WR X

Adversarially

Weekly Report

JUNE/ 13 - 20

2024

XG3 UNIT

xMDR powered by Cipher

ADVERSARIALLY
weekly report
June 13 - 20, 2024

XG3 UNIT

Adversary of the Week

Pineapple Cosmos Taurus

Type: Individual

Countries: 🌍

Maturity: 🟩⬛⬛

Sectors: All

Activity: Cybercrime

TTPs: Sell acess and information

Arid Viper

Type: Hacktivist Group

Countries: 🌍

Maturity: 🟧🟧⬛

Sectors: Education, Government,Technology

Activity: APT

TTPs: 56

Play

Type: Group

Countries: 🌍

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 36

Global

- **Lightsteelblue Cosmos TaurusX** is selling on BreachForum the database of users of the Chinese University of Hong Kong, including staff, students and graduate students.

- **Richblack Cosmos Taurus X** offers in LeakBase 900 Bitwarden accounts with login IDs and passwords.

- **Mediumslateblue Cosmos Taurus X** is selling on XSS 6TB of data to an unidentified European Biomedical Company with US contracts for $3,500.

- **Mediumslateblue Cosmos Taurus X** is selling access to a UK bank server with revenues approaching $200 million. Access is full root privileges, API access and more for $10,000.

- **IntelBroker has returned** to BreachForum and since 16 June has shared a number of posts. Among them is the **sale of a zero-day RCE for Atlassian's Jira**. He has also shared **classified documents from the US Department of Defence**, as well as the **source code for 3 very common Apple applications.**

- Several **spying campaigns** by the APT group **Arid Viper** have been detected, distributing **trojanised apps with the AridSpy** malware to Android users in Egypt and Palestine.

- Cybersecurity researchers have discovered a **new ransomware called ShrinkLocker** that **exploits BitLocker's security features** to encrypt corporate files. In addition, this ransomware removes the recovery option and deletes logs.

- **Pineapple Cosmos Taurus X** sells a new data breach related to the **SnowFlake** attack at BreachForum. In this case it involves the sale of **data on more than 4 million LASchools and Edgenuity students.** The price is 30BTC which is equivalent to approximately $2M.

Spain & Portugal

- **Pineapple Cosmos Taurus** is selling a new data leak from Banco Santander on BreachForum, affecting customers in Spain, Uruguay, and Chile. The database contains **1.6 billion lines of information** on customers, accounts, and banking transactions.

- The **DGT** has alerted about a **new phishing campaign** in which they try to obtain victims' information under the pretext of an unpaid fine. This campaign could be a **consequence of the data breach the DGT suffered last May**, in which thousands of users' data were exposed.

- The engineering and technology company **Amper** has **suffered a cyberattack** in which cybercriminals obtained more than **650GB of data** related to projects, users, and employees.of data related to projects, users, and employees.

- The political party **Esquerra Republicana has reported** to the Mossos d'Esquadra a **cyberattack** suffered this past Saturday, which resulted in **part of the party's database being exposed**. The group has not confirmed whether the data pertains to party members or leaders.

- **Illuminating Cosmos Taurus** is selling a database of Spanish citizens on XSS for $25K, which contains full names and addresses, DNI numbers, and dates of birth. They also offer a search option for $150.

LATAM

- **Illuminating Cosmos Taurus** is selling RDP access to the RMM tools of Brazil Telecom, which has revenues of 16 million dollars, for 1000$.

- **Illuminating Cosmos Taurus** is selling on XSS admin access to a Telecom Orion account that manages approximately 200 customers, including banks, trust funds, petroleum stations, etc., for $25,000.

- **Magicmint Cosmos Taurus** is offering on LeakBase the ExpoInclusion Uruguay database, which contains users and passwords from various companies, encoded only in base64.

- **Red Cosmos Taurus** is offering on BreachForum around 5 million records from Ecuador's citizen database, obtained via scraping activities in 2024. This includes 5,360,157 records and 11.7 GB of data.

- **Red Cosmos Taurus** is selling on BreachForum a database of Ecuadorian users from the Spanish telecommunications company Tuenti for $50.

- A campaign has been alerted targeting companies in Latin America, where cybercriminals distribute RATs (Remote Access Trojans) through emails impersonating HR departments.

- The **database** containing usernames and passwords from the intranet of the **Secretaría de Seguridad Ciudadana (SSC) of Mexico City has been leaked**. This leak specifically affects the "Sistema ATLAS," where sensitive information related to police intelligence is captured. The identity of the actor or actors responsible is still unknown.

Vulnerabilities & Exploits

- **Peru Cosmos Taurus** is selling on BreachForum a 0-day RCE vulnerability for Dahua cameras. The exploit is compatible with all versions of the device and is priced at $400,000.

- **Limegreen Cosmos Taurus** is selling on XSS a RCE exploit for QuickBooks, an accounting software designed for keeping track of income and expenses. The price is $1,000,000.

- **Update:** Asus has released several **patches** for various critical vulnerabilities. Among them is **CVE-2024-3080,** an authentication bypass vulnerability that allows unauthenticated remote attackers to take control of the device.

- **Alert 0-Day:** Possible **PHP injection detected.** Attackers are exploiting **CVE-2024-4577**, a PHP-CGI command injection flaw, to execute code and distribute TellYouThePass ransomware via a malicious HTML application.

- **CVE-2024-30103: Microsoft Outlook RCE vulnerability.** Can be circulated from user to user and doesn't require a click to execute. Rather, execution initiates when an affected email is opened.This is notably dangerous for accounts using Microsoft Outlook's auto-open email feature.

- **Lavenderpurple Cosmos Taurus** is selling on Breachforum an exploit for CVE-2024-30078, a remote code execution (RCE) vulnerability in the WiFi driver that affects all devices running Windows Vista and later.

- A vulnerability listed as **CVE-2024-37313** has been discovered in **NextCloud** that allows threat actors to **bypass the second authentication factor.**

- **CVE-2024-37079 & CVE-2024-37080 with scores 9.8:** Multiple heap-overflow vulnerabilities in the implementation of the DCE/RPC protocol! They could allow a bad actor with network access to vCenter Server to achieve remote code execution by sending a specially crafted network packet.

ADVERSARIALLY

weekly report

June 13 - 20, 2024

X G3 UNIT

⚠️ Warning of the week

- Hey! A threat actor is selling a $400k RCE exploit for **Dahua cameras.** Patch your cams now—don't let strangers star in your home surveillance videos! 📸🔒
- **QuickBooks** Alert! Is being sold a $1M RCE exploit for QuickBooks. Protect your finances—hackers should stay out of your business ledger! 💼🔒
- **Asus Update:** Asus has patched CVE-2024-3080, an authentication bypass flaw. Update ASAP—don't let your device become a hacker's playground!🖥️🔄
- **PHP Injection Alert: CVE-2024-4577** is a PHP-CGI injection flaw spreading ransomware. Patch up and keep your HTML squeaky clean—no malicious scripts allowed! 🌐🔒
- **Microsoft Outlook RCE:** Outlook users, CVE-2024-30103 can strike just by opening an email. Disable auto-open and keep your inbox free from nasty surprises! 📧🔒
- **WiFi Driver Exploit:** Threat actor in dark web is selling an RCE exploit for Windows WiFi drivers. Patch up and keep your WiFi hacker-free! 📶🔒
- **NextCloud vulnerability:** NextCloud users, **CVE-2024-37313** allows attackers to bypass your second factor. Update now and keep your cloud secure: no free rides! ☁️🔒
- **vCenter Server:** VMware customers, **CVE-2024-37079 and CVE-2024-37080** are serious heap overflow flaws. Don't let hackers sneak into your virtual network ⌧🔒.

ADVERSARIALLY
weekly report
June 13 - 20, 2024

XG3 UNIT

Ransomware

Total Victims = 105 (-2)

Spain - **4** (+3)
Latam - **3** (+1)
- WorldWide -**98** (-6)

The king is...

Data of the week

Top Countries

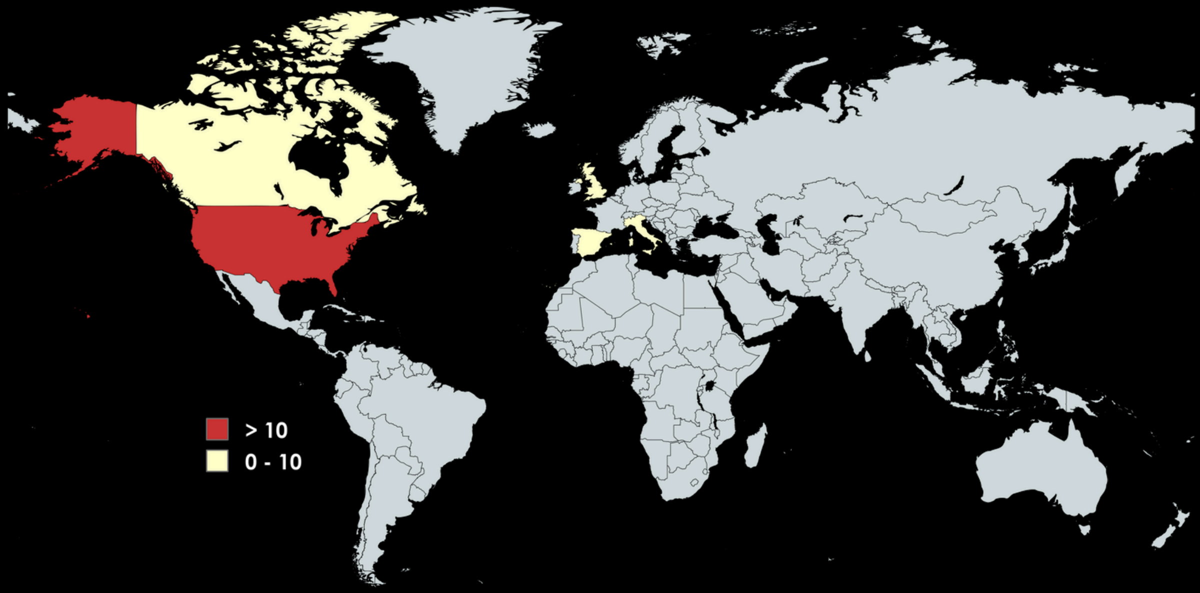
USA - **58** (-8)
CAN - **10** (+3)
GBR - **5** (+2)
ITL - **5** ☆
SPA - **4** ☆

Top Sectors

Manufacturing - **26** (+15)
Technology - **17** (+5)
Healthcare - **9**
Retail - **8** ☆
Education - **5** ☆

Top Groups

Play - **25** (+11)
Ransomhub - **8** ☆
Qilin - **7** (+1)
APT73 - **6** ☆
Medusa - **6** (-5)



Victims

- **Ransom Victim:** Parlorenzo | Group: Ransomhub | Sector: Insurace | Country: Spain
- **Ransom Victim:** Lider IT Consulting | Group: RansomHub | Sector: IT | Country: Spain
- **Ransom Victim:** Mundocar | Group: Cloak | Sector: Automotive | Country: Spain
- **Ransom Victim:** Grupo Amper | Group: BlackBasta | Sector: Defence | Country: Spain
- **Ransom Victim:** Amarilla Gas | Group: Play | Sector: Defence | Country: Argentina
- **Ransom Victim:** Cosimti SRL | Group: Dark Vault | Sector: Cybersecurity | Country: Bolivia
- **Ransom Victim:** Hospital Adventista de Manaus | Group: RansomHub| Sector: Health | Country: Brazil

ADVERSARIALLY
weekly report
June 13 - 20, 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 308

Top Most Relevant

- Command & Scripting Interpreter
- Financial Theft
- Phishing

Threat Actors 6

Top Most Relevant

- Yellowcrayola Cosmos Taurus
- Kimsuky, Velvet Chollima
- Ghostwriter, UNC1151

CVE's 2

Top Most Relevant

- CVE-2024-1800
- CVE-2024-21683

Tools 5

Top Most Relevant

- Sliver
- SansStealer
- Chameleon

xMDR

ADVERSARIALLY

weekly report

June 13 - 20, 2024

cipher

a Prosegur company