

# SPAIN

## Threat Landscape Report



**SOC**Radar<sup>®</sup>

**a3Sec**

August 2022







# TABLE OF CONTENTS

**03 | Executive Summary**

**04 | Key Findings**

**05 | Deep Web Threats**

**06 | Major Dark Web Posts**

**08 | Ransomware Threats**

**09 | Top Ransomware Gangs**

**13 | State-Sponsored APT Activities**

**15 | Phishing Treats**

**16 | Critical Asset Exposures & Vulnerabilities**

**18 | Credentials & Stolen Data Intelligence**

**19 | DDoS**



# EXECUTIVE SUMMARY

SOCRadar Threat Landscape Report provides organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions. The intelligence provided in this report can help plan enterprise-wide security programs, make investment decisions, and define cybersecurity requirements.

SOCRadar characterizes the threat landscape based on recently observed threat actor activities, malware campaigns, recent critical vulnerabilities, exploits, data gathered from open threat sharing platforms, and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities of SOCRadar Platform.

Organizations could consider cyber security solutions to overcome this rise in cyberattacks. This landscape report of Spain provides a comprehensive guide, and a collection of data related to cyberattacks in the country, within the past 12 months.

Within the last years, the number and frequency of various cyberattacks throughout Spain have increased. The Spanish National Institute of Cybersecurity says the country has suffered more than 150,000 cyber-attacks since the beginning of the Covid-19 pandemic. The same research shows that one in six companies has suffered a cybersecurity incident. One reason for this increase could be the action of digital transformation with Covid-19 that the world has been dealing with for previous years.

64 % of Spanish companies paid for a ransom after a ransomware cyberattack (data hijacking) in 2021, according to data from the insurer Hiscox. The average cost of this ransom was 19,400 Euros and what companies spent to recover from the attack was 10,771 Euros. Despite this outlay, almost half of the companies that paid (47%) suffered another cyberattack. Beyond ransomware, 51% of Spanish companies were cyberattacked.

The National Center for Critical Infrastructures (CNPIC) and the Cybersecurity Coordination Office (OCC), both Ministry of the Interior, neutralized more than 10,000 cyberattacks of varying intensity on essential services during 2021.





## KEY FINDINGS

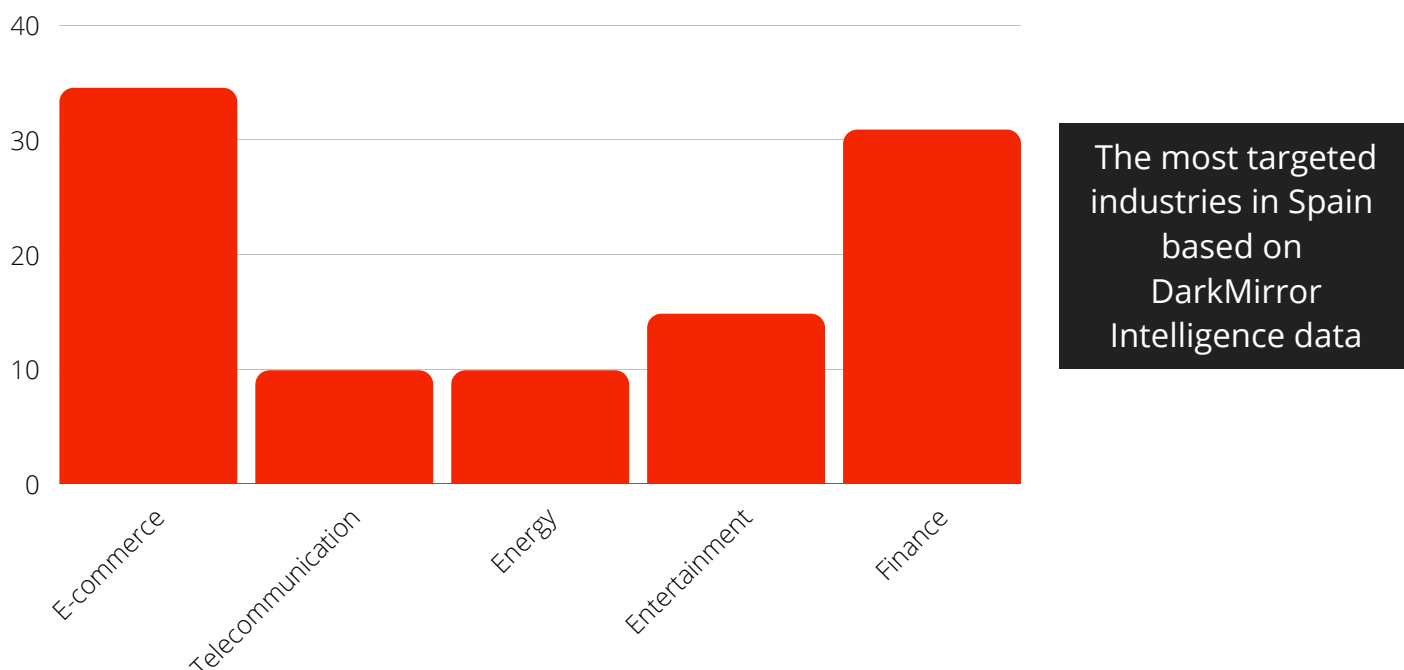
- SOCRadar DarkMirror Intelligence data show that past 12 months, threat actors have preferred the **e-commerce and finance industries** by a vast difference among organizations.
- Top ransomware gangs targeting Spain are "**LockBit 3.0, Conti, and AlphVM Blackcat**".
- Data from SOCRadar's platform shows that almost **90 % of Spanish organizations were compromised in at least one successful cyberattack in the past year.**
- **APT groups from China and Iran** have recently targeted leading organizations in the government, information technology, and finance sectors.
- SOCRadar has detected **1,800 phishing attacks** targeting Spain since the beginning of 2021.
- **More than 15 million customers' data were hacked** in cyberattacks in the first six months of 2022.
- Spain has been in several APT groups, **mainly affiliated with Russia and North Korea.**
- According to SOCRadar's data, **approximately 71 % of all phishing attacks were in HTTPS protocol. Registered phishing domains had valid certificates.**
- In June 2022, SMB Authentication was disabled on **approximately 20 % of SMB ports belonging to Spanish organizations.**
- **Madrid** was the city most affected by DDoS attacks in 2022. The most affected company was **Telefonica de Espana.**
- **79,050 Spanish users have been infected** with Stealer (Redline Raccoon, etc.).
- The most exposed credential information from Spain is **"amazon.es" in 2022.**



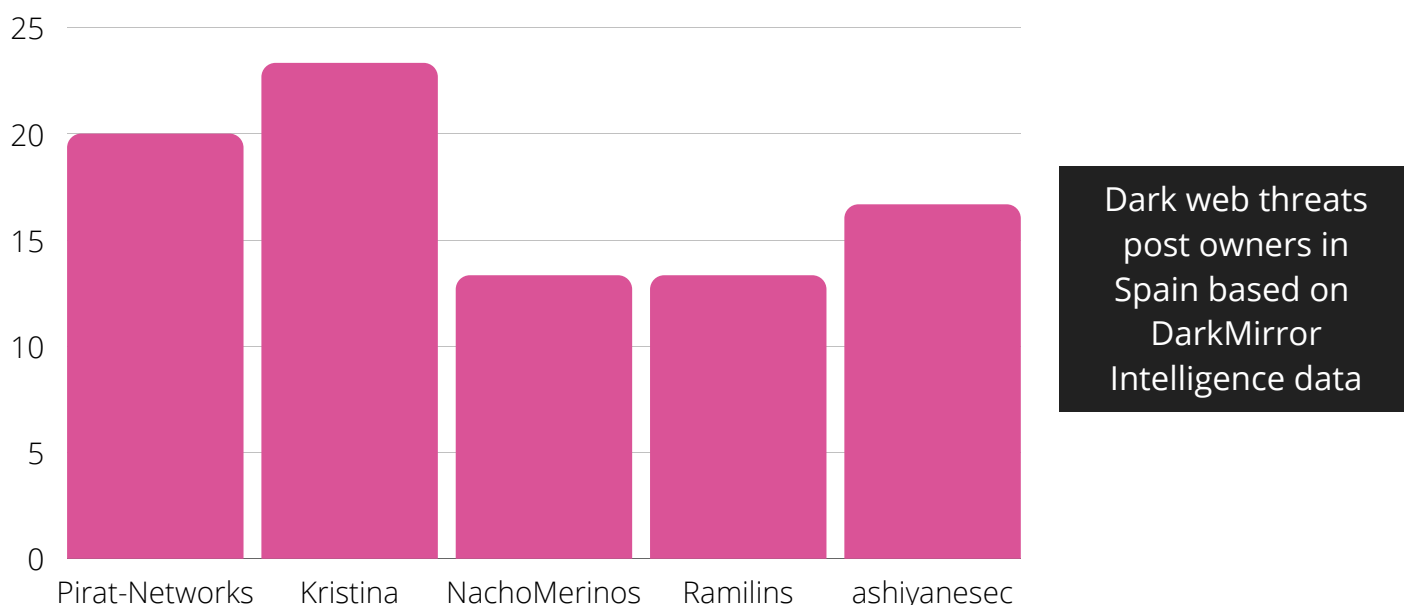
## Dark Web Threats

SOCRadar DarkMirror Intelligence data show that past 12 months, **threat actors have preferred the e-commerce and banking sectors by a vast difference among organizations**. E-Commerce has 34.5 % of the dark web threats in this sector, while finance has 30.9 %.

Other sectors, **telecommunication, energy, media, and entertainment, are 34.57 %**. This shows that Spanish banking and e-commerce companies are almost three times more at risk of getting hit by threat actors.



SOCRadar DarkMirror Intelligence data provide an overall perspective with the statistics of the dark web post owners related to the organizations in Spain. The threat actor called **"Kristina" is the most prominent dark web threats post owner related to Spain-based companies**, with a percentage of 23.33 %, and Pirat-Networks follow this with 20 %.





# Major Dark Web Posts

**SELLING** SPAIN Residential-landline: Database -14 million records  
- 2 hours ago

HELLO COMMUNITY,  
TODAY, I'M SELLING SPAIN Residential-landline- Database -14 million records

✓ CONTENTS:

Quote:

Name	Address	Zip Code	City	Province	Country	Phone
Moreno Aparicio Rafael S. Isidro,	Utiel	VALENCIA	SPAIN	34-962.1		
Martínez Castellanos Jose Miguel S. Isidro,	Utiel	VALENCIA	SPAIN	34-961.4		
Miota Hernandez Amparo S. Isidro,	Utiel	VALENCIA	SPAIN	34-962		
Moratalla Moya Luis Javier S. Isidro,	S/N 40000	Massalfassar	VALENCIA	SPAIN	34-961	
Mec Sponsorship Worldwide S.L. S. Jacinto,	1	Valencia	VALENCIA	SPAIN	34-963	
Maldonado Franco Jesus S. Jacinto,	1	Valencia	VALENCIA	SPAIN	34-963	

✓ DELIVERY : TELEGRAM OR MEGA.NZ

✓ PAYMENT : BTC - USDT - ETH

✓ ESCROW ACCEPT

✓ DATA PRICE = 600 USD

Residential database of 13 Million people in Spain is on sale

**Spanish Gas Supply (VNC)**  
13 minutes ago

Forums > Main \ main content > Data base & leakage \ Data base & leakage

13 minutes ago

VNC

Country:Spain  
IP:2  
PORT:  
Password:m  
Service:Gas Supply

Unauthorized VNC Access Sharing is detected for a Spanish gas supply company (March 2022)

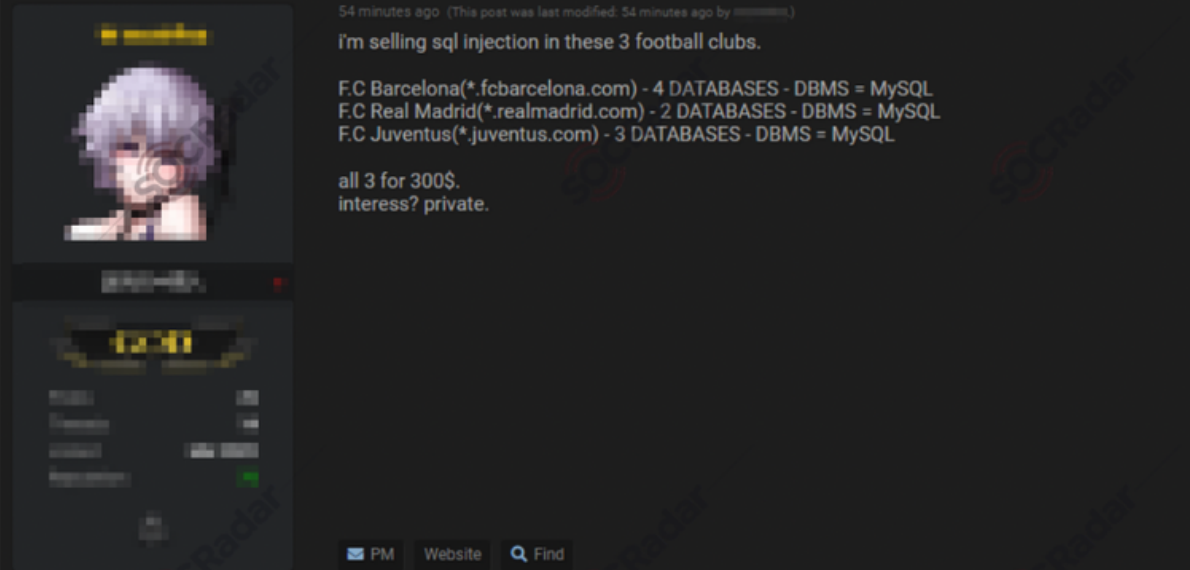
Power Company Iberdrola Admits Personal Details of 1.3 Million Customers were Hacked (March 2022)

Personal data of 1.3 million Iberdrola customers were hacked in a cyberattack on March 15. The criminals breached information from Iberdrola, including credentials. According to police, threat actors did not access bank account details or information about the client's use of energy.

# Major Dark Web Posts

## Football Clubs

by [redacted] - Wednesday May 4, 2022 at 07:25 AM



54 minutes ago (This post was last modified: 54 minutes ago by [redacted])

i'm selling sql injection in these 3 football clubs.

F.C Barcelona(\*.fcbarcelona.com) - 4 DATABASES - DBMS = MySQL  
F.C Real Madrid(\*.realmadrid.com) - 2 DATABASES - DBMS = MySQL  
F.C Juventus(\*.juventus.com) - 3 DATABASES - DBMS = MySQL

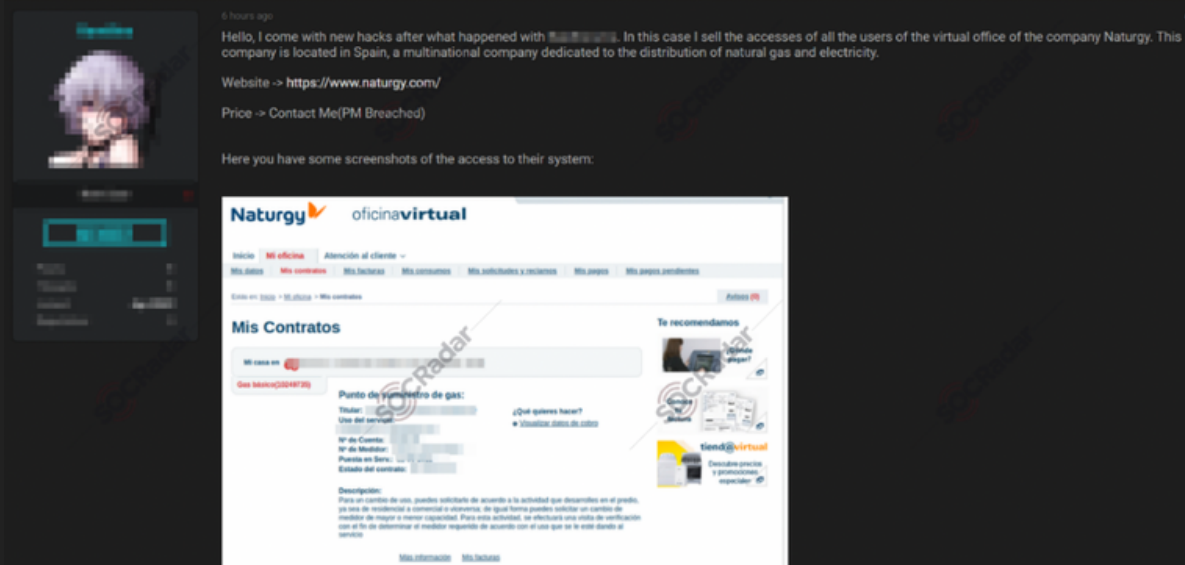
all 3 for 300\$.  
interest? private.

PM Website Find

SQL injection for various football clubs is on sale (May 2022)

## HACKED: Naturgy.com Access Virtual Office

by [redacted] - Thursday March 31, 2022 at 02:32 AM




6 hours ago

Hello, I come with new hacks after what happened with [redacted]. In this case I sell the accesses of all the users of the virtual office of the company Naturgy. This company is located in Spain, a multinational company dedicated to the distribution of natural gas and electricity.

Website -> <https://www.naturgy.com/>

Price -> Contact Me(PM Breached)

Here you have some screenshots of the access to their system:



The screenshot shows the 'oficinavirtual' interface of Naturgy. It includes a navigation bar with links like 'Inicio', 'Mi oficina', 'Atención al cliente', 'Mis datos', 'Mis contratos', 'Mis facturas', 'Mis consumos', 'Mis actividades y recargas', 'Mis pagos', and 'Mis pagos pendientes'. The main content area is titled 'Mis Contratos' and shows details for a gas contract, including the point of delivery, user information, and a description of the service.

Unauthorized Network Access Sale is detected for all the users of the virtual office of the company Naturgy (March 2022)

## Cyber Attack on Municipal IT Service Providers in Spain (May 2022)

ANIMSA is owned by 179 local units in the autonomous region of Navarre in northern Spain. Numerous services in 137 municipalities and in 35 other organizations are affected by the attack. Several municipalities in Navarra continue without electronic services after a cyberattack. Services such as email, municipal websites or electronic offices do not work. The public company that owns the local entities is working so that the recovery of services occurs as soon as possible.

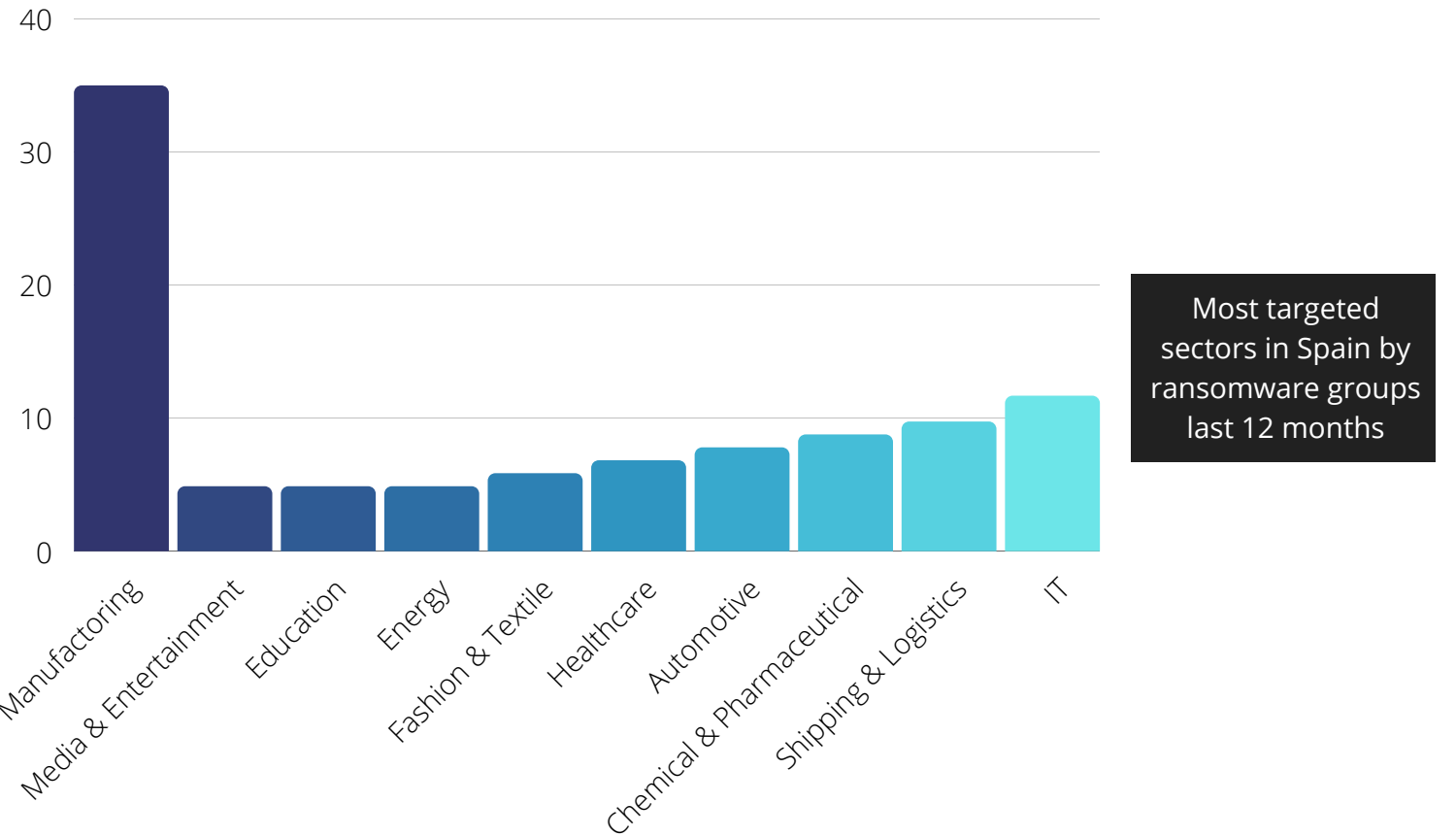


# Ransomware Threats

The general purpose of ransomware attacks is to make money by forcing the victim to pay a ransom. But most ransomware attacks have other damaging consequences, such as data leaks through "sensitive data loss and double extortion attacks" or prolonged disruption of the victim company's services. For these reasons, ransomware attacks have become one of the most valuable tools threat actors use to target government agencies, companies, and critical infrastructure.

On the 25th of May, 2022, the popular ransomware gang LockBit2.0 announced a new ransomware victim, Hospital San José, a private hospital located in the Canary Islands. This shows us that ransomware gangs do not hesitate to target companies providing critical services, such as hospitals.

SOCRadar detected nearly 150 ransomware attacks targeting Spanish organizations last year. Spanish organizations have suffered in the previous year resulting in the leaking of sensitive data belonging to the victim companies. This shows us that 64 % of the victims complied with the threat actors' requests and decided to pay the ransom, whereas approximately one-third of the victims opted not to pay the ransom.



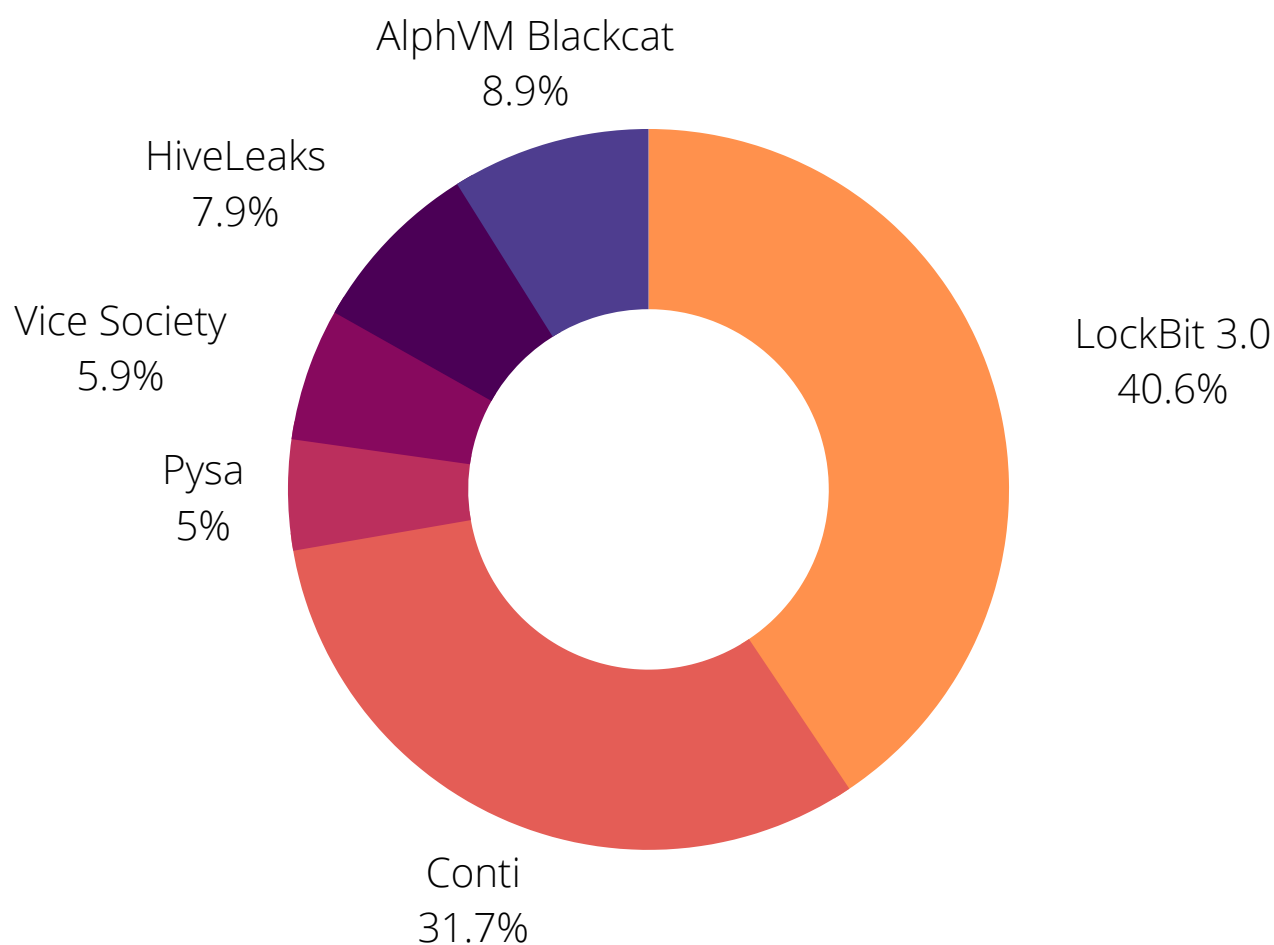
According to data from SOCRadar's DarkMirror, the top three most targeted verticals in Spain were Manufacturing, Information Technologies, and Shipping & Logistics. In addition to these sectors, ransomware gangs have been targeting Spanish companies in many other industries, such as the Automotive and Healthcare sectors.





## Top Ransomware Gangs

The top three most active ransomware gangs targeting Spanish organizations are **LockBit 3.0**, **Conti**, and **AlphVM Blackcat**. LockBit 3.0 and Conti's gangs are responsible for over half of all ransomware attacks targeting Spanish companies in the last year, with more than 70 successful attacks from six different gangs. Below, you can see the most active ransomware gangs targeting Spanish companies.



Distribution of  
ransomware gang  
activities targeting Spain  
last 12 months



## LockBit 3.0

- Ransomware-as-a-service (RaaS) operator.
- Has one of the best-designed locker algorithms regarding encryption speed and overall functionality.
- The gang declared a newer version would come with upgraded functionalities and better capabilities: LockBit 3.0.

### MITRE TTPs

#### Initial Access

T1078 Valid Accounts

T1190 Exploit Public-Facing Application

#### Execution

T1047 Windows Management Instrumentation

T1059 Command and Scripting Interpreter

T1059.003 Windows Command Shell

#### Persistence

T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

#### Privilege Escalation

T1055 Process Injection

#### Defense Evasion

T1055 Process Injection

T1070.004 Indicator Removal on Host: File Deletion

T1112 Modify Registry

T1497 Virtualization/Sandbox Evasion

#### Credential Access

T1056.004 Credential API Hooking

T1110 Brute Force

#### Discovery

T1012 Query Registry

T1018 Remote System Discovery

T1057 Process Discovery

#### Lateral Movement

T1021 Remote Services

T1021.001 Remote Services: Remote Desktop Protocol

T1021.002 Remote Services: SMB/Windows Admin Shares

#### Collection

T1056.004 Credential API Hooking

#### Command and Control (C2)

T1090.003 Proxy: Multi-hop Proxy

#### Exfiltration

T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

#### Impact

T1486 Data Encrypted for Impact

T1490 Inhibit System Recovery



## Conti

- Ransomware-as-a-service (RaaS) operator, operating out of Russia.
- Conti is one of the most active ransomware gangs, actively targeting enterprises worldwide.
- After the gang's stand in the cyber-crisis between Russia and Ukraine, their internal chats and locker source code were leaked by a Ukrainian hacker who previously has gained access to Conti's internal systems.
- Conti ransomware group shut down its cybercrime operations in June 2022.

### MITRE TTPs

T1016 System Network Configuration Discovery  
T1018 Remote System Discovery  
T1021.002 Remote Services: SMB/Windows Admin Shares  
T1027 Obfuscated Files or Information  
T1049 System Network Connections Discovery  
T1055.001 Process Injection: Dynamic-link Library Injection  
T1057 Process Discovery  
T1059.003 Command and Scripting Interpreter: Windows Command Shell  
T1078 Valid Accounts  
T1080 Taint Shared Content  
T1083 File and Directory Discovery  
T1106 Native API  
T1110 Brute Force  
T1133 External Remote Services  
T1135 Network Share Discovery  
T1140 Deobfuscate/Decode Files or Information  
T1190 Exploit Public Facing Application  
T1486 Data Encrypted for Impact  
T1489 Service Stop  
T1490 Inhibit System Recovery  
T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting  
T1566.001 Phishing: Spearphishing Attachment  
T1566.002 Phishing: Spearphishing Link  
T1567 Exfiltration over Web Service





## AlphVM BlackCat

- First disclosed in November 2011.
- Actively recruits ex-REvil and ex-BlackMatter members.
- The group's locker is written in Rust programming language, unlike other popular ransomware lockers.

### MITRE TTPs

T1027.002 – Obfuscated Files or Information: Software Packing

T1027 – Obfuscated Files or Information

T1007 – System Service Discovery

T1059 – Command and Scripting Interpreter

TA0010 – Exfiltration

T1082 – System Information Discovery

T1490 – Inhibit System Recovery

T1485 – Data Destruction

T1078 – Valid Accounts

T1486 – Data Encrypted For Impact

T1140 – Encode/Decode Files or Information

T1202 – Indirect Command Execution

T1543.003 – Create or Modify System Process: Windows Service

T1550.002 – Use Alternate Authentication Material: Pass the Hash

DIVE INTO THE  
DEEP WEB



**DARK MIRROR**



# State-Sponsored APT Activities

State Sponsored APT groups are another type of threat actor posing a significant threat to companies, government organizations, and critical infrastructures. Unlike ransomware gangs, APT groups are not financially motivated. They aim to carry out their nation's malicious cyber objectives.

Spain has been in the scope of several APT groups, mainly affiliated with Russia and North Korea. Spanish organizations have been affected by the cyber attacks carried out by these Advanced Persistent Threat groups.

## Significant APT Groups

- Carbon Spider
- Stardust Collima
- Cozy Bear
- Twisted Spider
- Doppel Spider
- Labryrinth Collima
- Fancy Bear
- Pinchy Spider
- Venomous Bear
- Wizard Spider

**SOCRadar collects Advanced Persistent Threat (APT) IOC Feeds from several public and private sources and sensors. These feeds are free and refreshed daily.**



**DOWNLOAD**



## Top 5 Malware

Spanish companies have been bombarded with cyberattacks in the last year, and threat actors are exploiting common vulnerabilities and utilizing malware to achieve their goals. Below, you can see the top 5 malware targeting Spain in June 2022.

1	Trojan-Ransom.Win32.GenericCryptor.pref	23,83%
2	Trojan-Ransom.JS.Alien.gen	11,57%
3	Trojan-Ransom.Win32.Crypren.gen	8,56%
4	Trojan-Ransom.Win32.Crymodng.gen	7,98%
5	Trojan-Ransom.Win32.Gen.gen	5,68%

## Top 5 Exploits

Below you can see the top 5 exploits in Spain in June 2022.

1	Exploit.MSOffice.CVE-2018-0802.gen	37,05%
2	Exploit.Win32.CVE-2010-2862.a	17,14%
3	Exploit.MSOffice.CVE-2017-11882.gen	14,71%
4	Exploit.HTTP.CVE-2017-5638.gen	7,56%
5	Exploit.OLE2.Wahel.a	7,09%





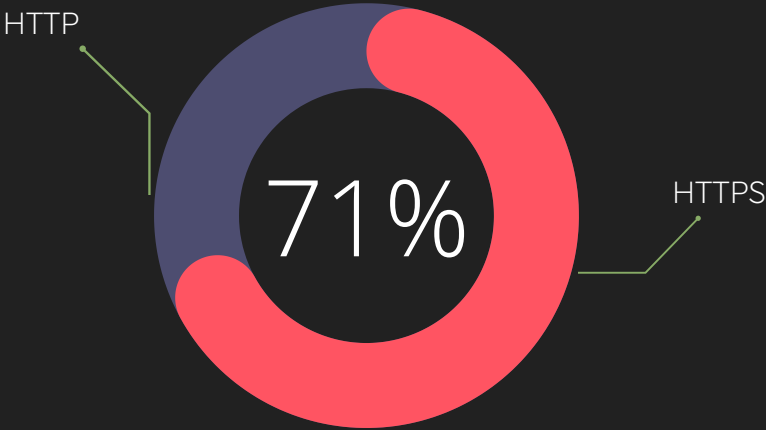
# Phishing Threats

Phishing is a great social engineering attack to lure victims into directly submitting the threat actor their sensitive credentials, which could be leveraged to gain initial access into a company's cyber infrastructure. Also, it is unsurprising that phishing attacks linked to this year's tax return will increase.

According to intelligence SOCRadar provides, there were **more than 1,800 phishing attacks targeting Spanish companies last 12 months**. Below, you can see the top three sectors with the most phishing attacks in Spain.



According to data from SOCRadar, **about 71% of all phishing websites** now use the HTTPS protocol. Attackers were increasingly using HTTPS to entice their victims to click on malicious links.



Search Your Domain On

Phishing Radar

Enter your domain



## Critical Asset Exposures & Vulnerabilities

Attack Surface Management (ASM) and Vulnerability Management are two crucial aspects of a company's security posture. Poor ASM and Vulnerability Management results in critical cyber attacks, so it is essential to consider and implement effective ASM and VM solutions. As of June 2022, Spain had more than 4 million open ports, some of which were Remote Desktop Protocol (RDP) ports (approximately 24 thousand open RDP ports were found on the 11th of June, 2022).

Open RDP ports pose a significant threat to companies with compromised credentials or brute force attacks since threat actors can remotely access a company's network through RDP protocol. Critical Asset Exposure is a significant consideration in building a strong security posture.

In June 2022, SMB Authentication was disabled on approximately 20 % of SMB ports belonging to Spanish organizations. In addition, even though the following vulnerabilities were patched for a long time, there were 2,553 hosts vulnerable to Heartbleed (CVE-2014-0160) and 54 hosts vulnerable to EternalBlue (CVE-2017-0144), and 1,094 hosts vulnerable to BlueKeep (CVE-2019-0708).

Attackers could exploit these vulnerabilities; as a result, Spanish companies could suffer significant losses from critical cyber-attacks. If the number of Remote Code Execution vulnerabilities is high, there will be an increased number of ransomware attacks affecting Spanish enterprises. Apart from these long-before-patched vulnerabilities, in the last year, Spanish companies have suffered cyber-attacks that stemmed from other significant vulnerabilities threat actors exploited.

	Vulnerable Hosts	CVE ID	CVSSv3
46,316	Path Traversal	CVE -2018-19052	CVSS: 7.5
42,008	Improper Authentication	CVE -2018-1312	CVSS: 9.8
41,016	Use of Incorrectly-Resolved Name or Reference	CVE-2021-34523	CVSS: 5.3
38,812	Incorrect Permission Assignment for Critical Resource	CVE-2017-15906	CVSS: 5.3
34,429	Session Fixation	CVE-2018-17199	CVSS: 7.5
34,363	Improper Restriction of Operations within the Bounds of a Memory Buffer	CVE-2017-7679	CVSS: 9.8
31,505	Improper Input Validation	CVE-2017-15715	CVSS: 8.1



Product	Host Count	TOP CVEs
AkamaiGHost	29,3621	CVE-2018-1312 CVE-2019-0220 CVE-2018-17199 CVE-2017-7679 CVE-2016-8612 CVE-2017-15710 CVE-2017-15715 CVE-2018-1283 CVE-2016-4975 CVE-2017-9798
Apache httpd	17,3127	CVE-2019-9637 CVE-2019-9638 CVE-2019-9639 CVE-2019-9641 CVE-2018-19935 CVE-2018-19395 CVE-2018-19396 CVE-2019-9020 CVE-2019-9021 CVE-2019-9023
nginx	14,7670	CVE-2017-15906 CVE-2018-15919 CVE-2016-10708 CVE-2014-1692 CVE-2016-0777 CVE-2014-2653 CVE-2016-0778 CVE-2014-2532
OpenSSH	10,7275	CVE-2013-4548
MikroTik bandwidth-test server	67,392	CVE-2015-0204 CVE-2015-4000 CVE-2017-10140 CVE-2020-12063 CVE-2008-2936 CVE-2011-1720 CVE-2012-0811
Postfix smtpd	64,674	CVE-2018-19052 CVE-2019-11072 CVE-2014-2323 CVE-2014-2324 CVE-2013-4559 CVE-2013-4560 CVE-2013-4508 CVE-2012-5533 CVE-2015-3200 CVE-2011-4362
lighttpd	56,768	CVE-2014-4078 CVE-2010-1899 CVE-2010-2730 CVE-2010-3972 CVE-2009-4445 CVE-2008-1446 CVE-2009-2521 CVE-2009-4444 CVE-2015-1635
Microsoft IIS httpd	41,033	CVE-2014-0160
Hikvision IP Camera	40,219	CVE-2015-0204





## Credentials & Stolen Data Intelligence

Using stolen credentials is one of the most common initial access techniques leveraged by your adversaries. C-level certificates are significantly more helpful for BEC attackers. Last year, **SOC Radar detected more than 1 billion exposed credentials by analyzing the breach datasets shared on the deep and dark web forums**, which are tied to plain-text passwords.

Password reuse is continuing to be a concern for security professionals. It becomes a bigger problem when it merges with the lack of MFA mechanisms. Ransomware and APT actors continuously seek access to sensitive information, intellectual property, confidential business data through stolen identities.

179,050 Spanish users have been infected with Stealer (Redline Raccoon, etc.). Two million twenty-seven thousand four hundred ninety credentials that access ".es domains" have been leaked from the users and distributed on the dark and deep web during the last 12 months.

### Top Leaked es. Domains:

- amazon.es
- us.es
- ebay.es
- orange.es
- plus.es
- vodafone.es

**CHECK FOR ACCOUNT BREACH**

Enter your domain/email

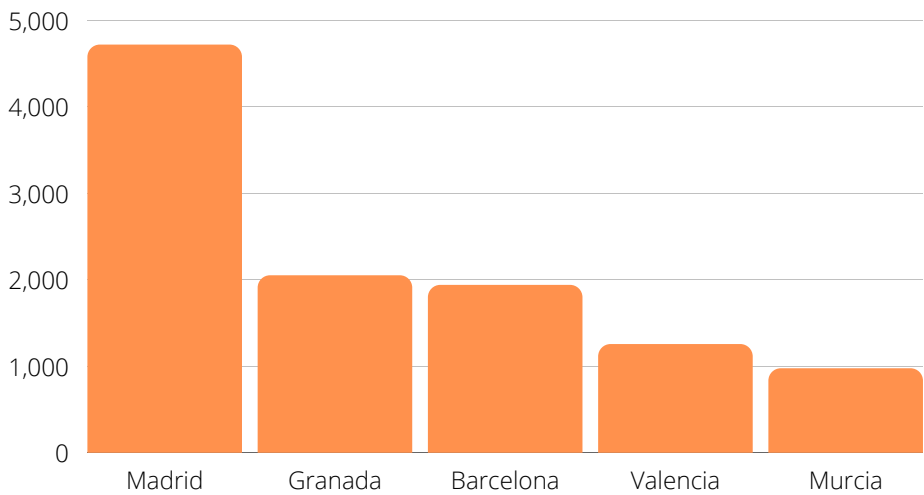




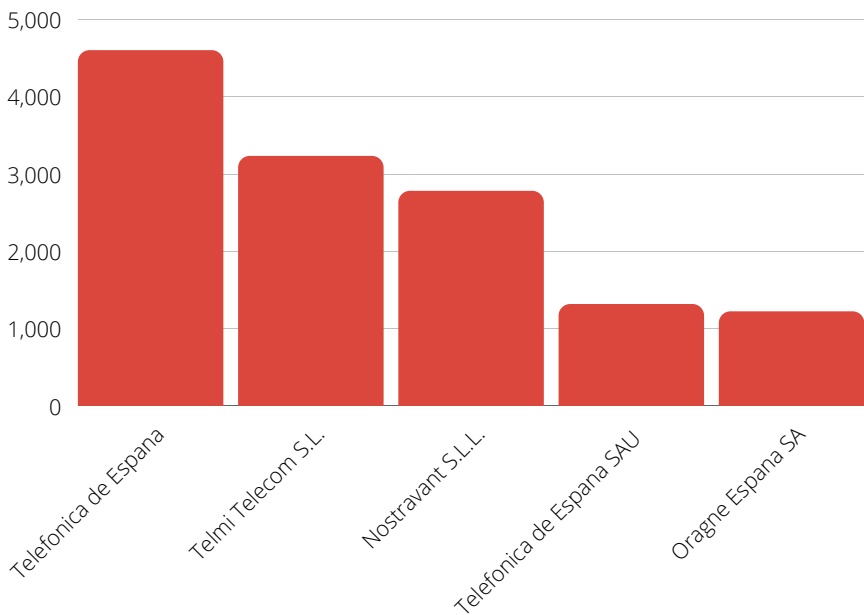
# DDoS

The global internet ecosystem is currently vulnerable and carrying high malicious traffic. Sophisticated threat actors, including ransomware gangs, exploit these potential vectors to amplify disruptive DDoS attacks against organizations, resulting in financial losses and numerous critical service outages worldwide.

## Top Cities Effectuated From DDoS Attacks



## Top Organizations Effectuated From DDoS Attacks



## DDoS Attacks from Spain

32,484

"Recursion: Enabled" Devices  
"Recursion: Enabled" Devices

84

"UPnP Enabled" Devices



## DDoS Attacks to Spain

Started	Events	Duration	ISP
12-06-2022 15:54	5,669	5 min	Orange Espagne SA
12-06-2022 15:15	5,065	5 min	Telefonica De Espana
12-06-2022 14:29	4,949	13 min	Xtra Telecom S.A.
12-06-2022 14:25	4,233	3 min	ServiHosting Networks S.L.
12-06-2022 12:05	3,5491	2 hours 15 min	ServiHosting Networks S.L.
12-06-2022 13:51	6,480	7 min	ServiHosting Networks S.L.
12-06-2022 12:32	3,877	9 min	Cogent Communications
11-06-2022 22:05	36,5158	8 hours 28 min	Vodafone Spain
11-06-2022 22:10	79,363	4 hours 4 min	Telefonica De Espana
29-05-2022 23:10	10,720	1 hour 14 min	Orange Espagne SA
25-05-2022 5:39	17,318	1 hour 22 min	Orange Espagne SA
01-02-2022 0:21	83,1771	17 hours 45 min	COLT Technology Services Group Limited
08-02-2022 4:26	46,517,981	41 days 4 hours 8 min	Cogent Communications





# ABOUT SOCRadar®

SOCRadar provides an early warning system with an extended threat intelligence platform. Extended Threat Intelligence (XTI) tool that is enriched with External Attack Surface Management and Digital Risk Protection. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with strong AI algorithms and a highly talented analyst team, together they eliminate false positives.

FOLLOW US!



If you have a business in Spain and want to benefit from the solutions offered by SOCRadar, you can contact our valued partner:

## a3sec

C/ Aravaca, 6 2ª Planta 28040 Madrid,  
Spain  
Phone:  
+34 915330978

## DISCOVER SOCRADAR® FREE EDITION

**With SOCRadar® Free Edition, you'll be able to:**

- Discover your unknown hacker-exposed assets
- Check if your IP addresses tagged as malicious
- Monitor your domain name on hacked websites and phishing databases
- Get notified when a critical zero-day vulnerability is disclosed

TRY FOR FREE



CONTACT US



info@socradar.io



+1 (571) 249-4598



651 N Broad St, Suite 205,  
Middletown, DE 19709