COUNTRY REPORT · BRANDEFENSE COUNTRY REPORT · SPAIN 2026 · TLP:CLEAR · 80 MIN READ

Brandefense Spain Cyber Threat Landscape Report 2026

Customer data, extortion and bank-account fraud in a large, digital economy

BY
Odin by Brandefense

REVISED
21 November 2026

READING TIME
80 min read

EDITION
Version 1.0 · Public Research Edition · TLP:CLEAR

RESEARCH WINDOW
1 January–20 November 2026

163 of 250
organisations had a credential listed for sale on the day of the check

87%
of posts tagged Spain came from one Turkish-language bot family

30
incidents involving Spanish organisations or customers, confirmed by the organisation or an authority

220
ransomware leak-site listings for Spain, 1 January–20 November 2026

CONTENTS

01 Executive summary
Report map
02 Spain's digital and threat context
03 National exposure: 250 leading organisations
04 What we see on the dark web
05 Confirmed incidents and claims by sector
06 Hacktivism and DDoS
07 Threat actors
08 The fraud economy
09 Banking and finance deep dive
10 Regulatory and national response
11 Outlook
12 Action plan
A Appendix A. Method
B Appendix B. Evidence register
C Appendix C. Sources
D Appendix D. Glossary
About this report

CHAPTER 1

Executive summary

01

THIS CHAPTER ANSWERS

What happened in 2026, what matters most for Spanish organisations, and what should leaders decide first?

4

decisions for leaders, each tied to evidence in the chapters

INSIDE THIS CHAPTER

Four decisions for leaders | The year in numbers

IN SHORT

Spain's 2026 picture is about customers' data and money. Large consumer brands confirmed customer-data incidents, and four confirmed incidents began at a supplier. Extortion groups posted 220 Spanish listings by 20 November, more than in all of 2025, as in neighbouring countries. The most-advertised underground product is bank accounts used to move fraud proceeds. A pro-Russian DDoS wave in February was loud but short. Act in this order: validate current credential listings, hold suppliers to breach-notice terms, then harden transfers and DDoS response.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 932,584 posts tagged as concerning Spain. Of these, 87% come from one Turkish-language bot family, and the cleaned range is 58,657-62,086 relevant posts. It also supplied infected-device and credential records for 250 selected organisations. Card material that appeared in clear text in posts comes from the same source. **Ransompedia** supplied ransomware leak-site listings for Spain and three comparators. **Atlas** exposure ratings were computed for the 250 organisations. These are separate populations and are never added together.

1. Extortion listings rose, in line with the region, and spread across many groups. Ransompedia holds 220 accepted Spanish listings dated 1 January-20 November 2026, already more than the 157 for the whole of 2025. Portugal, Italy and France also passed their full-year 2025 totals within the same partial year, by wider margins, so the rise does not look Spain-specific. Qilin (49), The Gentlemen (26) and Deadlock (14) lead, but 50 other group names account for 60% of listings. Town halls, a regional government, universities and a hospital were named; several confirmed an incident, others did not. A listing is a claim, not proof of encryption or theft. [S1]

2. Identity exposure is near-universal in the 250 organisations we assessed. Of them, 241 have infected-device associations, at least 1.2 million in total. And 243 have historical credential records, 11.6 million in all. In all, 163 of 250 organisations had a credential listed for sale when checked. Most device associations are outside the employee classification, most plausibly customers' own devices that logged in to a brand's site, though ownership is not established. [S2][S3]

3. Consumer brands confirmed customer-data incidents, some through suppliers. Organisations or authorities confirmed 30 incidents involving Spanish organisations or customers. Endesa (January) and Naturgy (May) exposed identification, contact and, for some customers, bank details. After the Adif and Renfe intrusion (September), Renfe told customers that ID numbers, hashed passwords and trips may have been exposed. Four of the 30 started at a current or former provider. Attackers' figures, such as "20 million people", were not confirmed. [S4][S5][S6]

4. Bank-account trading is the most-advertised crime family. After cleaning, bank and payment-account trading is the largest share of Spain posts (about 37%), ahead of cards, data leaks and identity documents. Post counts measure advertising, not the value of the trade. Spanish-language channels sell ready-made accounts, money "loads" and mule accounts. Police dismantled several bank-impersonation and money-laundering networks in 2026. [S3][S7][S8]

5. A pro-Russian DDoS wave hit public sites in February; recruitment followed. NoName057(16) and Server Killers claimed attacks on central-government and ministry websites, a regional parliament, councils and transport sites on 16-21 February. Interruptions were short. The same channels claimed access to industrial control panels and asked Spaniards for data on defence staff. Police arrested an alleged collaborator of pro-Russian groups in March (announced in July) and, in an operation announced in November, NoName057(16)'s alleged main instigator in Spain. Separately, members of the domestic group Anonymous Fénix were arrested in February. [S9][S10]

6. Espionage used Spanish government themes, according to vendor research. Recorded Future links a 2025-2026 campaign to BlueDelta (overlapping with APT28), with moderate confidence; its first lure imitated a Spanish ministry's meeting agenda. ESET reported that Webworm, a group it describes as China-aligned, targeted Spanish government bodies. Neither appeared in the leak-site and forum data we searched. [S11][S12]

Four decisions for leaders

1. **Treat current credential listings as an incident trigger.** Route every current listing tied to your domains to the identity team and record a disposition within 5 working days. Escalate if an active account without multi-factor authentication (MFA) is found (§3.4, §12.1).
2. **Hold suppliers to breach-notice terms.** Four of the 30 confirmed 2026 incidents began at a provider. Ask every supplier that holds your customer data how fast it will tell you, so that you can meet your own GDPR notification clock, and rehearse it with them (§5.8, §10.5).
3. **Break the fraud chain at transfers and SIM changes.** Banks should add friction to first transfers to new payees and "safe account" patterns; telecoms should harden SIM changes; everyone should brief call centres (§8, §12.1).
4. **Prepare for loud, short DDoS waves.** Agree who switches on upstream mitigation or time-boxed geo-filtering, and who speaks during an outage, before the next wave (§6.6).

The year in numbers

220

Ransompedia accepted ransomware listings for Spain dated 1 Jan-20 Nov 2026 (157 in all of 2025)

WHAT IT IS NOT

Not proof of encryption or data theft; unlisted cases are invisible

932,584

Blackhole posts tagged as concerning Spain, 1 Jan-20 Nov 2026

WHAT IT IS NOT

Not a count of attacks; 87% come from one Turkish-language bot family

58,657-62,086

relevant posts after cleaning (a range, not two counts)

WHAT IT IS NOT

Not unique incidents or offers

30

incidents involving Spanish organisations or customers confirmed by the organisation or an authority

WHAT IT IS NOT

Not a complete count; many incidents are never disclosed

250

leading public and private organisations assessed with Atlas ratings

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

1,217,865

infected-device associations with those 250 domains (lower bound; 46,895 employee-classified); cumulative, all records held on 21 Nov 2026

WHAT IT IS NOT

Not 2026-only, not unique people, not verified current infections

11,610,286

historical credential records for the same domains

WHAT IT IS NOT

Not 2026-only; not unique accounts or active passwords

163 of 250

organisations with a credential listed for sale at the time of the check

WHAT IT IS NOT

Not a count of accounts or of confirmed breaches

759

distinct cards attributed to Spain seen in clear text in collected posts

WHAT IT IS NOT

Not a fraud-loss figure; narrow scope (§8.2)

Report map

Twelve chapters, five reader paths. Start with the row that matches your role; each chapter opens with the question it answers, and chapters 2-12 close with three takeaways.

Board and executives
What happened, how exposed are we, and what should we decide?
GO TO 1 3 5 12

CISO and security leads
Which exposures are ours, which actors matter, and which controls come first?
GO TO 3 5 6 7 10 12

SOC and threat intelligence
What did actors post, how are they connected, and which techniques did espionage use?
GO TO 4 6 7 12 App. A-B

Fraud and customer protection
How are Spanish identities, accounts and cards traded, and where do banks see it?
GO TO 4 8 9

Communications and legal
How do we speak about unverified claims, and which rules apply now?
GO TO 5 6 10 12

01 **Executive summary**
What happened in 2026 and what leaders should decide first

02 **Context**
Which features of Spain shape the threats

03 **National exposure**
How 250 leading organisations rate with Atlas

04 **Dark web**
What criminals post about Spain beyond the bot noise

05 **Incidents**
Which incidents were confirmed and which are only claims

06 **Hacktivism**
What was claimed, what was confirmed, how to prepare

07 **Threat actors**
Who the actors are, how they connect, what reporting says

08 **Fraud economy**
How identities and accounts are turned into money

09 **Banking**
Where banks' visible exposure sits

10 **Regulation**
Which rules apply while NIS2 waits

11 **Outlook**
What to plan for and what would change the plan

12 **Action plan**
Who does what in 90 days

CHAPTER 2

Spain's digital and threat context

02

THIS CHAPTER ANSWERS

Which features of Spain shape the threats in this report?

96.8%

internet penetration, with 65.1 million cellular connections

INSIDE THIS CHAPTER

2.1 A large, connected population
2.2 Many administrations, many systems
2.3 A frequent target of politically framed claims
2.4 An election at the end of the window
2.5 A cyber law still waiting
2.6 National incident figures

IN SHORT

Four features shape Spain's 2026 threat picture. A large, digital population holds identity and bank data worth reselling. Regional and local administrations run many separate systems. Actors citing foreign-policy issues, chiefly Spanish support for Ukraine, claimed short DDoS attacks on Spanish sites. And its new cyber law is still waiting. Plan for identity fraud, supplier breaches and short DDoS bursts together.

2.1 A large, connected population

Spain had 46.3 million internet users in October 2026, a penetration of 96.8%. It had 65.1 million cellular connections (136% of the population) and 40.5 million social-media user identities [S13]. Almost every adult holds a national identity number (DNI or NIE) and a bank account number (IBAN) that appear in utility, telecom, retail and public-service records. This helps explain why so many 2026 incidents in this report are about customer records rather than encrypted servers.

2.2 Many administrations, many systems

Spain's public sector is spread across the central state, 17 autonomous communities, two autonomous cities, provincial councils and more than 8,000 municipalities. Each level runs its own websites, e-offices (sedes electrónicas), tax and school platforms and suppliers. In 2026 we found confirmed incidents at a ministry, a regional government, a regional health service, a port authority and several town halls (Chapter 5). In our reading, the pattern follows the architecture: smaller administrations with fewer staff, connected to shared software suppliers, are attractive targets for extortion.

2.3 A frequent target of politically framed claims

The CERT of the National Cryptologic Centre (CCN-CERT) placed Spain third among the countries most affected by hacktivist activity in its *Ciberamenazas y Tendencias* 2025 report, as reported in July 2026 [S14]. The report links the rise to campaigns against NATO members and supporters of Ukraine. In May the Secretary General of the National Intelligence Centre (CNI) said Spain is one of the most cyber-attacked countries, citing ransomware, espionage and influence activity [S15]. We report both as official assessments, not as measurements of our own.

In our 2026 data, politically framed claims against Spanish targets came mainly from pro-Russian DDoS groups, with a smaller number framed around Palestine (Chapter 6). These groups describe their own motives. This report quotes those descriptions as claims and takes no position on them.

2.4 An election at the end of the window

Royal Decree 806/2026 dissolved the Cortes on 6 October and called general elections for 29 November 2026, nine days after our cut-off [S16]. The campaign period began on 13 November. The Ministry of the Interior activated a network to anticipate risks such as cyberattacks and disinformation around the vote [S17]. Organisations that run public-information or media sites can treat the period as a planning context for short DDoS bursts and election-themed phishing. This is a planning assumption, not a forecast.

2.5 A cyber law still waiting

Spain has not yet transposed the EU NIS2 Directive, whose deadline was 17 October 2024. On 8 July 2026 the European Commission referred Spain, with Ireland, France and the Netherlands, to the Court of Justice and asked for financial penalties [S18]. The draft Law on Cybersecurity Coordination and Governance, published as a preliminary draft (anteproyecto) in January 2025, had not been submitted to the Cortes by our cut-off [S19]. Chapter 10 sets out what still applies and what organisations should do now.

2.6 National incident figures

The National Cybersecurity Institute (INCIBE) handled 122,223 incidents in 2025, 26% more than in 2024. They included 55,411 malware cases (392 of them ransomware) and 45,445 online-fraud cases, of which 25,133 were phishing. It handled 401 incidents at essential operators, 34% of them in banking [S20]. Catalonia's cybersecurity agency reported 6,544 incidents in 2025 at the Generalitat's public bodies and entities, almost twice the previous year [S21]. These are counts of handled cases, not prevalence rates, and the two bodies count differently.

KEY TAKEAWAYS

01

Spanish identity and bank data are the common thread of 2026 incidents across sectors.

02

Small administrations and their shared suppliers are a recurring point of entry.

03

NIS2 is still not law in Spain, so obligations depend on existing rules and sector regulators.

CHAPTER 3

National exposure: 250 leading organisations

THIS CHAPTER ANSWERS

How exposed are Spain's 250 leading public and private organisations when they are rated the way Brandefense Atlas rates a customer, and what should they act on first?

163 of 250

organisations had a credential listed for sale on the day of the check

INSIDE THIS CHAPTER

3.1 Universe card | 3.2 Exposure signals by sector | 3.3 Devices and credentials | 3.4 Current credential listings: the first item to triage | 3.5 Lookalike domains, exposed documents and mentions | 3.6 Email and web hygiene

IN SHORT

We assessed 250 leading Spanish organisations using Brandefense Atlas exposure ratings. In all, 163 of 250 organisations had a credential listed for sale when checked. Almost all have infected devices and historical credential records associated with their domains. The national Atlas headline is 66 out of 100. One in three domains does not enforce DMARC. Triage current listings first, then employee devices, then email authentication.

3.1 Universe card

Item	Definition
Population	250 organisations: 72 government (central, regional and city bodies), 27 education (universities), 25 banking and finance (banks and payment firms), 21 retail and holdings, 18 transport and logistics, 16 manufacturing and industry, 15 media and entertainment (including sport), 14 energy and utilities, 11 insurance, 11 healthcare, 10 telecom, 10 hospitality and tourism. 122 state-owned, 107 private, 21 foreign or joint
Selection	Purposive: central ministries and agencies, all autonomous-community governments, the largest city councils, banks supervised by the ECB or the Banco de España, payment infrastructure, state-owned enterprises, IBEX and market leaders. Selected for size or systemic role, not ranked by revenue
Unit	One primary domain per organisation. All 250 resolve in DNS (21 November 2026)
Measurements	Infected devices and employee devices, breach-database, stealer-log and combolist records, dark-web chat and forum mentions, lookalike domains, exposed documents and current credential-market listings; plus public DNS, TLS and HTTP header results
Date	Counts read 21 November 2026. Device, credential and listing counts are all records held on that date, whatever their capture date (cumulative, not 2026-only). Mention counts cover the previous 365 days; lookalike counts cover the last 30 days
Not deduplicated	Across sources, across organisations or across people. One person can appear in several sources; one device can hold logins for several organisations
Not representative	Results describe this list. They are not national prevalence rates

3.2 Exposure signals by sector

Each organisation received an Atlas exposure rating from 0 (no risk observed) to 100. The national Atlas headline for the 250 organisations is 66. This report publishes no sector ratings; the table shows measured counts by sector.

Terms used here.

Term	Meaning
National headline	The single Atlas figure for the whole list of 250, on the same 0-100 scale
Current listing	A credential tied to the domain on sale at the time of the check
Listing history	A credential tied to the domain was offered at some earlier point

Credentials and infected devices are near-universal; two in three organisations had a current credential listing

Share of organisations in each sector with the signal. Current credential listings are shown in coral.

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
Insurance (11)	100%	91%	100%	91%	91%	91%	91%
Education (27)	100%	96%	100%	85%	81%	96%	89%
Hospitality and tourism (10)	100%	100%	100%	80%	80%	100%	90%
Media and entertainment (15)	100%	100%	100%	80%	80%	87%	93%
Telecom (10)	90%	80%	100%	80%	60%	80%	80%
Retail and holdings (21)	95%	95%	100%	76%	76%	100%	95%
Banking and finance (25)	100%	76%	100%	68%	68%	92%	80%
Healthcare (11)	91%	82%	91%	64%	45%	73%	64%
Transport and logistics (18)	100%	100%	100%	61%	56%	56%	78%
Energy and utilities (14)	100%	86%	100%	57%	50%	79%	71%
Government (72)	93%	79%	92%	51%	50%	96%	69%
Manufacturing and industry (16)	94%	81%	100%	38%	0%	75%	88%

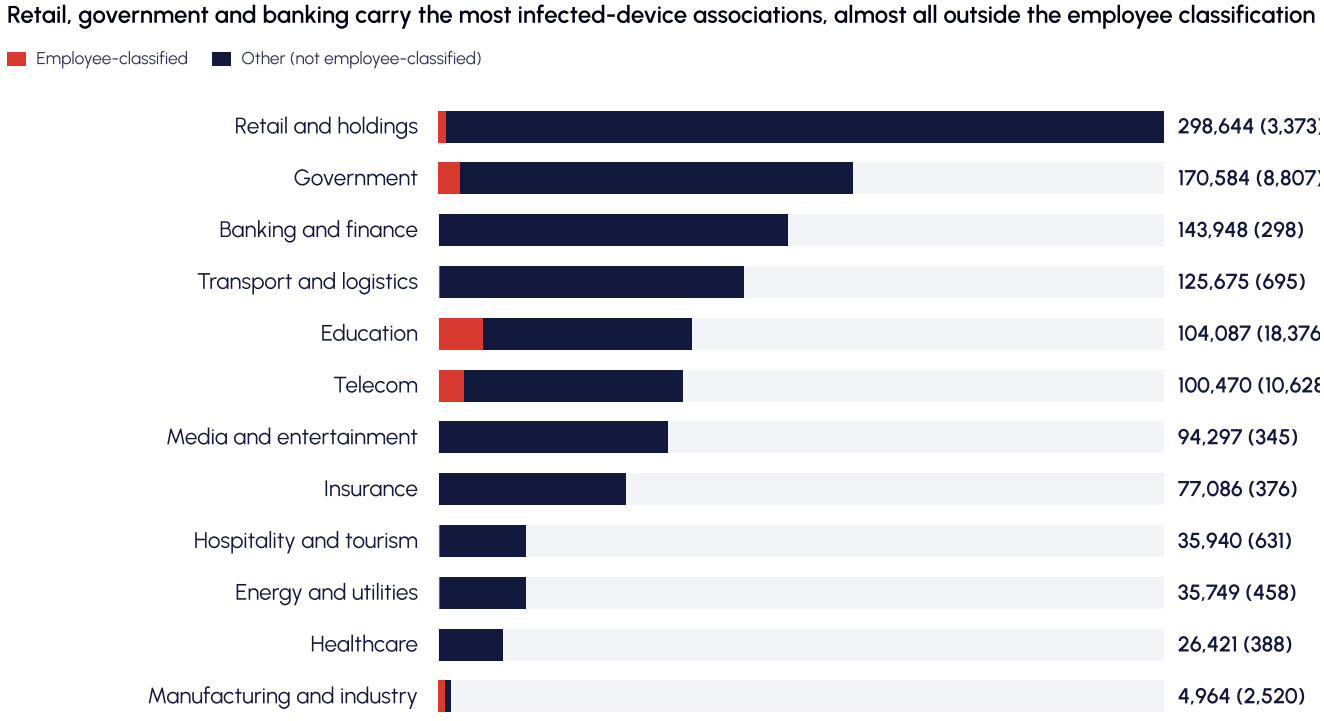
Source: Brandefense Atlas and Blackhole associations for 250 organisations, read 21 November 2026 [S2]. Records are cumulative, not 2026-only.

Sector	Orgs	Orgs with a current credential listing	Orgs with a listing history	Orgs with employee devices	Orgs with exposed docume
Government	72	37	36	57	
Education	27	23	22	26	
Banking and finance	25	17	17	19	
Retail and holdings	21	16	16	20	
Transport and logistics	18	11	10	18	
Manufacturing and industry	16	6	0	13	

Sector	Orgs	Orgs with a current credential listing	Orgs with a listing history	Orgs with employee devices	Orgs with exposed docume
Media and entertainment	15	12	12	15	
Energy and utilities	14	8	7	12	
Insurance	11	10	10	10	
Healthcare	11	7	5	9	
Telecom	10	8	6	8	
Hospitality and tourism	10	8	8	10	
All 250	250	163	149	217	

Reading the table. Current listings are most common in insurance (10 of 11), education (23 of 27) and media (12 of 15). They are least common in government (37 of 72) and manufacturing (6 of 16). Employee-classified devices appear at 217 of the 250 organisations. A listing is a reason to validate accounts, not proof of a breach (§3.4).

3.3 Devices and credentials



Source: Brandefense Atlas and Blackhole associations for 250 organisations, read 21 November 2026 [S2]. Records are cumulative, not 2026-only.

Sector	Orgs with infected devices	Devices, lower bound (employee)	Credential records	Credential share, two largest orgs
Retail and holdings	20 of 21	298,644 (3,373)	339,747	29%

Sector	Orgs with infected devices	Devices, lower bound (employee)	Credential records	Credential share, two largest orgs
Government	67 of 72	170,584 (8,807)	1,257,137	35%
Banking and finance	25 of 25	143,948 (298)	135,365	31%
Transport and logistics	18 of 18	125,675 (695)	131,230	41%
Education	27 of 27	104,087 (18,376)	2,943,162	21%
Telecom	9 of 10	100,470 (10,628)	6,077,675	84%
Media and entertainment	15 of 15	94,297 (345)	60,177	55%
Insurance	11 of 11	77,086 (376)	126,255	66%
Hospitality and tourism	10 of 10	35,940 (631)	81,178	56%
Energy and utilities	14 of 14	35,749 (458)	106,817	69%
Healthcare	10 of 11	26,421 (388)	122,527	63%
Manufacturing and industry	15 of 16	4,964 (2,520)	229,016	54%
All	**241 of 250**	**1,217,865 (46,895)**	**11,610,286**	**44%**

Some device totals are lower bounds. Banking rows are treated in more depth in Chapter 9. Credential records split into 2,050,519 breach-database records, 3,469,083 stealer-log lines and 6,090,684 combolist entries. The infected devices hold at least 4.2 million captured credentials in total (a lower bound), for all services, not only the organisation's own.

What this means.

- **Consumer brands carry the device load, mostly outside the employee classification.** 295,271 of 298,644 retail-associated devices and 143,650 of 143,948 bank-associated devices are not employee-classified. Their stealer logs include a login to the brand's site, so they are most plausibly customers' own computers, though ownership is not established. These associations are a fraud and account-takeover signal; they do not by themselves establish an intrusion into the company.
- **Universities and telecoms hold the employee-device problem.** Education has 18,376 employee-classified devices and telecom 10,628; together they are 62% of the national total in our list. University staff and students share domains, so "employee" here may include students. Telecom domains double as customer email addresses, which also explains why two telecom organisations hold 84% of that sector's 6.1 million credential records.
- **Government domains carry 1.26 million credential records, second among public bodies after universities.** Education, where 25 of 27 universities are state-owned, holds 2.94 million. Regional and city portals that issue staff and citizen accounts on the same domain are the likely reason; validation should separate the two.
- **The median organisation is not small.** The median organisation has about 1,900 infected-device associations and 4,500 credential records. Totals are dominated by a few heavy domains, so a sector total is a poor guide to a typical member.

3.4 Current credential listings: the first item to triage

At the check, 163 of 250 organisations had a credential tied to their domain on a monitored market. Of those, 149 also have a listing history.

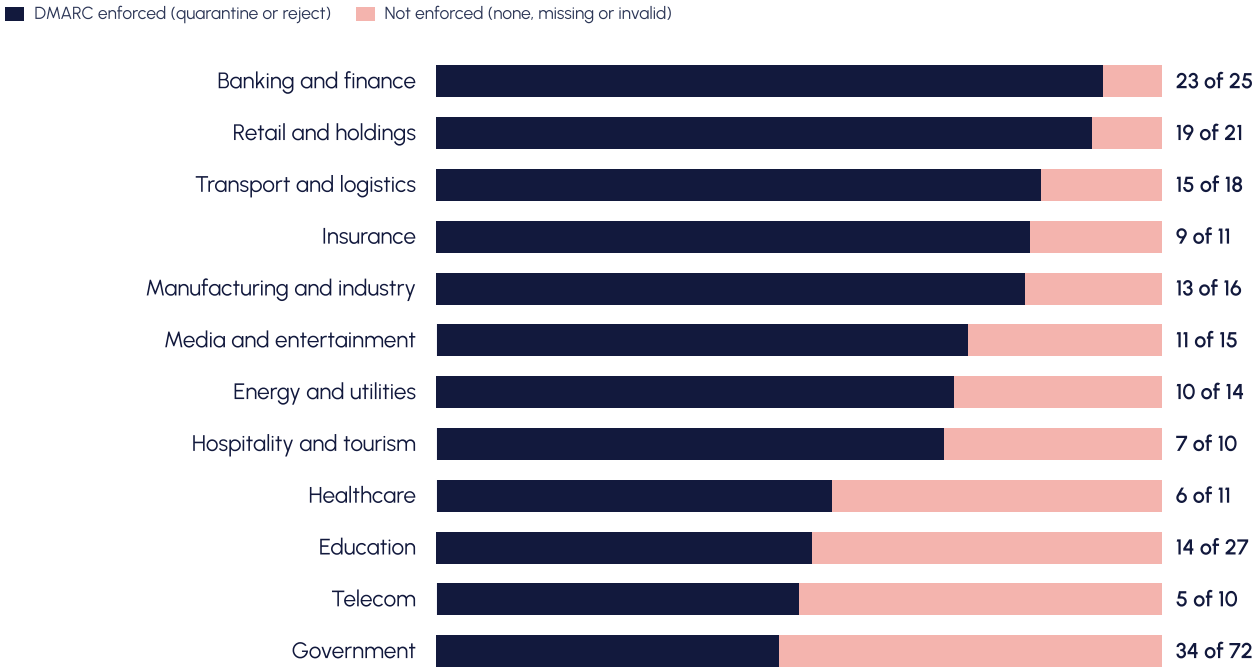
A current listing is the most direct market signal that a login tied to the domain is on offer. Whether that login still works is what validation must establish. The listing does not say how many accounts, whose accounts, or whether an account is active, protected by multi-factor authentication or already reset. The decision it supports is "validate the account now", not "declare a breach".

3.5 Lookalike domains, exposed documents and mentions

- **Lookalikes:** 221 organisations had at least one newly observed lookalike domain in the last 30 days. Short or generic brand names pick up unrelated domains; for the 182 organisations with a distinctive brand name, 153 had at least one; these counts are usable for triage. Lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 200 organisations have at least one exposed document that references their domain (6,990 in total).
- **Mentions:** 111 organisations were mentioned in dark-chat sources in the last 365 days and 82 in dark-web (onion) sources. Media and telecom domains dominate the largest counts because channels link to them; mention counts measure visibility, not hostility.

3.6 Email and web hygiene

Banks and retailers mostly enforce DMARC; government, telecom and education bodies often do not



Source: public DNS, TLS and homepage checks of 250 domains, 21 November 2026 [S22].

Results from our public DNS, TLS and homepage checks [S22]:

Control	Result (of 250 unless stated)	Reading
DMARC reject	99	Spoofed mail from the domain should be refused
DMARC quarantine	67	Spoofed mail should go to spam
DMARC p=none or missing	84 (62 none, 22 missing)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / redirect / no "all" term / none	182 / 45 / 1 / 4 / 1 / 17	17 domains publish no SPF policy
DKIM record found	193	Not finding a DKIM record is not proof that none exists
DS record observed (DNSSEC delegation)	43	No DS record observed for 207 domains; 28 of the 43 are government domains
TLS certificate invalid	13 of 234 checked	Expired, mismatched or untrusted certificates

Control	Result (of 250 unless stated)	Reading
HSTS on homepage	145 of 191 reachable	Most reachable sites force HTTPS for returning visitors
Mail provider	63 Microsoft 365, 20 Google, 27 no MX	The rest run their own or regional mail

Banks and retailers lead, public bodies lag. 23 of 25 banking and payment organisations and 19 of 21 retailers enforce DMARC. Government bodies (34 of 72), telecoms (5 of 10), universities (14 of 27) and healthcare (6 of 11) enforce least.

Government is also where DNSSEC delegation is most common: 28 of the 43 domains with a DS record observed are government domains. The sector is uneven rather than uniformly weak.

KEY TAKEAWAYS

01

Infected-device and credential associations are near-universal in the list; they call for validation, not alarm.

02

A current credential listing is the most direct sign that a login is on offer, so it is the first item to triage.

03

About half of the government bodies and universities we checked do not enforce DMARC, which leaves their names open to spoofing.

CHAPTER 4

What we see on the dark web

THIS CHAPTER ANSWERS

What do criminal channels and forums actually offer about Spain beyond the bot noise, and which offers deserve a defender's time?

87%

of posts tagged Spain came from one Turkish-language bot family

INSIDE THIS CHAPTER

4.1 Universe card | 4.2 Platforms, languages and volume | 4.3 Crime families after cleaning | 4.4 Spain-specific data offers | 4.5 Government-themed offers and recirculated material | 4.6 Case studies | 4.7 What the forums add

IN SHORT

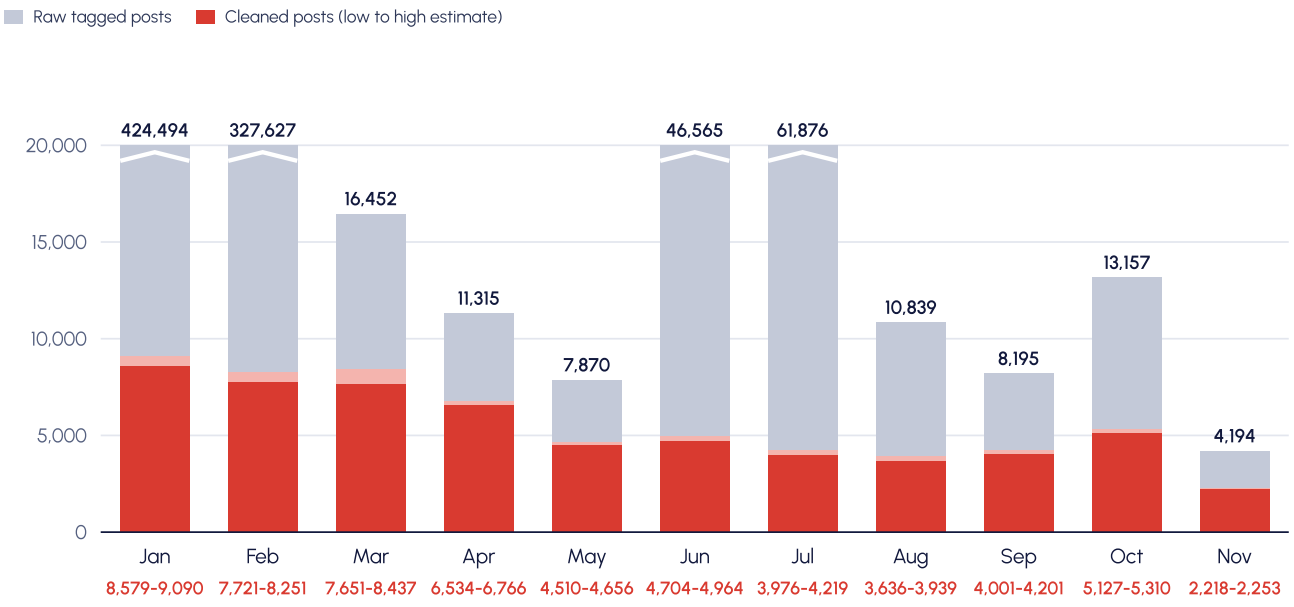
Posts tagged Spain number 932,584 for 2026, but 87% come from one Turkish-language bot family that tags every country. The cleaned range is about 60,000 relevant posts. The largest share trades bank and payment accounts, followed by cards, data leaks and identity documents. The most consequential offers were one tied to an energy retailer's confirmed incident and several large claims that the named organisations denied. Treat each listing as a lead to check, not as a breach.

4.1 Universe card

Item	Definition
Population	Posts in Brandefense Blackhole tagged as concerning Spain, post dates 1 January-20 November 2026: 932,584. Forum posts are 1,454 of them
Bot family	About 87% of tagged posts come from one Turkish-language automated template family that also tags Portugal, Italy, France and Türkiye. It is advertising noise, not a Spain-specific signal
Cleaned	58,657-62,086 relevant posts. The range is an uncertainty band, not two counts
Unit	A post. Posts are not unique offers, sellers, victims or incidents
Not established	That a listing is real, current, Spain-specific or sold. A country tag means "concerns Spain", not "targets Spain"

4.2 Platforms, languages and volume

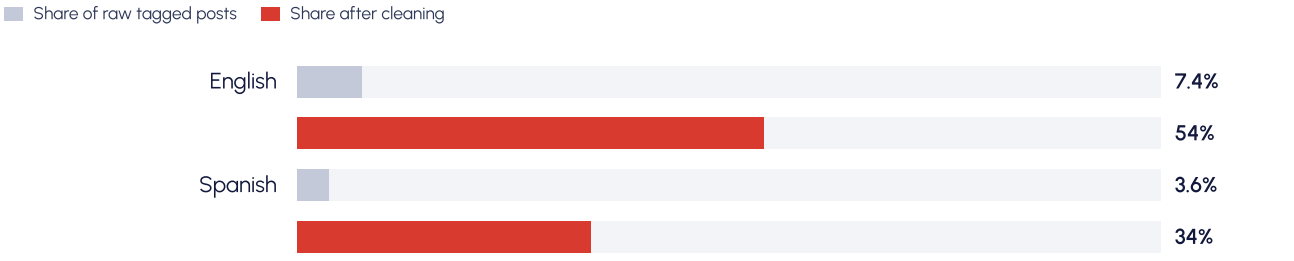
One bot family inflates January, February, June and July; cleaned volume stays between about 2,200 and 9,100 posts a month



Source: Brandefense Blackhole, posts tagged Spain, post dates 1 January–20 November 2026, November partial [S3]. Cleaned counts are an upper bound.

Telegram carries 99.8% of tagged posts. Forums carry few posts but most of the large database offers. Volume from the bot family peaks in January and February, and that peak appears for every comparator country. The June–July rise is far larger for Spain (about six times May's level in June) than for any comparator. It is still Turkish-language template traffic from the same family (Chart c09), so neither peak is a Spain-specific crime signal.

Turkish dominates the raw tag; after cleaning, English and Spanish posts carry the weight



Telegram carries 99.83% of tagged posts. Source: Brandefense Blackhole, posts tagged Spain, post dates 1 January–20 November 2026, November partial [S3]. Cleaned counts are an upper bound.

Language	Raw share	Share after cleaning
English	7.4%	54%
Spanish	3.6%	34%
Russian	1.6%	6%
Chinese	0.7%	5%

Turkish is 86.9% of the raw tag, mostly from the bot family. After cleaning the picture is 54% / 34% for English and Spanish. Spanish-language posts are mostly fraud and banking-service channels run for a Spanish-speaking audience. Russian appears mainly in DDoS and hacktivist channels (Chapter 6).

4.3 Crime families after cleaning

Bank and payment-account trading leads the cleaned corpus; cards, data leaks and identity documents follow



Source: Brandefense Blackhole, posts tagged Spain, post dates 1 January–20 November 2026, November partial [53]. Cleaned counts are an upper bound.

Family	Cleaned posts (low-high)	Median price in posts that state one
Bank and payment-account trading	22,417-23,173	180 USD
Carding	15,617-16,901	80 USD
Data leaks and databases	11,846-12,272	20 USD
KYC and identity documents	11,217-11,754	100 USD
Phishing and scams	6,273-6,548	60 USD
Malware and exploits	1,468-1,571	300 USD
Combolists	1,195-1,266	59 USD
Access sales	995-1,027	80 USD
Stealer logs	558-590	63 USD
Ransomware (mentions and relays)	477	not meaningful
DDoS and hacktivism (tagged)	67-71	not meaningful

A post can belong to more than one family, so the rows do not add up to the cleaned total. Prices are advertised asking prices in posts that state one; they are not transaction prices.

What stands out. The largest share of Spain's cleaned corpus (about 37%) is the trade in bank accounts, not database leaks. Spanish-language Telegram channels advertise "cuentas", "cargas" and "drops": ready-made or rented bank and payment accounts, money "loads" and mule accounts used to receive and move fraud proceeds. Channel names and posts name the largest Spanish retail banks and neobanks as products. This is a fraud economy aimed at banks' customers, and Chapter 8 treats it in detail.

4.4 Spain-specific data offers

When	Claimed source (role)	What was offered	Status
4 January	Endesa (electricity and gas retailer)	Customer database, "more than 20 million people", about 1 TB	Company confirmed an incident; figures not confirmed (Case A)
20 January, 5 February	PcComponentes (electronics e-commerce)	16.3 million user profiles; staff and logistics data	Company denied access to its databases and confirmed a credential-stuffing attack on accounts `[S23]`
30 January	A major energy retailer	Re-upload of customer data the poster dates to May 2024	Data dated by the poster to 2024, offered again (Case C)
31 January	A public-sector body	"47.3M citizens" with ID, address, phone and IBAN	Denied; forum buyers called it fake (Case B)
February-March	Spanish retail banks (customer "leads")	Price lists per bank for customer contact records	Claim; not verified (Case D)
21 August	A law-enforcement body's websites	Files said to come from a "simple scan"	Claim; not verified
August	Individuals in Spain	Several lists of names, tax IDs and IBANs; passport scans	Claims; origin unknown
2 November	A consumer-electronics retailer	Customer records (claimed count withheld)	Claim; not verified
4 November	A telecom infrastructure operator	Network inventory	Claim; not verified

EVIDENCE CARD B01 — 4 Jan 2026

spain Leak forum · Forum · English

ORIGINAL

```
BIGGEST Spain DATABASE (Endesa)
This database is new, fresh, never seen before, not a
previous leak
ONLY SELLING IT TO 1 PERSON [...]
Total size: (1,055,950,885,115 bytes)
If you want more information/buy message me on my Telegram
[contact removed]
More than +20.000.000 people in one single .sql [...]
[file list of customer, account, case and billing tables
removed]
```

HELD	The offer, the claimed size and the claimed number of people; the company separately confirmed an incident.
NOT ESTABLISHED	The number of people affected, the age of every file, any sale.

EVIDENCE CARD B03 — 31 Jan 2026

[alias withheld; it names the claimed body] Leak forum · Forum · English, with Spanish field names

ORIGINAL

```
Hello. Today I am selling the updated database of [a public-
sector body] containing the information of 47.3M citizens
The data includes: ID, DNI/NIF, Nombre completo, [...]
Direccion, [...] Telefono, IBAN, ContactEmail [...]
Sample: [sample records removed]
```

HELD	The claim and its field list; the sample uses values that look invented.
NOT ESTABLISHED	That any record comes from the named body, which said it found no trace of an incident.

EVIDENCE CARD B04 — 2 Feb 2026

Forum user Leak forum · Forum · English

ORIGINAL

```
This is a scam. The mails do not exist
```

HELD	A forum user publicly challenged the public-sector database claim two days after it was posted.
NOT ESTABLISHED	Who the replier is or how the emails were checked.

EVIDENCE CARD B06 — 5 Feb 2026

Leonsky Leak forum · Forum · English

ORIGINAL

```
I am selling a complete, private SQL dump of
PCComponentes.com (Spain's #1 Tech E-commerce). This is a
fresh extraction from January 2026
Users: 16,342,881 unique records
Fields: Full Name, Email, Bcrypt Hash, Salt, DNI/NIF, Phone,
Full Address [...]
Price 28.000$ [contact removed]
[staff sample removed]
```

HELD	The offer, its price and the claimed record count.
NOT ESTABLISHED	A database breach; the company denied access to its databases and confirmed a credential-stuffing attack on accounts.

4.5 Government-themed offers and recirculated material

Offers that name state bodies cluster around national registries and police systems. Most such offers fail basic checks. The January public-sector database sample uses values that look invented, such as sequential bank-account digits and textbook phone numbers, and forum users called it fake within two days. A February post by a forum persona relayed a ministry's own statement about a "technical incident" as proof of a breach; the ministry confirmed only a "very limited" incident (Chapter 5).

The same personas reappear. A persona that relayed the January leak of officials' data also re-uploaded energy-retailer data it dates to 2024 and advertised a travel-loyalty database first leaked by a ransomware group in December 2025. Re-uploading old material is cheap and earns forum reputation. For defenders the question is always: is this new, and is it ours?

EVIDENCE CARD B14 — 21 Aug 2026

updap Persona's own leak site · Forum · English

ORIGINAL

```
I was quietly searching the internet, as I usually do when I
felt like looking into the security of [a law-enforcement
body's] websites. [...] I decided to do a simple scan [...]
and, surprisingly, I found some interesting things. [...]
(it's nothing special, but it is interesting).
[download links removed]
```

HELD	The claim; the poster calls the result "nothing special".
NOT ESTABLISHED	What was found, or that any police system was accessed.

4.6 Case studies

A CASE A

A confirmed energy-customer incident and reposted advertisements

COMPANY CONFIRMED AN INCIDENT

Evidence card B01 | 4 Jan 2026 | Leak forum | Energy

Claim	On 4 January a persona calling itself "spain" offered a database it attributed to Endesa, claiming more than 20 million people and about 1 TB. It listed file names for customer, account, case and billing tables and was "only selling it to 1 person".
Chronology	The company told customers in January that a commercial platform had been accessed, exposing identification, contact and contract data and, for some customers, bank account numbers (Case G). On 16 February a second persona reposted the same size and wording under a 2026 title, with a new contact (B02); a third persona reposted it later.
What we can establish	That the offer preceded or coincided with the company's notice, and that the same advertisement was reposted by other personas. The posts do not establish the number of people affected, that any persona holds the data, or that any sale took place.
Alternatives	One seller using several names; resellers copying the listing; a mix of real and padded data.
Limits	No sample was assessed. The attacker's figure is not the company's.
Response	Customers of any energy retailer should expect calls and messages that quote real contract details. Retailers should brief call centres to never ask for full bank details on inbound contact.
BOTTOM LINE	**Confirmed incident, unconfirmed figures, reposted advertisements: warn customers about calls that quote real contract data.**

B CASE B

A public-sector database claim that buyers called fake

CLAIM DENIED

Evidence card B03 | 31 Jan 2026 | Leak forum | Government

Claim	On 31 January a persona whose alias names the claimed body offered "the updated database of [a public-sector body] containing the information of 47.3M citizens", with ID, address, phone, IBAN and payment fields.
Chronology	On 3 February the press reported that the body concerned had ruled out the claim; a spokesperson said it had found no trace of an incident [S24]. Within two days of the post, a forum user replied "This is a scam. The mails do not exist" (B04).
What we can establish	That the claim was made and challenged on the same forum. The sample values look invented.
Alternatives	Fabrication for reputation; a reseller's fake; a mix of public and old records.
Limits	We did not test the sample against any real data.
Response	Citizens will see government-themed phishing regardless, as INCIBE warnings in 2026 show (Chapter 8).
BOTTOM LINE	**Large state-database claims often fail basic checks; compare samples before anyone speaks of a breach.**

C

CASE C

Energy-retailer data the poster dates to 2024, offered again

DATA DATED BY THE POSTER TO 2024

Evidence card B05 | 30 Jan 2026 | Leak forum | Energy

Claim	On 30 January a forum persona posted a "database" of a major energy retailer, saying the data was exported in May 2024 from a cloud drive used by contact-centre staff.
What we can establish	That data the poster dates to 2024 was offered again in 2026 by a persona that also relays other leaks. The date comes from the post, not from an independent check.
Alternatives	A genuine 2024 export; a repackaged older dataset.
Response	Treat as a reminder that contact-centre exports outlive the incident. Review who can export customer lists to personal or shared drives.
BOTTOM LINE	**Contact-centre exports outlive the incident that produced them.**

EVIDENCE CARD B02 — 16 Feb 2026

Koipo Leak forum · Forum · English

ORIGINAL

```
ENDESA SPAIN (2026) IBAN 20M+
DM Price: [contact removed]
More than +20.000.000 people in one single .sql (fresh data,
never seen)
Total size: (1,055,950,885,115 bytes)
File Tree: [link removed]
SAMPLE ALL FILES: [link removed]
```

HELD	A second persona reposted the same advertisement, size and wording six weeks later with a new contact.
NOT ESTABLISHED	Whether the reposter holds any data, or only copied the advertisement; any sale.

EVIDENCE CARD B05 — 30 Jan 2026

IntelShadow Leak forum · Forum · English, with Spanish field names

ORIGINAL

```
Hi [forum], today I have uploaded the [energy retailer]
database, the data breach occurred in May 2024 [...] when
[file count removed] files were exported with the email
[address removed] from Google Drive.
DATA [field list: ID number, name, phone, address, IBAN,
supply point removed]
SAMPLE [records removed]
```

HELD	The poster dates the data to May 2024 and describes an export from a contact-centre cloud drive.
NOT ESTABLISHED	That the data is new, or that the retailer's systems were accessed in 2026.

D

CASE D

Customer "leads" priced per bank

CLAIM UNVERIFIED

Evidence card B07 | 28 Feb 2026 | Banking-services Telegram channel | Banking

Claim	A Telegram seller posted a price list of Spanish customer "leads" per bank, from 600 to 750 euros per 5,000 records, with a dated "new update".
What we can establish	That a seller markets bank-segmented contact lists. Such lists feed the bank-impersonation SMS and call campaigns that police dismantled in 2026 (Chapter 8).
Alternatives	Lists built from older breaches and public data rather than from any bank.
Response	Banks should assume customers will receive calls that know which bank they use, and repeat that the bank never asks to move money to a "safe account".
BOTTOM LINE	**Bank-segmented lead lists feed impersonation calls; warn customers about safe-account scams.**

EVIDENCE CARD B07 — 28 Feb 2026

L34ds Banking-services Telegram channel · Telegram · Spanish and English

ORIGINAL

```
Leads Spain EN VENTA:
[bank A]: 750€ - 5k
[bank B]: 750€ - 5k
[bank C]: 650€ - 5k
[...twelve banks and neobanks listed...]
Papa y mamá 600€ - 5k
NUEVA ACTUALIZACIÓN / NEW UPDATE 24-2-2026 [contact removed]
```

TRANSLATION

Spanish leads FOR SALE: [bank A]: 750 euros per 5,000 [...] "Mum and dad": 600 euros per 5,000. New update 24 February 2026.

HELD	Contact lists are marketed per bank, plus a list aimed at parents.
NOT ESTABLISHED	That any bank was breached; such lists are often built from older leaks.

EVIDENCE CARD B08 — 1 Jan 2026

Anonymous poster Spanish-language banking-fraud Telegram channel · Telegram · Spanish

ORIGINAL

```
Necesito
[bank A] + [crypto exchange]
[neobank] creada +1€
[neobank] a crear
DM [contact removed]
```

TRANSLATION

Wanted: a [bank A] account plus a [crypto exchange] account; an already opened [neobank] account (+1 euro); a [neobank] account to be opened. DM [contact removed].

HELD	Demand for ready-made and to-be-opened accounts, the core product of these channels.
NOT ESTABLISHED	Who would open the accounts or in whose name.

E

CASE E

Files advertised as login combinations for a bank login page

ADVERTISED FILES OBSERVED

Evidence card B15 | 26 Jun 2026 | Leak forum (automated bot) | Banking, retail, education

Claim	In May and June an automated forum bot published small credential files named after Spanish bank, retail and university login pages, each with a few dozen to a few hundred lines.
What we can establish	That files advertised as URL/email/password combinations are sorted by the login page they name and given away as samples.
Alternatives	Lines captured by infostealer malware; lines recycled from older combolists; padded or invalid lines given away to attract buyers.
Response	Banks and retailers should monitor for their login URLs in such files and force step-up authentication for the accounts concerned.
BOTTOM LINE	**Files advertised as login combinations name bank login pages; force step-up authentication for affected accounts.**

F

CASE F

A telecom network inventory

CLAIM UNVERIFIED

Evidence card B16 | 4 Nov 2026 | Leak forum | Telecom

Claim	On 4 November a forum persona offered what it described as the network inventory of a telecom infrastructure operator. The post gave counts of network assets and staff mailboxes.
What we can establish	That the offer exists. Such inventories are sensitive because they map physical infrastructure.
Alternatives	A planning extract shared with contractors; old data.
Response	Operators should check which contractors receive full inventory exports and whether those exports are watermarked.
BOTTOM LINE	**Network inventories map physical infrastructure; control and watermark contractor exports.**

EVIDENCE CARD B15 — 26 Jun 2026

Forum bot Leak forum (automated bot) · Forum · English

ORIGINAL

```
Log:Pass [Spanish bank online-banking login]-110
File Information
Total Lines: 110
Content Type: URL / Email / Password Combo
Sample Data: [credential lines removed]
```

HELD	A 110-line file advertised as URL/email/password combinations for one bank's online-banking login page.
NOT ESTABLISHED	That the logins are valid, where the lines came from, or that the bank's systems were accessed.

EVIDENCE CARD B16 — 4 Nov 2026

Forum persona Leak forum · Forum · English

ORIGINAL

```
[telecom infrastructure operator]: internal network platform
[asset and mailbox counts removed]
[operator and network description removed] [...]
[sample record and carrier list removed]
```

HELD	The claim and the kind of data described.
NOT ESTABLISHED	That the data is current or complete, or how it was obtained.

4.7 What the forums add

Forums carry few Spain posts but most of the large database claims. Replies matter: in at least three 2026 threads, forum users challenged a seller within days, calling the data fake, recycled from an earlier leak or taken from another company. Those replies are an inexpensive first check for a defender, though they can also be competitors talking down a rival.

KEY TAKEAWAYS

01

Bank-account trading, not database leaks, is the largest share of the cleaned Spain posts (about 37%).

02

Large claims against state bodies and retailers often fail basic checks or recycle old data.

03

An offer tied to a confirmed energy-customer incident was reposted by several personas within weeks.

CHAPTER 5

Confirmed incidents and claims by sector

05

THIS CHAPTER ANSWERS

Which Spanish organisations confirmed an incident in 2026, which only appear in an attacker's claim, and what does the pattern tell each sector?

30

incidents involving Spanish organisations or customers, confirmed by the organisation or an authority

INSIDE THIS CHAPTER

5.1 How we sorted the cases | 5.2 Energy and utilities: customer records at scale | 5.3 Transport, ports and logistics | 5.4 Public administration | 5.5 Education and health | 5.6 Retail, consumer services and technology | 5.7 Other confirmed incidents | 5.8 What the pattern shows

IN SHORT

Between January and our cut-off, organisations or authorities confirmed 30 incidents involving Spanish organisations or Spanish customers, and attackers claimed many more. The confirmed cases cluster in three places. First, customer databases at energy, retail and transport companies, some reached through a supplier. Second, town halls, a regional government and a port authority hit by ransomware or named in extortion claims. Third, universities and health services. Treat a supplier's customer database as your own attack surface, and rehearse the customer notice before you need it.

5.1 How we sorted the cases

We list an incident as **confirmed** when the organisation itself or a public authority said that an attack or unauthorised access took place. We name an organisation only in that case, and only when the incident was widely reported. Smaller confirmed cases, reported mainly by one outlet or a CERT summary, are described by role; the cited source names them. Everything else is a **claim**: an extortion listing, a forum post or a channel message. Claims are described by sector and role, never by name. A confirmed incident does not confirm the attacker's figures; where the two differ we give both.

The count. The 30 confirmed incidents are: energy 2, transport and ports 2, public administration 6, education and health 3, retail and technology 5, other confirmed incidents 7, and foreign platforms used by Spanish customers 5.

5.2 Energy and utilities: customer records at scale

CASE G

Endesa customer contract data (January)

Energy

COMPANY CONFIRMED

What was confirmed	Endesa told customers in January that unauthorised access to a commercial platform exposed identification, contact and contract data, national ID numbers and, for some customers, bank account numbers. It said passwords were not affected and notified the Spanish Data Protection Agency (AEPD) [S4][S25].
What was claimed or reported	A forum persona calling itself "spain" claimed about 1 TB on more than 20 million people [S25]. The company did not confirm a number. The resale of that offer is in Case A.
Response	Expect targeted phishing and fake-supplier calls that quote real contract details.
BOTTOM LINE	**Identity data, and for some customers bank data, were exposed; expect targeted phishing for months.**

H

CASE H

Naturgy data at an external provider (May)

Energy

COMPANY CONFIRMED

What was confirmed	Naturgy reported access to systems of an external provider, affecting about 3% of its customers in Spain, with identification, contract and in some cases bank data. It said its own systems were not attacked and no credentials were exposed [S5].
What was claimed or reported	A seller claimed a far larger customer set; the company figure and the claim are not reconciled.
Response	Ask every provider holding your customer data how fast they will tell you.
BOTTOM LINE	**The breach was at the provider; supplier notice terms decide how fast you can act.**

Two of Spain's largest energy retailers confirmed customer-data incidents within four months. Neither confirmed attacker figures. INCIBE warned Endesa customers of possible follow-up fraud, and the consumer body OCU warned Naturgy customers of phishing [S4][S5].

5.3 Transport, ports and logistics

I

CASE I

Adif and Renfe ticket-sales systems (September)

Transport

COMPANY CONFIRMED

What was confirmed	On 24 September an intruder reached ticket-sales systems of Renfe and of the rail infrastructure manager Adif. In November Renfe told customers that identification and contact data, ID document numbers, hashed passwords and trip records may have been exposed. It said the Guardia Civil had arrested a suspect in October [S6].
What was claimed or reported	Press reports of 500 GB taken and of AI-assisted intrusion were not confirmed by Renfe or Adif [S26].
Response	Force password resets where passwords may be weak, and warn customers about calls quoting real trips.
BOTTOM LINE	**ID numbers, hashed passwords and trips may be exposed; force resets and warn about calls quoting real trips.**

J

CASE J

Port of Vigo ransomware (March)

Transport

PORT AUTHORITY CONFIRMED

What was confirmed	An attack detected early on 24 March disrupted the port's cargo-management systems, and the port authority isolated its systems from external networks. The port's president said systems would stay offline until all security checks were complete, and authorities confirmed ransomware [S27].
What was reported	Port users switched to manual and paper procedures to keep cargo work moving. The president said the port's physical operations were not affected [S27].
What is not established	Whether data was taken, and which group was responsible.
Response	Keep a manual mode for port and logistics operations that can run for days.
BOTTOM LINE	**Paper procedures kept cargo work moving; rehearse a manual mode before you need it.**

5.4 Public administration

When	Body	What was confirmed	Claim, if any
January	Concello de Sanxenxo (town hall)	Ransomware encrypted documents on the municipal server; restored from backup; ransom not paid [S28]	None reported
February	Ministry of Science, Innovation and Universities	Unauthorised access to personal data of applicants for degree recognition, described as "very limited" [S29]	Persona "GordonFreeman" claimed passports, IDs and bank data
May	Ayuntamiento de Valdemoro (town hall)	Network incident on 5 May; servers disconnected; the National Cryptologic Centre (CCN) notified [S30]	Kairos claimed 1.8 TB
June (arrest announced November)	Ayuntamiento de Ciudad Real (city council)	The council suspended its Low Emission Zone platform after a cybersecurity incident in June [S31]. The Guardia Civil said an intruder entered the platform without authorisation and used AI tools. It said he attempted extortion but did not name the targets. A software firm supplying e-government services was also affected [S32]	None reported
August	Junta de Comunidades de Castilla-La Mancha (regional government)	Cyberattack confirmed; protocols activated, affected people informed [S33]	Panzer claimed about 3 GB, including student and family records
November	Ayuntamiento de San Cristóbal de La Laguna (town hall)	Incident on 2 November took down the website, e-office and case-management systems [S34]	None at our cut-off

Two further public bodies appeared in data-theft claims that the bodies denied or did not confirm. One was a claim of more than 47 million records against a public-sector body, posted on 31 January (Case B). The other was a claim against a state agency in September, which we describe by role only.

5.5 Education and health

K

CASE K

Universidad de Alicante containment (July)

Education

CONFIRMED BY THE UNIVERSITY

What was confirmed	The university described the most serious attack attempt against its systems to date. It isolated systems and temporarily suspended its e-office deadlines. It said some secondary servers were reached, but checks found no sign of data exfiltration [S35].
What was claimed or reported	None.
Response	Rehearse the decision to switch services off early.
BOTTOM LINE	**The university says early isolation limited the attack to secondary servers; rehearse that decision.**

L

CASE L

Universitat de València research server (May)

Education

CONFIRMED; CLAIM NOT RECONCILED

What was confirmed	The university confirmed an intrusion that, it said, reached one obsolete server of a research group [S36].
What was claimed or reported	NOVA claimed 300 GB including staff and student data.
Response	Inventory research servers outside central IT.
BOTTOM LINE	**The university says one obsolete research server was reached; inventory servers outside central IT.**

The Servicio Extremeño de Salud reported in October that automated access to its online health portal affected 18,416 users [S37]. A ransomware group listed a Barcelona hospital in October, and another listed a private hospital group in August; neither had confirmed an incident by our cut-off.

5.6 Retail, consumer services and technology

When	Organisation	What was confirmed
January	PcComponentes	No access to its databases, the company said, but a credential-stuffing attack on customer accounts using passwords reused from other breaches [S23]
April	Inditex	Unauthorised access to databases hosted by a former technology provider; the company said they held no names, contact details, passwords or payment data, and its own systems were not affected [S38]
April	Basic-Fit (Spanish members affected)	Access to a visit-recording system on 8 April; names, ID numbers, contact data, dates of birth and bank account details downloaded [S39]
June-July	Indra (one subsidiary)	Ransomware attack at a subsidiary, confirmed by the company [S40]; The Gentlemen listed it on its leak site, and that group attribution remains a claim [S1]
July	Lidl (online shop customers)	Access through an IT provider to a separate file with names, contact data, dates of birth and customer numbers [S41]

5.7 Other confirmed incidents

When	Organisation (role)	What was confirmed
January (breach in December 2025)	A ministry's immigration-services provider	Exposure of foreign residents' data held by the provider; the ministry confirmed it [S42]
January	A Canary Islands town hall	An attack took the website offline overnight; the council said citizens' data was not affected [S43]
June	A home-improvement retailer's home-services platform	Security incident acknowledged; a possible breach of some customers' names, contact data and ID numbers was still under investigation. The company said no passwords or bank data were affected. A leak claim cited about 55,000 records [S44]
July	A regional school-management platform	The regional government reported possible unauthorised access to some teachers' accounts, reset all professional users' passwords and reported it to police [S45]
September	An organisation that notified the AEPD	Breach described as carried out by an AI agent [S46]
October	A professional football club	Anomaly on data servers with possible impact on fans' personal data; notified to the AEPD [S47]
November	A video-game retailer	Unauthorised access detected on 9 November reached customer numbers, phone numbers, email addresses and order histories; the company said it stores no payment data [S48]

Besides Basic-Fit (§5.6), five more confirmed incidents happened at foreign platforms used by Spanish customers. Two were a European rail-pass operator in January [S49] and Booking.com in April [S50]. An education-software provider's May breach affected a Spanish university, one of almost 9,000 institutions affected worldwide; identification, contact and classroom-message data were potentially affected [S51]. The other two were a digital bank that disclosed data after fake government requests in September [S52] and a gift-experience platform that detected unauthorised access on 3 November [S53].

5.8 What the pattern shows

Sector	Confirmed	What the confirmations describe	One action
Energy and utilities	2	A commercial platform and an external provider	Breach-notice terms in supplier contracts
Transport and ports	2	Ticket-sales systems; ransomware on cargo systems	Password resets; a rehearsed manual mode
Public administration	6	Ransomware, extortion claims and e-office outages	Tested backups and early isolation
Education and health	3	Secondary and obsolete servers; automated portal access	An inventory of servers outside central IT
Retail and technology	5	Former and current providers; credential stuffing	Supplier list; MFA and reuse checks for customer accounts
Other	7	Providers, websites, club servers and teachers' accounts	Customer notice templates ready
Foreign platforms	5	Breaches at platforms that hold Spanish customers' data	Warn customers about follow-up phishing

The table sorts cases by sector, not by ownership. Counting public bodies, state-owned companies and a ministry's provider, 14 of the 30 touched the public sector. Besides the six in §5.4, they were Adif and Renfe, the Port of Vigo, two public universities and a regional health service. The other three are in §5.7: a Canary Islands town hall, a regional school platform and a ministry's immigration-services provider.

Four confirmed incidents (Naturgy, Inditex, Lidl and a ministry's immigration-services provider) started at a current or former provider of the Spanish organisation. A fifth (Basic-Fit) started at a secondary system that recorded club visits. The education-software incident is itself a provider's breach; we count it among foreign platforms. At Ciudad Real a software supplier was also affected, but the Guardia Civil did not say it was the entry point, so we do not count it as a supplier case.

Six confirmed incidents had ransomware confirmed or an extortion group listing or claiming the body. They were Sanxenxo, Vigo and an Indra subsidiary (ransomware confirmed), and Valdemoro, Castilla-La Mancha and the Universitat de València (listed or claimed). For the Indra subsidiary, the naming of a group is the group's own claim.

Public bodies made up five of the six: two town halls, a regional government, a port authority and a public university. The Guardia Civil said the Ciudad Real intruder attempted extortion without naming his targets, so that case is not in this count. Many attacker claims named organisations that never confirmed anything; a claim on its own is a reason to check, not a fact.

KEY TAKEAWAYS

01
Most confirmed 2026 incidents exposed customer records, not production systems.

02
Five confirmed incidents started at a supplier or a secondary system.

03
Public bodies made up five of the six confirmed incidents with confirmed ransomware or an extortion listing.

CHAPTER 6

Hacktivism and DDoS

THIS CHAPTER ANSWERS

Who claimed politically framed attacks on Spanish targets in 2026, what did those attacks actually disrupt, and how should defenders prepare for the next wave?

16-21 Feb
the main pro-Russian DDoS wave against Spanish public websites

INSIDE THIS CHAPTER

6.1 Timeline | 6.2 The February wave: claim against measurement | 6.3 Claims against industrial systems | 6.4 Recruitment and data on officials | 6.5 Other claims in their own words | 6.6 Lessons for defenders

IN SHORT

The year's main hacktivist event was a pro-Russian DDoS wave in mid-February against ministries, a regional parliament, city councils and transport sites, claimed by NoName057(16) and Server Killers. Disruption was short; the groups themselves said several targets had limited access to Spanish visitors. The same channels claimed access to industrial control panels and recruited Spaniards for data on defence staff. Police later arrested an alleged collaborator of pro-Russian groups and NoName057(16)'s alleged instigator in Spain. Prepare upstream mitigation, geo-filtering and DDoS statements before the next wave.

6.1 Timeline

26 Jan 2026 — **BD Anonymous Team**
Claims to have taken down a Galician city council's website, citing Palestine as its motive (B13)

9 Feb 2026 — **DDoSia Project (NoName057(16))**
Lists a Spanish sports body among sites it claims to have taken offline

16 Feb 2026 — **Server Killers with NoName057(16)**
Announces attacks on "critical government infrastructure" of Spain; lists central-government and ministry websites (B10)

16 Feb 2026 — **DDoSia Project (NoName057(16))**
Lists a regional parliament, tourism portals and city transport sites, citing Spanish aid to Ukraine (B11)

16 Feb 2026 — **Z-Pentest Alliance (relayed)**
Claims full access to the control panel of a wastewater pumping station in Spain (B12)

17 Feb 2026 — **Press and monitors**
Report temporary interruptions; authorities had not commented [S9]

19 Feb 2026 — **DDoSia Project (NoName057(16))**
Claims its attack on a network-equipment firm caused a business-telephony outage; the cause of that outage was not confirmed

22 Feb 2026 — **Guardia Civil**
Announces that the four main members of the domestic group Anonymous Fénix have been arrested, two in 2025 and two in February 2026

3 Mar 2026 — **Spanish-language channel relaying NoName057(16)**
Asks followers for personal data of Spanish defence-industry staff (B09)

24 Mar 2026 — **DDoSia Project (NoName057(16))**
Claims access to the ticketing terminal of a Spanish city bus

6 Jul 2026 — **Policía Nacional**
Announces the March arrest, on an FBI tip, of an alleged collaborator of CARR and Z-Pentest

17 Aug 2026 — **Press**
Reports a leaked list of about 1,000 police, Guardia Civil and military personnel, investigated as linked to NoName057(16)

20 Nov 2026 — **Policía Nacional**
Announces the arrest in Burgos of the alleged main instigator in Spain of NoName057(16); 447 attacks in Spain since 2024 attributed to the group

6.2 The February wave: claim against measurement

Between 16 and 21 February, channels of NoName057(16), its DDoSia volunteer project and the allied group Server Killers posted target lists for Spain almost every day. The lists named central-government and ministry websites, a regional parliament, a police e-office, a national cybersecurity body, city councils, public-transport sites in several cities and private companies. Press listed the targets as temporarily unavailable on 16 and 17 February [S9]. Each target in the channels came with a link to a public availability-check report as "proof" (B10, B11).

EVIDENCE CARD B10 — 16 Feb 2026

Server Killers (relayed) Spanish-language channel relaying Server Killers · Telegram · Spanish

ORIGINAL

```
Detuvimos todos los ataques. [...] Los siguientes sitios web
ya han sido cerrados por los propietarios [...] y solo se
puede acceder a ellos a través de direcciones IP españolas
[seven ministry and government sites listed]
Prueba: [availability-check links removed]
[closing boast removed]
```

TRANSLATION

We stopped all attacks. [...] The following websites have been closed by their owners [...] and can only be reached from Spanish IP addresses. [seven sites] Proof: [links removed]. [closing boast removed]

HELD	The group's own claim, including its statement that targets restricted access to Spanish addresses.
NOT ESTABLISHED	How long any site was down, or for whom; any impact beyond the group's own claim.

EVIDENCE CARD B11 — 16 Feb 2026

NoName057(16) DDoSia Project channel · Telegram · Russian

ORIGINAL

```
Показываем Испании последствия поддержки [...]
❌ [туристический портал города] (закрыт по гео)
❌ [региональный парламент] (закрыт по гео)
❌ [общественный транспорт города]
[two further transport sites listed]
#OpSpain NoName057(16)
```

TRANSLATION

We are showing Spain the consequences of supporting [...]. [A city tourism portal] (closed by geo); [a regional parliament] (closed by geo); [city public transport]; [two further transport sites].

HELD	A dated target list, framed by the group as a response to Spain's support for Ukraine (the group's wording omitted), and the group's own note that two sites were geo-restricted.
NOT ESTABLISHED	Actual outage duration or impact.

Point	Actor claim	Official account	Press and monitor reporting
What was attacked	"Critical government infrastructure" of Spain, dozens of sites over six days (B10, B11)	No official statement during the wave	Press listed ministries, a regional parliament, transport and council sites as temporarily unavailable [S9]
Impact	Sites "closed by their owners", reachable only from Spanish addresses (B10)	None published	Most pages worked normally again when reported; a DDoS attack does not steal data [S9]
Who	NoName057(16) and Server Killers, citing Spanish support for Ukraine	No official attribution during the wave; the Policía Nacional later announced the arrest of NoName057(16)'s alleged instigator in Spain (November) [S54]	Monitors relayed the groups' own claims

Reading the panel. The group's "proof" shows that a site did not answer availability checks from abroad at one moment. It does not show how long the outage lasted, who was affected or whether the site was blocking foreign traffic on purpose. The groups themselves noted that targets had limited access to Spanish addresses. If accurate, that is a mitigation working as intended.

6.3 Claims against industrial systems

In February and March the same channels relayed claims by Z-Pentest Alliance and others of access to Spanish industrial control panels. The claims named a wastewater pumping station, an irrigation controller, a desalination pump system, industrial refrigeration and a city-bus ticketing terminal. The posts show screenshots of web control interfaces and describe changing settings.

EVIDENCE CARD B12 — 16 Feb 2026

Z-Pentest Alliance (relayed)

Spanish-language channel relaying Z-Pentest Alliance · Telegram · Spanish

ORIGINAL

```
Nuestro estudiante de la Z-Pentest Alliance obtuvo acceso
completo al sistema de control industrial de una estación de
bombeo de aguas residuales en España [site name removed]
Esta interfaz SCADA/HMI monitoriza y controla las bombas
[...]
```

TRANSLATION

Our student of the Z-Pentest Alliance gained full access to the industrial control system of a wastewater pumping station in Spain [site name removed]. This SCADA/HMI interface monitors and controls the pumps [...]

HELD	The claim and the type of interface shown.
NOT ESTABLISHED	That any setting was changed or any process affected; no operator confirmed it.

We could not verify any of these claims, and no operator or authority confirmed one in public by our cut-off. The pattern matches a December 2025 joint advisory by US and allied agencies on CARR, Z-Pentest, NoName057(16) and Sector16: opportunistic access to internet-exposed control interfaces with weak passwords, and frequent false or exaggerated claims [S55]. The posts depict claimed interfaces; their authenticity, location and internet exposure were not established. The advisory describes the general risk of internet-exposed control interfaces, so operators should check their own assets [S55].

6.4 Recruitment and data on officials

A Spanish-language Telegram channel relays NoName057(16) activity. From March onward it also asked followers for personal data of Spanish military staff, defence-industry managers and workers, and Western politicians, and asked Spanish citizens to get in touch. No response or data transfer was established. In April it named Spanish defence and drone companies as targets for such data.

EVIDENCE CARD B09 — 3 Mar 2026

Channel administrator

Spanish-language Telegram channel relaying NoName057(16) · Telegram · Spanish

ORIGINAL

```
Necesitamos
Datos de empresarios y de trabajadores de empresas
armamentísticas españolas: nombres y apellidos, fotos,
números de DNI y de pasaportes, direcciones de sus
domicilios [...]
[recruitment appeal removed]
[contact removed]
```

TRANSLATION

We need data on owners and workers of Spanish arms companies: names, photos, ID and passport numbers, home addresses [...] [recruitment appeal removed] [contact removed]

HELD	The post solicits identifying and home-address information about defence-sector personnel; later posts repeat the request.
NOT ESTABLISHED	That anyone responded or transferred data, or who runs the channel.

In January a persona calling itself Vindex published personal data of senior public officials [S56]. In August the press reported a leaked list of about 1,000 police officers, Guardia Civil agents and military personnel with names, phone numbers and photographs, which investigators were examining as linked to NoName057(16) [S57]. In November the Policía Nacional announced the arrest in Burgos of the man it described as the main instigator in Spain of NoName057(16). It said he carried out propaganda and recruitment and was building the group's first physical cell in the country [S10][S54]. We report these as official statements and press reports; arrests are not convictions.

6.5 Other claims in their own words

- **Pro-Palestinian framing.** BD Anonymous Team claimed in January to have taken down a Galician city council's website, saying it acted because, in its view, the Spanish government no longer speaks up for Palestine (B13). We found no confirmation of an outage.
- **Domestic hacktivists.** The Guardia Civil said Anonymous Fénix attacked ministries, political parties and public institutions in Spain. It spread material against Spanish institutions and those of several South American countries, with a peak after the 2024 floods in Valencia. Its four main members have been arrested: its administrator and moderator in May 2025 and two of its most active members in February 2026 [S58][S59].

EVIDENCE CARD B13 — 26 Jan 2026

BD Anonymous Team Hacktivist Telegram channel · Telegram · English, as posted

ORIGINAL

```
[claim that the group took down the official website of a
Galician city council; availability-check link removed]
[motive statement paraphrased: the group says it acted
because the Spanish government no longer speaks up for
Palestine]
BD Anonymous Team #OpSpain
```

HELD	The claim and the motive the group gives.
NOT ESTABLISHED	That the site was down for anyone other than the checker.

6.6 Lessons for defenders

1. **Plan mitigation for short waves.** The groups said several targets limited access to Spanish visitors during the February wave. Use upstream scrubbing or a content-delivery network first. Geo-filter only for a set period, with an exception route for citizens abroad, and agree in advance

who can switch it on.

2. **Pre-agree a public statement.** Most DDoS claims rely on silence. A short notice saying that a service is degraded and that there is no evidence of data access so far undercuts the claim.
3. **Take control interfaces off the internet.** Any operator of pumps, irrigation, refrigeration or ticketing equipment should check for web control panels reachable from the internet and require strong authentication.
4. **Brief staff on recruitment and doxxing.** Defence, police and public-sector staff should know that their personal data is being sought and how to report an approach.

KEY TAKEAWAYS

01

The February DDoS wave was loud and short; the groups said geo-filtering limited their reach.

02

The same channels claimed access to industrial control panels and sought data on officials.

03

Police arrests in 2026 targeted recruitment and coordination, not only attack traffic.

CHAPTER 7

Threat actors

07

THIS CHAPTER ANSWERS

Which actors left a documented mark on Spain in 2026, what links them, and what does each one mean for a Spanish defender?

220

ransomware leak-site listings for Spain, 1 January–20 November 2026

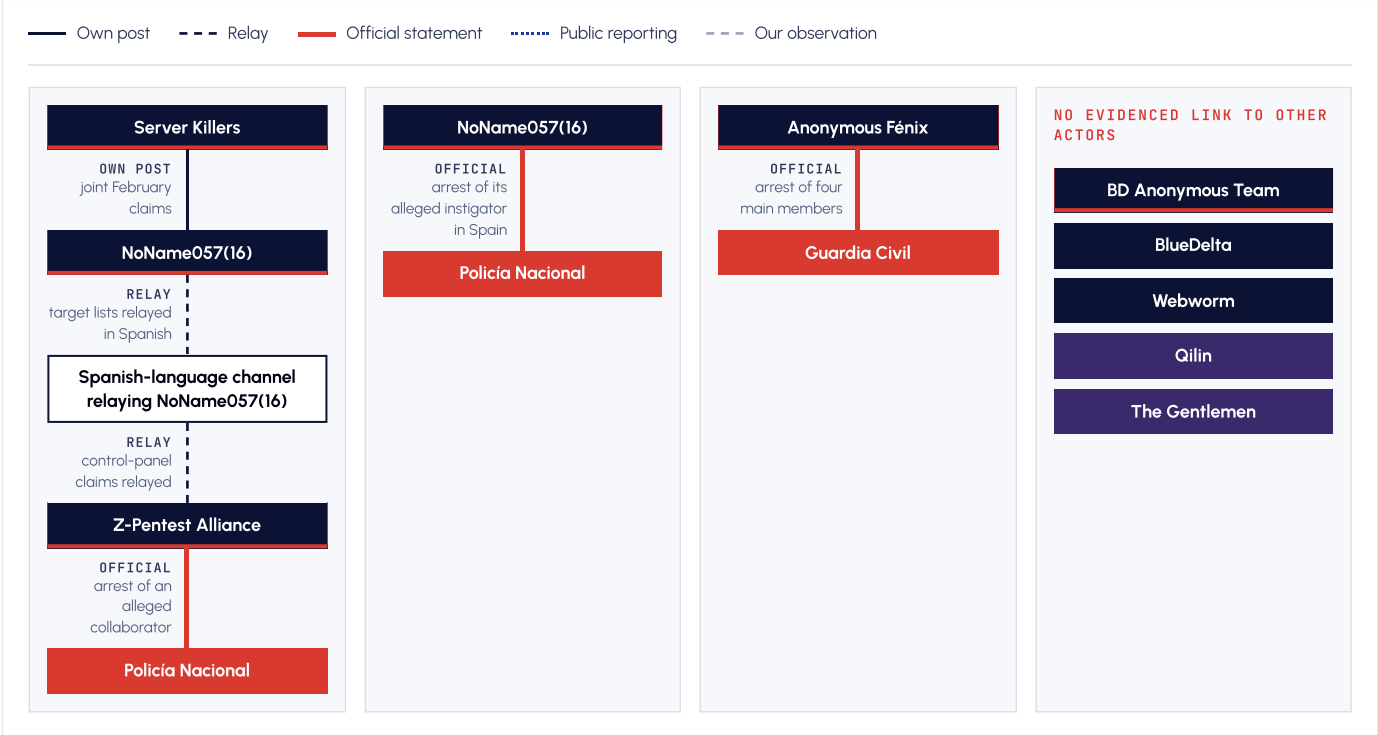
INSIDE THIS CHAPTER

7.1 How the actors connect | 7.2 State-linked espionage | 7.3 Hacktivist and DDoS actors | 7.4 Ransomware and extortion | 7.5 Criminal personas seen in Blackhole | 7.6 Unattributed intrusion campaigns

IN SHORT

Four kinds of actor shaped Spain's 2026 picture. Extortion groups, led by Qilin and The Gentlemen, posted 220 Spanish listings. Pro-Russian DDoS groups ran the loudest campaign. State-linked espionage groups used Spanish government themes and targeted Spanish public bodies, according to vendor research. Criminal sellers advertised bank accounts and customer data. Prioritise extortion readiness and tested backups, then email defences against government-themed lures.

7.1 How the actors connect



Lines show the evidence type for each link. A link means a shared post, an official statement or a vendor attribution, not a common operator. Where nothing links two actors, the map shows them alone; we do not join them into "networks" without a concrete shared element.

7.2 State-linked espionage

Actor (as named by the source)	What was observed	Attribution as stated	Meaning for Spain
BlueDelta (overlaps with APT28)	Macro-enabled Word lures, the first impersonating a Spanish ministry's meeting agenda (September 2025); campaigns to April 2026 against government, diplomatic and defence-manufacturing targets in Romania, Spain and Türkiye. The HOOKEDGE backdoor uses legitimate webhook services for control [S11]	Recorded Future Insikt Group, moderate confidence, a group it attributes to Russian military intelligence [S11]	Spanish government themes are used as bait; block macros in internet-origin documents
Webworm	New backdoors using Discord and Microsoft Graph for control; government targets in Belgium, Italy, Poland, Serbia and Spain	ESET, which describes it as China-aligned [S12]	Cloud-service C2 blends into normal traffic; monitor unusual OneDrive and Discord use from servers

BlueDelta

APT28, Fancy Bear, Forest Blizzard (overlaps per Insikt)

State-linked espionage

Attributed by Recorded Future to Russian military intelligence (GRU)

IN SPAIN, 2026

Sep 2025	First lure imitates a Spanish ministry's meeting agenda
to Apr 2026	HOOKEDGE campaigns against government, diplomatic and defence-manufacturing targets in Romania, Spain and Türkiye

CLAIMED TARGETS

Government, diplomatic and defence-manufacturing organisations

SEEN IN PUBLIC REPORTING

- [S11] Insikt Group, moderate confidence: macro-enabled Word lures deliver the HOOKEDGE backdoor, which uses webhook services for control and exfiltration
- [S11] Insikt Group: the lure's authenticity could not be verified; no compromise of the ministry is reported

OUR ASSESSMENT

Spanish government themes were used as bait. Block macros in internet-origin documents and alert on webhook-service traffic from servers.

CONFIDENCE **Moderate, as stated by the source**

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Resource Development	Execution	Persistence	Defense Evasion	Discovery	Collection
T1583.006 Web Services	T1059.003 Windows Command Shell	T1053.005 Scheduled Task	T1027.013 Encrypted/Encoded File	T1083 File and Directory Discovery	T1074.001 Local Data Staging
	T1059.005 Visual Basic		T1070.004 File Deletion		
	T1204.002 Malicious File		T1140 Deobfuscate/Decode Files or Information		

Command and Control	Exfiltration
T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel
T1105 Ingress Tool Transfer	T1567.004 Exfiltration Over Webhook

BlueDelta HOOKEDGE techniques. Technique IDs and tactics as given in Recorded Future Insikt Group's report of 27 August 2026. [S11]

Webworm

State-linked espionage | China-aligned (per ESET)

IN SPAIN, 2026

2025-26 Government organisations in Belgium, Italy, Poland, Serbia and Spain targeted

CLAIMED TARGETS

Government organisations

SEEN IN PUBLIC REPORTING

- [S12] ESET: new backdoors EchoCreep (Discord control) and GraphWorm (Microsoft Graph and OneDrive control); custom proxy tools

OUR ASSESSMENT

Cloud-service control channels blend into normal traffic. Monitor unusual Discord and OneDrive use from servers.

CONFIDENCE As stated by the source

Insikt says the lure's authenticity could not be verified and notes that BlueDelta has historically used authentic government documents, including public material [S11]. In our reading, nothing in the report indicates an intrusion at the ministry. The National Intelligence Centre said in May that Spain faces espionage as well as ransomware and influence activity [S15]. Neither campaign appeared in the leak-site and forum data we searched; the evidence for both comes from vendor research.

7.3 Hacktivist and DDoS actors

Actor	2026 activity against Spain	Evidence	Assessment
NoName057(16) and DDoSia Project	DDoS target lists in February; claims against transport ticketing in March	Own posts (B11); police statements	The most active claimant; disruption short
Server Killers	Joint DDoS claims with NoName057(16) in February	Own posts relayed (B10)	Amplifier of the February wave
Z-Pentest Alliance	Claims of access to Spanish control panels	Relayed posts (B12); allied advisory [S55]	Unverified claims; operators should check their own interfaces

Actor	2026 activity against Spain	Evidence	Assessment
A Spanish-language channel relaying NoName057(16)	Relays, recruitment and requests for data on officials	Own posts (B09)	Relays and requests for recruits and personal data; no technical capability shown
BD Anonymous Team	One claimed takedown of a council website	Own post (B13)	Single unconfirmed claim; motive given as Palestine
Anonymous Fénix	DDoS on public bodies, peaking after the 2024 floods	Guardia Civil statement [S58][S59]	Domestic group; main members arrested

NoName057(16)

DDoSia Project

Hacktivist (DDoS) | Pro-Russian (per CISA and partners)

IN SPAIN, 2026

9 Feb	Lists a Spanish sports body among sites it claims to have taken offline
16-21 Feb	Daily target lists for Spain, citing aid to Ukraine (B11)
24 Mar	Claims access to a city-bus ticketing terminal
20 Nov	Police announce the arrest of its alleged main instigator in Spain

CLAIMED TARGETS

Ministries, a regional parliament, city councils, public transport, tourism portals, private companies

IN THEIR WORDS

> *"We are showing Spain the consequences"* B11

SEEN IN PUBLIC REPORTING

- [S54] Policía Nacional: arrest in Burgos of its alleged main instigator in Spain
- [S10] Press report of the Policía Nacional statement: 447 attacks in Spain since 2024 attributed to the group
- [S81] Policía Nacional: March arrest of an alleged collaborator of the pro-Russian groups CARR and Z-Pentest
- [S55] CISA and partners: makes frequent false or exaggerated claims; volunteers run its DDoS tool

OUR ASSESSMENT

The most active claimant against Spanish public websites in 2026. Disruption was short; the group itself reported geo-restrictions, and its own figures are claims.

CONFIDENCE **High that it claimed the wave; impact unverified**

Z-Pentest Alliance

Z-Pentest

Hacktivist (OT claims) | Pro-Russian (per CISA and partners)

IN SPAIN, 2026

16 Feb	Claims full access to a wastewater pumping station's control panel (B12)
17-18 Feb	Claims access to a desalination pump system and industrial refrigeration
Mar	Further claims against Spanish control interfaces, relayed by a Spanish-language channel

CLAIMED TARGETS

Claimed control panels of pumps, irrigation, refrigeration and water treatment

IN THEIR WORDS

> *"obtuvo acceso completo al sistema de control industrial"* B12

SEEN IN PUBLIC REPORTING

- [S55] CISA and partners: one of four pro-Russian groups gaining access to exposed HMI devices, often through weak passwords
- [S81] Policía Nacional: an alleged collaborator of CARR and Z-Pentest was arrested in Palencia in March

OUR ASSESSMENT

No Spanish operator or authority confirmed any of its claims by our cut-off. The posts depict claimed interfaces whose authenticity and internet exposure were not established; CISA and partners describe the general risk, so operators should check their own assets.

CONFIDENCE **High that it posted the claims; access and impact unverified**

For defenders, the response to these actors is upstream DDoS mitigation and removing control panels from the internet (§6.6).

7.4 Ransomware and extortion

Spain had 220 leak-site listings in 2026 to 20 November, against 35 in Portugal, 286 in Italy and 295 in France

SPAIN	PORTUGAL	ITALY	FRANCE
220	35	286	295
Accepted listings, 1 Jan-20 Nov 2026	Accepted listings, 1 Jan-20 Nov 2026	Accepted listings, 1 Jan-20 Nov 2026	Accepted listings, 1 Jan-20 Nov 2026
2025: 157 · ALL TIME: 633	2025: 21 · ALL TIME: 103	2025: 161 · ALL TIME: 871	2025: 182 · ALL TIME: 885
GROUPS IN 2026: Qilin, The Gentlemen, Deadlock, NightSpire, SafePay, INC Ransom	GROUPS IN 2026: The Gentlemen, Qilin, SafePay, Majinahanashi, Nova, Booba-project	GROUPS IN 2026: Qilin, The Gentlemen, LockBit 5, SafePay, Deadlock, Space Bears	GROUPS IN 2026: Qilin, The Gentlemen, Coinbasecartel, Lapsus$, LockBit 5, NightSpire

Source: Brandefense Ransompedia accepted listings, all dates, to 20 November 2026 [S1].

Ransompedia recorded 220 accepted Spanish listings dated 1 January-20 November 2026, already more than the 157 for the whole of 2025 [S1]. Monthly counts ranged from 12 to 30. This compares a partial year with a full year, so it is not a growth rate.

Qilin posted 49, The Gentlemen 26 and Deadlock 14; the next were NightSpire (11) and SafePay (10). The top three account for 89 of 220 listings (40%); 50 other group names share the rest. The sector labels most often attached were consulting (27), manufacturing (17), construction (14), retail (14), technology (14), and health and an unspecified "global" label (13 each).

A listing is a criminal claim. It does not prove encryption, data theft or disruption, and the victim often confirms nothing. Several 2026 listings named town halls and a hospital; some named bodies confirmed an incident, others did not (Chapter 5). The Gentlemen's listing of an Indra subsidiary matches an incident the company confirmed (§5.6).

Qilin

Agenda

Ransomware and extortion · Financially motivated

IN SPAIN, 2026

2026	49 Spanish leak-site listings, the most of any group
May	Lists a Spanish supermarket chain; no confirmation found

CLAIMED TARGETS

Manufacturing, retail, services, energy and public bodies

SEEN IN PUBLIC REPORTING

- [S1] Ransompedia: 49 accepted Spanish listings dated 1 January-20 November 2026

OUR ASSESSMENT

The most frequent extortion claimant against Spanish organisations. A listing is a claim; plan recovery that does not depend on a group name.

CONFIDENCE **High for listing counts**

The Gentlemen

Ransomware and extortion · Financially motivated

IN SPAIN, 2026

Jun-Jul	Lists an Indra subsidiary; the company confirmed an incident (§5.6)
Oct	Lists a Barcelona hospital; no confirmation by our cut-off

CLAIMED TARGETS

Technology, health, logistics and services

SEEN IN PUBLIC REPORTING

- [S1] Ransompedia: 26 accepted Spanish listings, second only to Qilin
- [S40] INCIBE-CERT: cybersecurity incident at an Indra subsidiary

OUR ASSESSMENT

A frequent 2026 claimant whose Spanish listings range from technology to health.

CONFIDENCE **High for listing counts**

For defenders, plan recovery and tested backups that do not depend on which group lists you.

Law enforcement against extortion. On 30 September an international operation in which the Guardia Civil took part arrested three suspects of the KillSec extortion group, including a 16-year-old in Alicante suspected of being its administrator. Authorities linked the group to more than 1,000 attacks and more than 280 victims, seized five servers and secured at least 110 TB of stolen data [S60]. The investigation in Spain began after a 2025 attack on a Catalan organisation.

7.5 Criminal personas seen in Blackhole

Alias	Venue type	2026 activity	Note
spain	Leak forum	Endesa customer-database offer (B01)	Coincided with the company's notice
Koipo, Leads	Leak forum	Repost of the same advertisement (B02)	Reposters; contact changed
[alias withheld; it names the claimed body]	Leak forum	Public-sector database claim (B03)	Challenged as fake by forum users
IntelShadow	Leak forum	Re-uploads of older Spanish data (B05)	Reputation-building relay
Leonsky, daghetiaw	Leak forum	Electronics-retailer claims (B06)	Company denied a database breach
updap	Own site and forums	Claims against police, telecom and payment sites	Unverified; frequent poster
L34ds	Telegram	Bank-segmented customer "leads" (B07)	Feeds impersonation fraud

We list aliases only. They are personas, not identified people, and one person can use several.

7.6 Unattributed intrusion campaigns

The incidents at Adif and Renfe, the Port of Vigo and La Laguna town hall had no public attribution to a named group by our cut-off. The Castilla-La Mancha regional government was claimed by the extortion group Panzer (§5.4). Renfe said a suspect was arrested in October [S6]. We do not link these cases to any actor.

KEY TAKEAWAYS

01

Extortion groups named the most Spanish organisations; Qilin and The Gentlemen led.

02

Pro-Russian groups produced the most noise, and police targeted their Spanish recruiters.

03

Vendor research shows Spanish government themes used as espionage bait; it reports no compromise of the imitated body.

CHAPTER 8

The fraud economy

THIS CHAPTER ANSWERS

How do criminals turn Spanish identity and bank data into money, and where can banks, telecoms and public bodies break the chain?

180 USD

median asking price for a bank or payment account in posts that state one

INSIDE THIS CHAPTER

8.1 Bank and payment-account trading
8.2 Card material in posts: a narrow view
8.3 Identity, KYC and SIM services
8.4 Prices in context
8.5 What police and cyber authorities reported

IN SHORT

The most-advertised product in Spain's underground channels is bank and payment accounts: ready-made accounts, money "loads" and mule accounts, advertised mostly in Spanish-language Telegram channels. It is fed by customer lists, stolen identity documents and infostealer logs, and it pays out through impersonation calls and SMS. Police dismantled several such networks in 2026. Banks and telecoms should treat account opening, SIM changes and "safe account" calls as one chain.

8.1 Bank and payment-account trading

Bank and payment-account trading is the largest share of the cleaned Spain corpus (22,417-23,173 posts). Spanish-language Telegram channels, often named after Spanish banking, advertise four products:

Product	What is sold	How it is used
Ready-made accounts ("cuentas creadas")	Bank, neobank and crypto-exchange accounts opened with someone else's identity	To receive and move fraud proceeds
Loads ("cargas")	Funds pushed into an account from hijacked accounts or stolen cards, with a share kept by the loader	Cash-out of stolen money
Drops	Accounts of people paid to lend them, or recruited under false pretences	Money mules
Customer "leads"	Contact lists segmented by bank (Case D)	Targeting for impersonation calls and SMS

Posts name Spanish retail banks, neobanks and international e-money firms as products. Naming a brand does not mean that anyone entered that brand's systems. The accounts are opened or rented in other people's names, so the bank's own controls at onboarding and on outgoing transfers are where the chain breaks.

8.2 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

These figures cover only payment cards that appeared in clear text in the dark-web posts collected for this report. Brandefense detects stolen cards through many other methods not covered here. The figures are not a measure of card theft or fraud loss.

We found 759 distinct cards attributed to Spain in clear text in 624 posts, with 14 Spanish issuers named. Most appeared in automated checker-bot output and channel posts rather than in shops. These cards matter mainly as evidence that Spanish cards are routinely tested and resold; banks should treat any card seen in clear text as exposed and reissue it after validation. Issuers can receive such exposures from a threat-intelligence provider or through the card schemes' compromise programmes.

8.3 Identity, KYC and SIM services

KYC and identity-document offers (11,217-11,754 cleaned posts) include scans of Spanish ID cards and passports with selfies, "verified" account packs and forged-document templates. In August a Policía Nacional operation stopped a fraudster who, it said, used an AI-generated deepfake technique to obtain electronic-signature certificates in other people's names [S61]. In November the Policía Nacional arrested four people in Málaga for a network that used AI to build fraudulent websites, alongside phishing and SMS fraud [S62]. Telegram accounts on Spanish (+34) numbers are also sold, for use in scams.

8.4 Prices in context

Product	Median asking price (USD)	Middle half of prices (USD)
Bank and payment account	180	70-350
KYC and identity documents	100	35-250
Carding offers	80	15-300
Access sales	80	23-300
Phishing kits and scam services	60	25-250
Data leaks and databases	20	10-50

Prices are asking prices in posts that state one, converted where needed; they are not transaction prices. Database prices are low because most offers are resales of old data. A bank account costs more than a database because it can move money.

8.5 What police and cyber authorities reported

Date	Body	What was announced
January	Policía Nacional with Europol	34 arrests in a Black Axe-linked business email compromise network; losses over 15 years above 6 million dollars [S63]
March	Policía Nacional	Two arrests over the theft of almost ten million records from a regional education platform (a theft that came to light in 2023, separate from the July case in §5.7 and not counted among the 30), then monetised through fraud and underground sales [S64]
May	Guardia Civil	15 arrests in a bank-impersonation call network that took about 400,000 euros [S65]
June	Policía Nacional	A "son in trouble" WhatsApp fraud network that took almost 3 million euros [S66]
July	Policía Nacional	A network that took 140 million euros through computer fraud [S67]
July	Guardia Civil	Operation Fragmenta: smishing ring with a database of about 500,000 people; about 2,000 possible victims [S8]
September	Guardia Civil	Operation Ibermellow: bank-impersonation SMS network; 29 arrests, more than one million euros [S7]
October	Policía Nacional	The money-laundering arm of a cyber-fraud network that invested proceeds in wine and industrial machinery [S68]

INCIBE issued repeated warnings in 2026 about SMS and email campaigns impersonating the tax agency, the social-security treasury and the traffic authority with fake refunds and fines [S69][S70][S71]. The AEPD reported that stolen hotel-booking data was used to contact guests and demand payment, and that such cases drove much of the rise in its July breach notifications [S72].

What this means. The market and the police record describe the same chain: lists and stolen identities go in, impersonation calls and SMS create the payment, and mule accounts carry the money away. Every link has a Spanish organisation that can break it: the bank at onboarding and on transfers, the telecom at SIM changes, the public body by publishing how it really contacts citizens.

KEY TAKEAWAYS

01

Bank-account trading is the most-advertised crime family in the Spain data.

02

Impersonation of banks, the tax agency and the traffic authority is a recurring route from stolen data to money, according to police and INCIBE.

03

Police operations in 2026 hit every link of the chain, from data theft to laundering.

CHAPTER 9

Banking and finance deep dive

THIS CHAPTER ANSWERS

How exposed are Spain's banks and payment firms, and does the exposure sit in the banks or in their customers?

25 of 25
banking and payment organisations with infected-device associations

INSIDE THIS CHAPTER

9.1 What the numbers say | 9.2 Reading it | 9.3 Regulatory context

IN SHORT

Every one of the 25 banking and payment organisations we assessed has infected-device associations. Almost all are outside the employee classification; who owns those devices, and whether the data is current, is not established. Of them, 17 had a credential listed for sale on the day of the check. Banks enforce email authentication better than any other sector. Validate current listings first, and run employee-account checks and customer-fraud controls in parallel.

143,948
infected-device associations (lower bound), 298 of them employee-classified

17 of 25
had a credential listed for sale on the day of the check

23 of 25
enforce DMARC (15 reject, 8 quarantine)

9.1 What the numbers say

Signal	Banking and payment (25 organisations)
Current credential listing / listing history	17 / 17 organisations
Infected-device associations	143,948, lower bound; 298 employee-classified
Share of devices in the three largest organisations	42%
Credential records	135,365 (68,859 breach-database, 6,686 stealer-log, 59,820 combolist)
Exposed documents / lookalikes in 30 days	20 / 23 organisations
DMARC enforced / DNSSEC delegation	23 / 5 organisations
Distinct cards in clear text naming a bank in this list	414 across 13 banks; three banks hold 70%

Source: Atlas exposure ratings and Blackhole associations read 21 November 2026 [S2][S3]; DNS checks [S22]. Card figures follow the scope in §8.2.

9.2 Reading it

- **Mostly outside the employee classification.** 143,650 of 143,948 associations are not employee-classified. They come from stealer logs on devices that logged in to online banking. Many may be customers' computers, but ownership and freshness are not established. They are a fraud signal for the bank, not evidence of an intrusion.

- **Listings come first.** Of the 25 organisations, 17 had a credential listed for sale on the day of the check. Validate whether those accounts are customer or staff accounts before acting.
- **Concentration.** Three large retail banks hold 42% of device associations. The three banks with the most cards seen in clear text, not all the same banks, hold 70% of those cards. Smaller banks, cooperative banks and neobanks still appear in account-trading posts (Chapter 8).
- **Hygiene is strong.** Banking leads every sector on DMARC enforcement, which makes direct spoofing of bank domains harder and pushes criminals to lookalike domains and SMS sender names instead.

9.3 Regulatory context

INCIBE reported that banking accounted for 34% of the 401 incidents it handled at essential operators in 2025 [S20]. DORA has applied to Spanish financial entities since January 2025 (Chapter 10). Police operations in 2026 against bank-impersonation networks show where the losses fall: on customers who authorise transfers under pressure (Chapter 8).

KEY TAKEAWAYS

01

Bank device associations sit mostly outside the employee classification; their ownership and freshness are not established.

02

Current credential listings at 17 of 25 banking and payment organisations are the first accounts to validate.

03

Strong DMARC pushes impersonation to lookalike domains, SMS and calls.

CHAPTER 10

Regulatory and national response

THIS CHAPTER ANSWERS

Which rules already apply to Spanish organisations while NIS2 waits, what did regulators and police do in 2026, and what should a CISO do before the law arrives?

17 Oct 2024

NIS2 transposition deadline that Spain has not yet met

INSIDE THIS CHAPTER

10.1 Rules that apply today
10.2 What the NIS2 delay means
10.3 What regulators reported in 2026
10.4 What police reported in 2026
10.5 What CISOs should do now

IN SHORT

Spain's NIS2 law is still a draft, but organisations are not in a vacuum. Data-protection breach notification, the National Security Scheme for the public sector and its suppliers, the existing network-security decree and DORA for finance all apply today. The AEPD reported rising breach notifications and flagged booking-software breaches, and police dismantled several fraud and hacktivist networks. Map your obligations to the rules in force now, and prepare for NIS2 without waiting for its text.

10.1 Rules that apply today

Rule	Who it covers	What it requires	Notify whom	Status at our cut-off
EU General Data Protection Regulation and Organic Law 3/2018 (LOPDGDD)	Any organisation processing personal data	Controllers notify the authority without undue delay and, where feasible, within 72 hours of becoming aware, unless the breach is unlikely to put people at risk. Processors notify the controller without undue delay. Controllers tell affected people when the risk is likely to be high, unless an exception applies (GDPR Art. 33-34)	The AEPD; public bodies in Catalonia, the Basque Country and Andalusia notify their regional authority (APDCAT, AVPD or the Andalusian Council for Transparency and Data Protection)	In force
National Security Scheme (ENS), Royal Decree 311/2022	Public sector bodies and private suppliers of their systems	Security categorisation, controls, incident reporting	Public bodies: CCN-CERT. Private suppliers: INCIBE-CERT, which passes the notice to CCN-CERT	In force
Royal Decree-law 12/2018 and Royal Decree 43/2021 (NIS1 transposition)	Operators of essential services and digital service providers	Security measures and incident notification	The competent CSIRT: INCIBE-CERT for private operators, CCN-CERT for the public sector; operators relevant to national defence notify their CSIRT, which informs ESPDEF-CERT	In force until replaced
EU Digital Operational Resilience Act (DORA)	Banks, insurers, investment firms and other financial entities	ICT risk management, major-incident reporting, third-party oversight	The competent authority: Banco de España for banks (the ECB supervises significant banks; confirm the reporting channel with your supervisor), the CNMV or the Directorate-General for Insurance (DGSFP)	Applies since 17 January 2025

Rule	Who it covers	What it requires	Notify whom	Status at our cut-off
NIS2 Directive (EU) 2022/2555	Essential and important entities in 18 sectors	Management accountability, risk measures, 24-hour early warning	Not yet set in Spanish law	Not transposed; the draft had not been submitted to the Cortes by our cut-off

Sources: `[S73][S74][S75][S76][S77][S78][S18][S19]`. This table is a planning aid, not legal advice. Check the consolidated texts in the Official State Gazette (BOE) before relying on any line.

10.2 What the NIS2 delay means

The European Commission referred Spain to the Court of Justice on 8 July 2026 for failing to notify full transposition, and asked for a lump sum and daily penalties `[S18]`. The draft law, published as a preliminary draft (anteproyecto) in January 2025, had not been submitted by the cut-off. Its future legislative timetable is uncertain. Article 21 of the Government Act restricts a caretaker government's submission of bills `[S79]`. Transposition by royal decree-law remains legally possible `[S19]`.

Until then, entities that NIS2 would cover have no Spanish NIS2 statute. Public bodies may still face directly effective provisions, and many entities already fall under the ENS, NIS1 or DORA.

In practice, the delay changes the deadline, not the work. NIS2 asks for things that 2026 incidents show are needed anyway: supplier security, multi-factor authentication, tested backups and fast reporting.

10.3 What regulators reported in 2026

The Spanish Data Protection Agency (AEPD) publishes monthly reports on breach notifications. It received 788 notifications in March and 919 in July 2026 `[S80][S72]`. Its July report singled out hotels and their booking-software providers: criminals used stolen reservation data to contact guests and demand payment for bookings `[S72]`. In September the AEPD reported the first breach notification in Spain where the attack was described as carried out by an AI agent. The agency stressed that the details come from the notifying organisation and still need analysis `[S46]`.

10.4 What police reported in 2026

Spanish police announced several operations against groups whose activity matches the threats in this report. Fraud and data-theft operations are listed in §8.5; the table below adds the hacktivist, extortion and related cases. We list them as announced; arrests are not convictions.

Date	Force	What was announced
February	Guardia Civil	The four main members of the hacktivist group Anonymous Fénix arrested over DDoS attacks on public bodies, two of them in 2025 `[S58]`
July (arrest in March)	Policía Nacional, on an FBI tip	Arrest of an alleged collaborator of the pro-Russian groups CARR and Z-Pentest `[S81]`
30 September	Guardia Civil and partners	International operation against the KillSec extortion group; a 16-year-old suspected administrator arrested in Alicante `[S60]`
November	Policía Nacional	Announced arrest in Burgos of the alleged main instigator in Spain of NoName057(16) `[S10][S54]`

10.5 What CISOs should do now

1. **Map today's obligations.** List which of the GDPR, ENS, NIS1 and DORA apply to you and to each critical supplier.
2. **Rehearse the notification clock.** From the moment of awareness, practise deciding whether to notify the AEPD or your regional authority within 72 hours. Decide also whether to tell affected people. Include legal, communications and the supplier.

3. **Write supplier clauses for breach notice.** Processors must tell you without undue delay, and the terms should support your own clock. Four of the 30 confirmed 2026 incidents in this report started at a provider (Chapter 5).
4. **Build the NIS2 file now.** Board approval of risk measures, an asset inventory and a 24-hour early-warning procedure carry over to whatever law is passed.

KEY TAKEAWAYS

01

NIS2 is delayed in Spain, but breach notification, the ENS and DORA already apply.

02

Regulators flagged supplier and booking-software breaches as a growing source of notifications.

03

Police operations in 2026 targeted the same fraud and hacktivist activity this report observes.

CHAPTER 11

Outlook

THIS CHAPTER ANSWERS

What should Spanish organisations plan for next, and what evidence would change that plan?

5
key judgements, each with a signal to watch

INSIDE THIS CHAPTER

11.1 Key judgements | 11.2 What would change the assessment | 11.3 Conditional scenarios

IN SHORT

Plan for the threats that recurred through 2026. Customer-data incidents at large consumer brands and their suppliers, extortion of smaller public bodies, bank-impersonation fraud and short pro-Russian DDoS waves all came back during the year. AI-assisted intrusion appeared in official reporting for the first time. Leak-site listings passed their 2025 total before the year ended, as in neighbouring countries; we have no other comparable time series. Assign an owner to each signal below and review the plan monthly.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Identity exposure (devices, stealer logs, credential listings) is the most widespread measurable risk to Spain's leading organisations	High for the 250-organisation list	241 with devices, 243 with credential records, 163 with current listings; not national prevalence
If group activity holds, extortion groups will keep listing Spanish organisations at a pace similar to 2026	Medium (conditional)	220 listings to 20 November 2026, against 157 in all of 2025; Portugal, Italy and France passed their 2025 totals by wider margins. Listings are claims, and group activity shifts quickly
Customer-data incidents will keep starting at suppliers and secondary systems	Medium	Five of the confirmed 2026 incidents started at a provider or a secondary system; small sample
If actor channels keep citing Spanish support for Ukraine, plan for pro-Russian DDoS claims against public sites	Medium (planning assumption)	The February wave cited it; signal: target lists in actor channels
AI agents will appear in more intrusion reports	Low to medium	One AEPD notification, a Guardia Civil arrest of an intruder it said used AI (§5.4), and unconfirmed press reports on Renfe and Adif (§5.3); the AEPD said this first notification does not establish a statistical trend `[S46][S32][S26]`

11.2 What would change the assessment

Current interpretation	Evidence that would change it	Decision affected
Most large database claims against state bodies are unverified or false	An official confirmation, or a sample matched to a known schema	Trigger notification and customer-protection actions for that dataset
DDoS waves are short	Official confirmation of a sustained outage of an essential service	Revisit upstream mitigation capacity and continuity plans

Current interpretation	Evidence that would change it	Decision affected
Industrial-control claims are unverified	An operator or authority confirms manipulation of a physical process	Prioritise removing control interfaces from the internet across the sector
Current listings mean "validate", not "breached"	Validation finds active accounts without MFA among listed credentials	Escalate to incident response and enforce MFA for the affected users
NIS2 is not yet law in Spain	Publication of the transposition law in the BOE	Re-baseline obligations, deadlines and reporting channels

11.3 Conditional scenarios

These scenarios are planning assumptions, not measured intervals.

- **If** a large consumer brand confirms a customer-data incident, **then** plan for phishing and calls to its customers that quote real contract details. **Signal:** the company's notice and resale posts. **Decision:** warn customers and brief call centres the same day.
- **If** a pro-Russian channel posts a target list naming your sector, **then** plan for short DDoS bursts over the following days. **Signal:** availability-check links in actor channels. **Decision:** switch on upstream mitigation and the pre-agreed status statement.
- **If** a new critical vulnerability in an internet-facing product is disclosed, **then** plan for exploitation attempts by extortion groups. **Signal:** vendor advisories and CCN-CERT or INCIBE-CERT warnings. **Decision:** patch and verify internet-facing systems first, then hunt for persistence.

KEY TAKEAWAYS

01

Plan for the threats that recurred all year: customer-data incidents, extortion, impersonation fraud and DDoS.

02

Each judgement has a signal; change the plan when the signal changes.

03

AI-assisted intrusion is now on the record in Spain, but one case is not yet a trend.

CHAPTER 12

Action plan

THIS CHAPTER ANSWERS

What should each team do in the next 90 days, and how will the board know it was done?

23
actions with an owner and completion evidence

INSIDE THIS CHAPTER

12.1 30/60/90 days | 12.2 By role | 12.3 How Brandefense can help

IN SHORT

Start by confirming you receive credential-listing and device alerts, then act on the evidence that is specific to you: current listings, employee devices and internet-facing systems. Next, close supplier, email and customer-fraud gaps, and rehearse a combined DDoS and data-leak scenario. The board knows the work is done from each row's completion evidence and the scorecard below; report both by day 90.

12.1 30/60/90 days

This is a sequence, not a waiting period. A current material threat should enter your incident process immediately.

1 Days 1-30

Confirm that you receive credential-listing and infected-device alerts for your primary domains, from any provider or service you choose; if not, arrange them

OWNER
CISO and threat intelligence

COMPLETION EVIDENCE
Alert source named; first alert received

For every current credential listing tied to your domains, validate the account and its MFA status within 5 working days

OWNER
Identity team

COMPLETION EVIDENCE
Each listing has a disposition: reset, already remediated, or not ours, with a date

Validate employee-classified device associations; revoke sessions and tokens where active

OWNER
Identity and endpoint teams

COMPLETION EVIDENCE
Device list reconciled with asset inventory; revocations logged

2 Days 31-60

Where DMARC is p=none or missing, inventory senders and stage enforcement

OWNER
Messaging

COMPLETION EVIDENCE
Aligned senders; p=quarantine with a rollback route

Agree who can switch on upstream DDoS mitigation and time-boxed geo-filtering for public portals, and test it

OWNER
Infrastructure

COMPLETION EVIDENCE
Test record with time to activate

Patch and verify internet-facing systems against CCN-CERT and INCIBE-CERT warnings on exploited vulnerabilities

OWNER
Infrastructure

COMPLETION EVIDENCE
List of internet-facing systems with patch dates

Triage lookalike domains and request takedown of confirmed phishing sites (§3.5)

OWNER
Threat intelligence and legal

COMPLETION EVIDENCE
Lookalike list with a disposition per domain

3 Days 61-90

Run a timed restore test of one critical system

OWNER
Infrastructure

COMPLETION EVIDENCE
Restore time recorded against the recovery time objective

Sign DNS for primary domains where the registrar supports it; fix invalid TLS certificates

OWNER
Network and web teams

COMPLETION EVIDENCE
DNSSEC validates from an external resolver; certificates pass

Run a tabletop combining a DDoS wave with a simultaneous data-leak claim

OWNER
CISO, communications, legal

COMPLETION EVIDENCE
Decision log and timings

Build the NIS2 file: board approval of risk measures, an asset inventory and a 24-hour early-warning procedure (§10.5)

OWNER
CISO and board secretary

COMPLETION EVIDENCE
File approved by the board

List every supplier that holds your customer data and ask how fast it will notify you of a breach

OWNER
Procurement, legal and CISO

COMPLETION EVIDENCE
Supplier list with a notification commitment per supplier

Name the spokesperson and channel for service-status statements during DDoS and for unverified leak claims

OWNER
Communications, CISO and legal

COMPLETION EVIDENCE
A one-page playbook, approved

Rehearse the GDPR breach-notification decision and its 72-hour clock with legal and a key supplier

OWNER
Data protection officer and legal

COMPLETION EVIDENCE
Timed exercise record

Map GDPR, ENS, NIS1 and DORA duties for your organisation and each critical supplier, including whom to notify (§10.1)

OWNER
Legal and CISO

COMPLETION EVIDENCE
Obligation register

Public bodies: publish your official contact channels and what you never ask citizens for

OWNER
Communications

COMPLETION EVIDENCE
Page live and linked from the home page

Remove industrial and building-control web interfaces from the internet, or put them behind VPN and strong authentication

OWNER
OT and facilities

COMPLETION EVIDENCE
External check shows no exposed control panel

Banks and payment firms: add friction to first transfers to new payees and to "safe account" patterns; repeat customer warnings

OWNER
Fraud and digital channels

COMPLETION EVIDENCE
Rule live; warning sent

Telecoms: require strong verification for SIM changes and number porting

OWNER
Fraud and customer operations

COMPLETION EVIDENCE
Procedure signed off; test case caught

Brief call centres never to request full bank details or codes on inbound contact, and to warn customers who report such calls

OWNER
Customer operations

COMPLETION EVIDENCE
Script updated; staff briefed

Move privileged and remote users to phishing-resistant MFA (FIDO2 keys, passkeys or certificates)

OWNER
Identity team

COMPLETION EVIDENCE
Coverage recorded per user group

Block macros in documents from the internet and alert on outbound connections to webhook services from servers

OWNER
Endpoint and SOC

COMPLETION EVIDENCE
Policy enforced; alert tested

Report the scorecard against targets (below)

OWNER
CISO to board

COMPLETION EVIDENCE
Board paper with remaining gaps and owners

Scorecard targets. These are suggested defaults; set your own where policy differs.

Measure	Target
Current listings with a disposition within 5 working days	100% by day 90

Measure	Target
Employee-classified devices reconciled with the asset inventory	100% by day 90
Suppliers holding customer data with a breach-notification commitment	100% by day 90
Primary domains with DMARC at quarantine or reject	100%, or a dated plan, by day 90
Privileged and remote users on phishing-resistant MFA	100%, or a dated plan, by day 90
Restore test within the recovery time objective	Passed, or a dated fix, by day 90

12.2 By role

Role	First decision
Board	Ask for your current-listing and employee-device numbers and the date by which each is validated
CISO	Put listing and device monitoring in place, then supplier notification and internet-facing patching
SOC	Add detections for macro documents, webhook-service traffic from servers, and sign-ins from new devices for accounts seen in stealer logs (§3.3, Case E)
Fraud	Watch first transfers to new payees, SIM changes and accounts that receive and forward funds within hours
Communications	Prepare statements for DDoS and for unverified leak claims, separating claim, verified fact and action

KEY TAKEAWAYS

01
Confirm monitoring, then validate current listings and employee devices in the first 30 days.

02
Close supplier, DMARC, control-panel and customer-fraud gaps by day 60.

03
Test restore, sign DNS and rehearse a combined DDoS and leak scenario by day 90.

12.3 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The analysis in this report used the same data and ratings that the platform applies to monitored organisations: infected-device and credential associations, current credential-market listings, lookalike domains, exposed documents and dark-web mentions. It does not promise that every claim can be verified or that a historical record remains usable.

Bring your domains, brands and security priorities to a 30-45 minute demo with our team. The team can show how platform monitoring relates external signals to the assets you manage. A Brandefense team member or a partner in your region will follow up.

Request a demo

Appendix A. Method

A.1 Window, sources and priority

The research window is 1 January-20 November 2026 by the date a post or listing was published, not the date it was collected. Own data comes first: Brandefense Blackhole (dark-web and messaging posts, infected-device and credential associations, card material in posts), Ransompedia

(ransomware leak-site listings) and Brandefense Atlas exposure ratings.

External sources give context and are cited only after the supporting passage was read. Data were extracted on 21 November 2026. Brandefense's own data have no public address; every external source in Appendix C carries a link and a "verified on" date.

A.2 Blackhole posts

Item	Value
Posts with the Spain country tag	932,584
Turkish-language bot family	About 87% of tagged posts; advertising noise
Relevant posts after cleaning	58,657-62,086, a range rather than a single count

Cleaned counts are still an upper bound for criminal activity: some channels post the same offer daily, and some posts concern several countries at once. The bot family's January-February peak appears in every comparator country. Its June-July rise is far larger for Spain than for any comparator, and is still Turkish-language template traffic. We do not read either peak as Spain-specific.

A.3 The 250 organisations

Population and limits are in §3.1. Each organisation received an Atlas exposure rating. The measured signal counts in Chapter 3 are reported separately from the rating. Data were read on 21 November 2026. Some device totals are lower bounds.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating. This report publishes only the national headline (66), not sector or organisation ratings. Treat a current credential-market listing as a reason to validate accounts, not as proof of a breach.

A.5 DNS, TLS and web checks

Email, DNS, TLS and homepage results come from public, passive checks made on 21 November 2026. "DMARC enforced" means a reject or quarantine policy; a p=none policy or no record means no enforcement.

A.6 Card material in posts

Scope: only payment cards that appeared in clear text in the dark-web posts collected for this report. Brandefense detects stolen cards through many other methods, which are outside this report. These figures do not measure card theft or fraud loss. Figures are reported at issuer level only.

A.7 Ransomware

We used Ransompedia accepted listings for Spain, Portugal, Italy and France, dated by publication. The 2026 figures cover 1 January-20 November and the 2025 figures the full year, so the two are not a matched-period growth rate.

A.8 Incident coverage

Incident coverage draws on Blackhole posts and on public reporting for the whole window. Public sources include national and regional press, INCIBE, INCIBE-CERT and CCN-CERT reporting, Ministry of the Interior press notes for the Policía Nacional and the Guardia Civil, the AEPD and vendor research.

Coverage limits.

- Sales arranged privately leave few public traces, so post counts understate them.
- Posts removed early may be missing.

- Incidents that organisations handle without disclosure stay invisible.

That an incident is absent from this report does not mean it did not happen.

A.9 Confidence and boundaries

High confidence applies to a reproducible measurement, not to a criminal's underlying assertion. Medium indicates an interpretation with a clear supporting line and stated limits. "Unverified" means not independently established; it is neither proof of fabrication nor proof of a breach. Victim organisations are described by role; an organisation is named only where it or an authority confirmed the incident and it was widely reported.

Smaller confirmed cases are described by role even where the cited source names them (§5.1). Actor aliases are printed; links, contacts, indicators and personal data are withheld. Full provenance is held in an internal evidence register.

Appendix B. Evidence register

Every post quoted in this report appears as a redacted post card in the chapter shown. Excerpts are short; omissions are marked [...]; identifiers, contacts, links and victim organisations are replaced with labels in brackets, under the policy in A.9. Translations are ours unless the post carried the actor's own English. Posting dates are not intrusion dates. Post identifiers, links and full text are held internally.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-01-04	Leak forum	spain	English	§4.4
B02	2026-02-16	Leak forum	Koipo	English	§4.6
B03	2026-01-31	Leak forum	[alias withheld; it names the claimed body]	English, with Spanish field names	§4.4
B04	2026-02-02	Leak forum	Forum user	English	§4.4
B05	2026-01-30	Leak forum	IntelShadow	English, with Spanish field names	§4.6
B06	2026-02-05	Leak forum	Leonsky	English	§4.4
B07	2026-02-28	Banking-services Telegram channel	L34ds	Spanish and English	§4.6
B08	2026-01-01	Spanish-language banking-fraud Telegram channel	Anonymous poster	Spanish	§4.6
B09	2026-03-03	Spanish-language Telegram channel relaying NoName057(16)	Channel administrator	Spanish	§6.4
B10	2026-02-16	Spanish-language channel relaying Server Killers	Server Killers (relayed)	Spanish	§6.2
B11	2026-02-16	DDoSia Project channel	NoName057(16)	Russian	§6.2
B12	2026-02-16	Spanish-language channel relaying Z-Pentest Alliance	Z-Pentest Alliance (relayed)	Spanish	§6.3
B13	2026-01-26	Hacktivist Telegram channel	BD Anonymous Team	English, as posted	§6.5
B14	2026-08-21	Persona's own leak site	updap	English	§4.5
B15	2026-06-26	Leak forum (automated bot)	Forum bot	English	§4.6

Card	Posted	Venue	Alias as shown	Language	Shown in
B16	2026-11-04	Leak forum	Forum persona	English	§4.6

Appendix C. Sources

S1 Brandefense Ransompedia, accepted listings for Spain, Portugal, Italy and France, extracted 21 November 2026.

S2 Brandefense Atlas exposure ratings and Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, read 21 November 2026.

S3 Brandefense Blackhole post corpus concerning Spain, post dates 1 January–20 November 2026, extracted 21 November 2026.

S4 INCIBE, "Endesa notifica a sus clientes una filtración de datos personales". https://www.incibe.es/ciudadania/avisos/endesa-notifica-sus-clientes-una-filtracion-de-datos-personales. Verified on 21 November 2026.

S5 OCU, "Filtración de datos en Naturgy". https://www.ocu.org/tecnologia/ciberseguridad/noticias/filtracion-datos-naturgy. Verified on 21 November 2026.

S6 Diario Avanza, "Renfe alerta de un ciberataque que pudo exponer DNI, contraseñas y viajes de sus clientes". https://www.diarioavanza.es/nacional/renfe-alerta-ciberataque-que-pudo-exponer-dni-contrasenas-viajes-clientes/20261120090703031011.html. Verified on 21 November 2026.

S7 Moncloa.com (private news site), "La Guardia Civil desarticula en la operación Ibermellow una red de ciberestafas bancarias con 29 detenidos". https://www.moncloa.com/2026/09/15/guardia-civil-operacion-ibermellow-ciberestafas-detenidos-3431938/. Verified on 21 November 2026.

S8 CLM24, "La Guardia Civil desmantela una red con datos de 500.000 personas". https://www.clm24.es/articulo/toledo/guardia-civil-desmantela-red-datos-500000-personas/20260722125737480099.html. Verified on 21 November 2026.

S9 Escudo Digital, "El grupo pro-ruso Noname057(16) vuelve a paralizar distintas instituciones españolas con ataques DDoS". https://www.escudodigital.com/ciberseguridad/ataques-ddos-gobierno-espana-noname057.html. Verified on 21 November 2026.

S10 Moncloa.com (private news site), "La Policía Nacional detiene en Burgos al instigador de la célula en España del ciberterrorismo prorruso NoName057(16)". https://www.moncloa.com/2026/11/20/policia-nacional-noname057-ciberterrorismo-burgos-3471612/. Verified on 21 November 2026.

S11 Recorded Future Insikt Group, "BlueDelta targets defense and diplomacy with HOOKEDGE". https://www.recordedfuture.com/research/bluedelta-targets-with-hookedge. Verified on 21 November 2026.

S12 ESET, "ESET uncovers the expanded arsenal of China-aligned Webworm; European governments targeted". https://www.eset.com/us/about/newsroom/research/eset-research-china-aligned-webworm-european-governments-targeted/. Verified on 21 November 2026.

S13 DataReportal (Kepios), "Digital 2027: Spain". https://datareportal.com/reports/digital-2027-spain. Verified on 21 November 2026.

S14 El Español, "España ya es, tras Ucrania e Israel, el país más atacado por hackers rusos y chinos, según el último informe del CNI". https://elespanol.com/espana/20260711/espana-ucrania-israel-pais-atacado-hackers-rusos-chinos-ultimo-informe-cni/1003744316174_0.amp.html. Verified on 21 November 2026.

S15 El Español, "El CNI advierte que España es uno de los países más ciberatacados del mundo". https://www.elespanol.com/observatorio-defensa/20260505/cni-advierte-espana-paises-ciberatacados-mundo-toda-clase-artefactos/1003744233968_0.html. Verified on 21 November 2026.

S16 Legal Today, "El BOE publica el Real Decreto de disolución de las Cortes y la convocatoria electoral para el 29 de noviembre". https://www.legaltoday.com/actualidad-juridica/noticias-de-derecho/el-boe-publica-el-real-decreto-de-disolucion-de-las-cortes-y-la-convocatoria-electoral-para-el-29-de-noviembre-2026-10-06/. Verified on 21 November 2026.

S17 Demócrata, "Interior pone en marcha la red de seguridad para anticipar riesgos como ciberataques y desinformación el 29N". https://www.democrata.es/politica/interior-pone-en-marcha-la-red-de-seguridad-para-anticipar-riesgos-como-ciberataques-y-desinformacion-el-29n/. Verified on 21 November 2026.

S18 European Commission, "Commission refers Ireland, Spain, France and the Netherlands to the Court of Justice for failing to transpose rules". https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules. Verified on 21 November 2026.

S19 Cuatrecasas, "Ciberataques en sectores críticos: a la espera de NIS2". https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/ciberataques-sectores-criticos-espera-nis2. Verified on 21 November 2026.

S20 España Digital / INCIBE, "INCIBE gestionó 122.223 incidentes de ciberseguridad en 2025, un 26% más que el año anterior". https://espanadigital.gob.es/actualidad/incibe-gestiono-122223-incidentes-de-ciberseguridad-en-2025-un-26-mas-que-el-ano. Verified on 21 November 2026.

S21 3Cat, "Ciberatacs informàtics: es doblen els ciberincidents a sistemes públics". https://www.3cat.cat/3catinfo/ciberatacs-informatics-es-doblen-el-nombre-de-ciberincidents-a-sistemes-publics/noticia/3406320/. Verified on 21 November 2026.

S22 Brandefense public DNS, TLS and homepage checks of 250 domains, 21 November 2026.

S23 PcComponentes, "Actualización importante oficial sobre la seguridad de los datos". https://www.pccomponentes.com/actualizacion-importante-oficial-seguridad-datos. Verified on 21 November 2026.

S24 Escudo Digital, "Report that a public-sector body ruled out a claimed database breach, February 2026". https://www.escudodigital.com/ (article URL withheld). Verified on 21 November 2026.

S25 The Register, "Spanish power giant sparks breach probe amid claims of massive data grab". https://www.theregister.com/2026/01/14/endesa_breach/. Verified on 21 November 2026.

S26 Maldita, "Qué sabemos sobre el uso de inteligencia artificial en el ciberataque a Renfe y Adif". https://maldita.es/desinfo/20260929/renfe-sufre-un-ciberataque-siendo-el-primero-realizado-con-inteligencia-artificial-a-un-organismo-publico-en-espana/. Verified on 21 November 2026.

S27 The Cyber Express, "Port Of Vigo Cyberattack Disrupts Cargo Systems". https://thecyberexpress.com/port-of-vigo-cyberattack-disrupts-systems/. Verified on 21 November 2026.

S28 Escudo Digital, "Las copias de seguridad salvan al Concello de Sanxenxo de un ataque de ransomware". https://www.escudodigital.com/ciberseguridad/las-copias-de-seguridad-salvan-al-concello-de-sanxenxo-de-un-ataque-de-ransomware.html. Verified on 21 November 2026.

S29 Escudo Digital, "El Ministerio de Ciencia reconoce haber sufrido un hackeo, aunque con un alcance muy limitado". https://www.escudodigital.com/ciberseguridad/ministerio-ciencia-filtracion-datos.html. Verified on 21 November 2026.

S30 Escudo Digital, "El Ayuntamiento de Valdemoro sufre un ciberataque". https://www.escudodigital.com/ciberseguridad/ayuntamiento-valdemoro-ciberataque-ransomware.html. Verified on 21 November 2026.

S31 MiCiudadReal, "Suspendida la Plataforma de gestión de la Zona de Bajas Emisiones de Ciudad Real debido a un "incidente" de ciberseguridad". https://www.miciudadreal.es/2026/06/16/suspendida-la-plataforma-de-gestion-de-la-zona-de-bajas-emisiones-de-ciudad-real-debido-a-un-incidente-de-ciberseguridad/. Verified on 21 November 2026.

S32 Ministerio del Interior, "La Guardia Civil detiene en Ciudad Real a un hacker que utilizaba inteligencia artificial para perpetrar ciberataques". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Guardia-Civil-detiene-en-Ciudad-Real-a-un-hacker-que-utilizaba-inteligencia-artificial-para-perpetrar-ciberataques/. Verified on 21 November 2026.

S33 Escudo Digital, "Castilla-La Mancha confirma el ciberataque de Panzer". https://www.escudodigital.com/ciberseguridad/castilla-la-mancha-confirma-el-ciberataque-de-panzer-que-reivindica-el-robo-de-datos-de-alumnos-y-familias.html. Verified on 21 November 2026.

S34 RTVC, "Un incidente de ciberseguridad afecta a varios sistemas y servicios digitales del Ayuntamiento de La Laguna". https://rtvc.es/incidente-ciberseguridad-afecta-varios-sistemas-servicios-digitales-ayuntamiento-la-laguna-2-noviembre-2026/. Verified on 21 November 2026.

S35 Escudo Digital, "Un ciberataque obliga a la Universidad de Alicante a desactivar parte de sus servicios digitales". https://www.escudodigital.com/ciberseguridad/universidad-alicante-ciberataque.html. Verified on 21 November 2026.

S36 Escudo Digital, "La Universitat de València confirma haber sufrido un ciberataque". https://www.escudodigital.com/ciberseguridad/la-universitat-de-valencia-confirma-haber-sufrido-un-ciberataque.html. Verified on 21 November 2026.

S37 INCIBE-CERT, "Acceso no autorizado a información clínica del Servicio Extremeño de Salud". https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/acceso-no-autorizado-informacion-clinica-del-servicio-extremeno-de-salud. Verified on 21 November 2026.

S38 FashionUnited, "Inditex suffers cyberattack". https://fashionunited.com/news/business/inditex-suffers-cyberattack/2026041671809. Verified on 21 November 2026.

S39 Escudo Digital, "Basic-Fit sufre una brecha de datos que afecta a sus usuarios españoles". https://www.escudodigital.com/ciberseguridad/basic-fit-sufre-una-brecha-de-datos-que-afecta-a-sus-usuarios-espanoles.html. Verified on 21 November 2026.

S40 INCIBE-CERT, "Cybersecurity incident at an Indra subsidiary". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/cybersecurity-incident-indra-subsidiary. Verified on 21 November 2026.

S41 Escudo Digital, "Lidl informa a sus clientes en España sobre una filtración de datos". https://www.escudodigital.com/ciberseguridad/lidl-informa-a-sus-clientes-en-espana-sobre-una-filtracion-de-datos.html. Verified on 21 November 2026.

S42 GCN, "Breach at Spanish ministry vendor exposes sensitive information". https://gcn.com/breach-at-spanish-exposes-sensitive-information/17490/. Verified on 21 November 2026.

S43 RTVC, "La web del Ayuntamiento de Adeje sufre un ciberataque". https://rtvc.es/la-web-del-ayuntamiento-de-adeje-sufre-un-ciberataque-21-enero-20267/. Verified on 21 November 2026.

S44 INCIBE-CERT, "Investigation into a possible data breach relating to Leroy Merlin's Hogami". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/investigation-possible-data-breach-relating-leroy-merlins-hogami. Verified on 21 November 2026.

S45 Merca2, "Ciberataque a la Junta de Andalucía: datos de profesores y alumnos del sistema Séneca, en riesgo". https://www.merca2.es/2026/07/26/ciberataque-junta-andalucia-sistema-seneca-2424273/. Verified on 21 November 2026.

S46 AEPD, "Primera notificación de una brecha de datos personales causada por un ataque ejecutado mediante un agente de IA". https://www.aepd.es/prensa-y-comunicacion/blog/primera-notiviacion-brecha-datos-personales-causada-por-ataque-ejecutado-mediante-agente-ia. Verified on 21 November 2026.

S47 INCIBE-CERT, "Security incident in Levante UD systems with possible impact on personal data". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/security-incident-levante-ud-systems-possible-impact-personal-data. Verified on 21 November 2026.

S48 Escudo Digital, "GAME sufre un ciberataque que expone los datos personales e historiales de compra de sus clientes". https://www.escudodigital.com/ciberseguridad/game-ciberataque-brecha-datos.html. Verified on 21 November 2026.

S49 INCIBE-CERT, "Interrail takes action after security incident exposes its passengers' data". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/interrail-takes-action-after-security-incident-exposes-its-passengers-data. Verified on 21 November 2026.

S50 INCIBE-CERT, "Detection of unauthorised access to Booking user data". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/detection-unauthorized-access-booking-user-data. Verified on 21 November 2026.

S51 UOC, "Un incidente de seguridad del proveedor Canvas afecta a la UOC". https://www.uoc.edu/es/news/2026/un-incidente-de-seguridad-del-proveedor-canvas-afecta-a-la-uoc. Verified on 21 November 2026.

S52 INCIBE-CERT, "Data breach at Revolut following fraudulent government requests". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/data-breach-revolut-following-fraudulent-government-requests. Verified on 21 November 2026.

S53 Escudo Digital, "Smartbox sufre un ciberataque que expone los nombres y correos de sus clientes". https://www.escudodigital.com/ciberseguridad/smartbox-cajas-regalo-ciberataque-brecha-seguridad.html. Verified on 21 November 2026.

S54 Ministerio del Interior, "La Policía Nacional frustra la implantación de la primera célula en España de la organización ciberterrorista NoName057(16)". https://www.interior.gob.es/opencms/en/detail-pages/article/La-Policia-Nacional-frustra-la-implantacion-de-la-primera-celula-en-Espana-de-la-organizacion-ciberterrorista-NoName05716/. Verified on 21 November 2026.

S55 CISA, FBI, NSA and partners, "Pro-Russia hacktivists conduct opportunistic attacks against US and global critical infrastructure (AA25-343A)". https://media.defense.gov/2025/Dec/09/2003840175/-1/-1/0/JOINT_CSA_PRO-RUSSIA_HACKTIVISTS_CONDUCT_ATTACKS_AGAINST_CRITICAL_INFRASTRUCTURE.PDF. Verified on 21 November 2026.

S56 Escudo Digital, "Report on a January 2026 leak of senior public officials' personal data". https://www.escudodigital.com/ (article URL withheld). Verified on 21 November 2026.

S57 Escudo Digital, "Hackers prorrusos filtran los datos de cientos de policías, guardias civiles y militares españoles". https://www.escudodigital.com/ciberseguridad/hackers-prorrusos-filtran-los-datos-de-cientos-de-policias-guardias-civiles-y-militares-espanoles.html. Verified on 21 November 2026.

S58 Ministerio del Interior, "Detenidos los cuatro principales integrantes del grupo hacktivista Anonymous Fénix por ciberataques contra organismos públicos". https://www.interior.gob.es/opencms/es/detalle/articulo/Detenidos-los-cuatro-principales-integrantes-del-grupo-hacktivista-Anonymous-Fenix-por-ciberataques-contra-organismos-publicos/. Verified on 21 November 2026.

S59 Help Net Security, "Spanish police arrest suspected Anonymous members over DDoS attacks on government sites". https://www.helpnetsecurity.com/2026/02/23/spain-guardia-civil-arrests-anonymous-fenix-ddos-attacks/. Verified on 21 November 2026.

S60 INCIBE-CERT, "Arrest in Alicante in the international operation against KillSec". https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/arrest-alicante-international-operation-against-killsec. Verified on 21 November 2026.

S61 Ministerio del Interior, "La Policía Nacional detiene a un ciberdelincuente que utilizaba una técnica pionera mediante IA para obtener certificados de firma electrónica". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-detiene-a-un-ciberdelincuente-que-utilizaba-una-tecnica-pionera-mediante-IA-para-obtener-certificados-de-firma-electronica/. Verified on 21 November 2026.

S62 El Español, "Cae en Málaga una red que usaba inteligencia artificial para crear webs falsas y estafar a víctimas de toda España". https://elespanol.com/malaga/20261119/cae-malaga-red-usaba-inteligencia-artificial-crear-webs-falsas-estafar-victimas-toda-espana/1003744464404_0.html. Verified on 21 November 2026.

S63 BleepingComputer, "Spain arrests 34 suspects linked to Black Axe cyber crime". https://www.bleepingcomputer.com/news/security/spain-arrests-34-suspects-linked-to-black-axe-cyber-crime/. Verified on 21 November 2026.

S64 Escudo Digital, "La Policía desarticula una organización criminal autora del robo de diez millones de registros confidenciales". https://www.escudodigital.com/interior/la-policia-desarticula-una-organizacion-criminal-autora-del-robo-de-diez-millones-de-registros-confidenciales.html. Verified on 21 November 2026.

S65 Ministerio del Interior, "Desarticulada una red criminal que estafó 400.000 euros mediante llamadas que simulaban ser bancos". https://www.interior.gob.es/opencms/en/detail-pages/article/Desarticulada-una-red-criminal-que-estafo-400.000-euros-mediante-llamadas-que-simulaban-ser-bancos/. Verified on 21 November 2026.

S66 Ministerio del Interior, "La Policía Nacional desarticula un entramado criminal por estafar casi 3.000.000 de euros mediante el método del hijo en apuros". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-desarticula-un-entramado-criminal-por-estafar-casi-3.000.000-de-euros-mediante-el-metodo-del-hijo-en-apuros/. Verified on 21 November 2026.

S67 Ministerio del Interior, "La Policía Nacional desarticula una organización criminal que se apropió de 140 millones de euros mediante fraudes informáticos". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-desarticula-una-organizacion-criminal-que-se-apropio-de-140-millones-de-euros-mediante-fraudes-informaticos/. Verified on 21 November 2026.

S68 Ministerio del Interior, "Desarticulada la red de blanqueo de una organización de ciberdelincuencia que inyectaba el dinero de las estafas en compra de vino y maquinaria industrial". https://www.interior.gob.es/opencms/es/detalle/articulo/Desarticulada-la-red-de-blanqueo-de-una-organizacion-de-ciberdelincuencia-que-inyectaba-el-dinero-de-las-estafas-en-compra-de-vino-y-maquinaria-industrial/. Verified on 21 November 2026.

S69 INCIBE, "La Agencia Tributaria NO ha emitido ninguna comunicación dirigida a usted". https://www.incibe.es/ciudadania/avisos/la-agencia-tributaria-no-ha-emitido-ninguna-comunicacion-dirigida-usted. Verified on 21 November 2026.

S70 INCIBE, "Campaña de smishing suplantando a la Seguridad Social". https://www.incibe.es/ciudadania/avisos/campana-de-smishing-suplantando-la-seguridad-social. Verified on 21 November 2026.

S71 INCIBE, "Correos y SMS suplantan a la DGT para robar tus datos con falsas multas". https://www.incibe.es/ciudadania/avisos/correos-y-sms-suplantan-la-dgt-para-robar-tus-datos-con-falsas-multas. Verified on 21 November 2026.

S72 AEPD, "Notificaciones de brechas de datos personales, julio 2026". https://www.aepd.es/documento/informe-brechas-julio-2026.pdf. Verified on 21 November 2026.

S73 EUR-Lex, "Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 33-34". https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Verified on 21 November 2026.

S74 Boletín Oficial del Estado, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673. Verified on 21 November 2026.

S75 Boletín Oficial del Estado, "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191. Verified on 21 November 2026.

S76 Boletín Oficial del Estado, "Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257. Verified on 21 November 2026.

S77 Boletín Oficial del Estado, "Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018 (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-2021-1192. Verified on 21 November 2026.

S78 ECB Banking Supervision, "Operational resilience in the digital age". https://www.bankingsupervision.europa.eu/press/blog/2025/html/ssm.blog20250117~32b79d4efa.en.html. Verified on 21 November 2026.

S79 Boletín Oficial del Estado, "Ley 50/1997, de 27 de noviembre, del Gobierno, artículo 21 (texto consolidado)". https://www.boe.es/buscar/act.php?id=BOE-A-1997-25336. Verified on 21 November 2026.

S80 AEPD, "Notificaciones de brechas de datos personales, marzo 2026". https://www.aepd.es/documento/informe-brechas-marzo-2026.pdf. Verified on 21 November 2026.

S81 Ministerio del Interior, "La Policía Nacional detiene a un presunto colaborador de los grupos hacktivistas prorrusos CyberArmy of Russia Reborn (CARR) y Z-Pentest". https://www.interior.gob.es/opencms/es/detalle/articulo/La-Policia-Nacional-detiene-a-un-presunto-colaborador-de-los-grupos-hacktivistas-prorrusos-CyberArmy-of-Russia-Reborn-CARR-y-Z-Pentest/. Verified on 21 November 2026.

Appendix D. Glossary

- **AEPD:** Agencia Española de Protección de Datos, Spain's data-protection authority.

- **BEC:** business email compromise, fraud that impersonates a supplier or executive by email.
- **BIN:** the first digits of a card number, which identify the issuer.
- **CARR:** CyberArmy of Russia Reborn, a pro-Russian hacktivist group named in the CISA-led advisory.
- **CCN and CCN-CERT:** the National Cryptologic Centre and its CERT, which serves the Spanish public sector.
- **APDCAT and AVPD:** the Catalan and Basque data-protection authorities, which supervise public bodies in their regions.
- **CNI:** Centro Nacional de Inteligencia, Spain's national intelligence centre, to which the CCN is attached.
- **CNMV:** Comisión Nacional del Mercado de Valores, Spain's securities-market supervisor.
- **DGSFP:** Dirección General de Seguros y Fondos de Pensiones, Spain's insurance and pension-fund supervisor.
- **ECB:** the European Central Bank, which directly supervises significant banks in the euro area.
- **ESPDEF-CERT:** the Spanish armed forces' CERT for the defence sector.
- **E-money firm:** a licensed firm that issues electronic money and payment accounts but is not a bank.
- **IBEX:** the IBEX 35, the main index of the Madrid stock exchange.
- **INCIBE and INCIBE-CERT:** the National Cybersecurity Institute and its CERT, which serves citizens and private companies.
- **Neobank:** a bank or payment firm that serves customers only through apps and the web.
- **Stresser:** a paid service that floods a target with traffic, sold as load testing and used for DDoS.
- **Blackhole:** Brandefense's cybercrime data source covering posts, infected devices, credentials and card material.
- **Ransompedia:** Brandefense's ransomware database; listings record criminal claims.
- **Atlas:** Brandefense's external exposure rating; ratings run from 0 (nothing observed) to 100.
- **Infected device:** a device whose stealer log contains a login to the organisation's domain; "employee" is a classification from usage, not verified employment.
- **Credential-market listing:** a credential tied to the domain offered on a monitored market at the time of the check.
- **Combolist:** a list of login and password pairs assembled from various sources; age and validity vary.
- **Stealer log:** data captured by information-stealing malware from a device.
- **Credential stuffing:** trying passwords leaked from one service on accounts at another service.
- **Checker bot:** a bot that tests stolen cards against payment gateways and prints the result.
- **Post card:** a redacted reproduction of one dark-web post, with venue, date, alias, language and what it does and does not establish.
- **Relay:** a third-party channel or bot that reposts another actor's claim; weaker evidence than the actor's own post.
- **Cargas (loads):** money pushed into an account from hijacked accounts or stolen cards, for cash-out.
- **Drops and mule accounts:** people, and accounts opened in their names, used to receive and move fraud proceeds.
- **Smishing and vishing:** phishing by SMS and by phone call.
- **DDoS:** distributed denial of service, flooding a site with traffic so that legitimate users cannot reach it.
- **Geo-filtering:** limiting access to a service to visitors from selected countries.
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC and DS record:** signatures that let resolvers verify DNS answers, and the parent-zone record that links a domain to its keys.
- **HSTS:** a web header telling browsers to use HTTPS only.
- **MFA (multi-factor authentication):** a sign-in that needs a second factor beyond the password.
- **Phishing-resistant MFA:** sign-in tied to the real site (FIDO2 keys, passkeys or certificates), so a relay page cannot reuse it.
- **KYC:** "know your customer" identity checks at banks, exchanges and other services.
- **OT / SCADA / HMI:** operational technology, the supervisory control systems that run physical processes, and their human-machine interface screens.
- **C2:** command and control, the infrastructure an attacker uses to direct malware.
- **Webhook service:** a web service that receives HTTP requests; attackers abuse free ones for command and control.

- **ENS:** Spain's National Security Scheme for public-sector information systems and their suppliers.
- **NIS2:** the EU directive on network and information security that Spain has not yet transposed.
- **DORA:** the EU Digital Operational Resilience Act for financial entities.
- **National headline:** the single Atlas figure for the whole list of 250 organisations.
- **TLP:CLEAR:** may be shared without restriction; other legal duties still apply.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 21 November 2026. It replaces an earlier Brandefense draft on Spain prepared in October 2026, with new data and a 250-organisation assessment.

Research cutoff: 20 November 2026. The general election of 29 November 2026 falls after the cutoff. It is mentioned only as a date, as a planning context and for its effect on the legislative timetable. The report prioritises Brandefense's own data, keeps criminal claims separate from independently established incidents and does not claim a complete census of cybercrime affecting Spain. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. A Spanish-language edition, translated with AI, is being prepared; the English edition prevails where they differ.

© 2026 Brandefense. All rights reserved.