**
- Possible HIVE ransomware execution **(67.5)**
- Connections to remote LDAP servers **(66.5)**
- Linux password dump tools **(62.5)**



90-100 *Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores*

70-90 *Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores*

50-70 *Rules with all or some of these features: Medium attack techniques, risky adversaries, trending (or not) Mitre TTPs, medium CVE scores*

0-50 *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

- Application Layer Protocol
- User Execution
- Data Encrypted for Impact
- Exploitation for Client Execution
- OS Credential Dumping

Adversary Trends

Actors

Volt Typhoon
Lazarus Group
APT28
APT29
Kimsuky

Set Tools

GTPDOOR
WINELOADER
LITTLELAMB.WOOLTEA
LockBit-NG-Dev
GoldPickaxe

Vulnerabilities

Jetbrains / CVE-2024-27198
Linux / CVE-2022-48629
Ivanti / CVE-2023-38035
Ca / CVE-2024-2048

ADVERSARIALLY
weekly report
Feb 29 - Mar 7, 2024

XG3 UNIT

Ransomware

Total Victims = 115 (+26)

- Spain - **2** (+1)
- Latam - **1** (-1)
- WorldWide - **112** (+26)

The king is...

Data of the week

Top Countries

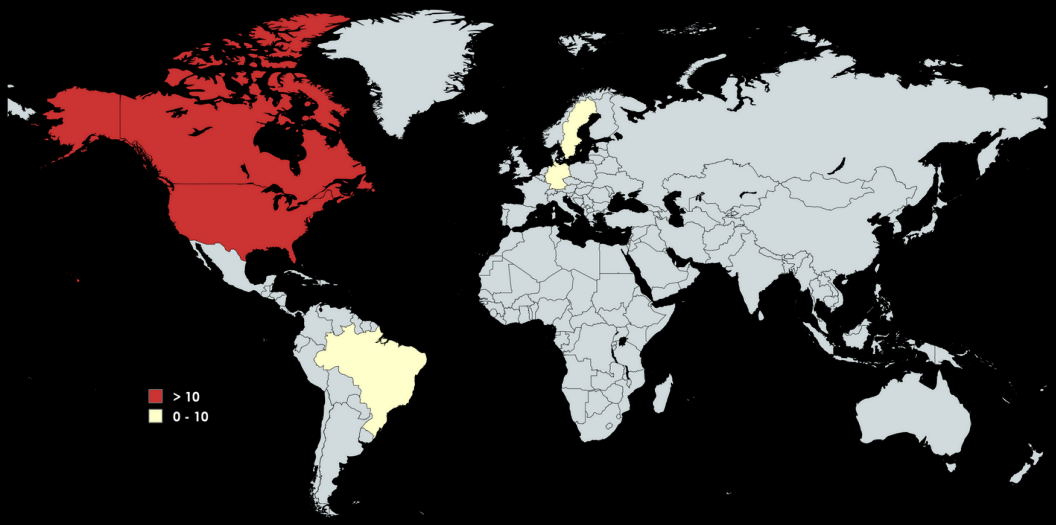
- USA - **51** (+10)
- CAN - **12** (+9)
- DEU - **5**
- SWE - **4**
- BRA - **3**

Top Sectors

- Services - **23** (+3)
- Industrial - **20**
- Health - **10** (+1)
- Transport - **6** (+2)
- IT- **6**

Top Groups

- Play - **18**
- Lockbit - **17** (+8)
- Cloak - **11**
- ALPHV - **8** (-1)
- Medusa - **8** (+2)



Victims

- **Ransom Victim:** Enplast | Group: 8base | Sector: Manufacturing | Country: Spain
- **Ransom victim:** Hotel Avenida Palace, Hostal Espoz y Mina, Hostal Arriazu, Pension Alemana | Group: Trigona | Sector: Services | Country: Spain and Portugal
- **Ransom victim:** Shooting House | Group: RansomHub | Sector: Services | Country: Brazil
- **Ransom victim:** Everplast | Group: Stormous | Sector: Manufacturing | Country: Brazil
- **Ransom victim:** YKP LTDA | Group: RansomHub | Sector: Other | Country: Brazil

xMDR

ADVERSARIALLY

weekly report

Feb 29 - Mar 7, 2024

cipher

a Prosegur company