ADVERSARIALLY weekly report

Feb 22 - 29 , 2024

by XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Feb 22 - 29, 2024

XG3 UNIT

Adversary of the Week

LulzSec

Type: Group

Countries: 🇦🇷

Maturity: 🟩⬛⬛

Sectors: Defense

Activity: Cybercrime

TTPs: Leak of confidential information

UAC-0184

Type: Group

Countries: 🇺🇦

Maturity: 🟧🟧⬛

Sectors:

Activity: Information theft and espionage

TTPs: 22

BlackCat

Type: APT

Countries: 🇺🇸 🇪🇺 🇯🇵 🇦🇺

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 189

🌍 Global

- Insurance company UnitedHealth Group has confirmed that its subsidiary **Optum Solutions** has been the **victim of ransomware**. The **attack targeted** the largest payment exchange platform between doctors, pharmacies, providers and patients in the US, **Change Healthcare**, on which Optum operated. The attack has led to the **shutdown of hundreds of hospitals, pharmacies and health services** across the US.

- **Update: LockBit reappears** 5 days after the FBI's breach of its TOR site with a new .onion address and announces its next steps. In the release they have published, they tell what happened, acknowledging that they had been breached by a **CVE corresponding to PHP** that they had not corrected because they had **"become lazy**". In addition, samples have been discovered that point to the **development of a new ransomware variant**, LockBit 4.0.

- A campaign against **Ukrainian entities** located in Finland has been detected by the threat actor **UAC- 0184**, which **distributes Remcos RAT via the IDAT Loader**.

- A number of hacktivist groups, including factions derived from **LulzSec and Anonymous**, among others, have been detected via Telegram joining together to carry out joint operations. Further **hacktivist activity** is therefore to be expected in the short to medium term.

- An attack **paralyses car body production** at the automotive division of the **ThyssenKrupp Group**. For the time being, it has only been acknowledged that it was an unauthorised access to its infrastructure, and that the systems were switched off as a temporary security measure. No information is yet available on the actor who may have been responsible.

Spain & Portugal

- Actor **Saffron Cosmos Taurus** offers in a well-known forum the database of the Catalan governmental institution "Forestal Catalana SA (FCSA)". It includes user, email, name, surname, phone number, password, activation key, etc.

- Actor **ResolutionBlue Cosmos Taurus** sells for $100 webshell access to the Generalitat Valenciana's subdomain "gva.es".

- Actor **Yellow Betelgeuse Taurus** offers in a Telegram channel a Spanish government database with 12k records of names, surnames and ID cards.

- Following the **cyber-attack** suffered by the **Regional Transport Consortium** last November, the **theft of private data**, including names, telephone numbers and addresses, of **holders of Public Transport Cards of the Community of Madrid has been confirmed.**

- A **man has been arrested in Murcia** for the discovery and disclosure of secrets for having **obtained the data of more than 40 million vehicle number plates** by **taking advantage of a computer vulnerability** in the Public Administration website to extract data corresponding to several autonomous communities such as Andalusia, the Balearic Islands and the Canary Islands.

ADVERSARIALLY
weekly report
Feb 22 - 29, 2024

LATAM

- Actor **Saffron Cosmos Taurus** offers in a well-known forum the databases of the Argentinean insurance companies "Seguros Sura", "Libra Seguros", "Galeno Seguros", "Provincia Seguros" and "Experta Seguros". The leaks contain a multitude of pdf files with personal data of each insured or policies.

- Actor **Crimson Rigel Taurus** offers in a well-known forum 44 GB of private information and documents of the Regional Government of Ucayali, Peru.

- Actor **Darkslateblue Cosmos Taurus** sells on a dark web forum Webshell accesses to the sedena.gob.mx subdomain of the Government of Mexico.

- Actor **Yaleblue Cosmos Taurus** offers on a dark web forum the database of the Mexican innovation and technology company bienDIG, which contains private information such as users, passwords, e-mails, etc.

- Actor **ResolutionBlue Cosmos Taurus** sells for $800 on a dark web forum 5 million medical records of Mexican patients with private information such as names, phone numbers, documents, etc.

- Actor **Red Cosmos Taurus** offers the database of the Ecuadorian battery recycling company BAPU for free on a well-known English forum. The leak contains private information such as names, IDs, users, passwords, etc.

- Actor **Cornflowerblue Cosmos Taurus** sells for $15,000 on popular Russian-language forum unauthorised access to a Brazilian currency exchange.

- The **group LulzSec Muslims** claim to have hacked into the Argentine Military Authority. They are said to have obtained data including names, surnames, telephone numbers, addresses, ID numbers, bank accounts and personal and military cards.

Vulnerabilities & Exploits

- A critical vulnerability has been detected in the **Ultimate Member add-on of Wordpress** catalogued as **CVE-2024-1071.** Cybercriminals can exploit this vulnerability and to **add additional SQL queries to extract sensitive data** from the database.

- **Active exploitation** by threat groups such as **BlackBasta** of vulnerabilities catalogued as **CVE-2024-1708** and **CVE-2024-1709** has been detected. The vulnerabilities in **ConnectWise ScreenConnect** allow attackers unauthorised access to directories and access to sensitive information through bypassing authentication. Threat actors are using this vulnerabilities to ranging from **ransomware deployment** to **information stealing and data exfiltration** attacks.

- Researchers have revealed a serious vulnerability (CVE-2024-23204) in the popular **Apple Shortcuts app**. This flaw lets attackers sneak past Apple's security on your iPhone, iPad, or Mac, and potentially steal private information without you even knowing.

- Zyxel has released fixes for **critical vulnerabilities in its firewall** and access point products, including a null pointer dereference (CVE-2023-6397), a post-authentication command injection (CVE-2023-6398), and two format string vulnerabilities (CVE-2023-6399, CVE-2023-6764). Failure to update leaves systems vulnerable to remote code execution, unauthorized command injection, and denial-of-service attacks.

⚠️ Warning of the week

- Heard about those **hacktivist groups throwing a cyber party on Telegram**? It's like the Avengers, but with keyboards. Quick tip: Guard your virtual castle like a knight. **Update defenses faster against DDoS in particular** than a cat video spreads, and don't let your passwords be as predictable as a pop song chorus.

- Hey WordPress warrior, have you heard about **the wild side of the Ultimate Member plugin with CVE-2024-1071**? It's as if the plugin has a behind-the-scenes pass for cybercriminals. Update that plugin soon and **strengthen your passwords**.

- Alert! The threat actors are having a field day with **CVE-2024-1708 and CVE-2024-1709**. Keep your software, apps, and systems updated, make those passwords tougher than as Sudoku puzzle and don't click like it's Tinder.

- Patch those vulnerabilities (**CVE-2023-6397, CVE-2023-6398, CVE-2023-6399, CVE-2023-6764**) ASAP, or attackers might sneak in and wreak havoc. Don't let your network become a playground for cyber-mischief!

- Uh oh, Shortcut lovers! There's a **sneaky bug (CVE-2024-23204)** lurking in the app that could let attackers grab your private info without you even noticing. Don't worry, though, Apple's already patched it in the latest updates (iOS 17.3, iPadOS 17.3, watchOS 10.3, and macOS Sonoma 14.3). Just make sure to update your devices and be cautious about running shortcuts from untrusted sources. **Stay safe out there!**

ADVERSARIALLY weekly report

Feb 22 - 29, 2024

XG3 UNIT

Detections by Risk

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

- Detection of Powershell obfuscation techniques in CL **(72.5)**
- Network connections using Mshta **(65.5)**
- Lolbin SCHTASKS suspicious executions **(58.5)**
- Disabling Windows Data recovery functionality **(57.5)**
- Running processes listing via WMI **(55.0)**

🟥	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
- Obfuscated Files or Information
- System Binary Proxy Execution
- Scheduled Task/Job
- Inhibit System Recovery

Adversary Trends

Actors	Set Tools	Vulnerabilities
Volt Typhoon	LockBit-NG-Dev	Connectwise / CVE-2024-1709
APT28	GoldPickaxe	Apache / CVE-2023-51747
APT29	Migo	Apache / CVE-2024-21742
UNC2452	VietCredCare	Php / CVE-2024-24401
Kimsuky	Backmydata	Azure / CVE-2024-27099

ADVERSARIALLY
weekly report
Feb 22 - 29, 2024

Ransomware

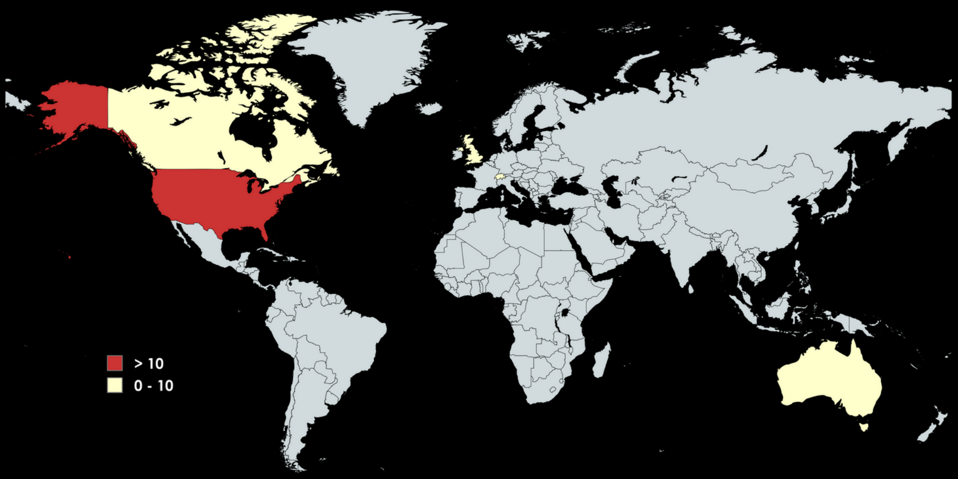
Total Victims = 89 (+9)

- Spain - **1** (+1)
- Latam - **2** (-6)
- WorldWide - **86** (+14)

The king is...

Data of the week

Top Countries	Top Sectors	Top Groups
USA - **41** (+7)	Services - **20** (+4)	ALPHV - **9** (+4)
GBR - **3** (-1)	Manufacturing - **20** ☆	Lockbit - **9** (-7)
CAN - **3** (-1) ☆	Health - **9** ☆	8base - **8** ☆
AUS - **3** ☆	Transport - **4** ☆	Blackbasta - **7** ☆
CHE - **3** ☆	Financial - **4** ☆	Medusa - **6** ☆



Victims

- **Ransom Victim:** Electro Matrix | Group: Alphv | Sector: Energy | Country: Spain
- **Ransom victim:** DTS | Group: Akira | Sector: Manufacturing | Country: Chile
- **Ransom victim:** Grupo Creativo Herrera | Group: Qilin | Sector: Professional Services | Country: Ecuador

xMDR

ADVERSARIALLY weekly report

Feb 22 - 29, 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.