WR X

Adversarially

Weekly Report

Mar 21 – Abr 4, 2024

2024

XG3 UNIT

xMDR powered by Cipher

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

Adversary of the Week

SandyTaupe Cosmos Taurus

Type: Individual

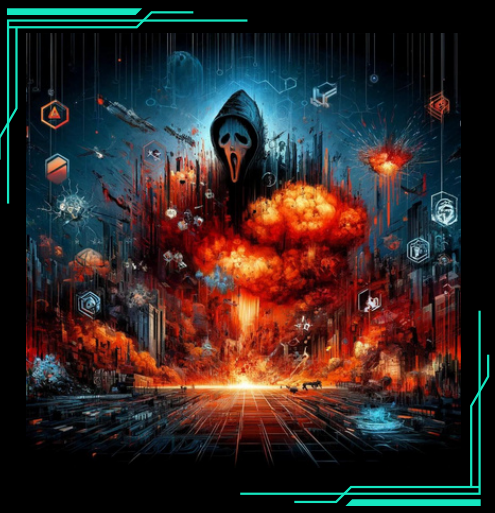
Countries:

Maturity:

Sectors: Government

Activity: Cybercrime

TTPs: Defacement



Kill Security

Type: Group

Countries:

Maturity:

Sectors: Finance, Government

Activity: Ransomware

TTPs: Indeterminated yet

BlackBasta

Type: Group

Countries:

Maturity:

Sectors: Health, Chemical, Logistic, Automobile...

Activity: RaaS

TTPs: 32

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

Global

- **Periwinkle Cosmos TaurusX** a **member of the CyberNiggers** group, announced on a well-known English forum that they have **obtained classified and private information from the United States National Security Agency.**

- In investigations related to the incident that **Air Europa** experienced in October, the company **has detected unauthorized access** subsequently, during which **attackers** may have **obtained private personal data from an undetermined number of customers.**

- There has been observed a **growth in electronic scams targeting individual objectives**, such as those carried out through phishing, **impersonating platforms like Booking or Airbnb**, taking advantage of the Easter holidays that have occurred in recent days.

- **New ransomware** group has been identified as **Kill Security**. It's a group that **seizes opportunities and vulnerabilities** to indiscriminately attack sectors and countries. Recently, attacks have been known to range from **targeting the Police in India or Romania to the Bank of India.**

- The **United States accuses** the threat groups **Islamic Revolutionary Guard Corps** of the Iranian Government and **Volt Typhoon** of **targeting critical infrastructure** and companies responsible for the supply of **drinking water and wastewater.**

- A **malware campaign named Sign1** has been detected, **infecting 39k Wordpress** websites. Victims are **redirected to fraudulent sites** through **malicious JavaScript injections.**

- A **new variant of TheMoon malware** botnet has **infected** nearly **7k ASUS routers** in a week. The attack could **be carried out** through **vulnerability exploitation**, although the **use of brute force** to obtain access passwords is not ruled out.

- A new threat group called the **Dark Army Hacking Group** has been discovered. It **comprises cybersecurity experts, hackers, pentesters**, and researchers **from the Republic of China and the Russian Federation.** They have a website on TOR, but no victims have been reported yet.

- A new group called **Phantom** is **recruiting members** through its Telegram channel **to carry out significant attacks against various targets.**

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

Spain & Portugal

- The **City Council of TorrePacheco** has **suffered a ransomware attack**, which may have **affected the data of residents** of the municipality. The attack was detected when the Local Police did not have access to their server.

- The political group **Podemos has suffered a cyber-attack** in which criminals have **stolen private information of registered members**, as well as information on the economic management of the group.

- The threat group **EvilMorocco** claims on its Telegram channel to have **hacked** the website of the **General Access Point of the Spanish Administration.**

- **Rebeccapurple Cosmos Taurus** claims on a well-known English forum to have **gained access to the servers of the political party Podemos**, **deleting 30GB** of information and **performing a defacement**. Additionally, they claim to **be in possession of private information** such as ID numbers, names, surnames, etc.

- **Prepay Technologies**, the company responsible for the recharge network of **Aucorsa**, the municipal bus company of Cordoba, has been the **victim of a cyberattack**, resulting in all the recharge stations in the city becoming inoperative.

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

LATAM

- The Argentinean prepaid healthcare company **Medifé** has suffered a **ransomware attack**. It should be noted that no known ransomware group has claimed responsibility for the attack.

- **LordPeña, a member of MexicanMafia,** has carried out an **attack** against the **Tax Administration Service (SAT)** portal, making **use of a reflected XSS vulnerability**, which allows the attacker to execute JavaScript code in the users' web browser.

- **SandyTaupe Cosmos Taurus** offers for free on a well-known English forum, a database of the National Registry of Persons with more than 110k images of Argentine citizens. In addition, the personal identification number is also displayed.

- **PinkSherbet Cosmos Taurus** offers in a well known English forum, a database of more than 11k records with email addresses and private information such as names belonging to the Police of the province of Rio Negro, Argentina. To obtain the complete database he offers his contact in TOX.

- **Team R70** claims to have carried out **DDoS attacks on 8 airport** websites in **Brazil**, including Salvador International Airport and Rio Branco International Airport.

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

Vulnerabilities & Exploits

- A critical vulnerability, listed as **CVE-2024-3094**, has recently been discovered that primarily affects **Linux distribution** systems, specifically **versions 5.6.0 and 5.6.1 of the open source XZ Utils** compression toolkit. Is a backdoor implemented in the aforementioned distributions that was initially thought to allow attackers to bypass sshd authentication (the OpenSSH server process) and remotely gain unauthorised access to the operating system, however after further investigation it has been concluded that **it is a remote code execution vulnerability**. The backdoor intercepts a function, verifies the signature with a fixed key and if successful, **executes malicious code** passed through the host without leaving a trace in the sshd logs. **The discovery** of this vulnerability has been **attributed** to engineer and developer **Andrés Freund**. The **backdoor was apparently implanted** via code commits in a GitHub project called Tukaani by a user called Jia Tan (JiaT75), who has been contributing to the project for 2 years.

- Active exploitations of the new vulnerability **CVE-2023-48788** in FortiClient EMS have been detected since Sunday, March 24, 2024. This has resulted in unauthorized installations of Atera Agent, ScreenConnect, and Meterpreter.

- On a popular Russian forum, a threat actor claimed to have exploited an RCE in FortiOS, offering a complete version 2 payload of **CVE-2024-21762** for sale. CVE-2024-21762 enables attackers to execute unauthorized code or commands via specially crafted requests in certain versions of Fortinet FortiOS.

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

⚠️ Warning of the week

- Linux lovers, beware of the sneaky backdoor **CVE-2024-3094**! **Update XZ Utils ASAP** and close the door to those uninvited intruders. Remember, even penguins need security guards: keep your Tux safe and sound! 🐧🔒

- Don't let **scammers ruin your holiday**: keep your cyber shield on! Remember: if it seems too good to be true, it's probably a scam. Be vigilant, avoid phishing messages and always check the addresses of the websites you visit 🔒💰

- Beware of **Sign1**: it seems that not even WordPress sites are safe from this digital graffiti artist. Stay alert: update plugins and keep an eye out for suspicious scripts! 🛡️💻

- Looks like **TheMoon** is going on a router rampage! If you have an ASUS-branded router, pay attention: update the firmware, strengthen the passwords and don't let cyber-lunatics into your network. 🌕🔒

- Uh-oh, **FortiClient EMS got caught napping**! Keep your shields up: **patch soon as posible**, lock the door on sneaky Atera Agents, and don't let Meterpreter crash your party. Stay vigilant, and keep those digital bouncers on high alert!🛡️🚪

- Looks like **FortiOS** has a chink in its digital armor! Don't let cyber crooks crash your Fortinet fortress: patch up, stay alert for suspicious requests, and keep those unauthorized code-crashers out of your digital domain!💻

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

Detections by Risk

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

- Suspicious remote connection from Rundll32 **(87.5)**
- Executing BASH files from a URL **(73.5)**
- Active Directoy Enumeration via Powershell **(73.5)**
- Local Privilege Escalation via Powershell **(73.5)**
- Pwdump usage tool detection **(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

- Command and Scripting Interpreter
- System Binary Proxy Execution
- Account Discovery
- Hijack Execution Flow
- OS Credential Dumping

Adversary Trends

Actors

APT31
Volt Typhoon
APT29
UNC2452
Storm-0558

Set Tools

UNAPIMON
Sing1
AcidPour
VCURMS
PhantomBlu

Vulnerabilities

Wordpress / CVE-2024-2879
Tukaani / CVE-2024-3094
Php / CVE-2024-24724
Vmware / CVE-2024-22246

ADVERSARIALLY
weekly report
Mar 21 - Abr 4, 2024

XG3 UNIT

Ransomware

Total Victims = 106 (+26)

- Spain - **1**
- Latam - **3** (+2)
  WorldWide - **102** (+24)

The king is...

Data of the week

Top Countries

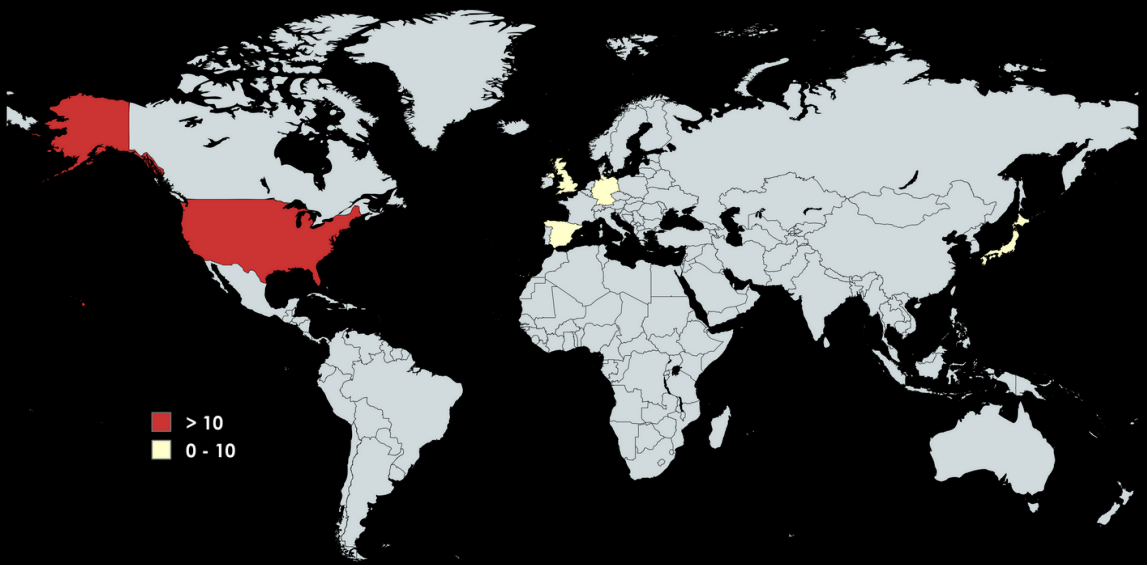
- USA - **47** (+10)
- DEU - **6** (+1)
- GBR - **3** (-3)
- ESP - **2** ☆
- JPN - **2** ☆

Top Sectors

- Manufacturing - **23** (+9)
- Services - **18** (+1)
- Technology - **6** ☆
- Others - **6** (+1)
- Health - **5** (+1)

Top Groups

- BlackBasta - **18** (+12)
- Play - **15** ☆
- Redransomware - **12** ☆
- Lockbit - **10** (-10)
- Incransom - **10** ☆



Victims

- **Ransom Victim:** casajove.com | Group: LockBit3 | Sector: Commercial Services | Country: Spain
- **Ransom Victim:** C&C Casa e Construção | Group: Ra World | Sector: Consumer & Retail | Country: Brazil
- **Ransom victim:** Grupo Equatorial Energia | Group: Cloak | Sector: Energy | Country: Brazil
- **Ransom victim:** HC Querétaro | Group: 8BASE | Sector: Manufacturing | Country: Mexico

xMDR

ADVERSARIALLY

weekly report

Mar 21 - Abr 4, 2024

cipher

a Prosegur company