ADVERSARIALLY

weekly report

Jan 25 - Feb 1, 2024

by

XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

Adversary of the Week

Honey Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Hotel & Logistic

Activity: Cybercrime

TTPs: Leak of confidential information

Akira

Type: Group

Countries:

Maturity:

Sectors: Education, Finance, Health

Activity: Ransomware

TTPs: 11

Mustang Panda

Type: APT

Countries:

Maturity:

Sectors: Education, Telecoms. Goverment

Activity: Information theft and espionage

TTPs: 28

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

Global

- **AI could lead to an increase in the ransomware** threat in the next 2 years. It has recently been noted that several groups are already developing generative criminal intelligence (**GenIA**) and offering it **as a service.** This also allows less experienced threat actors to start carrying out cyberattacks.

- **Schneider Electric has fallen victim to the Cactus ransomware** group. It is said to have stolen terabytes of **private information** such as customers' energy usage data. In addition, the gang is extorting the victim to publish the information if they do not pay the ransom demanded.

- **Threat actors** are once again **using** the legitimate **TeamViewer** tool **to carry out ransomware attacks**. According to the company, they are making use of previously leaked user credentials to access remote desktops of potential victims and download and deploy malicious files.

- According to various investigations, the Chinese-linked **Mustang Panda** actor group has reportedly **attacked Myanmar's Ministry of Defence and Foreign Affairs** as part of a **campaign to implement backdoors and RATs.** The attack exploits malicious DLL payloads in order to establish persistence and contact with a C2.

- The actor **APT29 aka Midnigth Blizzard is** allegedly **behind** the two **attacks reported by Microsoft and Hewlett Packard Enterprise (HPE)** last month. Both claim that they could be attacks that began months earlier and for a similar reason, to obtain private information and espionage on companies.

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

Spain & Portugal

- The **Concello de Teo** in A Coruña has suffered a **ransomware attack** in which all civil servants' devices have been affected, paralysing administrative activity. The unknown threat actors would have **requested a ransom** but **without** indicating **the amount** and where it would have to be paid, according to the Guardia Civil.

- In connection with the incident suffered by the Orange company, **cybersecurity researchers** have discovered more than **1572 compromised clients of RIPE**, the Asia-Pacific Network Information Center (APNIC), the African Network Information Center (AFRINIC) and the Latin American and Caribbean Network Information Center (LACNIC). The company **has also been affected by malware** activities involving known password stealers such as **Redline, Vidar, Lumma, Azorult and Taurus.**

- The **National Cybersecurity Institute (INCIBE)** has detected a **phishing campaign** targeting the Spanish population by **impersonating the Spanish Tax Agency** in order to steal victims' access credentials.

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

LATAM

- Five **developers of the Grandoreiro** malware **have been arrested** and 13 search and seizure actions have been carried out. The operation has been carried out by the Federal Police of Brazil together with Interpol, the Spanish National Police, ESET and CaixaBank.

- A **phishing campaign** is being carried out via corporate e-mails against **59 government domains in Brazil.** The threat actor or group behind this incident is currently unknown.

- A **new Android banking Trojan** dubbed as **PixPirate** has been discovered **targeting LATAM especially against Brazil.** Its main function is to impersonate applications known to users and thus **steal** sensitive information such as **valid banking credentials.**

- Actor **Tomato Cosmos Taurus** sells VPN access on a private Russian forum to an Argentinean company with a revenue of 11 million belonging to an undisclosed sector. The access is for sale for $500.

- Actor **Honey Cosmos Taurus** sells WebShell access to a private Russian forum to a Brazilian company with a revenue of $160 million in the logistics sector. The access is for sale for 800$.

- Actor **Honey Cosmos Taurus** sells access via WebShell on a private Russian forum to a Brazilian company with a revenue of 11 million dollars belonging to the hotel sector. The access is for sale for 500$.

- Actor **Saffron Cosmos Taurus** sells 31k My Argentina credentials on a popular dark web forum, gaining access to private information such as driver's licences and other state-issued documents.

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

Vulnerabilities & Exploits

- Unprivileged attackers can **get root access** on multiple major Linux distributions in default configurations by exploiting a newly disclosed local privilege escalation (LPE) vulnerability in the GNU C Library (glibc), know as **CVE-2023-6246.**

- A vulnerability with identifier **CVE-2024-23897** was detected, which involves the possibility of **arbitrary file reading** through the built-in command line interface (CLI). This vulnerability could be used by actors to **read binary files containing** sensitive information such as **passwords**.

- The **critical vulnerability** with identifier **CVE-2024-20253** affecting Cisco would allow threat actors to access and control unified communications systems. The vulnerability involves erroneous processing of user-supplied data, which could be used by the attacker to send specific messages to listening ports of vulnerable devices.

- **GitLab** has released **fixes to patch** a critical vulnerability in its Community Edition (CE) and Enterprise Edition (EE) **that could be exploited to write arbitrary files while creating a workspace**. It has been registered as **CVE-2024-0402** and has a CVSS score of 9.9 out of a maximum of 10.

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

Detections by Risk

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

- LoadLibrary called in CommandLine **(68.5)**
- Potential PuppetLoader command line execution **(68.5)**
- Windows Internal Packet Capture via netsh **(66.5)**
- .CHM execution - possible phishing from decoy file **(65.5)**
- Protocol and external IP in CL -possible C2 contact **(63.5)**

Top MITRE Covered

- Command and Scripting Interpreter
- Shared Modules
- Execution GuardrailsOS
- Native API
- Data from Local System

Adversary Trends

Actors

APT29
UNC2452
Volt Typhoon
Lazarus Group
UTA0178

Set Tools

Kasseika
NSPX30
SPICA
MediaPI
Phermedrone Stealer

Vulnerabilities

Docker / CVE-2024-21626
Linux / CVE-2023-6246
Gnu / CVE-2023-6246
Xen / CVE-2023-46839
Jenkins / CVE-2024-23897

ADVERSARIALLY
weekly report
Jan 25 - Feb 1, 2024

XG3 UNIT

Ransomware

Total Victims = 77 (-20)

- Spain - **2**
- Latam - **3** (-1)
  WorldWide - **75** (-16)

The king is...

Data of the week

Top Countries

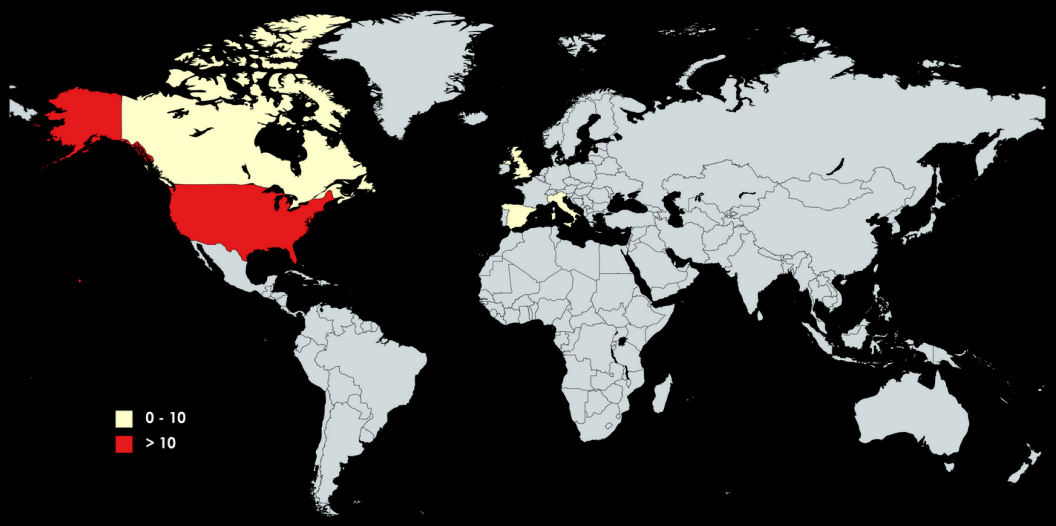
- USA - **40** (-2)
- GBR - **6** (+1)
- CAN - **4**
- ITL - **3** ☆
- SPA - **2**

Top Sectors

- Industrial - **10** (-13)
- Services - **9** (-13)
- IT - **7** ☆
- Financial - **6** ☆
- Healthcare - **6** ☆

Top Groups

- Akira - **9** (+3)
- 8Base - **9**
- Lockbit - **8** (-22)
- Mydata- **7** ☆
- BianLian - **6** ☆



Victims

- **Ransom victim:** Abecom | Group: Knight | Sector: Industrial | Country: Brazil
- **Ransom victim:** Brazilian Business Park (BBP) | Group: Akira | Sector: Services | Country: Brazil
- **Ransom victim:** mrm.com.mx | Group: Lockbit 3.0 | Sector: Services | Country: Mexico
- **Ransom victim:** Ausa | Group: Trigona | Sector: Industrial | Country: Spain
- **Ransom victim:** Concello de Teo | Group: Unknown | Sector: Goverment | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Jan25 - Feb1, 2024

cipher

a Prosegur company