

**WR**



# Adversarially

Weekly Report



**JUL./ 18 - 26**

**2024**



**xMDR**  
powered by Cipher

## Adversary of the Week



### Emeraldgreen Cosmos Taurus

**Type:** Individual

**Countries:** 

**Maturity:** 

**Sectors:** Manufacturing

**Activity:** Cybercrime

**TTPs:** Exploit Public-Facing Application



### Lightlategray Cosmos Taurus

**Type:** Individual

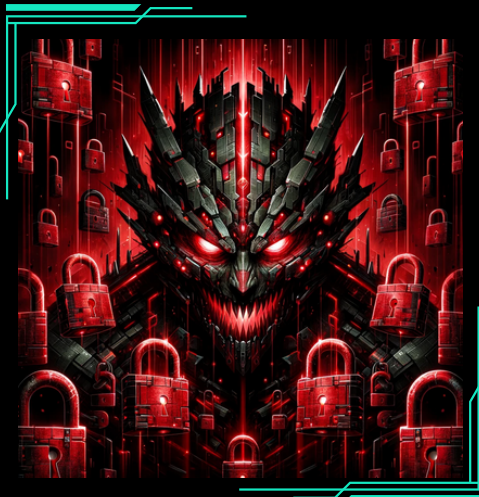
**Countries:**  

**Maturity:** 

**Sectors:** Food, retails, automotive, telecoms.

**Activity:** Cybercrime

**TTPs:** Exploit Public-Facing Application



### LockBit 3.0

**Type:** Group

**Countries:** 

**Maturity:** 

**Sectors:** All

**Activity:** RaaS

**TTPs:** 86

 **Global**

- **Richmaroon Cosmos Taurus X** is selling data of active-duty personnel from three branches of the US Armed Forces: the Army, Navy, and Air Force. The database includes information such as IDs, names, titles, emails, phone numbers, and unit details.
- Law enforcement in the U.K. **arrested a 17-year-old teenager** from Walsall who is suspected to be a **member** of the **Scattered Spider** cybercrime group. The arrest is the result of a joint international law enforcement **operation carried out by the U.K. National Crime Agency (NCA) and the U.S. Federal Bureau of Investigation (FBI)**.
- **Lightlategray Cosmos Taurus X** offers in BreachForum 5,110 rows of Loreal employees' information. The data breached include first name, last name, job title, email, person city, person state and person country.
- **Shockingpink Cosmos Taurus X** offers Singapore Ministry of Finance data. The database includes name and lname, access date, visit date, servers related to the main site, localapi, ip address.
- **CrowdStrike** now **warns** that **threat actors** are taking advantage of the situation with the update bug to **distribute Remcos RATs** to their customers in Latin America under the guise of providing a hotfix.





## Spain & Latam





- On 20 July 2024, **Spanish police arrested three people** suspected of being **affiliated with the hacktivist group NoName057(16)**. The operation, led by the Spanish Guardia Civil, arrested the suspects **in Mallorca, Huelva and Seville**. Searches at their residences yielded computer equipment and documents potentially related to the cyber attacks.
- **Lightgray Cosmos Taurus X** offers in Breachforum data over 3 million clients Spanish company Expandia. The breach includes over 303k unique email addresses, names, phone numbers and physical addresses.
- The Pakistani group **Team Insane PK**, affiliated with the pro-Russian group NoName057(16) are carrying out **DDoS attacks** following the arrest of three of their members in Spain.
- **Pearlwhite Cosmos Taurus X** leaks a database with 19.5 million Venezuelan citizens' data. The leaked data allegedly contains private information such as names, surnames, date of birth, etc.
- **Emeraldgreen Cosmos Taurus X** sells on Breachforum a database of Jamar Furniture. The actor claims to have 10,000 customer data.
- **Redpurple Cosmos Taurus X** claims in Breachforum to have leaked a file containing 49 SQL databases from various Mexican websites. The databases will contain more than 1,000,000 lines of data, including emails, full names, addresses, and phone numbers.



## Vulnerabilities & Exploits

- **Papayawhip Cosmos Taurus** Xclaim on Breachforum to have put up for sale a Preauth RCE (root) affecting HomeMatic. The total number of allegedly exploitable devices is 75,100 devices.
- **CVE-2024-26020**: This is an **arbitrary script execution** vulnerability with score 9.8 in the MPV functionality of Ankitects Anki 24.04. A specially crafted flashcard can lead to arbitrary code execution. An attacker can send a malicious flashcard to trigger this vulnerability.
- **CVE-2024-38021: Moniker RCE Vulnerability** Uncovered **in Microsoft Outlook**. It is a zero-click remote code execution (RCE) vulnerability that impacts most Microsoft Outlook applications. If exploited, the vulnerability can lead to potential data breaches, unauthorized access, and other malicious activities.
- A **new Oday** has been detected on **Android Telegram**. ESET researchers have labelled it 'EvilVideo' and it has been discovered in a multitude of Telegram chats, groups and channels. It is a method that **allows attackers to 'camouflage' exploits so that they appear as videos in chats** to avoid arousing suspicion among victims.
- Generative AI tools are as vulnerable to exploits as any other technology. **CVE-2023-46229 and CVE-2023-44467** affect open-source **library LangChain**, a framework to build LLMs. These two flaws could have **allowed attackers to execute arbitrary code and access sensitive data**, respectively.

## Warning of the week

- Be wary of 'hotfixes' bearing gifts! Threat actors are distributing Remcos RATs under the guise of updates in Latin America. Ensure your updates come from trusted sources to avoid unwanted malware masquerading as a solution 
- A preauth RCE affecting 75,100 HomeMatic devices is up for sale. Patch your devices and bolster your defenses. No one wants a hacker with root access running your smart home—especially not at bargain prices!
- Beware of malicious flashcards in Anki 24.04! An arbitrary script execution flaw could turn your study session into a hack fest. Update your Anki software and scrutinize flashcards like they're final exam questions 
- A zero-click RCE vulnerability in Microsoft Outlook could spell trouble. Update your Outlook applications swiftly to keep hackers from reading more than just your emails. After all, zero-click should mean zero worries!  
- EvilVideo exploit lets attackers disguise malware as videos in Telegram. Avoid suspicious video links and ensure your Telegram app is up to date. Remember, not all videos are worth a watch, especially those from unknown sources.
- Generative AI tools have their own vulnerabilities too! LangChain's recent flaws could allow arbitrary code execution and data access. Keep your AI tools updated and secure, or you might end up generating more problems than solutions.

# ADVERSARIALLY

## weekly report

July 18 - 26, 2024



### Ransomware

Total Victims = **108** (-14)

- Spain - **2** (2-)
- Latam - **2** (-5)
- WorldWide - **104** (-7)

### The king is...



### Data of the week

#### Top Countries

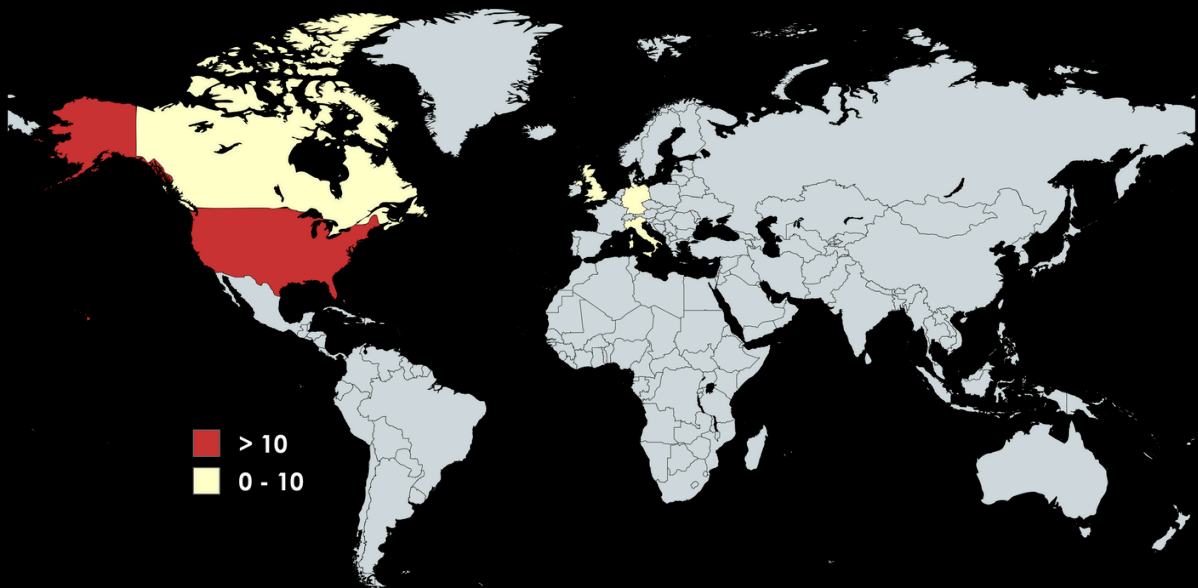
- USA - **51** (-6)
- DEU - **4** (-1)
- CAN - **4** (-1)
- ITA - **4** ☆
- GBR - **3** (-3)

#### Top Sectors

- Technology - **22** (+7)
- Healthcare - **11** (+3)
- Manufacturing - **10** (-10)
- Education - **7** (+3)
- Legal - **7**

#### Top Groups

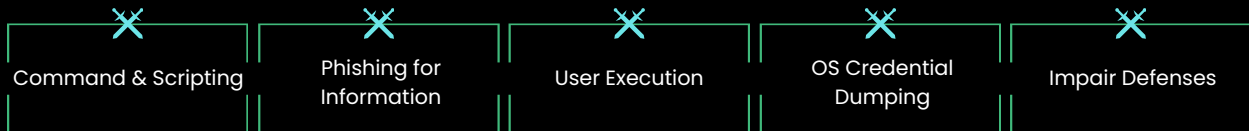
- Lockbit3 - **20** ☆
- Ransomhub - **16** (-3)
- Madliberator - **6** ☆
- Ransomhouse - **5** ☆
- Cactus - **4** ☆



### Victims

- Ransom Victim:** Santa Rosa | Group: hunters | Sector: Finance | Country: Argentina
- Ransom Victim:** Metal frío | Group: ransomhub | Sector: Manufacturing | Country: Brazil
- Ransom Victim:** VITALDENT | Group: madliberator | Sector: Healthcare | Country: Spain
- Ransom Victim:** Perfeita plastica | Group: ransomcortex | Sector: TBD | Country: Brazil

### Top MITRE TTP covered:



### Data added to Digital Adversary in the last week



TTP'S **71**

 Top Most Relevant

- Data Encrypted for Impact
- Ingress Tool Transfer
- Financial Theft



Threat Actors **8**

 Top Most Relevant

- Persiangreen Cosmos Taurus
- Jonquil Cosmos Taurus
- Crimsom Rigel Taurus



CVE's **1**

 Top Most Relevant

- CVE-2024-29849



**xMDR**

**ADVERSARIALLY**  
**weekly report**  
**July 18 - 26, 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.