ADVERSARIALLY

weekly report

Jan 18 - 25, 2024

by

XG3 UNIT

cipher
a Prosegur company

xMDR

ADVERSARIALLY
weekly report
Jan 18-25, 2024

XG3 UNIT

Adversary of the Week

Salmon Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Beverage & Food

Activity: Cybercrime

TTPs: Leak of confidential information

Star Blizzard

Type: APT

Countries:

Maturity:

Sectors: Thinks Tanks, Defense, NGO

Activity: Information theft and espionage

TTPs: 9

LockBit 3.0

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 41

ADVERSARIALLY
weekly report
Jan 18-25, 2024

XG3 UNIT

Global

- One of the **largest password thefts** in history has been detected, containing 71 million passwords. In relation to the usual suspicions that it is a compilation of previous data, it has been found that this registry has at least 20 million new records that have not been publicly known to date.

- A leak of the widely used business platform **Trello** has also been observed to have been posted on a popular underground hacking forum by the actor known as **Salmon Cosmos Taurus**.

- Continuing with data leaks, **VF Corp**, known for housing famous clothing brands such as **Vans and The North Face**, has experienced a cyberincident that has compromised the information of more than 35 million customers.

- It has been made public that China has managed to **bypass AirDrop data encryption**, leaving users' data exposed, as they have claimed to have the ability to intercept and breach AirDrop transmissions.

- **Microsoft** has suffered a cyberattack on its systems and points to a **Russian state-sponsored actor**; the multinational is unsure whether "clients, production systems, source code or artificial intelligence systems" have been affected.

- A new campaign carried out by the Russian state-linked **Coldriver aka Star Blizzard group** has been detected and has gone a step further in its phishing campaigns, adding the distribution of **SPICA malware** to steal confidential data from Western officials.

- The previous week saw the hacking of the **US Securities & Exchange Commission** (SEC) Twitter account, which publicised content about cryptocurrencies that affected the value of the currency. This week they have confirmed that this attack could be carried out thanks to the **SIM Swapping technique**, with which the malicious actors were able to bypass the 2FA.

ADVERSARIALLY
weekly report
Jan 18-25, 2024

Spain & Portugal

- Perfumery chain **Douglas** has alerted its Spanish customers that it has suffered a cyber-attack, and acknowledges that their **data has been exposed**. As part of its investigation, Douglas has identified a fake website that appeared to be intended to impersonate the real thing, and suspects that cybercriminals were planning to use customers' personal details to redirect them to the fraudulent site.

- Actor **Tomato Cosmos TaurusX** confirmed the sale on a private Russian forum of access via CITRIX to a Spanish company whose revenue has not been disclosed. The sale was made for USD 600 and provided local administrator access.

LATAM

- Actor **DeepPink Cosmos TaurusX** sells RDP access on a private forum of Russian origin to a Brazilian software industry company with revenue of $75 million. The access grants domain administrator permissions

- Actor **Thistle Cosmos TaurusX** sells RDP access on a private forum of Russian origin, to an Argentinean company dedicated to the service industry with revenue of $15 million. The access grants unprivileged user permissions.

ADVERSARIALLY
weekly report
Jan 18-25, 2024

XG3 UNIT

Vulnerabilities & Exploits

- Critical Vulnerability Alert **(CVE-2023-35636)**: A medium-severity flaw in Microsoft Outlook, WPA (Windows Performance Analyzer), and Windows File Explorer enables extraction of **NTLMv2 hashes**. Organizations are advised to take immediate action to mitigate risks.

- Apple's recent updates across macOS Sonoma, tvOS 17.3, iOS 17, and iPadOS 17 include fixes for a **WebKit security vulnerability CVE-2024-23222**, which was actively exploited. Alongside introducing features like Stolen Device Protection, these updates also address a GPU vulnerability highlighted by researchers. Apple extends these security patches to older OS versions, updating iOS 15 to 15.8.1 and iOS 16 to 16.7.5.

- Fortra disclosed a critical authentication **bypass vulnerability CVE-2024-0204** in GoAnywhere MFT, allowing remote attackers to create admin users. This vulnerability poses a severe security risk, potentially leading to unauthorized data access, malware infections, or complete device takeover. While there are no reports of active exploitation, the predecessor vulnerability (CVE-2023-0669) was exploited by ransomware groups like **Cl0p, LockBit, and BlackCat**, resulting in a 91% increase in ransomware attacks. Fortra recommends upgrading to GoAnywhere MFT version 7.4.1 or higher and provides alternative manual methods to mitigate the vulnerability. A public **Proof-of-Concept (PoC) exploit is available**, increasing the risk of exploitation. Organizations should monitor for new additions to the 'Admin users' group and observe last logon activities to detect potential compromises.

ADVERSARIALLY
weekly report
Jan 18-25, 2024

XG3 UNIT

Detections by Risk

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

- Detection of Powershell obfuscation techniques in CL **(78.5)**
- Potential Linux webshell execution **(73.0)**
- Download detected using different Powershell methods **(68.5)**
- External connections to internal RDP services **(63.5)**
- Potential Rose Flamingo loader filename **(63.5)**

Top MITRE Covered

- Command and Scripting Interpreter
- Exploitation for Client ExecutionExecution
- Obfuscated Files or Information
- Server Software Component
- External Remote Services

Adversary Trends

Actors

Sandworm
UTA0178
LAPSUS
Lazarus Group
ShinyHunters

Set Tools

MediaPI
SPICA
phermedrone_stealer
Bigpanzi
THINSPOOL

Vulnerabilities

Fortra / CVE-2024-0204
Vmware / CVE-2023-34048
Atlassian / CVE-2023-22527
Apple / CVE-2024-23222
Apache / CVE-2023-49657

ADVERSARIALLY
weekly report
Jan 18-25, 2024

XG3 UNIT

Ransomware

Total Victims = 97 (+24)

- Spain - **2** (+1)
- Latam - **4** (+2)
  WorldWide - **91**

The king is...

Data of the week

Top Countries

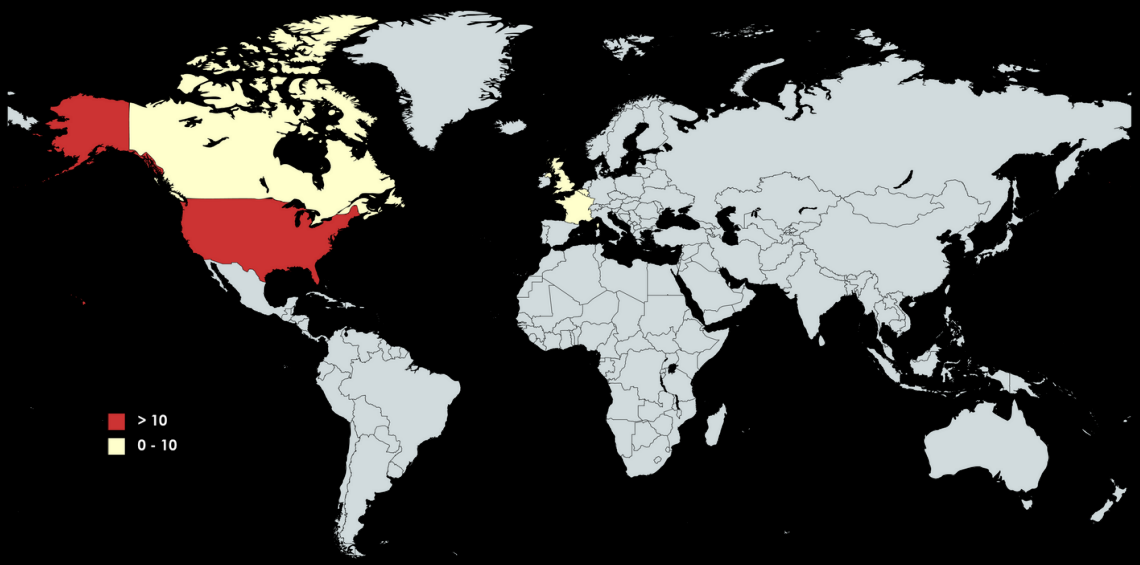
- USA - **42** (+13)
- FRA - **7** (+2)
- GBR - **5**
- CAN - **4**
- BEL - **3**

Top Sectors

- Industrial - **23**
- Services - **22**
- Education - **6**
- NGO - **6** (+3)
- Transport - **5** (+1)

Top Groups

- Lockbit - 30 (+16)
- Blackbasta - **12**
- 8Base - **9**
- Alphv - **7**
- Akira - **6**



Victims

- **Ransom victim:** uffs.edu.br | Group: Stormous | Sector: Education | Country: Brazil
- **Ransom victim:** Alupar Investimento SA | Group: Hunters | Sector: Energy | Country: Brazil
- **Ransom victim:** Jasman.com.mx | Group: Hunters | Sector: Energy | Country: Brazil
- **Ransom victim:** wendy.mx | Group: Lockbit 3.0 | Sector: Services | Country: Mexico
- **Ransom victim:** swiftair.com | Group: Lockbit 3.0 | Sector: Services | Country: Spain
- **Ransom victim:** Marxan.es | Group: Lockbit 3.0 | Sector: Services | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Jan 18-25, 2024

cipher

a Prosegur company