ADVERSARIALLY

weekly report

Feb 08 - 15 , 2024

by

XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

Adversary of the Week

Chive Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Telecoms

Activity: Cybercrime

TTPs: Leak of confidential information

Dark Casino

Type: APT

Countries:

Maturity:

Sectors: Goverment, Defense, Finance

Activity: Information theft and espionage

TTPs: 16

LockBit 3.0

Type: APT

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 41

ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

Global

- The new **RustDoor malware for macOS** masquerades as the Visual Studio update. RustDoor has commands to control the compromised system and leak data, and can persist on the device by modifying system files.

- A **ransomware attack** affected at least **18 hospitals in Romania**, including regional and cancer treatment centres. It is currently **unknown** which **ransomware group** carried out the attack or whether patients' personal or medical data was also stolen during the incident.

- **Bank of America service provider Infosys McCamish Systems (IMS)** was hacked by the **LockBit ransomware** group, **affecting** more than **57,000 customers**, with information such as names, social security numbers and even account and credit card numbers leaked.

- **BitLocker encryption**, one of the most important security features for Windows 11 Pro, **has been breached by a Raspberry Pico** that costs less than five euros. The hack was carried out by a hacker who **has shared his exploit on YouTube**. The hacker managed to **compromise the security in just 43 seconds**, exploiting a flaw in BitLocker's design.

- Actor **Periwinkle Cosmos Taurus** offers on a popular dark web forum part of the **Facebook Marketplace database**, which **was hacked by** Dsicord actor **Goldenrod Cosmos Taurus**. The database contains more than 200,000 entries with information such as names, phone numbers or physical IDs.

- **French healthcare institutions Viamedis and Almerys** have been compromised and data on more than **33 million French patients has been exposed**. Among the leaked data are, social security number, medical insurance details and more. **Private information** such as **bank and contact details were not affected.**

- The **FBI has dismantled the Warzone RAT malware** operation, seizing the entire web infrastructure and **arresting** two associates, **Daniel Meli and Nigerian prince Onyeoziri Odinakachi** for distributing the malware and providing customer support to its purchasers, respectively. Server infrastructures were also identified and seized in Canada, Croatia, Finland, Germany, the Netherlands and Romania.

- **DarkStorm** has announced a series of **cyber-attacks** against government services and websites of **NATO countries, Israel and countries supporting Israel**.

- **R00TK1T** has announced **Operation Thunderstorm**, which consists of large-scale **cyber-attacks against Iraq for its support of terrorism.**

ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

Spain & Portugal

- **Onclusive**, the Spanish subsidiary of Symphony Technology Group, recently **suffered a cyber-attack** that **affected its monitoring systems and caused a lack of service** to several clients such as Casa del Rey, Iberdrola and the Ministry of Finance. The company has admitted the cyber-attack but **claims to have no evidence of the leak of private data.**

- The **SATSE health union** has been a **victim** of the **ransomware group Hunters**, which has published the incident on its website.

- Actor **Chive Cosmos Taurus** offers **full access to the customer accounts** of the phone company **Llamaya**. The database contains private information such as phone numbers, passwords, PUK, national identity card numbers, among others.

LATAM

- A **new banking Trojan called "Coyote"** has been discovered that targets users of more than **60 banking institutions, mostly in Brazil**. The malware uses the **Squirrel installer to distribute itself**, leveraging NodeJS and a relatively new cross-platform programming language called Nim as a loader to perpetrate the infection.

- Actor **Umber Cosmos Taurus** offers the offers the **database** of public institutions linked to the Colombian government, including the **National Intelligence Directorate** and the **Mario Gaitán Hospital**, in a well-known forum on the dark web.

- The **Rooterror threat actor** claims to have **compromised** some **subdomains** of **Mexico's National Institute of Anthropology and History (INAH).**

ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

Vulnerabilities & Exploits

- The patched Roundcube mail server vulnerability **CVE-2023-43770** is being actively exploited. It consists of a **persistent cross-site scripting (XSS) bug** that allows attackers to access restricted information via plain text messages. It is unknown which threat actor or actor group is doing the exploit.

- **Update:** Exploitation of the **Ivanti SSRF vulnerability CVE-2024-21893** has been confirmed **to install a new backdoor called DSLog** which allows threat actors to remotely execute commands on compromised Ivanti servers.

- **Cisco ASA SSL VPN devices** are attempting to be breached through the **exploitation of old vulnerabilities by the Akira and LockBit ransomware** groups. This could be a new trend in the exploitation of apparently patched vulnerabilities.

- A new **critical vulnerability** has been detected in **FortiOS SSL VPN**, listed as **CVE-2024-21762**, which allows threat actors to execute arbitrary code and commands. The US Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its list of exploited vulnerabilities.

- The **DarkCasino** threat group has been **exploiting the zero-day** vulnerability listed as **CVE-2024-21412,** which **bypasses Windows Defender's SmartScreen** and is being used by the APT group to run phishing campaigns against forex trading forums **to get victims to install the DarkMe malware.**

ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

⚠ Warning of the week

- Hold the phone! **BitLocker**, Windows 11 Pro's fortress, breached by a Raspberry Pico costing less than a coffee. Thought BitLocker had your back, keeping your data secure? Think again! Time to explore alternative encryption and enhance your security game.

- "Coyote" prowls the cyber streets targeting banks. Consider additional authentication layers, **regularly monitor financial transactions**, and educate your team about phishing risks.

- Alert! Patched **Roundcube mail server** vulnerability CVE-2023-43770 actively exploited. Encrypt sensitive emails, educate your team on phishing risks, and encourage cautious email practices.

- Akira and LockBit ransomware groups target Cisco ASA SSL VPN devices. **Keep VPNs updated**, use multi-factor authentication, and educate your team about VPN best practices.

- DarkCasino exploits zero-day vulnerability CVE-2024-21412, bypassing Windows Defender's SmartScreen. **Strengthen browser security**, exercise caution with links, and encourage safe browsing practices.

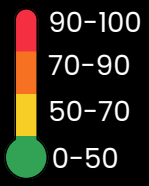
ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

Detections by Risk

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

- Possible malicious download from pastes domains **(57.5)**
- Internal FTP services connecting to outbound **(57.5)**
- Potential protocol tunneling via EarthWorm **(56.5)**
- Suspicious request to an URL shortener **(51.5)**
- Connection to External Network via telnet **(40.5)**



Rules with all or some of these features: Critical attack techniques, sophisticated adversaries, trending Mitre TTPs, relevant CVE scores
Rules with all or some of these features: High attack techniques, severe adversaries, trending Mitre TTPs, high CVE scores
Rules with all or some of these features: Medium attack techniques, risky adversaries, trending (or not) Mitre TTPs, medium CVE scores
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

- Application Layer Protocol
- System Network Configuration Discovery
- System Location Discovery
- Exfiltration Over Web Service
- Fallback Channels

Adversary Trends

Actors

Volt Typhoon
UNC2452
APT29
Scattered Spider
Strom-1567

Set Tools

Backmydata
RustDoor
Coathanger
Zardoor
KrustyLoader

Vulnerabilities

Microsoft / CVE-2024-21412
Microsoft / CVE-2024-21410
Microsoft / CVE-2024-21413
Adobe / CVE-2024-20738

ADVERSARIALLY
weekly report
Feb 08 - 15 , 2024

XG3 UNIT

Ransomware

Total Victims = 124 (+34)

- Spain - **4** (+1)
- Latam - **5** (-2)
  WorldWide - **115** (+35)

The king is...

Data of the week

Top Countries

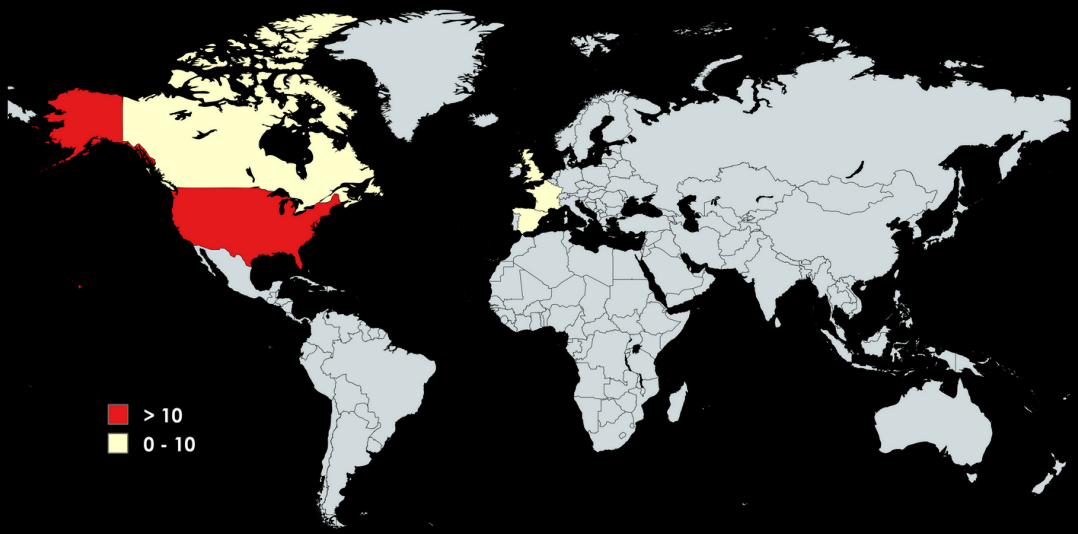
- USA - **53** (+10)
- CAN - **7** ☆
- GBR - **6** (-3)
- ESP - **5** ☆
- FRA - **5** (+1)

Top Sectors

- Services - **27** (+7)
- Manufacturing - **25** (+12)
- Health - **10** (+3)
- Other - **7** ☆
- Government - **6** ☆

Top Groups

- Lockbit - **48** (+22)
- Hunters - **16** ☆
- ALPHV - **12** ☆
- BlackBasta - **8** ☆
- Qilin - **7** ☆



Victims

- **Ransom Victim:** SATSE Health Union | Group: Hunters | Sector: Health | Country: Spain
- **Ransom victim:** Verdimed.es | Group: Lockbit| Sector: Services | Country: Spain
- **Ransom victim:** Movaral | Group: Lockbit | Sector: Services | Country: Spain
- **Ransom victim:** Sercide | Group: Alphv | Sector: Energy | Country: Spain
- **Ransom victim:** AXS | Group: Lockbit | Sector: Telecom | Country: Bolivia
- **Ransom victim:** Sea Telecom | Group: Akira | Sector: Telecom | Country: Brazil
- **Ransom victim:** YKP | Group: Ransomhub | Sector: Tech | Country: Brazil
- **Ransom victim:** Distecna | Group: Akira | Sector: Retail | Country: Argentina
- **Ransom victim:** ISSPOL | Group: Lockbit | Sector: Defense | Country: Ecuador

xMDR

ADVERSARIALLY

weekly report

Feb 08 - 15 , 2024

cipher

a Prosegur company