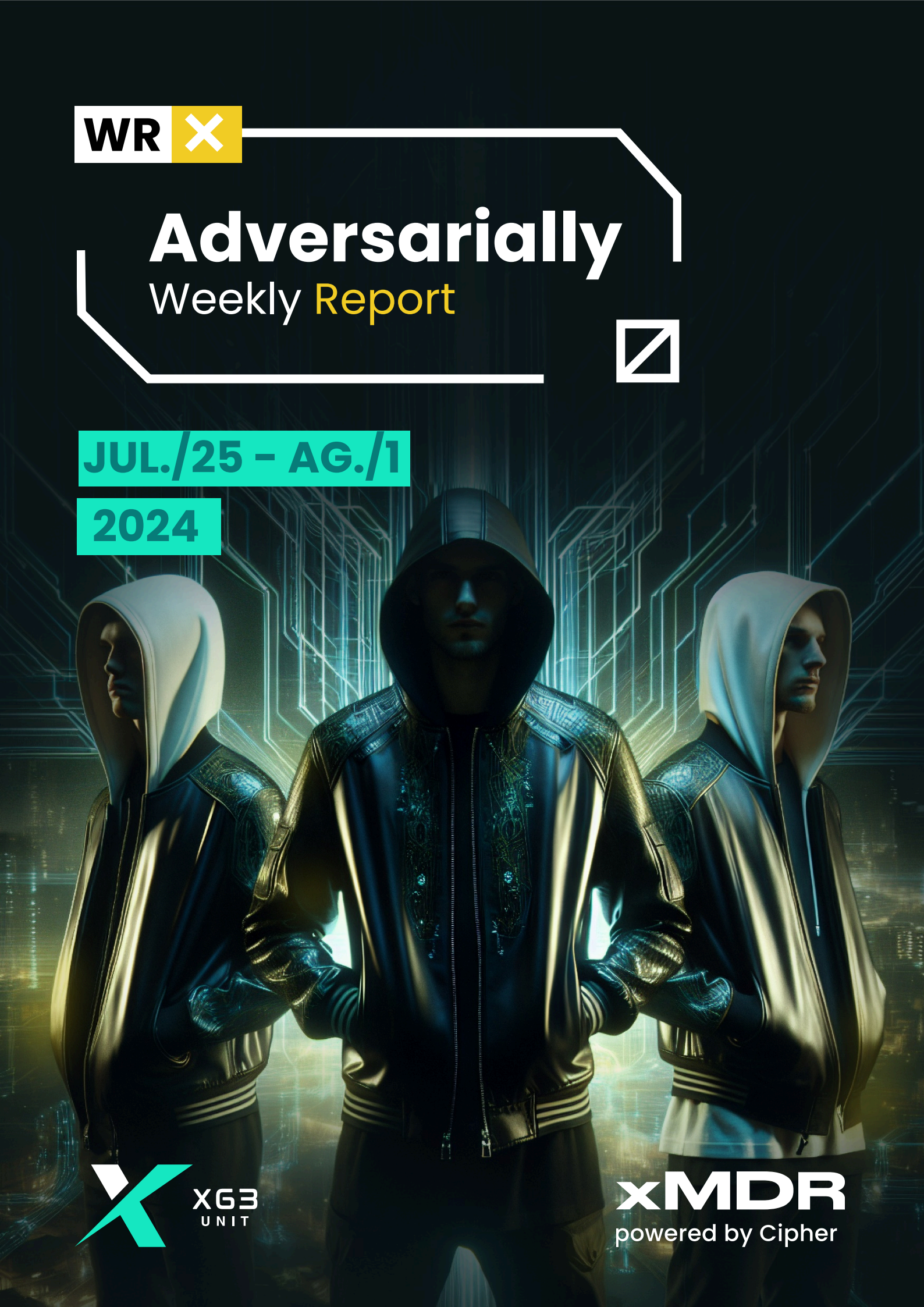
WR X

Adversarially

Weekly Report

JUL./25 – AG./1

2024



XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY
weekly report
July 25 - Aug 1, 2024

XG3 UNIT

Adversary of the Week

Rust Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Administration

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Periwinkle Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Finance, Defense, Government

Activity: Cybercrime

TTPs: Exploit Public-Facing Application

RansomHub

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 35

xMDR
powered by Cipher

ADVERSARIALLY
weekly report
July 25 - Aug 1, 2024

XG3 UNIT

Global

- **Periwinkle Cosmos Taurus** sells on Breachforum, an unauthorized access to critical repositories and social accounts of a well-known programming language. The offered access includes the language's NPM (Node Package Manager) and GitHub accounts, encompassing all private repositories.

- **Play Ransomware** has claimed on its Telegram channel to have formed an **alliance with LockBit.** According to the alleged talks, the agreement between the parties involves a **payment of $35,000 by Play Ransomware** in **exchange for LockBit tools**. In addition, **LockBit** will **offer its expertise and methods** to improve Play Ransomware's operational effectiveness and reach.

- Microsoft 365 users are falling victim to phishing campaigns that are leveraging email accounts of affected business partners and vendors to send emails with links that redirect users to a Microsoft 365 or Adobe phishing page.

- Ads from e-commerce sites using the **Polyfill.io** service have been blocked by Google after a **Chinese company acquired the domain and modified the JavaScript library** ('polyfill.js') to redirect users to **malicious and fraudulent sites**. More than 110,000 sites comprising the library were affected by the supply chain attack.

ADVERSARIALLY
weekly report
July 25 - Aug 1, 2024

XG3 UNIT

Spain & Latam

- Several threat groups including **NoName057(16), Holy League and CyberArmiyya** have been posting messages on their Telegram channels claiming to have **attacked various Spanish entities and websites**, including the Port of Cartagena, the Port of Palma de Mallorca and others.

- **Unidentified group** has announced that it has **gained unauthorized access to the Pipeline systems in Spain**. According to telegram messages made by the group, they currently maintain persistent access to these systems but have not yet caused any damage.

- **Willpowerorange Cosmos Taurus** offers on Breachforum a database containing more than 18 GB (8,000 photo files) of Mexican voter credentials.

- **Verypaleorange Cosmos Taurus** actor published a database of Tarjeta Naranja cardholders with 200,000 rows detailing full name, mobile phone number, address, city, card number and ID number.

- **Tangerineorange Cosmos Taurus** sells on Breachforum an unauthorized internal VPN access to military Police of São Paulo.

- **Chocolatebrown Cosmos Taurus** sells on Breachforum data of Ministry Df Health Of Peru (DIGESA). The DIGESA website, part of the Peruvian Ministry of Health (MINSA), typically offers information on environmental health.

- **Rust Cosmos Taurus** sells on Breachforum data leak purportedly includes sensitive personal information of over 78,711 citizens of Nuevo Leon affiliated with PRI and PAN. This data encompasses full names, voter IDs, addresses, CURPs (Unique Population Registry Codes), dates of birth, and affiliation dates.

ADVERSARIALLY
weekly report
July 25 - Aug 1, 2024

XG3 UNIT

Vulnerabilities & Exploits

- Microsoft warned today that ransomware gangs are actively exploiting a VMware ESXi authentication bypass vulnerability in attacks. Tracked as **CVE-2024-37085**, enables attackers to add a new user to an 'ESX Admins' group they create, a user that will automatically be assigned full administrative privileges on the ESXi hypervisor.

- **Palegoldenrod Cosmos Taurus** is selling on Breachforum a **remote code execution (RCE) exploit for the Albatross Protocol** for $10,000. According to the post, the exploit leverages a buffer overflow vulnerability, though it faces limitations with certain security measures.

- **Palegoldenrod Cosmos Taurus** is selling on Breachforum a LPE 0-day in the Linux kernel for $169,000. According to the post, the exploit affect kernels 6.8.12 to 6.8.8.

- A security issue in the latest version of **WhatsApp** for Windows **allows malicious Python and PHP attachments to be sent and executed without warning** when the recipient opens them. For the attack to succeed, Python must be installed, a prerequisite that can limit the targets.

- **CVE-2024-21413:** a **zero-day** vulnerability in the **Outlook mail manager**, caused by **insufficient validation of user-supplied input in Microsoft Outlook**. This vulnerability **allows a remote attacker to send emails executing malicious code on the recipient's system**, without the need for the user to click on any link in the email received.

ADVERSARIALLY
weekly report
July 25 - Aug 1, 2024

XG3 UNIT

⚠ Warning of the week

- Ransomware gangs exploiting VMware ESXi? It's like giving the wolf a key to the henhouse. **Patch your systems ASAP and keep your ESXi Admins group exclusive.** Otherwise, your hypervisor might get some very unwelcome administrators.

- Albatross Protocol has a $10,000 price tag on an RCE exploit. Time to shore up those buffer overflows before they sink your security. **Patch promptly**—don't let your network fall prey to this seabird of bad news.

- A Linux kernel LPE 0-day going for $169,000 is no small change. **Ensure your systems are up-to-date**, or that hefty price tag might be the least of your concerns.

- WhatsApp for Windows has a bug that lets malicious Python and PHP attachments slip through unnoticed. **If Python is installed, your PC could be in for a nasty surprise. Stay vigilant with attachments**—sometimes it's the script kiddies who are playing the pranks.

- A zero-day in Outlook that doesn't even need a click? Now that's a party crasher. **Update your Outlook and tighten your email security** before a rogue email turns your inbox into a malware minefield.

ADVERSARIALLY
weekly report
July 25 - Aug 1, 2024

XG3 UNIT

Ransomware

Total Victims = 139 (+31)

- Spain - **5** (+3)
  Latam - **3** (+1)
  WorldWide - **131** (+27)

The king is...

Data of the week

Top Countries

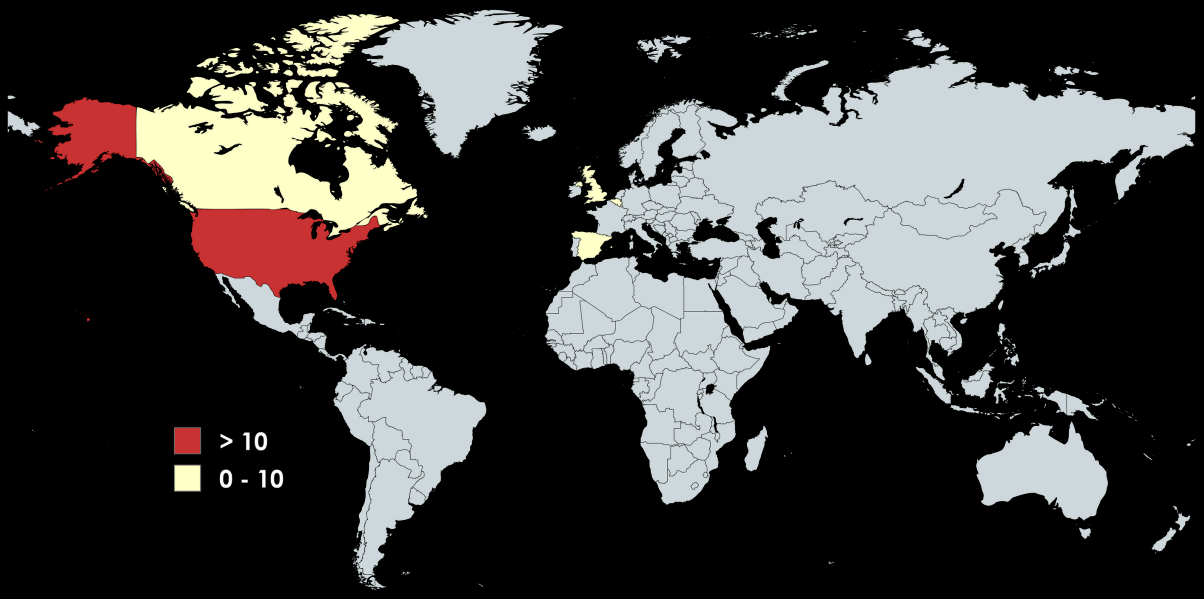
- USA - **65** (+14)
- GBR - **7** (+4)
- BEL - **6** ☆
- CAN - **6** (+2)
- SPA - **5** ☆

Top Sectors

- Manufacturing - **25** (+15)
- Technology - **17** (-5)
- Construction - **10** ☆
- Education - **9** (+2)
- Healthcare - **9** (-2)

Top Groups

- Ransomhub - **23** (+7)
- Cactus - **10** (+6)
- Akira - **9** ☆
- Meow - **7** ☆
- Play - **7** ☆



Victims

- **Ransom Victim:** oficina.oficinadasfinancas.com.br | Group: ransomhub | Sector: Finance | Country: Brazil
- **Ransom Victim:** Nuclep | Group: meow | Sector: Engineering | Country: Brazil
- **Ransom Victim:** Vivara | Group: medusa | Sector: Commerce | Country: Brazil
- **Ransom Victim:** Gemicar | Group: spacebears | Sector: Manufacturing | Country: Spain
- **Ransom Victim:** ORBINOX | Group: madliberator | Sector: Manufacturing | Country: Spain
- **Ransom Victim:** Industrial Bolsera | Group: donutleaks | Sector: Manufacturing | Country: Spain

ADVERSARIALLY
weekly report
July 25 - Aug 1, 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

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

Threat Actors 7

Top Most Relevant

- Lightlategray Cosmos Taurus
- Slate Cosmos Taurus
- Lockbit 3.0

xMDR

ADVERSARIALLY

weekly report

July 25 - Aug 1, 2024

xMDR

powered by Cipher