ADVERSARIALLY weekly report

Jan 12-18, 2024

by XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY

weekly report

Jan 12-18, 2024

Adversary of the Week

Tigerlily Cosmos Taurus

Type: Individual

Countries: 🇺🇸

Maturity: 🟩⬛⬛

Sectors: Beverage & Food

Activity: Cybercrime

TTPs: Valid Accounts
Leak of confidential information

APT-28

Type: APT

Countries: 🇺🇸 🇪🇺

Maturity: 🟥🟥🟥

Sectors: IT, Health, Goverment, Education

Activity: Information theft and espionage

TTPs: 68

LockBit 3.0

Type: Group

Countries: 🇪🇺 🇺🇸

Maturity: 🟥🟥🟥

Sectors: Health, Finance, Education

Activity: RaaS

TTPs: 41

Global

- A new victim portal for the **Noname ransomware** group has recently appeared. For now the victims are distributed mainly between the **United States** and **Brazil**. Among its extortion methods, it adds the new trend of notifying the competent authorities about the data breach in case of not reaching an agreement with the victim.

- **Fancy Bear** threat group was recently detected ted **carrying out a phishing campaign** aimed at organizations in Ukraine. During this operation, the threat actors **employed** three malware families: **OCEANMAP, MASEPIE, and STEELHOOK.** The primary goal of the campaign seems to be espionage.

- **Tigerlily Cosmos Taurus** claims in a cybercrime forum to have compromised the security of **McDonald's Corporation** and **sold the exfiltrated data**, including internal tools, names, emails, bank records and other private information.

- A new trend has recently been detected in the ransomware landscape. This is the **purchase of source code and infrastructure by new groups from old gangs**, which is leading to **mistaken attributions** in Ransomware as a Service campaigns. Among the actors following this trend are LockBit 3.0, who admitted that their code was based on code purchased from BlackMatter and code leaked from Conti with various upgrades.

ADVERSARIALLY
weekly report
Jan 12-18, 2024

Spain & Portugal

- **Calvià council** was the victim of a **ransomware cyber-attack** in the early hours of Saturday morning, according to the General Directorate of General Services. At the moment, **the actor** behind the attack **is unknown**, but we do know that the gang has demanded a ransom of approximately 10 million €.

- **BaladaInjector** malware is exploiting a vulnerability identified in a popular WordPress plugin called '**Popup Builder**'. This issue allows attackers to run malicious scripts on the infected websites. So far, it is estimated that this security flaw has affected more than 7751 websites worldwide. Among these sites, many correspond to Portugal and government from other countries.

- The **Basque Employment Service-Lanbide** detected a cyberattack on two "unused" servers since 2021 and advised individuals listed in files on these servers to take precautions against identity theft. This security incident, involving files affected by a cyberattack on an external supplier, was disclosed by Lanbide in a statement.

LATAM

- The private **data of hundreds of millions of Brazilians** were publicly accessible to threat actors, putting individuals at risk. Cybernews research revealed a publicly accessible **Elasticsearch instance**, which contained a staggering amount of private data belonging to Brazilian individuals.

- **Lotus Cosmos Taurus** requests in Raidforum "some police leaks in LATAM". This is a user whose registration is recent and only has this post.

- **Foliage Cosmos Taurus** sells CITRIX access to an undisclosed company from Brazil, with more than 1400 hosts and Local Admin permissions, in a Russian-speaking community. The sale is for $450 for the access.

- **Dewberry Cosmos Taurus** sells RDP access in a Russian-speaking community to a Brazilian company with 10.5M revenue. The access grants user privileges and is sold for 250$.

Vulnerabilities & Exploits

- **UPDATE:** More than 1,700 compromised Ivanti Connect Secure VPN devices have been detected infected with the **GIFFEDVISITOR** web shell. Attackers can execute arbitrary commands on all supported versions of Connect Secure and Policy Secure VPN devices, effectively combining two previously identified vulnerabilities, **CVE-2023-46805** and **CVE-2024-21887**. We have seen actors in the underground begin to show interest in developing a functional PoC that allows them to exploit the large number of vulnerable assets that are exposed on the internet before mitigation measures are applied.

- Critical vulnerability **CVE-2023-7028** affecting **GitLab** has been detected. The vulnerability is the result of an error in the email verification process. It is a flaw with which threat actors can reset user account passwords. According to GitLab, no abuse of this vulnerability has been detected.

- Vulnerability **CVE-2024-21591**, listed as critical, is an out-of-bounds write vulnerability in **Juniper Networks Junos OS SRX Series** and **EX Series J-Web** and allows an unauthenticated network-based attacker to cause a denial of service **(DoS)** or remote code execution **(RCE)** and gain **root privileges** on the device.

- Threat actors have been detected exploiting vulnerability **CVE-2023-36025**, already patched by Microsoft, to distribute an open source information stealer known as **Phemedrone Stealer**. The actors insert malicious files in Internet shortcuts or masked links that target browsers, crypto wallets and chat applications.

- A vulnerability has been detected in **Google authentication cookies**. This vulnerability allows attackers to access victims' accounts without changing passwords. In addition, threat actors can persist in the account undetected even if the victim changes passwords.

ADVERSARIALLY
weekly report
Jan 12-18, 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 Guardrails
- Native API
- Data from Local System

Adversary Trends

Actors	**Set Tools**	**Vulnerabilities**
Sandworm	Phemedrone_stealer	Google / CVE-2024-0519
UTA0178	CLINKSINK	Citrix / CVE-2023-6548
LAPSUS	THINSPOOL	Vmware / CVE-2023-34063
Lazarus Group	NoaBot	Gitlab / CVE-2023-7028
ShinyHunters	SpectraBlur	Fedoraproject / CVE-2023-45866

ADVERSARIALLY
weekly report
Jan 12-18, 2024

XG3 UNIT

Ransomware

Total Victims = 73 (+43)

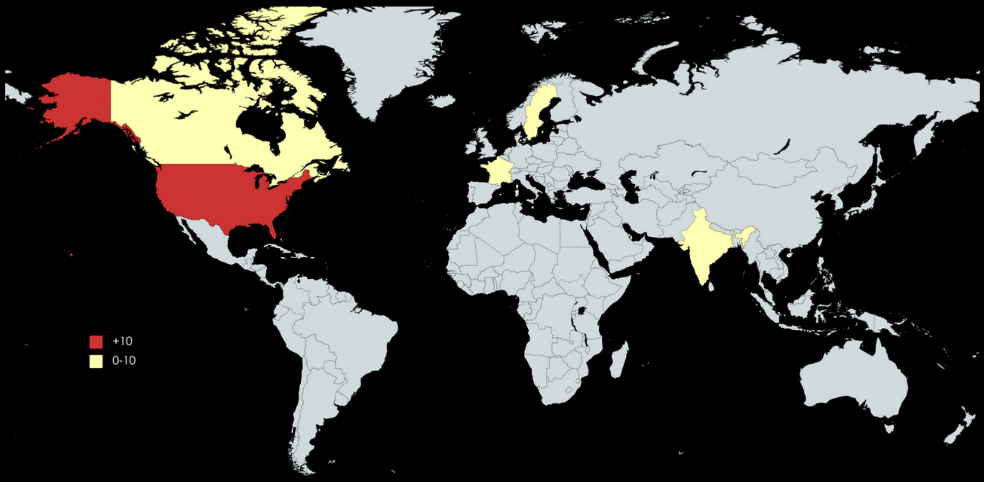
- Spain - **1**
- Latam - **2** (+1)

  WorldWide - **70** (+42)

The king is...

Data of the week

Top Countries	Top Sectors	Top Groups
USA - **29** (+15)	Manufacturing - **17** (+14)	Lockbit - **14** (+10)
FRA - **5** ☆	Commercial Serv.☆ - **15** (+8)	8Base - **10** ☆
CAN- **5** (+3)	IT - **6** ☆	Alphv - **7** ☆
IND - **3** ☆	Transport - **4** ☆	Akira - **6** ☆
SWE - **2** ☆	NGO - **3** ☆	Cactus - **5** ☆



Victims

- **Ransom victim:** Selmi[.]com[.]br | Group: Noname | Sector: Manufacturing | Country: Brazil
- **Ransom victim:** Promerica Bank | Group: Snatch | Sector: Finance | Country: Brazil
- **Ransom victim:** Calvià council | Group: Unknown | Sector: Government | Country: Spain

xMDR

ADVERSARIALLY
weekly report
Jan 12-18, 2024

cipher

a Prosegur company

LEGAL NOTICE: PROHIBITION OF DISTRIBUTION, USE OR SHARING WITHOUT AUTHORIZATION This document (hereinafter, “the Document”) is the exclusive property of Prosegur Ciberseguridad S.L. (hereinafter, “the Owner”). The Owner possesses all intellectual property rights associated with the Document, including, among others, copyright and property rights. Access to this Document is granted only to parties authorized by the Owner for the specific purpose of confidential evaluation.

Any distribution, reproduction, unauthorized use, disclosure or sharing of the Document, in whole or in part, with third parties without the prior and express written authorization of the Owner is strictly prohibited. Any unauthorized use of the Document will constitute a violation of the Owner’s intellectual property rights and may result in legal action. Access and use of this Document are subject to the terms and conditions established by the Owner. Any authorized party that receives the Document must comply with the restrictions and obligations established by the Owner.
Any questions or requests for authorization for distribution, reproduction or use of the Document should be directed to the Owner.

Failure to comply with these restrictions may have legal consequences. By accessing or using the Document, you accept and acknowledge the terms of this legal notice.