WR X

Adversarially

Weekly Report

APR./ 11-18

2024

XG3 UNIT

xMDR powered by Cipher

ADVERSARIALLY
weekly report
Abr 11 - 18, 2024

XG3 UNIT

Adversary of the Week

Delicious Cosmos Taurus

Type: Individual

Countries: 🇦🇷

Maturity: 🟩⬛⬛

Sectors: Government

Activity: Cybercrime

TTPs: Exploit Public-Facing Application

TA558

Type: Group

Countries: 🇺🇸 🇧🇷 🇨🇴

Maturity: 🟧🟧⬛

Sectors: Finance, Industrial,Government

Activity: Cybercrime

TTPs: 19

Hunters International

Type: Group

Countries: 🇺🇸

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 23

Global

- **Sisense** has fallen **victim to a cyberattack** in which **threat actors gained** access to the company's Gitlab code repository and found a token that allowed them **access to the company's Amazon S3 repositories**. The cybercriminals **obtained sensitive information from their customers** such as tokens, credentials, and access configurations.

- The **University Hospital of Düsseldorf** fell **victim** to a **ransomware** carried out by an undisclosed actor or group, **which resulted** in the collapse of the hospital and, as a consequence, the **death of a patient** who had to be transferred to another hospital located 30 km away.

- A darknet vendor, **googleXcoder**, has **advertised** a sophisticated **BEC software** integrated with artificial intelligence. This software, purportedly developed by the GXC Team, offers advanced features for **manipulating business invoices** by automatically **swapping bank details** such as IBAN and BIC codes on invoices. The software **can detect and edit PDF invoices from incoming emails.**

- **Update: RansomHub** has begun **leaking** what they claim are stolen corporate and **patient data from United Health's subsidiary, Change Healthcare**, in what has been a long and intricate extortion process for the company.

- **Ukrainian Blackjack** hacking group claims to have **damaged emergency detection** and response capabilities in Moscow and beyond the Russian capital **using** a destructive ICS **malware** dubbed **Fuxnet**.

- A joint **law enforcement** operation conducted by the Australian Federal Police (AFP) and the FBI resulted in the **arrest and charging of two individuals suspected of creating and selling the Firebird RAT**, which was later renamed as Hive.

- A new campaign conducted by the **TA558** hacking group is concealing **malicious code inside images** using steganography **to deliver various malware** tools onto targeted systems.

- **Periwinkle Cosmos Taurus X** is offering **documents from the cyber company Space-Eyes**, a geospatial intelligence firm, on a well-known English forum. These documents are said to **contain sensitive and confidential information** that could be related to the **national security of the U.S. government.**

Spain & Portugal

- **Waterspout Cosmos Taurus** X sells on a Russian-speaking forum unauthorized shell access to the web pages of two Spanish stores for $2000.

- The Dutch school supplies company **Iddink**, based in Catalonia and supplying schools, has been the **victim of a cyberattack** carried out **by the Cactus group**, which may have obtained personal information of customers such as names, addresses, phone numbers, or bank account numbers.

- **Richcarmine Cosmos Taurus** X sells Anydesk access with domain user privileges of a Spanish architecture company.

LATAM

- **Red Cosmos Taurus** X offers on a well-known English forum over 12k documents containing private and confidential information for the Peru Military.

- **Darkolivegreen Cosmos Taurus** X offers on a well-known English forum full source code for more then 25 companies from Uruguay and databeses with queries and developer comments.

- **Delicious Cosmos Taurus** X sells through Telegram for $3000 a database with all driver's licenses from Argentina, which contains 5.7 million records.

Vulnerabilities & Exploits

- A new **critical vulnerability** with a score of 10 has been discovered, assigned **CVE-2024-3400**. It's a command injection vulnerability **in Palo Alto Networks' PAN-OS software**, allowing an unauthenticated attacker to **execute arbitrary code** with root privileges on the firewall. The U.S. Cybersecurity and Infrastructure Security Agency (**CISA**) **added** said vulnerability to **its catalog of known exploited vulnerabilities.**

- **BarnRed Cosmos Taurus X sells** a **zero-click RCE exploit** for use against **Android and iOS devices** on a well-known English-speaking forum. For more information or price inquiries, they provide their contact on Telegram.

- **Remote Code Execution (RCE) vulnerability affecting Telegram** has been discovered. It is **due** to a typo writing **the extension .pyzw as pywz**, which allows attackers to automatically execute potentially malicious Python files.

⚠️ Warning of the week

- Keep your devices safe from **zero-click nasties! Update** your phone's operating system **ASAP**, avoid sketchy links and attachments, and **use reputable security software**. Don't let cyber-criminals waltz into your digital worldt! 📱🔒

- Yikes! Time to **fortify your Palo Alto Networks firewall**! **Patch pronto—updates** are your cyber-shield. Keep an eye out for suspicious activity, and limit access to your firewall. Don't let cyber-crooks seize control! 🛡️💻

- Uh-oh, **Telegram's got a typo trouble**! Stay safe: update your Telegram app pronto to **patch the glitch**. Avoid opening suspicious files, especially those with funky extensions. Don't let cyber-tricksters sneak into your chats—keep your app secure!📱🔒

- Watch out for shady offers like **BEC software**—it's like handing your wallet to a cyber-thief! Keep your guard up: e**ducate staff about BEC scams**, use email filters, and **double-check any changes** to financial documents! 💰🔒

ADVERSARIALLY

weekly report

Abr 11 - 18, 2024

Detections by Risk

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

- Potential oRAT HTTP request **(72.5)**
- Use of RDP tools from Linux **(70)**
- Potential PuppetLoader command line execution **(68.5)**
- 7za automated file extraction **(57.5)**
- Service creation using chkconfig Linux utility **(54)**

🟥 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

- Ingress Tool Transfer
- Application Layer Protocol
- Exploitation of Remote Services
- Remote Access Software
- Command and Scripting Interpreter

Adversary Trends

Actors

APT31
Sandworm
Volt Typhoon
APT29
UNC2452

Set Tools

UPSTYLE
SEXi
Byakugan
UNAPIMON
Sing1

Vulnerabilities

Paloaltonetworks / CVE-2024-3400
Fortinet / CVE-2023-48788
Tp link / CVE-2023-1389
Linux / CVE-2024-26915
Git / CVE-2024-31497

ADVERSARIALLY
weekly report
Abr 11 - 18, 2024

XG3 UNIT

Ransomware

Total Victims = 127 (+17)

- Spain - **3** (+2)
- Latam - **3**

WorldWide - **121** (+15)

The king is...

Data of the week

Top Countries

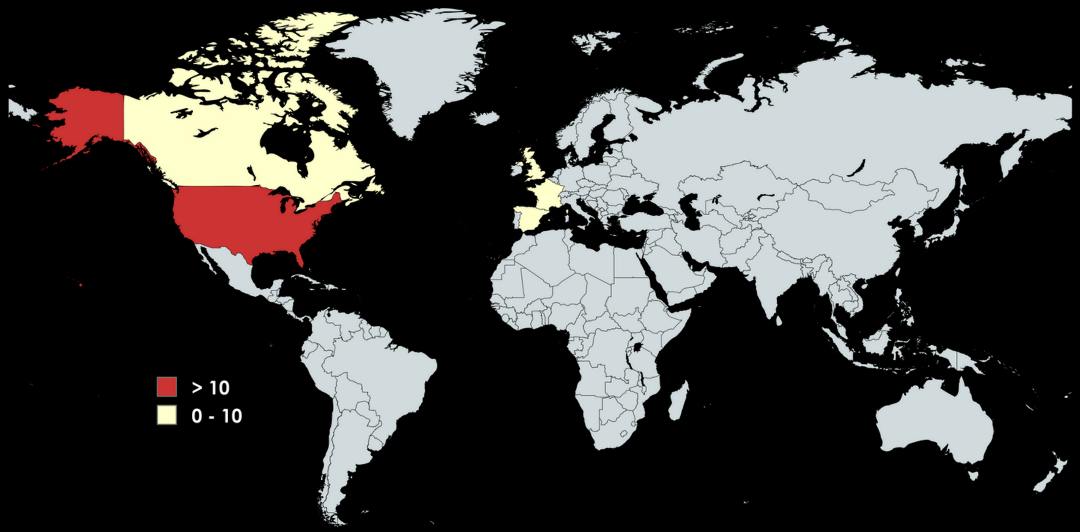
- USA - **75** (+19)
- GBR - **8**
- CAN - **6** (-1)
- FRA - **5** ☆
- ESP - **3** ☆

Top Sectors

- Technology - **18** (+7)
- Manufacturing - **14** (-11)
- Healthcare - **10** (-5)
- Transportation - **7** ☆
- Engineering - **7** ☆

Top Groups

- hunters - **16**
- darkvault - **16**
- play - **11**
- lockbit3 - **10**
- raworld - **9**



Victims

- **Ransom Victim:** Energía del Bajo Putumayo | Group: ransomhub | Sector: Energy | Country: Colombia
- **Ransom Victim:** Toyota Brazil | Group: hunters | Sector: Manufacturing | Country: Brazil
- **Ransom Victim:** qint.com.br | Group: darkvault | Sector: Technology | Country: Brazil
- **Ransom Victim:** Lopesan Hotels | Group: ransomhouse | Sector: Tourism | Country: Spain
- **Ransom Victim:** Grupo Cuevas | Group: ransomhub | Sector: TBD | Country: Spain
- **Ransom Victim:** Gimex | Group: raworld | Sector: TBD | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Abr 11 - 18, 2024

cipher

a Prosegur company

LEGAL NOTICE: PROHIBITION OF DISTRIBUTION, USE OR SHARING WITHOUT AUTHORIZATION This document (hereinafter, “the Document”) is the exclusive property of Prosegur Ciberseguridad S.L. (hereinafter, “the Owner”). The Owner possesses all intellectual property rights associated with the Document, including, among others, copyright and property rights. Access to this Document is granted only to parties authorized by the Owner for the specific purpose of confidential evaluation.

Any distribution, reproduction, unauthorized use, disclosure or sharing of the Document, in whole or in part, with third parties without the prior and express written authorization of the Owner is strictly prohibited. Any unauthorized use of the Document will constitute a violation of the Owner’s intellectual property rights and may result in legal action. Access and use of this Document are subject to the terms and conditions established by the Owner. Any authorized party that receives the Document must comply with the restrictions and obligations established by the Owner.
Any questions or requests for authorization for distribution, reproduction or use of the Document should be directed to the Owner.

Failure to comply with these restrictions may have legal consequences. By accessing or using the Document, you accept and acknowledge the terms of this legal notice.