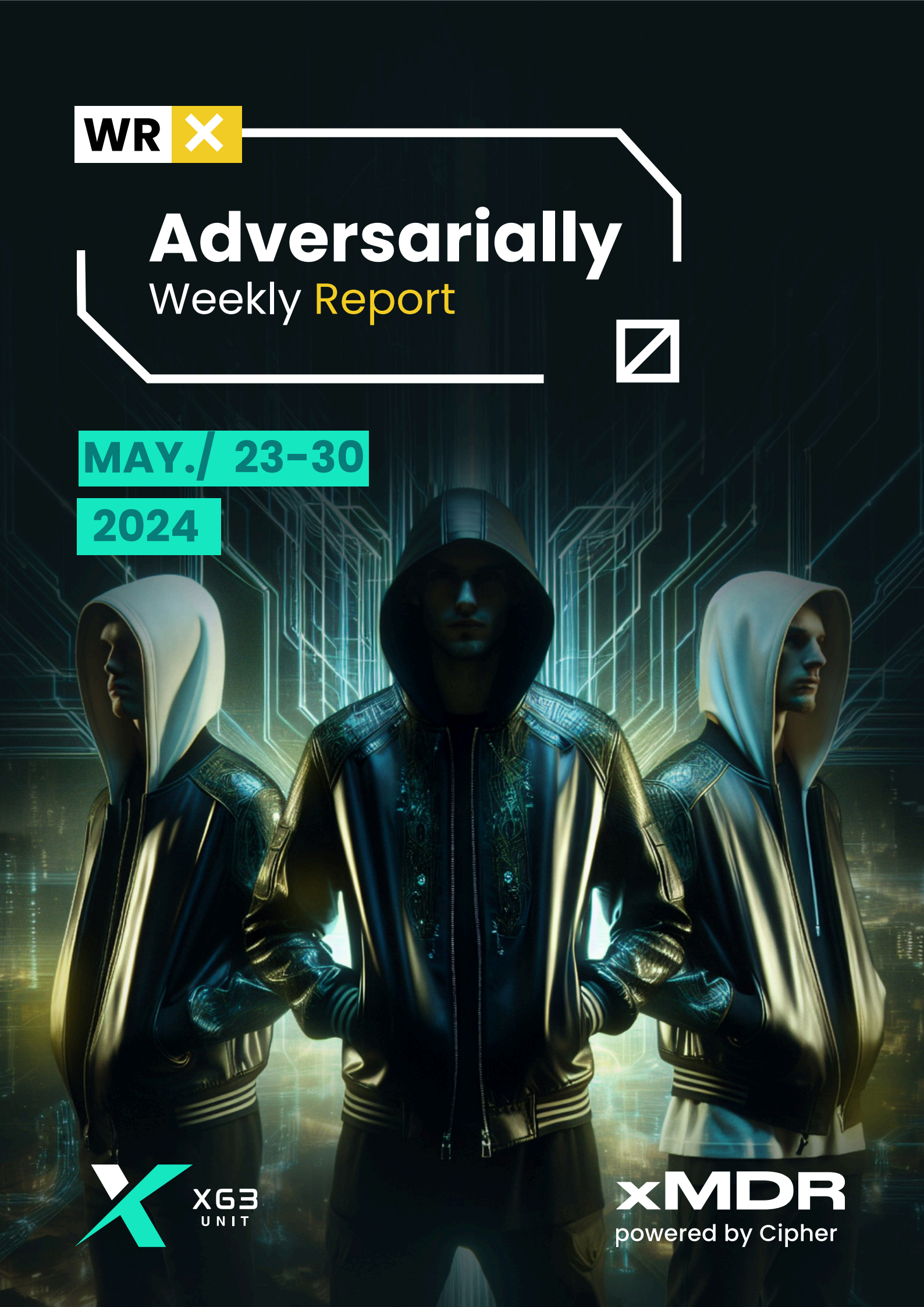
WR X

Adversarially

Weekly Report

MAY./ 23-30

2024



XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY
weekly report
May 23-30, 2024

XG3 UNIT

Adversary of the Week

Lightlategray Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: All

Activity: Cybercrime

TTPs: Sell acess

Noname057(16)

Type: Hacktivist Group

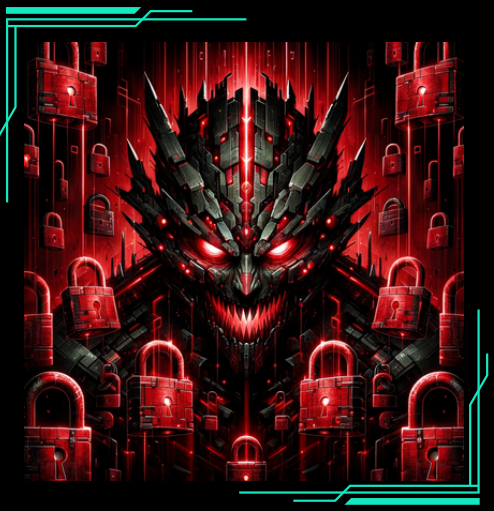
Countries:

Maturity:

Sectors: Retail

Activity: Hacktivism

TTPs: DDoS, Defacement



LockBit 3.0

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 54

ADVERSARIALLY
weekly report
May 23-30, 2024

XG3 UNIT

Global

- The popular **BreachForums** forum **is active again** after several days of suspension by the FBI. It has a page **on the clearweb** as well as **an .onion link** on the TOR network.

- BreachForum owner **ShinnyHunters** is **selling** the data of more than **500M Live Nation/TicketMaster users for $500k.**

- **Transparent Tribe**, a Pakistan-linked actor, is carrying out a series of **attacks against** various **critical sectors** such as government, defence and aerospace companies in India by **deploying malwares** written in Python, Goland and Rust. Additionally, it is conducting a **phishing campaign masquerading** as applications such as **Slack, Discord or Telegram.**

- **Linen Cosmos Taurus** is selling 3 administrator logins and a list of 50 login/password to an unidentified Korean organisation with a 30k co revenue, for 1800$.

- **Pacificblue Cosmos Taurus** offers on BreachForums the database of the Chinese company CNSERVERS, with private information of more than 440k users.

- **Turquoisegreen Cosmos Taurus** claims to have allegedly obtained internal Palm Beach County Government documents, including PDFs and .xls reports.

- **Lightlategray Cosmos Taurus** offers on BreachForums a list with more than 21k lines of private personal information about various Audi car company locations.

- **Storm-0539** is carrying out a **phishing campaign** via SMS and email in which it is **committing gift card fraud** and theft. The goal would be to redeem the value associated with these cards or sell them to other threat actors.

- **Updte:** UnitedHealth Group CEO Andrew Witty has admitted to making the $22 million ransom payment via Bitcoin to the APLHV group for the ransomware attack on Change Healthcare. He also admitted that they did not recover the encrypted data.

- **Vividorangepeel Cosmos Taurus** sells **Citrix access** to an unknown company with $10B revenue in the **insurance sector**. The sale is in auction format and starts at $25,000.

ADVERSARIALLY
weekly report
May 23-30, 2024

XG3 UNIT

Spain & Portugal

- **Lightlategray Cosmos Taurus X** offers on BreachForum information on more than 6500 employees of the Spanish company Decathlon.

- **Alabaster Cosmos Taurus X** offers in BreachForum more than 2M lines of information about Telefónica's customers and information about approximately 120k employees.

- An **unknown actor** offers on a Russian-language forum to sell **several million customer and employee data of Banco Santander**. It would contain information such as account numbers, credit card numbers, balance, personal information, etc. The sale is **for 2 million dollars in Bitcoin.**

- On 27 and 28 May, the **Noname057(16) group** carried out several **DDoS attacks** against the websites of various **mobility services in Madrid and Barcelona**, as well as against the **website of the Madrid Parliament**.

- The Organisation of Consumers and Users **(OCU) and the Bank of Spain** have **warned** about a **new attack** called **bluesnarfing**, in which threat actors **exploit** the vulnerability of **your mobile device's bluetooth** and connect to it to **steal information**. Although permission is almost always requested to connect to your device, cybercriminals sometimes make use of software that prevents this security measure.

- The electricity company **Ibredrola** suffered a cyber-attack on one of its suppliers that has resulted in the **leakage of contact and personal information** of more than **850,000 customers**. According to the company, no financial data was affected.

ADVERSARIALLY
weekly report
May 23-30, 2024

XG3 UNIT

LATAM

- The hacktivist group **GlorySec** has **gained access to 50 websites** of various **Venezuelan companies** during the so-called #OPVenezuela.

- **Ruddy Cosmos Taurus X** is offering on BreachForums a database in .csv format of the City Hall of Angra dos Reis, Brazil, containing private personal information of citizens.

- **Citizens in Latin America** have been alerted to a **campaign of scams** related to the recovery of stolen cryptocurrencies. The cybercriminals demand an initial payment to recover your cryptocurrencies but you never receive the service.

ADVERSARIALLY
weekly report
May 23-30, 2024

Vulnerabilities & Exploits

- **Wenge Cosmos Taurus** is selling a 0-day Remote Code Execution (RCE) exploit for Pulse Connect Secure VPN on a popular russian-language forum.
- **Safetyyellow Cosmos Taurus** sells a WordPress Admin Authentication bypass exploit for $50,000 on a popular Russian-language forum.
- **CVE-2024-5035:** A critical vulnerability affecting all versions of the **TP-Link Archer C5400X gaming router.** This vulnerability allows **remote code execution** on vulnerable devices.

ADVERSARIALLY
weekly report
May 23-30, 2024

XG3 UNIT

⚠️ Warning of the week

- A **0-day RCE for Pulse Connect Secure VPN** is the cyber equivalent of a golden ticket—for hackers! **Patch your VPNs**, and remember, security updates not always fun, but good for you!🔒🔧

- **WordPress** admin bypass exploit sell? It's way to mess up your site! **Update your plugins and themes, use strong passwords**, and remember: keeping your site secure is cheaper than a hacker's attack! 💻💸

- Got a **TP-Link Archer C5400X? Update that firmware ASAP!** This router's got a vulnerability that lets hackers in faster than you can say 'Game Over.' Secure it now and keep those digital invaders at bay! 🎮🔒

ADVERSARIALLY
weekly report
May 23-30, 2024

XG3 UNIT

Ransomware

Total Victims = 57 (-70)

- Spain - **1** (-4)
  Latam - **0** (-11)
- WorldWide - **56** (-55)

The king is...

Data of the week

Top Countries

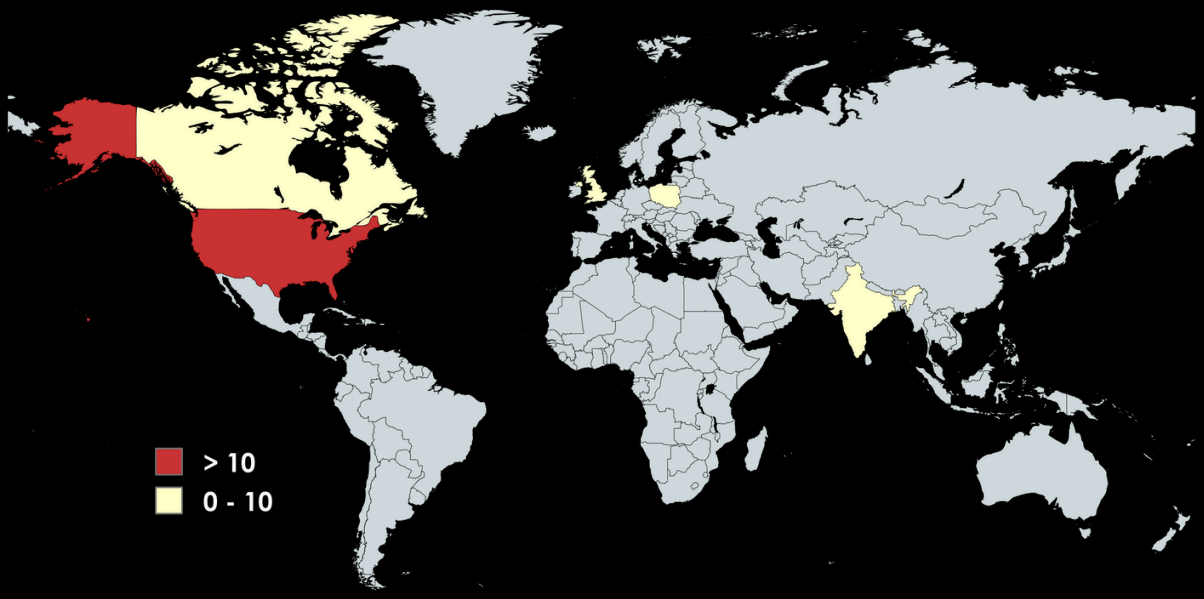
- USA - **31** (-40)
- GBR - **7** (-6)
- IND- **3** ☆
- CAN - **3** (-2)
- POL - **2** ☆

Top Sectors

- Healthcare - **11** (-2)
- Manufacturing - **10** (-4)
- Technology - **4** (-8)
- Energy - **4** ☆
- Construction - **3** ☆

Top Groups

- Lockbit3 - **13** (-4)
- Play - **12** ☆
- Icransom - **7** (-4)
- Ransomhouse - **6** ☆
- Blacksuit - **5** ☆



Victims

- **Ransom Victim:** cafesnovell.com | Group: lockbit3 | Sector: Commerce | Country: Spain

ADVERSARIALLY
weekly report
May 23-30, 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 63

Top 3 Most Relevant

- Network Denial of Service
- Exploit Public-Facing Application
- Phishing: Spearphishing Attachment

Threat Actors 3

Top Most Relevant

- SideWinder
- AnonymousEgypt
- Wildstrawberry Cosmos Taurus

CVE's 4

Top Most Relevant

- CVE-2024-22120
- CVE-2024-27130
- CVE-2024-4367

Tools 3

Top Most Relevant

- Agent Tesla
- Babuk
- 3PARA RAT

xMDR

ADVERSARIALLY

weekly report

May 23-30, 2024

cipher

a Prosegur company