Telefónica Tech

CYBER SECURITY

SIA Essentials

Threat Landscape Report 2023

telefonicatech.com

Index

01 Introduction

The shift to remote work has accelerated cloud adoption, and the new employee model, which embraces flexibility and mobility, has expanded the potential cyberattack surface.

In addition, in recent years, attacks have become more sophisticated and more difficult to detect. This has encouraged companies to look for more stringent cybersecurity solutions to protect their sensitive information.

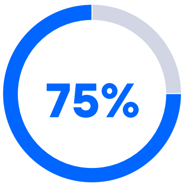
According to the Hiscox Cyber Readiness Report, 49% of Spanish companies admit to having suffered a cyberattack in 2023.[1]

The purpose of this document is to provide companies with information on the current threat landscape for digital and modern workplaces and, through Telefónica Tech's SIA Essentials service, to describe how a better security posture can help to protect your business.

[1] 22594 - Cyber Readiness Report 2023 - Spanish.pdf (hiscox.es)

02 Overview of the threat landscape

We live in an era of digitalization in which everything is interconnected and can be hacked. Cybercriminals have increasingly advanced technology, so it is essential to put emphasis on human capital, which is where attacks are mainly targeted.[2]



Of targeted cyber-attacks begin by opening an email with malicious content.

Malware, ransomware, and phishing are some of the most frequent threats.

Spain ranks as the third most cyberattacked country globally, registering up to 40,000 attacks per day.[3]

The three most common cyberattacks recorded in 2023 were DDoS attacks, financial fraud and ransomware attacks. Their main entry points have been email and instant messaging, web browsing, external storage devices, personal and corporate cell phones and social networks.[4] Attacks have also become more sophisticated and cybercriminals are always exploring new entry vectors, e.g. DDoS attacks are becoming larger and more complex and have started to target mobile networks.[5]

Most common cyberattacks in Spain in 2023

Ransomware

DDoS

Financial Fraud

Main attacks vectors

Email

Corp & Cloud Servers

Cell phones

1 in 2
organizations have been victims of a cyberattack in the last 3 years

4,35 M dollars
average cost of data breach

[2] SoSafe Compromiso de Lucas Perez Sanchez (highspot.com)
[3] ciberataques-españa-crecen-30%-2023 (cybersecuritynews.es)
[4] Los tipos de ciberataques más comunes que reciben las empresas – Sosmatic
[5] Ataques DDoS: Qué son, evolución y cómo prevenirlos y mitigarlos (computing.es)

Common Internet threats at present

Malware

Malicious software (such as ransomware) developed to damage or disrupt devices or their data (by encrypting them with a secret key) or to gain unauthorized access to a network.

Phising

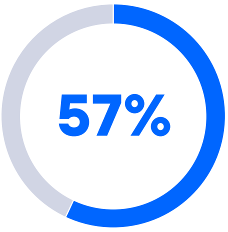
Web links in emails, SMS or other places designed to encourage watches that lead people to malicious websites where their valuable personal information can be collected. Some examples of phishing may include: Business Email Compromise (CEO Fraud) or financial fraud.

Bots maliciosos*

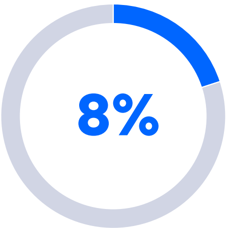
Software that is secretly installed on computers and controlled remotely. Malicious botnets find and upload valuable information, launch DDoS attacks, provide access to machines and much more.

*There are also legitimate bots that perform many repetitive tasks on the Internet

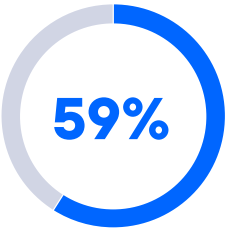
03 Business impact



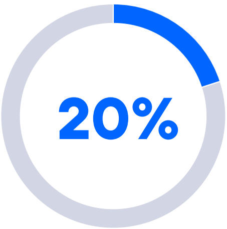
57% of small and medium-sized companies that close do so because of a cyber-attack, whether due to ransom paid, institutional sanction or loss of customer confidence.



Spanish companies lost 8% of their revenues during 2023 as a result of cyberattacks. A single cyberattack, especially one that results in a breach of customer data, will have long-term impacts on the company that suffers it.[7]



This is the average **increase paid in 2023** for ransomware in the event **of a cyber-attack**.[6]



In 2023, **20%** of spanish organizations **experienced a ransomware attack.**[8]

[6] El 57 % de las pymes que cesan su actividad en España es debido a un ciberataque – Atana

[7] España registró más de 220.000 ataques a dispositivos móviles en 2023 | Seguridad | IT Reseller

[8] El 20% de las empresas españolas ha sufrido un ataque de ransomware en 2023 | Seguridad | IT Reseller

04 SIA Essentials of Telefónica Tech

What does it do?

Telefónica Tech's service protects mobile users when accessing the Internet against security threats such as phishing or malware downloads such as ransomware.

How do I get it?

All you need to do is to contract a service compatible mobile tariff and Telefónica will activate the service automatically. [9]

How does it work?

It works by evaluating network traffic used for navigation (Domain Name System (DNS) queries) **to identify and block malicious activity.**

In addition to protecting costumers from malicious activity, administrators can manage content access policies to align with company policies for Internet content.

All of this is supported by the powerful configuration and visualization functionalities of the customer portal and without the need to download or install anything on the user´s device.

Service information

268.346.810
Total Blocked Threats (TBT)

233.903.642 (87,16%)
Blocked Access to malware websites

21.340.097 (7,95%)
Blocked bots

13.103.071 (4,88%)
Phishing websites blocked

719.022
Devices Protected

+373
Average Blocked Threats Per Device

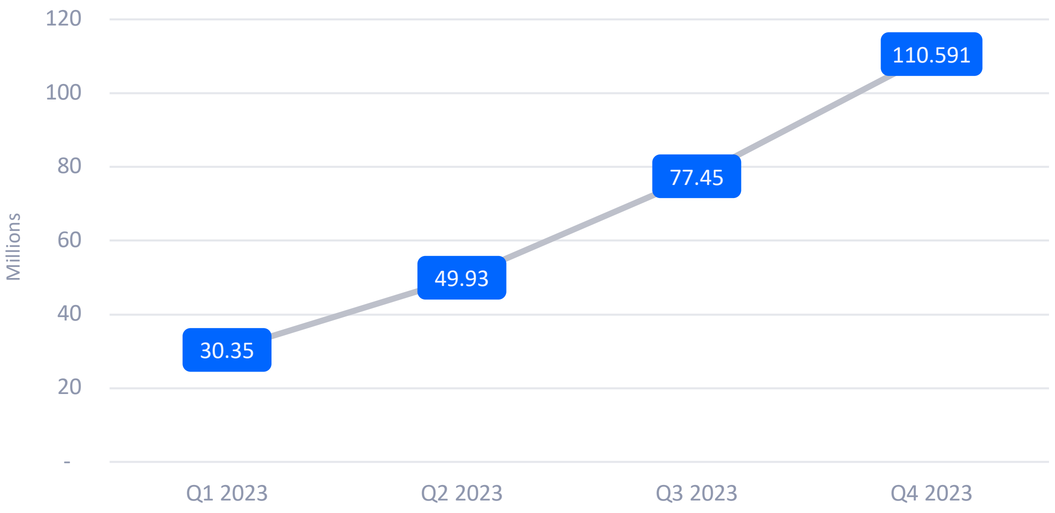
[9] To find out which tariffs are supported in Spain, ask for SRM (Seguridad en Red Móvil) - Telefonica's SIA Essentials service in Spain).

05 Trends 2023

Service evolution from Q1 to Q4 of 2023

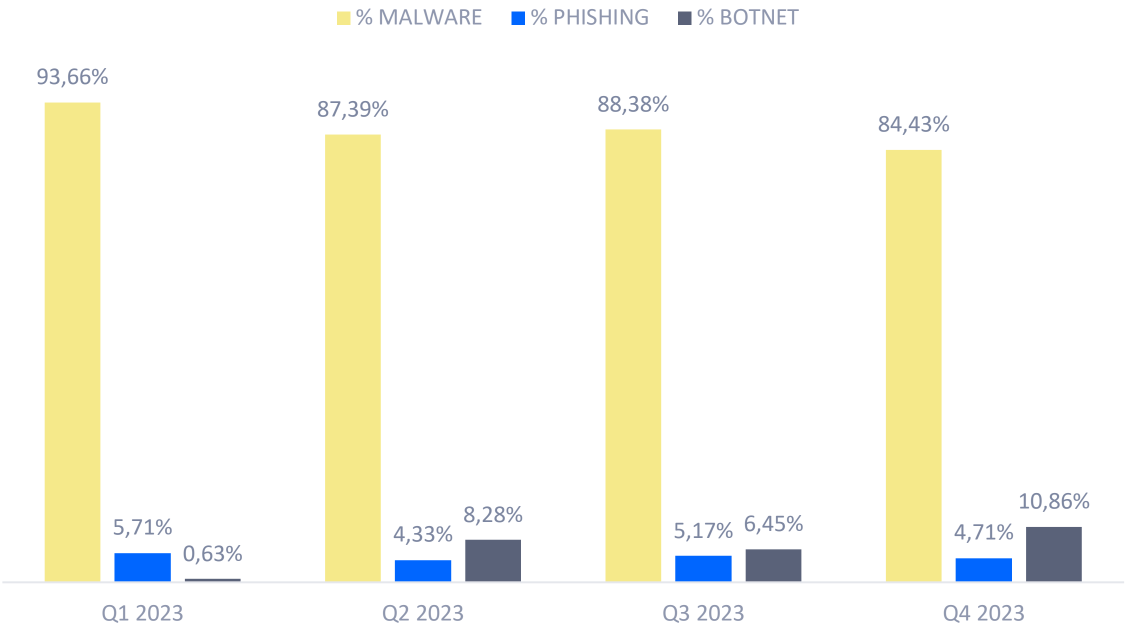
TOTAL THREATS BLOCKED IN COMPANIES (millions per quarter)

Source: TelefónicaTech/Akamai



TOTAL THREATS BLOCKED IN COMPANIES BY TYPE

Source: TelefónicaTech/Akamai



06 Conclusions

According to Allianz's latest risk barometer[10], the top global business risk for 2024 remains cyber incidents and business disruption. As cyber attacks increase in number and sophistication, companies must establish proactive cybersecurity defenses to protect assets and business continuity.

For small, medium and large companies, cyber-attacks are the number one risk as the main threat for 2024.

Specifically, ESET[11] has published a report, in which it indicates that Spain was the 3rd country with the most corporate cyber attacks in 2023.

Telefónica Tech's SIA Essentials offers companies effective cybersecurity against the most common threats, transparently and non-intrusively protecting corporate users access to email and the Internet

[10] https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf
[11] https://web-assets.esetstatic.com/wls/2023/02/eset_threat_report_t32022.pdf

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. It offers a wide range of integrated technological services and solutions in Cyber Security, Cloud, IoT, Big Data, Artificial Intelligence and Blockchain.

telefonicatech.com

Telefónica Tech