WR X

Adversarially
Weekly Report

AUG 1 - 8

2024

XG3 UNIT

xMDR
powered by Cipher

ADVERSARIALLY
weekly report
Aug 1 - 8, 2024

XG3 UNIT

Adversary of the Week

Plumpurple Cosmos Taurus

Type: Individual

Countries: 🇧🇷

Maturity: 🟩⬛⬛

Sectors: Logistic

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Violet Cosmos Taurus

Type: Individual

Countries: 🇻🇳 🇪🇸

Maturity: 🟧🟧⬛

Sectors: Health, Manufacturing

Activity: Cybercrime

TTPs: Exploit Public-Facing Application

Meow

Type: Group

Countries: 🌍

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 33

Global

- A Chinese hacking group known as **StormBamboo** has **compromised** an **undisclosed internet service provider (ISP)** to poison automatic software updates with malware. Cybersecurity researchers detected that the threat group had **exploited insecure HTTP software update mechanisms** that did not validate digital signatures to deploy malware payloads to victims' Windows and macOS devices.

- The ransom group have targeted **OneBlood,** a non-profit **blood donation centre** based in Orlando that **serves more than 350 hospitals** in four states of United States of America. Although the donation centres continue to collect, test and distribute blood, they have warned that they are operating at **significantly reduced capacity,** which could lead to more serious problems.

- Several **McLaren Health Care systems** and phone lines were **disrupted after** an attack linked to the **INC Ransom ransomware operation**. McLaren is a not-for-profit health care system with annual revenues of more than $6.5 billion, operating a network of **13 hospitals across Michigan supported by a team of 640 physicians.** It also has more than 28,000 employees and works with 113,000 network providers in Michigan, Indiana and Ohio.

- A **new technique** adopted by the threat actors **behind the Chameleon banking Trojan for Android** has been discovered **targeting users in Canada** by **masquerading as a customer relationship management (CRM) application**. Once the dropper app is installed, the app displays a fake login page for a CRM tool and then displays a fake error message urging victims to reinstall the app, when, in reality, it deploys the Chameleon payload.

Spain & Latam

- The website of the company **Tea Cegos S.A.**, which contained all the personal information of many candidates for the competitive examinations of **Radiotelevisión Española,** has **suffered a security breach** and has **exposed information such as bank details, identity documents,** professional certificates or proof of payment. At the moment it is not known the extent of the incident and whether it has affected all the registered candidates, more than 21,000.

- **Violet Cosmos Taurus** sells on Breachforum has listed data from Lookiero for sale. The compromised dataset includes 4.11 GB of information with 5 million records, including emails, usernames, and passwords.

- The hacktivist group **NoName(057)16** continues its **campaign of attacks against Spanish entities**, most recently against the Galician Ministry of Finance, the website of the city council of A Coruña, etc.

- The **Andalusian Health Service** has reported a **security incident** that has affected the websites of several hospitals and allowed the attacker to access the **personal data of more than 50,000 healthcare professionals.** The cybercriminal demanded a rescue payment of 2.5M Bitcoins, which was not paid.

- **Anonymous** is carrying out a **campaign against Venezuela** in which it has already attacked various entities such as **"Billetera Móvil"**, **"Canal Televen"** or various **governmental entities** such as the Ministry of the Interior, the Directorate of Military Counterintelligence, the National Assembly or the Ministry of Foreign Affairs.

- The group known as **MS BOTNET CyberHunters** has hacked and published the database of the **General Directorate of Military Counterintelligence** (DGCIM) of the Maduro regime in Venezuela.

- **Darkorange Cosmos Taurus** sells on Breachforum confidential information of the Mexico City Judiciary (PJCDMX), including the source code of the dating system, as well as access credentials of thousands of users.

- **Plumpurple Cosmos Taurus** sells on Breachforum 15M of users records of Ingresse with information such as SSN, name, phone, email, event name, order date, payment option, etc por $10,000.

Vulnerabilities & Exploits

- **Butterscotchyellow Cosmos Taurus** sells on XSS the **source code for a ".url" exploit**, which would be effective for Windows 10 and 11 systems. The vendor claims that the exploit can fool users and bypass security warnings, making it a powerful tool for malicious activity. The asking price is $10,000.

- A **critical vulnerability** has been discovered in Windows File Explorer, identified as **CVE-2024-38100**. This vulnerability allows attackers to gain administrator privileges through a privilege escalation exploit. In addition, several exploits confirming the exploitability of the flaw and its impact have also been published.

- Jenkins, the popular open source automation server, has issued an urgent advisory detailing **two vulnerabilities**, one of which is critical. These vulnerabilities, identified as CVE-2024-43044 and CVE-2024-43045. If attackers exploit **the most severe, CVE-2024-43044**, they can read arbitrary files from the Jenkins driver file system, potentially gaining access to sensitive configuration data, credentials or even source code. The second vulnerability listed as **CVE-2024-43045**, allows unauthorized access to users' "My Views," which are personalized dashboards in Jenkins.

- **CVE-2024-38856:** The new **zero-day pre-authentication remote code execution vulnerability** that **affects** the open source **Apache OFBiz enterprise resource planning (ERP) system** and could allow threat actors to achieve remote code execution on affected instances.

⚠ Warning of the week

- A $10,000 **.url exploit** is up for sale, claiming to bypass security warnings and trick users. **Patch your systems and train your team**—don't let your mouse clicks lead to a world of trouble. Remember, not every link deserves a click!

- A **critical bug in Windows File Explorer** could let attackers sneak into admin privileges. Time to **patch up** before your File Explorer becomes a hacker's expressway. Keep your system tidy—admin access is for you, not the bad guys.

- **Jenkins** has sprung a leak with two vulnerabilities, one allowing file snooping and another peeking into user dashboards. **Update your Jenkins server quickly**, or your source code and credentials might find themselves in the wrong hands. Jenkins deserves better than being a hacker's playground.

- A **zero-day in Apache OFBiz ERP** could let attackers remotely execute code—no login needed! **Secure your ERP with patches,** unless you fancy your business plans being executed by someone else. Don't let your enterprise resource planning turn into hacker resource planning.

ADVERSARIALLY

weekly report

Aug 1 - 8, 2024

Ransomware

Total Victims = 119 (-20)

- Spain - **5**
- Latam - **1** (-2)
- WorldWide - **113** (-18)

The king is...

Data of the week

Top Countries

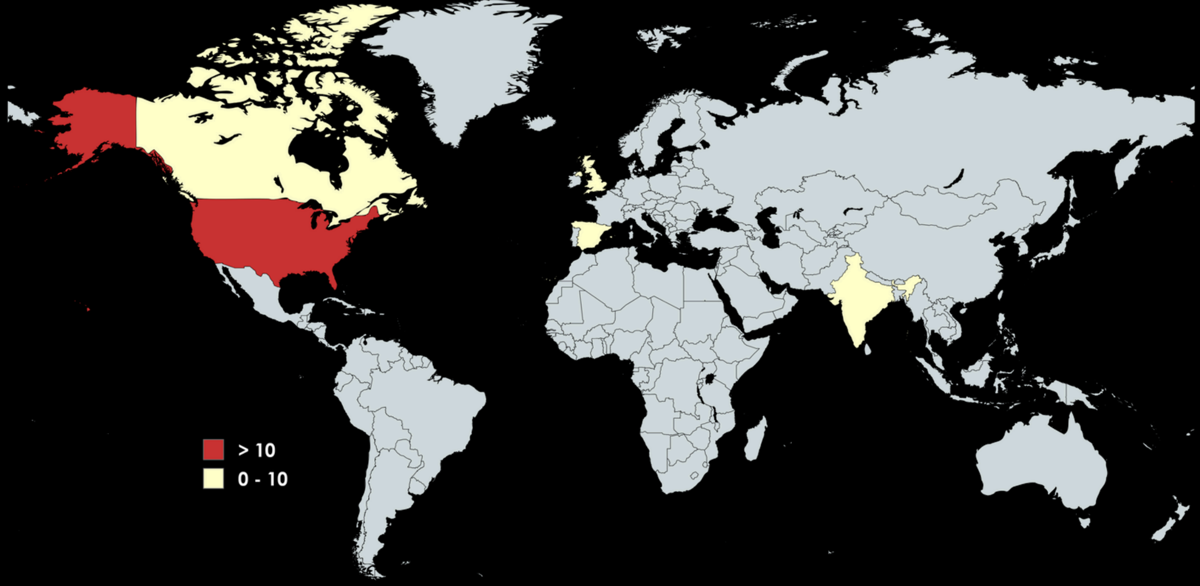
- USA - **54** (-11)
- CAN - **7** (+1)
- IND - **5** ☆
- SPA - **5**
- GBR - **4** (-3)

Top Sectors

- Manufacturing - **23** (-2)
- Technology - **11** (-6)
- Healthcare - **9** ☆
- Finance - **9** ☆
- Education - **8** (-1)

Top Groups

- Meow - **15** (+8)
- Ransomhub - **12** (-11)
- Cactus - **11** (+1)
- Hunters - **10** ☆
- Cicada3301 - **9** ☆



Victims

- **Ransom Victim:** BRASPRESS | Group: akira | Sector: Transportation | Country: Brazil
- **Ransom Victim:** www.bahia-principe.com | Group: ransomhub | Sector: Tourism | Country: Spain
- **Ransom Victim:** msprocuradores.es | Group: madliberator | Sector: Legal | Country: Spain
- **Ransom Victim:** Casco Antiguo | Group: hunters | Sector: Real Estate | Country: Spain
- **Ransom Victim:** Fractalia Group | Group: hunters | Sector: Technology | Country: Spain
- **Ransom Victim:** ciberviaxesespecial.net | Group: lockbit3 | Sector: Tourism | Country: Spain

xMDR
powered by Cipher

ADVERSARIALLY
weekly report
Aug 1 - 8, 2024

XG3 UNIT

Top MITRE TTP covered:

Command & Scripting

Phishing for Information

User Execution

OS Credential Dumping

Impair Defenses

Data added to Digital Adversary in the last week

TTP'S 35

Top Most Relevant

- OS Credential Dumping
- Supply Chain Compromise
- Exfiltration over C2 Channel

Threat Actors 7

Top Most Relevant

- Mediumorchid Cosmos Taurus
- Sienna Cosmos Taurus
- Volcano Demon

Tools 2

Top Most Relevant

- GoRed
- Akira

xMDR

ADVERSARIALLY

weekly report

Aug 1 - 8, 2024

xMDR

powered by Cipher