CYBER INSIGHTS AND BENCHMARK REPORT

Threat landscape analysis for Financial Industry, Retail & Commerce and Public Sector in Spain

Mastercard Advisors

September 2025

TABLE OF CONTENTS

This table of contents is interactive.
Click on any section name to link to that section. To return to this table of contents, click on "Return to Table of Contents" at the top right of any page.

1. Introduction

Return to Table of Contents

CONTEXT

The growth trend in digital activity is expected to continue. This means **cyber resilience** should be the cornerstone of organizations aiming to be competitive and stay in the game

This report delivers cybersecurity insights for Spain leveraging Mastercard's cybersecurity intelligence. It also includes an external analysis for the financial industry, retail & commerce and public sector in Spain based on publicly available information and Mastercard's risk-monitoring technology

The goal of this report is to elevate cybersecurity awareness in the explored sectors and ecosystem in Spain

OBJECTIVE

Some of the key questions addressed include:

- Who are the leading threat actors in the financial industry, retail & commerce and public sector in Spain and what are their motivations?
- What are the preferred attack methods and tools used by threat actors?
- What are the popular asset categories targeted by threat actors?
- How is the threat landscape changing over time?
- How strong is the security posture of the financial industry, retail & commerce and public sector from an external point of view?
- What are the critical areas for Spanish financial institutions, retailers, and public sector organizations to mitigate cyber threats?

By analyzing this data, companies can gain deeper insights into shifting threat actor behaviors, attack vectors, and targeted business assets, providing valuable input for enhancing their cybersecurity posture.

A deep look at the evolving cyber threat landscape, including main threat actors, attack methods, targeted assets, and important defenses to enhance

Our methodology and approach

Having built one of the world's leading global payments networks, Mastercard is powering the connected economy by building a stronger network of trust for people everywhere. We are now bringing our decades of expertise to the broader ecosystem

This report provides a view of the threat landscape for the financial industry, retail & commerce and public sector in Spain based on Mastercard's technology and cyber intelligence for the period between January 2024 and June 2025

INPUTS

Mastercard's strategic Threat Intelligence technology in **Cyber Insights integrated with Recorded Future** and **Cyber Quant***, leveraging multi-language intelligence datapoints from thousands of qualified clear, deep and dark web sources

An external analysis performed by **RiskRecon***, Mastercard's leading cyber risk monitoring technology, focusing only on publicly available and passively discovered info visible to threat actors

Exclusive internal Mastercard insights derived from anonymized **transaction decline and fraud activity**

ANALYSIS

Define the country's **threat landscape** (threat actors, attack methods and target assets) based on the threat intelligence captured and analyzed by our systems and our team of Subject Matter Experts

Validate threat intelligence data with global trends, anonymized Mastercard processed data, external assessment results and key cyber incidents recorded

OUTPUTS

Cyber Insights

- Threat Actors
- Attack Methods and TTPs
- Target Business Assets
- Target region and industry

Average maturity across critical security domains

Suggested leading security best practices for organizations

- Based on the identified threat landscape

*Refer to Section 3 for detailed information about Mastercard's cybersecurity solutions

Return to Table of Contents

We explored the potentially unique characteristics of the Spain cyber threat landscape across four topics

Regional Trends

Hypothesis
As a European country the Spain's threat landscape resembles the trends we see in Europe

Outcome
Similar to **Europe**, the top three industries targeted in Spain are **Public, Technology**, and **Financial**. The financial sector ranks first in the targeted industries togetger with technology in **Spain** in contrast to its third-place ranking across Europe.

Seasonality

Hypothesis
We expect seasonal factors to affect the cyberthreat profile

Outcome
We have noted couple surges in cyber-attacks at the beginning of 2024 September and early 2025. However, typically, cyber-attacks are seen to be triggered by events such as elections, pandemic, political tensions and global phenomena like the Olympic games or tournaments.

Domain Maturity

Hypothesis
The Spain market employs a similar level of cyber-security controls when compared to the rest of the world

Outcome
Most of the Financial companies analyzed are aligned with the industry. The domains with higher priority risks are:

- Application Security
- DNS Security
- Web Encryption
- Network Filtering

Extraordinary Events

Hypothesis
Events such as the **Ukraine-Russia / Israel-Palestine conflict,** are expected to cause a surge in cyber-attacks and possible shift in their profile.

COUNTRY OVERVIEW

- For the **past 18 months**, Spain has seen a volatile trend in cybersecurity incidents: A **total of 35,988 attacks were recorded between Jan 2024 and Jun 2025**, **averaging around 2,000 per month**. The trend was unstable, with incidents dropping to 845 in Aug 2024 and **peaking at 4,753 in May 2025**, showing a sharp escalation in 2025 across all industries
- Based on available intelligence, **a large share of incidents targeted critical infrastructure and public administration**, aligning **with the «essential» categories in the NIS2 directive**. The financial sector was repeatedly targeted, **by Black Hat attackers**. The Retail & Commerce sector was also increasingly exposed, **particularly to phishing, credential theft, and ransomware** and Public Sector targetted by **encryption ransomware and spyware.** The National Cybersecurity Strategy of Spain (2021–2025) provides the framework for these defenses. A notable event was Spain missing the October 2024 NIS2 transposition deadline.
- Spain is ranked in Tier 1* - «Role-modelling» in the Global Cybersecurity Index (GCI) 2024. While legal, technical, organizational and cooperation measures are areas of relative strength, **capacity development measures** are identified as opportunities for growth. This reflects a country's ability to build, sustain, and expand cybersecurity knowledge, skills, and infrastructure over time

INCIDENTS

In early 2024, authorities dismantled the Grandoreiro banking-trojan operation, which had heavily targeted Spanish online banking customers through email lures, overlays, and session hijacks

From 2024 into early 2025, Spain endured escalating cyber incidents including smishing, DDoS, and reconnaissance attacks on public services, strategic sites, and financial institutions, alongside ransomware and infostealer campaigns disrupting municipalities

By mid-2025, the financial sector became a primary target compated to other sectors, with groups like BlackCat, Medusa, and Lockbit driving a surge in encryption and credential-focused attacks. A June breach exposed sensitive political data, later sold via cryptocurrency transactions

STAYING AHEAD OF THREATS

In Spain, the Ministry of the Interior, the Ministry of Defense, the Ministry of Foreign Affairs, and the Department of National Security (within the Presidency of the Government) are key actors in cybersecurity governance. Operationally, the National Cybersecurity Institute (INCIBE) and the National Cryptologic Centre's CCN-CERT play central roles. CCN-CERT acts as the Government Computer Emergency Response Team for public administrations, while INCIBE manages cybersecurity for citizens and companies, including incident response through its CERT services.

Sources: Mastercard Cyber Insights Data

*The GCI classifies countries into five tiers based on their overall cybersecurity scores across five pillars, with Tier 1 being the highest. Scores are determined using publicly available data or verifiable evidence and do not reflect the quality or effectiveness of action, only whether they are in place.

Return to Table of Contents

Unveiling Sector Resilience in Spain: NIS2 (Network and Information Security 2) Directive

NIS2 is the EU-wide directive on measures for a common level of cybersecurity across the Union. It replaces the original NIS Directive (2016) and aims to harmonize cybersecurity requirements across EU Member States, expand the scope of regulated entities and strengthen risk management and incident reporting obligations. Organizations are now classified based on importance and are therefore divided into two categories, namely 'essential' and 'important' which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC. By April 17, 2025, these entities must be registered.

A directive is not a directly applicable law. Unlike a regulation (like the Cyber Resilience Act or DORA) a directive requires each member state to "transpose" it into national law

Feature	NIST2 Directive
Scope	With NIS2, the scope has expanded to include a wider variety of **essential** and **important** entities. The key criteria for their inclusion are the criticality of their industry or the services they offer, along with their size • Energy (electricity, oil, gas, heating and cooling) • Transport (air, rail, water, road) • Credit Institutions • Health • Drinking water and wastewater • Digital Infrastructure (Data centers, DNS, Trust service providers, Cloud computing service providers) • Public Administration • Space • B2B ICT Services (including MSPs, MSSPs) • Postal and courier service • Waste management • Manufacture, production and distribution of chemicals • Production, processing and distribution of food • Manufacturing • Digital providers • Research
Chapters 9 Chapters 46 Articles	What Does This Mean for Spain? ❖ Transposition deadline was 17 October 2024, but Spain is still finalizing its new Law on Cybersecurity Coordination and Governance ❖ The Ministry of the Interior, with the new National Cybersecurity Centre (CNCS), CCN, and INCIBE, are central to the rollout. Scope expands to about 12,000 entities across more sectors (e.g., public administration, transport, energy, food, space) ❖ Obligations tighten with stricter rules on governance, supply chain security, continuity, and vulnerability management ❖ Incident reporting must be faster, with shorter deadlines ❖ Executives face accountability, with boards and CISOs liable for non-compliance

COUNTRY UPDATES

- Cybersecurity in Spain is **managed through a combination of national agencies and ministries**, **with coordination being a central priority.** No single authority holds full control, and effective governance depends on collaboration across government and specialized cybersecurity bodies
- The Ministry of the Interior plays a leading role, **supported by the newly established National Cybersecurity Centre (CNCS), which is designed to centralize oversight**, incident reporting, and coordination with EU partners. Other key stakeholders include the Ministry of Economic Affairs and Digital Transformation, as well as Spain's National Cryptologic Centre (CCN) and the National Institute of Cybersecurity (INCIBE), which provide operational support, awareness campaigns, and technical expertise
- The forthcoming **Law on Cybersecurity Coordination and Governance** will serve as the legislative vehicle for implementing NIS2 in Spain

Here are some additional resources that you may find helpful:

- NIS2 Directive
- Seguridad Nacional (National Security Department)
- National Institute of Cybersecurity (INCIBE)

Return to Table of Contents

Unveiling Sector Resilience in Spain: Esquema Nacional de Seguridad Espanol

The ENS is Spain's National Security Framework for information systems. It sets mandatory rules for public administrations and the private companies that provide them with digital services. Its goal is to ensure that electronic services remain confidential, available, and trustworthy, while promoting a consistent level of cybersecurity across the country.

Feature	Esquema Nacional de Seguridad Espanol
Legal Basis	With Royal Decree 311/2022, the ENS was updated to strengthen Spain's cybersecurity model. It establishes a common approach to protect public sector systems and requires suppliers to meet the same standards.
Scope	Entire Public Sector, plus private-sector providers under contract to public entities; systems handling classified information as required
Security Dimensions	❖ Confidentiality, ❖ Integrity, ❖ Availability ❖ Authenticity ❖ Traceability
Minimum Requirements	❖ Clear governance and security policies ❖ Risk analysis and secure configuration ❖ Access control and user identification ❖ Data protection in storage and transit ❖ Monitoring, logging, and incident response ❖ Continuity of operations and supply chain security ❖ Training and accountability of staff

COUNTRY UPDATES

- Cybersecurity under the **ENS is coordinated by the Centro Criptológico Nacional (CCN)**, which develops the framework, issues guidance, and oversees certification and audits for compliance
- The **Ministry of the Interior and other ministries work alongside the CCN** to ensure that public administrations and their technology providers meet ENS obligations
- The **National Institute of Cybersecurity (INCIBE) provides awareness, training, and technical assistance** to support organizations in applying ENS requirements
- ENS compliance is seen as a foundation for **Spain's broader digital trust strategy**, ensuring that critical services delivered by government and suppliers remain secure, reliable, and resilient

Here are some additional resources that you may find helpful:

- ENS
- Royal Decree 311/2022 of 3 May regulating the National Security Framework

Return to Table of Contents

CONTEXT & KEY CONCLUSIONS:

With sophisticated cyber threats on the rise, Spain's digital economy is facing growing risks. Mastercard Advisors produced this report to deliver a cybersecurity assessment of Spanish Public sector between January 2024 and June 2025. It utilizes Mastercard's proprietary threat intelligence platforms (Cyber Insights, Cyber Quant, and RiskRecon) to provide a data-driven view of the most active threat actors, attack methods, and targeted assets in the region.

Who Are the Attackers?
The most active threat actors in Spain include:

ShinyHunters: A financially motivated hacking group known for stealing large datasets from companies and selling them on dark web forums
Natohub: A threat actor that focuses on defacing websites and leaking data from Western military, government, and political targets
UNC5537: A financially motivated threat actor known for breaching Snowflake customer environments using stolen credentials for extortion or resale
IntelBroker: A blackhat hacker known for leaking sensitive information from government and corporate entities by exploiting vulnerabilities

These actors are not amateurs or "script kiddies." They are highly capable, well-resourced, and often state-sponsored or ideologically driven. Their presence in Spain's cyber landscape signals a serious and persistent threat that demands robust and proactive cybersecurity controls.

Source: Mastercard Cyber Insights, Cyber Quant and RiskRecon Data. Based on data for the period Jan 2024 – June 2025

Return to Table of Contents

CONTEXT & KEY CONCLUSIONS:

What Do They Do?
The most common attack methods observed include:

Malware: Malware remains the top attack method, persistently targeting business systems, customer personal information, and intellectual property. Its widespread use underscores its effectiveness in enabling broader campaigns.
Ransomware: Ransomware attacks surged in Q2 2025, showing a trend toward extortion-based campaigns. Targets include business systems, customer financial information, and intellectual property.
Email Phishing: Email phishing also increased in Q2 2025, with more sophisticated campaigns targeting business systems, customer and financial personal information. Phishing often serves as the entry point for more advanced threats like ransomware or credential theft.

Given that these attacks are being carried out by **Black Hat** and **Cyber Warrior** threat actors, the threat level is high. These are not opportunistic or random attacks—they are strategic, calculated, and capable of causing significant disruption and damage.

What's Being Targeted?
The most frequently targeted assets include:

Business Systems: Including core systems, cloud systems, and operational platforms, often targeted to disrupt services, steal data, or enable deeper access into organizational networks.
Customer Personal and Financial Information: Such as credentials, identity information, payment cards, and cryptocurrency wallets. This information is commonly exploited for fraud, financial theft, or broader compromise.

This pattern of targeting confirms the hypothesis that attackers are not only after data but also aim to disrupt physical operations and critical infrastructure. It reinforces the need for Spain institutions to take cybersecurity seriously and implement solid, layered defenses.

Source: Mastercard Cyber Insights, Cyber Quant and RiskRecon Data. Based on data for the period Jan 2024 – June 2025

Return to Table of Contents

CONTEXT & KEY CONCLUSIONS:

With sophisticated cyber threats on the rise, Spain's digital economy is facing growing risks. Mastercard Advisors produced this report to deliver a cybersecurity assessment of Spanish Retail & Commerce sector between January 2024 and June 2025. It utilizes Mastercard's proprietary threat intelligence platforms (Cyber Insights, Cyber Quant, and RiskRecon) to provide a data-driven view of the most active threat actors, attack methods, and targeted assets in the region.

Who Are the Attackers?
The most active threat actors in Spain include:

ShinyHunters: A financially motivated hacking group known for stealing large datasets from companies and selling them on dark web forums
UNC5537: A financially motivated threat actor known for breaching Snowflake customer environments using stolen credentials for extortion or resale
Storm-0844: A group known for deploying Akira ransomware, likely gains access through valid accounts and uses readily available tools for discovery, lateral movement, and data exfiltration before deployment
IntelBroker: A blackhat hacker known for leaking sensitive information from government and corporate entities by exploiting vulnerabilities

These actors are not amateurs or "script kiddies." They are highly capable, well-resourced, and often state-sponsored or ideologically driven. Their presence in Spain's cyber landscape signals a serious and persistent threat that demands robust and proactive cybersecurity controls.

Source: Mastercard Cyber Insights, Cyber Quant and RiskRecon Data. Based on data for the period Jan 2024 – June 2025

Return to Table of Contents

CONTEXT & KEY CONCLUSIONS:

What Do They Do?
The most common attack methods observed include:

Malware: Malware is the top attack method, targeting business systems, customer personal and financial information.
Ransomware: Ransomware attacks surged in Q2 2025, focusing on business systems, customer financial information, and legal documents in extortion-driven campaigns.
Email Phishing: Email phishing peaked in Q1 2025, with increasingly sophisticated campaigns targeting business systems as well as customer and financial personal information. Phishing often acts as a gateway to more advanced threats such as ransomware and credential theft.

Given that these attacks are being carried out by **Black Hat** and **Cyber Warrior** threat actors, the threat level is high. These are not opportunistic or random attacks—they are strategic, calculated, and capable of causing significant disruption and damage.

What's Being Targeted?
The most frequently targeted assets include:

Business Systems: Including core systems, AI systems, and operational platforms, often targeted to disrupt services, steal data, or enable deeper access into organizational networks.
Customer Personal and Financial Information: Such as credentials, identity information, cryptocurrency wallets, payment and credit cards. This information is commonly exploited for fraud, financial theft, or broader compromise.

This pattern of targeting confirms the hypothesis that attackers are not only after data but also aim to disrupt physical operations and critical infrastructure. It reinforces the need for Spain institutions to take cybersecurity seriously and implement solid, layered defenses.

Source: Mastercard Cyber Insights, Cyber Quant and RiskRecon Data. Based on data for the period Jan 2024 – June 2025

Return to Table of Contents

CONTEXT & KEY CONCLUSIONS:

With cyber incidents steadily increasing, Spain's financial sector has emerged as one of the most targeted industries between January 2024 and June 2025. Mastercard Advisors produced this report to provide a data-driven view of the key threat actors, attack methods, and targeted assets in Spain's financial industry, leveraging proprietary platforms (Cyber Insights, Cyber Quant, and RiskRecon)

Who Are the Attackers?
The most active threat actors in Spain's financial sector include:

BlackCat: A ransomware group executing large-scale encryption campaigns, heavily involved in financial data extortion
Lockbit: A persistent ransomware operator targeting core financial services and infrastructure
RansomEXX Group: Responsible for 17% of ransomware-linked incidents, conducting aggressive extortion-based attacks
Scattered Spider: Driving 97% of phishing activities, specializing in stealing credentials for deeper compromise
Additional groups: Including Phobos (6%), Punk Spider (16%), and Evil Corp (8%), each contributing to the ransomware landscape

These actors are not opportunistic attackers. They are organized, well-resourced, and in many cases linked to transnational cybercrime networks. Their continued targeting of Spain's financial ecosystem demonstrates the urgent need for robust, layered cybersecurity defenses

Source: Mastercard Cyber Insights, Cyber Quant and RiskRecon Data. Based on data for the period Jan 2024 – June 2025

Return to Table of Contents

CONTEXT & KEY CONCLUSIONS:

What Do They Do?
The most common attack methods observed in Spain's financial sector include:

Encryption Ransomware: Activity peaked in Q1 and Q2 2025, driven by groups such as BlackCat, Akira, and Lockbit. These campaigns typically encrypted business-critical systems and demanded ransom payments in exchange for decryption keys. The disruptions extended to banking operations, and customer-facing services, significantly impacting financial stability and consumer trust

Infostealer Malware: Gained prominence from late 2024 onward, with the majority of attacks attributed to Lumma. This malware focused on harvesting customer credentials and personal identification information, which were then used for fraud, account takeovers, or resale on underground markets. Its persistence demonstrates attackers' interest in long-term exploitation of sensitive data

Phishing & Credential Theft: Dominated by Scattered Spider, responsible for 97% of phishing activity. These campaigns used social engineering emails, SMS lures, and spoofed login portals to capture access credentials. Often, phishing served as the initial entry vector for larger attacks, including ransomware deployments and account-draining fraud

What's Being Targeted?
The most frequently targeted assets in Spain's financial sector include:

Business Systems & Operations: Cloud platforms, payment systems, and core banking infrastructure, often disrupted to extort or steal

Customer Financial Data: Identity information, credentials, and payment card details exploited for fraud or resale

AI & Core Systems: Increasingly leveraged as entry points, representing a growing risk for future attacks

This pattern of targeting confirms the hypothesis that attackers are not only after data but also aim to disrupt physical operations and critical infrastructure. It reinforces the need for Spain institutions to take cybersecurity seriously and implement solid, layered defenses

Source: Mastercard Cyber Insights, Cyber Quant and RiskRecon Data. Based on data for the period Jan 2024 – June 2025

2. Cyber Insights

Powered by

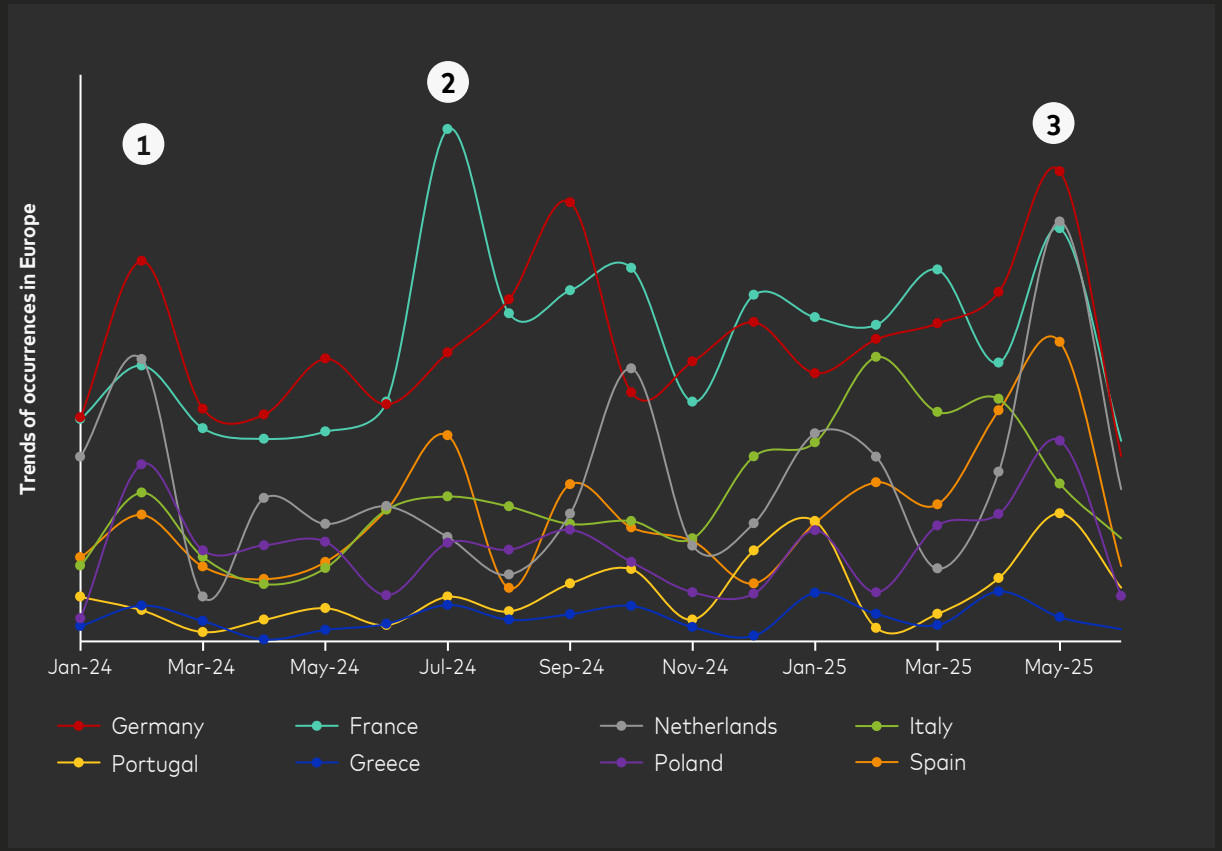
CYBERQUANT mastercard

CYBERINSIGHTS mastercard

riskrecon mastercard

Return to Table of Contents

France is the most targeted European country, hit by highest number of cyber events, while Spain ranks fifth



KEY INSIGHTS

1. In February 2024, Germany experienced several ransomware incidents, including attacks on PSI Software, the Hessen Consumer Center, and German political parties. Additionally, the Black Basta ransomware group claimed responsibility for a data breach impacting Germany

2. France reported over 140 cyberattacks during the 2024 Olympics, targeting government, transport, telecom and sports sectors, including denial-of-service attacks and data compromises. In parallel, a ransomware strike targeted the Grand Palais and about 40 affiliated museums, though crucial Olympic systems remained unaffected

3. The increase in threat activity in May 2025 was driven by a combination of factors. State-sponsored cyberattacks targeted NATO and EU allies focusing on defense and tech sectors. At the same time, a wave of ransomware and supply chain attacks hit critical industries across Europe

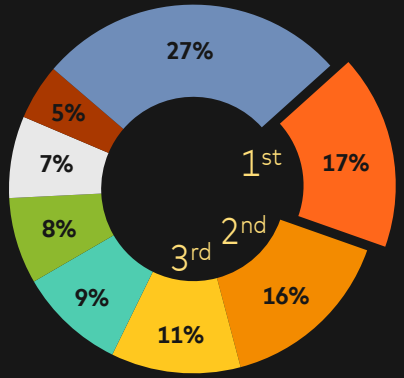
Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 - June 2025

Return to Table of Contents

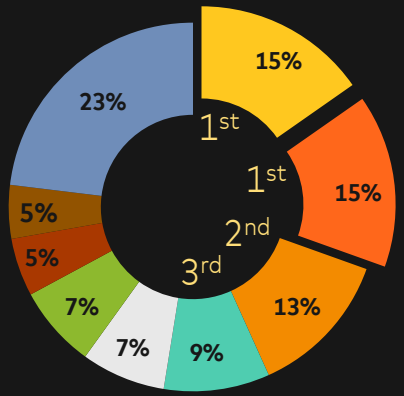
Across the entire European region, as well as in Spain, the public industry is the second most targeted sector in all cyber incidents

Events per Industry

Europe



Spain



Technology
Public
Financial
Media
Services
Industrial
Research
Communication
Other

***Industries below 5% are grouped together with the «Other» category**

- *Retail, Education, Healthcare, Communication, Energy*

Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 - Junel 2025

Most popular Assets, Actors and Methods

Assets

27%

of events targeting **Business Systems**

Europe average: 29%

Actors

42%

of events were attributed to **Black Hat**

Europe average: 31%

Methods

38%

of attacks were performed through **Malware and Ransomware**

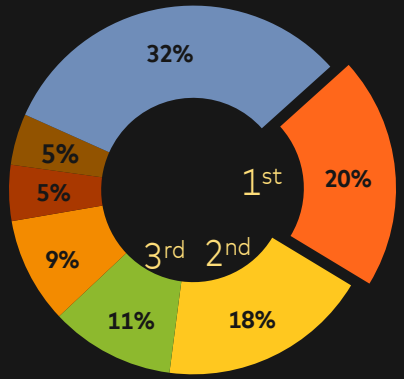
Europe average: 39%

Return to Table of Contents

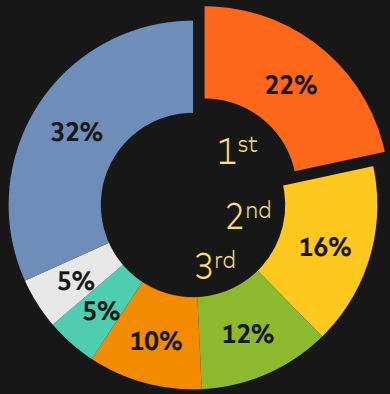
Malware, ransomware and email phishing are the top three attack methods in both Europe and Spain, appearing in the same order

Attack Methods – All Industries

Europe



Spain



Malware
Ransomware
Reconnaissance
Email Phishing
Legitimate Tool
Command & Control
Denial of Service
Pretexting
Other

***TTP below 5% are grouped together with the «Other» category**

- *Supply Chain Attack, Pretexting, Credential Access, Denial of Service, Command & Control, Legitimate Tool, Persistence*

Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 - June 2025

Most common Tactics, Techniques, and Procedures

Malware

38%

of events mostly targeting **Software Companies, Government Agencies** and **Construction and Engineering**

Europe average: 45%

Ransomware

30%

of events mostly targeting **Software Companies, Government Agencies** and **Healthcare Providers and Services**

Europe average: 41%

Email Phishing

35%

of events mostly targeting **Software Companies, Government Agencies** and **Construction and Engineering**

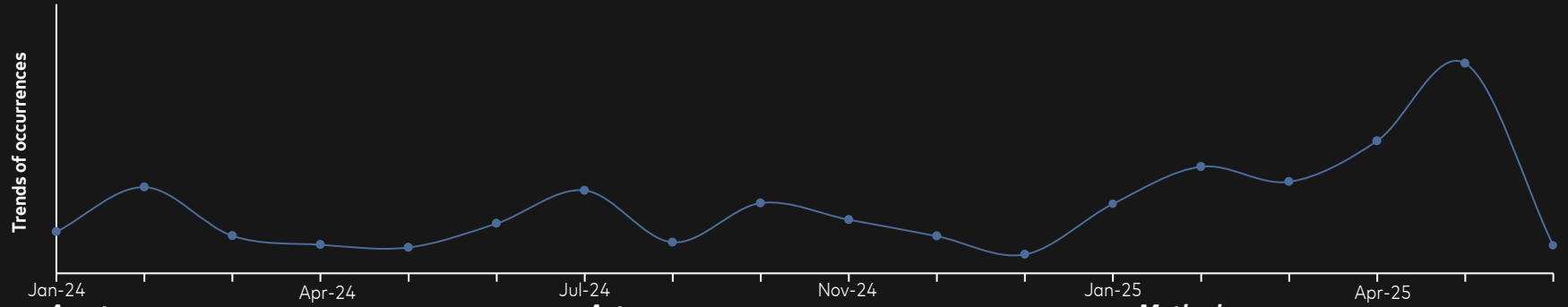
Europe average: 46%

Return to Table of Contents

Public sector in Spain was targeted the most across the second quarter of 2025

Events per Public sector in Spain

Spain



Assets

44%

of events targeting **Business System** or **Customer Personal Information**

European average: 41%

Actors

40%

of events were attributed to **Black Hat**

European average: 26%

Methods

38%

of attacks were performed through **Malware** or **Ransomware**

European average: 40%

Examples:

- *Business operations*
- *Identity information*
- *Cloud systems*
- *Core systems*

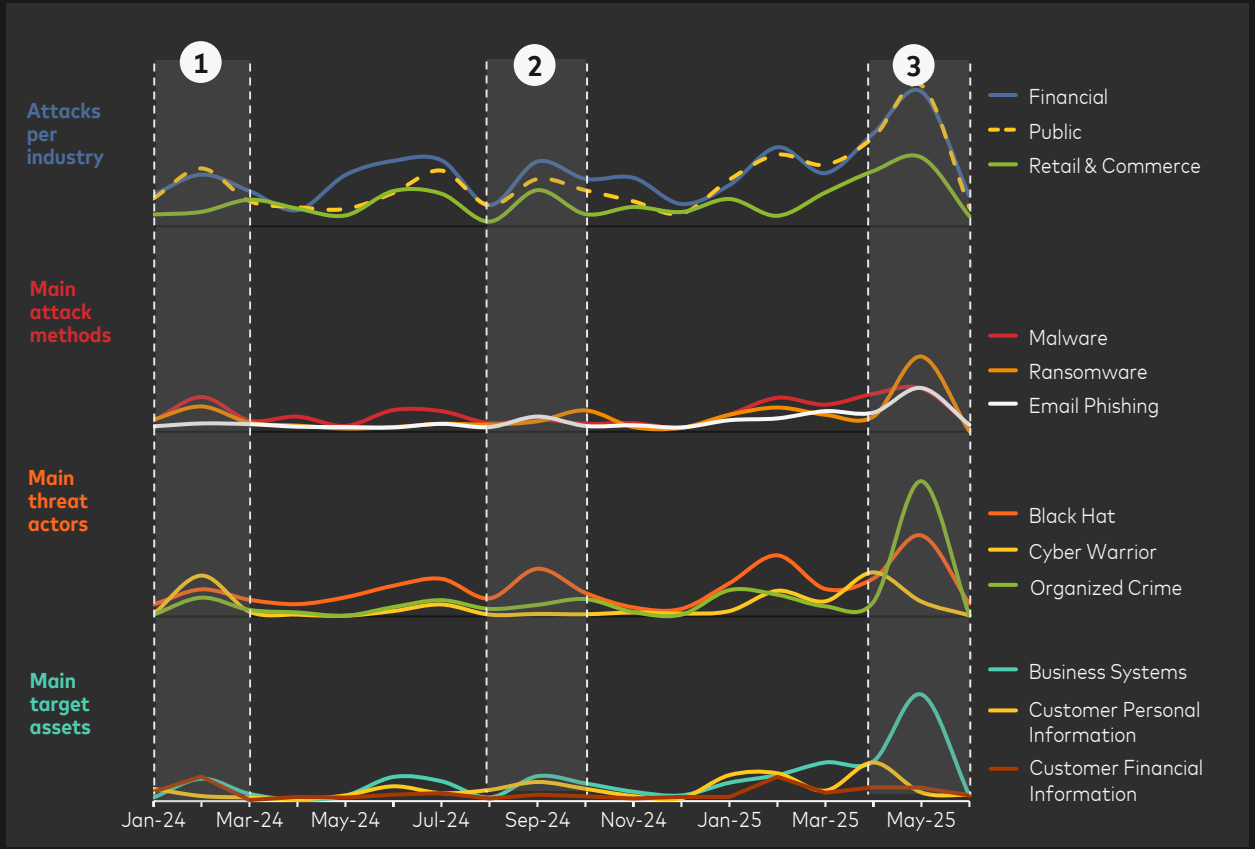
- *ShinyHunters*
- *Natohub*
- *UNC5537*
- *IntelBroker*

- *Lockbit (Encryption ransomware)*
- *Pegasus spyware (Spyware)*
- *BlackCat (Encryption ransomware)*

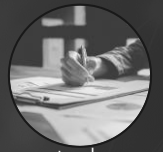
Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 - June 2025
* Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list Please find details in appendix.

Return to Table of Contents

Public sector in Spain saw 3 important peaks in number of cyber events during this period



KEY INSIGHTS



1. A spate of cyberattacks targeted municipalities in Spain, causing service disruptions and while recovery efforts were under way, authorities mobilized cybersecurity specialists and national agencies to contain the damage[1]

2. Europol and law enforcement agencies dismantled the iServer phishing-as-a-service platform responsible for ensnaring nearly 483,000 victims and arrested 17 suspects, including the administrator behind the five-year operation[2]

3. Spain's Interior Ministry has confirmed a cyberattack in June 2025 involving the theft and leak of personal data belonging to high-ranking political figures. The stolen data was sold online, with transactions carried out in cryptocurrency to avoid detection[3]

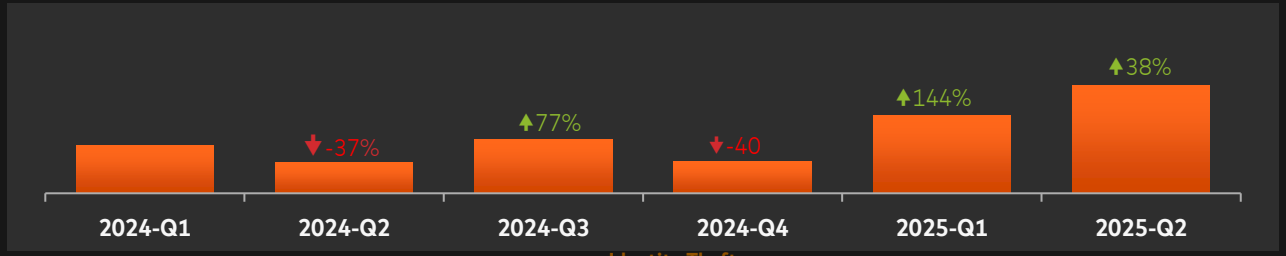
[1]THE RECORD [2]EUROPOL [3]POLICIA.ES

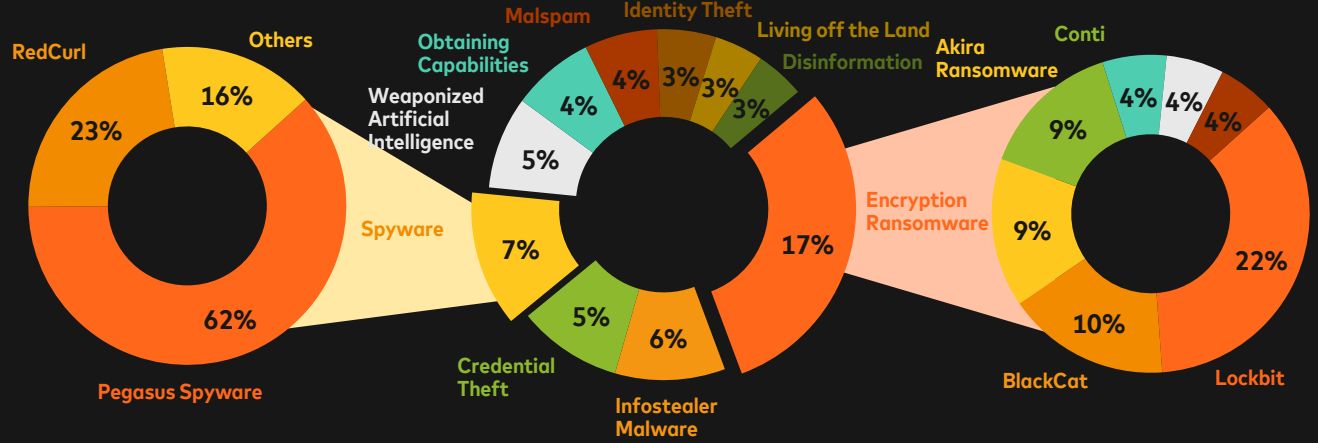
Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025

21% of cyber events targeting the Public sector in Spain leveraged **Malware** attack methods

Events per attributed TTP

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

Return to Table of Contents

KEY INSIGHTS

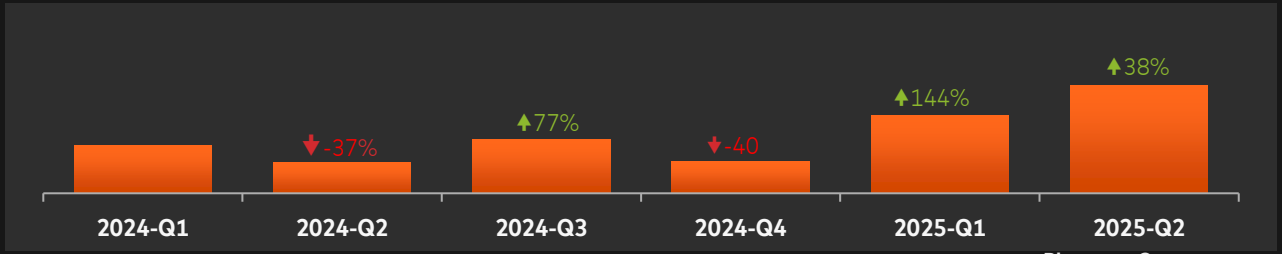
- **Cyber-attacks** occurrences have varied quarterly, especially between 2024 Q4 and 2025 Q1 periods, a significant increase of %144 has been observed
- Since Q1 2024, the top three most used TTPs in Spain have shown some variations each quarter. While certain threats like **Malware** and **Email Phishing** have persisted, it is notable that new threats, such as **Ransomware** and **Reconnaissance**, have emerged in the latest quarter
- Based on our analysis, it was found that **7%** of the utilized methods were linked to **Spyware**, which can be attributed to the **Pegasus Spyware** while the **Encryption Ransomware** attacks are attributed to **Lockbit**

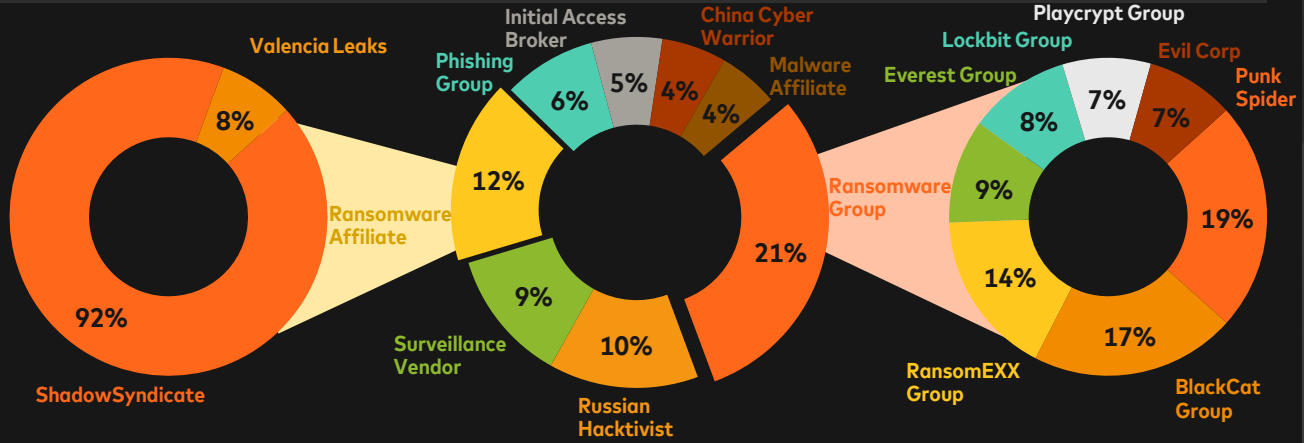
Return to Table of Contents

40% of cyber events targeting the Public sector in Spain were attributed to **Black Hat**

Events per attributed Actor

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

KEY INSIGHTS

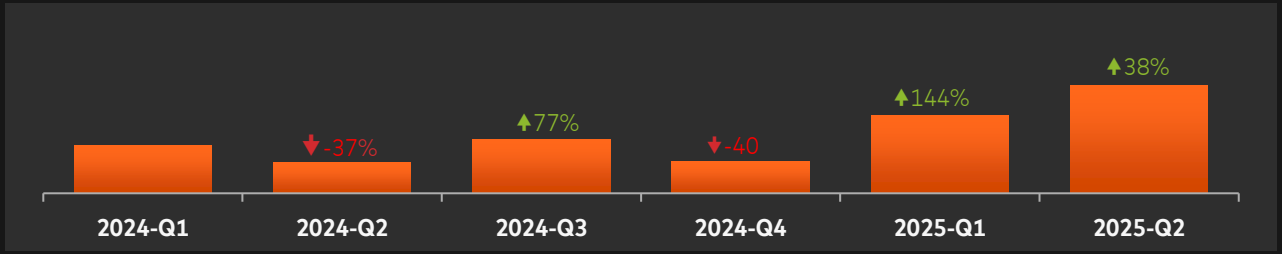
- **Black Hat** and **Organized Crime** actors were observed in over **60%** of total attack occurrences from the beginning of 2024 until the end of June 2025
- Since the first quarter of 2024, **Black Hat** and **Organized Crime** have been prominent as leading threat actors in Spain. However, as of **Q2 2024**, **State Sponsored** and **Cyber Warrior** actors are also emerging
- According to our analysis, **24%** of **Ransomware Group** activities can be attributed to the **Punk Spider** and **BlackCat** groups. Moreover **92%** of **Ransomware Affiliate Actors** can be attributed to the **ShadowSyndicate**

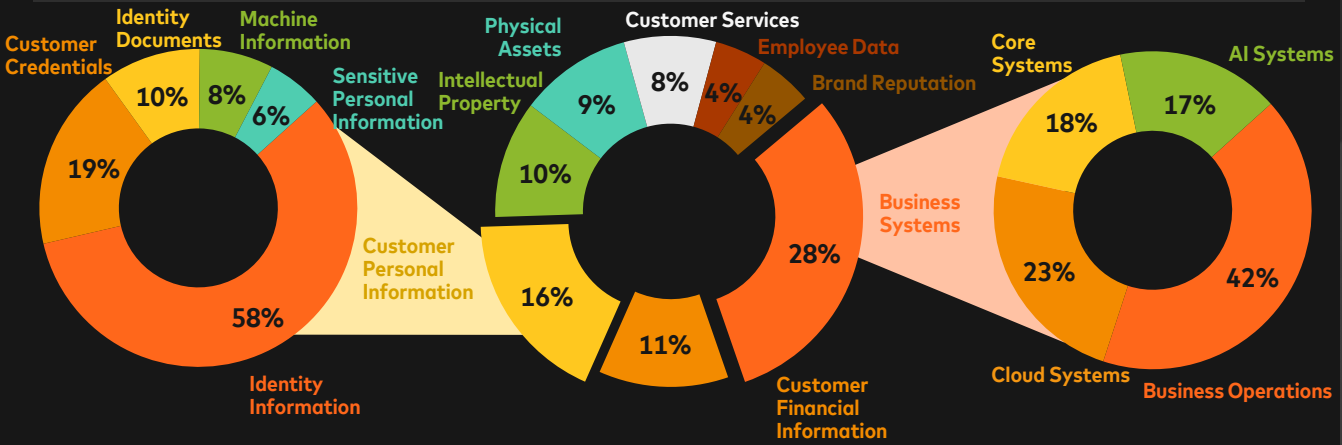
Return to Table of Contents

28% of cyber events targeting the Public sector in Spain focused on **Business Systems**

Events per targeted Asset

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

KEY INSIGHTS

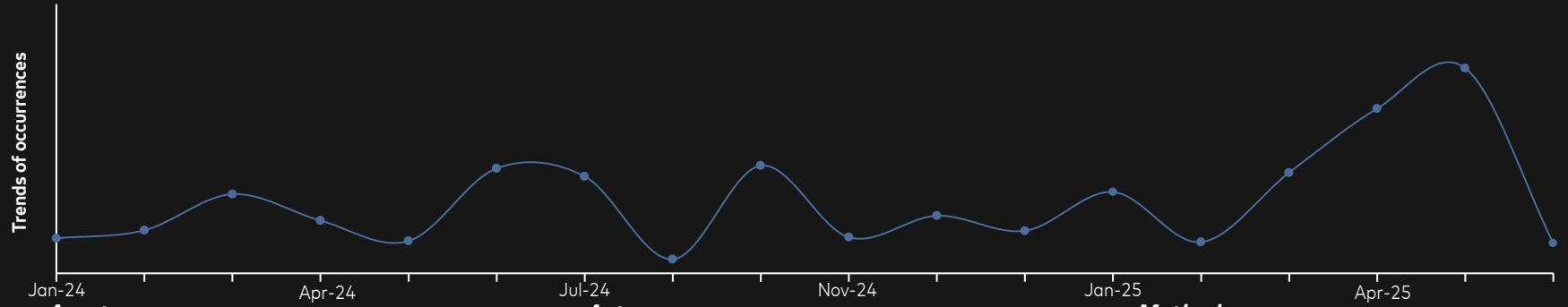
- **Customer Personal Information** and **Business Systems** were observed in **40%** of total attack occurrences
- Since Q1 2024, **Business System** and **Customer Personal Information** have been among the most targeted assets in Spain. However, as of Q2 2025, **Intellectual Property** has also emerged as a prominent target
- Our analysis indicates that **Business Operations** were among the most targeted assets for Business Systems. Regarding Customer Personal Information **Identity Information** ranked the most targeted asset within the timeframe in Spain

Return to Table of Contents

Retail & Commerce sector in Spain was targeted the most across the second quarter of 2025

Events per Retail & Commerce sector in Spain

Spain



Assets

43%

of events targeting **Business System** or **Customer Personal Information**

European average: 44%

Actors

41%

of events were attributed to **Black Hat**

European average: 36%

Methods

37%

of attacks were performed through **Malware** or **Ransomware**

European average: 41%

Examples:

- *Business operations*
- *Cloud systems*
- *Identity information*
- *AI systems*

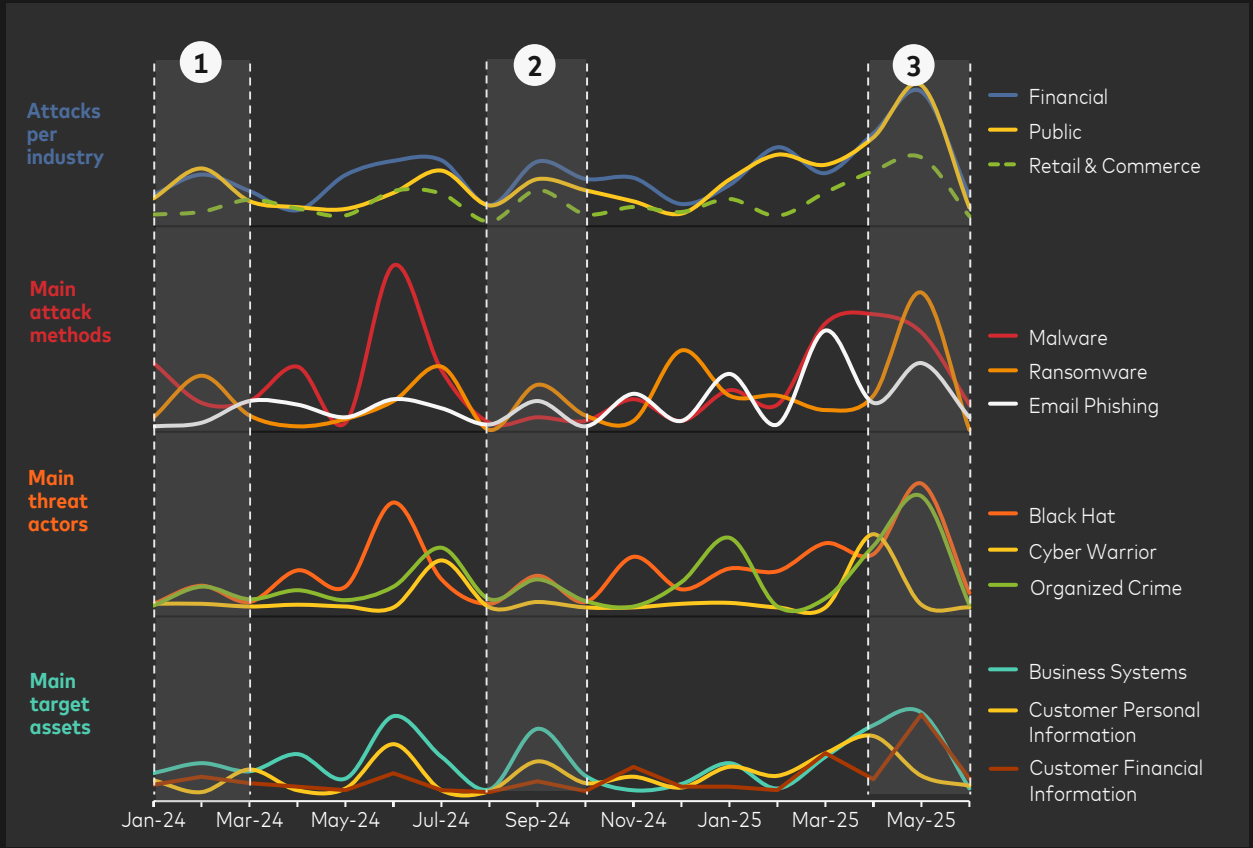
- *ShinyHunters*
- *UNC5537*
- *Storm-0844*
- *IntelBroker*

- *BlackCat (Encryption ransomware)*
- *DragonForce Ransomware (Encryption ransomware)*
- *8Base (Encryption ransomware)*

Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 - June 2025
* Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list Please find details in appendix.

Return to Table of Contents

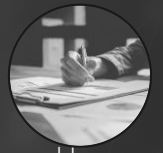
Retail & Commerce sector in Spain saw 3 important peaks in number of cyber events during this period



[1]THE RECORD [2]KASPERSKY [3]THE RECORD

Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025

KEY INSIGHTS



1. Orange España suffered a roughly three-hour internet outage after a hacker hijacked its RIPE account using easily compromised credentials and caused significant traffic loss before services were restored and no customer data was compromised[1]

2. A malware campaign active since mid-September used fake CAPTCHA prompts on ad-heavy websites to trick users into downloading infostealing software. Victims across several countries had sensitive browser data and cryptocurrency wallets targeted[2]

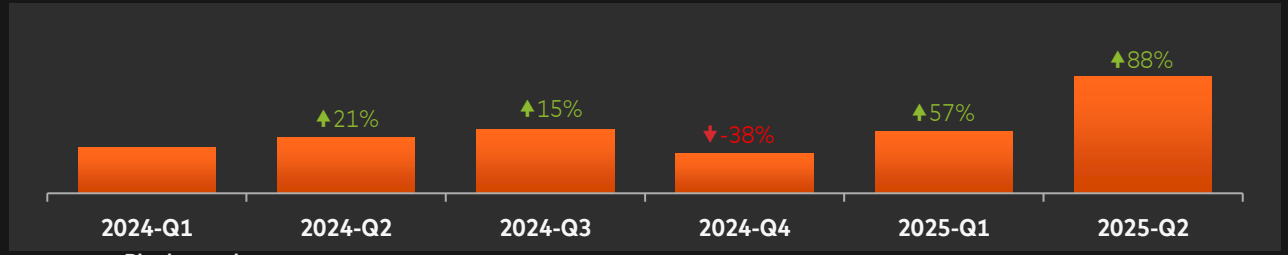
3. In April 2025, hackers exploited a Microsoft zero-day vulnerability in the Windows Common Log File System driver to carry out ransomware attacks using PipeMagic malware against organizations[3]

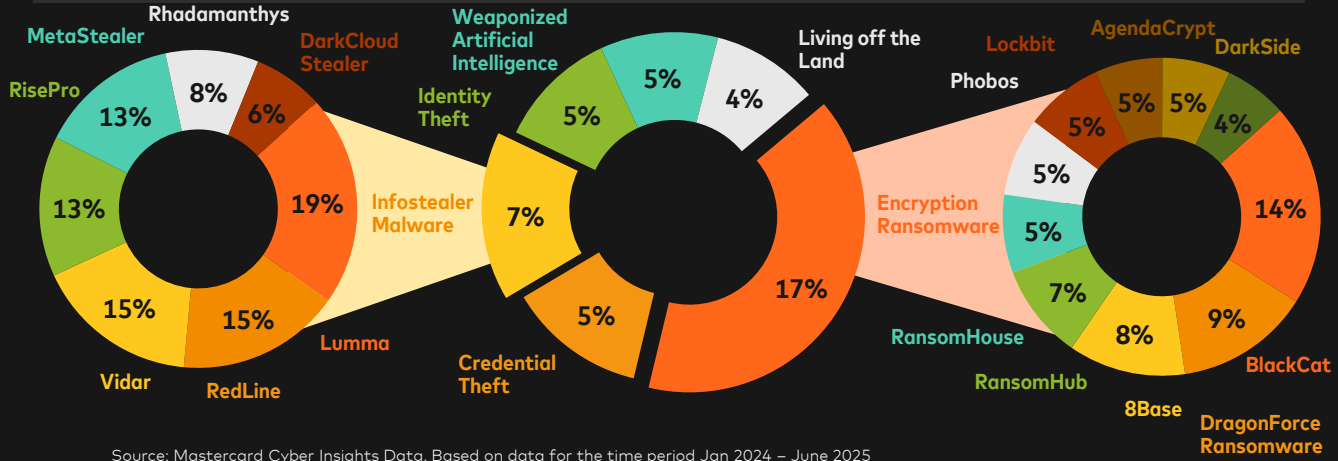
Return to Table of Contents

22% of cyber events targeting the Retail & Commerce sector in Spain leveraged **Malware** attack methods

Events per attributed TTP

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

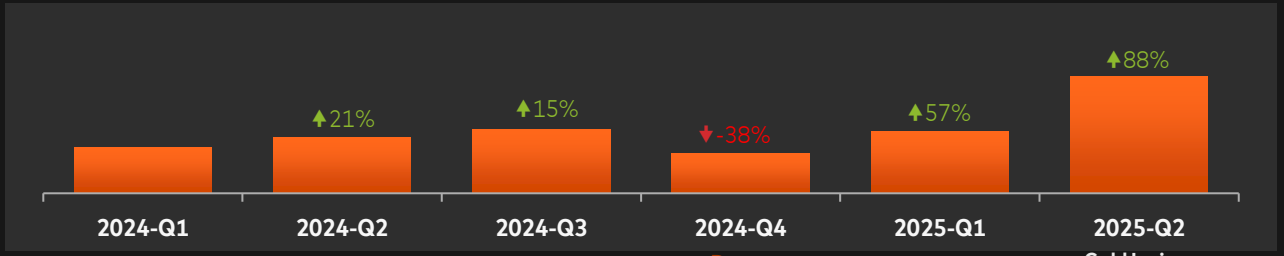
KEY INSIGHTS

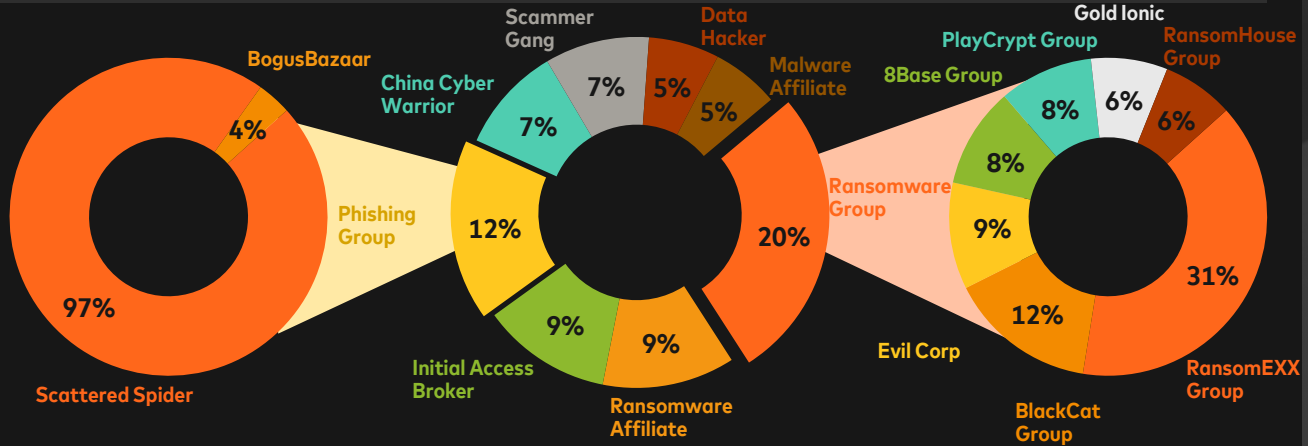
- **Cyber-attacks** occurrences have varied quarterly, especially between 2025 Q1 and 2025 Q2 periods, a significant increase of %88 has been observed
- Since Q1 2024, the top three most used TTPs in Spain have shown some variations each quarter. While certain threats like **Malware** has persisted, it is notable that new threats, such as **Ransomware** and **Reconnaissance**, have emerged in the latest quarter
- Based on our analysis, it was found that **17%** of the utilized methods were linked to **Encryption Ransomware**, which can be attributed to the **BlackCat** group while the **Infostealer Malware** attacks are attributed to **Lumma**

41% of cyber events targeting the Retail & Commerce sector in Spain were attributed to **Black Hat**

Events per attributed Actor

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

Return to Table of Contents

KEY INSIGHTS

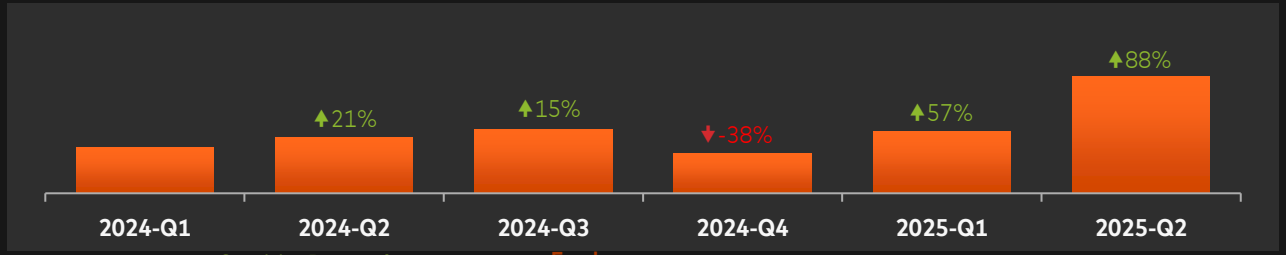
- **Black Hat** and **Organized Crime** actors were observed in over **70%** of total attack occurrences from the beginning of 2024 until the end of June 2025
- Since the first quarter of 2024, **Black Hat** and **Organized Crime** have been prominent as leading threat actors in Spain. However, as of **Q3 2024**, **Cyber Warrior** actors are also emerging
- According to our analysis, **31%** of **Ransomware Group** activities can be attributed to the **RansomEXX Group**. Moreover **97%** of **Phishing Group** activities can be attributed to **Scattered Spider**

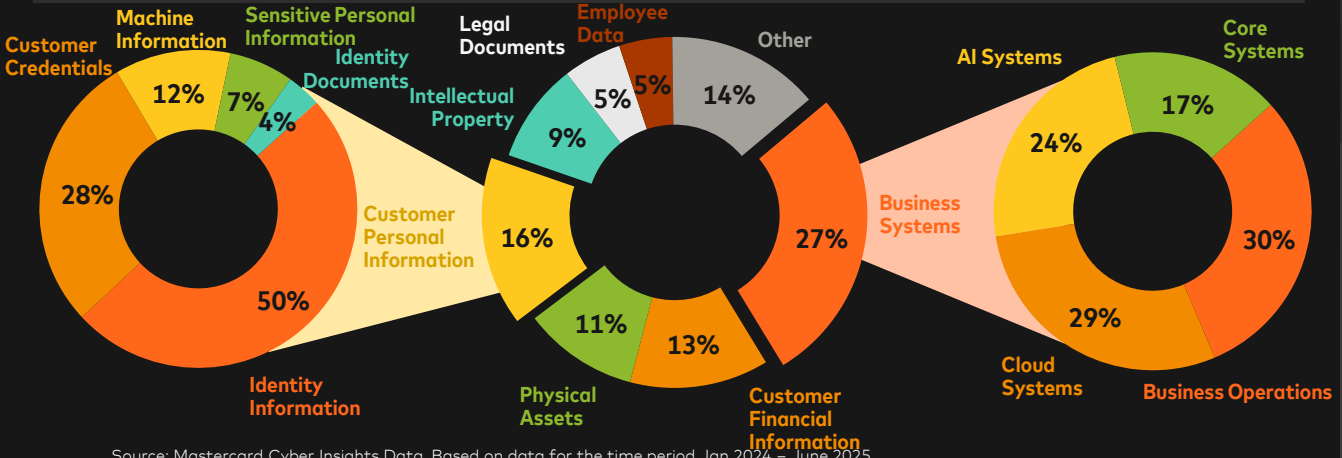
Return to Table of Contents

27% of cyber events targeting Retail & Commerce sector in Spain focused on **Business Systems**

Events per targeted Asset

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

KEY INSIGHTS

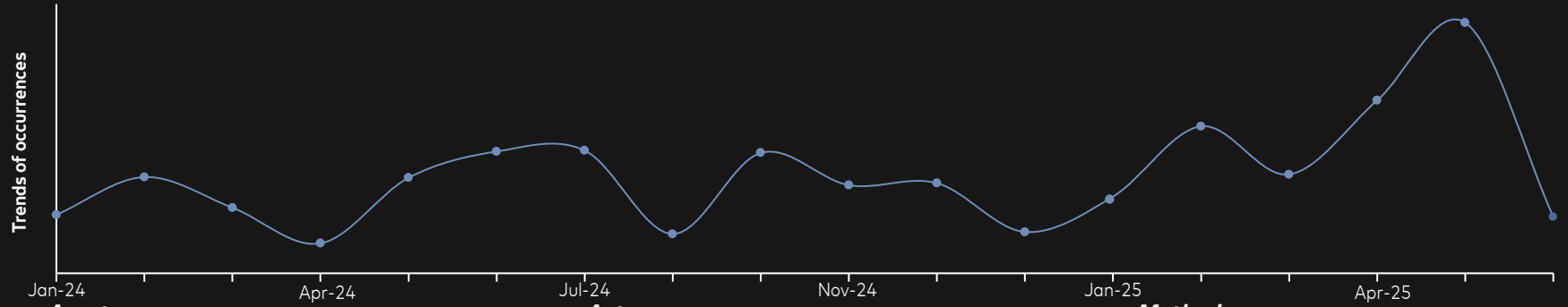
- **Customer Personal Information** and **Business Systems** were observed in **43%** of total attack occurrences
- Since Q1 2024, **Business Systems** have been among the most targeted assets in Spain. However, as of Q2 2024, **Customer Financial Information** and **Intellectual Propert** have also emerged as prominent targets
- Our analysis indicates that **Business Operations** were among the most targeted assets for Business Systems. Regarding Customer Personal Information **Identity Information** ranked the most targeted asset within the timeframe in Spain

Return to Table of Contents

Financial sector in Spain was targeted the most across the second quarter of 2025

Events per Financial sector in Spain

Spain



Assets

41%

of events targeting **Business System** or **Customer Financial Information**

European average: 39%

Actors

46%

of events were attributed to **Black Hat**

European average: 39%

Methods

37%

of attacks were performed through **Malware** or **Ransomware**

European average: 40%

Examples:

- *Business operations*
- *Cloud systems*
- *Payment Cards*
- *AI systems*

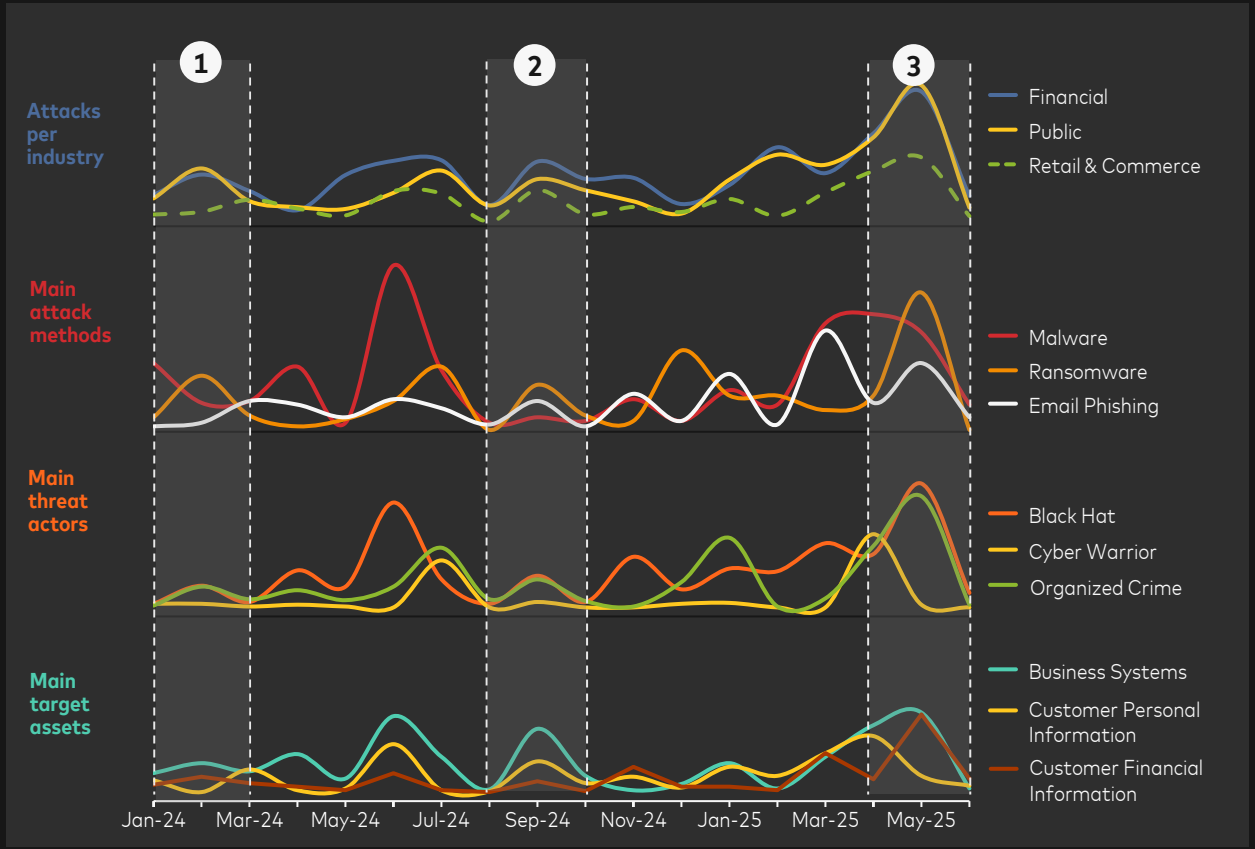
- *ShinyHunters*
- *Wazawaka*
- *UNC5537*
- *IntelBroker*
- *Odyssey Spider*

- *Lockbit (Encryption ransomware)*
- *Lumma (Infostealer)*
- *Grandoreiro (Banking Trojan)*

Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 - June 2025
* Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list Please find details in appendix.

Return to Table of Contents

Financial sector in Spain saw 3 important peaks in number of cyber events during this period



[1] INTERPOL [2] OCU.ORG [3] INFO-VERITAS

Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025

KEY INSIGHTS

1. The grandoreiro banking-trojan crackdown happened during January and March 2024, the police in Brazil with support from Spain & INTERPOL dismantled the Grandoreiro operation that had heavily targeted Spanish online-banking customers via email lures, overlays and session hijack [1]

2. Consumer watchdog OCU and ING warned its clients of a SMS campaign "nuevo dispositivo" aimed at credential theft and draining accounts in September 2024. This Smishing campaing aimed at account-takeover attempts [2]

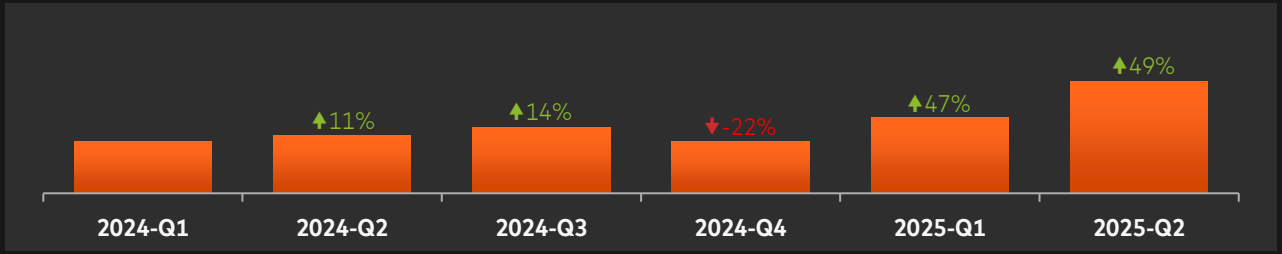
3. In early March, Spain suffered a sharp rise in DDoS against public/strategic sites and smishing attacks. A bank targetted was CaixaBank [3]

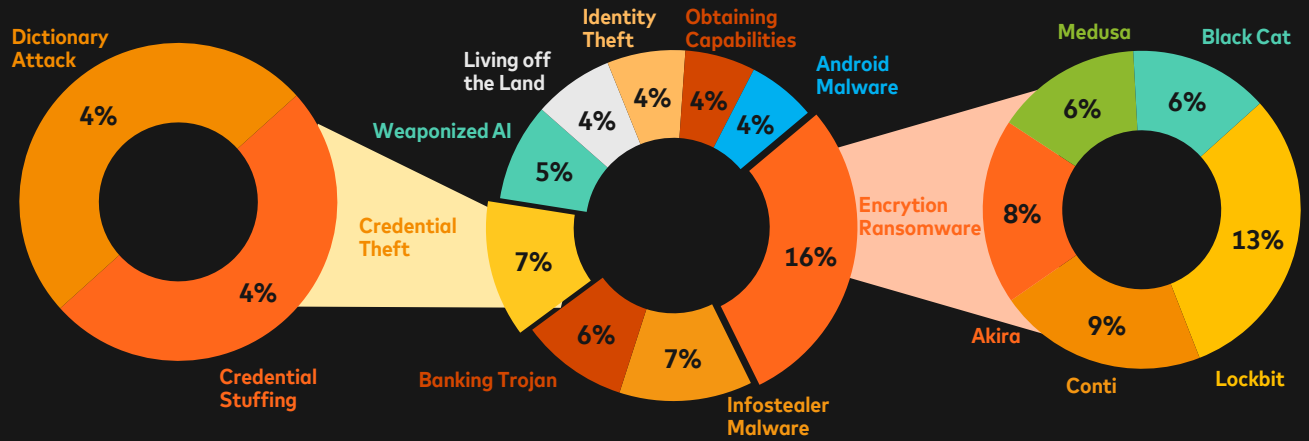
Return to Table of Contents

16% of cyber events targeting the Financial Sector in Spain leveraged **Malware** attack methods

Events per attributed TTP

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

KEY INSIGHTS

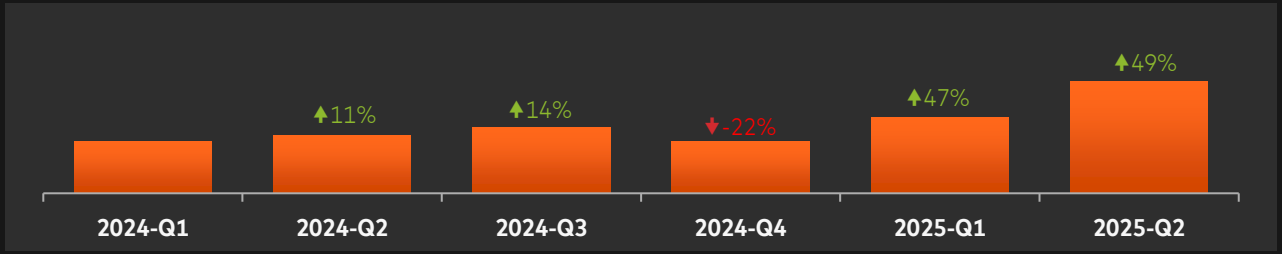
- Cyber-attacks occurrences in Spain's financial sector continued to evolve through 2025. **Between Q2 2025 and Q3 2025, attack volumes showed a marked shift**
- Since early 2025, the most prominent TTPs have **been Encryption Ransomware, Infostealer Malware, and Credential-focused attacks**. While traditional Malware remains prevalent, **new ransomware families** such as Medusa, BlackCat, Akira, and Lockbit became increasingly active
- Based on the analysis, **16% of all cyber events targeting Spain's financial sector leveraged Malware-based attack methods**. Within these, Infostealer Malware gained traction in late 2024 and persisted into 2025, while Encryption Ransomware reached its peak in Q1 2025, primarily tied to BlackCat operations.

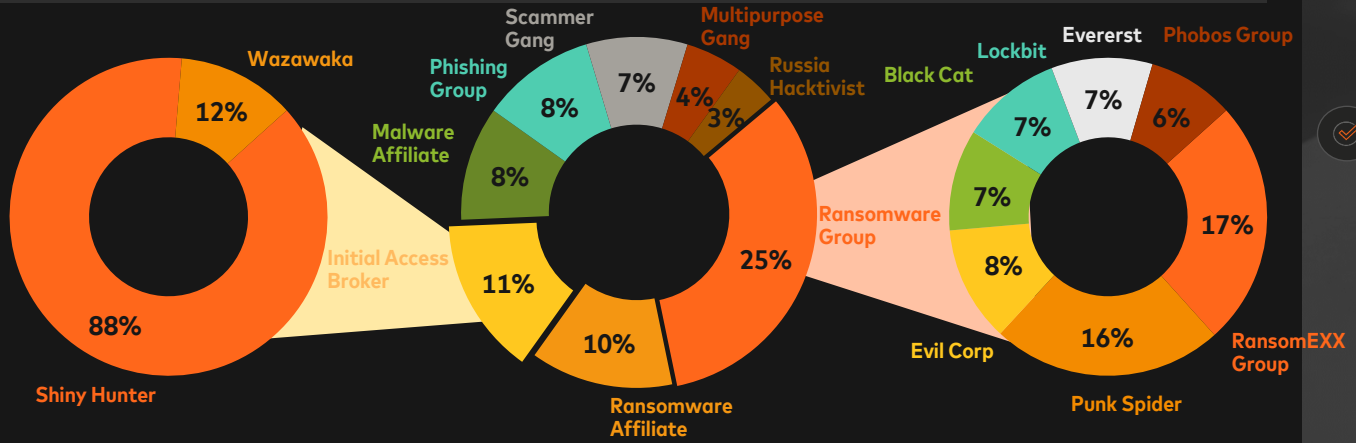
Return to Table of Contents

25% of cyber events targeting the Financial sector in Spain were attributed to **Ransomware Groups**

Events per attributed Actor

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

KEY INSIGHTS

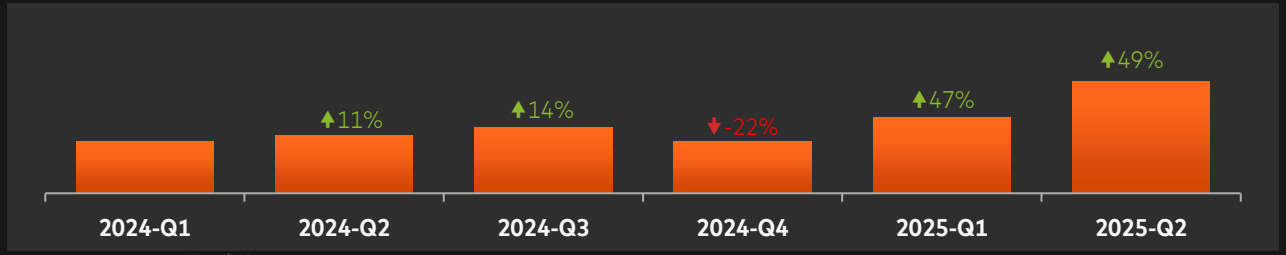
- **Black Hat, Organized Crime, and Ransomware Groups** were responsible for a significant share of cyber events targeting Spain's financial sector
- In fact, **25% of total cyber incidents between Q1 2024 and Q2 2025** were linked directly to Ransomware Groups, highlighting their central role in the evolving threat landscape
- Since early 2024, Black Hat and Organized Crime actors have remained highly active, with new waves of Ransomware affiliates gaining momentum throughout 2025. By Q2 2025, **ransomware groups such as Phobos Group (6%), RansomEXX Group (17%), Punk Spider (16%), and Evil Corp (8%) emerged as dominant forces**

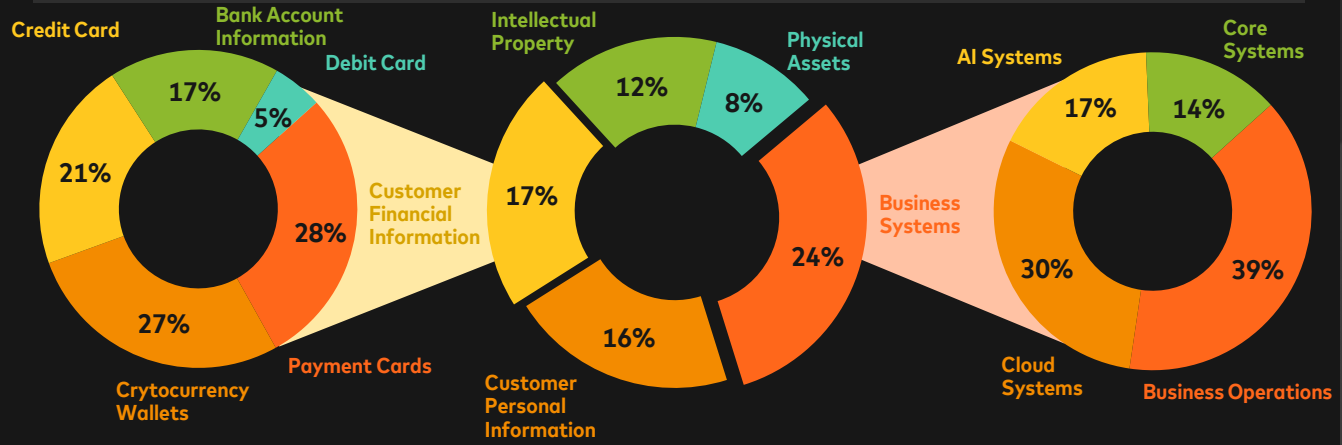
Return to Table of Contents

24% of cyber events targeting Financial sector in Spain focused on **Business Systems**

Events per targeted Asset

Spain





Source: Mastercard Cyber Insights Data. Based on data for the time period Jan 2024 – June 2025
Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.
**Categories with lower percentages have not been added to the piecharts

KEY INSIGHTS

- **Customer Financial Information** and **Business Systems** were observed in **41%** of total attack occurrences
- Since Q1 2024, **Customer Financial Information** have been among the most targeted assets in Spain. However, as of Q2 2024, **Business Systems** and **Customer Personal Information** have also emerged as prominent targets
- Our analysis indicates that **Business Operations** were among the most targeted assets for Business Systems. Regarding Customer Financial Information **Payment Cards** ranked the most targeted asset within the timeframe in Spain

Return to Table of Contents

Case Study: The MOVEit attack

ATTACK TIMELINE

- MOVEit, a file transfer system utilized by large organizations for handling sensitive data, fell victim to a flaw that cybercriminals started widely exploiting in **late May 2023**.
- However, recent evidence indicates that these hackers had been testing the vulnerability as early as **2021**. They strategically chose **Memorial Day weekend** for the attack, as IT departments often have reduced staffing during holiday weekends.
- **In June 2023**, while the investigation was ongoing, new vulnerabilities associated with MOVEit came to light, adding to the severity of the situation.
- **Clop** ransomware, the group responsible for the attack, claimed to have successfully stolen data from multiple organizations and demanded ransom negotiations from all victims before **June 14**.
- **On June 14th**, Clop escalated the situation by posting the profiles of allegedly breached companies on its data leak website but refrained from publishing any of the stolen data.
- **On July 11**, Clop issued a threatening message to all victims, warning them not to waste time and to pay the ransom promptly, or else their data would be made public.

ATTACK IMPACTS

- **Over 140 organizations** have been severely impacted by a massive hack targeting the MOVEit file transfer tool.
- The personal data of more than **15.5 million** people has been compromised due to a security vulnerability in MOVEit, which hackers exploited to carry out their attack.
- Progress Software's enterprise file transfer tool, MOVEit Transfer, was the specific target of the attack, leaving hundreds of organizations vulnerable to data theft.

Sources: Mastercard Cyber Insights Data; TechCrunch, SecurityWeek, cshub

Return to Table of Contents

Case Study: The QakBot (Qbot) Malware

ATTACK TIMELINE

The QakBot (Qbot) malware, known for its **resilience and adaptability**, has undergone significant evolution in its attack techniques over the years. Originally surfacing as a banking trojan, QakBot has expanded its capabilities to facilitate ransomware attacks and extensive financial fraud.

QakBot first emerged as a banking trojan at 2007.

It evolved to adopt various delivery vectors, including malicious email attachments, links, and more recently, embedded images.

There has been a notable increase in QakBot activity, with the malware using sophisticated techniques to evade detection and spread. This includes using ZIP file extensions, enticing file names, and Excel 4.0 macros for malicious attachments. The malware's modularity allows it to adapt its attack chain depending on the network environment, making it a challenging threat to detect and mitigate.

In 2024, **despite a major international operation that dismantled QuakBot's infrastructure**, **the malware resurfaced with new campaigns distributing other types of malware**. This indicates that while the initial takedown was significant, the threat from QuakBot persists, affecting organizations across Europe, including Poland.

ATTACK IMPACTS

QakBot's activities have led to significant impacts worldwide:

Extensive Infections: Over 700,000 victim computers were infected globally.

Facilitation of Ransomware and Financial Fraud: QakBot has been used as an initial means of infection by various ransomware groups, such as Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta.

Financial Damages: The attacks caused hundreds of millions of dollars in damage, significantly impacting businesses, healthcare providers, and government agencies across the globe.

Multinational Operation and Takedown: In a massive effort led by the United States, involving several countries, the infrastructure of QakBot was disrupted at August 2023. This operation led to the deletion of the malicious code from victim computers and the seizure of approximately $8.6 million in cryptocurrency linked to the cybercriminals behind QakBot.

The case of QakBot underscores the continuous evolution of cyber threats and the importance of international cooperation in combating such sophisticated cybercrime operations. It also highlights the need for organizations to stay vigilant and adopt proactive measures against evolving cyber threats

Sources: Mastercard Cyber Insights Data; Disruption-of-Qakbot, Europol (europa.eu)

Return to Table of Contents

Case Study: LockBit Ransomware Group

ATTACKS TIMELINE

LockBit is a Russian-based ransomware group initially observed in **2019**. They are known for **their ransomware variant of the same name** and operate using a Ransomware-as-a-Service (RaaS) model. This involves licensing their ransomware software to affiliated cybercriminals, who then pay LockBit a percentage of any ransom payments they receive. Since 2019, they've targeted thousands globally, costing billions in ransoms and recovery. Some major attacks as follows:

- LockBit group attacked ION Group in **January 2023**, a UK-based software company whose products are used by financial institutions, banks, and corporations for trading, investment management, and market analytics.
- LockBit group attacked Royal Mail, the UK's national postal service, in **January 2023**, which paralyzed their mail delivery system.
- **LockBit 3.0**, a highly **sophisticated ransomware variant**, has continued its malicious activities across various sectors, from **January 2023 to March 2024 peaking at Q4 2023**. This ransomware operates under a Ransomware-as-a-Service (RaaS) model.
- US arm of the Industrial and Commercial Bank of China was hit by a LockBit attack that disrupted their trades in the U.S. Treasury market in **November 2023**.
- LockBit group has published **43GB** of data stolen from Boeing after the aerospace giant refused to give in to ransom demands following a cyber-attack in **November 2023**.

OVERALL IMPACTS

- LockBit conducted around **800 significant attack** in **2023** across the globe.
- The LockBit ransomware attack impacted ION Group's Cleared Derivatives interrupting the services of several(**at least 42 clients**) prominent banks, **hedge funds, and brokerages**.
- Ransomware attack on Royal Mail **severely impacted** their systems, leaving millions of letters and parcels stuck in the company's system for 6-8 weeks.
- **LockBit 3.0** ransomware, was one of the most prominent variant of the attack, leaving hundreds of organizations vulnerable to cyber attack. . LockBit 3.0 has targeted various sectors, particularly critical infrastructure.
- Recently, **LockBit group has been disrupted** by an international law enforcement task force called **Operation Cronos** in **February 2024**. The operation was led by the UK's National Crime Agency and the US FBI. LockBit's technical infrastructure and its public-facing leak site on the dark web was seized after a months-long operation.

Sources: Mastercard Cyber Insights Data; ION GROUP ATTACK, LOCKBIT ATTACK 2023 SUMMARY, ICBC BANK ATTCK, ROYAL MAIL ATTACK , BOEING ATTACK, healthitsecurity

Return to Table of Contents

Case Study: CrowdStrike Incident Timeline

ATTACK TIMELINE

- On July 19–20, 2024, a faulty update from CrowdStrike's Falcon Sensor for Windows was released, leading to widespread system crashes. The issue originated from a corrupted content update, not from a cyberattack or external threat actor.
- Systems affected experienced Blue Screen of Death (BSOD) errors, primarily on Windows 10 and 11 environments.
- The incident rapidly escalated due to the automated deployment of the update via EDR tools and managed service providers (MSPs).
- Organizations across sectors (finance, healthcare, public services) saw devices rendered inoperable within minutes of the update.
- CrowdStrike released a fix shortly after identifying the issue and worked with customers to recover systems.

ATTACK IMPACTS

- Affected tens of thousands of endpoints globally, disrupting business continuity.
- Airlines, banks, hospitals, and retail operations experienced downtime due to endpoint crashes.
- Incident exposed operational risks of centralized security platforms and automated updates.
- Created significant helpdesk backlogs and forced many organizations to revert to manual recovery methods.
- Despite no malicious intent, the event shook confidence in third-party cybersecurity vendors.
- Sparked industry-wide discussions on resilience planning, update validation, and rollback strategies.

Sources: Mastercard Cyber Insights Data; Crowdstrike Outage Explained,

Return to Table of Contents

Top factors driving cyber trends in Spain

CYBER

- As the digital economy expands in Europe, so does the prevalence of digital crime
- Top threat actors executing cyber-attacks in Spain are **financially motivated Black Hat** attack groups
- Several cyber incidents have influenced the trajectory of cyber trends. A few notable occurrences are as follows:
- Scattered Spider – June 2024: Key member arrested in Spain; group tied to phishing, SIM-swaps, MFA-bombing
- NoName057(16) – July 2025: Spain issued arrest warrant in Europol's Operation Eastwood
- LockBit / BlackCat – 2024–2025: Active ransomware groups targeting finance & infrastructure; Spain listed among top ransomware-hit nations

GEOPOLITICAL

- Escalation in politically driven cyber activities is a known pattern, especially when notable political events take place. This can be caused by internal conflict and/or global distress .
- For e.g. the ongoing conflict between Russia and Ukraine as well as Israel and Palestine has had a notable impact on shaping cyber trends across Europe. This conflict has resulted in an increased acknowledgement of cyberspace's significance as an emerging domain of warfare, on par with land, air, sea, and space
- For instance, in June 2024 the pro-Russian group NoName057(16) carried out a DDoS attack on a Spanish defense contractor refurbishing tanks for Ukraine, highlighting how geopolitical conflicts directly shape cyber operations[1]

REGULATORY

- European financial market is **heavily regulated** aiming to protect individuals and maintain a safe environment to nourish the financial ecosystem.
- **NIS2** and **GDPR** are some of the regulations with intentions to establish digital resilience and safe environment to process personal and sensitive data.
- Also, the other important regulation will be the **Digital Operational Resilience Act (DORA)**, which has been published in the Official Journal of the EU, entered into force in January 2023, and expected to be implemented in January 2025 by all participating countries

WHAT SHOULD ORGANIZATIONS DO?

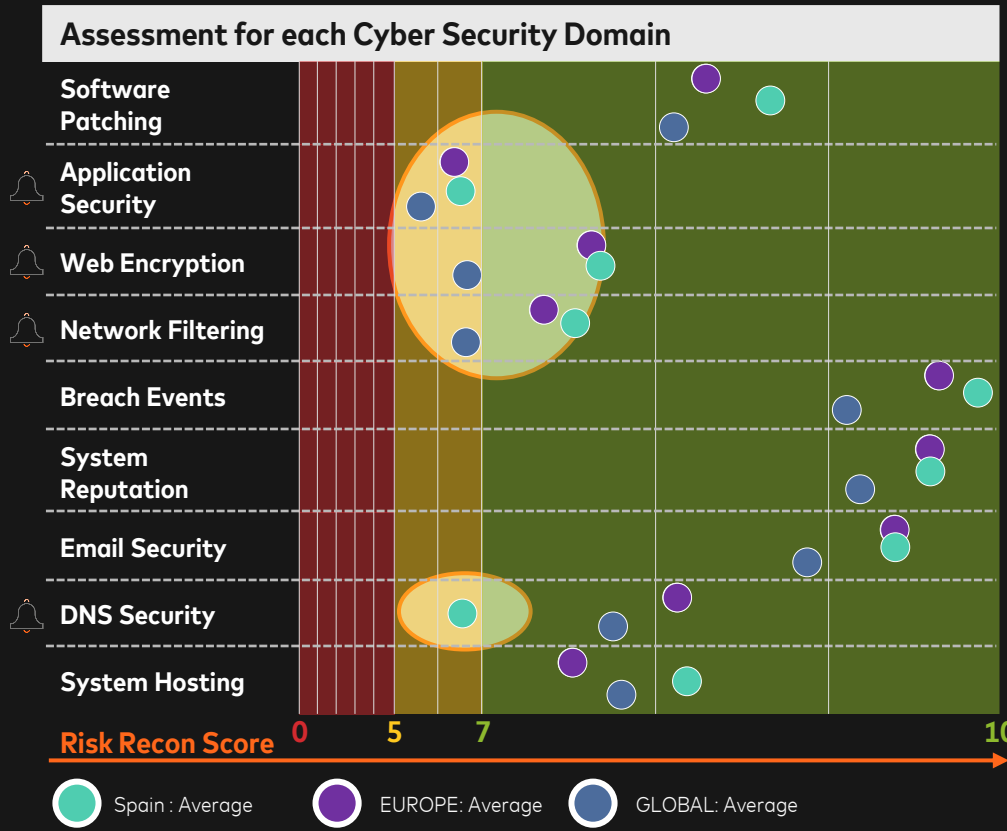
- Both public and private organizations **must work closely** to navigate newly enacted cybersecurity laws and regulations in Spain. **Without clear alignment** in expectations, organizations will likely **spend additional resources to figure out** the intent and desired outcome of enacting these laws and regulations
- Organizations must be aware of factors (i.e., Social Economic, Political, Regulatory) that shape their threat landscape. This can be achieved by continuously monitoring popular threat actors and attack methods globally, in their region and the industry. Based on the threat landscape, the current cybersecurity control maturity must be assessed and mapped to related threats
- Once initial assessments are complete, the organization needs to design its desired state based on its current capabilities, available resources, business priorities and the severity of the risks
- Finally, a prioritized remediation or maturity roadmap based on a risk and return on investment calculation should be established
- In any case, organizations should identify their most sensitive information and valuable assets to be protected. Protection efforts should be prioritized and optimized by focusing on low hanging initiatives that can yield the best outcomes given the available resources

Sources: Mastercard Cyber Insights Data

[1]REUTERS https://therecord.media/pall-mall-process-commercial-spyware-hacking-paris-diplomacy

Return to Table of Contents

Mastercard's RiskRecon scoring has identified significant domain maturity gaps among Spain's organizations



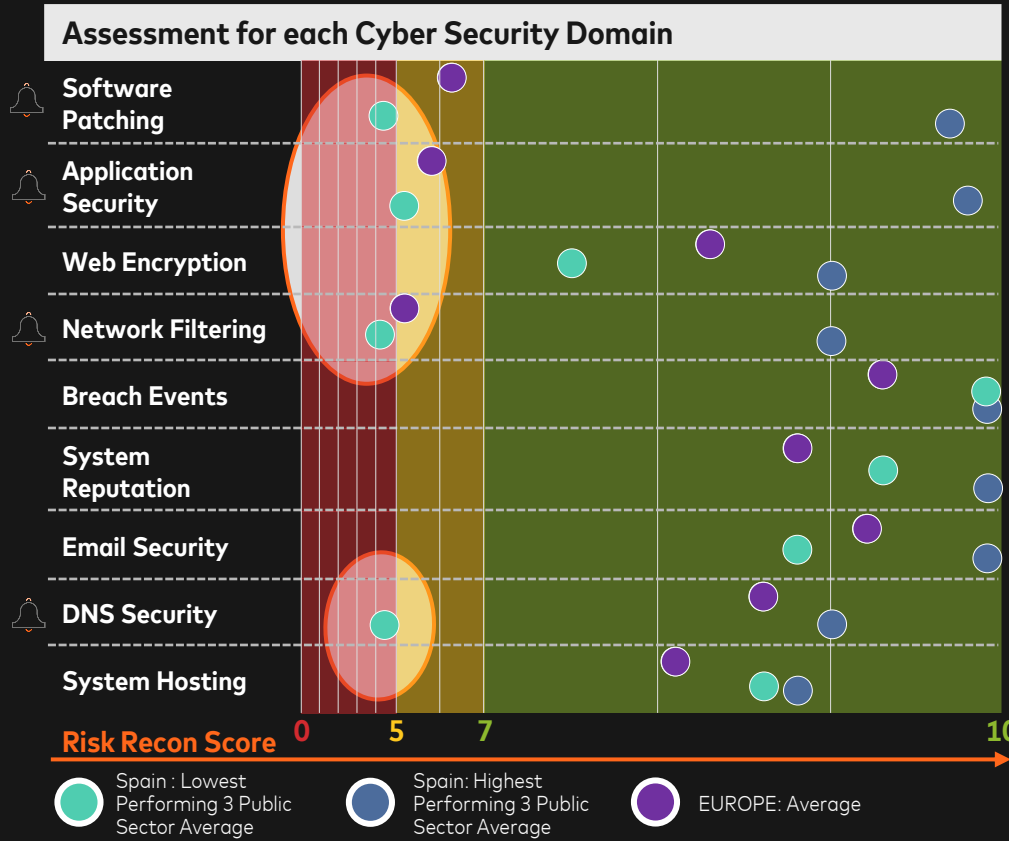
Score Averages
Overall score (out of 10)

Spain	7.6
Europe	7.2
Global	6.9

Source: Mastercard RiskRecon data. RiskRecon allows companies to evaluate the level of security of their internet-facing assets; cyber security domains shown above are a selection.

Return to Table of Contents

Mastercard's RiskRecon scoring has identified significant domain maturity gaps among Spain's Public Sector



Score Averages

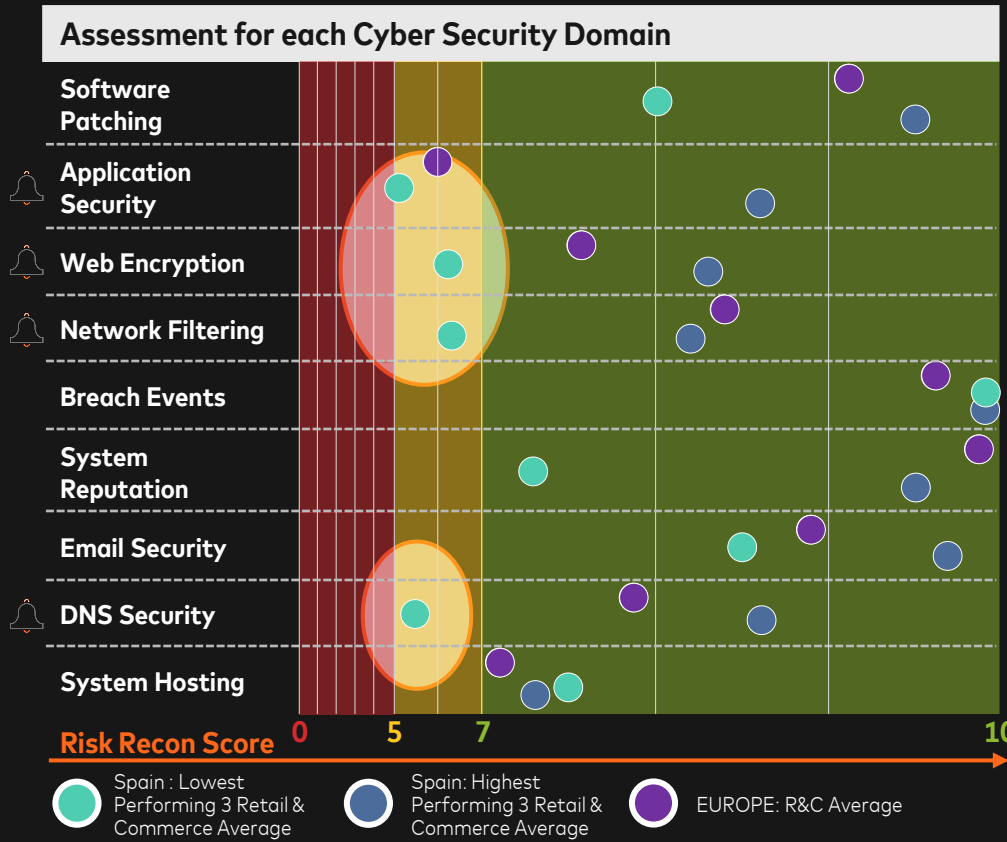
Overall score (out of 10)

Spain : Lowest Performing 3 Public Sector Average	4.8
Spain: Highest Performing 3 Public Sector Average	9.5
EUROPE: Average	5.9

Source: Mastercard RiskRecon data. RiskRecon allows companies to evaluate the level of security of their internet-facing assets; cyber security domains shown above are a selection.

Return to Table of Contents

Mastercard's RiskRecon scoring has identified significant domain maturity gaps among Spain's Retail & Commerce sector



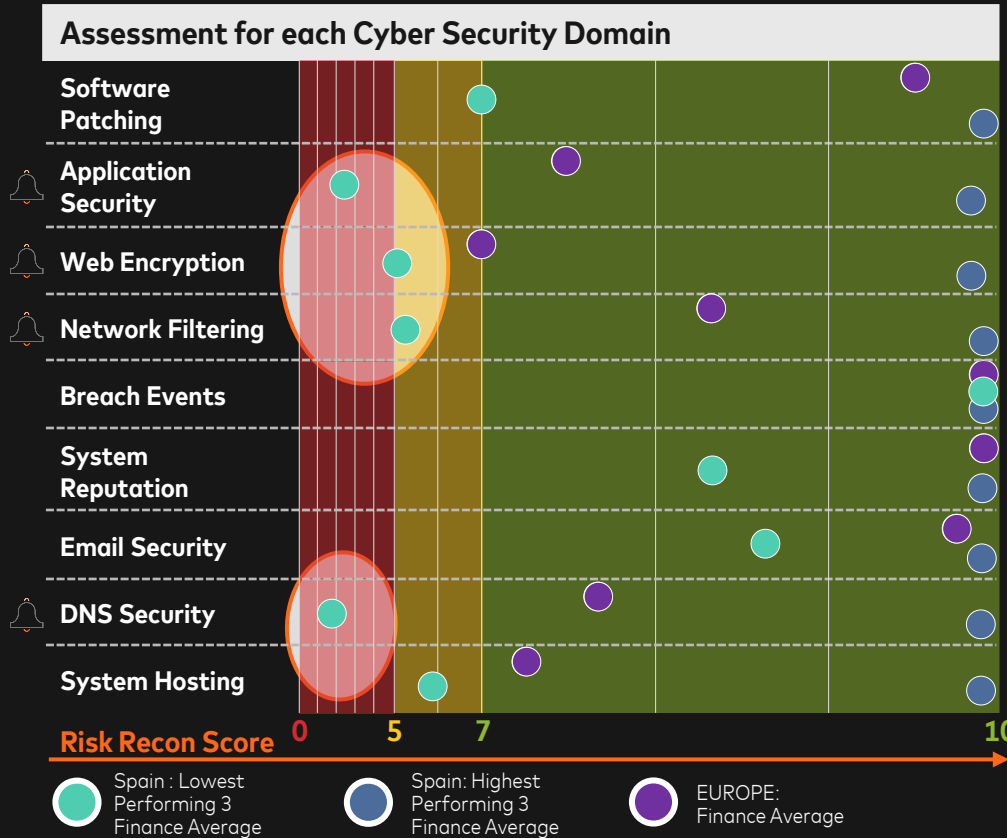
Score Averages
Overall score (out of 10)

Spain : Lowest Performing 3 Retail & Commerce Average	6.5
Spain: Highest Performing 3 Retail & Commerce Average	8.8
EUROPE: Average	7.7

Source: Mastercard RiskRecon data. RiskRecon allows companies to evaluate the level of security of their internet-facing assets; cyber security domains shown above are a selection.

Return to Table of Contents

Mastercard's RiskRecon scoring has identified significant domain maturity gaps among Spain's Finance Industry



Score Averages
Overall score (out of 10)

Spain : Lowest Performing 3 Merchants Average	3.1
Spain: Highest Performing 3 Merchants Average	10
EUROPE: Average	8.2

Source: Mastercard RiskRecon data. RiskRecon allows companies to evaluate the level of security of their internet-facing assets; cyber security domains shown above are a selection.

3. Leading practices for organizations

Identifying enemies in the cyberspace is just the first step. Enhancing defenses against the right threats, in the right places and in the right amounts is a constant and significant challenge.

Organizations can build and maintain a good cyber security posture by regularly running assessments on a set of controls

Path forward

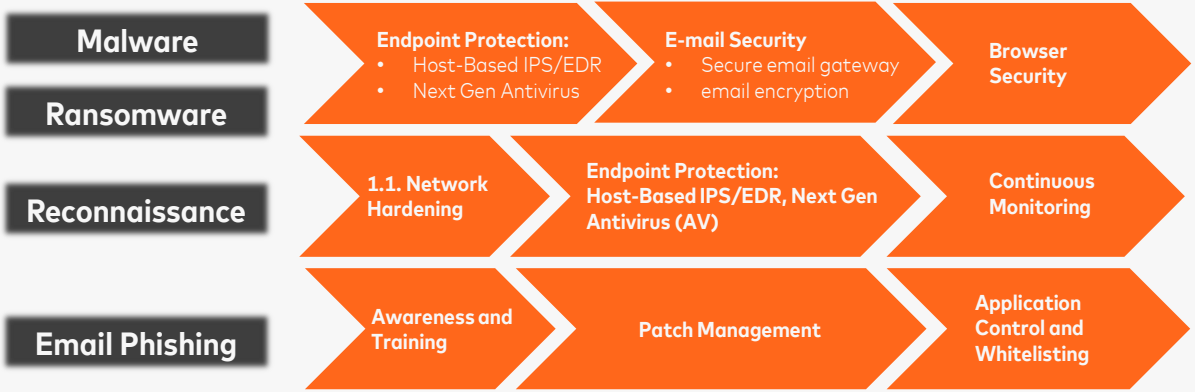
Organizations must ensure controls are enhanced to prevent, defend and react **against the most common attack methods identified in the region**, such as **Malware**, **Ransomware** and **Email Phishing**.

Essential control categories against top threats identified in Spain:

- Awareness and training
- Network content scanning & filtering
- Patch & vulnerability management
- Endpoint anti-malware (signature and behavior)
- Removable media control
- Third party risk management
- Incident detection (SIEM)
- Mobile devices management (MDM)
- Privileged account management
- Authorized software policy and control
- Hardening
- External intelligence gathering & analysis
- Response and forensics
- Penetration Testing
- Client secure browsing
- Firewall, IPS, IDS
- Data classification policy and mapping
- Secure development framework
- Policy compliance enforcement

Given the industry's common threat landscape, prioritizing defenses against the most prevalent attack vectors enables organizations to maximize the impact of their cybersecurity investments and improve overall risk posture.

Spain's four **major cyber threats** and **respective controls**.



Four areas where **Spanish Companies** should aim to improve based on Risk Recon security assessment

Security Domains	Rating
Application Security	6.7
DNS Security	6.7
Network Filtering	7.5
Web Encryption	7.8

Considering the cyber threat landscape in Spain, some of the identified remediation opportunities become even more important to address in a timely manner.

Strategic prioritization for superior investments; essential scenarios and best practices in remediation for cyber threat landscape in Spain

Ransomware/Malware

Threat Scenario: A major financial services company faces a ransomware attack orchestrated by a well-organized hacking group. Leveraging a zero-day exploit, the attackers infiltrate the institution's network and swiftly deploy ransomware across critical systems. The malware encrypts vital databases containing transaction histories and client information. Subsequently, a ransom demand is issued, threatening to permanently erase the encrypted data unless a substantial amount is paid in cryptocurrency.

1.1. Endpoint Protection: Host-Based IPS/EDR, Next Gen Antivirus (AV)

- Host based IPS systems protects a unique host by attaching itself closely to the OS and forming a security layer by allowing only legitimate requests.
- EDR is a set of capabilities that allow for continuous monitoring and analysis of endpoint activity to identify, detect, and respond to advanced threats in real time. EDR tools go beyond detecting suspicious activity and automatically respond to threats
- Next Gen AV, uses artificial intelligence and automation to try to identify things that could be a virus or are behaving like a virus and shut them down.

1.2. E-mail Security

- Email security is a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise.
- Besides security awareness training, a multi-faceted approach supplemented with technical controls is recommended to mitigate the file based and URL-based nature of email attacks.
- One of the first best practices that organizations should put into effect is implementing a secure email gateway. An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. It's also important to deploy an automated email encryption solution as a best practice.

1.3. Browser Security

- The browser and end-user devices security policy and hardening activities help reducing the risk from malicious software and content-based attacks. (cookie policy, internet history protection, managing add-ons, plugins & extensions)
- Antimalware and antivirus software: It monitor internet content as well as software running directly on the platform
- Sandboxing: A successful attack against a browser is less likely to compromise the rest of the platform if it is contained inside a sandbox
- Updates: As the attack surface of browsers is very large, and the chances of facing malicious code is high, these security updates are recommended to be installed regularly and quickly following their release.

Strategic prioritization for superior investments; essential scenarios and best practices in remediation for cyber threat landscape in Spain

Reconnaissance

Threat Scenario: An organized threat actor group initiate a process of gathering information against a corporation. They systematically collect detailed information about the company's network infrastructure such as active IP addresses, hostnames, open ports, credentials, certificates and employee habits without triggering any security alerts for three months. Utilizing this intelligence, they identify vulnerabilities in the infrastructure. Exploiting this weakness, they manage to infiltrate the system undetected and creating a base for potential future attacks.

1.1. Network Hardening

- Ensure your perimeter security is properly established, configured, logged and all rules are regularly reviewed.
- Secure remote access points and users, block any unused or unneeded open network ports, disable and remove unnecessary protocols and services, implement access lists, encrypt network traffic and limit your exposure including being careful in what you release such as news and events.
- Establish an automated and comprehensive vulnerability identification and patching system. Systematically identify vulnerabilities and prioritize remediation.

1.2. Continuous Monitoring

- Continuosly monitor and test your environment against the most prevalent attacks, vulnerabilities and threats. Penetration tests and red team operations allow you to identify vulnerabilities and predict potential threats by emulating the reconnaissance tactics of attackers.
- Utilize breach attack simulation tools to continuously simulate the behavior of a real-life hacker and understand the effectiveness of your security controls against most prevalent threats.
- Monitor network traffic from varios areas to capture anomalies, suspicious loads or spikes centerally, such as in a SIEM tool so that you can perform in-depth analysis and correlate different events each other.

1.3. Endpoint Protection: Host-Based IPS/EDR, Next Gen Antivirus (AV)

- Host based IPS systems protects a unique host by attaching itself closely to the OS and forming a security layer by allowing only legitimate requests. It also analyze network traffic patterns and detect anomalies indicative of reconnaissance activity.
- EDR is a set of capabilities that allow for continuous monitoring and analysis of endpoint activity to identify, detect, and respond to advanced threats in real time. EDR tools go beyond detecting suspicious activity and automatically respond to threats. It will resist the attacker's reconnaissance efforts to gain unauthorized access via your ports.
- Next Gen AV, uses artificial intelligence and automation to try to identify things that could be a virus or are behaving like a virus and shut them down.

Strategic prioritization for superior investments; essential scenarios and best practices in remediation for cyber threat landscape in Spain

E-Mail Phishing

Threat Scenario: A major financial institution is targeted in an email phishing attack. Employees receive seemingly authentic emails, urging urgent login credential updates through a provided link. Unbeknownst to them, the link deploys malware, granting cybercriminals unauthorized access to sensitive financial data. This could result in unauthorized transactions, compromised accounts, and financial losses for both the institution and its clients.

1.1. Awareness and Training

- Phishing awareness training refers to a training campaign that educates end-users on specific phishing threats they may encounter in their daily lives.
- Effective **phishing awareness training** typically leverages phishing simulations to deepen employee knowledge, allowing them to spot warning signs and report phishing threats in a safe environment.

1.2. Patch Management

- Patch management involves identifying system features that can be improved or fixed, creating that improvement or fix, releasing the update package, and validating the installation of those updates.
- The three most common types of patches are **security patches**, **bug fixes**, and **feature updates.**
- **Identify systems** that are noncompliant, vulnerable, or unpatched. Scan systems daily. **Prioritize patches** based on the potential impact. Calculate risk, performance, and time considerations. **Test patches** before placing them into production.

1.3. Application Control and Whitelisting

- Application Control is primarily intended to prevent the installation of unapproved applications. The installation package is tested against a list of permitted applications when someone tries to install a new application. The installation process is allowed to continue if the application is found to be approved.
- An application whitelist is a list of applications and application components (libraries, configuration files, etc.) that are authorized for use in an organization. Only validated and whitelisted files and applications are allowed to run using application whitelisting, which makes use of a range of application file and folder properties.

Focus on most common security issues | HTTP Security Headers help protect websites from clickjacking, cross-site scripting (XSS), and MIME type sniffing

Application Security
HTTP Security Headers

Description	• It is recommended for each web site the presence of five HTTP security headers - x-frame-options, strict-transport-security, x-content-type-options, and x-xss-protection OR content-security-policy • A web site that is not implementing one or more of these important HTTP security headers doesn't provide instructions to the browser for secure interaction with the web server, such as always encrypting browser requests, not allowing site content framed in other systems, and helping to prevent cross-site scripting and other similar attacks
Recommendation	• Implement Browser Security principles • Ensure Internet navigation is controlled and secured by means of multiple security layers (e.g., browser app, Secure Web Gateway, etc.)
Useful links:	• https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Focus on critical security issues | Missing domain hijacking protection can allow unauthorized control over domains, especially those handling business functions.

DNS Security
Domain Hijacking Protection

Description	• RiskRecon identified one or more domains that do not have basic configurations in place to help prevent domain hijacking. • Without implementing proper DNS configurations, threat actors could gain control of the insecure domains.
Recommendation	• Ensure strong access control for domain administration. Use domain hijacking protection codes, such as the ICANN-defined clientTransferProhibited. • Choose reputable domain registrars that offer administrative controls and require extra authentication before making changes to a domain.
Useful links:	• https://blog.riskrecon.com/

Focus on critical security issues | Unsafe network services expose organizations to data breach, malware infection and service disruption

Network Filtering
Unsafe Network Services

Description	• Unsafe Network Services consist of products and protocols such as database servers and remote access protocols that are widely considered to be unsafe and inappropriate to operate on the Internet • MySQL, postgresql, Samba and Telnet are among the most common products and protocols linked with Unsafe Network Services that may favor the exploitation of a vulnerability • The causes of Unsafe Network Services are multiple; in example, improper API design, misconfiguration in access control lists, insufficient data filtering or limited implementation of secure coding practices
Recommendation	• Implement Attack Surface Management process and solutions • Centralize the management of network devices (e.g., firewalls, routers) and define secure configurations to be deployed enterprise-wide
Useful links:	• https://blog.riskrecon.com/ • https://www.riskrecon.com/signals-of-insecurity

Focus on critical security issues | Invalid certificate subjects on HTTPS websites lead to browser security warnings and undermine trust in systems handling sensitive data.

Web Encryption
Certificate Management

Description	• Correctly configured web encryption is essential to ensuring that communications are protected from eavesdropping and that people can verify the authenticity of the system. • RiskRecon identified encryption implementations with expired encryption certificates and have invalid X.509 encryption certificate subjects.
Recommendation	• Replace all expired encryption certificates with certificates that are not expired. Implement processes to ensure that encryption certificates are replaced before expiration. • To improve security, start by fixing the most important systems that handle sensitive information. Replace the SHA-1 hash algorithm with stronger ones like SHA-2 or SHA-3. Turn off old, insecure protocols such as SSLv2, SSLv3, and TLS 1.0, and use newer, safer protocols. • Ensure all X.509 certificates are valid and correctly match the system they protect. For less important systems, decide on fixes based on their specific needs.
Useful links:	• https://blog.riskrecon.com/

Essential practices to enhance your cyber posture

Establish a non-negotiable cybersecurity culture

Strengthening the awareness and training program, thus ensuring collaborators are defenders of cybersecurity by eliminating bad habits that negatively affect the organization's security posture. Invest in user training.

Patch apps and systems

The management of patches and vulnerabilities in an organization is one of the main components in managing and administering risk; in fact, the management of patches and vulnerabilities is the center of **cyber resilience and hygiene**.

Collect, monitor, and analyze information to build cyber intelligence

Build a **management program for the management, intelligence, and investigation of cybersecurity incidents** to minimize the adverse impacts on your operations by carrying out identification, analysis, treatment, response, and containment activities, through the correct articulation of the attention and response teams.

Build a third-party risk management program

Establish a program to allow you to **manage and monitor your critical third parties to prevent their risk becoming your risk**.

Strengthening your controls against malware

Implementing controls for **monitoring users' behavior, network content scanning & filtering, secure browsing, and powerful awareness, culture, and training programs** allow you to protect against these attacks.

Manage change management and hardening programs

Incorrect settings are a gateway for attackers. Building a **robust change management program** allows organizations to manage and review changes before they are converted into a door for attackers or put the organization at risk.

Establish and know your cyber perimeter

Due to the current situation, the **limits or perimeter of the network are not drawn and no longer exist**, or single-entry points defined. This panorama obliges the Corporation to have identified its borders and limits in order to identify the associated risks and implement the appropriate controls such as **network access, firewall, IPS, IDS**.

Cybersecurity best practices for organizations

Organizations' cybersecurity posture should have sufficient controls to prevent and defend against cyberattacks.

DNS Security

- Place DNS servers behind a firewall, shut down all non-required DNS resolvers and require DNS operators to use multifactor authentication.
- Proactively deploy security updates to DNS servers and enable DNSSEC to ensure that DNS responses are digitally signed.
- Capture DNS logs (and enable debug logs) in a centralized log management server and security information and event management system to detect attacks such as DDOS and cache poisoning.

Network Filtering

- Periodically adjust network filtering capabilities and settings according to the continuously evolving threat landscape.
- Limit internet-facing systems and network services strictly to those that are necessary.
- Follow a layered security approach especially for perimeter security controls.
- Beyond securing perimeter network controls, implement appropriate network segmentation and micro-segmentation to improve resiliency against malware propagation.

Email Security

- Dedicate sufficient resources to properly analyze your organization's email infrastructure to better configure Domain-Based Message Authentication, Reporting, and Conformance (DMARC). A misconfigured DMARC can block legitimate emails causing disruption to operations.
- While configuring DMARC, SPF, and DKIM authentication records does prevent direct impersonation of your domain, security awareness trainings should be provided to employees and contractors on a regular basis.

Application Security

- Establish and implement DevSecOps program that will reinforce/embed security throughout the software development lifecycle from the start at the design phase.
- Incorporate Breach Attack Simulation (BAS) and/or penetration testing program on application before going live and after every update, where feasible.
- Deploy dedicated web application firewalls (WAF) in front of every internet-facing application.

Web Encryption

- Implement cryptographic key management processes to make sure that keys used to sign certificates are managed appropriately, renewed on a regular basis and preserved in a secure environment.
- Use the most updated and secure encryption protocols.

System Hosting

- Ensure that systems are hosted in reputable countries and that hosting providers are following applicable regulations and laws.
- Minimize high fragmentation of hosting with a large number of hosting providers to reduce management complexity and attack surface.

Software Patching

- Track software inventory and regularly check for software updates.
- Patch all known vulnerabilities; if patching is not possible, ensure compensating controls.
- Disable unnecessary services, remove unnecessary scripts, drivers, features and sub-systems.

Return to Table of Contents

Why Mastercard

Mastercard has been applying our cybersecurity principles to secure our global payments network for the past 50 years

- We Securely Store Over 18 Petabytes of Sensitive Data
- Secure Data & Transactions for 2 Billion Cards Annually
- Mitigate 3.2 Million Phishing Attempts on Our Network Annually
- Detect & Defeat 200 Attacks on our Network Every Minute of Every Day

We are now bringing our decades of expertise and those same high standards of quality, reliability, security, and privacy to the broader ecosystem

Return to Table of Contents

How Mastercard can help

Our offerings help organizations address key cybersecurity concerns

Strategic Threat Landscape

What is the external threat landscape – main threat actors, attack methods and targeted business assets – facing my organization today and where should I focus my cyber resilience.

Cybersecurity Risk Quantification

How mature are my cybersecurity controls compared to their importance and what is the financial risk impact of possible cyber security incidents and risk mitigating investments.

Cybersecurity Attack Simulation

How resilient is my technical infrastructure against thousands of real-world cybersecurity attack methods and how can I close the gaps.

Third Party Risk Monitoring

How can I ensure that my third-party providers such as vendors and suppliers adhere to my security requirements and do not risk my assets and how secure is my own external posture.

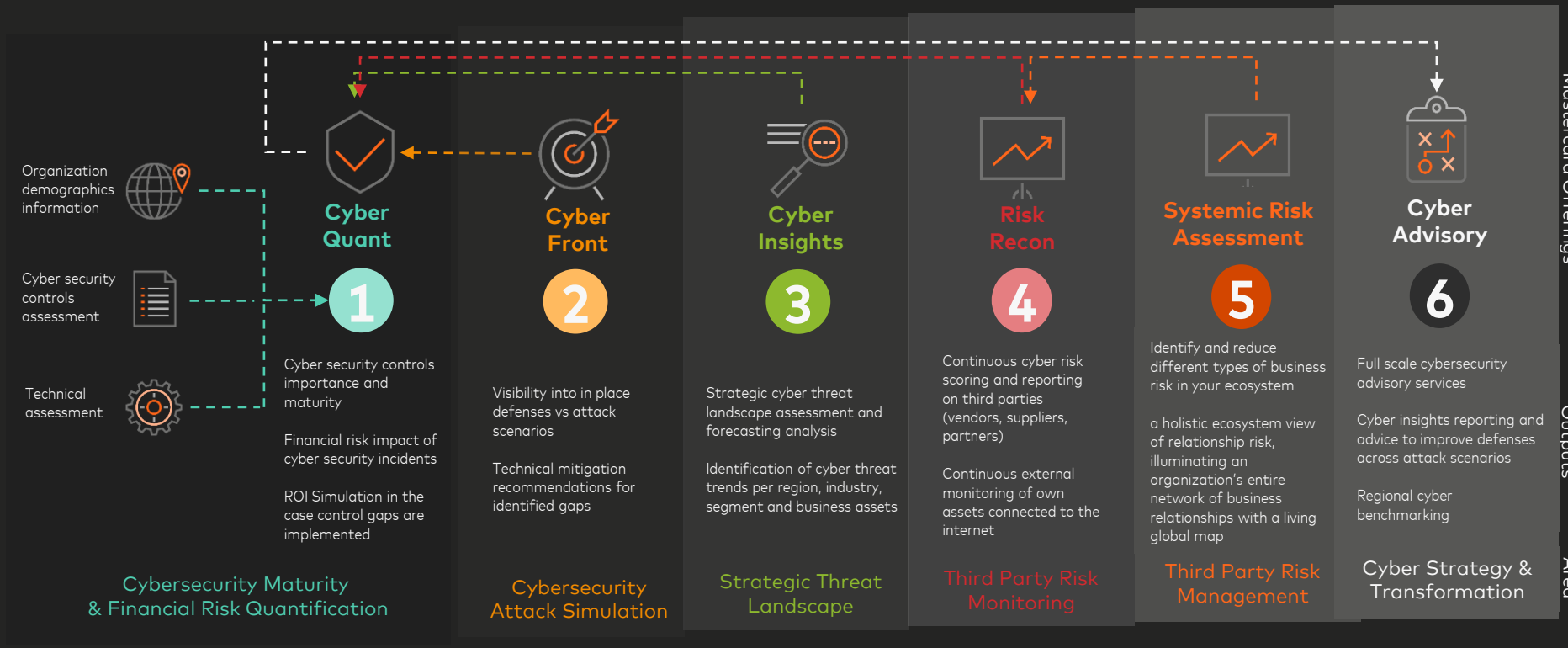
Cyber Strategy & Transformation

Massive cybersecurity breaches have become almost commonplace. Do I have the right strategy, governance and technology to protect my business from emerging cybersecurity risks.

Return to Table of Contents

High Level Offerings Overview

How we help our customers to improve their cybersecurity capabilities as a strong core of their digital resilience



Return to Table of Contents

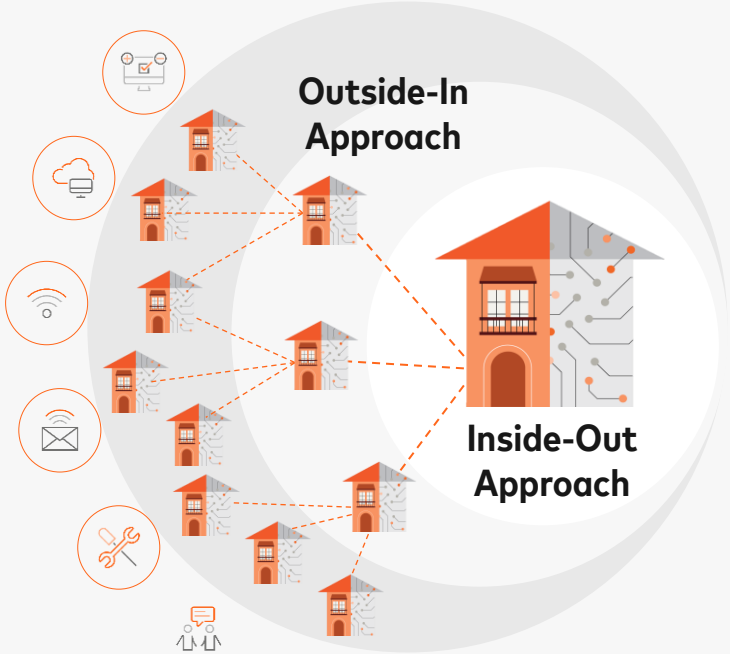
Understand how your organization is protected by assessing your cybersecurity posture externally and internally

Cyber Quant

Cyber Insights

Inside-Out Approach

- Are your organization **assets** secured?
- Cyber Quant enables businesses **to reduce** their **risk exposure** by assessing internal facing cybersecurity capabilities



Risk Recon

Outside-In Approach

- Are **entries** into your organization secured?
- RiskRecon enables businesses **to pinpoint**, **prioritize** and **mitigate cyber risk from third-parties**

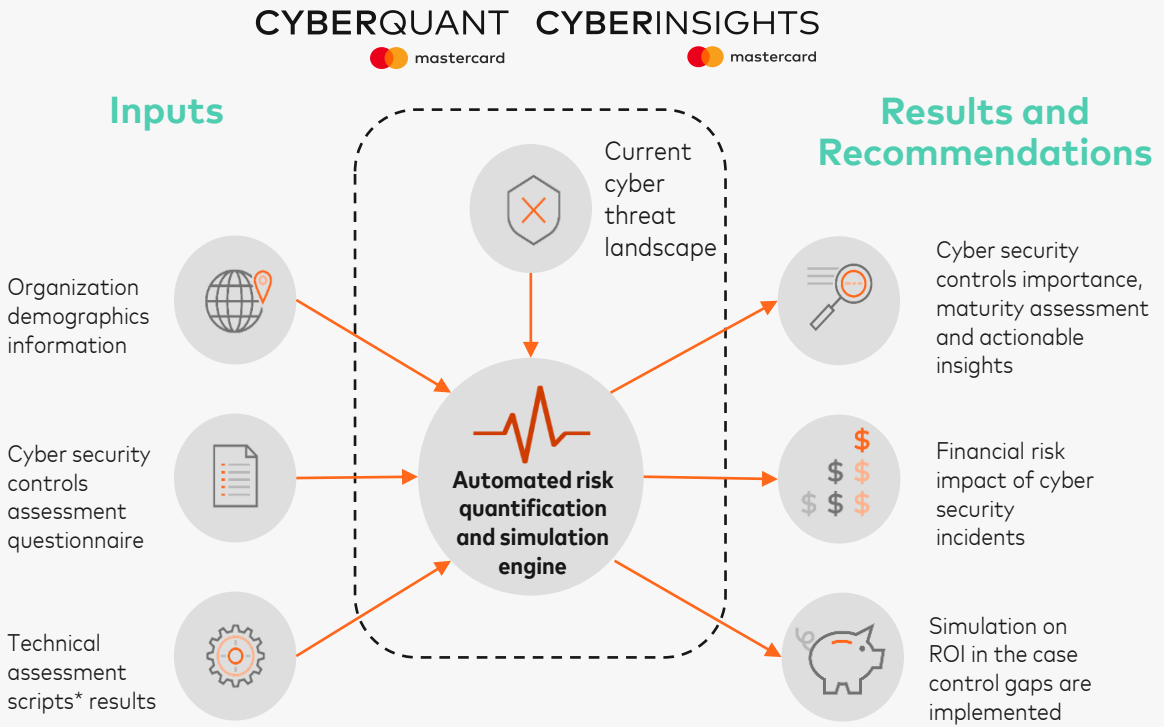
Cyber Quant

Cyber Insights

How does Cyber Quant work?

Mastercard **Cyber Quant** is an exposure evaluation of a client's **cybersecurity processes**, technology infrastructure, and workforce security practices. It **evaluates the maturity levels** of over 50 types of security measures to understand the **risk exposure** of the Company.

Then, helps companies to **identify** gaps, **prioritize** improvement of these response measures in accordance with the contextual threat landscape, creating **personalized results** and recommendations for each Company.



* Scripts developed by the Center for Internet Security (CIS)

Cyber Front

How does Cyber Front work?

Mastercard team collaborates with the customer to setup the platform for enabling ongoing simulation tests based on 9000+ unique threats and 500+ unique scenarios resulting in better identification of threats to address.

1 Cyber Front incorporates 7,600+ threats, updated daily

2 Simulated malicious traffic are sent to the Cyber Front agent

3 Remaining undetected traffic identified by Cyber Front is reported to the Cyber Front Simulator

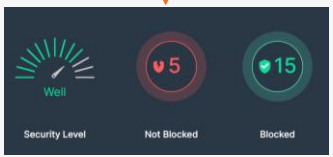
Global Cyber Threats

Cyber Front Threat Simulator

Simulated Malicious Traffic

Infiltrated Traffic

Cyber Front Agent



Cyber Front Dashboard

4 The type of breach and attack scenarios tested and results of these tests, as well as the remediation recommendations, can be accessed through the Cyber Front dashboard

Return to Table of Contents

Cyber Quant

Remediation prioritization of gaps to reduce your cyber risk

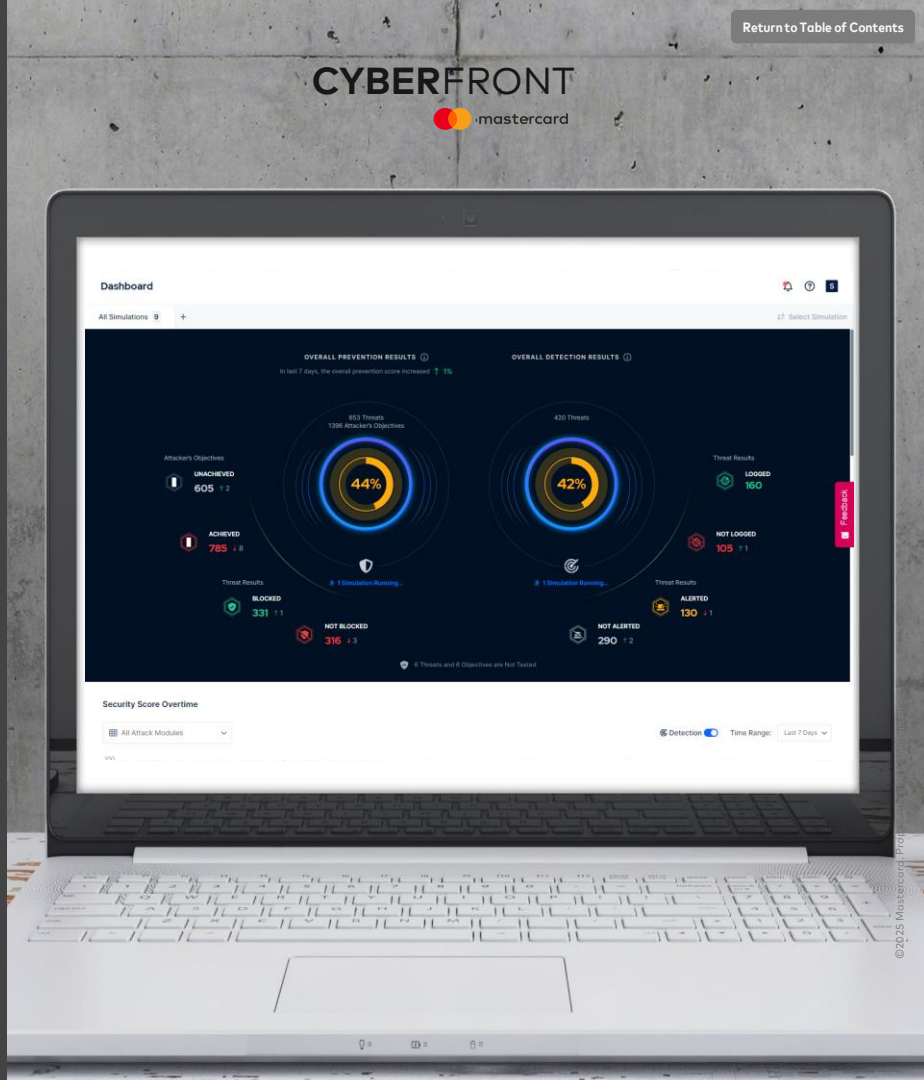
- ✓ Comprehensive assessment of cyber security capabilities and risks engaging broadly to assess adherence to security policies, procedures, and technical capabilities
- ✓ Contextualized analysis of cyber security controls and strategies matched to the threat landscape
- ✓ Strategies to reduce financial costs associated with a breach
- ✓ Prioritized risk reduction areas to drive maximum return on investment
- ✓ Simulation engine for ongoing evaluation of cyber projects
- ✓ Continual updates to account for updates to cyber practices and projects, and based on changing cyber threats

Return to Table of Contents

Cyber Front

Identify and defend most relevant threats with breach and attack simulations

- ✓ Validate security infrastructure, configuration settings and prevention technologies are operating as intended
- ✓ Continuously test existing security infrastructure, without the need to wait for vulnerability scanning windows
- ✓ Understand the probability of a threat by identifying threats and attack vectors
- ✓ Ensure security ops staff and incident responders can detect attacks and respond accordingly during cyber response exercises

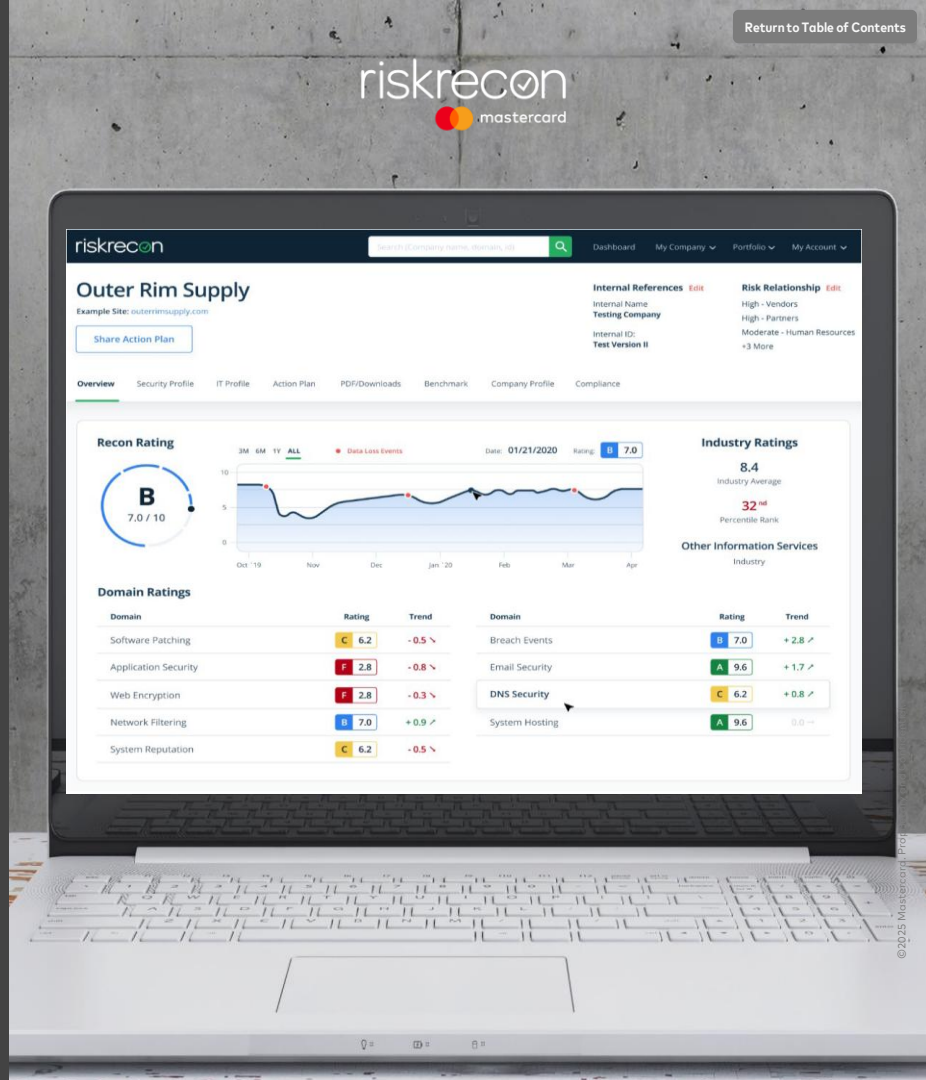


Return to Table of Contents

Risk Recon

Pinpoint and prioritize cyber risk from third parties

- ✓ Aggregated cyber risk rating for every third-party service provider and vendor based on the assessment of their cyber environment
- ✓ Alerts on issues exceeding risk thresholds, not just a general listing of all issues uncovered
- ✓ Downloadable detailed reports on all uncovered vulnerabilities
- ✓ Benchmarking of third-party service providers and vendors against standardized compliance frameworks and amongst one another
- ✓ Actionable risk plans are easily shared with third-party service providers and vendors using the collaboration portal



Return to Table of Contents

SRA

Optimize operational resilience across relationships against evolving business risks

- ✓ Proactively monitor and assess complex, evolving business risk across multiple dimensions throughout your entire network of business relationships
- ✓ Gain greater control, adaptability, resiliency with continuous, proactive monitoring of risk at chosen intervals and thresholds to improve adaptability for future disruption
- ✓ Reduce financial losses from threats associated with suppliers, merchants, third parties and business partners with solvency or liquidity issues or operations in restricted countries
- ✓ With a holistic view of risk across business networks in one solution that requires no implementation or ongoing maintenance and replaces costly, time-consuming, manual, fragmented projects save time and resources

4. Appendix

THREAT ACTORS

Attack	Description
State Sponsored	A threat actor group that is directly sponsored by a nation state, usually as part of the state's government or military infrastructure. Its motivations are political, and it targets other nation states through sophisticated attacks or covert cyberespionage. It commands an ample resource-base and has an advanced skill set. Falls under the category of Advanced Persistent Threats (APT).
Cyber Warrior	A threat actor group that may be indirectly sponsored or controlled by a nation state. Its motivations are political and/or ideological, and it targets nation states (including the one it operates from in certain cases) through sophisticated attacks or covert cyberespionage. It can command an ample resource-base and has an advanced skill set. This threat actor type includes cyber mercenary groups. Often falls under the category of Advanced Persistent Threats (APT).
Cyber Terrorist	A threat actor group that is directly sponsored or controlled by a recognized terrorist organization. Its motivations are ideological, and it targets nation states or ideologically opposed organizations through disruptive attacks. It has a limited resource-base and an intermediate skill set.
Hacktivist	An individual or threat actor group that may be connected to a nation state but generally operates independently. Their motivations are ideological, and they target public or private organizations through disruptive attacks. They have a limited resource-base and an intermediate skill set.
Corporate Spy	A private organization operating independently to steal sensitive corporate information for commercial advantage. Its motivations are financial, and it targets other private organizations (generally competitors in their industry) through data exfiltration attacks and covert cyberespionage. It can command an ample resource-base and has an intermediate skill set. It sometimes outsources operations to external cyber mercenaries. This threat actor type includes legal adversaries.
Black Hat	An individual or small threat actor group operating independently. They are motivated by financial and personal gain, and they target public or private organizations through relatively sophisticated attacks. They have a limited resource-base and an advanced skill set. This threat actor type includes fraudsters.

THREAT ACTORS

Attack	Description
Organized Crime	A threat actor group that may be connected to a nation state but generally operates independently and is similar in structure and hierarchy to an organized physical crime gang. Its motivations are financial, although in certain cases they may be ideological as well, and it targets public or private organizations through sophisticated attacks. It commands an ample resource-base and has an advanced skill set. Often falls under the category of Advanced Persistent Threats (APT).
Unskilled	An individual with low technological sophistication making use of externally provided attack TTPs (tactics, techniques, and procedures). They are motivated by personal gain and target public or private organizations through disruptive or defacement attacks. They have a limited resource-base and an elementary skill set. This threat actor type includes script kiddies and cyber vandals.
Privileged Insider	An individual who is currently or was previously connected to an organization (as an employee, contractor, vendor, etc.), in a role granting them elevated or privileged permissions (such as an IT position). They are motivated by financial and/or personal gain, or in certain cases by ideology or revenge, and target their own organization through data exfiltration attacks. They have an intermediate or low skill set but their capabilities and resources are significant due to their insider knowledge and access to the organization.
Malicious Insider	An individual who is currently or was previously connected to an organization (as an employee, contractor, vendor, etc.), in a role granting them only low-level permissions. They are motivated by financial and/or personal gain, or in certain cases by ideology or revenge, and target their own organization through data exfiltration attacks. They have an intermediate or low skill set but their capabilities and resources may be significant due to their insider knowledge of the organization.
Accidental Insider	An individual who is currently or was previously connected to an organization (as an employee, contractor, vendor, etc.), and unintentionally targets their own organization through negligence or external lures. Their capabilities may be significant due to their insider knowledge and access to the organization.

ATTACK METHODS

Attack	Description
Denial of Service (DoS/ DDoS)	The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses.
Unauthorized Device	Unauthorized devices that are connected to the environment can cause malware distribution and data leakage. Attack examples are Unauthorized removable media connection and Unauthorized network device connection.
Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Adversary in the Middle	This type of attack targets the communication between two components (typically client and server). The attacker places himself in the communication channel between the two components. Whenever one component attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and it is then passed on to the other component as if it was never intercepted. This interposition is transparent leaving the two compromised components unaware of the potential corruption or leakage of their communications. The potential for Adversary-in-the-Middle attacks yields an implicit lack of trust in communication or identify between two components.
Credential Access	In this attack, some asset (information, functionality, identity, etc.) is protected by a finite secret value. The attacker attempts to gain access to this asset by using several techniques such as brute-forcing or credential stuffing. Examples of secrets can include, but are not limited to, passwords, encryption keys, database lookup keys, and initial values to one-way functions.

ATTACK METHODS

Attack	Description
Privilege Escalation	An attacker actively targets exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage access to its resources or authorize utilization of its functionality. Such exploitation can lead to the complete subversion of any control the target has over its data or functionality enabling almost any desired action on the part of the attacker. Attack examples are Software Integrity Attacks, Authentication Bypass or Abuse, Privilege Escalation, Authentication Bypass and Exploitation of Session Variables, Resource IDs and other Trusted Credentials.
Legitimate Tool	An attacker manipulates legitimate tools or functions of an application to perform an attack. Attack examples are Abuse of legitimate business processes and Abuse of legitimate channels.
Physical Attack	An adversary conducts a physical attack a device or component, destroying or tampering with it such that it no longer functions as intended.
Web Phishing	Attack patterns within this category focus on the manipulation and exploitation of people over the web.Attack examples are Drive-by Downloads, Watering-Hole attacks, Malvertising and Drive-by Downloads.
Email Phishing	Attack patterns within this category focus on the manipulation and exploitation of people using E-Mails. Attack examples are Spam, Scams, Phishing and Spear-Phishing.
Pretexting	Attack patterns within this category focus on the manipulation and exploitation of people in the interpersonal level. Attack examples are Bribery, Elicitation, Extortion and Influence.
Malware	Malware or malicious software performs undesirable operations such as data theft or some other type of computer compromise. Some of the main types of malware include trojans, viruses, worms and spyware.

ATTACK METHODS

Attack	Description
Command and Control	Malware is a command-and-control channel (botnet). It is the collection of internet Command & Control (C&C) activity refers to communication between a group of infected machines (botnet) and their control server. Activity includes communication of task commands, which can range from keeping control of an Internet Relay Chat (IRC) channel to sending spam emails or participating in DDoS attacks.
Mobile Device Attack	Attack patterns within this category focus on disrupting, gathering sensitive information and gaining access to mobile devices (such as iOS, Android, Windows, etc.). Malware and Phishing are common vectors.
Resource Manipulation	Attack patterns within this category focus on the adversary's ability to manipulate one or more resources, or some attribute thereof, in order to perform an attack. This is a broad class of attacks wherein the attacker can change some aspect of a resource's state and thereby affect application behavior or information integrity. Attack examples are Infrastructure Manipulation, File Manipulation, Registry Manipulation, Remote Code Execution and Cache Poisoning.
Control System Attack	Attack patterns within this category focus on disrupting control system infrastructure, gathering sensitive information or gaining access to control systems (such as ICS endpoints and controllers). Malware and physical attacks are common vectors.
Transaction Terminal Attack	Attack patterns within this category focus on disrupting, gathering sensitive information and gaining access to terminal stations (such as POS, kiosk, ATM, etc.). Malware and physical attacks are common vectors.
Reconnaissance	Activity patterns within this category focus on the collection of information on a target before an attack, and creation of an attack infrastructure (weaponization). The adversary may collect information through a variety of methods including active querying as well as passive observation. Information retrieved may aid the adversary in making inferences about potential weaknesses, vulnerabilities, or techniques that assist the adversary's objectives. This information may include details regarding the configuration or capabilities of the target, clues as to the timing or nature of activities, or otherwise sensitive information. The weaponization stage then includes creating phishing, botnet or other infrastructure from which to launch an attack.

ATTACK METHODS

Attack	Description
Web Application Attack	Attack patterns within this category focus on web/local applications and services. Attack examples include exploitation of a vulnerability or weaknesses in the applications, abusing their APIs, runtime environments, buffer memory or services.
Supply Chain Attack	Attack patterns within this category focus on the disruption of the supply chain lifecycle by manipulating computer system hardware, software, or services for the purpose of espionage, theft of critical data or technology, or the disruption of mission-critical operations or infrastructure. Supply chain operations are usually multi-national with parts, components, assembly, and delivery occurring across multiple countries offering an attacker multiple points for disruption.
Ransomware	Ransomware refers to a type of malware that infects the computer systems of users and manipulates the infected system in a way that the victim cannot (partially or fully) use it and the data stored on it. The victim is usually asked to pay a ransom to regain full access to system and files. In many cases, data exfiltration also takes place and the victim is extorted by threat of making sensitive files public.
Network Attack	Attack patterns within this category focus on the adversary's ability to manipulate one or more network resources, or some attribute thereof, to perform an attack. Attack examples are Protocol Manipulation, Cache Poisoning and DNS Hijacking.
Persistence	After gaining access to a system or network, an attacker will often perform discovery techniques to gain further knowledge about its internal environment and identify further attack options. Discovery is usually accompanied by persistence, whereby an attacker utilizes techniques to maintain a foothold on the system and ensure continued access.

BUSINESS ASSETS

Domain	Description
Business Information	Confidential business information refers to information and data whose disclosure may harm the business. Such information may include business plans, secret information on mergers and acquisitions, new product plans, organization's financial information, etc.
Company Financial Information	Digitized Information that can be considered as the equivalent to money. This data can be resident on some storage device or in transmission over electronic channels. Financial transactions may include wired money transfer, credit card transactions etc.
Customer Financial Information	Client's financial information is an asset held in cash or cash equivalent. That is, monetary assets are assets that can easily be liquidated. Examples include stocks and savings accounts, bank accounts and credit card information.
Brand Reputation	A company's reputation is an asset and wealth that gives that company a competitive advantage because this kind of a company will be regarded as a reliable, credible, trustworthy and responsible for employees, customers, shareholders and financial markets.
Intellectual Property	Intellectual property (IP) is a category of property that includes intangible creations of the human intellect, and primarily encompasses copyrights, patents, trademarks, trade secrets, and product designs. Compromise of IP can result financial, legal or competitive loss.
Customer Personal Information	Any information or set of information relating to a person that identifies such person or could be used to identify such person, including without limitation, a person's name, address, ID number, telephone number, email address or call data records, user-ids and passwords. This information is often used to commit identity fraud.
Supplier Data	Suppliers, contractors or vendors data/Information which is maintained by the organization under a covenant of privacy. Such information may include clients' financial information, client's health information, etc.

BUSINESS ASSETS

Domain	Description
Legal Documents	A document indicating a relationship between the organization and any other organization/individual stipulating expectations and covenants between the two or more parties. Such agreements may include service agreements, service definitions, contracts, SCRs, NDAs, etc.
Employee Data	Data/Information about an employee that is to be maintained confidential between the employee and the employer. Such information may include CV, salary letters, references, personal sensitive information, disciplinary information, pension information, starter mover joiner process.
Customer Services	Various services provided to clients by the organization. These services are revenue generating and/or add value to the organization when operational, or services which the organization is obliged to provide to its client by law. Such services may include online payments, online purchases, government services, support services, etc.
Publicly Available Data	Data about the organization that is publicly advertised.
Business Systems	Core business system (aka mission-critical application) is a software program or suite of related programs that must function continuously in order for a business or segment of a business to be successful. If a mission-critical application experiences even brief downtime, the negative consequences are likely to be financial. In addition to lost productivity, a mission-critical app's failure to function may also damage the business' reputation. For example, CRM, ERP, payment system etc.
Health Information	Any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
Physical Assets	Hardware and physical equipment belonging to the organization or its employees or used as part of the organization's business processes. These include laptops, devices, ATM machines, USB drives, etc.

CYBER INCIDENTS IN SPAIN (JAN 2024 – JUNE 2025)

Incident	Description
Santander Breach Tied to ShinyHunters	On 14 May 2024, Santander confirmed that hackers had accessed a third-party database containing personal information of customers in Spain, Chile, and Uruguay, as well as current and some former employees. The bank emphasized that no online banking credentials or transactional information were compromised, and its systems remain secure. The incident is believed to be linked to a broader cloud-storage breach involving Snowflake, which has also impacted Ticketmaster.[1]
Crocodilus Android Trojan	A new banking trojan named Crocodilus was first identified in March 2025. It targets Android users in Spain and multiple other countries, posing as a fake browser update to infiltrate nearly all major Spanish banks. The malware exploits Accessibility Services to overlay fraudulent login screens and harvest credentials and OTPs. More recent versions have escalated their tactics by injecting fake contacts into victims' address books to facilitate deceptive calls that bypass fraud detection systems. These latest campaigns are distributed via short-lived styled Facebook ads, often viewed by people over 35, showing a strategic focus on financially mature targets.[2]
Crypto Fraud Ring Dismantled in Spain	On 25 June 2025, Spanish authorities, supported by Europol and law enforcement from France, Estonia, and the U.S., broke up a global cryptocurrency investment scam. Five suspects were arrested in Madrid and the Canary Islands. The group is accused of defrauding more than 5,000 victims worldwide and laundering approximately €460 million through shell companies and crypto wallets in Hong Kong, banks, and payment services.[3]
Spanish Municipalities Hit by Ransomware	In late January and early February 2024, Spanish municipalities including Teo (Galicia) and Sant Antoni de Portmany (Ibiza) were hit by ransomware attacks that disrupted public services. In Teo, administrative work and social services were paralyzed, while in Sant Antoni, employees lost access to IT systems, forcing the council to advise citizens to call before visiting offices.[4] Earlier in the same month, on 13 January 2024, the municipality of Calvià (Majorca) was also struck by a ransomware attack. Cybercriminals demanded nearly €10 million, but the council refused to pay, instead setting up a crisis cabinet, suspending administrative deadlines, and beginning recovery efforts.[5]

Source: [1]bbc.com, [2]therecord.media, [3]europol.europa.eu, [4]therecord.media, [5]therecord.media
* Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.

MOST ACTIVE THREAT ACTORS IN SPAIN

Threat Actor	Description
ShinyHunters	A financially motivated cybercriminal group, notorious for high-profile data breaches and mass exfiltration of sensitive user and corporate information. They exploit phishing, SaaS abuse, unsecured cloud repositories, and DevOps credentials to gain access and sell or leak stolen data on underground forums. Their targets span retail, e-commerce, finance, and other high-value sectors.
UNC5537	A financially motivated threat actor actively targeting Snowflake customer database instances by leveraging stolen credentials obtained via infostealer malware. They exploit accounts lacking multi-factor authentication to exfiltrate large amounts of data and then extort victims or sell the stolen data on cybercrime forums.
IntelBroker	A prolific cybercriminal known for orchestrating high-impact breaches and monetizing access. They exploited software vulnerabilities and spear-phishing to extract and sell data before being detained by law enforcement in France early 2025.
Wazawaka	A prolific access broker and ransomware affiliate in the Russian cybercrime ecosystem. He has worked with ransomware groups to enable high-impact attacks via initial access sales. He was arrested in Russia in late 2024 for malware development and ransomware-related offenses.
Odyssey Spider	A threat actor typically targeting hospitality, travel, finance, and sometimes manufacturing sectors. They employ custom multi-stage delivery chains to deploy malware. Their operations emphasize financial gain over espionage or long-term persistence.
Natohub	A self-proclaimed solo hacker responsible for breaches targeting NATO, the U.S. Army, and Spanish government institutions. They leaked thousands of UN and ICAO records on BreachForums before being arrested by Spanish police in early 2025.
Storm-0844	A financially motivated cybercriminal group initially known for distributing Akira ransomware. They gain access mainly by abusing valid accounts, then use freely available tools to perform reconnaissance, lateral movement, exfiltration, and ransom deployment.

Mastercard Cyber Insights Intelligence

To provide visibility into cyber threats, Mastercard continuously monitors thousands of clear, deep and dark web sources to understand and visualize trends in cyber activity globally.

Input from threat intelligence sources in 15+ languages

Mastercard internal CTI feeds	**Open-source threat intelligence**	**Geopolitical reports and articles**
Feeds from security vendors	**Security breach case studies**	**Third-party benchmark reports**
Cybersecurity event alerts	**Regulatory breach notifications**	**Dark web marketplaces**
Threat actor communities	**RSS feeds**	**Cybersecurity Blogs**
Online news sources	**Google "Dorking" alerts**	**Instant Messaging platforms**

Return to Table of Contents

Output

Threat Actors
Actors with the means and motivation to wage cyberattacks and who can be working independently or within resource-rich criminal organizations.

Attack Methods
Known tactics, techniques and procedures used by threat actors during cyberattacks.

Target Industries
An industry or business sector as a potential target for threat agents.

Target Assets
Anything of value to an organization (funds, intellectual property, reputation, employee data, customer data, physical property and infrastructure) that could be of interest to a threat actor.

Regions
Areas of the world where an organization can do business and where threat actors are hosted or focus their attacks.

Cyber Trends
An analysis of the prior period to forecast potential cyber activity in the future.

How the assessment works

Through discovery, observation and analysis of region and sector via external analysis performed by Mastercard's cyber risk monitoring technology, eight security domains were assessed:

- **Software patching**
- **Application security**
- **Web encryption**
- **Network filtering**
- **System reputation**
- **Email security**
- **DNS security**
- **System hosting**

Based on the external assessments, organizations are rated on each of these domains. The assessment reflects the average results of the top 10 organizations in country and sector.

Among these organizations, the average rating of the highest scoring three organizations is shown as best in class, and the average rating of the top 10 organizations is shown as the average for the region. The average results of 10 of the largest organizations in each of the region's countries are also added to provide insight into the scoring of the overall regional industry.

Results illustrate the average performance of the top 10 organizations in the region (across the eight security domains) relative to prior period and organizations operating in the region. Further analysis is provided presenting the risk distribution.

Return to Table of Contents

What we do and don't do

What we do...

- Continuously monitor over 4M companies, 2.9M domains and 33M IP addresses
- Deep mining of domain registration databases
- Deep mining of network registration databases
- Analysis of Internet DNS IP to hostname resolution logs
- DNS queries
- Lightly browse websites, obeying robots.txt instructions
- Analytics of publicly accessible code, content, configurations
- Monitoring and analysis of commercial and open-source IP reputation feeds
- Mining the internet for relevant information such as indicators of data loss events
- Analyze Internet port scan data sourced from a commercial provider

What we don't do...

- Tamper with parameters
- Inject code
- Conduct cross-site scripting
- Conduct SQL injection
- Attempt to bypass authentication
- Execute memory overflow tests
- Fill out form fields
- Guess credentials
- Execute vulnerability exploits
- Attempt to bypass security controls

Return to Table of Contents

Assessment domains

Software Patching

The software patching domain enumerates systems that are running end of life, systems that are unsupported and vulnerable software. This security domain is broken down into four security criteria based on the type of software implementation. The four security criteria within the software patching security domain are as follows:

- **Application Server Patching**
- **OpenSSL Patching**
- **CMS Patching**
- **Web Server Patching**

Application Security

The application security domain assesses each web application for essential, observable application security practices that are leading indicators of the quality of the application security program. This security domain is broken down into five underlying security criteria as described below.

- **CMS Authentication**
- **HTTP Security Headers**
- **External Threat Intelligence Alerts**
- **High-Value System Encryption**
- **Malicious Code**

Return to Table of Contents

Assessment domains

Web Encryption

The web encryption security domain analyzes the effectiveness of encryption implementations, determining if they are properly configured to prevent errors, use secure protocols and apply minimum key lengths necessary to ensure communication privacy. This security domain includes the following security criteria:

- **Certificate expiration date**
- **Certificate valid date**
- **Encryption hash algorithm**
- **Encryption key length**
- **Encryption protocols**
- **Certificate subject**

System Hosting

The system hosting security domain analyses the hosting practices of the organization, enumerating the hosting providers and the countries that systems are hosted in. Systems should be hosted in reputable countries and the host country data privacy laws should be obeyed. High fragmentation of hosting with many hosting providers is a leading indicator of gaps in IT governance. The system hosting security domain provides measurement of system hosting practices across the security criteria listed below:

- **Cotenant IP Hosting**
- **Hosting Fragmentation**
- **Hosting Geolocations**

Return to Table of Contents

Assessment domains

System Reputation

The system reputation security domain enumerates systems owned by the organization that appear in reputable intelligence sources to provide insights if systems appear to be compromised or are exhibiting malicious behavior. This domain is broken down into the following control criteria:

- **Command and control servers**
- **Botnet hosts**
- **Hostile hosts: hacking**
- **Hostile hosts: scanning**
- **Phishing sites**
- **Other blacklisted hosts**
- **Spamming hosts**

Email Security

The email security domain assesses the use of authentication and encryption controls necessary to ensure that email messages are not spoofed and that communications are private. The domain also enumerates the email hosting providers, providing visibility into email hosting provider practices and fragmentation. The email security domain includes the criteria and measurements listed below.

- **Email Authentication (SPF or DKIM)**
- **Email Encryption (STARTTLS)**
- **Email Hosting Providers**

Return to Table of Contents

Assessment domains

DNS Security

The DNS security domain assesses the use of controls to prevent unauthorized modification of domain records resulting in domain hijacking. This domain also enumerates the DNS hosting providers to determine the level of fragmentation. The underlying security criteria for this security domain are as follows:

- **DNS Hosting**
- **Domain Hijacking Protection**

Network Filtering

The network filtering security domain analyzes if internet- accessible systems and network services are strictly limited to those that are necessary and if they have security controls sufficient to reasonably ensure confidentiality, integrity and availability. Every internet-facing system and its network services are constantly probed for vulnerabilities to gain unauthorized access to the system or degrade system performance.

Deployment of unsafe and unnecessary network services increases the likelihood of a system compromise. The underlying security criteria for this security domain are as follows.

- **Unsafe Network Services**
- **IoT Devices**

Return to Table of Contents

SOURCES OF INFORMATION

Reference	Source
1	Mastercard Cyber Insights strategic threat intelligence data
2	Mastercard RiskRecon external analysis data
3	Mastercard processed data for transaction decline and fraud activity
4	External sources

Associations, Interest Groups & Research Institutes

Spain Security Board (KSÖ): https://kuratorium-sicheres-oesterreich.at

Spain Trust Circle (ATC): https://Spainntrustcircle.at/

KIRAS Security Research: https://www.kiras.at/en

Spain Institute of Technology (AIT): https://www.ait.ac.at

SBA Research: https://www.sba-research.org

Association of Spain Software Industry (VÖSI): https://voesi.or.at/home-en

Cyber Security Spain (CSA) Association: https://www.cybersecuritySpain.at

Regulatory Links

Federal Chancellery (BKA) - Cyber Security Platform (CSP) & Cyber Security Steering Group (CSS): https://www.bundeskanzleramt.gv.at

Ministry of Interior (BMI) - Federal Criminal Police Office (BK) & Cyber Crime Competence Center (C4): https://www.bundeskriminalamt.at/en

Online Security Portal: https://www.onlinesicherheit.gv.at

CERT Overview: https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/CERTs.html

Statement of Confidentiality and Disclaimer

Information in this presentation or in any report or deliverable provided by MasterCard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both MasterCard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.