ADVERSARIALLY

weekly report

Jan 04-11, 2024

by

XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Jan 04-11, 2024

XG3 UNIT

Adversary of the Week

Tinsel Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Telecom

Activity: Cybercrime

TTPs: Valid Accounts

UAC-0050

Type: Group

Countries:

Maturity:

Sectors: All

Activity: Espionage

TTPs: Leak of confidential information

Hunters International

Type: Group

Countries:

Maturity:

Sectors: **All**

Activity: Ransomware

TTPs: Exfiltration & Impact

ADVERSARIALLY
weekly report
Jan 04-11, 2024

XG3 UNIT

Global

- **Carrefour's finance** company suffers a cyber-attack that steals information and ID cards of its customers, among other data.

- The threat actor known as **UAC-0050** is leveraging phishing attacks to distribute **Remcos RAT** using new strategies to evade detection from security software.

- A new variant of remote access trojan called **Bandook** has been observed being propagated via phishing attacks with an aim to infiltrate Windows machines. A campaign related to the **Carbanak** malware, which uses compromised websites designed to host malicious installation files, has also been detected.

- A new cyber-espionage campaign targeting technology and telecoms companies in the Netherlands has been identified, carried out by **Sea Turtle,** an actor with links to Turkey. Security firm Hunt & Hackett reveals that the campaign focuses on targets with supply chain vulnerabilities, gathering political information.

- A recent campaign involving the **Lumma Stealer** malware has been identified, which exploits hacked **YouTube channels** as a distribution medium. The attackers post videos on these compromised channels, promising cracked software, and embed harmful URLs in the video descriptions. These URLs direct users to download a ZIP file, initiating a complex, multi-layered attack that eventually runs a .NET loader followed by the Lumma Stealer.

- **Tinsel Cosmos Taurus** is offering the **"Predator"** tool for sale on its private telegram channel. The tool has an initial starting price of $150 and is reportedly a stealer with network reconnaissance capabilities, targeting e-commerce, web development and CMS sites. It would also have a **malicious artificial intelligence module**.

- A cybersecurity incident has taken place at **Beirut Rafic Hariri International Airport** in Lebanon. The attack targeted the Flight Information Display System (FIDS), which was severely compromised.

ADVERSARIALLY
weekly report
Jan 04-10, 2024

XG3 UNIT

Spain & Portugal

- Actor **Fiesta Cosmos BetelgeuseX** is looking for members with web pentesting skills to carry out operations against individuals and companies in Barcelona. The actor required the applicants to have knowledge of javascript and offered remuneration.
- **STA Seguros**, the insurance brokerage of the Colegio de Aparejadores de Madrid, has been the victim of a cyber attack that has rendered its website unusable and paralysed its services.

LATAM

- Computer attack that has affected the business division of the **Tigo** telephony company in **Paraguay**, the culprits are the ransomware group Black Hunt. The report said that more than 300 companies working with Tigo were affected by the cybersecurity incident.

- Poorly secured Microsoft SQL (MS SQL) servers are under attack in Latin America (LATAM) as part of an ongoing financially motivated campaign to gain initial access, called **RE#TURGENCE by Turkish actors**. The analysed threat campaign appears to end in two ways: selling 'access' to the compromised host or delivering ransomware payloads.

- **"Coral Cosmos Taurus X"** sells access to a brazilian company that belongs to the retail sector and has 8M% of revenue. The access was offered in auction mode starting at $160.

- **"Desert Cosmos Taurus X"** sells access to a non-profit organisation with a revenue of 247M$. The access was offered in auction mode starting at an opening bid of $800. The access pointed to an RDWeb web resource with user permissions.

ADVERSARIALLY
weekly report
Jan 04-11, 2024

XG3 UNIT

Vulnerabilities & Exploits

- **APT29** took advantage of **CVE-2023-42793**, a recognized vulnerability that bypasses authentication and permits remote code execution. This flaw impacts several versions of the JetBrains TeamCity Server and has been used in broad-spectrum targeting. This affects worldwide IT and software development organizations, including a provider of IT services to critical U.S. infrastructure. Available public reports support the exploitation of the JetBrains flaw by APT29, suggesting widespread exploitation by the group starting from late September 2023, aiming at numerous global software development companies.

- Some active underground groups leveraged **CVE-2022-24086**, a vulnerability related to template injection in Magento Open Source and Adobe Commerce platforms, to install a webshell and then deploy a **WarlockWagon** loader script. Various eCrime entities appear to be deploying WarlockWagon for distinct operations.

- Chinese hackers exploiting two NEW ZERO-DAY vulnerabilities (**CVE-2023-46805 & CVE-2024-21887**) in Ivanti Connect Secure and Policy Secur attributed to a hacker group that it tracks under the name **UTA0178**. These together allow a remote attacker to access restricted resources by bypassing control checks and to send specially crafted requests and execute arbitrary commands on the device.

ADVERSARIALLY
weekly report
Jan 04-11, 2024

XG3 UNIT

Detections by Risk

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

- Suspicious remote connection from Rundll32 **(77.5)**
- Executing BASH files from a URL **(72.5)**
- Pwdump usage tool detection **(62.5)**
- Execution of netsh to open or redirect ports **(48.0)**
- Winrar execution using a .iso file **(36.5)**

Top MITRE Covered

- Command and Scripting Interpreter
- System Binary Proxy Execution
- User Execution
- Create or Modify System Process
- Modify Authentication Process

Adversary Trends

Actors

Lazarus Group
LAPSUS
Sandworm
ShinyHunters
Scattered Spider

Set Tools

SpectralBlur
Xamalicious
FalseFont
JaskaGo
NKAbuse

Vulnerabilities

Cisco / CVE-2024-20272
Cisco / CVE-2024-20287
Ivanti / CVE-2024-21887
Ivanti / CVE-2023-46805
Citrix / CVE-2023-4966

ADVERSARIALLY
weekly report
Jan 04-11, 2024

XG3 UNIT

Ransomware

Total Victims = 30 (-13)

- SPAIN - 1 (+1)
- LATAM - 1 (-1)
  Global - 28 (-13)

The king is...

Data of the week

Top Countries

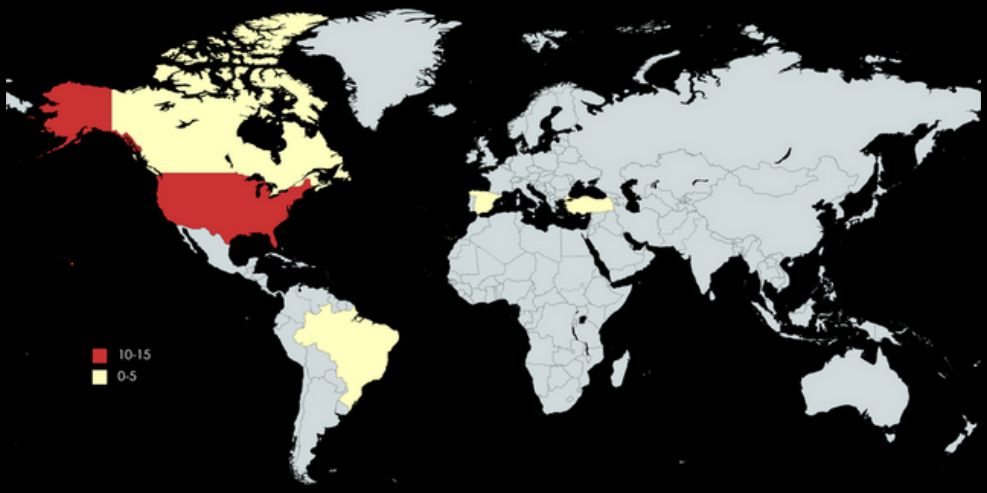
- USA - 14 (-6)
- CAN- 2
- ESP - 1
- BRA - 1
- TUR - 1

Top Sectors

- Commercial Serv. - 7 (-3)
- Healthcare - 4
- Manufacturing - 3 (-3)
- Education - 2
- Other - 2

Top Groups

- Hunters - 4
- Akira - 4
- Lockbit - 4 (-2)
- Knight - 2
- Blacksuit - 2



Victims

- **Ransom victim:** Grupo SCA. Grupo: Knight, Sector: Commercial Services. Country: Spain
- **Ransom victim:** Tigo. Grupo: Black Hunt. Sector: Telecom. Country: Paraguay

xMDR

ADVERSARIALLY

weekly report

Jan 04-11, 2024

cipher

a Prosegur company