WR X

Adversarially

Weekly Report

MAR./ 7-14

2024

XG3 UNIT

xMDR powered by Cipher

ADVERSARIALLY

weekly report

Mar 7 - 14, 2024

Adversary of the Week

Tomato Cosmos Taurus

Type: Individual

Countries: 🇪🇸 🇦🇷 🇧🇷

Maturity: 🟩⬛⬛

Sectors: Unknow

Activity: Cybercrime

TTPs: Sells unauthorised access

Magnet Goblin

Type: Group

Countries: 🇺🇸 🇪🇺

Maturity: 🟧🟧⬛

Sectors: Technology

Activity: Cybercrime

TTPs: Exploit Public-Facing Application

Play

Type: Group

Countries: 🇺🇸 🇪🇺

Maturity: 🟥🟥🟥

Sectors: Government, Finance, Media.

Activity: RaaS

TTPs: 36

Global

- **YX International,** a technology firm handling global SMS routing, **rectified a security lapse in an exposed database** that leaked one-time security codes for major platforms like Facebook, Google, and TikTok. The vulnerable database **contained sensitive data** and although the company addressed the issue, the duration of exposure remains undisclosed.

- The **Cybersecurity and Infrastructure Security Agency (CISA)** reported that **two critical systems**, linked to U.S. infrastructure, **were hacked through Ivanti product vulnerabilities**. CISA shut down the affected systems, emphasizing no operational impact while investigating potential data access or theft.

- A **Nerbian RAT campaign**, associated with the **Magnet Goblin group**, is using 1-day exploits against facing servers that have vulnerabilities they can exploit. Among them, a recent POC, **Ivanti Connect Secure VPN**, was published.

- On 10 March, **RansomedVC announces the closure of its operations** and publishes a last communiqué at the request of one of its programmers, offering code services. They attach several communication links via telegram. It is probably a side effect of the operation against Lockbit and ALPHV.

- Numerous **French official computer services** were the **victims of a cyber-attack** of "unprecedented intensity" claimed by a group calling itself **Anonymous Sudan**, supported by Russia and various Islamist groups. Among the targets were the ministries of culture, health, economy and ecological transition, as well as civil aviation. **Several of these ministries were either unusable** for much of the day or had many access problems.

- A new ransomware blog called **"Donex ransomware leakage"** has been identified. The group claims, in an identified ransom note, to both encrypt and steal data. Like other ransomware blogs, the blog is used to name victims and to share stolen data. **The blog lists five victims** that, according to the posted date on the blog, **were all claimed in February 2024**. Contact information is also provided on the blog, including an email and TOX ID.

Spain & Portugal

- **Tomato Cosmos Taurus** sells access to an unknown Spanish company with an annual revenue of more than 4 billion dollars, with VPN access pulse secure as a user, for 1000 dollars.

- According to national media, the **national actor Alcasec** plans to establish a new cybersecurity company named havenio.tech, focusing on the digital protection of assets.

- **Saffron Cosmos Taurus** offers on a well-known English forum, **2.8GB** of **confidential documents** and emails from the **Mossos D'Escuadra**, the Catalan police.

LATAM

- **Dark Storm Team** allegedly conducted DDoS attack on **Congonhas International Airport** over Brazil's support for Israel, according to their Telegram channel.

- Users in Brazil are the target of a **new banking Trojan** known as **CHAVECLOAK** that spreads via **phishing emails with PDF attachments.** The attack involves the PDF downloading a ZIP file and then **using DLL sideloading techniques** to execute the final malware.

- **Tomato Cosmos Taurus** sells access to an unknown Brazilian company with an annual revenue of more than $140 million, with FortiVPN access as a user for $600.

- **Sunflower Yellow Cosmos Taurus** sells access to an Ecuadorian corporation with a revenue of approximately 23 Billion dollars, with VPN access, in auction mode for a bid of 9000 dollars and a direct sale of 13000 dollars.

- **Lion Cosmos Taurus** sells access to an Argentinean company in the software development sector with an annual revenue of 6 million dollars, the access is RDP with local admin. It is sold in bidding format for 100$ and direct sale for 500$.

- **Hazelnut Cosmos Taurus** allegedly leaked the database of Mexican companies covering banks, financial institutions, leasing companies and SMEs. The compromised data includes contact information, lease details and asset information.

- **Darkorange Cosmos Taurus** offers on a well-known English forum a database with private information such as internal credentials, names or telephone numbers of the Government of Quintana Roo, Mexico.

- **Saffron Cosmos Taurus** offers in a well-known English forum a database with 2859 lines of private information of the National University of Cordoba, Argentina.

Vulnerabilities & Exploits

- Threat actors from the **BianLian ransomware** group have exploited vulnerabilities in JetBrains TeamCity for their campaigns, starting with a compromised TeamCity server to deploy a PowerShell version of their Go backdoor. The attack exploited **CVE-2024-27198 or CVE-2023-42793** for entry, followed by user creation and command execution for further access. The exact vulnerability used is unknown. BianLian installs custom backdoors and remote desktop tools in each attack. Recently, they used an obfuscated PowerShell backdoor ('web.ps1') to establish additional network communications, allowing arbitrary command execution on affected hosts.

- Experts revealed technical information and a **proof-of-concept exploit for CVE-2024-1403** in Progress Software's OpenEdge Authentication Gateway and AdminServer. This authentication bypass flaw impacts OpenEdge versions up to 11.7.18, 12.2.13, and 12.8.0, occurring when configured with an OS local authentication provider in an OpenEdge Domain. Exploitation could grant unauthorized access during login attempts.

- A new vunerability, **CVE-2024-21762, in Fortinet FortiOS**, affecting **roughly 150,000 devices**. Fortinet had warned of active exploitation of this **remote code execution issue** in February, caused by an out-of-bounds write vulnerability exploitable via crafted HTTP requests. Fortinet advises turning off SSL VPN to mitigate the risk. However, Shadowserver Foundation found around 150,000 devices still at risk, mainly in the United States, India, and Brazil, despite the flaw being listed in Fortinet's Known Exploited Vulnerabilities catalog.

⚠️ Warning of the week

- **Ransomware bad guys, the BianLian gang, are crashing TeamCity servers!** They're sneaking in through holes (CVE-2024-27198 or CVE-2023-42793) and deploying backdoors like bouncers at a shady nightclub. Patch your TeamCity server faster than you can say "cybersecurity" and be super careful about those suspicious emails.

- **Yikes! Progress Software's OpenEdge is wide open!** Security researchers spilled the beans on a flaw (CVE-2024-1403) in Progress Software's OpenEdge that lets anyone waltz right in. Update to the latest version (11.7.19, 12.2.14 or 12.8.1) quicker than a hacker on a sugar rush!

- **Attention Fortinet fans! Don't let hackers turn your firewall into a pincushion!** A nasty bug (CVE-2024-21762) is lurking in Fortinet FortiOS, and hackers are exploiting it like crazy. Fortinet says turning off SSL VPN helps, but there are still 150,000 devices at risk! Update your software ASAP and don't be a statistic.

- **Brazilian users, beware of CHAVECLOAK trying to steal your hard-earned Reais! If you're reading this from Brazil, watch out!** A new banking Trojan called CHAVECLOAK is hiding in PDF attachments sent through phishing emails. This malware is like a sneaky samba dancer, trying to steal your banking info. Don't click on suspicious links and be super careful about those PDFs!

- **Remember that Ivanti vulnerability we mentioned a few weeks ago? Turns out Nerbian RAT is throwing a cyber-party on it! Patch your Ivanti software ASAP!** We warned you about this vulnerability (linked to U.S. infrastructure hacks!), and now malicious actors are exploiting it with Nerbian RAT malware. Don't be a party guest – update your software and stay secure!

- **French computer systems got hacked in a big way!** While the details are fuzzy, this is a good reminder to tighten up your cybersecurity. Update your software, be cautious about emails, and don't click on anything suspicious. Remember, prevention is the best medicine (or baguette) against cyberattacks!

ADVERSARIALLY
weekly report
Mar 7 - 14, 2024

XG3 UNIT

Detections by Risk

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

- Detected write operation to /etc/passwd **(69)**
- Download detected using different Powershell methods **(68.5)**
- Windows Internal Packet Capture via netsh **(66.5)**
- Connections to remote LDAP servers **(66.5)**
- Detection of WIDETONE malware parameters 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

- OS Credential Dumping
- Exploitation for Privilege Escalation
- Exploitation for Credential Access
- Command and Scripting Interpreter
- Data from Local System

Adversary Trends

Actors

UNC2452
APT29
Storm-1567
APT28
Lazarus Group

Set Tools

VCURMS
CHAVECLOAK
ToddlerShark
GTPDOOR
WogRAT

Vulnerabilities

Microsoft / CVE-2024-21334
Fortinet / CVE-2023-48788
Apache / CVE-2024-27894
Apache / CVE-2024-27135
Kubernetes / CVE-2024-28175

ADVERSARIALLY weekly report

Mar 7 - 14, 2024

XG3 UNIT

Ransomware

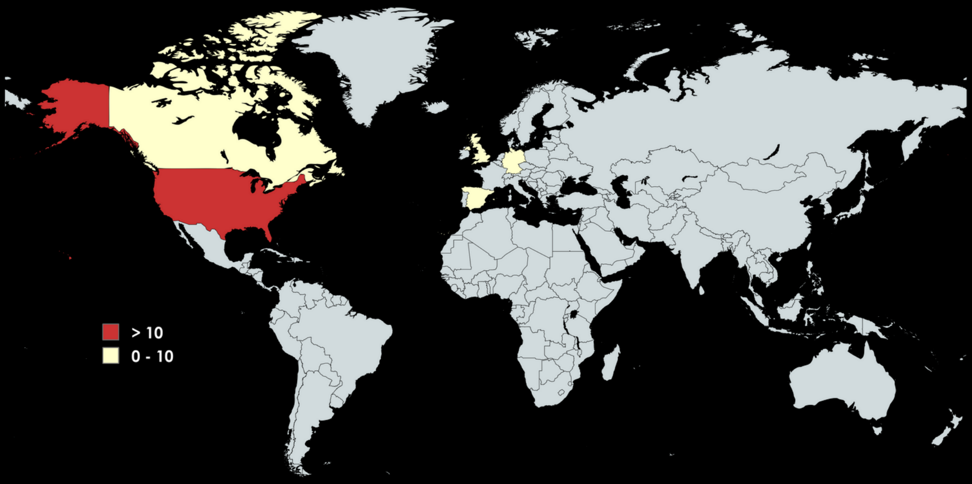
Total Victims = 100 (-15)

- Spain - **2**
- Latam - **3** (+2)
- WorldWide - **95** (-17)

The king is...

Data of the week

Top Countries	Top Sectors	Top Groups
USA - **41** (-10)	Services - **26** (-3)	Play - **19** (+1)
GBR - **7** ☆	Industrial - **12** (+8)	Blackbasta - **11** ☆
DEU - **5**	Other - **10** ☆	Ransomhub - **11** ☆
CAN - **4** (-1)	Health - **10** (+4)	Medusa - **8**
ESP - **2** ☆	Financial- **6** ☆	Lockbit - **8** (-9)



Victims

- **Ransom Victim:** Reny Picot | Group: Cactus | Sector: Retail | Country: Spain
- **Ransom victim:** Fincas Revuelta | Group: Everest | Sector: Real Estate | Country: Spain
- **Ransom victim:** Derrama Magisterial | Group: LockBit | Sector: Services | Country: Peru
- **Ransom victim:** SP Mundi | Group: RansomHub | Sector: Finance | Country: Brazil
- **Ransom victim:** TeleCentro | Group: Akira | Sector: Telecoms | Country: Argentina

xMDR

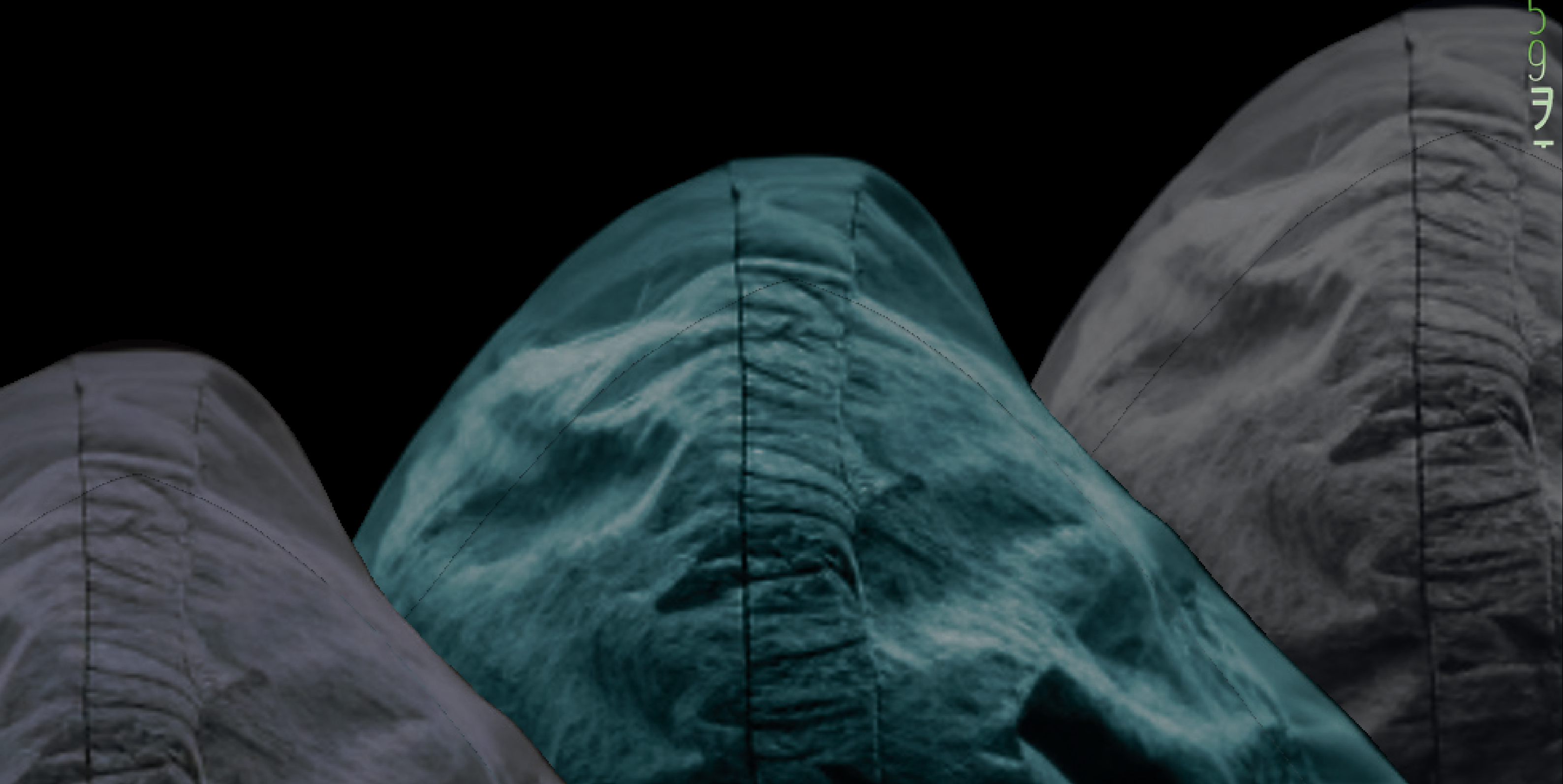
ADVERSARIALLY

weekly report

Mar 7 - 14, 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.