WR X

Adversarially

Weekly Report

AUG 29–SEP 5

2024

XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 2024

XG3 UNIT

Adversary of the Week

Mint Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Social Media

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Darkolivegreen Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Salud, Legal

Activity: Cybercrime

TTPs: Exploit Public-Fancing Application

Ransomhub

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 35

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 2024

XG3 UNIT

Global

- **Mint Cosmos Taurus** sells on BreachForum 390.4 million leaked records from Russia's largest social networking and media service, VKontakte. The database reportedly contained personal information of users, including ID number, first name, surname, gender, profile picture, country and city.

- A **new ransomware** called **Cicada3301** has been detected, **targeting Windows and Linux/ESXi hosts** with sophisticated encryption techniques. This ransomware attack starts with the use of legitimate, stolen or brute-force login credentials to **gain access through ScreenConnect.**

- A **malware campaign** has been detected that is **spoofing Palo Alto Networks' GlobalProtect VPN software** to **distribute** a variant of the **WikiLoader** via a search engine optimisation (SEO) campaign. The actors often use SEO poisoning as an initial access vector to trick people into visiting a page that spoofs the legitimate search result to deliver malware instead of the targeted product.

- A hacktivist group known as **Head Mare** has been linked to cyber attacks that exclusively **target organizations** located in **Russia** and **Belarus**. The attackers **took advantage** of the relatively recent **CVE-2023-38831** vulnerability in **WinRAR**, which allows the attacker to **execute arbitrary code** on the system via a specially prepared archive. This approach allows the group to deliver and disguise the malicious payload more effectively.

- A **campaign** has been identified **on GitHub** where **replies to comments** on projects are being used to **distribute the Lumma Stealer** malware. The attackers are **masquerading as people** offering bug fixes, but are actually **spreading malware** designed to steal information.

- **Transport for London (TFL)**, has been the **victim of a cyber attack**, although there is no evidence that customer data has been compromised and there has been no impact on TFL services. The attack appears to have mainly **affected** the transport **provider's backroom systems** at its headquarters, and citizens have been asked to telework to prevent transport from being brought to a standstill and sensitive customer data being stolen by the attackers.

- A new **malware campaign** has been discovered and is **spreading a backdoor** called **Voldemort** to organisations in the **insurance, aerospace, transportation and education** sectors, masquerading as tax agencies in the US, Europe and Asia.

- The **FBI** has warned in a statement that **North Korea** is conducting **advanced social engineering campaigns against** employees in the **DeFi** and **cryptocurrency sectors** to deploy malware and steal digital assets. North Korean threat actors pose as recruiters or known contacts to gain the trust of victims.

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 2024

XG3 UNIT

Spain & Latam

- **The Lynx group** claims to have **hacked IDOM**, a Spanish multinational company providing professional **consulting, engineering and architectural** services. Client contracts, postal correspondence, employees' personal data and financial documents were leaked.

- The Spanish threat actor known as **Farlopa** has made a statement on his blog DEFSEC in which he **announced his retirement** due to personal reasons. He also warns of the **ceasing of DEFSEC** as a group and warns that no further communication should be taken into further consideration.

- The **MeowLeaks** group sells a database linked to Instituto Cardiovascular del Cesar, S.A., based in Valledupar, Colombia. It is a highly complex cardiovascular medical centre. The database contains information on identity cards, driving licences, medical records and confidential information.

- **Darkolivegreen Cosmos Taurus** sells on BreachForum a compilation of the iSaludCollege server, which contains multiple databases and back-up files with alumni information.

- **Darkolivegreen Cosmos Taurus** sells on BreachForum the Ecofield Legal database which contains personal information of users and customers such as names, usernames, e-mail addresses, passwords, etc.

- **Anonymous** has once again accessed **Aviación Militar Bolivariana**, exposing names, surnames, IDs, user IDs, confidential information and bank accounts of **Venezuelan military personnel.**

- Cybersecurity researchers have detected the **sale of sophisticated phishing kits targeting** various **banks in Mexico** by **Blackdatabase**. The kits feature a reverse proxy tool designed to steal banking credentials and bypass two-factor authentication (2FA) systems.

- Mobile device **users in Brazil** are the target of a **new malware campaign** that distributes a **new android banking trojan** called **Rocinante**. This malware is capable of performing **keylogging** using the Accessibility Service, as well as **stealing** victims' personally identifiable **information** using **phishing screens** posing as different banks.

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 2024

XG3 UNIT

Vulnerabilities & Exploits

- Microsoft's threat intelligence team claims that the **Citrine Sleet aka Hidden Cobra** group **linked** to the **North Korean government** was discovered using **zero-day exploits** against a type confusion flaw in the JavaScript engine and WebAssembly Chromium V8. The vulnerability is identified as **CVE-2024-7971**. It primarily **targeted financial institutions** and organisations and **individuals handling cryptocurrencies.**

- A new vulnerability has been detected as **CVE-2024-43044** and is an **arbitrary file read vulnerability**, which allows an agent to read Jenkins driver files. Additionally a **proof-of-concept (PoC) has been found** where this vulnerability is **successfully exploited.**

- Security researcher **Sergey Kornienko** shared a **proof-of-concept (PoC)** exploit that demonstrates how an attacker could **exploit** vulnerability **CVE-2024-38106** to escalate privileges. The **zero-day vulnerability** was actively **exploited** by a North Korean threat actor known as **Citrine Sleet aka Hidden Cobra**. The group used the vulnerability as part of a sophisticated exploit chain that began with directing targets to a malicious domain controlled by the attackers.

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 2024

XG3 UNIT

⚠ Warning of the week

- **Hidden Cobra** is at it again, targeting financial institutions with a zero-day flaw in Chromium V8's JavaScript engine **(CVE-2024-7971.)**. Keep your browsers updated and your assets secure—no one wants to end up funding a covert operation with their cryptocurrency!

- **Jenkins** has sprung a leak, letting attackers read sensitive driver files with **CVE-2024-43044.** Patch promptly before hackers take your Jenkins for a joyride through your critical files—no one likes an uninvited backseat driver in their systems.

- **Hidden Cobra** is using a **CVE-2024-38106 zero-day exploit** to elevate their privileges, and they've even got a malicious domain ready to reel you in. Steer clear of suspicious links, update your systems, and keep your privileges where they belong—safe from North Korean hackers!

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 2024

XG3 UNIT

Ransomware

Total Victims = 132 (+18)

- Spain - 1 (-1)
- Latam - 4 (+1)
- WorldWide - 137 (+10)

The king is...

Data of the week

Top Countries

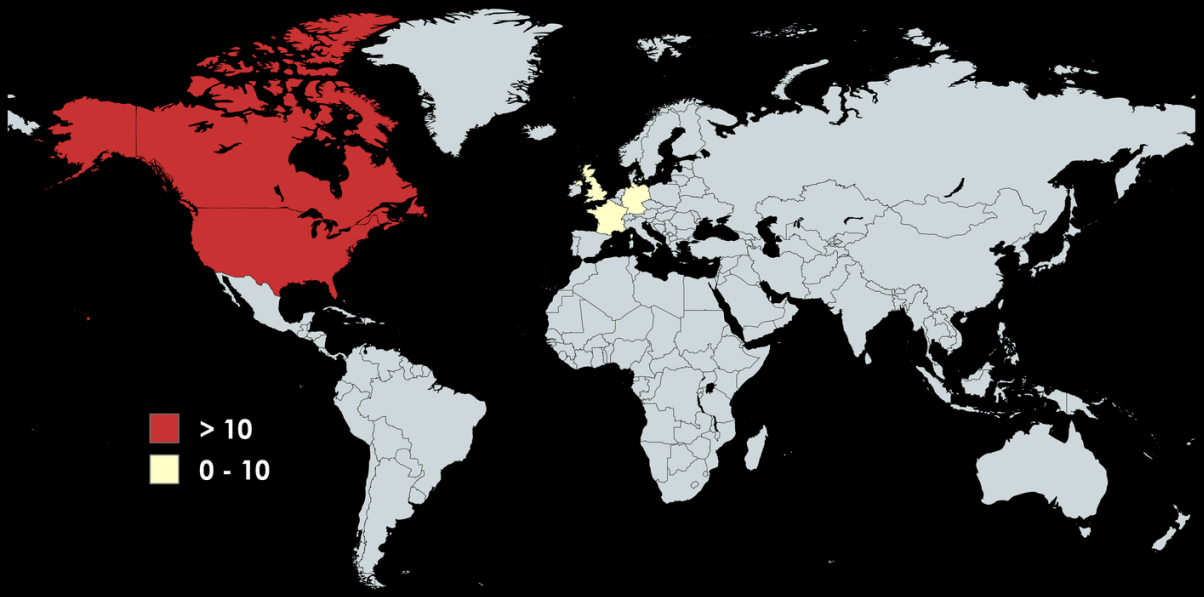
- USA - 54 (+11)
- CAN - 13 (+7)
- GBR - 6 (-4)
- FRA - 4 ☆
- DEU - 3 ☆

Top Sectors

- Manufacturing - 30 (+13)
- Construction - 11 (+4)
- Technology - 11 (-5)
- Engineering - 10 ☆
- Finance - 10 (-4)

Top Groups

- Ransomhub - 32 (+20)
- Lockbit3 - 15 ☆
- Cactus - 13 ☆
- Play - 11 (+3)
- Blacksuit - 10 ☆



Victims

- **Ransom Victim:** Instituto Cardiovascular del Cesar | Group: meow | Sector: Healthcare | Country: Colombia
- **Ransom Victim:** LFE Wines | Group: ransomhub | Sector: Agriculture | Country: Chile
- **Ransom Victim:** Grupo Modesto Cerqueira | Group: meow | Sector: TBD | Country: Brazil
- **Ransom Victim:** Alconca | Group: lockbit3 | Sector: Agriculture | Country: Venezuela
- **Ransom Victim:** Idom | Group: lynx | Sector: Engineering | Country: Spain

ADVERSARIALLY
weekly report
Aug 29 - Sep 5, 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 80

Top Most Relevant

- Financial Theft
- Ingress Tool Transfer
- Exploitation for Client Execution

Threat Actors 9

Top Most Relevant

- Slategray Cosmos Taurus
- RipperSec
- CGPLLNET

xMDR

ADVERSARIALLY

weekly report

Aug 29 - Sep 5, 2024

xMDR
powered by Cipher