WR X

Adversarially
Weekly Report

AUG/ 22 - 29
2024

XG3 UNIT

xMDR
powered by Cipher

ADVERSARIALLY
weekly report
Aug 22 - 29, 2024

Adversary of the Week

Slateblue Cosmos Taurus

Type: Individual

Countries: 🇪🇸

Maturity: 🟩⬛⬛

Sectors: Sport

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Burntorange Cosmos Taurus

Type: Individual

Countries: 🇦🇷 🇧🇷 🇵🇪

Maturity: 🟧🟧⬛

Sectors: Finance

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Ransomhub

Type: Group

Countries: 🌍

Maturity: 🟥🟥🟥

Sectors: All

Activity: RaaS

TTPs: 35

Global

- Cybercriminals managed to **take control of McDonalds' Instagram account, creating a post** and editing the profile **to promote a cryptocurrency** called Grimace, a coin based on the Solana blockchain platform.

- **Periwinkle Cosmos Taurus X aka IntelBroker** and **Plum Cosmos Taurus X aka EnergyWeaponUser** claim to have obtained internal communications from **AMD**, including data from platforms like “idmprod.xilinx.com” and “amdsso.okta.com.” The compromised data reportedly contains a range of sensitive information such as case numbers, user credentials, case descriptions, and internal resolutions.

- The **arrest of Pavel Durov,** founder and **CEO of Telegram in France** has led several cybercriminal groups such as **UserSec and CyberDragon** to organise and carry out a **campaign of DDoS attacks against French targets,** including the website of the French National Court and the Paris court. They have also warned of attacks against insurance companies such as AXA.

- **Blue Cosmos Taurus X** claims to have leaked top secret documents from EPS Tech relating to the design of electronic equipment used by the Air Force.

- Cybersecurity researchers have discovered a **new Android malware** called **NGate**, which can steal credit and debit card payment data by transmitting NFC (Near Field Communication) information to an attacker-controlled device. It **targets banks in the Czech Republic** and **allows** criminals **to clone victims' physical cards** and use that information to perform fraudulent transactions or withdraw money from ATMs.

- A cybersecurity researcher has uncovered a **critical vulnerability** in the AI-powered assistant **Copilot**, which **enables malicious actors to exfiltrate sensitive data.** The exploit, combines several sophisticated techniques, posing significant risks to data security and privacy. It begins with the recipient **receiving a malicious email** or document containing concealed instructions. When these instructions are processed by Copilot, the tool automatically activates, searching for additional emails and documents, thereby escalating the attack without user intervention.

Spain & Latam

- **Navantia**, in charge of building the S-80 class submarines for the Spanish Navy, mistakenly **disclosed sensitive information** about the S-82 submarine in a public technical specification. **The document**, published on the state procurement platform, **included detailed plans** of the location of torpedoes, command and control systems, and other key elements. This information has been exposed to everyone and may have **fallen into the hands of actors or cybercriminal groups** who can trade it on the dark web.

- **Slateblue Cosmos Taurus X** offers a database of the Royal Spanish Athletics Federation with private information of 140K users. According to the actor the database contains each entry with ID, full name, phone number, date of birth and address.

- **Upforestgreen Cosmos TaurusX**sells on BreachForum a database of a big Italian energy company, Eni Plenitude. The alleged database contains over 800,000 rows of data, including name, email, phone number, address, IBAN, and more of Spanish citizens.

- **Popstar Cosmos Taurus X** is selling a CISCO internal management access to an infrastructure in Argentina.

- **Burntorange Cosmos Taurus X** offers a database with private information about clients of various Latin American banks.

Vulnerabilities & Exploits

- Cybersecurity researchers have discovered a **PoC** for the vulnerability listed as **CVE-2024-38063.** This is a **remote code execution (RCE)** vulnerability that affects the **Windows TCP/IP stack**, specifically when handling IPv6 traffic. It allows an unauthenticated attacker to execute arbitrary code on a target system by sending specially crafted IPv6 packets.

- Google has confirmed that **CVE-2024-7965**, a high-severity **zero-day** vulnerability in the **Chrome browser**, has been actively exploited in the wild. This newly highlighted vulnerability carries a CVSS score of **8.8** and allowed a remote attacker to potentially **exploit heap corruption via a crafted HTML page**.

- **Hillstone Networks**, has released a security advisory addressing a critical vulnerability, **CVE-2024-8073** in its **Web Application Firewall (WAF) product**. This vulnerability, rated with a CVSS score of **9.8**, allows remote attackers to **execute arbitrary code** on affected systems, potentially leading to full system compromise.

- The Chinese group **Velvet Ant exploited** a patched **zero-day vulnerability** (**CVE-2024-20399**, CVSS 6.7) in Cisco switches to **gain control over devices** and bypass threat detection systems. This vulnerability allowed the attackers to **implant a unique malware** and achieve extensive control over the compromised system. Velvet Ant leveraged the exploit to execute arbitrary commands on Linux, operating under the NX-OS shell.

- A severe security flaw (**CVE-2024-6386, CVSS 9.9**) has been discovered in the widely-used **WPML plugin for WordPress**, potentially exposing over one million websites to the risk of complete takeover. CVE-2024-6386 is a **remote code execution vulnerability stemming** from a Twig Server-Side Template Injection (SSTI) flaw in the WPML plugin, specifically affecting all versions up to, and including, 4.6.12. This vulnerability **allows authenticated users with access to the post editor to execute malicious code remotely on the server**, leading to severe consequences such as data theft, website defacement, and the installation of backdoors for future attacks.

⚠️ Warning of the week

- An IPv6 packet shouldn’t come with a side of remote code execution! Patch **CVE-2024-38063** immediately, or your system could be taken for a spin by a rogue packet. Protect your network traffic, before it drives straight into trouble.

- A crafted HTML page should be harmless, not heap havoc. With **CVE-2024-7965** actively exploited in Chrome, it’s time to update your browser. Don’t let your browsing turn into a bug hunt where you’re the prize.

- Your firewall should be guarding the gates, not leaving them wide open! Patch the critical **CVE-2024-8073** vulnerability in Hillstone Networks' WAF before attackers turn your defenses into their new playground for arbitrary code execution.

- **Velvet Ant** are more than just a pest—they’re exploiting Cisco switches with a zero-day. Patch your systems to avoid falling victim to their crafty command executions. Don’t let your network devices become a hive of attacker activity.

- A **severe flaw (CVE-2024-6386) in the WPML plugin** could leave your **WordPress** site wide open for takeover. Update now before your site becomes a hacker’s sandbox. After all, you don’t want your website content edited by someone with a malicious agenda.

ADVERSARIALLY
weekly report
Aug 22 - 29, 2024

XG3 UNIT

Ransomware

Total Victims = 132 (+18)

- Spain - **2** (+2)
- Latam - **3**
- WorldWide - **127** (+16)

The king is...

Data of the week

Top Countries

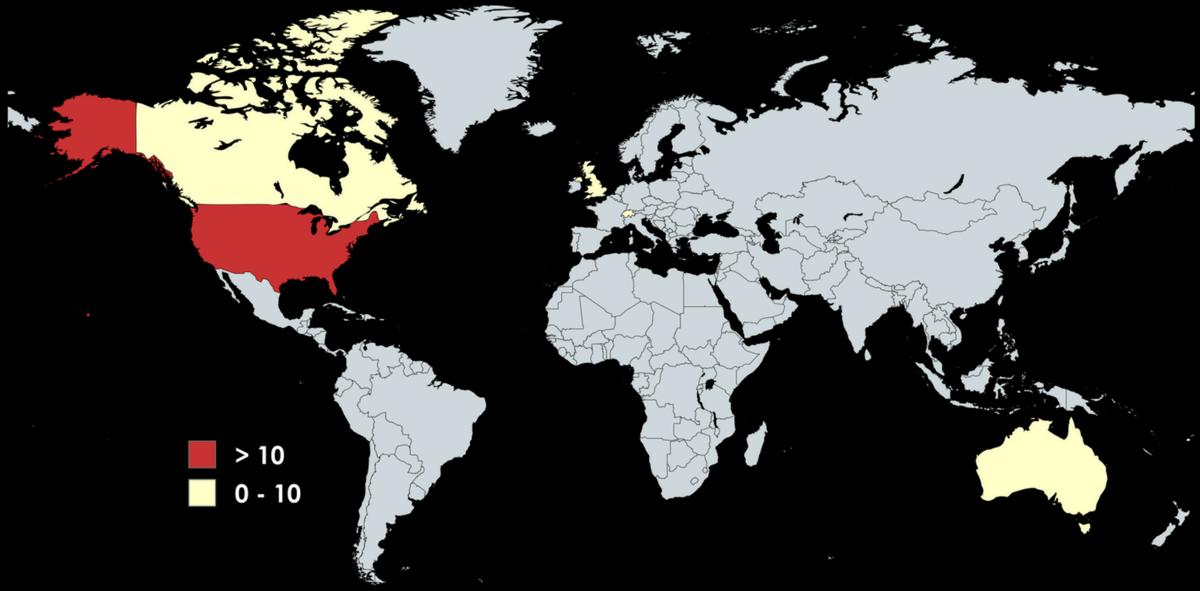
- USA - **54** (+11)
- GBR - **10** (-4)
- CAN - **6** (+3)
- AUS - **4** ☆
- CHE - **4** ☆

Top Sectors

- Manufacturing - **17** (- 3)
- Technology - **16** (+2)
- Finance - **14** (+4)
- Healthcare - **11** (+1)
- Construction- **7** ☆

Top Groups

- Ransomhub - **12** (-14)
- Meow - **12**
- Cicada3301 - **10**☆
- Helldown - **8**
- Play - **8** (+1)



Victims

- **Ransom Victim:** South American Tours | Group: meow | Sector: Tourism | Country: Argentina
- **Ransom Victim:** terralogs.com.br | Group: killsec | Sector: Agriculture | Country: Brazil
- **Ransom Victim:** Woden | Group: meow | Sector: TBD | Country: Colombia
- **Ransom Victim:** Artesanía Chopo | Group: meow | Sector: Arts and Entertainment | Country: Spain
- **Ransom Victim:** Modulkit | Group: meow | Sector: Manufacturing | Country: Spain

cipher
a Prosegur company

ADVERSARIALLY
weekly report
Aug 22 - 29, 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 43

Top Most Relevant

- Command and Scripting Interpreter
- System Information Discovery
- Phishing

Threat Actors 5

Top Most Relevant

- Hazelnut Cosmos Taurus
- Chive Cosmos Taurus
- UAC-0020

Tools 1

Top Most Relevant

- Msupedge

cipher
a Prosegur company

xMDR

ADVERSARIALLY

weekly report

Aug 22 - 29, 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.