WR X

Adversarially

Weekly Report

APR / 25 - MAY / 9

2024

XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

Adversary of the Week

Lime Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Education

Activity: Cybercrime

TTPs: Indeterminated yet

Coral Blue Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Government, Telecoms

Activity: Cibercrime

TTPs: Exploit Public-Facing Application

LockBit 3.0

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 54

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

Global

- A **new ransomware collaboration program** has been published on the well-known RAMP forum. They offer to work together **using the Psoglav Ransomware**, a new ransomware with features such as self-deletion or the lack of need to connect to the internet to process files.

- The multinational automobile company **Volkswagen** has been the **victim of a cyberattack** by an undisclosed group affiliated with the Chinese government, which is said to have **stolen over 19,000 files** containing critical information about electric vehicle technologies and production strategies.

- **Okta** has issued a **warning about the increasing number of credential stuffing attacks** against its identity and access management solutions, attempting to access users' accounts.

- Dropbox, Inc., specifically its **DropboxSign environment**, has been the victim of a cyberattack. In it, **threat actors accessed user information** such as email addresses or names. Additionally, the threats actors gained access to information **such as hashed passwords or authentication data**, such as API keys, OAuth tokens from a subset of users. The company states that they have **no evidence that the actors accessed the content of the accounts or payment information.**

- A few days ago, the NCA revealed the **identity of the user @Lockbitsupp**, through the theft of one of his mirrors that simulates his .onion site, publishing several posts, including one that points out the identity of one of the biggest figures in cybercrime: **Dmitry Khoroshev**.

- **Periwinkle Cosmos Taurus** offers on a well-known English dark web forum the **HSBC & Barclays database with over 512 lines of private information**, as well as documents, source code, SQL files, and JSON.

- **Skyblue Cosmos Taurus** is offering **unauthorized access to a VPN** of a major Japanese automotive corporation with earnings of $15B. The sale is conducted in an auction format and starts at $40k.

- The **UK Armed Forces payment system** has experienced a security incident in which personal **information such as names or banking details** of active-duty, reserve, or retired agents **has been leaked**. The attack has not affected April payrolls or pensions.

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

Spain & Portugal

- **Lime Cosmos Taurus** is offering on a well-known English forum the **database of a Spanish driving school company**, which allegedly contains over 200k rows of private customer data.

- **Fuchsia Cosmos Taurus** is offering on a Russian-speaking forum **unauthorized RDP access to a Spanish company** with an annual revenue of over €6 million. The company holds private information such as banking or personal data of between 1 and 5 million users (individuals, municipalities, private companies...).

- The **Spanish newspaper "El Confidencial"** has been the **victim of a cyberattack using SQL injection and XSS** techniques to attempt to access the newspaper's content management system and try to modify its front page.

- The **Spanish multinational Ayesa** has fallen victim to the **BlackBasta ransomware**. This company provides technological services to businesses and public administrations in 23 countries. Initially, the company stated that it had not suffered any impact, but recently, the BlackBasta ransomware group **has shared a 4.5TB data leak on their TOR site**. This leak includes confidential information from the company, as well as private information of clients and employees.

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

LATAM

- **Turquoisegreen Cosmos Taurus** is offering on a well-known English forum a database from the Central Bank of Argentina that allegedly contains private information of clients such as full names or ID numbers. They are willing to negotiate the price, and payment would be made through BTC or XMR.

- **Coral Blue Cosmos Taurus** is offering on a well-known English forum a 2TB database from the Secretariat of Public Education of Mexico that allegedly contains private information such as financial information, emails, or source codes.

- An unknown **bucket hosted** on Google has **exposed 8000 private official documents**, including Chile's Digital Vaccination Pass.

- **Maroon Red Cosmos Taurus** is selling access to the administration panel that manages the internet access points of all air terminals in Mexico on a well-known English forum. The company responsible for this is SolarWinds.

- **Crimson Rigel Taurus** offers over 4k documents with private information of clients from the Colombian insurance company 'Sura' in an English forum.

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

Vulnerabilities & Exploits

- Two vulnerabilities have been discovered **affecting Linksys E5600 routers** running firmware version 1.1.0.26. The vulnerabilities, cataloged as **CVE-2024-33788 and CVE-2024-33789**, allow attackers to **execute arbitrary commands** on the routers and inject malicious code due to insufficient input validation mechanisms within the firmware.

- A vulnerability rated 9.9 has been discovered, cataloged as **CVE-2024-29212**. It is a vulnerability that **allows attackers to execute remote code on the Service Provider Console (VSPC)**. The flaw is due to an insecure deserialization method used during communications between the management agent and its components.

- A high-severity vulnerability **CVE-2024-26585** has been discovered affecting **Linux kernels.** Attackers can exploit this to achieve privilege escalation on Container-Optimized OS and Ubuntu nodes.

- The **TOTOLINK EX1800T wireless** extender contains a vulnerability in the apcliEncrypType parameter, categorized as **CVE-2024-34257**, which allows **unauthorized arbitrary command execution**, enabling attackers to obtain administrator privileges on the device.

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

⚠️ Warning of the week

- Yikes! Don't let **BlackBasta's ransomware** ruin your day! Beef up your cybersecurity: **back up your data regularly, update your systems** and security software, and train employees to recognize phishing attempts. Stay vigilant and keep your sensitive info locked down tight! 📝🔒

- Watch out for sneaky hackers trying to **stuff credentials into your Okta account!** Beef up security: enable multi-factor authentication, use strong and unique passwords, and monitor for suspicious login attempts.🛡️🔒

- Time to beef up your **Linksys E5600 router's security! Update to the latest firmware version** pronto to patch those vulnerabilities. Also, change default passwords, disable remote management, and keep an eye out for any suspicious activity on your network. Stay safe and keep your router locked down!" 🛡️

- Lock down your **Service Provider Console pronto! Update to patch CVE-2024-29212**. Also, limit access to the console, **monitor for any unusual activity**, and educate your team about the risks of insecure deserialization. Don't let cyber-crooks sneak in through the back door! 🚪🔒

- Secure your **Linux kernels to prevent privilege escalation!** Patch immediately to fix CVE-2024-26585. Also, regularly **update your system**, monitor for suspicious activity, and **limit user privileges.** Don't let attackers gain a foothold!

- Watch out for **sneaky Wi-Fi extenders like TOTOLINK EX1800T**—they're not just boosting your signal, they're boosting cyber-crooks too! **Update your device ASAP**. Stay safe, and keep your Wi-Fi password stronger than your morning coffee!☕🔒

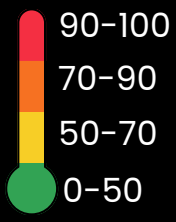
ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

Detections by Risk

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

- Network Communication With Crypto Mining Pool **(46.5)**
- CVE-2023-23397 Exploitation Attempt **(42.5)**
- Linux Crypto Mining Pool Connections **(41.5)**
- Suspicious Eventlog Clear or Configuration Change **(41.5)**
- Windows Defender Threat Detection Disabled - Service **(41.5)**



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

- User Execution
- Resource Hijacking
- Impair Defenses
- Remote Services
- Indicator Removal

Adversary Trends

Actors

APT28
Sandworm
Lazarus Group
Kimsuky
APT-31

Set Tools

ArcaneDoor
Brokewell
Mal.Metrica
Wpeeper
BirdyClient

Vulnerabilities

Totolink / CVE-2024-34257
Php / CVE-2024-31961
Apple / CVE-2024-27793
Veeam / CVE-2024-29212
Linux / CVE-2024-3661

ADVERSARIALLY
weekly report
Apr 25 - May 9, 2024

XG3 UNIT

Ransomware

Total Victims = 192 (-241)

- Spain - **3** (+1)
- Latam - **3** (-1)
- WorldWide - **186** (-241)

The king is...

Data of the week

Top Countries

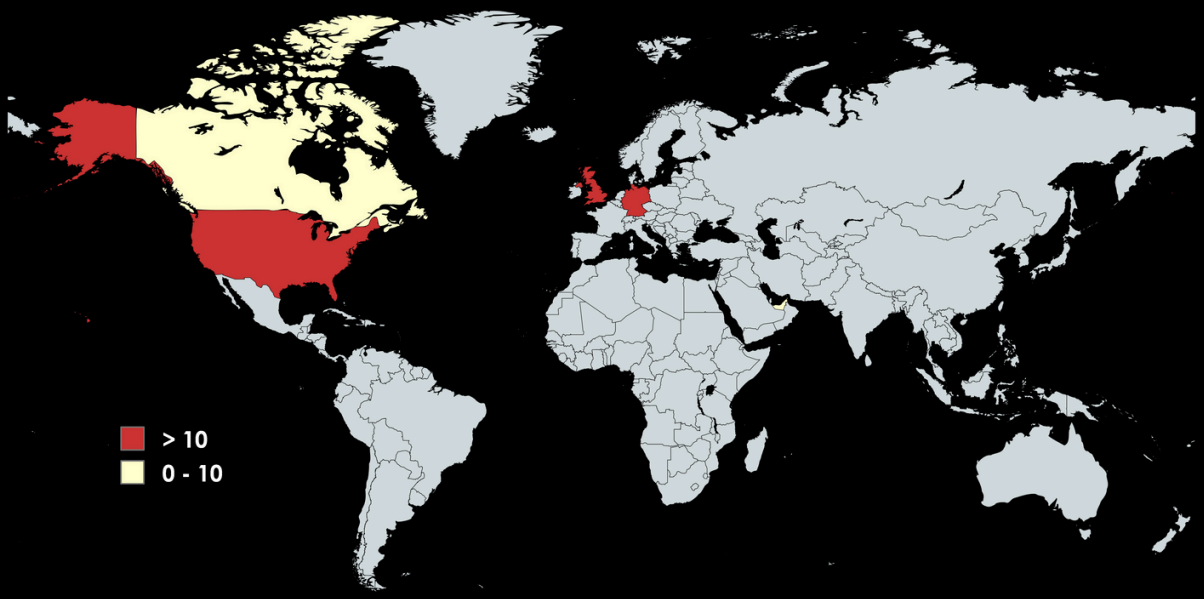
- USA - **95** (+49)
- DEU - **14** (+7)
- GBR - **12**
- CAN - **8** (-2)
- ARE - **7**

Top Sectors

- Technology - **39** (-13)
- Manufacturing - **25** (-24)
- Healthcare - **17** (-31)
- Services - **11**
- Construction - **11**

Top Groups

- Lockbit3 - **56 (+44)**
- Medusa - **12**
- Underground - **12**
- Incransom - **11**
- Play - **11**



Victims

- **Ransom Victim:** Lopez Hnos | Group: rhysida | Sector: Manufacturing | Country: Argentina
- **Ransom Victim:** aletech.com.br | Group: darkvault | Sector: Education | Country: Brazil
- **Ransom Victim:** cli*********.com | Group: cloak | Sector: Technology | Country: Colombia
- **Ransom Victim:** acsistemas.com | Group: lockbit3 | Sector: Technology | Country: Spain
- **Ransom Victim:** ayesa.com | Group: blackbasta | Sector: Engineering | Country: Spain
- **Ransom Victim:** awwg.com | Group: underground | Sector: TBD | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Apr 25 - May 9, 2024

cipher

a Prosegur company