

WR



Adversarially

Weekly Report



JUN/ 27 - JUL/ 4

2024



xMDR
powered by Cipher

ADVERSARIALLY

weekly report

June 27 - July 4, 2024



Adversary of the Week



Hunt3r Kill3rs

Type: Group

Countries:

Maturity:

Sectors: All

Activity: Cybercrime

TTPs: Sell access



CyberVolk

Type: Hacktivist Group

Countries:

Maturity:

Sectors: Retail, Finance, Government, News...

Activity: Hacktivism

TTPs: Ransomware



RansomHub

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 35

ADVERSARIALLY

weekly report

June 27 - July 4, 2024



Global

- Remote control software **TeamViewer** warns that its corporate environment has been breached in a cyber attack by the Russian APT29 group (Cozy Bear, NOBELIUM, Midnight Blizzard), the extent of the data breach is not yet known.
- Another alleged data breach related to **Snowflake** has been detected: 4 million students' information is for sale for \$2 million. The threat actor "Sp1d3r," known for Snowflake-related data breaches, is now selling millions of students' information allegedly exfiltrated from LASchools[.]net and Edgenuity.
- **KT Corporation**, South Korea's largest ISP, is under investigation for installing malware on the computers of 600,000 users to block P2P file-sharing services. Police have charged 13 employees and subcontractors. KT defends itself by claiming that the affected software was malicious.
- **Hunt3r Kill3rs** claims that Supervisory Control and Data Acquisition (SCADA) systems in Germany have been hacked. It states that this attack was carried out because warnings were not taken seriously.
- **Leukemia** has allegedly leaked the data belonging to the Information Monitoring System from the Thailand Directorate of Intelligence of the Royal Thai Army. This data included 2,939 files of secret documents and PDFs from 2019 to May 2024.
- The Romanian branch of **NTT DATA**, has been listed as a victim by the RansomHub ransomware group. The hackers allegedly exfiltrated 230 GB of data.
- **CyberVolk**, a formidable group of hackers and cybersecurity experts from Russia, have released their own ransomware named "CyberVolk Ransomware". The encrypted file have the '.cvenc' extension. The ransom note is named "CyberVolk_Readme.txt"



Spain & Latam





- A massive crash is affecting the apps of major **Spanish banks**, including Caixabank, Imagin, ING and Sabadell, preventing users from accessing their services. The banks have acknowledged the problem and are working on a solution. It could be a cyberattack related to suppliers.
- The Guardia Civil has arrested two people responsible for more than 100 cyberattacks on public bodies and private entities, both national and international, operating under the pseudonym "**GUARDIACIVILX**". The cyberattacks, which began in October 2022, compromised networks and login credentials, which were sold on cybercrime marketplaces. The investigation, in collaboration with other agencies, included the interception of cryptocurrencies and culminated in the arrests in Seville and Asturias.
- Data Leak at the **Barcelona Chamber of Commerce** It has been reported that the Barcelona Chamber of Commerce suffered an attack that compromised its database, exposing critical information of associated companies and individuals. This incident may have serious consequences for the operations of the affected companies.
- A user of a hacking forum put up for **sale several databases** supposedly belonging to the company **Rappi**, with more than 52 million records from 5 countries, including Colombia, Peru, Mexico and Brazil.
- Cyber attacker **IntelBroker** reportedly leaked a 6.74GB collection of source code from #Actinver, a leading private investment management bank. "In July 2024 Actinver Mexican bank, suffered a data breach that compromised its intranet".



Vulnerabilities & Exploits

- A threat actor is allegedly selling a **0-Click Google Keep Client-Side DOS** vulnerability for \$1,500. This vulnerability can be exploited against millions of users and cause very significant damage on a large scale.
- A threat actor is allegedly selling a **0-Day Oneclick RCE to ClassLink Agent** (Windows). The RCE can be triggering just by visiting a webpage (html) the victim should click on "allow" also it support process continuation the 0day is reliable 100%.
- A **critical remote code execution (RCE) vulnerability** has been discovered in SSH. Although it is difficult to exploit, if it were to be exploited, it would be a high risk as SSH use is very common in the enterprise environment.

Warning of the week

- Hey **Google Keep users**, heads up! A threat actor is allegedly selling a \$1,500 0-Click DOS vulnerability that could impact millions. Stay alert and keep your app updated to avoid any headaches! 
- **ClassLink Agent users**, listen up! A 0-Day Oneclick RCE exploit for Windows is on the market. All it takes is a webpage click on "allow" to wreak havoc. Patch immediately and stay vigilant! 
- **SSH users**, beware! A critical RCE vulnerability has been discovered. It's tough to exploit but could be disastrous if breached. Ensure your systems are secured and updated! 
- **TeamViewer corporate users**, alert! Russian APT29 (Cozy Bear) has breached the environment. The full extent is unknown, so stay cautious and monitor your systems closely! 

ADVERSARIALLY

weekly report

June 27 - July 4, 2024



Ransomware

Total Victims = 97 (-10)

- Spain - 1
- Latam - 5
- WorldWide - 91 (-14)

The king is...



Data of the week

Top Countries

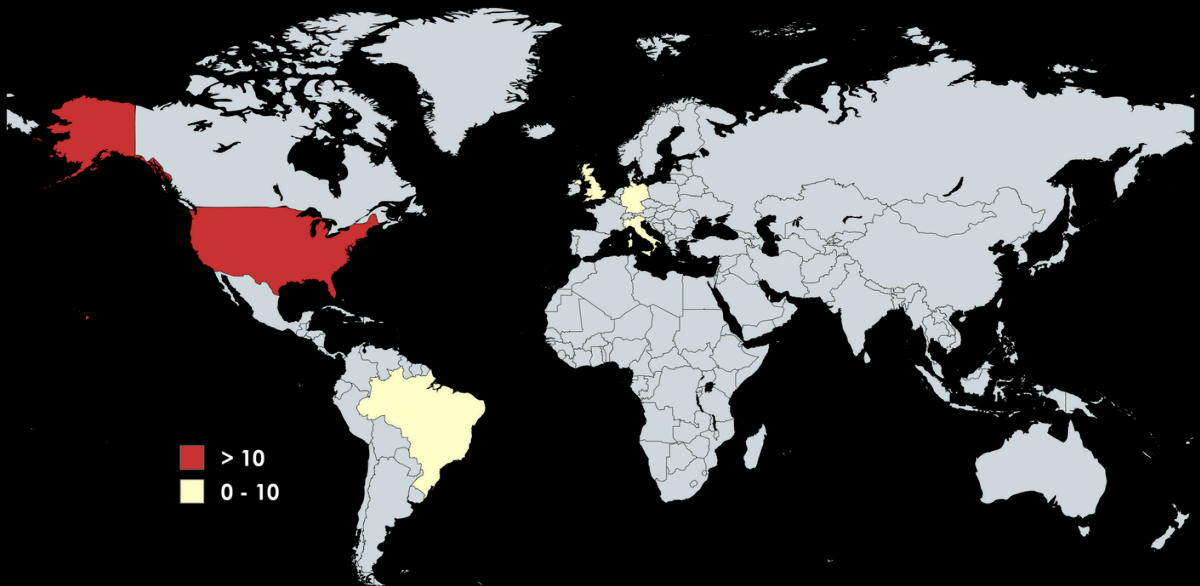
- USA - 66 (+39)
- GBR - 7 (+4)
- ITA - 6 ☆
- DEU - 4 ☆
- BRA - 4 (+2)

Top Sectors

- Manufacturing - 14 (+3)
- Technology - 11 (-1)
- Healthcare - 8 (-1)
- Retail - 5 ☆
- Transport - 5 ☆

Top Groups

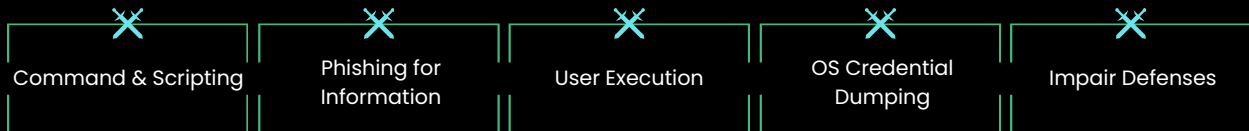
- Ransomhub - 18 ☆
- Akira - 8 ☆
- Dragonforce - 7 ☆
- Arcusmedia - 7 ☆
- Cactus - 6 ☆



Victims

- Ransom Victim:** Salton | Group: akira | Sector: TBD | Country: Brazil
- Ransom Victim:** Sicoob.com.br | Group: ransomhub | Sector: TBD | Country: Brazil
- Ransom Victim:** life.vet.br | Group: darkvault | Sector: TBD | Country: Brazil
- Ransom Victim:** equinocioplay.com.br | Group: ransomhub | Sector: TBD | Country: Brazil
- Ransom Victim:** Explomin | Group: akira | Sector: TBD | Country: Peru
- Ransom Victim:** Gestores Administrativos Reunidos | Group: ransomhouse | Sector: TBD | Country: Spain

Top MITRE TTP covered:



Data added to Digital Adversary in the last week



TTP'S 36

 **Top Most Relevant**

- Exploit Public-Facing Application
- Ingress Tool Transfer
- Phishing



Threat Actors 6

 **Top Most Relevant**

- DarkSalmon Cosmos Taurus
- Darkred Cosmos Taurus
- Black Masker Army



CVE's 1

 **Top Most Relevant**

- CVE-2017-3506

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.