WR X

Adversarially

Weekly Report

AUG/ 8 - 15

2024

XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY weekly report

Aug 8 - 15, 2024

XG3 UNIT

Adversary of the Week

Cadetblue Cosmos Taurus

Type: Individual

Countries: 🌍

Maturity: 🟩⬛⬛

Sectors: Government

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Anonymous

Type: Group

Countries: 🌍

Maturity: 🟧🟧⬛

Sectors: All

Activity: Hacktivism

TTPs: DDoS

Ransomhub

Type: Group

Countries: 🌍

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 35

Global

- **The Lockbit group** has this week published on its website more than 50 victims, although, as in the past, not all are new victims, as some old ones have been observed. After Operation Cronos, Lockbit seems to have struggled to get back into the swing of things, but this spike in activity could be a sign that it is back in the game and back to normal activity.

- The Cleveland FBI office announced **the disruption of the ransomware group "Radar/Dispossessor,"** led by a figure known as "Brain." The FBI dismantled servers and domains linked to the group in the U.S., UK, and Germany. The group, active since August 2023, targeted U.S. entities initially but impacted 43 companies worldwide.

- **The actor Cadetblue Cosmos Taurus** has announced on a well-known English-speaking hacking forum a collection of server data from the Israeli Ministry of Defence, including hundreds of signed documents, technical information and images. It has a total size of 2.5gb and is readily available to the public, although there is a small fee.

- **The actor Tiffanyblue Cosmos Taurus** is selling unauthorised access to the European Online Casino infrastructure. The company has a revenue of $5 million and is selling at a starting price of $10,000.

- South Korea claims **DPRK hackers stole technical data** from a spy plane and the country's main battle tanks, putting national security at risk.

- The video content streaming platform **Netflix has suffered a major leak about its upcoming content,** with full episodes of some of the most eagerly awaited series being leaked on the internet. It seems that this data leak comes from the test versions of this type of content.

- **France has suffered more than 140 cyber attacks during the Olympic Games** event. Between 26 July and 11 August, the government cybersecurity agency Anssi recorded 119 reports of low-impact "security events" and 22 incidents in which "a malicious actor" successfully attacked a victim's information system.

Spain & Latam

- **Slateblue Cosmos Taurus X** has leaked information on Breachforum about the Spanish Padel Federation, reporting compromising the data of 190K users. These include bank details, such as IBAN, among other personal data.

- **LulzSec Muslims group,** one of the most active hacktivist groups, allegedly hacked CitizenGO, an ultra-conservative lobby group based in Spain. The group claims to have 95,000 pieces of user data, including names, addresses, phone numbers, etc.

- **The personal details of RFEC members (Royal Spanish Cycling Federation)** have been leaked in a cyber-attack, although they claim that no bank details have been leaked, they have reported that various personal details have been stolen.

- **The hacktivist group MS BOTNET CyberHunters** has stolen and published the database of the **General Directorate of Military Counterintelligence (DGCIM)** of the Maduro regime in Venezuela, due to political tensions in the country in question, in a show of support for the anti-Maduro population.

- **The Anonymous group,** also hacktivist and in solidarity with the events in Venezuela, has also carried out a series of campaigns in the country in question, attacking different targets, including the **Caracas metro or the national television station in Caracas**, but the most notable ones have been against government sites, such as the ministry of internal relations or the national assembly, leaving them without access.

- **The actor Khaki Cosmos Taurus X** has leaked the database of the **library of the Instituto Superior Universitario Cotopaxi** in a hacking forum, where approximately 4 gb of data have been shown.

- **The actor Unitednationsblue Cosmos Taurus X** has put 24gb of the **Mobex company**, in Brazil, up for sale. The alleged breach involves the complete compromise of Mobex's online infrastructure. Price is unknown but the threat actor is accepting offers via Telegram.

Vulnerabilities & Exploits

- An exposed vulnerability in **AMD processors affecting all CPU models since 2006** has been exposed in DEFCON by author **Enrique Nissim**. It is a problem in a specific sector of the processor (CPU), the central component of any computer. This vulnerability is based on the **System Management Mode (SMM)**, where the flaw has been exploited to execute code in an arbitrary manner and which could be a mechanism for generating **advanced persistence**, as this type of code is invisible to antivirus or anti-cheat engines.

- Microsoft has disclosed a **high-severity zero-day vulnerability affecting Office** 2016 and later versions, identified as **CVE-2024-38200**. This security flaw is caused by an information disclosure weakness that allows unauthorised actors to access protected information, such as system state or configuration data, personal information or connection metadata.

- **Microsoft** has released an urgent security update to address a critical remote code execution vulnerability in the **Windows TCP/IP stack**. The flaw tracked as **CVE-2024-38063**, affects all supported Windows and Windows Server versions, including Server Core installations. **CVE-2024-38063** is a remote code execution vulnerability in Windows TCP/Iwith a maximum severity rating of Critical

⚠️ Warning of the week

- **Strengthening Your AMD Defenses** If you've got an AMD processor in your system (and that's a lot of us since 2006), it's time for a security check-up. Make sure your firmware is up to date and keep an eye out for any unusual activity. Regularly review your system logs and consider advanced security measures to keep sneaky exploits at bay. Don't let your CPU become a hacker's playground! 🛡️🔍

- **Keep Your Office Suite Safe and Sound Using Microsoft Office 2016** or later? It's crucial to install the latest updates right away. Double-check your document-sharing settings and limit access to sensitive data. Implement multi-factor authentication (MFA) to add an extra layer of security. Remember, better safe than sorry—don't let cyber snoopers turn your documents into their next treasure hunt! 📄🔓

- **Patch Your Windows Systems—No Time to Lose!** Running any version of Windows or Windows Server? Make sure to apply the latest security patches immediately. Regularly scan for vulnerabilities and ensure your firewalls are robust. Educate your team about the importance of timely updates. You wouldn't leave your front door open, so don't leave your network unprotected. 🌐⚠️

- Secure Your Online Casino Operations **If you're in the online casino business, it's time to double down on your cybersecurity**. Conduct a thorough security audit of your systems, monitor network traffic for any anomalies, and strengthen your access controls. Encrypt sensitive data and keep your software up to date. Don't gamble with your cybersecurity—keep the bad actors out and your customers' trust in! 🎰💸

ADVERSARIALLY
weekly report
Aug 8 - 15, 2024

XG3 UNIT

Ransomware

Total Victims = 122 (+3)

- Spain - **2** (-3)
  Latam - **5** (+4)
  WorldWide - **115** (+2)

The king is...

Data of the week

Top Countries

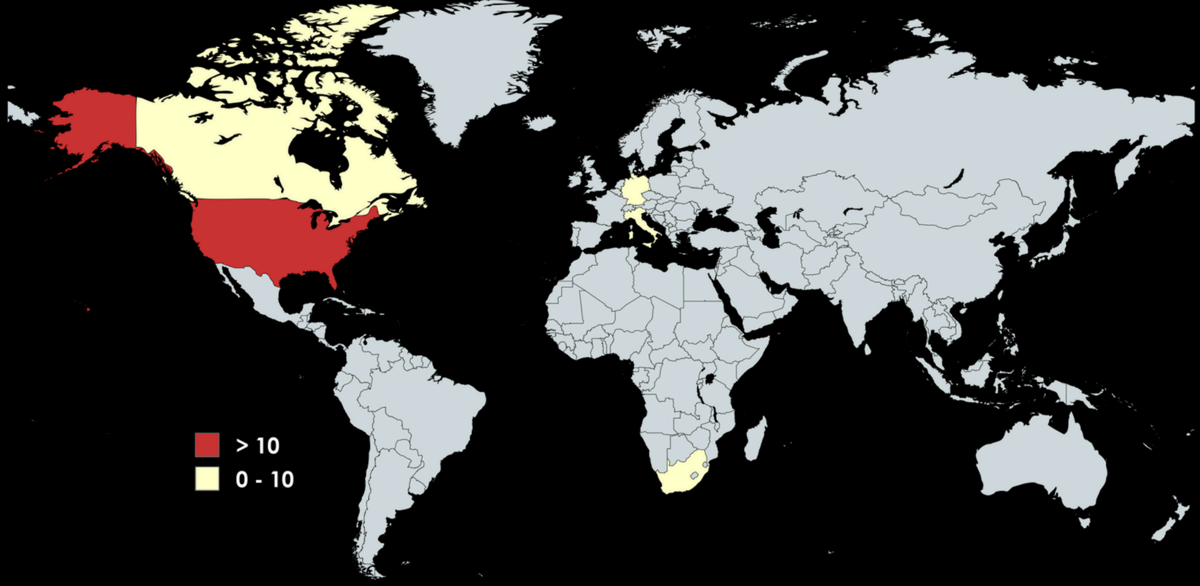
- USA - **57** (+3)
- CAN - **3** (-4)
- **ITA - 3** ☆
- DEU - **3**☆
- GBR - 3 (-4)

Top Sectors

- Manufacturing - **21** (-2)
- Technology - **17** (+6)
- Healthcare - **12** (+3)
- Commerce - **11** ☆
- Construction - **6** ☆

Top Groups

- Ransomhub - **20** (+8)
- Lockbit3 - **17** ☆
- Helldown - **10**☆
- Play - **9**
- Meow - **9** (-6)



Victims

- **Ransom Victim: www.sicoob.com.br> | Group: ransomhub | Sector: Banking | Country: Brazil**
- **Ransom Victim: comoferta.com | Group: darkvault | Sector: Commerce | Country: Brazil**
- **Ransom Victim: mercadomineiro.com.br | Group: darkvault | Sector: Commerce | Country: Brazil**
- **Ransom Victim: clinicatezza.com.pe | Group: lockbit3 | Sector: Healthcare | Country: Peru**
- **Ransom Victim: infotexim.pe | Group: ransomhub | Sector: Technology | Country: Peru**
- **Ransom Victim: luisoliveras.com | Group: lockbit3 | Sector: Agriculture | Country: Spain**
- **Ransom Victim: suandco.com | Group: madliberator | Sector: Legal | Country: Spain**

ADVERSARIALLY

weekly report

Aug 8 - 15, 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 27

Top Most Relevant

- Command and Scripting Interpreter
- System Information Discovery
- Financial Theft

Threat Actors 8

Top Most Relevant

- Palegoldenrod Cosmos Taurus
- LigthSalmon Cosmos Taurus
- Gold Cosmos Taurus

xMDR

ADVERSARIALLY

weekly report

June 27 - July 4, 2024

xMDR
powered by Cipher

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.