



Adversarially

Weekly Report



MAY/ 16-23

2024



xMDR
powered by Cipher

Adversary of the Week



Wildstrawberry Cosmos Taurus

Type: Individual

Countries: 

Maturity: 

Sectors: All

Activity: Cybercrime

TTPs: Sell access



AnonymousEgyp

Type: Hacktivist Group

Countries: 

Maturity: 

Sectors: All

Activity: Hacktivism

TTPs: DDoS,
Defacement



LockBit 3.0

Type: Group

Countries: 

Maturity: 

Sectors: All

Activity: RaaS

TTPs: 54



Global

- More than 50,000 rows of employees' personal data exposed in the **leak at Nissan**, which suffered a ransomware attack in late 2023.
- The North Korea-linked **Kimsuky group** has been blamed for a new social engineering attack using **fictitious Facebook accounts targeted via Messenger** aimed at spreading malware for espionage, as it appears to be directed at specific users.
- A new type of malware, which is spreading on android devices by spoofing a Chrome update, has novel capabilities such as directly accessing banking apps or taking remote control of the phone.
- Russia-linked **Turla APT** allegedly used two new backdoors, named Lunar malware and LunarMail, to target **European government agencies**. The two backdoors compromised a European ministry of foreign affairs (MFA) and its diplomatic missions abroad.
- New campaign brings back the **Grandoreiro malware**, which is attacking more than 1500 banks worldwide, despite the police operation that allegedly interrupted its activity. The malware has reportedly developed new technical capabilities and, in addition, has expanded its targets to include English-speaking countries.
- Breach Forums Admin **ShinyHunters Claims Domain Reclaimed from FBI**. ShinyHunters, the hacker group and primary administrator of Breach Forums informed that they regained access to the forum's clear net and dark web domains. Currently it does not appear that the old forum has been restored or a new one created.
- A **KeyPlug implant** attacking industries in Italy has been discovered. It appears that the **APT41 group** is behind the spread of this backdoor malware. It could be used for espionage campaigns.



Spain & Portugal

- New data breach **affecting CCOO** exposes more than 6000 user credentials. This could be related to the event of a few months ago, where a database containing CCOO data was put on sale, being this additional information that could complement the one that already happened.
- The **Junta de Andalucía website** is being attacked, using it to redirect users to malicious pages. It seems to be due to a vulnerability that affects FCKeditor in versions prior to 2.6.41. This is a bug that was published in 2009 and for which there is a public exploit.
- The data of 400 companies, mostly Basque, was stolen in a cyberattack on a consultancy in Álava. It appears to be ransomware, as it has been reported that a financial payment was demanded from the firm to return the confidential data stolen, but it has not yet been claimed by any group.
- A well-known forum has announced the sale of a database belonging to **ATSistemas**, where the company's confidential data, which appears to belong to the internal CRM, is exposed.
- Actor **Wildstrawberry Cosmos TaurusX** sell RDP access, cybersecurity sector, admin domain by the wayt VMware Horizon. Price 1300\$.

ADVERSARIALLY

weekly report

May 16 - 23, 2024



LATAM











- The cybercriminal group **AnonymousEgypt** has again leaked a **Banco Santander Mexico** database on its Telegram channel, which had already been publicly exposed in July 2023.
- **Wow**, a Chilean telecommunications company, has suffered a **data breach** that has exposed more than one million prepaid mobile contracts, containing a variety of personal data. Anyone in the last few months could have accessed this information.
- The group **CiberinteligenciaSV** publishes new data from the **Government of El Salvador**, specifically from the Alcaldía Municipal de Santa Ana, a local governmental entity.



Vulnerabilities & Exploits

- The Cybersecurity and Infrastructure Security Agency (CISA) has issued a warning about a critical vulnerability in **NextGen Healthcare Mirth Connect software**, identified as CVE-2023-43208. This security flaw allows remote code execution without authentication, due to errors in data deserialisation.
- CVE-2024-22120 (CVSS 9.1): **Zabbix SQLi Vulnerability** Exposes IT Infrastructure to Attack. POC has been detected as available. Zabbix server can perform command execution for configured scripts. Once the command is executed, an audit entry is added to the Audit Log. Because the "clientip" field is not sanitised, it is possible to inject SQL into "clientip" and exploit time-based blind SQL injection.
- Unauthorised RCE vulnerability caused by **QNAP QTS overflow** (CVE-2024-27130) allowing remote code execution. QNAP NAS devices are popular among small and medium-sized businesses as well as ransomware gangs, so an urgent upgrade is recommended.
- CVE-2024-4367, a **vulnerability in PDF.js** found by Codean Labs. PDF.js is a JavaScript-based PDF viewer maintained by Mozilla. This bug allows an attacker to execute arbitrary JavaScript code as soon as a malicious PDF file is opened.

Warning of the week

- Think twice before clicking that **'Chrome update'** on your Android! It's actually **sneaky malware** in disguise, aiming for your banking apps and phone control. Stay safe: **only update through the official Google Play Store!**  
- Got **NextGen Healthcare Mirth Connect**? Time for a security checkup! CISA says a nasty bug, **CVE-2023-43208**, can let attackers in without a password. **Patch it up**, or your data might need a real doctor!   
- Running Zabbix? **CVE-2024-22120** means it's time to lock down! This **SQLi bug** can sneak in **via the 'clientip' field**. **Patch up** or risk your IT infrastructure being the hackers' playground!  
- Do you have a **QNAP NAS**? It's time to **upgrade ASAP** or risk your data becoming the next big ransomware buffet due to an **unauthorised RCE!** 
- Opening a PDF with **CVE-2024-4367** is like opening a can of worms, with JavaScript inside! **Update PDF.js** and avoid opening unknown documents.  

ADVERSARIALLY

weekly report

May 16 - 23, 2024



Ransomware

Total Victims = 127 (-52)

- Spain - 5 (-5)
- Latam - 11 (-12)
- WorldWide - 111 (-35)

The king is...



Data of the week

Top Countries

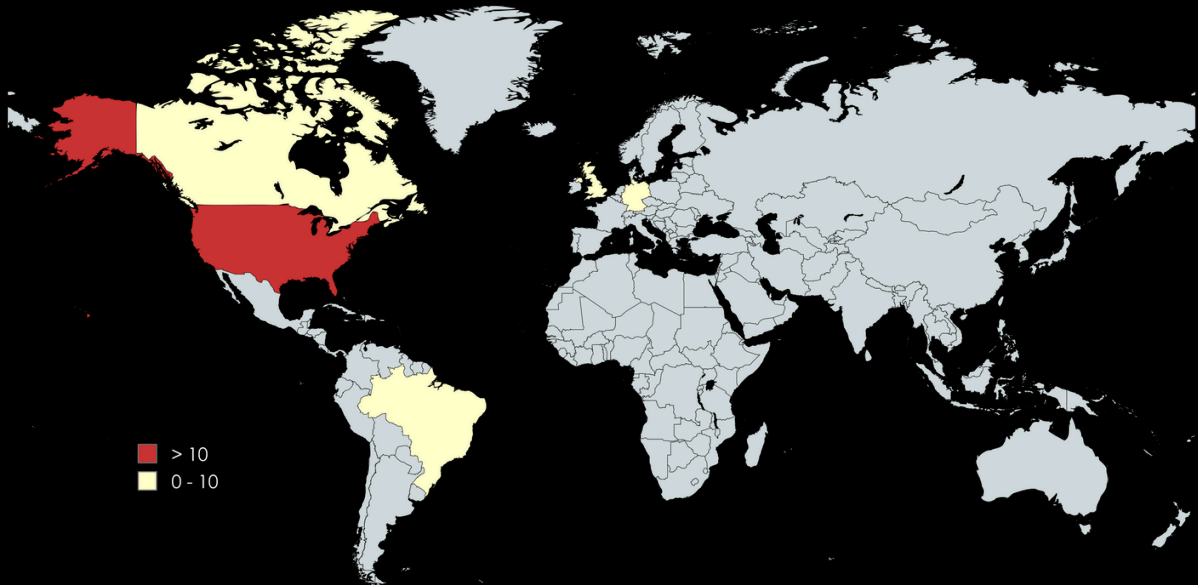
- USA - 71 (+10)
- BRA - 7 (-6)
- CAN - 6 ☆
- GBR - 5 (-11)
- DEU - 5 ☆

Top Sectors

- Manufacturing - 14 (-21)
- Healthcare - 13 (-3)
- Technology - 12 ☆
- Transportation - 8 ☆
- Education - 8 (-5)

Top Groups

- Lockbit3 - 17 (-71)
- Play - 12 ☆
- Icransom - 11 (-2)
- Arcusmedia - 11 (+3)
- Ransomhub - 10 (+4)

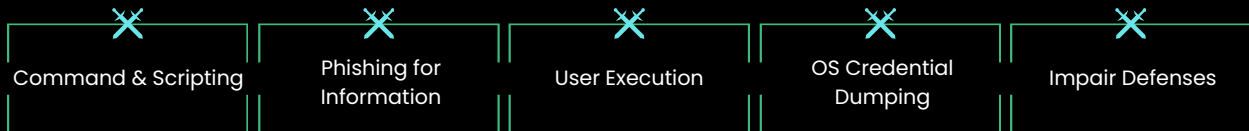


> 10
0 - 10

Victims

- Ransom Victim:** Cusat | Group: arcusmedia | Sector: Technology | Country: Argentina
- Ransom Victim:** Colégio Nova Dimensão | Group: arcusmedia | Sector: Education | Country: Brazil
- Ransom Victim:** Grupo SASMET | Group: arcusmedia | Sector: TBD | Country: Brazil
- Ransom Victim:** Cusat | Group: arcusmedia | Sector: Technology | Country: Argentina
- Ransom Victim:** Frigorífico Boa Carne | Group: arcusmedia | Sector: Manufacturing | Country: Brazil
- Ransom Victim:** Grupo SASMET | Group: arcusmedia | Sector: TBD | Country: Brazil
- Ransom Victim:** RIO TECHNOLOGY | Group: arcusmedia | Sector: Technology | Country: Colombia
- Ransom Victim:** Matadero de Gijón | Group: ransomhub | Sector: Energy | Country: Spain
- Ransom Victim:** Motor Munich | Group: dragonforce | Sector: Commerce | Country: Spain
- Ransom Victim:** Coplosa | Group: 8base | Sector: Manufacturing | Country: Spain

Top MITRE TTP covered:



Data added to Digital Adversary in the last week



TTP'S **37**

Top 3 Most Relevant

- User Execution: Malicious File
- Phishing for Information: Spearphishing Attachment
- Boot or Logon Autostart Execution: Registry Run Keys /Startup ForIde



Threat Actors **8**

Top 3 Most Relevant

- Turquoisegreen Cosmos Taurus
- EMBARGO Ransomware Group
- Zero Tolerance Gang



CVE's **—**

Top 3 Most Relevant

- CVE-2021-44228 (10)
- CVE-2022-36067 (10)
- CVE-2021-22893 (10)



Tools **2**

Top 3 Most Relevant

- Mirai Botnet
- Gomir
-

xMDR

ADVERSARIALLY
weekly report
May 16 - 23, 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.