WR X

Adversarially

Weekly Report

MAY./ 9-16

2024

XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY

weekly report

May 9 - 16, 2024

Adversary of the Week

Mediumblue Cosmos Taurus

Type: Individual

Countries: 🇧🇷

Maturity: 🟧🟧⬛

Sectors: Government, Administration

Activity: Cybercrime

TTPs: Indeterminated yet

UTA0178 aka. UNC5221

Type: APT

Countries: 🇺🇸 🇪🇺

Maturity: 🟧🟧⬛

Sectors: IT

Activity: Cibercrime

TTPs: Exploitation for Privilege Escalation

LockBit 3.0

Type: Group

Countries: 🌍

Maturity: 🟥🟥🟥

Sectors: **All**

Activity: RaaS

TTPs: **54**

ADVERSARIALLY
weekly report
May 9 - 16, 2024

XG3 UNIT

Global

- A **new ransom group** called "**Embargo**" has **claimed** responsibility for the **leak of 500GB of data from** Australia's largest non-bank lender, **Firstmac Limited**, on their TOR site.

- **Periwinkle Cosmos Taurus** X is selling on a well-known English forum information about **Europol**. The compromised information includes the **source code of FOUO**, classified information, PDFs, and other private documents.

- **Update: MITRE confirms** through an investigation that the IOCs found in the security **breach suffered last April** are directly **linked to the UTA0178 APT**, which is a China-linked APT group.

- The well-known English forum **BreachForum has been taken down** by the **FBI** and the Department of Justice. They currently control the Telegram channel, have **taken down the website** and are trying to extract information from the backend.

- According to their Telegram channel, **LockBit claims to have discovered** while attacking a company with the letters "HMW" that one of its employees was consuming child pornography material.

- **Papayaorange Cosmos Taurus** X is selling on Exploit and XSS forums **for $300k, the source code of the INC ransomware** for Windows and Linux/ESXi. The sale appears to be legitimate as the actor, according to their profile, is affiliated with RaaS. However, it's worth noting that the actor doesn't have much seniority or reputation on the forum.

- The **Phorpiex botnet has been used by LockBit** to send millions of phishing emails and **carry out a large-scale ransomware distribution campaign.** The emails contain an executable .ZIP file that implements the ransomware payload.

- **Urobilin Cosmos Taurus** X is offering a **Remote Code Execution (RCE) 0-Day exploit for Outlook** on various dark web forums. This exploit is targeted at x86/x64 versions of Microsoft Office 2016, 2019, LTSC 2021, and Microsoft 365 Apps for Enterprise, **priced at $1.8 million.** They **provide a Proof of Concept (PoC)** privately and a 100% success guarantee.

- Cybersecurity experts have discovered that **threat actors could abuse the digital rotating shutter of CMOS camera sensors in autonomous vehicles** from Tesla or Baidu Apollo. With this attack, they could **cause the cars to fail to correctly recognize traffic signals** such as a red traffic light, potentially leading to serious accidents.

Spain & Portugal

- **Rocketmetallic Cosmos Taurus X** has sold on a well-known English forum the database of **Complutense University of Madrid**, which contains personal private information of over 140k users and 16GB of data.

- **Update:** The **minor detained** for accessing the inbox of the Mossos d'Esquadra last March managed to **steal personal data from over 500 officers**, as well as **disseminate information about 60 of these** affected officers via Telegram.

- **Banco Santander** has confirmed that it has been the **victim of a cyberattack** where unauthorized access to its systems occurred. In the attack, **confidential and private information of Santander's clients in Chile, Spain, and Uruguay**, as well as all employees and some former employees of the group, **has been compromised.**

- **Cadmiumyellow Cosmos Taurus X** is selling on a well-known English-speaking forum, **access to the General Directorate of Traffic (DGT) and a database with over 34k lines of information** such as vehicle registration number, owner's name, ID number, and address.

LATAM

- A joint police operation has been carried out resulting in the **dismantling of one of Argentina's most significant cybercriminal gangs**, which had caused **scams worth $1.5M**. 64 raids have been conducted on residences, 20 arrests made in Argentina, and 9 international arrest warrants issued by INTERPOL.

- **Turquoisegreen Cosmos Taurus X** a member of the new group ZeroTolerance, is **selling** on Breach forum an **access shell to Telecom Argentina**, containing 121 GB of information.

- **Mediumblue Cosmos Taurus X** is selling personal **private information of 5 million Brazilian citizens** for $450 on a Breach forum.

- **Yellowgreen Cosmos Taurus X** is offering on Breach the **database** containing personal and private information of **over 800 patients** belonging to Sirex Medica, a healthcare technology company of Perú.

Vulnerabilities & Exploits

- Two critical vulnerabilities, identified as **CVE-2024-21793** and **CVE-2024-26026**, **affecting F5 Next Central Manager** have been discovered. These vulnerabilities would **allow** attackers to **gain total control** over vulnerable devices and **create hidden administrator accounts** for persistence on the system.

- **Update:** The vulnerabilities **CVE-2023-46805 and CVE-2024-21887** previously discovered in Ivanti Connect Secure devices **are being exploited to distribute the Mirai botnet**, highlighting the constant evolution of threat actors.

- The **zero-day vulnerability**, identified as **CVE-2024-4671**, **affecting Chrome** in the Visuals component of the browser, **which was actively being exploited, has been patched** with necessary updates by Google. The vulnerability allowed attackers to execute arbitrary code on compromised systems.

- A **new PoC** has been developed **for the** recently discovered vulnerability **CVE-2024-21111, affecting** versions prior to 7.0.16 of **Oracle VirtualBox**. This PoC demonstrates how local privilege escalation can be achieved through a symbolic link that triggers arbitrary file deletion and movement.

- **Microsoft has warned** about the existence of **multiple vulnerable Android applications on Google Play,** which accumulate more than 4 billion downloads. Among the **vulnerabilities found** in these applications are **authentication token theft and arbitrary code execution.** Currently, most of the relevant applications are said to have addressed these vulnerabilities.

- A series of **vulnerabilities affecting Cinterion cellular modems** have been discovered, which allow **remote code execution and unauthorized privilege escalation**. Among the most critical are those categorized as **CVE-2023-47610, CVE-2023-47611, and CVE-2023-47612**. Exploiting these security flaws could be **critical for** comprehensive communication networks and fundamental **IoT devices in industrial, healthcare, automotive, financial, and telecommunications** sectors.

ADVERSARIALLY weekly report

May 9 - 16, 2024

⚠️ Warning of the week

- Watch out for shady deals on the dark web, are **offering** an expensive **exploit for Outlook**! Keep your Office updated, and protect your inbox like it's Fort Knox. Keep those digital doors locked tight! 🔒🚪

- It appears that **Ivanti's Connect Secure** devices have been **attacked by Mirai's botnet.** Stay ahead of the curve: **update your devices**, use strong passwords and keep an eye out for suspicious activity! 🤖🔒

- Looks like cyber-crooks are trying to give **Tesla and Baidu Apollo** a green light to chaos! **Stay safe on the road: keep your autonomous vehicles updated,** and maybe **double-check** those **traffic lights**, just in case! 🚗🚦

- Uh-oh, **Banco Santander** got a visit from cyber-crooks! Keep your money safe: monitor your accounts, **change passwords regularly**, and **stay alert** for any suspicious activity. Don't let hackers mess with your financial! 💳♨️

- Don't let cyber-crooks manage your **F5 Next Central Manager! Patch those vulnerabilities pronto**—like giving your digital bouncer an upgrade. Keep control in your hands, not in the hands of sneaky hackers. Keep your system secure!🛡️

- **Chrome got a makeover!** Make sure your browser is as fresh as a new haircut—**update to patch CVE-2024-4671**. Stay secure and keep browsing safely! 🔒

- **Oracle VirtualBox** has been revamped, but not the way you want it! **Upgrade to version 7.0.16** before the cybercriminals start doing their evil deeds! 🛡️💻

- It seems that some **Android apps** were playing hide-and-seek with cybercriminals. Keep your apps up to date and stay alert for suspicious activity! 📱🔒

ADVERSARIALLY weekly report

May 9 - 16, 2024

XG3 UNIT

Detections by Risk

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

- Legitimate binary outside its usual path **(73.0)**
- Disabling event log service **(71.5)**
- Windows Internal Packet Capture via netsh **(71.5)**
- NSLOOKUP to external host in CL **(63.5)**
- Detection of rubeus by name or by kerberos attack argument in CL **(62.5)**

🟥	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

- Masquerading
- Service Stop
- Data from Local System
- Automated Collection
- Adversary-in-the-Middle

Adversary Trends

Actors	Set Tools	Vulnerabilities
Lazarus Group	ArcaneDoor	Google / CVE-2024-4947
Kimsuky	Brokewell	Microsoft / CVE-2024-30040
APT28	Mal.Metrica	Google / CVE-2024-4761
Sandworm	GooseEgg	Wordpress / CVE-2024-3750
Volt Typhon	Wpeeper	Cinterion / CVE-2023-47610

ADVERSARIALLY
weekly report
May 9 - 16, 2024

XG3 UNIT

Ransomware

Total Victims = 179 (-13)

- Spain - **10** (+7)
- Latam - **23** (+20)
- WorldWide - **146** (-40)

The king is...

Data of the week

Top Countries

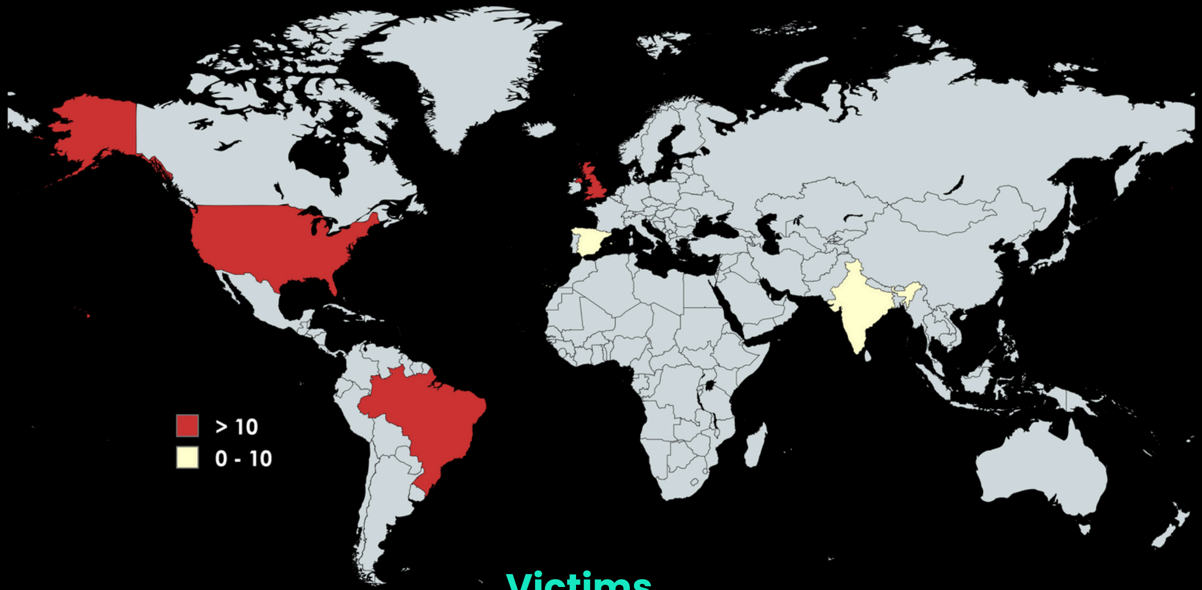
- USA - **61** (-34)
- GBR - **16** (+4)
- BRA - **13** ☆
- IND - **10** ☆
- ESP - **10** ☆

Top Sectors

- Manufacturing - **35** (+10)
- Healthcare - **16** (-1)
- Education - **13** ☆
- Technology - **12** (-27)
- Administration - **8** ☆

Top Groups

- Lockbit3 - **88** (+32)
- Incransom - **13**(+2)
- Arcusmedia - **8** ☆
- 8base - **8** ☆
- Ransomhub - **6**☆



Victims

- **Ransom Victim:** GOLD RH S.A.S | Group: arcusmedia | Sector: Human Resources | Country: Colombia
- **Ransom Victim:** Banco central argentina | Group: zerotolerance | Sector: Banking | Country: Argentina
- **Ransom Victim:** dagma.com.ar | Group: lockbit3 | Sector: TBD | Country: Argentina
- **Ransom Victim:** Cusat | Group: arcusmedia | Sector: Technology | Country: Argentina
- **Ransom Victim:** amsoft.cl | Group: lockbit3 | Sector: Technology | Country: Chile
- **Ransom Victim:** Grupo SASMET | Group: arcusmedia | Sector: TBD | Country: Brazil
- **Ransom Victim:** uniter.net | Group: lockbit3 | Sector: Manufacturing | Country: Spain
- **Ransom Victim:** cttxpress.com | Group: lockbit3 | Sector: Transportation | Country: Spain
- **Ransom Victim:** Fribin | Group: incransom | Sector: Manufacturing | Country: Spain

xMDR

ADVERSARIALLY

weekly report

May 9 - 16, 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.