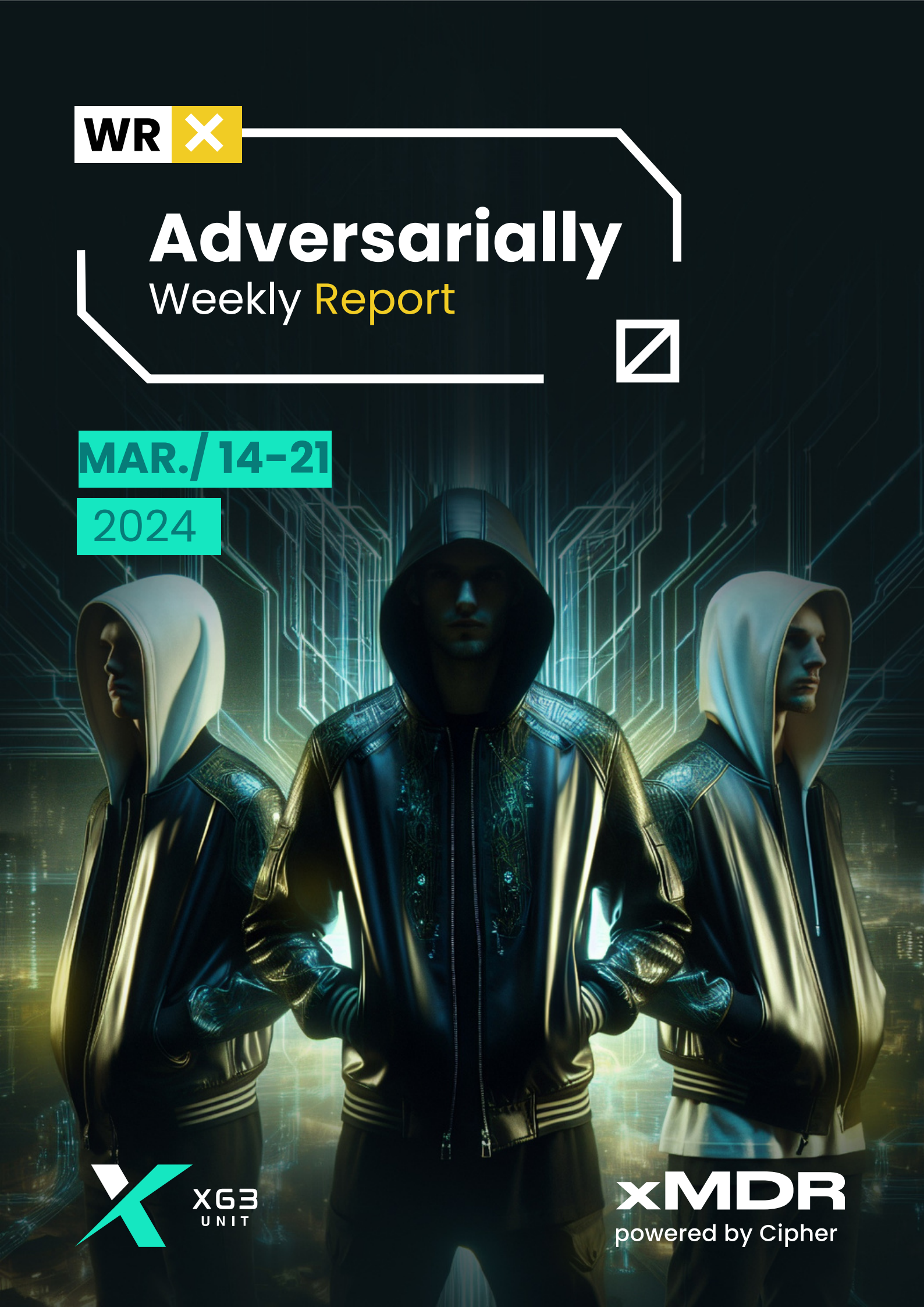
WR X

Adversarially

Weekly Report

MAR./ 14-21

2024



XG3 UNIT

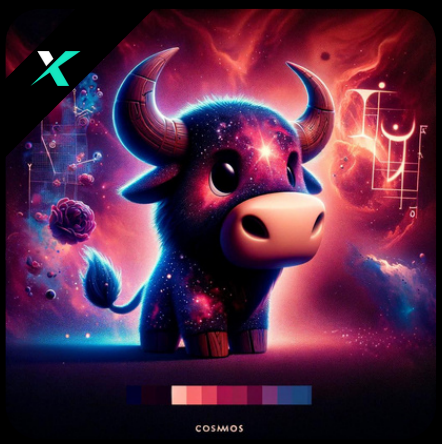
xMDR

powered by Cipher

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

Adversary of the Week



Rosewood Cosmos Taurus

Type: Individual

Countries:

Maturity:

Sectors: Government

Activity: Cybercrime

TTPs: Defacement

Horizon3

Type: Group

Countries:

Maturity:

Sectors: Education, Healthcare

Activity: Cybercrime

TTPs: Exploit Public-Facing Application

Raworld

Type: Group

Countries:

Maturity:

Sectors: Health, Chemical, Logistic, Automobile...

Activity: RaaS

TTPs: Indeterminated yet

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

Global

- Threat actor group **LAPSUS$ has announced** on its Telegram channel the launch and sale of **its new FUD ransomware**. Features include disabling UEFI, C disk encryption and the ability to disable Windows Bitlocker.

- On March 17, 2024, over **70 million AT&T records were leaked** on the Breached forum by 'MajorNelson.' Data authenticity, dating back to a 2021 theft, has been confirmed. In 2021, ShinyHunters and Scarfac33 claimed they had AT&T customer data, attempting an auction for $200,000. Despite AT&T's denial of a breach, Social Security numbers were involved.

- Hacktivists linked to '**Handala Hack**,' a pro-Palestinian group, allege **they've hacked Viber, taking 740GB of data**, including source code, demanding 8 Bitcoin as ransom. While Viber refutes the breach, it's probing the claim. A confirmed breach could expose Viber user messages, calls, contacts, and financial data.

- France's employment agency, **France Travail,** reported a major **data breach impacting 43 million users** registered in the last 20 years, possibly revealing personal details such as names, social security numbers, and contact information.

- **McDonald's restaurants are suffering global IT outages** that prevent employees from taking orders and accepting payments, causing some stores to close for the day. The outages started overnight and are impacting restaurants globally.

- Researchers have noticed a **comeback of the CryptoWire ransomware**, first seen in 2018, now spread chiefly through phishing emails and built with Autoit script. The decryption key for CryptoWire is either embedded in the Autoit script or found in the data transmitted to the command and control (C2) servers.

- A **new campaign** named "**PhantomBlu**" has been identified, targeting organizations in the US with the **NetSupport RAT via manipulated Microsoft Office documents** using OLE template techniques.

- Japanese tech giant **Fujitsu discovered that several of its systems were infected by malware** and warns that the hackers stole customer data, including sensitive information of customers.

- **Nissan** suffers a **data breach** following a ransomware attack executed by the criminal group **Lockbit** in its new version **3.0**.

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

Spain & Portugal

- **FIATC Seguros** has informed its customers of a **security breach** that has **affected its entire database**, although it assures them that no health or banking data has been leaked, and has not informed them of the real extent of the situation.

- **Mint Cream Cosmos Taurus X** is selling access with local admin privileges to a Spanish company with $10 million in revenue. The sector is not disclosed. The price is $700.

- **Tomato Cosmos Taurus X** sells Pulse Secure access only VPN, from an unidentified Spanish company, with revenues of more than 4 billion for 1500$.

- **Springgreen Cosmos Taurus X** offers access to spanish crypto exchange's admin panel for $10,000 in Monero.

- **Springgreen Cosmos Taurus X** sells for $2000 in Monero access to the Dirección General de Tráfico (DGT) in Spain to search for license plates or people by their DNI.

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

LATAM

- **VividOrangePeel Cosmos Taurus** 𝕏 is offering access to a financial services company in Brazil, with revenues of $44 million, for $6000.
- **Rosewood Cosmos Taurus** 𝕏 allegedly claims to have defaced a sub-domain of the Belém Municipal Council in Brazil.
- **Venetian Red Cosmos Taurus** 𝕏 allegedly claims to have defaced a subdomain of the Instituto Federal do Espírito Santo (IFES).
- The hacktivist group **La Resistencia** leaks data from the Marketplace Katapulk, which offers online shopping services to all of Cuba.
- **Museo de La Plata website** has been **defaces**, exposing configuration files with sensitive information and **leaking a database with 697k rows and 22k users with passwords.**

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

Vulnerabilities & Exploits

- In March 2024, Microsoft's Patch Tuesday addressed 61 security flaws, with two critical vulnerabilities in Windows Hyper-V that could lead to remote code execution and denial of service. The most severe non-critical flaw was a remote code execution issue in Open Management Infrastructure. Adobe, Fortinet, and SAP also released patches for various critical vulnerabilities in their products, enhancing security against potential exploitation.

- Criminals target a flaw (**CVE-2024-23334**) in the aiohttp Python library, impacting concurrent HTTP requests handling. This vulnerability, patched in version 3.9.2, lets attackers remotely access files outside the server's root directory. Detected since late February, these attacks are linked to the ShadowSyndicate ransomware group. Despite uncertain total impact, around 44,170 aiohttp instances are exposed globally, with the highest number in the US. The prevalence of outdated versions complicates patching efforts, leaving systems vulnerable to exploitation.

- WordPress has issued a warning to uninstall miniOrange's Malware Scanner and Web Application Firewall plugins due to a critical vulnerability, identified as **CVE-2024-2172**. This issue impacts up to Malware Scanner 4.7.2 and Web Application Firewall 2.1.1, with both plugins discontinued as of March 7, 2024. The flaw enables attackers without authentication to gain admin rights by changing user passwords, risking entire site security. Wordfence highlighted the risk of file uploads and content alterations by attackers. Additionally, a serious vulnerability in the RegistrationMagic plugin, **CVE-2024-1991**, affecting versions up to 5.3.0.0, was fixed in the 5.3.1.0 update on March 11, 2024.

- Researchers at Tarlogic have discovered that vulnerabilities **CVE-2023-4586** and **CVE-2024-21306** can be exploited through BlueSpy, a PoC they have developed which allows listening in on conversations from Bluetooth headsets without the knowledge of their users.

- A recently remediated SQL injection vulnerability (**CVE-2023-48788**) in Fortinet's FortiClient Endpoint Management Server (EMS) solution has piqued the interest of threat actors. The Horizon3 attack team is going to make a release with technical details and a PoC. In addition, a user created a GitHub page announcing a "new exploit" for CVE-2023-48788 and linked it to a post on SatoshiDisk.com, a web platform where users can upload files they want to sell and others can download them if they pay a set price.

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

⚠️ Warning of the week

- Get your digital tomahawks ready: **LAPSUS$ is launching a new ransomware** boat! Keep your cyber treasure safe: update defences, make backups and don't let those scoundrels block your loot! 🏴‍☠️💰

- Guess who's back? **CryptoWire, the ransomware** with a flair for drama! Stay sharp: avoid suspicious emails like you dodge spoilers, and keep those cyber defenses strong enough to ward off even the most persistent script kiddies!" 💻

- Watch out for the **PhantomBlu**—it's not a friendly ghost! Keep your guard up: treat suspicious Microsoft Office docs like hot potatoes and don't let the **NetSupport RAT** sneak into your digital fortress!🛡️

- Watch out for those sneaky **Python snakes! Update aiohttp** like a pro—version 3.9.2 is your shield against file-wielding villains. Don't let cyber-crooks snoop outside your server's root; keep your digital garden secure!" 🐍🔒

- Time to **clean up your WordPress plugins** like Marie Kondo! Say '**Thank you, next!**' to **miniOrange's Malware Scanner and Web Application Firewall**. **Update RegistrationMagic too**—keep your site tidy and safe from cyber clutter! 🧹

- Watch out for **SQL injection sharks lurking in FortiClient's** waters! Don't let threat actors catch you swimming unprotected. **Stay alert for fishy GitHub links**—keep your data safe and avoid sinking like a ship in choppy cyber seas!" 🦈🛡️

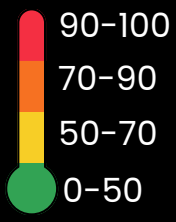
ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

Detections by Risk

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

- Possible Cobalt Strike library loaded **(76.5)**
- Possible Mimikatz library loaded **(76.5)**
- DNS requests from Cobalt Strike beacons **(75.5)**
- Netcat network activity **(66.5)**
- Account set with Kerberos DES encryption activated **(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

- User Execution
- Application Layer Protocol
- Exfiltration Over Alternative Protocol
- Ingress Tool Transfer
- Non-Standard Port

Adversary Trends

Actors

UNC2452
Volt Typhoon
Storm-1567
APT29
Lazarus Group

Set Tools

AcidPour
StopCrypt
VCURMS
GTPDOOR
ToddlerShark

Vulnerabilities

Jetbrains / CVE-2024-27198
Wordpress / CVE-2024-2387
Fortinet / CVE-2023-48788
Phyton / CVE-2024-23334

ADVERSARIALLY
weekly report
Mar 14 - 21, 2024

XG3 UNIT

Ransomware

Total Victims = 80 (-20)

- Spain - **1** (-1)
- Latam - **1** (-2)
  WorldWide - **78** (-17)

The king is...

Data of the week

Top Countries

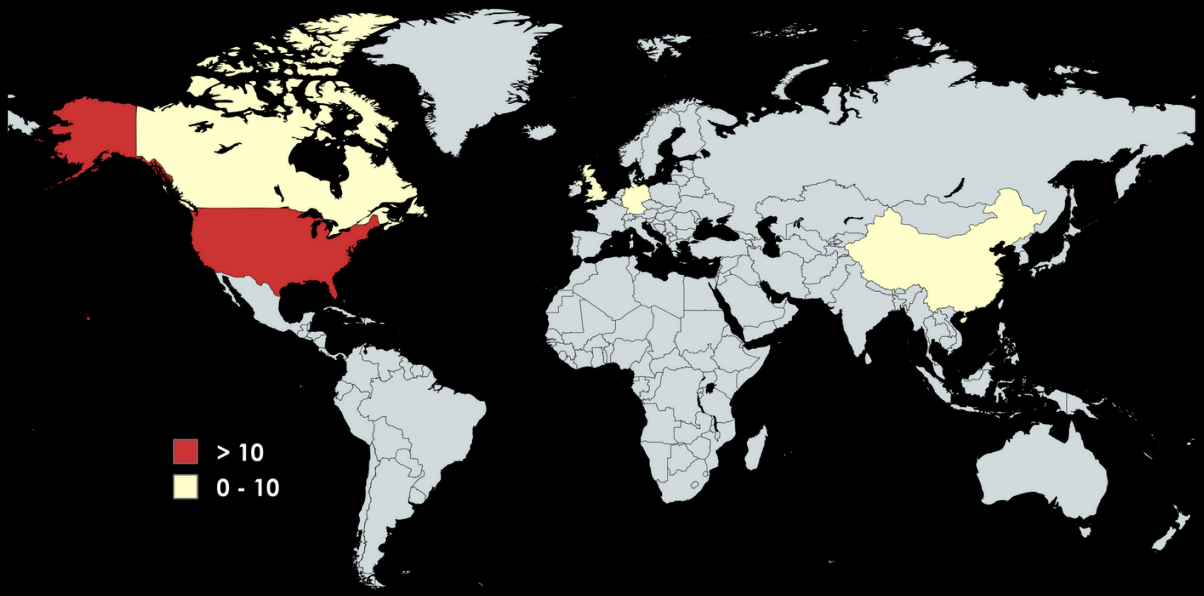
- USA - **36** (-5)
- GBR - **6** (-1)
- CAN - **5** (+1)
- DEU - **5**
- CHN - **3** ☆

Top Sectors

- Services - **17** (-9)
- Manufacturing - **14** ☆
- Financial- **13** (+7)
- Health - **12** (+2)
- Others - **5**

Top Groups

- Raworld - **30** ☆
- Lockbit - **20** (+12)
- Hunters - **9** ☆
- Medusa - **8**
- BlackBasta - **6** (-5)



Victims

- **Ransom Victim:** HSI | Group: Hunters International | Sector: Technology | Country: Spain
- **Ransom victim:** Bwizer | Group: Trigona | Sector: Education | Country: Portugal
- **Ransom victim:** Cosmocolor | Group: Hunters International | Sector: Technology| Country: Mexico
- **Ransom victim:** | Group: | Sector: | Country:

xMDR

ADVERSARIALLY

weekly report

Mar 14 - 21, 2024

cipher

a Prosegur company