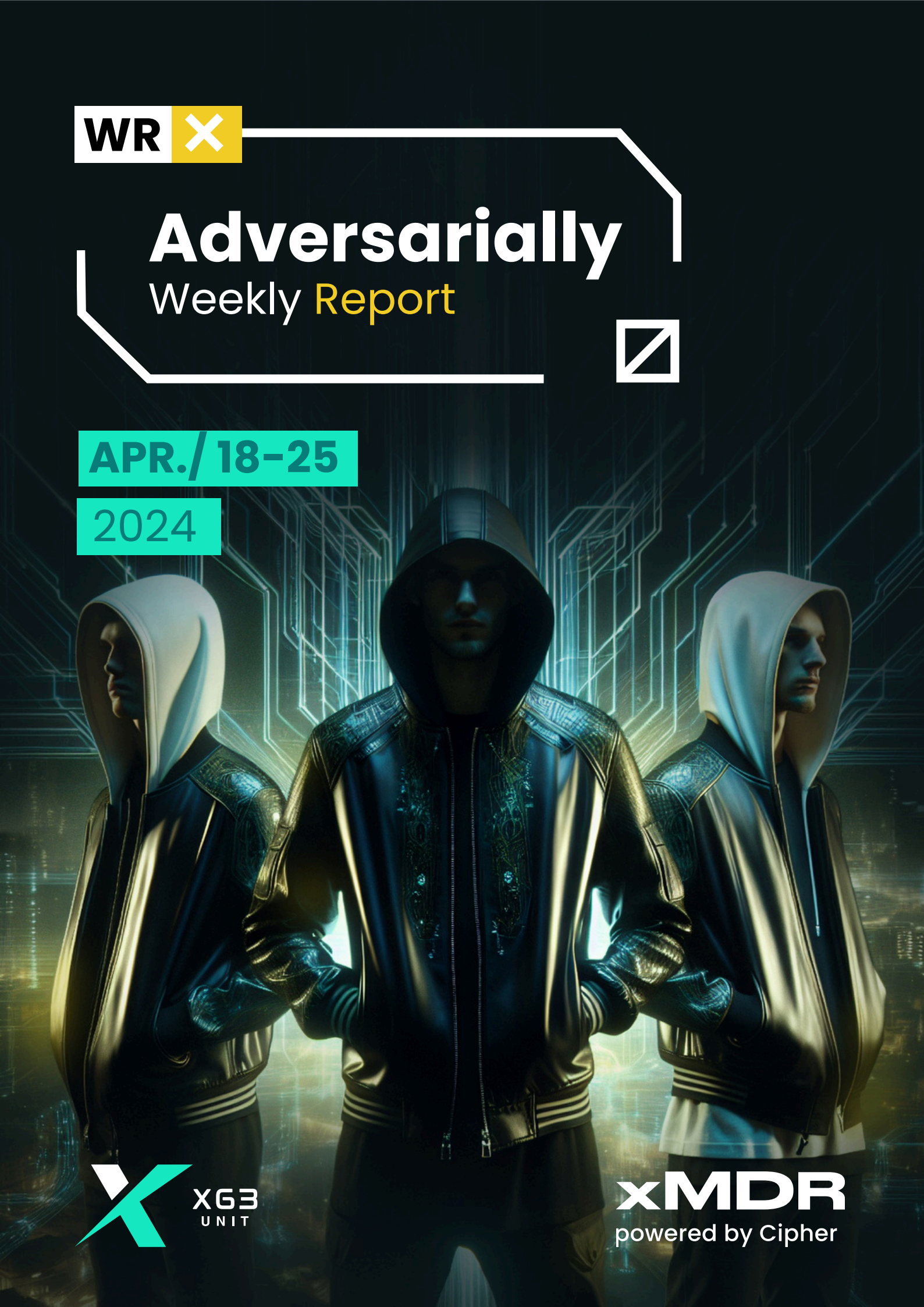
WR X

Adversarially

Weekly Report

APR./ 18-25

2024



XG3 UNIT

xMDR

powered by Cipher

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

Adversary of the Week

Sandworm Team

Type: APT

Countries:

Maturity:

Sectors: Government, Telecoms, Energy

Activity: Sabotage and destruction

TTPs: 70

Noname057(16)

Type: Group

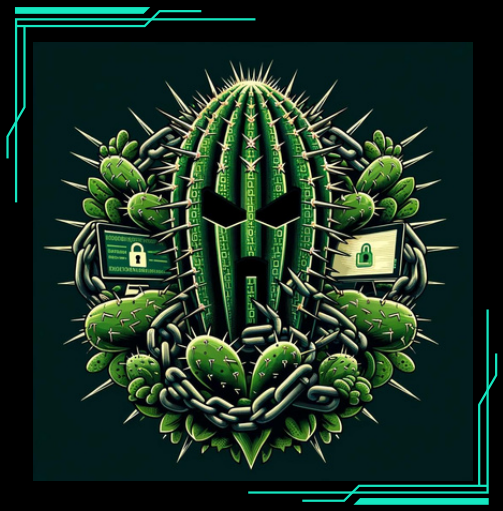
Countries:

Maturity:

Sectors: Transport, Telecoms, Defense...

Activity: Sabotage and destruction

TTPs: 19



Cactus

Type: Group

Countries:

Maturity:

Sectors: All

Activity: RaaS

TTPs: 46

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

Global

- The **BlackTech group** is carrying out a **new campaign** against the **technology**, **research**, and **governmental** sectors in the Asia-Pacific, **using** their Waterbear backdoor and a **new variant** they have developed known as **Deuterbear**.

- The threat group **UserSec** has announced via its Telegram channel that it is launching a **campaign aimed at targets in Europe and NATO**. It claims it will **damage servers**, which could lead to system outages and leaks of private information.

- Russia's **Sandworm** launched a major **assault on Ukrainian critical infrastructure**. They made **use** of various backdoors such as **Biasboat, Loadgrip, Queueseed and Gossipflow**, which allowed them to discover the threat group that carried out the attack.

- **UTA0178,** the actor-state-nation linked to China, may have been responsible for the **security incident suffered by NERVE**, a **collaborative network** that provides storage resources **to MITRE**. This incident unfolded by exploiting two zero-day vulnerabilities to compromise an internal VPN and thus bypass MFA through session hijacking.

- The **South Korean National Police Agency** has issued a security **notice warning** Korean companies about the **Lazarus, Andariel and Kimsuky** groups. It has been revealed in an investigation that these groups carried out successful **attacks against state defence-related companies**, stealing classified information.

- **FIN7** has been linked to a **spear-phishing campaign** targeting the U.S. automotive industry to **deliver** a known backdoor called **Carbanak** (aka Anunak).

- The **Australian Federal Police** (AFP) has **arrested five men** as part of a global raid on a cyber-criminal gang linked to industrial-scale phishing. **The sting relates to the website LabHost**, which was used to steal personal information from 94,000 people in Australia, and many more overseas.

- **Lazarus** reappears carrying out its **attacks through Linkedin** and managing to deploy **malwares** against its victims to steal information from their devices as well as passwords or cryptographic keys.

- A **new stealer** has been detected for sale on the darkweb called **Samurai Stealer.** Among its features is that it has **zero dependencies** and can **run on different versions of the Windows** operating system, and that **all logs** sent to the server **are encrypted and decrypted on the server side only**.

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

Spain & Portugal

- **Update:** The Civil Guard has detected a **phishing campaign** in which the ransomware group that stole private information weeks ago is sending emails **pretending to be the medical recognition company** to its agents **with malicious links.** The entire police force is being alerted to delete the email and not fall victim to the cyberattack.

- A new **smishing campaign** has been alerted in which threat actors are **impersonating CORREOS** (the Spanish postal service) and attempting to get you to fill out a form with your personal information, as well as pay a sum of money. With this impersonation, attackers can gather private information as well as banking details from victims.

- **Rocketmetallic Cosmos Taurus** is sharing private information about 1.8k users of Miguel Hernandez University on a well-known English forum.

- **Rocketmetallic Cosmos Taurus** is offering for 150$ a database with private information such as names, addresses, NIF/CIF, etc., about 138k user records from FNMT (Fábrica Nacional de Moneda y Timbre) on a well-known english forum.

- **Palegreen Cosmos Taurus** claims on a well-known Russian-speaking forum to have gained access to EVO Banco's systems and obtained private and confidential information of customers such as names, addresses, and even IBAN numbers.

- **Noname057(16)** has been carrying out **denial of service attacks** on various **Spanish entities**, both public and private, on the **18th, 19th, 21st, and 22nd of April.** Among them are websites of various town halls, Spanish banks, and transportation companies.

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

LATAM

- **Radicalred Cosmos Taurus** is offering corporate access via Fortinet VPN to a Mexican company for 4000$ on a well-known English-speaking forum.

- **GlorySec** has announced via their Telegram channel that they have managed to breach the systems of the Central Bank of Venezuela and the United Socialist Party of Venezuela.

- A **new ransomware group** known as **Quiolong** is waging a **campaign** against the **health sector in Brazil**. Among the victims is the Andréa Rechia plastic surgery clinic, which has managed to extract more than 30GB of private and sensitive patient information.

- **Lightlategray Cosmos Taurus** claims on a well-known English forum to have obtained PII information about over 28k users of the Chilean store 'El Carnicero'.

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

Vulnerabilities & Exploits

- A **vulnerability affecting GitHub** was actively exploited by various threat actors. This vulnerability allowed them to attach documents or files through posting comments on legitimate projects using a URL that would be loaded into GitHub's CDN and associated with the related project. An added issue is that even if the company becomes aware of this problem, they have no available option to manage those attached files.

- **Orchid Cosmos Taurus** is allegedly **selling** on a well-known Russian forum an **exploit for a zero-day vulnerability** targeting the **VMWare ESXi Shell service** that allows attackers to bypass authentication and thus get the vpxuser to remotely load files into the /scratch directory. The selling **price** is **$1,5M** payable via Monero.

- Cybersecurity expert engineer **Jaime Gómez-Obregón** has **found a vulnerability** affecting the **City council minutes recorded on video** throughout Spain, through which it **is possible to view part of the application's source code**, details of the structure, and information about some developers.

- A new vulnerability has been discovered, identified as **CVE-2024-21111**, with a score of 7.8, which **affects VirtualBox installations on Windows**. It allows attackers to perform a local privilege escalation to system level.

- A **critical vulnerability** tracked as **CVE-2024-31497** has been identified **in PuTTY** versions 0.68 to 0.80, **the biased ECDSA nonce generation** that allows an attacker to retrieve a user's NIST P-521 secret key via a quick attack in approximately 60 signatures.

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

⚠️ Warning of the week

- Watch out for **sneaky attachments on GitHub!** Be cautious of comments with **suspicious URLs**—don't click unless you trust the source. Report any suspicious activity to GitHub, and be careful with what you download. Stay safe and keep your code clean! 🛡️👀

- **Secure your VirtualBox setup**, mate! Update to the latest version pronto to **patch CVE-2024-21111**. Be cautious of what you download and run on your system. Keep your guard up and don't let cyber-snoopers sneak into your Windows machine! 🛡️💻

- Yikes! **Keep your systems safe from GlorySec's antics**. Tighten security: **update passwords**, install firewalls, and monitor for unusual activity. Don't let cyber-crooks take over your private information—stay vigilant and protect your digital turf! 💰🔒

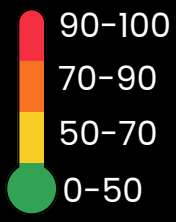
ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

Detections by Risk

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

- Command line utility executed from Mshta **(67.5)**
- Potential OpenSSH backdoor logging activity **(62.5)**
- Execution of Csvde to gather AD information **(60.5)**
- Execution of suspicious commands from an external removable device **(57.5)**
- Appinstaller lolbin suspicious execution **(38)**



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

- System Binary Proxy Execution
- Compromise Client Software Binary
- Modify Authentication Process
- Account Discovery
- Replication Through Removable Media

Adversary Trends

Actors

Sandworm
Storm-1567
APT28
Lazarus Group
Kimsuky

Set Tools

GooseEeg
Kapeka
SoumniBot
UPSTYLE
MadMxShell

Vulnerabilities

Paloaltonetworks / CVE-2024-3400
Microsoft / CVE-2022-38028
CrushFTP / CVE-2024-4040
Freerdp / CVE-2024-32658
Dell / CVE-2024-28976

ADVERSARIALLY
weekly report
Apr 18 - 25, 2024

XG3 UNIT

Ransomware

Total Victims = 433 (+306)

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

WorldWide - **427** (+306)

The king is...

Data of the week

Top Countries

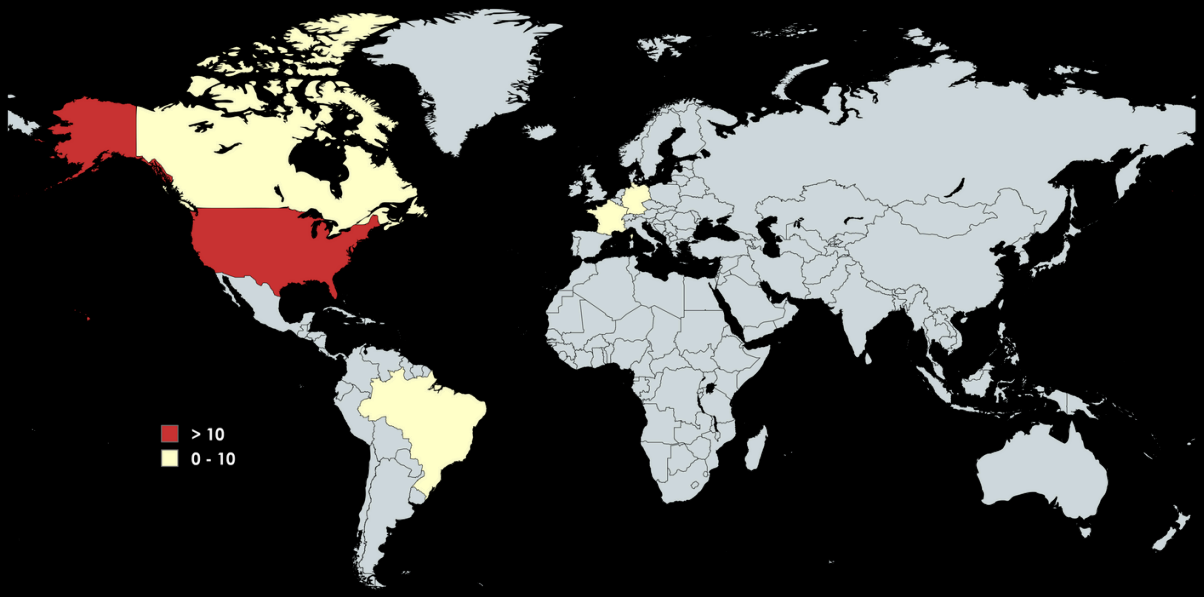
- USA - **46** (-29)
- CAN -**10** (+4)
- DEU - **7**
- BRA - **4**
- FRA - **4** (-1)

Top Sectors

- Manufacturing - **49** (+35)
- Healthcare - **48** (+38)
- Technology - **39** (+21)
- Finance - **24**
- Education - **19**

Top Groups

- Cactus - **16**
- Lockbit3 - **12** (+2)
- Ransomexx - **11**
- Ransomhub - **9**
- Bianlian - **9**



Victims

- **Ransom Victim:** www.drlincoln.com.br | Group: qiulong | Sector: Healthcare | Country: Brazil
- **Ransom Victim:** www.rosalvoautomoveis.com.br | Group: qiulong | Sector: Commerce | Country: Brazil
- **Ransom Victim:** draandrearechia.com.br | Group: qiulong | Sector: Healthcare | Country: Brazil
- **Ransom Victim:** FábricaInfo | Group: ransomhub | Sector: Manufacturing | Country: Brazil
- **Ransom Victim:** Consorci Sanitari Integral | Group: ransomexx | Sector: Healthcare | Country: Spain
- **Ransom Victim:** ebir.com | Group: cactus | Sector: Technology | Country: Spain

xMDR

ADVERSARIALLY

weekly report

Apr 18 - 25, 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.