WR X

Adversarially

Weekly Report

ABR./ 4-11

2024

XG3 UNIT

xMDR
powered by Cipher

ADVERSARIALLY

weekly report

Abr 4 - 11, 2024

Adversary of the Week

GhostWhite Cosmos Taurus

Type: Individual

Countries: 🌍

Maturity: 🟩⬛⬛

Sectors: **All**

Activity: Cybercrime

TTPs: Exploit Public-Facing Application

CyberNiggers

Type: Group

Countries: 🇺🇸

Maturity: 🟧🟧⬛

Sectors: Entertainment, Government

Activity: Cybercrime

TTPs: Indeterminated yet

Blacksuit

Type: Group

Countries: 🇺🇸

Maturity: 🟥🟥🟥

Sectors: Health, Retail, IT, Education, Government

Activity: RaaS

TTPs: **28**

Global

- **NordVPN claims** to have discovered through extensive research that more than **54 billion cookies have been leaked on the dark web**. Among the **most affected** countries are **Brazil, Indonesia or Spain** and most of the cookies from the latter were still active.

- The **CyberNiggers group** allegedly **claims** to have **breached HSBC and Barclays banks**, compromising extensive databases and source code.

- **Ghostwhite Cosmos Taurus** X has allegedly **sale of a zero-day vulnerability** tailored explicitly **for a WordPress 0-day Remote Code Execution (RCE)** exploit. The price is $15000.

- **In March**, cybersecurity experts identified **31 new ransomware variants.** This wide variety shows that threat **actors are reinventing themselves every day**. With each new variant, cybercriminals **refine their tactics, making detection and mitigation increasingly difficult.**

- Researchers at **AhnLab have identified new variants of the Cuba ransomware** that employ advanced and **complex attack methods** and are more difficult to detect and remove. Attackers are now threatening victims with the **publication of stolen data if the ransom is not paid.**

- **Periwinkle Cosmos Taurus** X and **VividMalachite Cosmos Taurus** X allegedly compromised online retailer Sugargoo, a competitor of PandaBuy, previously compromised by the same threat actors.

- The **Israeli Ministry of Justice** claims to have been a **victim of a security incident** that they are investigating. This comes after the group "**Anonymous for Justice**" **claimed** to have **gained access to the servers** of the Israeli Ministry of Justice in various coordinated attacks, allegedly **stealing nearly 300GB of sensitive and confidential information.**

Spain & Portugal

- The National Police has warned of a **new phishing campaign** on the occasion of the income tax return, in which threat actors **impersonate the Tax Agency** in order to obtain personal and financial data.

- **ZinnwalditeBrown Cosmos Taurus X** is offering on a well-known Russian-speaking forum a **database of Spanish citizens** born between 1926 and 2004, which allegedly contains **38.9 million lines of private and personal information** such as ID numbers, names, surnames, addresses, etc. The information is being sold **for $10,000.**

- **KyotoSH Security** has published through its Telegram channel several **denial-of-service attacks against** Spanish entities, including the **Bank of Spain** and the **website of the National Police.**

- **VerypaleYellow Cosmos Taurus X** is offering a database with 1.3 million pieces of private and personal information from a Spanish bank on a well-known English-speaking forum for the price of $35,000.

- **Onyx Cosmos Taurus X** offers on a well-known English forum a **database of the megacursos.com website**, which contains private information such as names, emails, phone numbers or addresses.

- **Tomato Cosmos Taurus X** is offering OpenVPN access to a Spanish company with revenue of less than $5M for $500.

LATAM

- **TA558** has deployed a **new campaign** against various sectors such as the hotel, government and financial sectors, targeting parts of **Latin America, Spain and Portugal**, in which it is **deploying the VenomRAT** malware.

- **SacramentoStateGreen Cosmos TaurusX** is offering for free on a well-known English forum a database with over **5 million photographs of citizens of El Salvador**, which also includes the DUI number. Additionally, they **add a database with PII**. In another post, the same actor also **shares private information about over 96k pregnant women**, alluding to the notion that no Salvadoran deserves to be safe.

- **SacramentoStateGreen Cosmos TaurusX** has published a **vulnerability affecting Invex Mexico**, inviting other actors to exploit it freely. The vulnerability involves the ability to **obtain the encryption password of the Invex Control app**, **causing requests to respond without token verification**, resulting in the ability to query other cards with the same user token.

- An **unknown actor** allegedly **sold the Initial Access** to a **company from Chile with a revenue of $465M** on a well-known Russian-speaking forum. This would involve corporate access through a Citrix VPN.

Vulnerabilities & Exploits

- Two **zero-day** vulnerabilities, tracked as **CVE-2024-29745 and CVE-2024-29748**, are being actively exploited by forensic companies to get their hands on device data. The two vulnerabilities **affect Google Pixel** mobile devices. The first was identified as Pixel's fastboot firmware that **supports unlocking, flashing and locking operations**. The second vulnerability allows local attackers to **interrupt factory resets triggered by applications via the device admin API.**

- Unknown threat actors have made use of a default **NotePad++ add-on** called **"mimeTools.dll"** to **execute malicious code** unnoticed by the victim, compromising the security of hundreds of systems that use it.

- **Update:** Several groups, including the notorious **Volt Typhoon**, are actively **exploiting** the known vulnerabilities **CVE-2023-46805, CVE-2024-21887 and CVE-2024-21893**, which affect the Ivanti Connect Secure and Ivanti Policy Secure gateways.

- Researchers at the **AhnLab SEcurity Intelligence Center** have detected that **Metasploit's Meterpreter** malware is being distributed **via Redis** (Remote Dictionary Server) services. Attackers could have exploited configuration errors or command executions through possible vulnerabilities.

- A new vulnerability called **HTTP/2 CONTINUATION Flood** has been discovered by researcher Bartek Nowotarski. It involves **exploiting the CONTINUATION frame to carry out Denial of Service attacks**. The threat actor could initiate a new HTTP/2 sequence against a target server by leveraging a vulnerable implementation, **sending HEADERS and CONTINUATION frames without setting the END_HEADERS flag**, generating an infinite sequence of headers that the HTTP/2 server needs to analyze and store in memory.

⚠️ Warning of the week

- **Pixel problems**, huh? Keep your Google goodies safe: **update your Pixel pronto** and **avoid shady apps** like the plague. Don't let cyber gremlins meddle with your factory resets—lock 'em out and keep your Pixel secure!📱🔒

- Watch out for **sneaky add-ons like "mimeTools.dll" in NotePad++**—they're like uninvited guests at a party, but way less fun! Kick 'em out if you don't need 'em and keep your software updated! 📝🛡️

- Last call for **Ivanti users**!📞 If you haven't yet **updated your gateways** with the latest patches it's time. Volt Typhoon and his friends are exploiting vulnerabilities 🔒

- Watch out for **sneaky malware hitching a ride on Redis**! Keep your Redis server **updated and secure**, like locking your doors at night. **Patch any vulnerabilities** pronto and stay vigilant for any suspicious activity on your network🚪🔒

- Keep an eye out for the **HTTP/2 CONTINUATION Flood**! Make sure your server's defenses are up to snuff—**patch vulnerabilities, set up rate limiting**, and keep an eye on unusual traffic patterns 💻

- Stay on guard for **TA558's** sneaky tricks! Keep your defenses up: **update antivirus software**, **educate employees about phishing**, and **be cautious with email attachments** and links. Don't let VenomRAT check in to your systems—keep 'em locked tight! 🛡️🔒

ADVERSARIALLY weekly report

Abr 4 - 11, 2024

XG3 UNIT

Detections by Risk

Top 5 Weekly Rules Added/Updated by Adversary Rule Risk:

- Suspicious processes spawned from MS Office applications**(86)**
- Deletion of shadow copies **(72.5)**
- LoadLibrary called in CommandLinel **(71)**
- Adore rootkit execution **(64)**
- Protocol and external IP in CL -possible C2 contact **(63.5)**

🟥	90-100	*Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores*
🟧	70-90	*Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores*
🟨	50-70	*Rules with all or some of these features: Medium attack techniques, risky adversaries, trending (or not) Mitre TTPs, medium CVE scores*
🟢	0-50	*Rules with all or some of these features: Low attack techniques, not related to any adversaries, trending (or not) Mitre TTPs, low CVE scores*

Top MITRE Covered

- Command and Scripting Interpreter
- Application Layer Protocol
- Office Application Startup
- User Execution
- Inter-Process Communication

Adversary Trends

Actors	Set Tools	Vulnerabilities
APT31	UNAPIMON	GitHub / CVE-2024-24576
Storm-0558	Byakugan	Microsoft / CVE-2024-29988
Volt Typhoon	SEXi	Layerslider / CVE-2024-2879
APT29	Sing1	Microsoft / CVE-2024-26230
Storm-1567	AcidPour	Google / CVE-2024-29745

ADVERSARIALLY
weekly report
Abr 4 - 11, 2024

Ransomware

Total Victims = 110 (-4)

- Spain - **1** (-2)
- Latam - **3** (-2)

WorldWide - **106**

The king is...

Data of the week

Top Countries

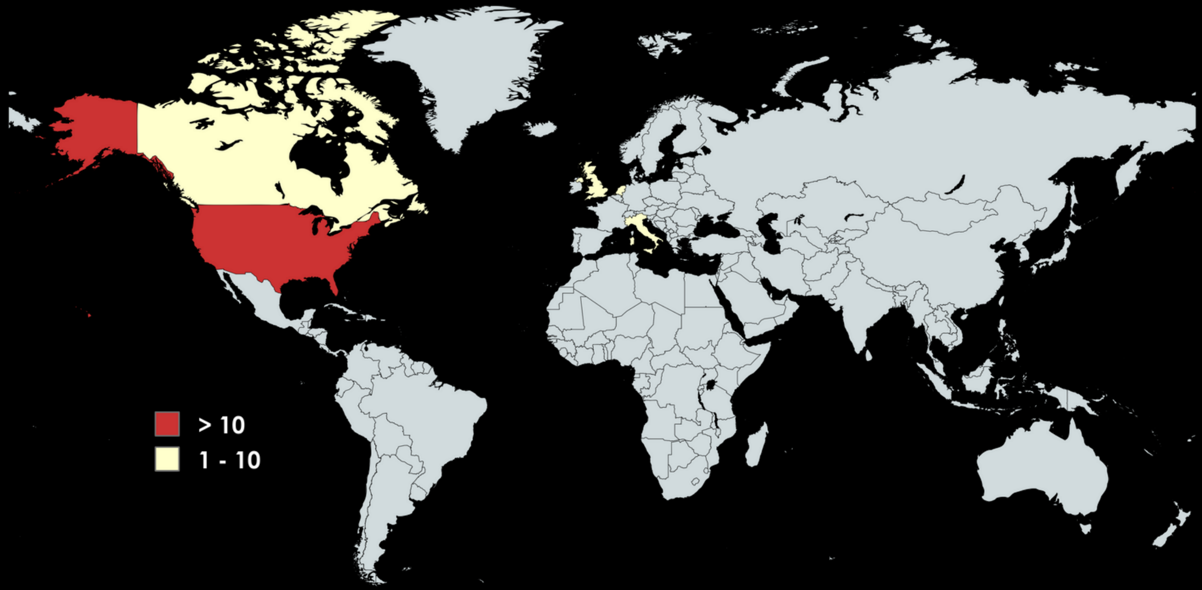
- USA - **56** (-3)
- ITA - **10** (+5)
- GBR - **8** (+4)
- CAN - **7** ☆
- NLD - **3** ☆

Top Sectors

- Manufacturing - **25** (+5)
- Healthcare - **15** (+4)
- Technology - **11** (-3)
- Finance - **9** (+1)
- CCnostruction - **8**

Top Groups

- Blacksuit - **17** (+4)
- Ransomhub - **15** (+4)
- Blackbasta - **11**
- Dragonforce - **10**
- Medusa - **8** (-2)



Victims

- **Ransom Victim:** Consilux | Group: Akira | Sector: Technology | Country: Brazil
- **Ransom Victim:** Agencia Host | Group: Ransomhub | Sector: TBD | Country: Brazil
- **Ransom Victim:** Agencia Host "agenciahost.com" | Group: Ransomhub | Sector: Services | Country: Brazil
- **Ransom Victim:** Mu*****.eu | Group: Cloak | Sector: TBD | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Abr 4 - 11, 2024

cipher

a Prosegur company

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.