BRANDEFENSE COUNTRY REPORT · PORTUGAL 2026

Brandefense Portugal Cyber Threat Landscape Report 2026

Public-sector disruption, third-party supply-chain exposure and mobile-identity fraud across Portugal's digital services

Odin by Brandefense
Research window: 1 January to 26 November 2026 (UTC; recent 12 to 26 November)
Version 1.0 · Public Research Edition · TLP:CLEAR · 27 November 2026

83 of 247
assessed domains had a credential listed for sale when checked

20
officially confirmed and widely reported public incidents (14 dossiers)

36
Portugal-labelled ransomware listings across 17 claimant labels (vs 21 in 2025)

51
severe DORA ICT incidents reported to Banco de Portugal in 2025 (+16 YoY)

CONTENTS

Contents

01	Executive brief and defender priorities	05
	Report map	08
02	National digital profile and 2026 landscape	09
03	National exposure and selected-domain observations	16
04	Underground claims and cases	27
05	Confirmed public incidents and disclosures	40
06	Disruption, hacktivism and claim versus reality	51
07	Ransomware, extortion listings and threat profiles	55
08	Fraud, identity abuse and secondary harm	65
09	Banking, payments and digital-identity resilience	69
10	Regulation, reporting clocks and national response	72
11	Outlook and conditional planning scenarios	76
12	Action plan and completion evidence	80
A	Appendix A. Method, scope and exclusions	86
B	Appendix B. Evidence register	89
C	Appendix C. Sources	90
D	Appendix D. Glossary	96
	About this report	98

Executive and board	01 02 10 11
CISO and security operations	03 05 07 12
Fraud, banking and identity lead	04 08 09
Public-sector and OT resilience lead	05 06 12
Legal, privacy and compliance lead	05 10 A

About this edition

51/100

National Atlas headline across 247 assessed Portuguese domains (27 November 2026 snapshot)

744,809

Portugal-tagged underground posts (1 January to 26 November 2026; 97.7% in Jan-Feb)

36

Portugal-labelled ransomware listings (1 January to 26 November 2026; 21 in full-year 2025)

EUR 5.3M

Electronic-payment fraud losses in H1 2025 (down 40.4% YoY; 51 severe DORA incidents in 2025)

Contents and reading routes

Chapter	Question answered
1 Executive brief	Which findings and decisions require leadership action first?
2 National profile	How do Portugal's digital footprint, official threat tempo and bulk volume interact?
3 National exposure	Which credential, device and email-policy observations require owner validation?
4 Underground claims	What do forum listings, buyer requests and recycled archives show around Portugal?
5 Public incidents	Which confirmed 2026 events and late-November incidents affected Portuguese services?
6 Disruption and hacktivism	How do claims compare with official records and real service impact?
7 Ransomware and groups	Which extortion labels claim Portuguese targets and how do peers compare?
8 Fraud and secondary harm	How do exposed identifiers, mobile malware and spoofed calls drive Portuguese fraud?
9 Banking and payments	How are attackers targeting Portuguese retail banking, Multibanco, MB WAY and CMD?
10 Regulation and clocks	Which authorities, portals and statutory deadlines govern Portuguese incident response?
11 Planning scenarios	Which operational triggers should shift defensive posture after 26 November 2026?
12 Action plan	Who acts, on which trigger, and what completion evidence shows the control works?
Appendix A-D	Scope and exclusions, evidence register, verified sources and plain-language glossary

CHAPTER 01

Executive brief and defender priorities

01

THIS CHAPTER ANSWERS

Which 2026 signals require action from Portuguese defenders today?

5

core findings grounded in distinct evidence populations

1.1 Five findings for leadership 06

1.2 Four immediate executive decisions 07

1.3 Scope and boundaries of this report 07

CHAPTER 01

Executive brief and defender priorities

IN SHORT

Portugal's 2026 cyber threat landscape centres on municipal and public-service disruption, supplier exposure, mobile-identity abuse and wide credential leaks. Across 247 assessed domains, 83 (33.6%) had credentials listed for sale when checked. The national Atlas headline is 51/100. Ransomware listings rose to 36 (vs 21 in 2025), alongside 20 confirmed public incidents including a late-November wave across six organisations. Isolate vendor portals and OT controllers, enforce MFA on clinical and municipal logins, and close the 87-domain email-authentication gap now.

1.1 Five findings for leadership

- **Active credential listings affect one third of assessed Portuguese domains.** When checked on 27 November 2026, **83 of 247 assessed Portuguese domains (33.6%)** had a credential tied to their domain listed for sale, and the assessed portfolio's **national Atlas headline is 51/100** [S4]. Cumulative historical signals span **235 domains** with infected-device associations and **238 domains** with historical credential records, while **87 of 250 selected domains (34.8%)** still lack enforcing DMARC policies [S3][S4].
- **Local government and public bodies bore repeated confirmed disruption across 2026.** Confirmed attacks hit **Câmara Municipal da Guarda** (February), **Câmara Municipal de Serpa** (May), **Câmara Municipal de Ovar** (October) and **Câmara Municipal de Santa Maria da Feira** (November) [S34-S36][S43-S45][S60-S61][S66-S67]. National registries were also exposed at **SNS 24 / SPMS** (May, over 100,000 patient records via stolen medical credentials) and **ANEPC** (October, ~60,000 firefighter records) [S39-S42][S62-S63]. A concentrated **11 to 26 November** wave then hit **Worten**, **SMAS de Sintra**, **IMT**, **ASAE**, **Câmara Municipal do Porto** and **ADENE**, with all six confirmed or notified to customers from 12 November [S68-S78].
- **Third-party suppliers and remote OT vendors turned external flaws into local impact.** In May, the global **Instructure Canvas** breach affected Portuguese university users [S37][S38]. In October, an external web contractor's test server exposed non-classified **SIRP** public-website records [S58][S59]. In November, a pan-European refrigeration-controller attack hit seven **Intermarché Portugal** stores [S64][S65].
- **Ransomware leak-site listings rose sharply, led by The Gentlemen and Qilin.** Brandefense Ransompedia recorded **36 Portugal-labelled listings** between 1 January and 26 November 2026 (at most **35 distinct claimed entries** after one same-day duplicate), surpassing **21 across all of 2025** [S2]. Thirty listings arrived between June and November, and two aligned with publicly confirmed attacks at **Santa Casa da Misericórdia de Santo Tirso** (Qilin) and **Metro Mondego** (The Gentlemen) [S2][S46-S50].
- **Electronic-payment losses fell under Banco de Portugal controls while social engineering and mobile malware adapted.** Official **Banco de Portugal** data show H1 2025 electronic-payment fraud losses dropped **40.4%** year on year to **EUR 5.3 million**, aided by beneficiary confirmation and **SPIN** [S12][S13]. In parallel, **ANACOM** saw caller-ID and SMS spoofing complaints double by mid-July 2025, and **CERT.PT** documented surging phishing and Android banking trojans (`ToxicPanda`) [S5][S15]. February 2026 research also exposed the **Massiv** trojan targeting **Chave Móvel Digital** [S81].

1.2 Four immediate executive decisions

1. **Separate third-party development, SaaS and remote-maintenance paths from core systems.** Require written guarantees that external web agencies never copy live citizen submissions into test environments, and remove direct internet exposure from third-party refrigeration, building and utility OT controllers.
2. **Enforce phishing-resistant MFA and query-rate limits on public, clinical and remote-access portals.** Restrict bulk lookup and export functions on national registries, require phishing-resistant MFA on VPN gateways and staff email, and deploy endpoint detection capable of catching infostealers before stolen sessions reach underground markets.
3. **Close Portugal's 87-domain email-authentication gap and audit exposed web forms.** Move the **68** monitoring-only (`p=none`) and **19** missing or invalid domains to enforcing `quarantine` or `reject` DMARC policies, and harden public web-form handlers that collect tax numbers (`NIF`) and bank details (`IBAN`).
4. **Rehearse Portugal's 2026 regulatory reporting clocks before an incident hits.** Portugal's **Regime Jurídico da Cibersegurança** (Decreto-Lei n.º 125/2025, in force 3 April 2026) and **MyCiber** (Regulamento n.º 756/2026) run alongside **DORA** (Lei n.º 73/2025) and **GDPR** (Lei n.º 58/2019) [S22-S27]. Each regime carries distinct deadlines and supervisory authorities.

1.3 Scope and boundaries of this report

This report covers the activity window from **1 January to 26 November 2026 (UTC)**, with a dedicated recent-activity review covering **12 to 26 November 2026** [S1][S2]. Exposure and passive configuration observations reflect a **27 November 2026** snapshot across **250 selected Portuguese domains** [S3][S4]. External exposure covers **247 assessed domains**, while **3** unassessed domains remain unknown rather than zero [S4]. Rolling 365-day domain mentions span **27 November 2025 to 26 November 2026** [S4].

Four separate evidence populations remain distinct throughout. First are retained underground forum, Telegram, paste and Discord posts [S1]. Second are extortion leak-site listings in **Ransompedia** [S2]. Third are external exposure and passive configuration observations across 250 selected Portuguese domains [S3][S4]. Fourth are official Portuguese, EU and press sources verified on 27 November 2026 [S5-S93]. Underground claims and unconfirmed leak-site entries are never treated as confirmed breaches. Organisations are named as incident victims only where official confirmation and wide public reporting both exist, recorded in `public_names.json`.

KEY TAKEAWAYS

01

Active credential listings touch 83 of 247 assessed Portuguese domains, while 87 of 250 lack enforcing DMARC.

02

Municipal outages, national registries and third-party suppliers dominated confirmed 2026 disruption in Portugal.

03

Separate unverified forum claims and recycled historical leaks from confirmed breaches before triggering statutory notifications.

Report map

Twelve chapters, five reader paths. Follow the decision that matches your responsibility while preserving the boundary between verified records and unverified underground claims.

Executive and board	Size Portugal's 2026 exposure, ransomware rise and regulatory urgency	01 02 10 11
CISO and security operations	Prioritise credential validation, DMARC enforcement, supplier isolation and patching	03 05 07 12
Fraud, banking and identity lead	Counter spoofed SMS/calls, CMD mobile malware, KYC mules and Multibanco abuse	04 08 09
Public-sector and OT resilience lead	Separate real outages from claims and harden municipal IT and remote OT controllers	05 06 12
Legal, privacy and compliance lead	Align MyCiber (NIS2), DORA, CNPD (GDPR) and CRA incident clocks and evidence	05 10 A

CHAPTER 02

National digital profile and 2026 landscape

02

THIS CHAPTER ANSWERS

How do Portugal's digital footprint, official threat tempo and bulk volume shape 2026 risk?

89.0%

internet penetration across 10.4 million residents entering 2026

2.1 High digital adoption and shared national rails 10

2.2 Official Portuguese threat tempo from 2024 through 2026 10

2.3 Interpreting Portugal's underground publication volume 12

CHAPTER 02

National digital profile and 2026 landscape

IN SHORT

Portugal entered 2026 with 9.26 million internet users (89.0% penetration) and shared national rails around Chave Móvel Digital, SNS 24 and SIBS interbank services. Official RASI 2025 figures show CERT.PT non-automated incidents rose roughly 40% to 3,864 (61,798 total), ransomware rose 71% to 60 and vulnerability exploitation jumped 162%. Retained underground observations logged 744,809 Portugal-tagged posts through 26 November 2026, with 97.7% arriving in January and February, mostly bulk Turkish-language Telegram promotions. Separate bulk noise from March–November targeting before assigning analysts.

2.1 High digital adoption and shared national rails

DataReportal's Digital 2026: Portugal report records **9.26 million internet users** in Portugal at the end of 2025, representing **89.0%** internet penetration across an estimated **10.4 million** population in October 2025 [S20]. Active cellular mobile connections reached **13.9 million** (equivalent to **133%** of the population), and social-media user identities stood at **7.59 million** (**72.9%**) in October 2025 [S20].

Portugal's everyday economy depends on tightly shared digital rails. Citizens authenticate to public and private services through **Chave Móvel Digital (CMD)** and interact online with tax (`Portal das Finanças`), health (`SNS 24`), mobility (`IMT`) and municipal portals [S39][S74][S81]. Retail and bill payments rely heavily on **SIBS** domestic infrastructure, including **Multibanco** ATM payment references and **MB WAY** instant mobile transfers, alongside **Banco de Portugal's** beneficiary-confirmation and **SPIN** proxy-lookup services [S12][S13].

That high concentration delivers convenience and strong retail-payment security, yet it also magnifies systemic dependencies. When a shared national platform, a common municipal software stack or a single external contractor fails, disruption and secondary phishing reach tens of thousands of residents rapidly [S39][S58][S62]. Portugal's grid interconnection with Spain also underlined physical interdependence during the **28 April 2025** Iberian power outage [S16][S17]. The **ENTSO-E** technical report, validated by **ACER** and presented on 20 March 2026, attributes the outage to multiple technical factors, including insufficient voltage control, beginning in the Spanish system [S16][S17]. The cited official sources identify no cyber cause [S16][S17].

2.2 Official Portuguese threat tempo from 2024 through 2026

Official Portuguese government reporting documents a sustained multi-year rise in both incident volume and technical sophistication heading into 2026. In the 6th edition of CNCS's Riscos & Conflitos report (covering 2024), **CERT.PT** recorded **2,758 validated cybersecurity incidents** (up **36%** year on year; **11,163** including automated detections), with **78%** occurring in private organisations [S6][S7].

The official **Relatório Anual de Segurança Interna (RASI) 2025**, published by the Portuguese Government in 2026, shows a further sharp climb across every official agency [S5]. RASI's implied 2024 base (**2,761**) differs slightly from the Riscos & Conflitos figure (**2,758**) [S5][S6]:

Official Portuguese indicator (2025 vs 2024)	2025 official figure	Year-on-year trend	Source
CERT.PT total recorded incidents (incl. automated feeds)	61,798	+50,635 (driven by automated infostealer feeds)	RASI 2025 / CNCS [S5]
CERT.PT non-automated incidents (from 8,891 notifications)	3,864	+40% (+1,103 incidents; notifications +75%)	RASI 2025 / CNCS [S5]
CERT.PT ransomware incidents	60	+71% (top labels incl. Akira, MAKOP, Qilin, INC Ransom)	RASI 2025 / CNCS [S5]
CERT.PT vulnerability-exploitation incidents	118 (46 CVEs)	+162% (median CVSS Critical; SharePoint and DNN top CVEs)	RASI 2025 / CNCS [S5]
CERT.PT non-automated phishing and DDoS growth	Phishing +93% / DDoS +36%	Energy joined Banking, ISPs, Health and Public Admin lures	RASI 2025 / CNCS [S5]
DGPJ recorded computer crimes (`participações`)	2,826	+13.4% (+334; computer forgery +29.1%; unauth. access +8.4%)	RASI 2025 / DGPJ [S5]
Polícia Judiciária suspects named / arrests	2,559 / 83	Suspects +28.5% / arrests +88.6%	RASI 2025 / PJ [S5]
Ministério Público Gabinete de Cibercrime email reports	Annual total	+13.16% year on year (continuous rise since 2016)	MP [S8]
CNPD personal-data breach proceedings opened	472	+42% (vs 332 in 2024; 375 private and 115 public entities reported across the 472 proceedings; 27% human error)	CNPD [S9][S10][S11]

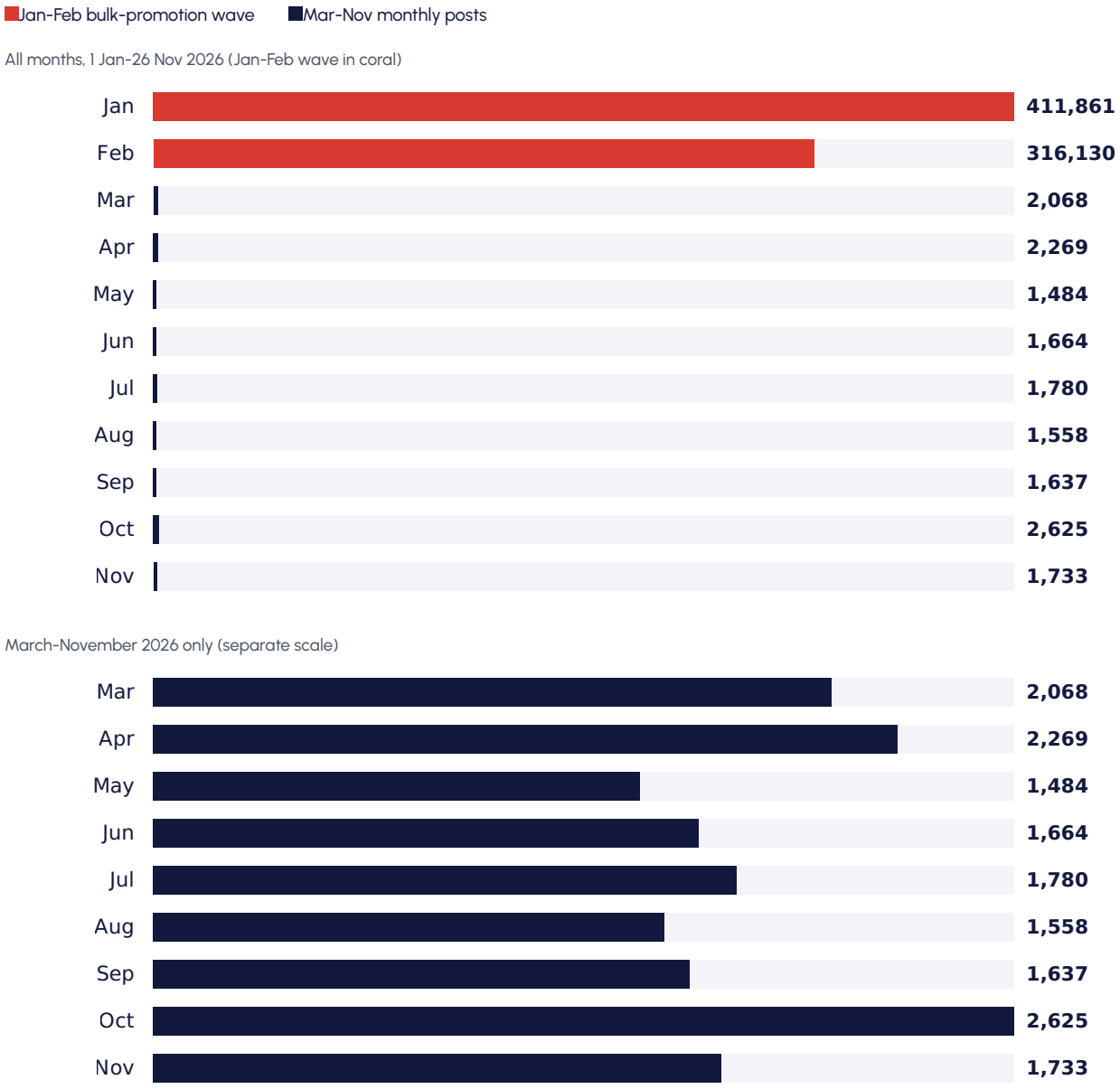
Infostealers dominated CERT.PT's automated detections in 2025, with non-privileged account theft reaching **47,953 incidents** (**78%** of 61,798 recorded cases) [S5]. **Lumma** alone accounted for **25,430 incidents** (**59%** of malware-linked cases), alongside emerging **Acreed** (**6%**) and Android threats **BadBox2.0** and **ToxicPanda** [S5]. Excluding automated feeds, third-party reports were led by social engineering (**1,054** cases), malicious code (**931**, up **224%**) and fraud (**806**, **82%** phishing) [S5]. Within social engineering, CERT.PT logged **192** CEO Fraud, **118** fake recruitment, **99** "Olá Pai / Olá Mãe" and **85** vishing incidents [S5].

During early 2026, Portuguese institutions also reinforced election-integrity monitoring ahead of the **January–February 2026 presidential election**. The **Comissão Nacional de Eleições (CNE)** launched a public disinformation reporting channel [S18]. A joint study by **ERC** and **LabCom-UBI** covered 17 November 2025 to 8 February 2026 and reviewed **8,047** official candidate posts across social platforms [S19]. The study logged **26** disinformation cases (**7** using AI-generated or AI-altered material) and estimated over **12.8 million** views; **ERC** opened **8** regulatory proceedings [S19].

2.3 Interpreting Portugal's underground publication volume

Between **1 January and 26 November 2026**, Odin by Brandefense recorded **744,809 Portugal-tagged underground posts** [S1]. Looking at that raw total without monthly and language context would seriously distort Portugal's threat picture.

Monthly Portugal-tagged underground posts from January to November 2026



Source: Odin by Brandefense, Portugal-tagged underground posts, 1 January–26 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

Month (2026)	Portugal-tagged posts	Share of window	Operational pattern
January	411,861	55.3%	Multi-country Turkish-language Telegram promo-bot surge (409,800 TR)
February	316,130	42.4%	Continuation of same multi-country Telegram promo-bot surge (314,145 TR)
March	2,068	0.3%	Return to baseline; carding, financial accounts, 25 forum posts
April	2,269	0.3%	Peak forum activity (26 posts); boilerplate retail listings and combolists
May	1,484	0.2%	Domain Admin IAB relay; stealer extracts; 7 forum posts
June	1,664	0.2%	Local-government VPN post; card-shop batch updates
July	1,780	0.2%	Summer ransomware surge; carding and KYC/document ads
August	1,558	0.2%	Rising Spanish-language (204) and Russian-language (194) Telegram traffic
September	1,637	0.2%	Repeated airline-dataset reposts; growing financial-account OTC volume
October	2,625	0.4%	Post-February peak driven by Russian-language OTC account chats (960 RU)
November (to 26 Nov)	1,733	0.2%	715 posts in 12-26 Nov recent window; 785 RU; 7 forum posts
Total (1 Jan-26 Nov)	**744,809**	**100.0%**	**727,991 (97.7%) in Jan-Feb; 16,818 (2.3%) in Mar-Nov**

Of the **727,991** January and February posts, **723,945** (**99.4%**) were in Turkish, consistent with automated marketing bots posting into multi-country groups [S1]. Exactly the same January–February surge appears in **Spain** (`424,494` Jan; `327,627` Feb), **France** (`419,017` ; `322,647`) and **Italy** (`415,967` ; `321,784`), whereas **Ireland** (`1,531` ; `1,450`) was untouched by that bot wave [S1].

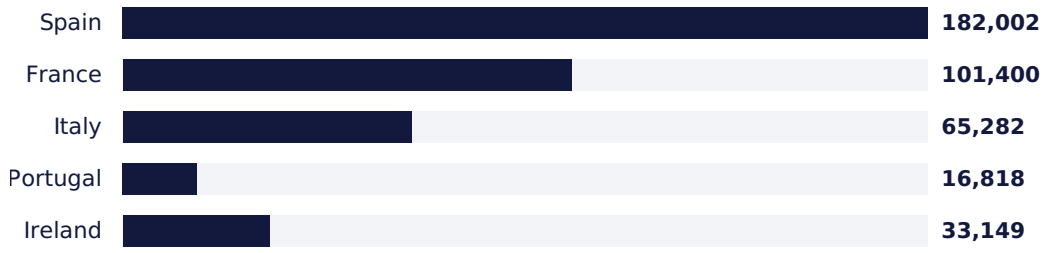
Monthly underground post volume comparing Portugal with Spain, France, Italy and Ireland

Jan-Feb 2026 Mar-Nov 2026

1 Jan-26 Nov 2026 total (Jan-Feb in coral, Mar-Nov in navy)



March-November 2026 only (separate scale)



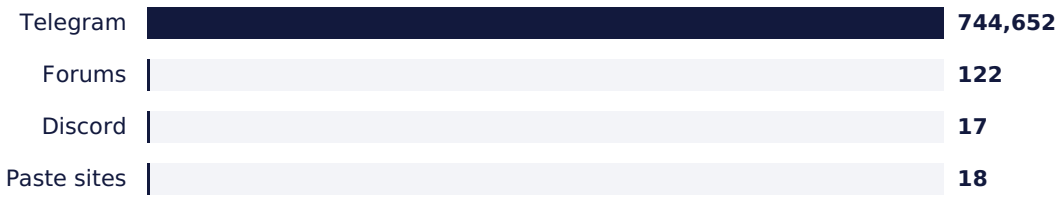
Country-tagged raw posts across monitored channels; not adjusted for population or source coverage. Source: Odin by Brandefense, Portugal-tagged underground posts, 1 January-26 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

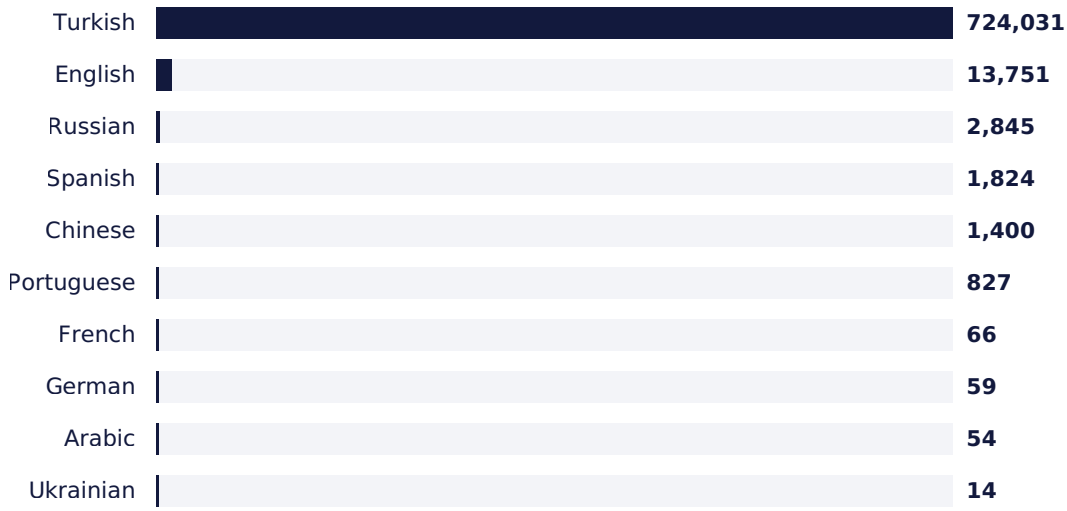
In the **March to November** baseline (`16,818` posts), Portugal's steady volume ran roughly half of **Ireland's** (`33,149`) and one quarter of **Italy's** (`65,282`) [S1]. It also stayed roughly one sixth of **France's** (`101,400`) and under one tenth of **Spain's** (`182,002`) [S1]. Across the full window, **Telegram** carried **744,652** posts (`99.98%`), **forums 122**, **paste sites 18** and **Discord 17** (`0` on Tor) [S1]. Excluding the Turkish-language bulk wave, **English** (`13,751`), **Russian** (`2,845`), **Spanish** (`1,824`), **Chinese** (`1,400`) and **Portuguese** (`827`) led Portugal-tagged communications [S1].

Platform and language distribution of Portugal-tagged underground posts

Platform



Language



Source: Odin by Brandefense, Portugal-tagged underground posts, 1 January–26 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

A distinct autumn shift merits defender attention: Russian-language Portugal-tagged traffic jumped from `90-194` posts per month in January–September to **960** in October and **785** in November through 26 November [S1]. Reviewed posts in that spike came mainly from Russian-language over-the-counter (OTC) Telegram chan-
nels brokering European and Portuguese verified financial accounts, KYC drops and card-shop stock updates [S1].

KEY TAKEAWAYS

01

High reliance on shared national rails (CMD, SNS 24, Multibanco, MB WAY) amplifies supplier and credential incidents in Portugal.

02

Official CERT.PT non-automated incidents rose 40% in 2025 while ransomware jumped 71% and vulnerability exploitation rose 162%.

03

January and February accounted for 97.7% of raw Portugal-tagged volume, mostly shared multi-country Telegram promo bots; March-November shows the real operational tempo.

CHAPTER 03

National exposure and selected-domain observations

03

THIS CHAPTER ANSWERS

Which exposure signals and configuration gaps require validation across 250 Portuguese domains?

83 of 247

assessed domains had a credential listed for sale when checked

3.1 Universe card and assessment boundary 17
3.2 National Atlas headline and current credential listings 18
3.3 Infected-device and historical credential-record associations 20
3.4 Documents, similar domain names and 365-day underground mentions 23
3.5 Mail authentication, DNSSEC, TLS and HSTS across 250 Portuguese domains 23
3.6 Turning exposure signals into separate validation queues 25

CHAPTER 03

National exposure and selected-domain observations

IN SHORT

On 27 November 2026, 83 of 247 assessed Portuguese domains (33.6%) had a credential listed for sale when checked. The national Atlas headline is 51/100. Historical signals cover 235 domains with device associations (at least 523,733 total; 38,013 employee) and 238 domains with 13,777,936 credential records. Across all 250 domains, 163 (65.2%) enforce DMARC while 87 (34.8%) do not. Triage the 83 current listings first, enforce DMARC on the 87 non-enforcing domains and fix 20 broken apex TLS endpoints.

3.1 Universe card and assessment boundary

We assembled a purposive portfolio of **250 DNS-verified Portuguese domains** organised into ten equal sector cells of 25 domains each [S3][S4]. Individual domain identities remain private to avoid exposing unverified security observations.

Item	Scope
Reference dates	Activity window runs 1 January to 26 November 2026; rolling 365-day domain mentions run 27 November 2025 to 26 November 2026; exposure and passive snapshots are dated 27 November 2026; external sources verified 27 November 2026
Portfolio	250 selected Portuguese domains across 10 equal cells of 25 domains each (130 private, 63 state-owned or central government, 57 public municipal, health and education bodies)
Selection	Purposive portfolio spanning central ministries, agencies, municipalities, universities, hospitals, supervised banks, insurers, energy, telecom, transport, manufacturing and retail leaders; not a national census
Unit	One primary domain per organisation; all 250 resolved in DNS on 27 November 2026 [S3]
Exposure snapshot	247 of 250 selected domains assessed on 27 November 2026; 3 domains remain unknown (1 in energy and utilities, 1 in industry and manufacturing, 1 in transport, maritime and logistics) [S4]
Exposure signals	Cumulative infected-device and employee-device associations, historical credential records, current credential listings, listing history, document associations and 30-day similar-name observations [S4]

Item	Scope
Mention context	Rolling 365-day dark-chat and dark-web domain mentions across all 250 domains (27 November 2025 to 26 November 2026), with the 1 January to 26 November 2026 subset reported separately [S4]
Passive snapshot	Public DNS, DMARC, SPF, DKIM, DNSSEC, CAA, TLS and HSTS observations across all 250 domains on 27 November 2026 [S3]
Publication boundary	National Atlas headline only (51/100); no per-sector ratings, per-group ratings or organisation scores are published [S4]
Inference limit	Signals can overlap across domains and individuals; missing observations are never treated as zero and no count alone establishes a confirmed breach

Exposure observations and passive configurations measure distinct risks. Historical credential records frequently reflect consumer or alumni accounts on large public-facing brands rather than internal compromise, whereas an enforcing DMARC policy reduces direct domain spoofing without stopping stolen-session reuse. Keep every metric tied to its stated denominator (**247** assessed domains for exposure; **250** selected domains for configuration and mentions).

3.2 National Atlas headline and current credential listings

When checked on 27 November 2026, **83 of 247 assessed Portuguese domains (33.6%)** had a credential tied to their domain listed for sale [S4]. All 83 also carry prior listing histories totalling **2,621 historical listing entries** across the assessed portfolio [S4].

The assessed portfolio's national Atlas headline is 51/100 [S4]. Higher values on the 0 to 100 scale indicate greater observed external exposure across the assessed domains. Only this single national headline is published. No per-sector ratings, per-group ratings or individual organisation scores appear anywhere in this report.

This national figure supports portfolio-wide prioritisation. It is not a breach rate, a probability of future intrusion or a census of Portugal's economy. The three unassessed domains remain unknown rather than zero.

Current credential listings and exposure signals across 247 assessed Portuguese domains

	Current listings	With devices	Employee devices	With credentials	With documents	Similar names (30d)
Public administration	7/25	23/25	17/25	24/25	14/25	21/25
Regional and local administration	2/25	25/25	21/25	24/25	16/25	25/25
Banking and finance	13/25	24/25	21/25	25/25	15/25	23/25
Energy and utilities	6/24	22/24	17/24	23/24	8/24	15/24
Telecom and digital services	9/25	24/25	21/25	25/25	13/25	19/25
Industry and manufacturing	2/24	21/24	21/24	24/24	14/24	13/24
Transport, maritime and logistics	8/24	23/24	20/24	23/24	12/24	15/24
Health and life sciences	5/25	24/25	16/25	20/25	8/25	16/25
Education and research	12/25	25/25	25/25	25/25	21/25	20/25
Retail, media and consumer services	19/25	24/25	23/25	25/25	16/25	24/25

Current credential listings by sector (coral). Each cell shows observed domains / assessed domains (24 or 25); signals overlap. Source: Brandefense exposure observations for 247 assessed domains out of 250 selected Portuguese domains, 27 November 2026 snapshot (3 domains remain unknown) [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector cell	Assessed (of 25)	Current listings	With devices	With employee devices	With credentials	With documents	With 30-day similar names
Public administration	25	7	23	17	24	14	21
Regional and local administration	25	2	25	21	24	16	25
Banking and finance	25	13	24	21	25	15	23
Energy and utilities	24	6	22	17	23	8	15
Telecom and digital services	25	9	24	21	25	13	19
Industry and manufacturing	24	2	21	21	24	14	13
Transport, maritime and logistics	24	8	23	20	23	12	15

Sector cell	Assessed (of 25)	Current listings	With devices	With employee devices	With credentials	With documents	With 30-day similar names
Health and life sciences	25	5	24	16	20	8	16
Education and research	25	12	25	25	25	21	20
Retail, media and consumer services	25	19	24	23	25	16	24
Total assessed	**247**	**83**	**235**	**202**	**238**	**137**	**191**

Current credential listings concentrate in consumer-facing, financial and university cells. **Retail, media and consumer services** recorded **19** listed domains, **Banking and finance 13**, **Education and research 12**, **Telecom and digital services 9** and **Transport, maritime and logistics 8** [S4]. **Public administration** (7), **Energy and utilities** (6) and **Health and life sciences** (5) also show active exposure [S4]. **Regional and local administration** (2) and **Industry and manufacturing** (2) show fewer current listings despite wide historical presence [S4].

3.3 Infected-device and historical credential-record associations

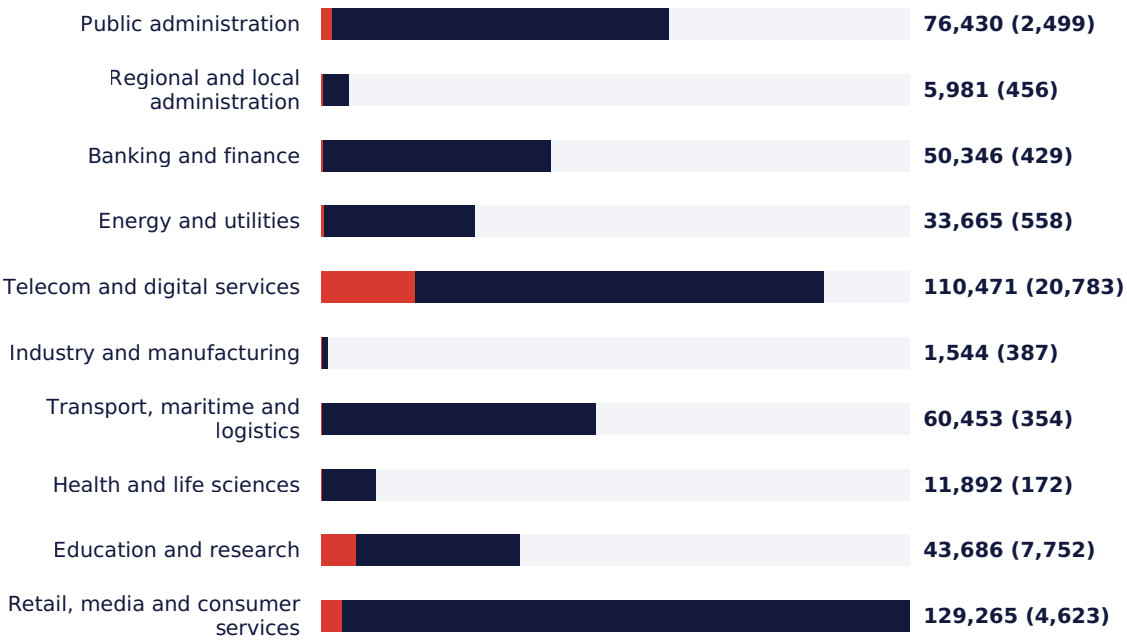
Across the **247 assessed domains**, **235 domains (95.1%)** showed cumulative infected-device associations totalling **at least 523,733** records [S4]. Device totals are minimum counts, not exact totals [S4]. Within that total, **202 domains (81.8%)** carried **38,013 employee-device associations**, while **485,720** reflected other or customer-device associations [S4].

Historical credential-record associations appeared on **238 of 247 assessed domains (96.4%)**, totalling **13,777,936 records**: **6,414,548** combolist records, **4,898,461** breach-database records and **2,464,927** stealer records [S4]. Exposure skews heavily toward mass-market webmail, telecom and consumer portals. **Telecom and digital services** accounts for **10,154,007** records (**73.7%**) and **Retail, media and consumer services** for **2,050,002** (**14.9%**) [S4]. The two largest domains alone represent **86.7%** of all observed credential records [S4].

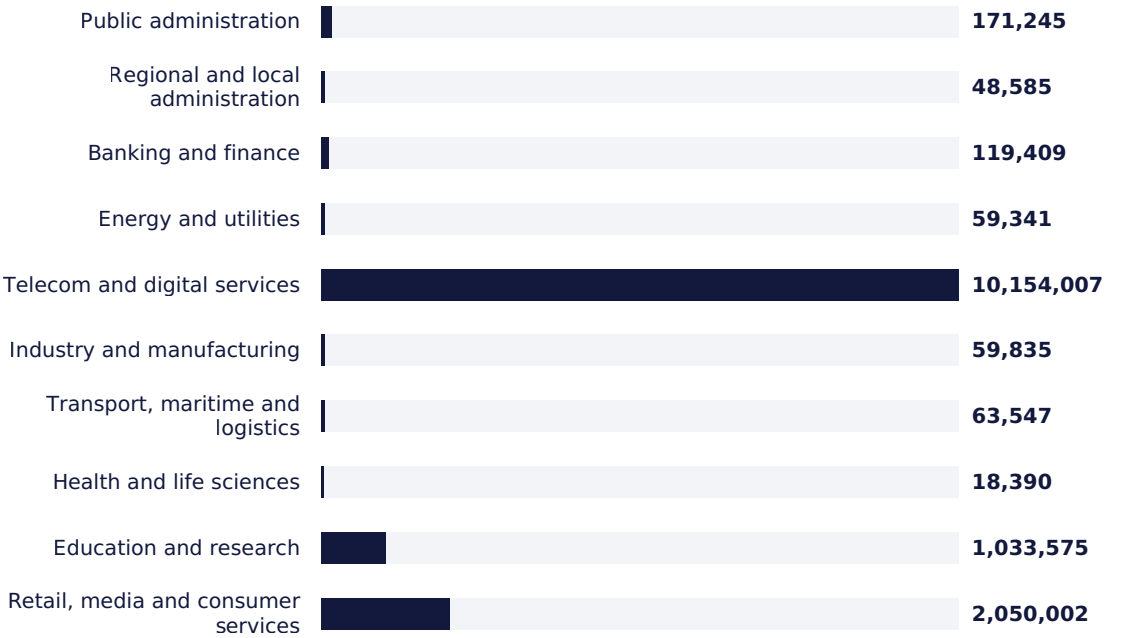
Cumulative device, credential, document and similar-name observations by sector across 247 assessed domains

Employee device associations Other device associations

Device associations, at least (employee subset in parentheses)



Credential-record associations (separate scale)



Source: Brandefense exposure observations for 247 assessed domains out of 250 selected Portuguese domains, 27 November 2026 snapshot (3 domains remain unknown) [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector cell	Assessed	Devices (at least)	Employee devices	Creden-tials total	Breach database	Stealer	Combolist	Docu-ments	Similar names (30d)
Public adminis-tration	25	76,430	2,499	171,245	28,296	61,028	81,921	93	5,032

Sector cell	Assessed	Devices (at least)	Employee devices	Credentials total	Breach database	Stealer	Combolist	Documents	Similar names (30d)
Regional and local administration	25	5,981	456	48,585	12,333	15,347	20,905	29	13,935
Banking and finance	25	50,346	429	119,409	63,836	9,294	46,279	53	2,374
Energy and utilities	24	33,665	558	59,341	24,926	9,986	24,429	34	772
Telecom and digital services	25	110,471	20,783	10,154,007	3,518,551	1,821,600	4,813,856	314	8,363
Industry and manufacturing	24	1,544	387	59,835	31,660	6,850	21,325	29	66
Transport, maritime and logistics	24	60,453	354	63,547	26,291	11,669	25,587	48	2,467
Health and life sciences	25	11,892	172	18,390	8,995	3,624	5,771	12	886
Education and research	25	43,686	7,752	1,033,575	103,535	430,052	499,988	98	4,092
Retail, media and consumer services	25	129,265	4,623	2,050,002	1,080,038	95,477	874,487	91	2,073
Total assessed	**247**	**523,733**	**38,013**	**13,777,936**	**4,898,461**	**2,464,927**	**6,414,548**	**801**	**40,060**

The employee-device column deserves special priority. Every single assessed university and research domain (**25 of 25**) showed employee-device associations (**7,752** devices) alongside **430,052** stealer records, consistent with open bring-your-own-device campus networks [S4]. Public administration recorded **2,499** employee-device associations across **17** domains and **61,028** stealer records, directly reinforcing CERT.PT's finding that infostealers drive Portugal's largest single incident class [S4][S5].

3.4 Documents, similar domain names and 365-day underground mentions

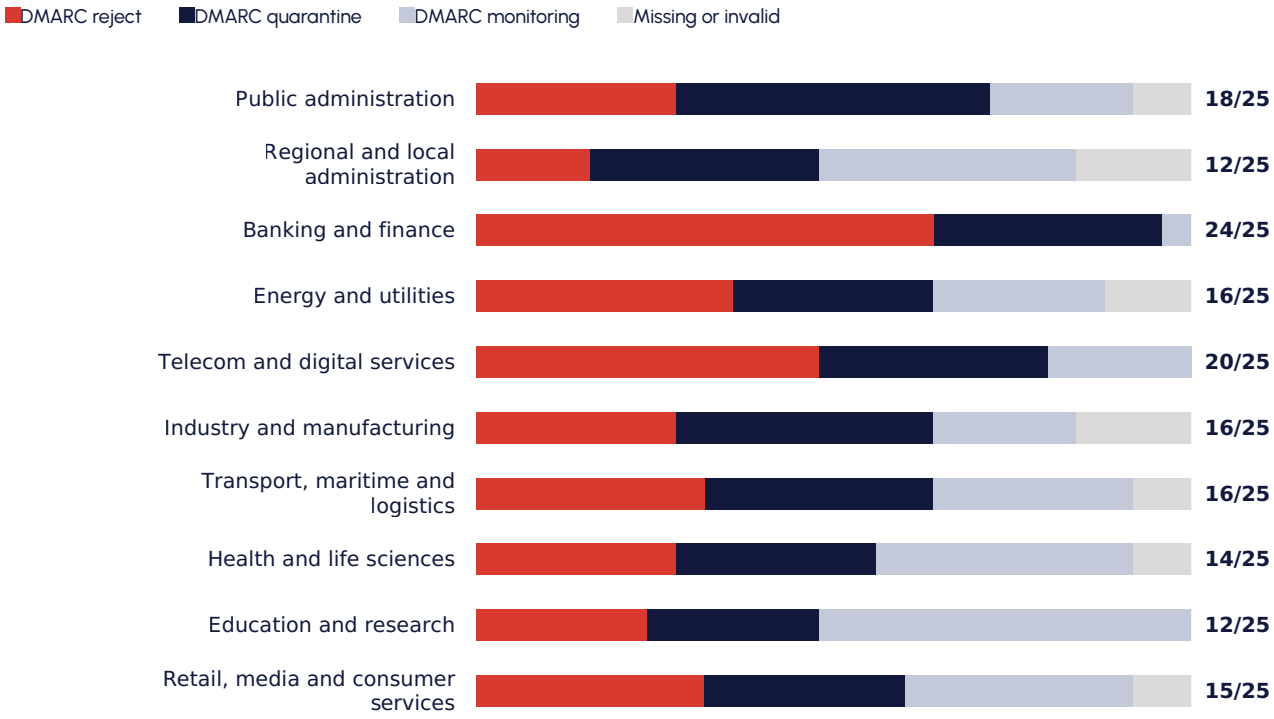
Exposed-document associations appeared on **137 of 247 assessed domains (55.5%)**, totalling **801 documents**, led by **Telecom and digital services** (`314`), **Education and research** (`98`), **Public administration** (`93`) and **Retail, media and consumer services** (`91`) [S4]. Thirty-day similar-name observations covered **191 of 247 domains (77.3%)**, totalling **40,060** similar domain names, with the highest volume around **Regional and local administration** (`13,935`), **Telecom and digital services** (`8,363`) and **Public administration** (`5,032`) [S4]. Similar names include benign parked or coincidental registrations alongside phishing lookalikes, so defenders should filter for newly resolved MX or TLS certificates before taking action.

Across all **250 domains** in the rolling 365-day window (**27 November 2025 to 26 November 2026**), **58 domains (23.2%)** appeared in underground mentions [S4]. Specifically, **39 domains** appeared in dark-chat channels (`363` mentions) and **31 domains** on dark-web sources (`244` mentions) [S4]. Restricting to the **1 January to 26 November 2026** activity window, **27 of 250 domains (10.8%)** registered **212** direct domain mentions [S4].

3.5 Mail authentication, DNSSEC, TLS and HSTS across 250 Portuguese domains

Public configuration observations on **27 November 2026** covered all **250 selected domains** [S3]. Overall, **163 of 250 domains (65.2%)** publish an enforcing DMARC policy (**84** `reject` and **79** `quarantine`), while **87 domains (34.8%)** remain non-enforcing (**68** monitoring-only `p=none` and **19** missing or invalid) [S3][S82].

Email authentication DMARC policy distribution across 250 selected Portuguese domains



Right-hand values show enforced (reject or quarantine) / 25 selected domains per sector. Source: passive configuration observations for 250 selected Portuguese domains, 27 November 2026 snapshot [S3]. Published policies do not establish message-level enforcement or prevented spoofing.

Sector cell (25 domains each)	DMARC reject	DMARC quarantine	DMARC none	Missing/ invalid	SPF	DKIM	DNSSEC	Valid TLS	HSTS (of reachable)
Public administration	7	11	5	2	25	17	14	17/23	13/20
Regional and local administration	4	8	9	4	21	19	5	23/25	18/21
Banking and finance	16	8	1	0	23	14	7	22/23	21/22
Energy and utilities	9	7	6	3	24	21	12	23/24	20/23
Telecom and digital services	12	8	5	0	25	21	8	23/23	17/20
Industry and manufacturing	7	9	5	4	24	23	5	22/24	15/22
Transport, maritime and logistics	8	8	7	2	23	21	10	23/25	17/22
Health and life sciences	7	7	9	2	24	18	4	21/22	16/24
Education and research	6	6	13	0	25	20	17	20/23	14/21
Retail, media and consumer services	8	7	8	2	25	22	2	23/25	13/17
Total (250 domains)	**84**	**79**	**68**	**19**	**239**	**196**	**84**	**217/237**	**164/212**

Sector gaps are stark and immediately actionable [S3]:

- **Banking and finance leads email and transport hardening.** Twenty-four of 25 finance domains (**96.0%**) enforce DMARC (**16** `reject`, **8** `quarantine`), and **21 of 22** reachable web endpoints (**95.5%**) publish HSTS [S3] [S82][S85].
- **Municipalities, universities and health lag sharply on DMARC enforcement.** Only **12 of 25** domains (**48.0%**) enforce DMARC in **Regional and local administration** (`9` `p=none`, `4` missing) and **12 of 25** (**48.0%**) in **Education and research** (`13` `p=none`) [S3]. **Health and life sciences** follows closely behind at **14 of 25** (**56.0%**) [S3]. Those three sectors were highlighted in RASI 2025 as facing heavy phishing and ransomware pressure in 2025 [S5].
- **Transport security and DNS signing leave avoidable gaps.** Across all 250 domains, **239 (95.6%)** publish SPF and **196 (78.4%)** had a DKIM record found, while only **84 (33.6%)** publish DNSSEC DS records and **34 (13.6%)** publish CAA records [S3][S83][S84]. Of **237** reachable apex TLS endpoints, **217** validated cleanly and **20** failed validation (**10** missing intermediate certificate chains, **8** apex hostname mismatches and **2** expired certificates; **13** apex endpoints were unreachable) [S3]. Across **212** reachable HTTP endpoints, **164 (77.4%)** set HSTS (**38** endpoints unavailable) [S3][S85].
- **Mail hosting concentrates heavily on cloud suites.** Half of the portfolio (**126 of 250**, **50.4%**) routes inbound email through Microsoft 365, **12** through Google Workspace and **13** publish no MX records [S3]. The **March 2026 Tycoon 2FA** disruption, which affected over **160 organisations in Portugal**, targeted exactly this kind of cloud-mailbox MFA session [S29].

3.6 Turning exposure signals into separate validation queues

Defenders should separate external signals into three distinct operational queues rather than blending them into one inbox:

1. **Immediate identity-compromise queue:** Validate the **83 domains** with current credential listings and the **202 domains** showing employee-device associations by checking corporate identity logs, revoking active refresh tokens and isolating infected endpoints [S4].
2. **Domain-impersonation prevention queue:** Move the **87 non-enforcing domains** to DMARC `quarantine` or `reject`, monitor newly active lookalike domains resolving MX or TLS records, and remediate the **20** apex TLS chain or certificate faults [S3][S82].
3. **Public-exposure hygiene queue:** Review the **801** document associations for accidental public uploads and audit historical breach or combolist exposure (`238` domains) to drive mandatory password resets where legacy credentials overlap with current services [S4].

KEY TAKEAWAYS

01

The national Atlas headline is 51/100 across 247 assessed Portuguese domains (27 November 2026 snapshot), with 83 domains (33.6%) showing current credential listings.

02

Banking enforces DMARC on 24 of 25 domains, while municipalities and education remain at 12 of 25 each.

03

Cloud-mailbox concentration (126 of 250 on Microsoft 365) makes phishing-resistant MFA essential across Portugal.

CHAPTER 04

Underground claims and cases

04

THIS CHAPTER ANSWERS

What are threat actors actually advertising, seeking and recycling around Portugal?

7

documented underground claim and demand cases (15 redacted posts)

4.1 How to read underground claims 28

4.2 Retail boilerplate listings and recycled historical datasets 28

4.3 Credentials, public portals and claimed initial-access offers 31

4.4 Banking leads, KYC mule demand and Portuguese payment-rail abuse 34

CHAPTER 04

Underground claims and cases

IN SHORT

Underground forums and Telegram channels targeting Portugal in 2026 show four main patterns. Sellers posted boilerplate retail ads, recycled a historical airline dataset as "2026" and shared monthly Portugal combolists alongside claimed Domain Admin and VPN access. Buyers also sought Portuguese KYC mules, domestic bank drops and spoofed bank SMS routes. All seven cases withhold unconfirmed victim identities. Validate every listing against live schemas and historical archives before treating it as a new intrusion.

4.1 How to read underground claims

An underground post establishes one fact with high confidence: an account published that text on that date in that venue [S1]. It does **not** establish server-side intrusion, fresh collection, record authenticity, active network access or a completed financial transfer. Across all seven cases below (`Case A` through `Case G`), unconfirmed victim names, domains, personal records, hashes and credential strings are withheld to prevent unverified harm.

4.2 Retail boilerplate listings and recycled historical datasets

A

CASE A

Boilerplate three-section listings naming Portuguese retail and business brands

Retail and business data

Claim unverified

CLAIM	On 4 January 2026 (`B01`), a forum seller advertised a purported 284,000-row customer, subscription and support-ticket dataset attributed to a Portuguese telecommunications operator [S1]. On 3 April 2026 (`B02`), the same forum account posted three consecutive listings within six minutes claiming more than 400,000 rows each across two Portuguese retail brands and a business-information portal [S1]. Every post used identical boilerplate phrasing claiming the data was "fresh and organized across 3 main sections" [S1].
WHAT IS NOT ESTABLISHED	No official breach confirmation existed at cut-off for any of these listings. Identical multi-brand wording posted minutes apart strongly points toward scraped, synthetic or repackaged files.

RESPONSE

Data custodians alerted to template-style listings should compare claimed table headers and sample fields against production CRM and storefront schemas before initiating breach notifications.

Bottom line

Compare advertised table schemas against live CRM and storefront exports before issuing customer alerts.

Evidence card B01 — 4 Jan 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

Offering a dataset originating from [Portuguese telecom operator]. It provides a detailed look at the organization's operations, including Customers, Service subscriptions, Support tickets. The data is fresh and organized across 3 main sections.

Note. The named operator is withheld because no official breach confirmation was identified; identical phrasing recurs on 3 April.

Held

A forum seller advertises a purported 284,000-row customer and ticket dataset attributed to a Portuguese telecommunications operator.

Not established

System intrusion, record authenticity, fresh 2026 capture, affected customer count or completed sale.

Evidence card B02 — 3 Apr 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

Offering a dataset originating from [Portuguese retail brand]. It provides a detailed look at the organization's operations, including Contacts, Orders, Delivery Logs. The data is fresh and organized across 3 main sections.

Note. Boilerplate wording repeated across unrelated Portuguese brands is a strong indicator of repackaged or synthetic listings.

Held

Within six minutes on 3 April, the same forum account posts three identical three-section listings claiming more than 400k rows each across two retailers and a business directory in Portugal.

Not established

Source-system access, data authenticity or fresh extraction.

CASE B

B Repeated 2026 recycling of a historical airline dataset

Aviation and consumer data

Recycled dataset

CLAIM

Across 6 April, 12 September, 13 September (`B03`), 22 September and **23 November 2026** (`B13`, recent window), multiple forum accounts re-offered a customer dataset attributed to an airline serving Portugal [S1]. One September listing appended `2026` to the title. Yet sample rows in both September and 23 November still display historical loyalty-programme identifier fields with 2017–2018 dates from an older, previously disclosed leak [S1].

WHAT IS NOT ESTABLISHED

None of the 2026 forum reposts establish a new 2026 compromise of the airline or newly captured passenger data.

RESPONSE

Incident-response teams monitoring dark-web alerts must hash and date-check sample rows against prior breach archives so recycled historical leaks do not trigger false crisis escalations.

Bottom line

Check sample registration dates against historical leaks before treating a 2026 forum listing as a new breach.

Evidence card B03 — 13 Sep 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

[Airline serving Portugal] Customer Database with Date of Birth 2026 [...] FULL_NAME BIRTH_DATE SALUTATION COMMUNICATION_LANGUAGE NATIONALITY GENDER ADDRESS_CITY [redacted sample rows]

Note. Matching threads on 6 April, 12 September, 22 September and 23 November (B13) carry identical loyalty-ID fields and 2017-2018 registration dates from an older, previously disclosed leak.

Held

A forum broker advertises passenger contact records attributed to an airline serving Portugal using a 2026 title.

Not established

A 2026 airline compromise, fresh data extraction or verified current accuracy.

Evidence card B13 — 23 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

[Airline serving Portugal] Data [...] [loyalty_id] birth_date salutation communication_language first_name last_name full_name nationality gender address_city [redacted; registration_date 17/08/2018]

Note. Paired with B03, confirms that late-November forum activity mixes recycled historical archives alongside newer listings.

Held

Inside the recent window, another forum seller re-offers the same airline passenger table seen in April and September, still carrying 2018 registration timestamps.

Not established

A November 2026 airline compromise or newly captured passenger data.

4.3 Credentials, public portals and claimed initial-access offers

CASE C

C

Monthly Portugal credential combolists and unconfirmed public-portal leaks

Credentials and public portals

Claim unverified

CLAIM

From January through November 2026, automated forum accounts posted repeated Portugal `Email:Pass` combolists advertising 14,150 to 356,000 lines per drop [S1]. Examples include a 101,000-line April file (`B04`, reposted in August) and a 71,000-line file dated **23 November 2026** (`B14`, recent window) [S1]. Separately, May Telegram relays listed stealer-log extracts matching Portuguese public-service login URLs [S1]. On **14 November 2026** (`B11`, recent window), a forum user also shared a claimed CSV of school-coordinator accounts from a public education portal [S1].

WHAT IS NOT ESTABLISHED

Combolist labels such as `FRESH` and `HQ` do not verify working passwords or fresh 2026 theft, and no official confirmation was located by cut-off for the 14 November public-portal claim.

RESPONSE

Public agencies and consumer portals should assume stealer-harvested logins circulate continuously, enforce MFA across webmail and administrative accounts and monitor login telemetry for credential stuffing.

Bottom line

Enforce MFA on public-portal and webmail accounts and hunt for stealer-log infections on staff devices.

Evidence card B04 — 30 Apr 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

Database: Portugal Type: Email : Password Date: [29/ APR/2026] Combo: [101 K++] Line Status: FRESH | HQ

Note. Labels such as FRESH and HQ are routine marketing terms on recycled credential compilations; the same 29 April file reappeared on another forum in August.

Held
A forum thread promotes a Portugal-labelled email-and-password list claiming more than 101,000 lines, mirroring similar monthly posts from January through November.

Not established
Working passwords, unique residents, fresh collection date or a single Portuguese source breach.

Evidence card B11 — 14 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

DATABASE [Portuguese public education-programme portal] [...] sample: id,school-Id,obs,temp,email,phone,name,password,subject,coordinator [redacted sample rows]

Note. Portal domain, programme name, personal details and password hashes are withheld because no official confirmation was located by cut-off.

Held
Inside the recent window, a forum poster shares a claimed CSV export of educator and school-coordinator accounts attributed to a Portuguese public education-programme portal.

Not established
Official breach confirmation, current password validity, full row count or confirmed unauthorised portal access.

Evidence card B14 — 23 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

[71 K++] { Portugal } Email:Pass FRESH [23-11-2026] Database : Portugal Type : Email , Password Condition: Fresh,HQ Combo: 71 K++ Line

Note. Follows the exact same automated formatting used across earlier 2026 Portugal combolist drops.

Held
Inside the recent window, a forum account posts a 71,000-line Portugal-labelled email-and-password compilation dated 23 November 2026.

Not established
Unique valid accounts, fresh credential theft in November or compromise of any specific Portuguese organisation.

CASE D

D

Claimed corporate Domain Admin, e-commerce admin and local-government VPN access

Claim unverified

Corporate and municipal access

CLAIM	Four underground posts in 2026 advertised or leaked claimed direct system access inside Portugal [S1]. On 28 February, a forum seller offered claimed admin-panel access to a Portuguese e-commerce merchant claiming over EUR 2 million in annual revenue and payment-redirection capability [S1]. On 1 May (B05), a leak-monitor channel relayed a forum offer selling claimed **Active Directory Domain Admin** access to a Portuguese technology/SaaS company ($100M-$500M stated revenue) [S1]. On 2 June (B06), a Telegram channel posted claimed plaintext GlobalProtect VPN credentials for a Portuguese local-government body [S1]. On 9 July, a Telegram market listed claimed web-administration access to a public-sector .gov.pt subdomain [S1].
WHAT IS NOT ESTABLISHED	None of the four posts carry independent victim confirmation, verified active login validity or confirmed follow-on ransomware deployment.
RESPONSE	Security teams should enforce phishing-resistant MFA on all VPN gateways and administrative consoles, audit privileged Active Directory accounts and rotate credentials immediately if exposed on remote-access portals.

Bottom line

Require phishing-resistant MFA on all VPN gateways, admin panels and Active Directory privileged tiers.

Evidence card B05 — 1 May 2026

Channel monitor (alias withheld) | Telegram channel relay | Telegram | English

ORIGINAL

Selling: [Active Directory (Domain Admin)] Technology / SaaS - Portugal ($100M - $500M revenue) [forum reference redacted]

Note. Initial-access offers in Portugal appear infrequently in public listings but represent high-impact precursors when valid.

Held

An underground leak-monitor channel relays a forum initial-access listing offering claimed Active Directory Domain Admin access to a mid-to-large technology company in Portugal.

Not established

Live domain access, confirmed victim identity, stated revenue accuracy, ransomware follow-on or completed sale.

Evidence card B06 — 2 Jun 2026

Channel poster (alias withheld) | Telegram channel | Telegram | English

ORIGINAL

Here are some brief steps to configure access to [Portuguese local-government body]. 1. Access the website [VPN URL redacted]/global-protect/login.esp [credentials redacted]

Note. All organisational identifiers, URLs and credential strings are removed; the post illustrates the exposure of single-factor remote-access portals.

Held

A Telegram channel posts claimed plaintext remote-access VPN login instructions pointing to a Portuguese local-government GlobalProtect gateway.

Not established

Active credential validity, absence of MFA, unauthorised network entry or confirmed municipal data access.

4.4 Banking leads, KYC mule demand and Portuguese payment-rail abuse

CASE E

E

Recent-window banking and nationwide Portuguese consumer lead listings

Claim unverified

Banking and consumer leads

CLAIM

Inside the **12 to 26 November 2026** recent window, a single forum account posted two large Portuguese lead listings two days apart [S1]. On **21 November** (B12), the seller advertised 55,000 purported customer leads containing names, phone numbers, emails, Portuguese tax numbers (NIF) and postal addresses attributed to a major Portuguese retail bank [S1]. On **23 November** (B15), the same account advertised 500,000 purportedly updated Portuguese consumer leads as a one-time sale without sample rows [S1]. Separately in April and May, another forum user posted claimed datasets attributed to two further Portuguese organisations [S1].

WHAT IS NOT ESTABLISHED

No official breach confirmation existed at cut-off for the bank-labelled lead file, the 500,000-row consumer list or the two April-May claims. Lead files

containing `NIF` and address fields are routinely compiled from marketing brokers or historical leaks.

RESPONSE

Banks and telecom operators should monitor for NIF-referenced vishing and smishing lures even when no internal system breach occurred, because accurate personal identifiers increase social-engineering conversion.

Bottom line

Monitor for targeted NIF-referenced phishing and smishing campaigns even when a bank-labelled lead list is unverified.

Evidence card B12 — 21 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

[SELLING] 55k LEADS [Portuguese retail bank] [...] format: NAME,TELE-PHONE,EMAIL,NIF,ADDRESS,CITY,COUNTRY,ZIPCODE [redacted sample rows]

Note. Bank identity and all personal fields are removed; lead lists with NIFs are commonly compiled from third-party brokers or older leaks.

Held

Inside the recent window, a forum seller advertises 55,000 purported customer lead records containing Portuguese NIF tax numbers and addresses attributed to a Portuguese retail bank.

Not established

Bank system breach, authentic customer provenance, freshness of records or completed transfer.

Evidence card B15 — 23 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

[SELLING] 500k LEADS PORTUGAL (PT) I am selling 500k leads from Portugal {PT}, these are updated leads, one-time sale. Those interested should send a PM.

Note. Illustrates commercial aggregation of Portuguese consumer contact data feeding phone, SMS and investment-fraud operations.

Held

Two days after B12, the same forum account advertises a 500,000-row Portuguese consumer lead package described as a one-time sale without sample rows.

Not established

Origin of records, data accuracy, consent status, breach provenance or completed purchase.

CASE F

F ■ Portuguese KYC mule recruitment, domestic bank drops and spoofed bank SMS routes

Demand unverified

Identity, telecom and drops

IDENTITY AND DROP DEMAND

Forum buyers recruited Portuguese residents for live KYC checks in January and April (paying USD 30 per check) and sought Portugal-verified Wise and Revolut Pro accounts in March [S1]. On 30 June (`B08`), a Russian-language buyer requested a Portuguese bank drop for inbound domestic transfers of **EUR 2,000 to EUR 10,000** [S1].

TELECOM AND SMS SPOOFING SUPPLY

A virtual-SIM bot added disposable Portuguese `+351` numbers on 31 March (`B07`) [S1]. On **17 November 2026** (`B10` , recent window), a Portuguese-lan-

guage Telegram post advertised bulk-SMS routes with spoofed Sender IDs targeting customers of a major retail bank [S1].

WHAT IS NOT ESTABLISHED	Recruitment and route advertisements do not verify how many Portuguese accounts were opened, how many messages reached handsets or which specific fraud losses resulted.
RESPONSE	Financial institutions should tighten liveness checks during remote onboarding, flag newly created domestic accounts receiving rapid inbound transfers and coordinate with carriers and **ANACOM** against spoofed alphanumeric SMS headers.

Bottom line

Tighten onboarding liveness checks, flag new-account mule inflows and monitor spoofed SMS sender traffic.

Evidence card B07 — 31 Mar 2026

Forum poster (alias withheld) | Forum thread | Forum | Russian / English

ORIGINAL

Hello, dear forum members! Portugal has been added to the bot for disposable numbers. SMS numbers in the bot [handle redacted]

Note. Disposable +351 SMS and SIM-rental services lower the cost of passing local phone verification checks in account-creation abuse.

Held

An automated virtual-SIM verification operator announces the addition of Portuguese (+351) disposable SMS numbers to its Telegram bot.

Not established

Volume of Portuguese numbers held, carrier origin or confirmed linkage to a specific fraud case.

Evidence card B08 — 30 Jun 2026

Forum poster (alias withheld) | Forum thread | Forum | Russian

ORIGINAL

[Translated] One-off drop needed in PT (Portugal) for domestic inbound transfers 2-10k; established services and reputable actors only, contacts in PM.

Note. Matches repeated Portuguese KYC recruitment posts in January, March and April and aligns with PJ RASI 2025 reporting on money-mule dissipation.

Held

A Russian-language forum buyer seeks a Portuguese domestic bank-account drop to receive transfers between EUR 2,000 and EUR 10,000.

Not established

Completed recruitment, a named receiving bank or verified financial loss.

Evidence card B10 — 17 Nov 2026

Channel poster (alias withheld) | Telegram channel | Telegram | Portuguese

ORIGINAL

[Portuguese retail bank] em Portugal [...] temos rotas para dar suporte perfeito [...] Rotas novas, Sender ID estável [handles redacted]

Note. Bank name withheld. The post is consistent with ANACOM and Banco de Portugal warnings regarding spoofed-header bank smishing.

Held

Inside the recent window, a Portuguese-language Telegram post advertises new bulk-SMS routes with stable spoofed Sender IDs targeting customers of a major Portuguese retail bank.

Not established

Delivery success on Portuguese mobile networks, live campaign volume or compromise of the named bank.

CASE G

G Domestic Multibanco reference tooling, high-risk MB WAY rails and mobile banking malware

Mixed evidence

Payments and mobile banking

CLAIM

Underground discussions in 2026 paired domestic payment-rail abuse with mobile-malware tooling relevant to Portugal [S1]. On 5 April (B09), a forum thread promoted a Multibanco reference generator for its "No Refunds - Realtime transactions" property in Portugal [S1]. A September Russian-language processor listing also advertised **Multibanco** and **MB WAY** settlement for high-risk merchants [S1]. On 21 February, forums recirculated technical details of the **Massiv** Android trojan targeting Portugal's **Chave Móvel Digital** ecosystem [S1][S81]. Separately, June–August and 8 November posts promoted Android NFC-relay and banking-trojan kits (VIPER NFC , RedHook , WindRelay) across Iberian markets [S1].

WHAT IS NOT ESTABLISHED

Tool promotions and malware discussions do not prove compromise of SIBS or Multibanco infrastructure, nor do they quantify live Portuguese infection volumes beyond confirmed research cases [S81].

RESPONSE

Retail banks and digital-identity custodians should combine Android Accessibility and overlay telemetry with customer warnings against sideloaded IPTV apps and unsolicited Multibanco reference payments.

Bottom line

Detect Android Accessibility abuse and alert customers against sideloaded IPTV apps and fraudulent Multibanco references.

Evidence card B09 — 5 Apr 2026

Forum poster (alias withheld) · Forum thread · Forum · English

ORIGINAL

Multibanco Reference Generator - Online Version [...] For Sellers: Method number 1 in Portugal - No Refunds - Realtime transactions - Automatic Process. For Clients: ATM Payment (Multibanco).

Note. Demonstrates how fraud actors exploit domestic payment-rail familiarity and irreversibility rather than technical flaws in the interbank network.

Held

A forum user bumps a thread advertising an online Multibanco payment-reference generator promoted for irreversible real-time settlement in Portugal.

Not established

Active tool uptime, transaction volume or compromise of SIBS or Multibanco core infrastructure.

KEY TAKEAWAYS

01

Underground posts establish active criminal demand around Portugal, not verified breaches.

02

Sample date checks exposed older airline records still being resold as "2026" on 23 November alongside boilerplate retail claims.

03

Active demand for Portuguese KYC mules, +351 disposable SIMs and spoofed bank SMS routes feeds directly into domestic fraud operations.

CHAPTER 05

Confirmed public incidents and disclosures

THIS CHAPTER ANSWERS

Which 2026 cyber incidents were publicly confirmed in Portugal, and what disrupted real services?

20

officially confirmed and widely reported public incidents (14 dossiers)

5.1 Naming discipline and incident scope 41

5.2 Confirmed incidents from January to early November 2026 41

5.3 Recent activity: 12 to 26 November 2026 49

CHAPTER 05

Confirmed public incidents and disclosures

IN SHORT

Between January and 26 November 2026, Portuguese public authorities, critical utilities, municipalities, healthcare bodies, universities and retailers publicly confirmed 20 major cyber incidents summarised in fourteen dossiers below. Ransomware, municipal network encryption, unauthorised registry scraping, third-party contractor test servers, volumetric DDoS and pan-European refrigeration OT attacks all struck Portuguese services. Six confirmed public incidents had disclosures or customer notices in the 12 to 26 November recent window alone. Isolate administrative IT from clinical and operational networks, restrict bulk citizen-registry exports and harden public web forms immediately.

5.1 Naming discipline and incident scope

An affected Portuguese organisation is named in this chapter only when **both** conditions hold: the organisation or a competent authority officially confirmed the incident **and** national or regional media widely reported it (`public_names.json`). Claims lacking official confirmation, single-outlet reports without institutional confirmation and historical 2023 municipal cases are excluded from confirmed counts and explained in Appendix A.7.

5.2 Confirmed incidents from January to early November 2026

CASE H

H

Câmara Municipal da Guarda prolonged digital-service paralysis

Municipal administration

Confirmed attack

CHRONOLOGY AND IMPACT	On **12 February 2026**, **Câmara Municipal da Guarda** detected a complex cyberattack that disrupted external communications and forced the preventive shutdown of municipal platforms and its public website for several weeks [S34][S35]. On 4 March, the municipality issued a formal order suspending administrative deadlines retroactively to 12 February while technical teams rebuilt services [S36].
OFFICIAL NOTIFICATION	Municipal authorities confirmed reporting the intrusion to the **Polícia Judiciária** and coordinating containment with national responders [S35].
RESPONSE	Municipalities should maintain tested offline immutable backups and pre-drafted legal orders for suspending statutory deadlines when digital portals are taken offline.

Bottom line

Maintain offline immutable backups and pre-approved legal procedures for suspending statutory municipal deadlines.

CASE I

Global Instructure Canvas breach affecting Portuguese higher education

Higher education (supplier)

Confirmed breach

CHRONOLOGY AND IMPACT

In early **May 2026**, global learning-management vendor **Instructure** confirmed a security incident affecting its **Canvas** platform that reached students and staff across multiple Portuguese higher-education institutions [S37] [S38]. Exposed records included names, institutional email addresses, student identifiers and platform messages, while passwords, financial details and internal university networks remained unaffected [S37][S38].

OFFICIAL NOTIFICATION

Affected Portuguese institutions notified the **Comissão Nacional de Proteção de Dados (CNPD)** and warned academic communities about targeted phishing using genuine course details [S37]. Individual institutions are not listed beyond Instructure and Canvas where official statements varied in scope.

RESPONSE

Universities should inventory every third-party SaaS learning tool holding student directories and issue prompt course-context phishing warnings whenever a cloud vendor reports a breach.

Bottom line

Inventory third-party learning platforms holding student data and prepare targeted phishing warnings after vendor breaches.

CASE J

SNS 24 / SPMS unauthorised patient-record extraction

National health services

Confirmed breach

CHRONOLOGY AND SCOPE

On **21 May 2026**, **SPMS** (Serviços Partilhados do Ministério da Saúde) notified the **CNCS** after detecting unauthorised automated queries through the **SNS 24** portal [S39][S40]. Investigators established that stolen credentials belonging to a physician were used across several days to query administrative records for **more than 100,000 citizens nationwide** (without clinical files) [S39][S41].

OFFICIAL INVESTIGATION	The director of the **Polícia Judiciária** cybercrime unit (**UNC3T**) noted that the automated extraction speed raised the possibility of AI-assisted scripting [S39]. SPMS deactivated the misused credentials to halt extraction while **CNCS / CERT.PT** and **PJ** ran joint forensics, and regulator **ERS** issued a statement [S40][S42]. No individual physician or local health unit is identified here.
RESPONSE	National health registries must enforce phishing-resistant MFA on clinician portals, cap per-account lookup velocity and trigger automated session revocation on abnormal nationwide record queries.

Bottom line

Apply rate limits, anomalous-query alerts and phishing-resistant MFA on clinician portals accessing national patient registries.

CASE K

K ■ Câmara Municipal de Serpa file-encryption attack

Municipal administration

Confirmed attack

CHRONOLOGY AND IMPACT	Between 04:00 and 08:30 on **27 May 2026**, a file-encryption cyberattack disabled **Câmara Municipal de Serpa** IT systems alongside fixed and mobile municipal telephone lines [S43][S44]. Technical teams shut down servers and rebuilt infrastructure from daily backups, isolating permanent operational data loss to the window between 18:00 on 26 May and 08:00 on 27 May [S43].
OFFICIAL NOTIFICATION	The municipality warned residents that some documents might have been copied before encryption and formally notified **CNCS**, **Ministério Público**, **CNPD** and **Polícia Judiciária** [S43][S45].
RESPONSE	Local authorities should test full bare-metal restoration from offline daily backups and segment municipal accounting and citizen-service servers from general office workstations.

Bottom line

Test full bare-metal restoration from daily offline backups and segment municipal finance systems from general workstations.

CASE L

L ■ Santa Casa da Misericórdia de Santo Tirso Qilin ransomware

Healthcare and social care

Confirmed attack

CHRONOLOGY AND IMPACT	On **8 June 2026**, **Santa Casa da Misericórdia de Santo Tirso** suffered a ransomware intrusion that disrupted outpatient medical appointments and diagnostic systems, while residential elderly-care operations continued normally [S46][S47]. An external response team was engaged to contain and rebuild systems [S46].
OFFICIAL NOTIFICATION AND EXTORTION LISTING	The institution reported the incident to **Polícia Judiciária**, **CNCS** and **CNPD** [S47]. On **16 June 2026**, the ransomware label **Qilin** listed the organisation in Ransompedia and published purported stolen files [S2][S47].
RESPONSE	Healthcare and social-care institutions should isolate clinical care networks from administrative servers and validate any ransomware leak-site publication against internal forensic logs before scoping personal-data notices.

Bottom line

Isolate clinical care systems from administrative networks and verify ransomware leak-site claims against forensic logs.

CASE M

M ■ Metro Mondego ransomware and transit-pass holder alert

Public transport

Confirmed attack

CHRONOLOGY AND IMPACT	On **6 July 2026**, **Metro Mondego** experienced a ransomware attack affecting part of its internal administrative systems [S48][S49]. The operator confirmed that metrobus passenger transport operations remained unaffected and that payment-card terminals were strictly isolated from corporate IT [S49].
DATA EXPOSURE AND EXTORTION LISTING	On **16 July**, the ransomware label **The Gentlemen** posted a matching claim in Ransompedia [S2]. On **26 July**, Metro Mondego warned personalised transit-pass holders and email correspondents that personal data (name, birth date, address, phone, photo, **NIF**, ID number and usage) was likely copied [S48]. The operator confirmed notifications to **CNCS**, **CNPD** and **Polícia Judiciária** [S50].

RESPONSE	Public transport operators should maintain strict segmentation between ticketing-payment terminals, vehicle operations and office networks, and prepare rapid direct alerts for transit-pass holders when administrative databases are copied.

Bottom line

Keep payment-card terminals and transit-control operations isolated from corporate IT and notify pass holders rapidly.

CASE N

N Universidade de Aveiro ransomware with email and database exfiltration

Higher education

Confirmed attack

CHRONOLOGY AND IMPACT	**CNCS / CERT.PT** confirmed receiving notification on **20 July 2026** of a ransomware attack against **Universidade de Aveiro**, which disclosed the breach publicly on 29 July [S51]. The university confirmed data exfiltration from email accounts and at least one database, enforced a campus-wide password reset and restored core services from backups [S51][S52].
OFFICIAL COORDINATION AND LATER CLARIFICATION	Universidade de Aveiro worked with **CNCS**, **CNPD**, **Polícia Judiciária** and **SIS** [S52]. In September 2026, the university separately clarified that brief campus network faults stemmed from a routine August system update and bore no connection to the July ransomware intrusion [S52].
RESPONSE	Academic institutions should segment institutional mail and research databases, maintain tested campus-wide credential-rotation playbooks and communicate clearly when later routine faults are unrelated to a prior intrusion.

Bottom line

Segment university mail and research databases, enforce campus-wide credential rotation playbooks and test backup integrity.

CASE O

O Grupo Águas de Portugal administrative IT cyberattack

Water utilities

Confirmed attack

CHRONOLOGY AND IMPACT	On **31 July 2026** (confirmed publicly on 4 August), **Grupo Águas de Portugal (AdP)** suffered a high-complexity cyberattack targeting administrative IT systems across 13 continental operational companies [S53].

OPERATIONAL BOUNDARY AND NOTIFICATIONS	Both AdP and Portugal's Environment Minister confirmed on 4 and 7 August that water supply, treatment and water quality were completely unaffected and that investigators had found no evidence of personal-data exfiltration [S53][S54]. AdP notified **Polícia Judiciária**, **CNCS** and **CNPD** [S53].
RESPONSE	Critical utilities must maintain strict, auditable network isolation between corporate IT and operational technology so an administrative compromise cannot propagate into water treatment or distribution controls.

Bottom line

Preserve strict IT/OT network separation so an administrative intrusion cannot cross into water treatment or distribution controls.

P

CASE P

MEO volumetric DDoS waves and Web Summit 2026 traffic load

Telecommunications

Confirmed DDoS

CHRONOLOGY AND IMPACT	Across **14 and 15 September 2026**, **MEO** mitigated three volumetric distributed denial-of-service (**DDoS**) waves (00:45–02:55, 17:30–19:30 and 22:45–01:05) targeting international network links [S55][S56]. Secondary BGP instability triggered more than 7,200 user outage reports on Downdetector before traffic stabilised [S55]. MEO confirmed zero internal system intrusion and zero customer-data access [S55][S56].
HIGH-PROFILE EVENT BASELINE	Separately, during the first two days of **Web Summit 2026** in Lisbon (**9 to 10 November**), MEO reported intercepting **6,020,686** attack attempts across event infrastructure without major disruption [S57].
RESPONSE	Telecom carriers and major event hosts should rehearse upstream volumetric scrubbing, BGP route-dampening safeguards and transparent outage bulletins ahead of peak national gatherings.

Bottom line

Test upstream DDoS scrubbing, BGP route resilience and customer outage communications before peak national events.

CASE Q

Q SIRP external web-contractor test-server breach

Public-sector supply chain

Official notice

CHRONOLOGY AND OFFICIAL CLARIFICATION	On **7 October 2026**, an underground forum listing advertised a purported 120 GB archive (claiming 312,144 files, 96 databases and 180 website sources) linked to Portuguese intelligence portals [S58][S59]. On **8 October**, **Sistema de Informações da República Portuguesa (SIRP)** confirmed the files came from an external web contractor's development and testing server [S58][S59]. That server hosted public institutional websites (`SIRP`, `SIS`, `SIED`) alongside websites for dozens of other contractor clients [S58].
SCOPE BOUNDARY	SIRP confirmed that **no classified, operational or internal systems or data** of SIRP, SIS or SIED were affected, noting that only limited non-confidential recruitment-portal items appeared in the exposed test copy [S58]. SIRP formally reported the incident to the **Procuradoria-Geral da República (PGR)** [S59]. The external contractor is not named beyond SIRP's official scope.
RESPONSE	Public agencies must contractually prohibit live citizen submissions on vendor development or test servers and verify periodic data deletion during contractor audits.

Bottom line

Prohibit live citizen submissions on external contractor test servers and enforce contractual data-destruction audits.

CASE R

R ANEPC National Firefighters Registry breach and Aveiro-district municipal outages

Emergency services and municipalities

Confirmed cases

ANEPC RNBP BREACH (24 OCTOBER)	On **24 October 2026**, the **Autoridade Nacional de Emergência e Proteção Civil (ANEPC)** confirmed a cyberattack that copied personal records from the **Registo Nacional de Bombeiros Portugueses (RNBP)** covering approximately **60,000 firefighters** [S62][S63]. Exposed fields included name, Citizen Card (`CC`), `NIF`, `NISS`, `SNS` number, driving licence, address, photograph and blood group, while banking details were unaffected [S62][S63]. ANEPC immediately suspended the registry with **CNCS** and **Rede Nacional de Segurança Interna (RNSI)**, and alongside the **Liga dos Bombeiros Portugueses** warned personnel against phishing, smishing, vishing and quishing lures [S62][S63].

AVEIRO-DISTRICT MUNICIPALITIES (18 OCTOBER AND 5 NOVEMBER)	Eighteen days apart in the same district, two municipalities suffered disruptive intrusions with no established technical link between them [S60][S66]. **Câmara Municipal de Ovar** shut down digital services on **18 October**, suspended administrative deadlines, warned residents of possible personal-data exposure and continued phased recovery into November [S60][S61]. On **5 November**, **Câmara Municipal de Santa Maria da Feira** confirmed an overnight cyberattack halting IT systems, email and municipal landlines, notifying **CNCS** [S66][S67].
RESPONSE	National registries must restrict bulk export privileges and audit API downloads, while municipalities should pool 24/7 SOC monitoring and backup engineering through the **Fórum de Cibersegurança da Administração Local (FCSAL)** [S5].

Bottom line

Restrict bulk export rights on national personnel registries and build shared municipal SOC monitoring through the Local Administration Cybersecurity Forum (FCSAL).

S

CASE S

Intermarché Portugal refrigeration OT supply-chain attack

Retail refrigeration OT

Confirmed attack

CHRONOLOGY AND PHYSICAL IMPACT	On **2 November 2026**, a pan-European cyberattack targeting a remote refrigeration-management supplier raised refrigerator and freezer temperatures across supermarkets in several European countries [S64][S65]. **Grupo Mosqueteiros** and **APED** confirmed that **seven Intermarché stores in Portugal** were hit: **three stores** suffered total loss of refrigerated merchandise, while **four stores** avoided merchandise damage [S64][S65]. The group's central supply chain remained unaffected [S64].
RESPONSE	Retail operators and facilities teams must eliminate direct public internet exposure on third-party refrigeration and building controllers, enforce MFA on vendor remote maintenance and verify local manual temperature overrides.

Bottom line

Remove direct internet exposure on third-party refrigeration controllers and enforce MFA on vendor remote-maintenance access.

5.3 Recent activity: 12 to 26 November 2026

The final 15 days before cut-off (**12 to 26 November 2026**) produced **715 Portugal-tagged underground posts**, including **6** forum posts and **8** Portuguese-language Telegram posts (including `B10`) [S1]. Separately, **25 forum posts** mentioned Portugal across tagged and untagged threads (from which `B11` – `B15` are drawn), alongside **six confirmed public incidents** (`Cases T-U`) [S1]. Ransompedia logged **2 unverified Portugal-labelled listings** (`Booba-project` on 17 November and `N0n` on 25 November, identities withheld) [S2]. These figures describe strictly this 15-day recent window and do not imply a longer observation period.

CASE T

T ■ Worten customer-data breach and SMAS de Sintra web-form exposure

Confirmed breaches

Retail and municipal water (recent)

WORTEN (DISCLOSED 11 NOVEMBER; CUSTOMER NOTICES 12 NOVEMBER)	Retail group **Worten** confirmed unauthorised access to limited customer and service-provider records (`NIF`, telephone number, email address and certain order numbers), while confirming that **no passwords or payment-card details** were accessed [S68][S69][S70]. Worten patched the exploited technical flaw and notified **CNCS**, **CNPD** and **Polícia Judiciária** [S68][S70].
SMAS DE SINTRA (CONFIRMED 12 NOVEMBER)	Municipal water and sanitation utility **SMAS de Sintra** confirmed a cyberattack targeting online customer submission forms that copied records (`name`, `address`, `telephone`, `NIF`, `ID document` and `IBAN`) for a subset of customers [S71][S72]. SMAS de Sintra confirmed that payment histories and direct-debit mandates were not affected and notified **CNPD** and **CNCS** [S72].
RESPONSE	Retail and utility operators should patch public web-form vulnerabilities immediately, minimise long-term storage of `NIF` and `IBAN` submissions on web servers and alert affected users against invoice-redirection pretexting.

Bottom line

Patch public web-form flaws rapidly, minimise stored NIF and IBAN fields and warn affected customers against pretexting.

CASE U

U ■ Late-November public-portal disruptions and ADENE SCE intrusion

Confirmed cases

Public portals and energy (recent)

IMT (DISRUPTED FROM 14 NOVEMBER; CONFIRMED MID-NOVEMBER)	The **Instituto da Mobilidade e dos Transportes (IMT)** confirmed consecutive cyberattacks forcing the preventive suspension of its digital services,

disrupting driving schools and licensing workflows while reporting no indication of personal-data exfiltration [S74].

ASAE (15 NOVEMBER) AND CÂMARA MUNICIPAL DO PORTO (21 NOVEMBER)	On **15 November**, an official **ASAE** (Autoridade de Segurança Alimentar e Económica) source confirmed a website defacement taking the public portal offline, with **CNCS** confirming outreach [S73]. On **21 November**, **Câmara Municipal do Porto** confirmed a CMS defacement across its homepage and sub-pages with **no personal-data compromise** and formal notification to **CNCS** [S75][S76]. Protest imagery and intruder slogans are omitted here.
ADENE (23 NOVEMBER)	On **23 November 2026**, the national energy agency **ADENE** confirmed an unauthorised intrusion and isolated affected systems [S77]. ADENE temporarily suspended the **Sistema de Certificação Energética dos Edifícios (Portal SCE)** while keeping issued certificates valid, notifying **CNCS** and **Polícia Judiciária** [S77][S78].
LAW-ENFORCEMENT MILESTONES IN THE SAME WINDOW	On **17 November**, **PJ UNC3T** arrested two suspects over fraudulent retail use of cloned French payment cards exceeding **EUR 48,000** [S31]. On **23 November**, **PJ** participated in Europol's **Operation PowerOFF** against DDoS-for-hire platforms, securing **59 Google delistings from 62 requests**, the highest tally among 20 participating countries [S32].
OTHER 12 TO 26 NOVEMBER UNDERGROUND SIGNALS (B10–B15)	Posts inside this 15-day window included spoofed Portuguese bank SMS routes (B10 , 17 Nov), an unconfirmed education-portal export (B11 , 14 Nov) and 55,000 bank-labelled leads (B12 , 21 Nov) [S1]. On 23 November, accounts also posted recycled historical airline records (B13), a 71,000-line Portugal combolist (B14) and 500,000 purported consumer leads (B15) [S1].

Bottom line

Harden public CMS instances, separate web-facing portals from core registries and rehearse rapid failover hosting.

KEY TAKEAWAYS

01

Twenty officially confirmed 2026 incidents show real operational impact across municipalities, national registries, healthcare, utilities, retail and telecoms.

02

Grupo Águas de Portugal water supply and Metro Mondego metrobus operations were reported unaffected, while a vendor-managed refrigeration system was hit at seven Intermarché stores.

03

Six confirmed incidents (disclosed or notified to customers from 12 November) and two PJ operations landed in the recent window.

CHAPTER 06

Disruption, hacktivism and claim versus reality

06

THIS CHAPTER ANSWERS

How should Portuguese defenders separate real operational impact from hacktivist claims and non-cyber outages?

+36%

YoY rise in CERT.PT DDoS availability incidents in 2025 (115 cases)

6.1 Chronology of 2026 disruption, enforcement and resilience milestones 52

6.2 Hacktivism, DDoS pressure and municipal readiness 53

6.3 Claim versus official record 53

CHAPTER 06

Disruption, hacktivism and claim versus reality

IN SHORT

Portugal's 2026 disruption landscape combines verified volumetric DDoS and portal defacements, unverified Telegram hacktivist claims and non-cyber technical failures that are often misattributed online. The March 2026 ENTSO-E technical report attributed the 28 April 2025 Iberian blackout to technical voltage-control factors, and the cited official sources identify no cyber cause. Meanwhile, CERT.PT logged a 36% rise in DDoS cases in 2025 and SIS flagged pro-Russian hacktivist OT sabotage risks. Ground crisis communications strictly in owned service telemetry and official findings.

6.1 Chronology of 2026 disruption, enforcement and resilience milestones

15 Jan 2026	CNPD and CNCS sign national cooperation protocol for 24/7 emergency coordination [S9]
12 Feb 2026	Câmara Municipal da Guarda suffers prolonged cyberattack blocking municipal digital services [S34] [S35]
4 Mar 2026	PJ arrests two suspects in Europol LeakBase takedown and supports Tycoon 2FA disruption (>160 PT organisations) [S29]
20 Mar 2026	ENTSO-E technical report on the 28 April 2025 Iberian blackout cites voltage-control factors; no cyber cause identified [S16][S17]
3 Apr 2026	Decreto-Lei n.º 125/2025 (NIS2 transposition) enters into force across Portugal [S22]
21 May 2026	SPMS notifies CNCS of unauthorised SNS 24 access reaching over 100,000 patients [S39][S40]
23 Jun 2026	CNCS Regulation n.º 756/2026 operationalising MyCiber portal enters into force [S23][S24]
31 Jul 2026	Grupo Águas de Portugal detects administrative IT cyberattack; water supply remains unaffected [S53] [S54]
14 Sep 2026	MEO mitigates three volumetric DDoS waves affecting international links without intrusion [S55][S56]
28 Sep 2026	Câmara Municipal de Valongo runs CIBER 26 municipal critical-service cyber exercise [S21]
24 Oct 2026	ANEPC suspends National Firefighters Registry (RNBP) after attack copies ~60,000 records [S62][S63]
2 Nov 2026	Pan-European refrigeration-controller OT attack hits seven Intermarché stores in Portugal [S64][S65]
23 Nov 2026	ADENE isolates Portal SCE after intrusion; PJ reports 59 delistings in Europol Operation PowerOFF [S32] [S77]

6.2 Hacktivism, DDoS pressure and municipal readiness

Official reporting in **RASI 2025** established a clear availability baseline heading into 2026: **CERT.PT** recorded a **36% year-on-year increase** in denial-of-service availability incidents (**115** cases) [S5]. In the same report, **SIS** warned that pro-Russian nationalist hacktivist collectives represent an ongoing cybersabotage threat against European and Portuguese critical-infrastructure and industrial or operational management systems [S5]. In July 2025, **Eurojust** and **Europol** disrupted the **NoName057(16)** DDoS infrastructure (described by Eurojust as pro-Russian) across 12 countries, taking down over 100 servers and issuing seven arrest warrants [S33].

Inside our 2026 Portugal-tagged Telegram corpus, three unverified hacktivist claims surfaced and must be handled without amplification [S1]:

- **313 Team (26 March 2026):** A Telegram channel claimed a brief DDoS attack against a Portuguese law-enforcement website; no official outage confirmation was found [S1].
- **Z-Pentest Alliance (11 May 2026):** A Spanish-language Telegram relay posted an unverified claim targeting an internet-exposed industrial lighting and automation controller in Portugal [S1]. No official disruption was confirmed, though the target class falls within the SIS warning in RASI 2025 on cybersabotage against critical-infrastructure and industrial or operational management systems [S5].
- **BNCT (31 October 2026):** A channel claimed the defacement of two exhibition subdomains belonging to a Portuguese public cultural institution (institution and subdomains withheld due to absence of official confirmation) [S1].

Separately, Portuguese civil-protection and local authorities expanded preparedness exercises in 2026. On **28 September 2026**, **Câmara Municipal de Valongo** ran the **CIBER 26** municipal cyber-emergency exercise simulating simultaneous disruptions across water supply, energy distribution and schools [S21]. Ahead of Portugal's **2026 presidential election**, the **Comissão Nacional de Eleições (CNE)** opened a public disinformation-reporting channel, and media regulator **ERC** published a joint study with **LabCom-UBI** on online disinformation patterns [S18][S19]. Those initiatives addressed online information integrity rather than technical election-system intrusions.

6.3 Claim versus official record

Routine IT outages, historical events and opportunistic hacktivist posts regularly blur public perception in Portugal. Specialist timeline tracking by Ciberseguranca.PT logged **32 public Portuguese cyber events** through 23 November 2026 alongside clearly separated non-attack IT failures (including clinical IT outages, emergency-dispatch faults and Microsoft 365 disruptions) [S79].

Claim or public perception	Established record	Defensive discipline
Speculation attributing the 28 April 2025 Iberian power outage to a cyberattack [S16][S17]	The ENTSO-E technical report validated by ACER and presented on 20 March 2026 attributes the outage to multiple technical factors, including insufficient voltage control, with initial failures in Granada, Badajoz and Seville, and no cyber cause identified [S16][S17]	Do not attribute grid or infrastructure outages to cyberattacks unless official technical investigations confirm one

Claim or public perception	Established record	Defensive discipline
Forum posts on 7 October claim compromise of Portuguese secret-service classified networks [S58][S59]	SIRP confirmed on 8 October that the exposed files came from an external web contractor's development server for public websites, with zero classified or operational systems affected [S58] [S59]	Separate external vendor web hosting from internal environments and verify official scope notices rapidly
Forum sellers advertise an airline dataset as "2026" on 13 September and 23 November (`B03` , `B13`) [S1]	Sample rows display historical loyalty-programme identifier fields with 2017–2018 dates matching an older, previously disclosed leak; no 2026 airline breach is established [S1]	Hash and date-check sample rows against historical breach archives before escalating
September campus network faults at Universidade de Aveiro perceived as a second cyberattack [S52]	Universidade de Aveiro clarified that the September outage resulted from a routine August system update unrelated to the confirmed July ransomware attack [S52]	Publish transparent root-cause notices distinguishing maintenance faults from security incidents
Telegram hacktivist posts claim attacks on Portuguese law-enforcement portals or exposed OT controllers (313 Team, Z-Pentest Alliance) [S1]	Neither claim received official confirmation of operational disruption; however, exposed OT controllers carry real risk as demonstrated in November (`Case S`) [S5][S64]	Measure real service availability, inspect exposed OT assets directly and omit actor rhetoric from public updates

KEY TAKEAWAYS

01

Official technical findings attribute the April 2025 Iberian blackout to voltage-control factors and identify no cyber cause.

02

Distinguish verified DDoS and defacements from unverified Telegram claims and routine IT outages.

03

Exercise municipal cross-service continuity (as in Valongo's CIBER 26) and communicate strictly from owned telemetry.

CHAPTER 07

Ransomware, extortion listings and threat profiles

THIS CHAPTER ANSWERS

Which extortion labels are targeting Portugal in 2026, and how does Portugal compare with regional peers?

36

Portugal-labelled ransomware listings across 17 claimant labels (vs 21 in 2025)

7.1 Portugal ransomware trajectory and comparator benchmark 56

7.2 Threat network and profiled groups 58

7.3 State-attributed espionage context and hacktivist profiles 63

CHAPTER 07

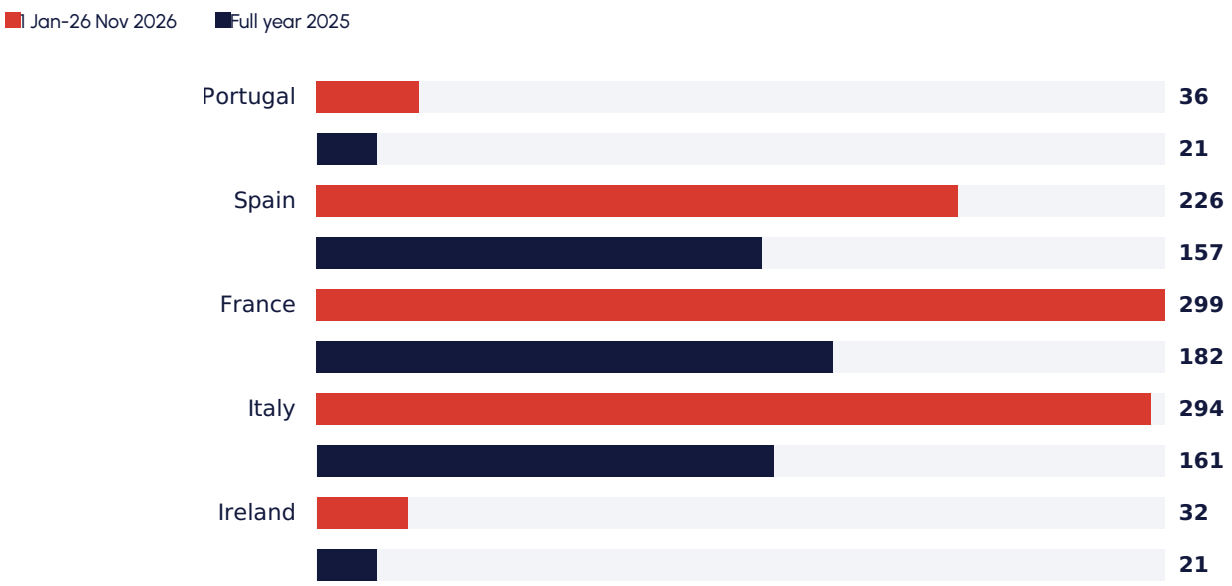
Ransomware, extortion listings and threat profiles

IN SHORT

Ransompedia recorded 36 Portugal-labelled ransomware listings between 1 January and 26 November 2026, up from 21 across all of 2025, with 30 of 36 (83.3%) arriving between June and November. The Gentlemen (9) and Qilin (7) lead activity, each matching one publicly confirmed victim (Metro Mondego and Santa Casa da Misericórdia de Santo Tirso). Thirty-four listings remain unverified, and one Nova duplicate bounds unique claims to at most 35. Verify every extortion listing against owned forensic logs and test offline immutable backup restores regularly.

7.1 Portugal ransomware trajectory and comparator benchmark

Portugal's 36 ransomware listings in 2026 surpass full-year 2025 totals alongside regional peers



Source: Brandefense Ransompedia, 1 January-26 November 2026 versus full-year 2025 [S2]. Unequal periods; country-labelled claims, not unique victims, confirmed intrusions or a national security ranking.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Between **1 January and 26 November 2026**, Ransompedia recorded **36 Portugal-labelled ransomware listings** across **17 claimant labels**, rising **71.4%** above the **21 listings** logged across full-year **2025** (and contributing to **104** all-time Portugal-labelled entries) [S2]. Across Portugal's four regional comparators (2026 window vs full-year 2025), **Spain** logged **226** listings (vs 157) and **France** logged **299** (vs 182) [S2]. **Italy** logged **294** (vs 161) and **Ireland** logged **32** (vs 21) [S2].

Four analytical nuances keep Portugal's 2026 ransomware count accurate [S2]:

- **Sharp second-half acceleration.** Monthly Portugal listings climbed steeply after May: February (1), March (3), April (1), May (1), June (5), July (10), August (2), September (7), October (3) and November (3) [S2]. Two of the three November entries appeared inside the 12–26 November recent window [S2]. Exactly **30 of 36 listings (83.3%)** occurred from June onward [S2].
- **Distinct claims.** On 24 June 2026, `Nova` published two same-day entries naming the same Portuguese organisation under both its domain and short name [S2]. Portugal's 36 listings therefore correspond to **at most 35 distinct claimed entities** [S2].
- **Only two listings are publicly confirmed.** Independent public confirmations exist for **Santa Casa da Misericórdia de Santo Tirso** (`Qilin` , 16 June, `Case L`) and **Metro Mondego** (`The Gentlemen` , 16 July, `Case M`) [S2] [S47][S48]. The other **34 listings** remain unverified criminal assertions whose identities are withheld.
- **Sector tags.** Source-assigned sector tags led with **manufacturing (7)**, **consulting (4)**, **construction (3)**, **finance (3)**, **education (3)**, **global (3)**, **logistics (2)** and **health (2)** [S2]. Single entries spanned agribusiness, engineering, heavy industry, road transport, software/SaaS, universities, high-tech and culture [S2]. Several of Portugal's confirmed municipal attacks (`Cases H, K, R`) did not appear on tracked leak sites, a reminder that public extortion trackers can undercount total operational encryption events.

Claimant label	2026 PT listings	Active months (2026)	Verification status
The Gentlemen	9	Feb, Mar, Jun, Jul, Sep	1 publicly confirmed (`Metro Mondego` , `Case M`); 8 claims unverified [S2][S48]
Qilin	7	Mar, Jun, Jul, Aug, Oct, Nov	1 publicly confirmed (`Santo Tirso` , `Case L`); named by CERT.PT in RASI 2025; 6 claims unverified [S2][S5] [S47]
SafePay	3	Mar, May, Sep	Also logged 12 Spain-labelled listings in 2026; Portugal claims unverified [S2]
N0n	2	Oct, Nov (25 Nov)	Active inside 12–26 Nov recent window; claims unverified [S2]
Majinahanashi	2	Jul, Oct	Claims unverified [S2]
Nova	2	Jun (same day)	Two same-day entries for one entity; claim unverified [S2]

Claimant label	2026 PT listings	Active months (2026)	Verification status
Eleven single-listing labels	11	Mar–Nov	`Arcus Media`, `Booba-project` (17 Nov), `Dead-lock`, `DragonForce`, `Lockbit5`, `M3rx`, `Panzer`, `Section9`, `Settra`, `Space Bears`, `UnSafe`; all unverified [S2]
Total recorded	**36**	**Feb–Nov 2026**	**At most 35 distinct claimed entities; 2 publicly confirmed** [S2]

7.2 Threat network and profiled groups

The relationship view below strictly separates Brandefense own-source observations (`own data`), official agency reporting (`official`) and confirmed public reporting (`public reporting`). No unverified operational link is inferred between criminal ransomware labels, hacktivist channels and state-attributed espionage assessments.

Own post Relay Official statement Public reporting Our observation

SafePay

Own data
3 listings, S2 ↓

Portugal-labelled listings

Own data
9 listings, S2 ↑

The Gentlemen

public reporting
Metro Mondego confirmed 6 Jul ransomware, S48-S50 ↓

Confirmed PT ransomware

public reporting
Santo Tirso confirmed 8 Jun ransomware, S46-S47 ↑

Qilin

NOn

Own data
2 listings incl. 25 Nov, S2 ↓

Portugal-labelled listings

Own data
7 listings, S2 ↑

Qilin

Nova & Majinahanashi

Own data
2 listings each (incl. 1 Nova duplicate), S2 ↓

Portugal-labelled listings

Z-Pentest Alliance

Own data
Claim class matches SIS OT context (S1, S5); no official link to the group ↓

RASI 2025 / Eurojust

official
Eurojust disruption (S33); SIS/CERT.PT DDoS context (S5) ↓

NoName057(16)

The Gentlemen

Thegentlemen (Ransompedia listing label)

Ransomware/extortion listing label | No state attribution established here

CLAIMED TARGETS

Portugal-labelled entries spanning transport, construction, manufacturing, finance and education; 8 unconfirmed identities withheld

IN PORTUGAL, 2026

2026 window

9 Portugal-labelled listings (February, March, June, July and September 2026), S2; 1 confirmed publicly (Metro Mondego, S48-S50)

SEEN IN PUBLIC REPORTING

[S2] 9 listings recorded in Ransompedia (highest single claimant on Portugal in 2026)

[S48-S50] Metro Mondego confirmed 6 July ransomware and public extortion claim affecting personalised transit-pass holder data

OUR ASSESSMENT

The Gentlemen accounted for one quarter of Portugal-labelled ransomware listings in 2026 (9 of 36), peaking in July and September. Metro Mondego independently confirmed a 6 July ransomware incident matching the 16 July listing; the remaining eight listings remain individually unverified claims.

CONFIDENCE

High for the recorded count and Metro Mondego confirmation; other 8 claims unverified

Qilin

Label in Ransompedia and CERT.PT 2025 taxonomy

Ransomware-as-a-service extortion label | No state attribution established here

IN PORTUGAL, 2026

2026 window

7 Portugal-labelled listings (March, June, July, August, October and November 2026), S2; 1 confirmed publicly (Santa Casa da Misericórdia de Santo Tirso, S46-S47)

CLAIMED TARGETS

Portugal-labelled entries across logistics, healthcare, manufacturing, technology, finance and consulting; 6 unconfirmed identities withheld

SEEN IN PUBLIC REPORTING

[S2] 7 listings recorded in Ransompedia (second largest claimant on Portugal in 2026)

[S5] Named by CERT.PT in RASI 2025 among the ransomware variants most frequently observed in Portugal in 2025

[S46-S47] Santa Casa da Misericórdia de Santo Tirso confirmed the 8 June intrusion; Qilin listed the organisation on 16 June

OUR ASSESSMENT

Qilin demonstrates sustained multi-year pressure on Portuguese organisations, bridging CERT.PT's 2025 incident response records and seven 2026 leak-site listings. While Santa Casa da Misericórdia de Santo Tirso confirmed the June attack, the other six 2026 listings require independent internal verification.

CONFIDENCE
High for recorded counts, CERT.PT 2025 baseline and Santo Tirso confirmation; other 6 claims unverified

SafePay

Safepay (Ransompedia listing label)

Ransomware/extortion listing label | No state attribution established here

IN PORTUGAL, 2026

2026 window

3 Portugal-labelled listings (March, May and September 2026), S2

CLAIMED TARGETS

Portugal-labelled commercial, manufacturing and consulting entries; all identities withheld

SEEN IN PUBLIC REPORTING

[S2] 3 Portugal-labelled listings and 12 Spain-labelled listings recorded in Ransompedia across 2026

OUR ASSESSMENT

SafePay is the third largest claimant on Portugal-labelled entries (3 of 36) and is concurrently active across neighbouring Spain (12 listings). None of the three Portugal-labelled entries had an official public confirmation by cut-off, so each must be treated strictly as an unverified extortion claim.

CONFIDENCE
High for the recorded count; individual Portugal claims unverified

NOn

Label in Ransompedia

Ransomware/extortion listing label | No state attribution established here

IN PORTUGAL, 2026

2026 window

2 recorded Portugal-labelled listings (24 October; 25 November, inside the recent window), S2

CLAIMED TARGETS

Manufacturing and construction entries; identities withheld

SEEN IN PUBLIC REPORTING

[S2] 2 Portugal-labelled listings recorded in Ransompedia in October-November 2026

OUR ASSESSMENT

N0n accounts for one of the two Portugal-labelled ransomware listings posted during the 12-26 November recent window (alongside Booba-project on 17 November). Listings lack independent victim confirmation and require forensic verification before assuming operational impact.

CONFIDENCE

High for the recorded count; individual claims unverified

Nova and Majinahanashi

Labels in Ransompedia

Ransomware/extortion listing labels | No state attribution established here

IN PORTUGAL, 2026

2026 window

2 recorded listings each in Ransompedia (Nova on 24 June; Majinahanashi in July and October 2026), S2

CLAIMED TARGETS

Consulting, agribusiness and manufacturing entries; identities withheld

SEEN IN PUBLIC REPORTING

[S2] Nova posted two same-day entries for the same entity on 24 June; Majinahanashi has two recorded entries (July and October)

OUR ASSESSMENT

Nova's two 24 June listings reference the same organisation under a domain and a short name, so Portugal's 36 listings correspond to at most 35 distinct claimed entities.

CONFIDENCE

High for the recorded counts; individual claims unverified

7.3 State-attributed espionage context and hacktivist profiles

In **RASI 2025**, **Polícia Judiciária** and **Serviço de Informações de Segurança (SIS)** assess sustained state-linked cyber espionage and disruption risks against Portuguese critical sectors, diplomacy and dual-use research [S5]. Portuguese authorities attribute those primary state-linked threats to actors connected with **Russia, North Korea, China and Iran** [S5]. Those attributions belong strictly to Portuguese authorities in RASI 2025; no independent Brandefense state attribution is added here. Alongside espionage risks, **SIS** and **Eurojust** highlight sustained pro-Russian hacktivist pressure targeting public portals and exposed industrial controls [S5][S33].

Z-Pentest Alliance

Z-Alliance (Telegram channel label)

Hacktivist channel (self-described pro-Russian) | Pro-Russian alignment self-declared in its Telegram channel; RASI 2025 does not name the group

IN PORTUGAL, 2026

May 2026

Claimed cyberattack targeting an industrial lighting/automation controller in Portugal on 11 May 2026, S1

CLAIMED TARGETS

Internet-exposed industrial automation and OT controllers

SEEN IN PUBLIC REPORTING

[S1] Spanish-language Telegram relay of a Z-Pentest Alliance claim against an internet-exposed industrial lighting and automation controller in Portugal (11 May 2026)

[S5] SIS chapter of RASI 2025 highlights cybersabotage risks from pro-Russian nationalist hacktivist groups targeting industrial and OT systems in Portugal

OUR ASSESSMENT

The May Telegram claim remains unverified by Portuguese authorities and shows no confirmed physical disruption. However, it falls within the target class that SIS describes in RASI 2025: critical-infrastructure and industrial or operational management systems.

CONFIDENCE

High for the Telegram claim record and SIS baseline; technical impact unverified

NoName057(16)

DDoSia hacktivist collective

Pro-Russian hacktivist DDoS collective (Eurojust attribution) | Pro-Russian hacktivist alignment as stated by Eurojust

IN PORTUGAL, 2026

2025-2026 context

In July 2025, an international Eurojust/Europol take-down disrupted over 100 servers and issued seven arrest warrants (S33); SIS RASI 2025 flags ongoing pro-Russian hacktivist risk against European and Portuguese critical infrastructure (S5)

CLAIMED TARGETS

Government portals, transport, energy and financial public websites across EU and NATO states

SEEN IN PUBLIC REPORTING

[S33] Eurojust release detailing the 12-country disruption of NoName057(16) botnet and volunteer mobilisation infrastructure

[S5] RASI 2025 documents a 36% rise in CERT.PT DDoS incidents in 2025 alongside SIS warnings on pro-Russian hacktivism

OUR ASSESSMENT

Although no Portugal-specific NoName057(16) claim appeared in the 2026 Portugal-tagged corpus after the international disruption, CERT.PT's 36% DDoS increase in 2025 and MEO's September 2026 volumetric DDoS underline persistent denial-of-service exposure for Portuguese networks.

CONFIDENCE

High for Eurojust and RASI 2025 official reporting

Technique identifiers are omitted where cited public passages do not supply an explicit mapping. Defenders should treat both criminal ransomware surges and official state-threat baselines as concrete prompts to patch internet-facing appliances (§12.2), enforce phishing-resistant MFA and test immutable backup restoration.

KEY TAKEAWAYS

01

Portugal's 36 Ransompedia listings rose 71.4% above 2025, with 83.3% concentrated from June through November.

02

The Gentlemen (9) and Qilin (7) drive nearly half of Portugal's listings and match two publicly confirmed 2026 victims.

03

Keep criminal extortion labels, hacktivist claims and official RASI 2025 state assessments strictly separate.

CHAPTER 08

Fraud, identity abuse and secondary harm

THIS CHAPTER ANSWERS

How are phishing, spoofed SMS and leaked citizen identifiers shaping Portugal's fraud economy?

EUR 14.7M

fake Portuguese-language crypto investment fraud logged by PJ in RASI 2025

8.1 National digital-fraud trends across Banco de Portugal, PJ, CNCS and ANACOM 66

8.2 Secondary harm from 2026 citizen-data breaches and mobile malware 67

8.3 Observed payment-card postings: narrow scope 67

CHAPTER 08

Fraud, identity abuse and secondary harm

IN SHORT

Everyday cyber harm in Portugal centres on social engineering, phishing, caller-ID/SMS spoofing and investment fraud rather than pure technical exploits. Banco de Portugal logged a 40.4% drop in H1 2025 payment-fraud losses (EUR 5.3 million) under Strong Customer Authentication and Confirmation of Payee. Yet PJ recorded EUR 14.7 million in fake crypto-investment scams, CERT.PT saw phishing rise 93% and ANACOM saw spoofing complaints double by mid-2025. Link every citizen-data breach (NIF, CC, IBAN) directly to customer anti-fraud warnings and carrier spoofing blocks.

8.1 National digital-fraud trends across Banco de Portugal, PJ, CNCS and ANACOM

Multiple official Portuguese institutions provide complementary benchmarks showing both defensive gains in regulated payment rails and persistent losses in social engineering:

- **Banco de Portugal payment-fraud gains (`H1 2025` report released May 2026):** Total payment-fraud losses fell **40.4% year-on-year** to **EUR 5.3 million** in H1 2025 [S12]. Card fraud stood at **66 cases per million** (average **EUR 48**), with Strong Customer Authentication (**SCA**) cutting rates over sevenfold (**0.0008%** vs **0.0058%**) [S12]. Credit transfers averaged **10 cases per million** (**EUR 2,564**, mainly payer manipulation), and direct debits **4 per million** (**EUR 11.50**) [S12].
- **Beneficiary checks and new monitoring hub:** Since May 2024, **Confirmation of Payee** and **SPIN** avoided **EUR 6.5 million** in fraudulent transfers and cut payer-manipulation transfer fraud by **21%** [S13]. On **25 May 2026**, Banco de Portugal launched its **Digital Fraud Monitoring Platform** (Plataforma de Acompanhamento da Fraude Digital) [S13][S14].
- **Polícia Judiciária and Ministério Público pressure:** In **RASI 2025**, **PJ** documented **EUR 14,715,736.21** in losses to fake Portuguese-language cryptocurrency investment platforms and sustained growth in IT fraud [S5]. The **Ministério Público Cybercrime Office** confirmed a **13.16% rise** in emailed cybercrime complaints in 2025 [S8]. During 2026, PJ recovered roughly **EUR 500,000** in stolen digital assets under **Operation Cryptoclaim** and joined March takedowns of **Tycoon 2FA** (over 160 Portuguese organisations) and **LeakBase** (two arrests) [S29] [S30]. On **17 November**, PJ UNC3T also arrested two suspects over cloned French payment cards exceeding **EUR 48,000** [S31].
- **CNCS / CERT.PT and ANACOM lure trends:** In **RASI 2025**, CERT.PT logged a **93% surge in phishing** alongside **192 CEO Fraud** cases (**+20%**) and **118** fake-recruitment scams [S5]. CERT.PT also logged **99** "Olá Pai / Olá Mãe" scams, **85** vishing reports and active **ToxicPanda** Android banking-trojan campaigns [S5]. On **25 June 2026**, CNCS warned of fraudulent emails impersonating CNCS itself to push a fake critical system update [S80]. By mid-July 2025, **ANACOM** had received about **70** caller-ID and SMS spoofing complaints, more than double the roughly **30** for all of 2024 (about 75% in Q2 2025), and proposed legislative countermeasures [S15].

Official indicator	Value	Period and issuer	Operational significance
Payment-fraud losses	EUR 5.3M (-40.4% YoY)	H1 2025 (Banco de Portugal, published May 2026) [S12]	SCA (0.0008% vs 0.0058%) and payee checks cut rail-level losses
Fraud avoided via CoP and SPIN	EUR 6.5M (-21% manipulation)	May 2024–May 2026 (Banco de Portugal) [S13]	Real-time beneficiary matching meaningfully slows transfer scams
Fake crypto-investment losses	EUR 14,715,736.21	RASI 2025 (Polícia Judiciária) [S5]	Authorised-push investment scams dwarf technical card theft
CEO fraud / fake recruitment / family scams	192 / 118 / 99	2025 (CNCS / CERT.PT via RASI 2025) [S5]	Phishing jumped +93%; corporate BEC and messaging lures expand
Caller-ID and SMS spoofing complaints	~70 (vs ~30 in 2024)	Jan to mid-Jul 2025 vs full-year 2024 (ANACOM) [S15]	Matches live underground ads for spoofed Portuguese bank SMS routes (`B10`)

8.2 Secondary harm from 2026 citizen-data breaches and mobile malware

Confirmed 2026 breaches repeatedly exposed structured identifiers (`NIF` , Citizen Card `CC` , `NISS` , `SNS` , `IBAN` , email and phone numbers). Affected disclosures spanned **SNS 24** (`>100,000`), **ANEPC RNBP** (`~60,000`), **Metro Mondego**, **Worten**, **SMAS de Sintra** and **Canvas** [S37][S39][S48][S62][S70][S72]. None of those disclosures exposed banking passwords or payment cards, yet combined `NIF` , address and `IBAN` details give fraudsters high-credibility context for spoofed SMS (`B10`), phone pretexting and fake **Multibanco** payment references (`B09`) [S1][S63][S72].

In **February 2026**, **ThreatFabric** documented the **Massiv** Android banking trojan disguised as a sideloaded IPTV application targeting Portugal's **Chave Móvel Digital** ecosystem [S81]. The malware abuses Android Accessibility services to capture credentials and authorise fraudulent transfers [S81]. That finding aligns directly with underground forum chatter on **21 February** recirculating Massiv mechanics and summer–autumn Iberian advertisements for Android NFC-relay kits (`Case G`) [S1].

8.3 Observed payment-card postings: narrow scope

SCOPE OF THE CARD FIGURES

These figures describe a limited observed publication population in retained underground posts. They do not estimate Portuguese payment-card theft, national card-fraud losses or live card validity.

Across retained 2026 underground posts, Brandefense observed **155 Portugal-issuer card occurrences** covering **132 distinct masked card numbers** across **114 posts** [S1]. Those records span **51 distinct six-digit BINs** and **6 named Portuguese issuers** (identities withheld) [S1]. By card network, **Mastercard** accounted for **73** distinct records, **Visa** for **44** and other networks for **15**; by card type, **Debit** accounted for **46**, **Credit** for **42** and unspecified cards for **44** [S1].

Cards can appear across multiple venues: **80** distinct cards (**89** occurrences) appeared in checker-bot outputs, **35** (**36** occurrences) in chats and **21** (**30** occurrences) on forums [S1]. Status labels were unspecified for **72** cards (**85** occurrences), network errors for **46** (**48**), declined for **9** (**13**) and approved for **9** (**9**) [S1]. Separately, **1,776 offer posts** without clear-text cards named Portugal, including **1,433 multi-country shop batch listings** [S1]. Across those batches, **49** listed Portugal first, with medians of **49 countries**, **1,485 cards** and **USD 10 to 25** per card [S1].

KEY TAKEAWAYS

01

Payment-fraud losses fell 40.4% in H1 2025, which Banco de Portugal links to SCA, Confirmation of Payee and SPIN; social-engineering and crypto-investment losses remain high.

02

Leaked NIF, CC and IBAN records from 2026 breaches feed directly into spoofed SMS, Multibanco reference fraud and Chave Móvel Digital malware lures.

03

Treat the 132 observed clear-text card records as a narrow publication signal, never a measure of national card theft.

CHAPTER 09

Banking, payments and digital-identity resilience

THIS CHAPTER ANSWERS

How exposed is Portugal's financial sector externally, and where are operational controls strongest?

51

severe DORA ICT incidents reported to Banco de Portugal in 2025 (+16 YoY)

9.1 Banking-sector exposure aggregates (no bank names or scores) 70

9.2 Domestic payment-rail abuse, Chave Móvel Digital and DORA continuity 71

CHAPTER 09

Banking, payments and digital-identity resilience

IN SHORT

Portuguese banking leads all domestic sectors in domain hygiene, with 24 of 25 domains enforcing DMARC and 21 of 22 reachable hosts setting HSTS. Yet 13 of 25 assessed finance domains still showed current credential listings, and 99.1% of device records reflect non-employee endpoints. Banco de Portugal also logged 51 severe DORA incidents in 2025 affecting 1.3 million users, while criminals advertise spoofed bank SMS routes and domestic drops. Separate staff containment from customer fraud queues and test DORA supplier failover continuously.

9.1 Banking-sector exposure aggregates (no bank names or scores)

In the **27 November 2026** snapshot, all **25 domains** in Portugal's **Banking and finance** sector cell were assessed for both passive configuration and Atlas exposure [S3][S4]. All figures below are strict sector or subset aggregates; **no individual bank is named** and **no sector or group Atlas score is published**:

- **Strongest email and transport hygiene in Portugal:** Twenty-four of 25 banking domains (**96.0%**) enforce DMARC (**16** `reject`, **8** `quarantine`, `1` `p=none`, `0` missing) [S3][S82]. Among reachable hosts, **22 of 23** hold valid apex TLS certificates and **21 of 22** (**95.5%**) publish HSTS [S3][S85].
- **Full 25-domain Banking and finance cell:** Thirteen of 25 domains (**52.0%**) showed a current credential listing when checked [S4]. Twenty-four of 25 showed **50,346** cumulative device associations: **429** employee (**0.9%**) versus **49,917** non-employee (**99.1%**) [S4]. All **25** carried **119,409** historical credentials (`63,836` breach database, `46,279` combolist, `9,294` stealer), while **23** showed **2,374** similar names and documents totalled **53** [S4].
- **Strict 15-domain matched card-issuing bank subset:** Within the cell, **10 of 15** matched card-issuing institutions had a current listing when checked [S4]. Fourteen of 15 showed **34,341** non-employee devices (top three represent **56.4%**), and **13 of 15** showed **327** employee devices [S4]. Six issuers matched **86** attributed masked cards in §8.3 (top three **79.1%**) [S1]. Non-employee devices reflect infected consumer endpoints rather than bank breaches, and card posts establish no issuer ranking.

Banking-sector question	Observed aggregate signal (27 Nov 2026)	Responsible owner
Do Portuguese banking domains enforce DMARC and HSTS?	24 of 25 enforcing DMARC (96.0%); 21 of 22 reachable HSTS (95.5%) [S3]	Messaging and domain security
How many finance domains carry current credential listings?	13 of 25 finance domains (10 of 15 in matched card-issuer subset) [S4]	Identity operations and SOC
Are finance device records mostly staff or retail customers?	50,346 total: 429 employee (0.9%) vs 49,917 non-employee (99.1%) [S4]	Endpoint containment vs retail fraud
What underground services target Portuguese bank customers?	Spoofed bank SMS routes (`B10`), EUR 2K–10K bank drops (`B08`), Multibanco tools (`B09`), 55K leads (`B12`) [S1]	Fraud operations and brand protection
Does an observed BIN or lead listing prove a bank breach?	No; neither BIN posts nor marketing lead files verify bank intrusion [S1]	SOC triage and fraud intelligence

9.2 Domestic payment-rail abuse, Chave Móvel Digital and DORA continuity

Portuguese retail banking relies on tightly coupled national rails (**SIBS**, **Multibanco**, **MB WAY**, **SPIN**) and national digital identity (**Chave Móvel Digital**). Underground listings in 2026 targeted the human and telecom edges rather than core settlement switches. Activity spanned Portuguese KYC recruitment (`USD 30`), **EUR 2,000–10,000** domestic bank drops (`B08`) and spoofed SMS gateways (`B10`) [S1]. Actors also promoted Multibanco reference tools (`B09`) and Android trojans (`Massiv` , `ToxicPanda`) targeting mobile signing flows [S1][S5][S81].

Banco de Portugal's 2025 Payment Systems Report also underscored operational continuity as a board risk [S12]. Supervised entities logged **51 severe ICT incidents under DORA in 2025** (**+16** YoY), affecting **1.3 million users** and **EUR 2.4 billion** in transaction value (**EUR 751 million** excluding TARGET) [S12]. Under **Lei n.º 73/2025**, **Banco de Portugal** serves as the single DORA major-incident hub for credit and payment institutions alongside **CMVM** and **ASF** [S25]. Financial CISOs should rehearse three DORA drills: telecom degradation during peak Multibanco/MB WAY clearing, Android trojan surges targeting `Chave Móvel Digital` and rapid mule-account inflow detection.

KEY TAKEAWAYS

01

Banking leads Portugal in DMARC (24/25) and HSTS (21/22), yet 13 of 25 assessed domains still show current credential listings requiring rapid triage.

02

Non-employee devices represent 99.1% of banking device records, separating consumer-endpoint malware from staff-credential containment.

03

Fifty-one severe DORA incidents in 2025 show that ICT and third-party resilience demands the same board priority as anti-fraud controls.

CHAPTER 10

Regulation, reporting clocks and national response

THIS CHAPTER ANSWERS

Which Portuguese authority, portal and legal deadline applies when an incident hits in 2026?

3 April 2026

Decreto-Lei n.º 125/2025 (NIS2 transposition) entered into force in Portugal

10.1 Portugal's 2026 statutory baseline 73

10.2 Distinct Portuguese reporting clocks and recipients 74

10.3 Practical compliance lessons from 2026 Portuguese incidents 75

CHAPTER 10

Regulation, reporting clocks and national response

IN SHORT

Five statutory frameworks govern cyber and privacy reporting in Portugal during 2026. Decreto-Lei n.º 125/2025 (NIS2, 3 April) and CNCS Regulation n.º 756/2026 (MyCiber, 23 June) operate alongside Lei n.º 73/2025 (EU DORA under Banco de Portugal, CMVM and ASF). GDPR under Lei n.º 58/2019 (CNPD) and EU Cyber Resilience Act manufacturer reporting (11 September 2026) run on separate clocks. Register on MyCiber, appoint required officers and log awareness separately from classification.

10.1 Portugal's 2026 statutory baseline

Five interlocking statutory frameworks define executive accountability, reporting deadlines and compliance priorities across Portugal in 2026:

- **Cybersecurity Legal Regime (Decreto-Lei n.º 125/2025, in force 3 April 2026):** Transposes EU NIS2 across 17 sectors plus public administration and designates **Centro Nacional de Cibersegurança (CNCS)** as National Cybersecurity Authority [S5][S22]. Article 42 sets a **24-hour** early warning, a **72-hour** update and a **one-month** final report [S22]. Maximum administrative fines reach EUR 10 million or 2% of global turnover for essential entities, and EUR 7 million or 1.4% for important entities [S22].
- **CNCS Implementing Regulation (Regulamento n.º 756/2026, in force 23 June 2026):** Operationalises the **MyCiber** platform, setting self-identification and qualification rules with a 10-working-day prior hearing [S23] [S24]. Entities must designate a **Cybersecurity Officer** (Responsável de Cibersegurança) and **Permanent Point of Contact** (Ponto de Contacto Permanente) [S23]. Minimum measures align with **QNRCS**, with phased adaptation windows up to 24 months [S23][S24].
- **National DORA Execution (Lei n.º 73/2025) and Delegated Regulation (EU) 2025/301:** Allocates EU DORA supervision across **Banco de Portugal**, **CMVM** and **ASF** [S25]. Banco de Portugal serves as the single major ICT incident receipt hub for credit and payment institutions [S25]. Commission Delegated Regulation (EU) 2025/301 Article 5 sets strict major-incident notification windows [S27].
- **GDPR and National Data Protection Law (Lei n.º 58/2019, 8 August 2019):** Designates the **Comissão Nacional de Proteção de Dados (CNPD)** as Portugal's supervisory authority, enforcing the 72-hour personal-data breach notification clock [S26]. On **15 January 2026**, **CNPD** and **CNCS** signed a cooperation protocol establishing a 24/7 emergency channel, joint audit capability and a roadmap toward an interoperable single-entry reporting portal [S9]. Public reporting also noted CNPD staffing pressure: **472** breach proceedings opened in 2025 (**+42%** YoY) while only **two GDPR fines totalling EUR 47,000** were issued during the year [S9][S10][S11].
- **EU Cyber Resilience Act (Regulation (EU) 2024/2847):** Under Articles 14 and 71, mandatory manufacturer reporting for **actively exploited vulnerabilities** and **severe incidents** started on **11 September 2026** [S28]. Broader product-conformity duties apply from **11 December 2027** [S28].

10.2 Distinct Portuguese reporting clocks and recipients

One cyber incident routinely triggers multiple statutory notifications simultaneously. The operational summary below outlines principal Portuguese triggers and deadlines (general guidance, not legal advice):

Regime	Core trigger	Principal reporting sequence	Competent Portuguese recipient
Regime Jurídico da Cibersegurança (`DL 125/2025` , `Reg. 756/2026`)	Significant incident affecting an essential or important entity across 17 sectors or public administration	Early warning within **24 hours** of awareness; incident update within **72 hours** of awareness; intermediate report on request and final report within **1 month** (Article 42) [S22][S23]	**CNCS / CERT.PT** via **MyCiber** platform and designated sector authorities [S22][S23]
GDPR and `Lei n.º 58/2019`	Personal-data breach unless unlikely to result in a risk to individuals' rights and freedoms	Notify within **72 hours** of becoming aware where feasible; notify affected data subjects without undue delay when high risk is likely [S26]	**CNPD** (Comissão Nacional de Proteção de Dados) [S9] [S26]
DORA (`Lei 73/2025` , EU Reg. `2022/2554` , Del. Reg. `2025/301` Art. 5)	Major ICT-related incident at an in-scope financial entity	Initial notification within **4 hours** of major classification and no later than **24 hours** from detection; intermediate report within **72 hours** of initial notice; final report within **1 month** [S25][S27]	**Banco de Portugal** (single receipt hub for credit and payment institutions), **CMVM** or **ASF** [S25]
Cyber Resilience Act (EU Reg. `2024/2847` , Arts. 14 and 71)	Manufacturer awareness of an **actively exploited vulnerability** or **severe incident** in a digital product (applies from **11 September 2026**)	Early warning within **24 hours**; vulnerability or incident notification within **72 hours**; final report within **14 days** (vulnerabilities after fix) or **1 month** (severe incidents) [S28]	Coordinator CSIRT (**CERT.PT**) and **ENISA** simultaneously via CRA Single Reporting Platform [S28]
Criminal investigation	Suspected unauthorised access, ransomware, sabotage or computer fraud	Prompt criminal complaint preserving volatile forensic evidence and logs [S5][S29] [S39]	**Polícia Judiciária (UNC3T)** and **Ministério Público (Gabinete de Cibercrime)** [S5][S8][S29]

Under DORA Delegated Regulation 2025/301 Article 5, entities unable to meet a deadline must notify their authority before expiry with documented reasons [S27]. Weekend deferral does not exempt credit institutions, central counterparties, trading venues or NIS2 essential and important financial entities from initial or intermediate notices [S27].

10.3 Practical compliance lessons from 2026 Portuguese incidents

Three practical lessons stand out across Portugal's 20 confirmed 2026 disclosures. First, **multi-authority filing is now routine**. **Serpa**, **Santo Tirso**, **Metro Mondego**, **Universidade de Aveiro**, **Grupo Águas de Portugal** and **Worten** all notified **CNCS**, **CNPD** and **Polícia Judiciária** together, while **SMAS de Sintra** notified **CNPD** and **CNCS** [S45][S47][S50][S52][S53][S68][S72]. Second, **vendors do not remove controller duties**. Incidents at **Canvas** (`Case I`), **SIRP's web contractor** (`Case Q`) and **Intermarché's cooling supplier** (`Case S`) still required rapid Portuguese outreach and triage [S37][S58][S64]. Third, **unverified underground posts are not automatic notification triggers**: organisations should validate technical scope against live systems first while keeping dated decision logs.

KEY TAKEAWAYS

01

Portugal's NIS2 regime (DL 125/2025 and Reg. 756/2026), DORA (Lei 73/2025), GDPR (CNPD) and EU CRA run on separate legal clocks.

02

Complete MyCiber qualification, appoint a Cybersecurity Officer and Permanent Point of Contact, and verify backup reporting credentials now.

03

Unverified underground listings require forensic triage before triggering formal statutory notices.

CHAPTER 11

Outlook and conditional planning scenarios

11

THIS CHAPTER ANSWERS

Which concrete triggers should shift Portuguese defensive posture after 26 November 2026?

4

conditional planning scenarios grounded in owned evidence

11.1 Key judgements and evidential limits 77

11.2 Four conditional planning scenarios 78

11.3 What would change this assessment 79

CHAPTER 11

Outlook and conditional planning scenarios

IN SHORT

The 2026 Portuguese evidence justifies sustained readiness across four concrete fronts: municipal and healthcare ransomware resilience, bulk citizen-registry protection, exposed vendor-managed OT and multi-channel social engineering backed by leaked NIF and IBAN records. It does not establish a single coordinated actor behind Portugal's diverse incidents or predict attack probabilities. Link each conditional scenario below to pre-agreed technical isolation, legal notification and public communication playbooks.

11.1 Key judgements and evidential limits

Judgement	Basis and confidence	Key limit	Owned decision
Municipalities, universities and healthcare remain Portugal's sharpest operational ransomware exposure	High based on confirmed attacks (`Cases H, K, L, N, R`), low DMARC enforcement (`48%–56%`) and RASI 2025 baselines [S3][S5] [S43][S47][S51]	Several confirmed municipal encryption events never appeared on leak sites; sector maturity varies widely	Pool 24/7 municipal SOC monitoring via **FCSAL**, test offline restores and enforce DMARC
Bulk citizen-registry scraping and public web-form flaws drive severe secondary fraud exposure	High based on **SNS 24** (`>100,000`), **ANEPC RNBP** (`~60,000`), **Worten**, **SMAS de Sintra** and **Metro Mondego** [S39][S48][S62][S70] [S72]	Exposed populations overlap in unknown ways across distinct controllers and cannot be summed	Enforce query rate limits, phishing-resistant MFA and rapid web-form patching
External vendor IT and remote OT controllers create cross-border shockwaves inside Portugal	High based on **Intermarché** (7 stores), **Instructure Canvas** and **SIRP** contractor breaches [S37][S58][S64]	Third-party exposure depends on individual supplier remote-access hygiene	Remove vendor OT controllers from public internet and audit contractor test servers
Ransomware leak-site pressure accelerated sharply in H2 2026 (`83.3%` in Jun–Nov)	High for **36** Ransompedia listings across 17 labels (up 71.4% vs 21 in 2025) [S2]	**34 of 36** listings remain individually unverified; one Nova duplicate limits unique entries to at most 35	Verify every listing against internal forensic logs before negotiating or notifying

Judgement	Basis and confidence	Key limit	Owned decision
Payment-rail controls cut card fraud while social engineering and crypto scams expand	High based on **Banco de Portugal** (`-40.4%` H1 2025 losses; `EUR 6.5M` avoided) vs **PJ** (`EUR 14.7M` crypto fraud), **ANACOM** spoofing and underground SMS ads [S1][S5][S12][S13][S15]	Underground advertisements do not measure campaign conversion or bank-level losses	Pair SMS Sender ID defence and Android trojan telemetry with targeted customer alerts
External identity exposure across Portugal's 247 assessed domains requires separate staff and customer triage	High for **51/100** national headline, **83** current credential listings and **202** domains with employee devices [S4]	Cumulative signals do not prove 2026 intrusion or national prevalence; 3 of 250 domains remain unknown	Validate current credential listings within five working days and separate staff from customer queues

11.2 Four conditional planning scenarios

Scenario A: A municipal, university or healthcare network detects active encryption or portal defacement

If monitoring detects rapid file encryption (`Cases H, K, L, N, R`) or public CMS defacement (`Case U`), invoke pre-authorised network isolation immediately while keeping clinical care or critical municipal continuity on segmented fallback procedures. Preserve volatile memory and firewall logs for **Polícia Judiciária (UNC3T)** and notify **CNCS / CERT.PT** within 24 hours under **DL 125/2025** if in scope. Trigger municipal deadline-suspension orders where needed (`Case H`) and restore only from verified offline immutable backups.

Scenario B: Abnormal automated lookup velocity or web-form theft hits a citizen or customer database

If logs show high-volume queries from one clinician, staff or API account (`Case J`) or public web-form abuse (`Cases R, T`), revoke active tokens immediately. Lock down bulk export endpoints and scope exact exposed fields (`NIF` , `CC` , `IBAN`). File parallel **CNPD** (72h) and **CNCS** notices as required, and publish plain-language citizen alerts warning specifically against phishing, smishing and fake Multibanco references citing those fields.

Scenario C: An underground listing, combolist or Ransompedia entry names a Portuguese organisation

If monitoring flags a forum dataset (`Cases A, B, E`), initial-access post (`Case D`) or extortion entry (§7.1), validate sample schemas, registration timestamps and credentials against live production databases and historical breach archives first. Confirm whether historical data recycling (`Case B`), boilerplate template scraping (`Case A`) or unrelated end-user stealer logs explain the post before triggering crisis notices or customer password resets.

Scenario D: Vendor-managed OT controllers or international network links face sudden disruption

If facilities telemetry detects abnormal setpoint shifts on refrigeration, energy or building controllers (`Case S` ; §6.2), disconnect remote vendor links immediately. Shift to safe local manual overrides and alert **CNCS** and **PJ**. If volumetric DDoS degrades external connectivity (`Case P`), engage upstream carrier scrubbing and publish factual timestamped availability bulletins without speculating on cyber causes for uninvestigated infrastructure faults (§6.3).

11.3 What would change this assessment

Confirmed forensic attribution linking multiple 2026 Portuguese municipal or public-portal intrusions (`Cases H, K, R, U`) to a single shared access broker or vulnerability chain would warrant elevating coordinated cross-sector campaign warnings. Confirmation of active, unmitigated staff credentials among the **83 domains** carrying current credential listings, or exposure observations for the **3 currently unassessed domains**, would likewise refine sector triage. Conversely, broad **MyCiber** onboarding and migration of the **87 non-enforcing domains** to DMARC `quarantine` or `reject` would materially reduce impersonation risk. Enacting the caller-ID and SMS anti-spoofing rules proposed by **ANACOM** would further curb domestic fraud.

KEY TAKEAWAYS

01

Tie every strategic judgement to its evidential boundary so budgets target verified operational gaps.

02

Pre-authorise isolation, bulk-query lockouts, claim validation and vendor-OT manual fallbacks ahead of incidents.

03

Track MyCiber adoption, DMARC enforcement and ANACOM anti-spoofing rules as primary indicators of national progress.

CHAPTER 12

Action plan and completion evidence

12

THIS CHAPTER ANSWERS

Who acts, on which trigger, and what shows each control works in practice?

30 / 60 / 90

assurance milestones; urgent edge patching and active credential triage start today

12.1 Priority action lanes and completion evidence 81

12.2 Vulnerability remediation reference 83

12.3 Supporting continuous external validation 84

CHAPTER 12

Action plan and completion evidence

IN SHORT

Urgent patching of exposed edge appliances and PHP web portals, removal of internet-facing vendor OT controllers and validation of active credential listings begin immediately. Use the 30, 60 and 90-day milestones below to assign named technical and executive owners across Portuguese organisations, requiring verifiable operational test evidence rather than paper policies before marking work complete.

12.1 Priority action lanes and completion evidence

1**Immediate (0–7 days)**

Inventory all internet-facing gateways, remote-support appliances, PHP/CMS public portals and third-party OT/refrigeration controllers; apply current fixed builds in §12.2, cut direct internet access to vendor OT controllers and pre-authorise rapid DMZ isolation

OWNER

Infrastructure, OT engineering and CISO

COMPLETION EVIDENCE

Signed external-asset register, patch verification logs and approved emergency isolation playbook

Validate any current credential listing (affecting **83 of 247** assessed domains) within five working days; audit Microsoft 365 and cloud-identity tenants (`126 of 250` portfolio domains) for **Tycoon 2FA**-style adversary-in-the-middle sessions, anomalous forwarding rules and OAuth consents

OWNER

Identity and SOC leads

COMPLETION EVIDENCE

Dated listing-triage register, revoked session logs and Conditional Access / MFA enforcement export

2**30 days**

Reconcile employee-classified device associations (**202** assessed domains, **38,013** devices) against managed endpoint inventories to isolate infected staff machines while keeping non-employee records routed to customer fraud queues

OWNER

Endpoint security and fraud operations

COMPLETION EVIDENCE

Reconciled endpoint-triage ledger with dated device containment or documented closure

Move non-enforcing domains (**87 of 250**; led by municipalities, universities and health) to full-coverage DMARC `quarantine` or `reject`, remediate the **20** apex TLS validation faults and publish HSTS across remaining public portals

OWNER

Messaging and domain security

COMPLETION EVIDENCE

Live DNS DMARC verification report and clean external TLS/HSTS scan across owned domains

Complete **MyCiber** self-identification and qualification under **Regulamento n.º 756/2026**, formally designate the **Cybersecurity Officer** and **Permanent Point of Contact**, and verify parallel reporting access for **CNCS**, **CNPD**, **Banco de Portugal / CMVM / ASF** (if DORA-scoped) and **PJ UNC3T**

OWNER

Legal, compliance and CISO

COMPLETION EVIDENCE

Dated MyCiber confirmation, named officer appointments and tested portal login roster

3**60 days**

Implement per-account lookup velocity caps, anomalous-export alerts and phishing-resistant MFA on national, municipal and healthcare citizen registries (`Cases J, R`); audit public web forms for `NIF` / `IBAN` minimisation and eliminate live citizen data on vendor development/test servers (`Cases Q, T`)

OWNER

Application engineering, DPO and vendor risk

COMPLETION EVIDENCE

Query-throttling test log, web-form security review and signed contractor test-server audit

For financial and consumer platforms, coordinate carrier SMS spoofing controls with **ANACOM** guidance, monitor for Android Accessibility abuse targeting **Chave Móvel Digital** (`Massiv` / `ToxicPanda`) and tighten liveness and mule-inflow controls on newly opened domestic accounts

OWNER

Fraud operations and digital channels

COMPLETION EVIDENCE

Signed anti-fraud control test report and carrier/mobile-detection telemetry review

4**90 days**

Run a joint continuity and restoration tabletop plus bare-metal offline backup recovery test (aligned with **DL 125/2025**, **DORA** or municipal **CIBER 26** models), covering IT/OT isolation, statutory municipal deadline suspension and calm telemetry-based status bulletins

OWNER

Executive sponsor, continuity lead and CISO

COMPLETION EVIDENCE

Dated exercise after-action report, measured recovery time objectives and signed residual-risk register

12.2 Vulnerability remediation reference

The table below lists affected and fixed versions verified from **NIST NVD** and **CVE CNA** records on **27 November 2026**. It covers edge appliances, PHP web runtimes and CERT.PT's top exploited platforms relevant to Portugal. Later cumulative security releases supersede earlier minimum patch builds on supported branches:

Product and CVEs	Affected versions (NVD / CNA)	Fixed versions and defensive action	Sources
BeyondTrust Remote Support / PRA (`CVE-2026-1731` CVSS 3.1 `9.8` ; `CVE-2026-102764` CVSS 3.1 `9.8`)	`CVE-2026-1731` : Remote Support (`RS`) `⩽ 25.3.1` and Privileged Remote Access (`PRA`) `⩽ 24.3.4` . `CVE-2026-102764` : Remote Support `⩽ 26.2.3` .	Upgrade **Remote Support** past `26.2.3` (covering both February pre-auth RCE and October origin-validation fixes) and **PRA** past `24.3.4` ; inspect exposed support appliances for pre-patch persistence and rotate service credentials.	[S86][S88]
Citrix NetScaler ADC and Gateway (`CVE-2026-88771` CVSS 3.1 `9.8` ; `CVE-2026-88772` CVSS 3.1 `8.1` ; superseded by `CVE-2026-120868` CVSS 4.0 `9.3`)	September builds: `14.1` before `14.1-73.37` , `13.1` before `13.1-64.23` , `14.1` FIPS before `14.1-73.37` FIPS, `13.1` FIPS/NDcPP before `13.1-37.279` . November (`CVE-2026-120868`): `14.1` before `14.1-73.57` , `13.1` before `13.1-64.39` , `14.1` FIPS before `14.1-73.58` FIPS, `13.1` FIPS/NDcPP before `13.1-37.293` .	Upgrade directly to `14.1-73.57` , `13.1-64.39` , `14.1-73.58` FIPS or `13.1-37.293` FIPS/NDcPP (or later supported builds); migrate End-of-Life appliances, hunt for pre-patch shells and rotate active session secrets.	[S87][S91]
Ivanti Connect Secure (`CVE-2026-104935` CVSS 3.1 `8.6`)	ICS `22.8R2` to `22.8R2.4` and `25.1.x` releases before `25.1.3.0` ; `22.8R2.5` , `22.7R2.14` and earlier are not affected.	Upgrade exposed `ICS` appliances to `25.1.3.0` (or later `25.1.3` builds) or `22.8R2.5` (or later supported releases); verify VPN MFA and audit logs for spoofing.	[S89]

Product and CVEs	Affected versions (NVD / CNA)	Fixed versions and defensive action	Sources
PHP Web Runtime (`CVE-2026-109618` CVSS 3.1 `9.8` ; `CVE-2026-109619` CVSS 3.1 `8.1` ; superseded by 19 Nov `CVE-2026-115560` and `CVE-2026-129289` CVSS 4.0 `9.2`)	October flaws: `8.2` before `8.2.35` , `8.3` before `8.3.36` , `8.4` before `8.4.27` , `8.5` before `8.5.12` (plus EOL branches). November flaws (`CVE-2026-115560` session-serializer RCE; `CVE-2026-129289` PHP-FPM request smuggling): `8.2` before `8.2.36` , `8.3` before `8.3.37` , `8.4` before `8.4.28` , `8.5` before `8.5.13` .	Upgrade directly to `8.5.13` , `8.4.28` , `8.3.37` or `8.2.36` (or supported OS/LTS backports); migrate EOL `8.1` and older (note `8.2` reaches EOL on 31 December 2026). Set `session.upload_progress.enabled=0` in server/FPM configuration and align session serializers across shared stores.	[S90][S92]
Microsoft SharePoint Server and DNN CMS (`CVE-2025-53770` CVSS 3.1 `9.8` ; `CVE-2025-64095` NVD Primary CVSS 3.1 `9.8` / CNA `10.0`)	On-premises Microsoft SharePoint Server vulnerable to deserialisation RCE (`CVE-2025-53770`); DNN CMS prior to `10.1.1` (`CVE-2025-64095`). Both highlighted by **CERT.PT** in **RASI 2025** among Portugal's top exploited vulnerabilities.	Verify cumulative Microsoft SharePoint security updates and machine-key rotation for `CVE-2025-53770` ; upgrade DNN CMS installations to `10.1.1` or later and audit public web directories for unauthorised uploads.	[S5][S93]

12.3 Supporting continuous external validation

Organisations seeking tailored visibility into Portuguese domain exposure, stealer-credential alerts, similar domain names and underground brand claims can request a Brandefense briefing at Brandefense demo request [S94].

KEY TAKEAWAYS

01

Patch exposed edge gateways and PHP portals, isolate vendor OT controllers and validate current credential listings immediately.

02

Complete MyCiber qualification and close the 87-domain non-enforcing DMARC gap within 30 days.

03

Require dated recovery, query-throttling and continuity test evidence to mark milestones complete.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Method, scope and exclusions · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

94

sources

Appendix A. Method, scope and exclusions 86
Appendix B. Evidence register 89
Appendix C. Sources 90
Appendix D. Glossary 96

Appendix A. Method, scope and exclusions

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Observation windows and evidence separation

Distinct reference dates apply across this report and are never blurred. The **2026 activity window** runs from **1 January to 26 November 2026** (UTC, by publication timestamp) for underground observations, Ransompedia listings, 2026 domain mentions and public incidents [S1][S2][S4]. Inside that window, **12 to 26 November 2026** is examined separately in §5.3 and does not imply a longer surveillance period [S1][S2]. Rolling 365-day dark-chat and dark-web domain mentions span **27 November 2025 to 26 November 2026**, reported separately from the 2026 subset [S4].

Brandefense Atlas exposure observations (**247 of 250** selected domains) and passive domain configuration observations (**all 250** domains) reflect a **27 November 2026** snapshot [S3][S4]. All external public advisories, statutes, official PDFs, NVD records and press sources were verified on **27 November 2026**. Every source supports only its own proposition.

A.2 Underground post volume and corpus boundary

The observed Portugal-tagged underground population totals **744,809 posts** across the 1 January to 26 November 2026 window [S1]. January (`411,861`) and February (`316,130`) together account for **727,991 posts (97.7%)**, driven by repetitive multi-country Telegram promotional traffic tagged Turkish (`723,945` in Jan–Feb; `724,031` across the full window) [S1].

March through November totals **16,818 posts** (`16,716` Telegram, `82` forum, `14` paste, `6` Discord) [S1]. The recent **12 to 26 November** window holds **715** Portugal-tagged posts and **25** forum posts mentioning Portugal across tagged and untagged threads [S1]. Detailed excerpts (`B01` – `B15`) derive from a narrower retained corpus and do not represent a complete census of everything published online. November is partial through 26 November.

A.3 Selected 250-domain portfolio and passive configuration snapshot

The passive portfolio comprises **250 DNS-resolving Portuguese domains** distributed evenly across ten sector cells of **25 domains** each, snapshotted on **27 November 2026** [S3]. Selection is purposive across major public and private Portuguese institutions and is not a statistical census of all `.pt` domains. Email authentication figures reflect published policy categories (`reject` , `quarantine` , `none` , missing) rather than verified receiver behaviour (`RFC 7489`) [S3][S82]. TLS (`217/237` valid) and HSTS (`164/212` present) preserve their reachable denominators; unreachable apex endpoints (`13` TLS, `38` HTTP) are counted separately rather than treated as failures [S3].

A.4 Selected-domain exposure assessments and mentions

Brandefense Atlas exposure observations cover **247 of the 250 selected domains** on the **27 November 2026** snapshot [S4]. Exposure remains **unknown** for **3 selected domains** (1 in Energy and utilities, 1 in Industry and manufacturing, 1 in Transport, maritime and logistics); unassessed domains are never treated as zero [S4]. Only the single national Atlas headline (**51/100**) is published; no per-sector, per-group or organisation scores, medians or grade distributions appear anywhere in this report.

Portfolio signals include **83** domains with current credential listings (**2,621** historical listings) and at least **523,733** cumulative device associations (**38,013** employee across **202** domains) [S4]. Assessed domains also hold **13,777,936** historical credentials (**238** domains), **801** documents (**137** domains) and **40,060** 30-day similar names (**191** domains) [S4]. Signals may overlap across domains and individuals and do not represent unique people, 2026-only activity or confirmed breaches [S4]. The strict **15-domain** card-issuing bank subset in §9.1 retains its smaller denominator inside the 25-domain Banking and finance cell [S4].

A.5 Ransomware listings

The **36 Portugal-labelled listings** recorded in Ransompedia through **26 November 2026** (versus **21** in full-year 2025 and **104** all-time) measure criminal leak-site claims rather than verified breaches or unique victims [S2]. One same-day duplicate under `Nova` (24 June) bounds distinct claimed entities to **at most 35** [S2]. Two listings match confirmed public disclosures (`Cases L and M`), while **34 remain unverified** with identities withheld. Comparator prior-year totals span full-year 2025 whereas 2026 covers through 26 November [S2].

A.6 Payment-card scope

SCOPE OF THE CARD FIGURES

These figures describe a limited observed publication population in retained underground posts. They do not estimate Portuguese payment-card theft, national card-fraud losses or live card validity.

Retained underground posts contained **155 Portugal-issuer card occurrences** covering **132 distinct masked cards** (`114` posts, `51` six-digit BINs, `6` named issuers withheld) [S1]. Separately, **1,776 offer posts** lacked clear-text card lines, including **1,433** multi-country shop batch listings (median **USD 10–25**) [S1]. Neither figure verifies card issuance, stolen status, active balance or bank infrastructure compromise [S1].

A.7 Public incidents, exclusions and naming discipline

Fourteen public-incident dossiers (`Cases H-U`) document **20 officially confirmed and widely reported 2026 Portuguese incidents**, alongside seven underground claim cases (`Cases A-G`). Four categories were explicitly excluded from 2026 confirmed incident counts:

1. **28 April 2025 Iberian power outage:** Excluded as a 2025 grid outage attributed to technical voltage-control factors in the March 2026 ENTSO-E report validated by ACER, with no cyber cause identified [S16][S17].
2. **Historical 2023 municipal and utility cyberattacks:** Prior-year incidents (including 2023 attacks on municipal and local utility networks) fall outside the 2026 window.
3. **Unconfirmed claims and unverified local reports:** Unverified Ransompedia listings (`34 of 36`), unverified Telegram hacktivist claims (`313 Team` , `Z-Pentest Alliance` , `BNCT`) and single-outlet local reports lacking official institutional confirmation are excluded from confirmed victim naming.
4. **Routine non-attack IT outages:** Confirmed non-cyber technical outages, such as Universidade de Aveiro's September routine-update network fault [S52] and operational IT failures tracked separately by Cibersegurança.PT [S79].

An organisation is named only when **both** officially confirmed and widely reported (`public_names.json`). No individual person (including the clinician involved in `Case J`), no unconfirmed external contractor (`Case Q`) and no withheld victim domain appears anywhere in this package.

Appendix B. Evidence register

Redacted authentic excerpts from Brandefense's retained Portugal underground corpus appear inline in the chapters listed below (`B01` – `B15`). Dates reflect UTC publication timestamps; no post establishes a confirmed breach or completed transaction on its own.

Card	Date (UTC)	Venue	Alias	Language	Section
B01	2026-01-04	Forum thread	Alias withheld	English	§4.2
B02	2026-04-03	Forum thread	Alias withheld	English	§4.2
B03	2026-09-13	Forum thread	Alias withheld	English	§4.2
B04	2026-04-30	Forum thread	Alias withheld	English	§4.3
B05	2026-05-01	Telegram channel relay	Alias withheld	English	§4.3
B06	2026-06-02	Telegram channel	Alias withheld	English	§4.3
B07	2026-03-31	Forum thread	Alias withheld	Russian / English	§4.4
B08	2026-06-30	Forum thread	Alias withheld	Russian	§4.4
B09	2026-04-05	Forum thread	Alias withheld	English	§4.4
B10	2026-11-17	Telegram channel	Alias withheld	Portuguese	§4.4
B11	2026-11-14	Forum thread	Alias withheld	English	§4.3
B12	2026-11-21	Forum thread	Alias withheld	English	§4.4
B13	2026-11-23	Forum thread	Alias withheld	English	§4.2
B14	2026-11-23	Forum thread	Alias withheld	English	§4.3
B15	2026-11-23	Forum thread	Alias withheld	English	§4.4

Appendix C. Sources

S1: Odin by Brandefense. Retained underground observations and publication counts (1 Jan-26 Nov 2026; recent 12-26 Nov 2026). URL withheld (own data). Verified on 2026-11-27.

S2: Ransompedia. Country-labelled ransomware listings (1 Jan-26 Nov 2026 and full-year 2025). URL withheld (own data). Verified on 2026-11-27.

S3: Odin by Brandefense. Configuration snapshot of 250 selected Portuguese domains (27 Nov 2026). URL withheld (own data). Verified on 2026-11-27.

S4: Brandefense Atlas and Odin by Brandefense. Exposure observations for 247 assessed Portuguese domains (27 Nov 2026) and rolling 365-day dark-chat/dark-web mentions across 250 domains (27 Nov 2025 to 26 Nov 2026; 2026 subset 1 Jan to 26 Nov 2026). URL withheld (own data). Verified on 2026-11-27.

S5: Governo de Portugal / Sistema de Segurança Interna. Relatório Anual de Segurança Interna (RASI) 2025 (including CNCS/CERT.PT, DGPJ, PJ and SIS chapters). https://portugal.gov.pt/api/media/edge/Project/Portal-do-Governo/Portal-do-Governo/gc25/Files/Documentos/rasi-2025-relatorio-anual-de-seguranca-interna/rasi_2025_-_relatorio_anual_de_seguranca_interna.pdf Verified on 2026-11-27.

S6: Diário de Notícias da Madeira / Lusa. CNCS Riscos & Conflitos 6th edition: CERT.PT recorded 2,758 validated incidents in 2024 (+36%). https://www.dnoticias.pt/2025/9/16/463051-incidentes-de-ciberseguranca-registados-em-2024-sobem-36-para-2758/ Verified on 2026-11-27.

S7: Pplware. CNCS Riscos & Conflitos 6th edition summary (2024 baseline and emerging risks). https://pplware.sapo.pt/internet/cncs-portugal-registou-aumento-de-incidentes-ciberneticos/ Verified on 2026-11-27.

S8: Ministério Público - Gabinete de Cibercrime. Cibercrime em 2025: denúncias recebidas por correio eletrónico (+13.16% YoY). https://cibercrime.ministeriopublico.pt/destaque/cibercrime-em-2025-denuncias-recebidas Verified on 2026-11-27.

S9: Comissão Nacional de Proteção de Dados (CNPD). CNPD and CNCS sign cooperation protocol (15 January 2026) and 2025 breach case statistics (472 cases, +42%). https://www.cnpd.pt/comunicacao-publica/noticias/comissao-nacional-de-protecao-de-dados-e-centro-nacional-de-ciberseguranca-assinam-protocolo-de-cooperacao/ Verified on 2026-11-27.

S10: Observador / Lusa. Personal-data breach proceedings at CNPD rose 42% in 2025 to 472 (16 January 2026). https://observador.pt/2026/01/16/processos-por-violacao-de-dados-pessoais-aumentaram-42-em-2025/ Verified on 2026-11-27.

S11: Observador. Staffing constraints slow CNPD GDPR fines: two fines totalling EUR 47,000 in 2025 (17 May 2026). https://observador.pt/2026/05/17/falta-de-pessoal-trava-aplicacao-de-coimas-por-violacao-de-dados-pessoais/ Verified on 2026-11-27.

S12: Dinheiro Vivo / Diário de Notícias / Lusa. Banco de Portugal 2025 Payment Systems Report: H1 2025 payment fraud losses fell 40.4% to EUR 5.3M; 51 severe DORA incidents (21 May 2026). https://dinheirovivo.dn.pt/economia/perdas-em-fraudes-com-pagamentos-recuam-para-53-milhes-no-1-semestre-de-2025 Verified on 2026-11-27.

S13: Observador / Lusa. Banco de Portugal beneficiary-confirmation and SPIN tools avoided EUR 6.5M in fraud; launch of Digital Fraud Monitoring Platform (25 May 2026). https://observador.pt/2026/05/25/ferramentas-do-banco-de-portugal-ja-evitaram-65-milhoes-de-euros-em-fraudes-desde-maio-de-2024/ Verified on 2026-11-27.

S14: CCSL Advogados. Overview of Banco de Portugal Plataforma de Acompanhamento da Fraude Digital (26 May 2026). https://ccsllegal.com/2026/05/26/banco-de-portugal-lanca-plataforma-de-acompanhamento-da-fraude-digital/?lang=pt-pt Verified on 2026-11-27.

S15: CNN Portugal / Lusa. ANACOM reports caller-ID and SMS spoofing complaints more than doubled in 2025 to mid-July compared with full-year 2024 and proposes legal amendment. https://cnnportugal.iol.pt/telefones/fraude/fraudes-com-numeros-de-telefone-mais-do-que-duplicam-em-2025-e-anacom-quer-nova-lei/20250720/687ca1f7d34e3f0baea0b5ed Verified on 2026-11-27.

S16: ERSE - Entidade Reguladora dos Serviços Energéticos. ERSE Explica: ENTSO-E Expert Panel Factual Report on the 28 April 2025 Iberian power outage. https://www.erse.pt/media/owjmzbx3/erseexplica_relat%C3%B3rio-factual-vf.pdf Verified on 2026-11-27.

S17: Governo de Portugal. ENTSO-E technical report validated by ACER on the 28 April 2025 Iberian power outage (20 March 2026). https://portugal.gov.pt/gc25/comunicacao/noticias/apagao-eletrico-relatorio-iliba-portugal-de-responsabilidades Verified on 2026-11-27.

S18: RTP. Comissão Nacional de Eleições launches disinformation reporting channel ahead of 2026 presidential election. https://www.rtp.pt/noticias/pais/cne-cria-canal-de-denuncia-para-combater-fake-news-a-desinformacao-nao-vota-mas-influencia_n1708395 Verified on 2026-11-27.

S19: ERC - Entidade Reguladora para a Comunicação Social. ERC and LabCom-UBI publish study on social-media disinformation during the 2026 Presidential Election. https://www.erc.pt/pt/a-erc/noticias/erc-e-labcom-ubi-publicam-estudo-sobre-desinformacao-nas-redes-sociais-durante-as-presidenciais-2026/ Verified on 2026-11-27.

S20: DataReportal. Digital 2026: Portugal (9.26M internet users, 89.0% penetration at end of 2025; 10.4M population in October 2025). https://datareportal.com/reports/digital-2026-portugal Verified on 2026-11-27.

S21: ECO. Valongo municipal cybersecurity and emergency response exercise CIBER 26 (28 September 2026). https://eco.sapo.pt/2026/09/28/valongo-testa-resposta-a-ciberataque-com-impacto-na-agua-energia-e-escolas/ Verified on 2026-11-27.

S22: Procuradoria-Geral Distrital de Lisboa (PGDL). Decreto-Lei n.º 125/2025, de 4 de dezembro - Regime Jurídico da Cibersegurança (NIS2 transposition, in force 3 April 2026). https://www.pgdlisboa.pt/leis/lei_mostra_estrutura.php?tabela=leis&artigo_id=&nid=3985&nversao=&tabela=leis&so_miolo=S Verified on 2026-11-27.

S23: Diário da República (CNCS). Regulamento n.º 756/2026, de 22 de junho - Implementing regulation of the Cybersecurity Legal Regime and MyCiber platform. https://files.diariodarepublica.pt/2s/2026/06/118000000/0003200120.pdf Verified on 2026-11-27.

S24: Abreu Advogados. Legal briefing on CNCS Regulation n.º 756/2026 and MyCiber entity qualification procedures. https://abreuadvogados.com/conhecimento/publicacoes/regulamento-de-execucao-do-regime-juridico-da-ciberseguranca/ Verified on 2026-11-27.

S25: Procuradoria-Geral Distrital de Lisboa (PGDL) / Abreu Advogados. Lei n.º 73/2025, de 23 de dezembro - National execution of EU DORA designating Banco de Portugal, CMVM and ASF. https://abreuadvogados.com/conhecimento/publicacoes/implementacao-do-regulamento-dora/ Verified on 2026-11-27.

S26: Diário da República. Lei n.º 58/2019, de 8 de agosto - National execution of the GDPR in Portugal. https://files.dre.pt/1s/2019/08/15100/0000300040.pdf Verified on 2026-11-27.

S27: Official Journal of the European Union (Publications Office). Commission Delegated Regulation (EU) 2025/301 - DORA major ICT incident notification time limits (Article 5). https://publications.europa.eu/resource/cellar/36795cde-ef2b-11ef-981b-01aa75ed71a1.0006.03/DOC_1 Verified on 2026-11-27.

S28: Official Journal of the European Union (Publications Office). Regulation (EU) 2024/2847 - Cyber Resilience Act (CRA). https://publications.europa.eu/resource/cellar/21b7d4eb-a6e2-11ef-85f0-01aa75ed71a1.0006.03/DOC_1 Verified on 2026-11-27.

S29: Observador / Lusa. Polícia Judiciária arrests two suspects in Europol LeakBase takedown and participates in Tycoon 2FA disruption affecting over 160 Portuguese organisations (4 March 2026). https://observador.pt/2026/03/04/pj-detem-dois-suspeitos-em-operacao-da-europol-que-desmantela-leakbase-um-dos-maiores-foruns-de-cibercrime-do-mundo/ Verified on 2026-11-27.

S30: Correio da Manhã / Lusa. Polícia Judiciária UNC3T Operation Cryptoclaim recovers ~EUR 500,000 in stolen digital assets. https://www.cmjornal.pt/portugal/detalhe/pj-recupera-e-devolve-meio-milhao-de-euros-a-vitima-de-burla-informatica Verified on 2026-11-27.

S31: Observador / Lusa. Polícia Judiciária UNC3T arrests two suspects over fraudulent use of French payment cards in Portugal (17 November 2026). https://observador.pt/2026/11/17/dois-estrangeiros-detidos-pela-pj-por-abuso-de-cartao-bancario-e-fraude-informatica/ Verified on 2026-11-27.

S32: The Portugal News / Lusa. Polícia Judiciária participates in Europol Operation PowerOFF against DDoS-for-hire services, securing 59 removals (23 November 2026). https://www.theportugalnews.com/pt/noticias/2026-11-23/policia-portuguesa-participa-em-operacao-internacional-contra-ciberataques/1008950 Verified on 2026-11-27.

S33: Eurojust. International operation disrupts NoName057(16) hacktivist DDoS infrastructure (16 July 2025). https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down Verified on 2026-11-27.

S34: CNN Portugal / Lusa. Câmara Municipal da Guarda digital services blocked after complex cyber incident on 12 February 2026 (20 February 2026). https://cnnportugal.iol.pt/camara-da-guarda/ataque-informatico/camara-da-guarda-ha-uma-semana-com-varios-servicos-bloqueados-apos-incidente-cibernetico-complexo/20260220/6998d02bd34e6a48f446cb32 Verified on 2026-11-27.

S35: Correio da Manhã / Lusa. Câmara Municipal da Guarda confirms preventive unavailability of platforms and PJ notification after 12 February cyberattack. https://www.cmjornal.pt/politica/detalhe/camara-da-guarda-continua-sem-acesso-a-plataformas-servicos-digitais-apos-ciberataque-de-12-de-fevereiro Verified on 2026-11-27.

S36: Jornal o Interior. Câmara Municipal da Guarda suspends administrative deadlines retroactive to 12 February cyberattack. https://www.ointerior.pt/sociedade/camara-da-guarda-suspende-prazos-administrativos-devido-a-ataque-informatico/ Verified on 2026-11-27.

S37: SOL. Global Instructure Canvas breach affects Portuguese higher-education students and triggers CNPD notifications (8 May 2026). https://sol.iol.pt/sociedade/noticias/ataque-cibernetico-mundial-a-plataforma-canva-ha-estudantes-portugueses-afetados/20260508/69fdeef30cf2d0ed34b84128 Verified on 2026-11-27.

S38: Pplware. Instructure confirms early-May Canvas security incident affecting Portuguese university users. https://pplware.sapo.pt/internet/tem-conta-no-canvas-a-sua-conta-esta-em-risco/ Verified on 2026-11-27.

S39: ECO / Lusa. Polícia Judiciária UNC3T reports unauthorised access to SNS patient records reached over 100,000 victims nationwide (25 May 2026). https://eco.sapo.pt/2026/05/25/acesso-indevido-a-dados-do-sns-atinge-mais-de-100-000-vitimas-de-todo-o-pais/ Verified on 2026-11-27.

S40: Observador / Lusa. CNCS, SPMS and PJ conduct joint forensic investigation into SNS 24 data-access incident notified on 21 May (1 June 2026). https://observador.pt/2026/06/01/centro-de-ciberseguranca-continua-a-realizar-acoes-forenses-sobre-ataque-ao-sistema-nacional-de-saude-com-policia-judiciaria/ Verified on 2026-11-27.

S41: RTP. PJ investigates unauthorised access to administrative SNS patient records via stolen medical credentials; health regulator ERS statement. https://www.rtp.pt/noticias/pais/pj-investiga-acesso-indevido-a-dados-de-centenas-de-utentes_n1742852 Verified on 2026-11-27.

S42: ERS - Entidade Reguladora da Saúde. Official ERS statement on unauthorised accesses to health information via SNS 24. https://www.ers.pt/pt/comunicacao/destaques/lista-de-destaques/comunicado-ers-alegados-acessos-indevidos-a-informacao-de-saude-atraves-de-consulta-ao-portal-sns-24/ Verified on 2026-11-27.

S43: Rádio Pax. Câmara Municipal de Serpa confirms 27 May 2026 cyberattack encrypting files and triggering server rebuild. https://www.radiopax.com/ataque-informatico-paralisou-servicos-da-camara-de-serpa-e-levanta-preocupacoes-de-seguranca/ Verified on 2026-11-27.

S44: Correio Alentejo. Câmara Municipal de Serpa confirms external cyberattack reported to authorities and investigated by PJ (28 May 2026). https://correioalentejo.com/ataque-a-infraestrutura-informatica-da-camara-de-serpa/ Verified on 2026-11-27.

S45: Rádio Voz da Planície. Câmara Municipal de Serpa confirms notification to CNCS, Ministério Público, CNPD and PJ. https://www.vozdaplanicie.pt/index.php/noticias/camara-municipal-de-serpa-alvo-de-ataque-informatico Verified on 2026-11-27.

S46: Observador / Lusa. Santa Casa da Misericórdia de Santo Tirso confirms June 2026 cyberattack disrupting outpatient medical units (9 June 2026). https://observador.pt/2026/06/09/santa-casa-da-misericordia-de-santo-tirso-alvo-de-ciberataque-no-fim-de-semana/ Verified on 2026-11-27.

S47: TugaTech. Santa Casa da Misericórdia de Santo Tirso reports notifications to CNCS, CNPD and PJ following 8 June intrusion and Qilin listing. https://tugatech.com.pt/t85651-ataque-informatico-expoe-dados-da-misericordia-de-santo-tirso-na-dark-web Verified on 2026-11-27.

S48: RTP / Lusa. Metro Mondego alerts personalised transit-pass holders of probable personal-data copy in 6 July ransomware attack. https://www.rtp.pt/noticias/economia/dados-pessoais-poderao-ter-sido-copiados-durante-ataque-informatico-a-metro-mondego_n1755936 Verified on 2026-11-27.

S49: Observador / Lusa. Metro Mondego confirms ransomware on internal systems while transport operations and card terminals remained isolated (26 July 2026). https://observador.pt/2026/07/26/dados-pessoais-poderao-ter-sido-copiados-durante-ataque-informatico-a-metro-mondego/ Verified on 2026-11-27.

S50: Diário de Notícias / Lusa. Metro Mondego confirms CNCS, CNPD and criminal-investigation notifications following 6 July ransomware. https://www.dn.pt/sociedade/metro-mondego-alerta-que-dados-pessoais-podero-ter-sido-copiados-durante-ataque-informtico Verified on 2026-11-27.

S51: RTP / Lusa. CNCS/CERT.PT confirms notification on 20 July of Universidade de Aveiro ransomware with email and database exfiltration. https://www.rtp.pt/noticias/economia/equipa-de-resposta-a-incidentes-de-ciberseguranca-notificada-a-20-julho-de-ocorrencia-na-universidade-de-aveiro_n1756821 Verified on 2026-11-27.

S52: Rádio Ria / Lusa. Universidade de Aveiro confirms collaboration with CNCS, CNPD, PJ and SIS and separates September update outage from July ransomware. https://radioria.pt/noticias/universidade/ua-afasta-ligacao-entre-falhas-na-rede-sentidas-em-setembro-e-ciberataque-de-julho Verified on 2026-11-27.

S53: ECO. Grupo Águas de Portugal confirms high-complexity cyberattack on administrative IT systems; water supply unaffected (4 August 2026). https://eco.sapo.pt/2026/08/04/aguas-de-portugal-alvo-de-ciberataque-fornecimento-e-qualidade-da-agua-nao-esta-em-causa/ Verified on 2026-11-27.

S54: Observador / Lusa. Environment Minister confirms Grupo Águas de Portugal attack remained contained to administrative systems (7 August 2026). https://observador.pt/2026/08/07/ciberataque-ao-grupo-aguas-de-portugal-nao-afetou-fornecimento-de-agua-diz-ministra-do-ambiente/ Verified on 2026-11-27.

S55: Observador. MEO confirms mass attack degrading international network links without system intrusion or customer data access (14 September 2026). https://observador.pt/2026/09/14/meo-foi-alvo-de-ataque-em-massa-que-afetou-servicos-de-telecomunicacoes/ Verified on 2026-11-27.

S56: ECO / Lusa. MEO technical analysis confirms distributed denial-of-service (DDoS) waves across 14-15 September 2026 (15 September 2026). https://eco.sapo.pt/2026/09/15/incidentes-na-meo-foram-provocados-por-ataque-de-negacao-de-servico/ Verified on 2026-11-27.

S57: ECO. MEO reports 6,020,686 blocked attack attempts during the first two days of Web Summit 2026 in Lisbon (10 November 2026). https://eco.sapo.pt/2026/11/10/web-summit-foi-alvo-de-seis-milhoes-de-tentativas-de-ciberataque-em-dois-dias/ Verified on 2026-11-27.

S58: RTP / Lusa. SIRP confirms external web-contractor development server breach exposed non-classified data from public websites; no operational or classified systems affected. https://www.rtp.pt/noticias/pais/ciberataque-expoe-na-internet-dados-nao-classificados-das-secretas-portuguesas_n1770309 Verified on 2026-11-27.

S59: Diário de Notícias / Lusa. SIRP confirms 8 October 2026 clarification and report to Procuradoria-Geral da República following 120 GB forum listing. https://www.dn.pt/sociedade/ciberataque-expe-na-internet-dados-no-classificados-das-secretas-portuguesas Verified on 2026-11-27.

S60: Rádio Nova. Câmara Municipal de Ovar confirms October 2026 cyberattack suspending municipal services. https://www.radionova.fm/atualidade/camara-de-ovar-foi-alvo-de-ataque-informatico-e-tera-servicos-encerrados-ate-quarta-feira/ Verified on 2026-11-27.

S61: Notícias de Ovar. Reporting on Câmara Municipal de Ovar October 2026 cyberattack recovery and cybersecurity measures. https://noticiasdeovar.pt/news/o-ataque-informatico-a-camara-de-ovar-e-os-investimentos-feitos-na-area/ Verified on 2026-11-27.

S62: Observador / Lusa. ANEPC confirms cyberattack copying personal records from the 60,000-entry National Firefighters Registry (RNBP) and immediate suspension with CNCS and RNSI (24 October 2026). https://observador.pt/2026/10/24/piratas-informaticos-atacam-base-de-dados-dos-bombeiros-e-acedem-a-dados-pessoais/ Verified on 2026-11-27.

S63: Diário de Notícias / Lusa. ANEPC and Liga dos Bombeiros Portugueses confirm RNBP data copy excluding banking records and issue phishing/smishing/quishing warnings. https://www.dn.pt/sociedade/base-de-dados-dos-bombeiros-foi-alvo-de-ciberataque-comprometendo-dados-pessoais Verified on 2026-11-27.

S64: RTP. Grupo Mosqueteiros confirms seven Intermarché stores in Portugal affected by European refrigeration-controller supply-chain cyberattack (2 November 2026). https://www.rtp.pt/noticias/mundo/sete-lojas-do-intermarche-atingidas-por-ciberataque-em-portugal_n1776375 Verified on 2026-11-27.

S65: Observador. APED confirms three of seven affected Intermarché Portugal stores suffered total refrigerated merchandise loss (2 November 2026). https://observador.pt/2026/11/02/ataque-informatico-atinge-frigorificos-e-congeladores-de-supermercados-na-belgica-luxemburgo-e-suecia/ Verified on 2026-11-27.

S66: Azeméis.Net / Lusa. Câmara Municipal de Santa Maria da Feira confirms 5 November 2026 cyberattack halting IT, email and landlines and notifying CNCS. https://azemeisnet.sapo.pt/ataque-informatico-camara-feira-depois-ovar-servicos-afetados/ Verified on 2026-11-27.

S67: Rádio Sintonia. Câmara Municipal de Santa Maria da Feira official statement on 5 November 2026 overnight intrusion and CNCS coordination. https://radiosintonia.pt/2026/11/05/camara-municipal-de-santa-maria-da-feira-alvo-de-ataque-informatico/ Verified on 2026-11-27.

S68: Observador / Lusa. Worten confirms unauthorised access to limited customer and supplier data, patching exploited flaw and notifying CNCS, CNPD and PJ (11 November 2026). https://observador.pt/2026/11/11/worten-alvo-de-ciberataque-que-acedeu-a-dados-de-clientes-e-prestadores-de-servicos/ Verified on 2026-11-27.

S69: RTP / Lusa. Worten confirms no passwords or payment-card details accessed in November 2026 cyberattack. https://www.rtp.pt/noticias/economia/worten-alvo-de-ciberataque-que-acedeu-a-dados-de-clientes-e-prestadores-de-servicos_n1778556 Verified on 2026-11-27.

S70: ECO. Worten notifies affected customers on 12 November 2026 that NIF, telephone, email and some order numbers were accessed (12 November 2026). https://eco.sapo.pt/2026/11/12/ciberataque-a-worten-acedeu-a-nif-contactos-telefonicos-e-email-de-clientes/ Verified on 2026-11-27.

S71: Correio da Manhã. SMAS de Sintra confirms November 2026 cyberattack affecting online customer forms. https://www.cmjornal.pt/portugal/detalhe/ataque-informatico-saca-dados-dos-clientes-dos-smas-de-sintra Verified on 2026-11-27.

S72: TugaTech. SMAS de Sintra notifies affected customers of web-form data copy including NIF, ID and IBAN and notifies CNPD and CNCS. https://tugatech.com.pt/t94480-smas-de-sintra-sofrem-ataque-informatico-que-expoe-dados-pessoais-e-iban-de-clientes Verified on 2026-11-27.

S73: Observador. ASAE official source confirms 15 November 2026 website defacement; CNCS confirms outreach (15 November 2026). https://observador.pt/2026/11/15/site-da-asae-indisponivel-apos-ataque-informatico-que-usou-imagem-de-jose-socrates/ Verified on 2026-11-27.

S74: Executive Digest. IMT confirms consecutive cyberattacks forcing preventive suspension of digital services with no indication of data exfiltration. https://executivedigest.sapo.pt/ciberataques-ao-imt-deixam-servicos-em-dificuldades-atencao-as-possiveis-burlas/ Verified on 2026-11-27.

S75: Rádio Metropolitana Porto. Câmara Municipal do Porto confirms 21 November 2026 website defacement limited to institutional portal with no personal-data compromise and CNCS notification. https://www.radiometropolitanaporto.pt/website-da-camara-do-porto-alvo-de-ataque-informatico/ Verified on 2026-11-27.

S76: Ciberseguranca.PT. Technical analysis of Câmara Municipal do Porto CMS modification (21 November 2026) and broader 2026 Portuguese public-portal defacements. https://www.ciberseguranca.pt/camara-do-porto-paginas-oficiais-exibem-assinatura-de-intruso-e-os-seus-dados/ Verified on 2026-11-27.

S77: ADENE - Agência para a Energia. Official ADENE communiqué confirming 23 November 2026 intrusion, preventive suspension of Portal SCE and notifications to CNCS and PJ. https://www.adene.pt/adene-alvo-de-ataque-informatico-suspende-temporariamente-o-acesso-ao-sce/ Verified on 2026-11-27.

S78: RTP / Lusa. ADENE suspends Building Energy Certification System (SCE) following unauthorised intrusion (23 November 2026). https://www.rtp.pt/noticias/economia/adene-suspende-acesso-ao-sistema-de-certificacao-energetica-dos-edificios-apos-ciberataque_n1781185 Verified on 2026-11-27.

S79: Ciberseguranca.PT. Overview of 2026 cyber-incident timeline highlighting 32 public Portuguese cases through 23 November 2026. https://www.ciberseguranca.pt/188-ciberincidentes-em-2026-o-que-a-linha-do-tempo-do-ano-revela/ Verified on 2026-11-27.

S80: Burlómetro / Tek Notícias (citing CNCS). CNCS/CERT.PT alert on phishing emails impersonating CNCS requesting a critical system update (25 June 2026). https://burlometro.pt/alertas/email-cncs-atualizacao-critica/ Verified on 2026-11-27.

S81: ThreatFabric. Massiv Android banking trojan masquerading as an IPTV app targeting Portuguese digital identity wallet and Chave Móvel Digital (February 2026). https://www.threatfabric.com/blogs/massiv-when-your-iptv-app-terminates-your-savings Verified on 2026-11-27.

S82: IETF RFC Editor. RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC). https://www.rfc-editor.org/rfc/rfc7489.html Verified on 2026-11-27.

S83: IETF RFC Editor. RFC 7208 - Sender Policy Framework (SPF). https://www.rfc-editor.org/rfc/rfc7208.html Verified on 2026-11-27.

S84: IETF RFC Editor. RFC 6376 - DomainKeys Identified Mail (DKIM) Signatures. https://www.rfc-editor.org/rfc/rfc6376.html Verified on 2026-11-27.

S85: IETF RFC Editor. RFC 6797 - HTTP Strict Transport Security (HSTS). https://www.rfc-editor.org/rfc/rfc6797.html Verified on 2026-11-27.

S86: NIST NVD. CVE-2026-1731 - BeyondTrust Remote Support / Privileged Remote Access pre-authentication RCE (CVSS 9.8). https://nvd.nist.gov/vuln/detail/CVE-2026-1731 Verified on 2026-11-27.

S87: NIST NVD. CVE-2026-88771 and CVE-2026-88772 - Citrix NetScaler ADC and Gateway input-validation vulnerabilities (CVSS 9.8 / 8.1). https://nvd.nist.gov/vuln/detail/CVE-2026-88771 Verified on 2026-11-27.

S88: NIST NVD. CVE-2026-102764 - BeyondTrust Remote Support improper message origin validation (CVSS 9.8). https://nvd.nist.gov/vuln/detail/CVE-2026-102764 Verified on 2026-11-27.

S89: NIST NVD. CVE-2026-104935 - Ivanti Connect Secure authentication bypass by spoofing (CVSS 8.6). https://nvd.nist.gov/vuln/detail/CVE-2026-104935 Verified on 2026-11-27.

S90: NIST NVD. CVE-2026-109618 and CVE-2026-109619 - PHP out-of-memory and global-state memory-corruption flaws (CVSS 9.8 / 8.1). https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Verified on 2026-11-27.

S91: NIST NVD. CVE-2026-120868 - Citrix NetScaler ADC and Gateway packet-processing memory overflow (CVSS 4.0 9.3). https://nvd.nist.gov/vuln/detail/CVE-2026-120868 Verified on 2026-11-27.

S92: NIST NVD. CVE-2026-115560 and CVE-2026-129289 - PHP session-serializer RCE and PHP-FPM request smuggling (CVSS 4.0 9.2). https://nvd.nist.gov/vuln/detail/CVE-2026-115560 Verified on 2026-11-27.

S93: NIST NVD. CVE-2025-53770 (Microsoft SharePoint) and CVE-2025-64095 (DNN CMS) - Top vulnerabilities observed by CERT.PT in 2025. https://nvd.nist.gov/vuln/detail/CVE-2025-53770 Verified on 2026-11-27.

S94: Brandefense. Brandefense demo and advisory contact page. https://brandefense.io/request-a-demo/ Verified on 2026-11-27.

Appendix D. Glossary

- **National Atlas headline.** The single 0 to 100 Brandefense Atlas exposure figure published for the assessed Portuguese portfolio as a whole; higher values indicate greater observed external exposure and never represent a breach percentage or sector ranking [S4].
- **CNCS / CERT.PT.** Portugal's National Cybersecurity Centre (Centro Nacional de Cibersegurança) and its national computer-emergency response team [S5][S22].
- **Decreto-Lei n.º 125/2025.** Portugal's Cybersecurity Legal Regime transposing the EU NIS2 Directive, in force from 3 April 2026 [S22].
- **Regulamento n.º 756/2026 and MyCiber.** CNCS implementing regulation (in force 23 June 2026) and electronic platform governing entity qualification, Cybersecurity Officer designation and minimum security measures [S23][S24].
- **QNRCS.** Portugal's National Cybersecurity Reference Framework (Quadro Nacional de Referência para a Cibersegurança) defining baseline security controls [S23].
- **CNPD and Lei n.º 58/2019.** Portugal's Data Protection Authority (Comissão Nacional de Proteção de Dados) and national GDPR execution statute [S9][S26].
- **DORA and Lei n.º 73/2025.** EU Digital Operational Resilience Act and Portugal's national implementing statute designating Banco de Portugal, CMVM and ASF [S25][S27].
- **PJ UNC3T.** The cybercrime investigation unit (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica) within Portugal's Polícia Judiciária [S29][S39].
- **RASI 2025.** Portugal's Annual Internal Security Report (Relatório Anual de Segurança Interna) combining official CNCS/CERT.PT, PJ, DGPJ and SIS chapters [S5].
- **FCSAL.** Local Administration Cybersecurity Forum (Fórum de Cibersegurança da Administração Local), bringing together Portuguese inter-municipal entities, the National Association of Portuguese Municipalities and local authorities for alert sharing and good practice [S5].
- **RNSI.** Portugal's National Internal Security Network (Rede Nacional de Segurança Interna), which supported ANEPC and CNCS in suspending the RNBP registry [S62].
- **Chave Móvel Digital (CMD).** Portugal's national mobile electronic-authentication and digital-signature credential for public and private services [S81].
- **Multibanco, MB WAY and SPIN.** Portugal's national interbank ATM/payment-reference network, mobile instant-payment service and Banco de Portugal payee-lookup tool [S13].
- **NIF / CC / NISS / SNS.** Portuguese tax number (Número de Identificação Fiscal), Citizen Card (Cartão de Cidadão), social-security number and national health-service number; personal identifiers are context, never authentication [S39][S62].
- **DMARC, SPF, DKIM and HSTS.** Published DNS email-authentication standards (`RFC 7489` , `RFC 7208` , `RFC 6376`) and strict HTTPS transport policy (`RFC 6797`) [S82][S83][S84][S85].
- **AiTM (adversary-in-the-middle).** Phishing technique placing a live proxy between a user and a login portal to intercept passwords and active MFA session tokens (as in Tycoon 2FA) [S29].

- **BIN (bank identification number).** Leading six digits of a payment card number identifying the card network and issuing institution [S1].
- **KYC (Know Your Customer).** Identity-verification and customer due-diligence checks run by regulated financial institutions before onboarding accounts [S1].
- **TLP:CLEAR.** Shareable without Traffic Light Protocol restriction while observing privacy and statutory duties.

About this report

Prepared by Odin by Brandefense. Version 1.0 applies distinct reference dates. The 2026 activity window runs from 1 January to 26 November 2026 (UTC, by publication timestamp), with 12 to 26 November 2026 examined separately as recent activity. Rolling 365-day domain mentions span 27 November 2025 to 26 November 2026. Exposure observations (247 of 250 selected domains) and passive domain configurations (all 250 domains) reflect a 27 November 2026 snapshot, with 3 selected domains remaining unknown in exposure observations. All external sources were verified on 27 November 2026.

The European Portuguese edition translates the English master; the English edition prevails where wording differs. Recommendations require validation against each organisation's own assets, dependencies and legal obligations.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO