BRANDEFENSE COUNTRY REPORT · BELGIUM 2026

Brandefense Belgium Cyber Threat Landscape Report 2026

Identity exposure, shared suppliers and operational continuity

Odin by Brandefense
Research window: 1 January–22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · 9–22 November 2026

63 of 250
selected organisation domains had a credential listed for sale when checked

1,025
distinct retained forum posts, with limited coverage beyond these venues

22
ransomware group labels in the retained Belgian listing population

11 of 25
selected banking and finance domains had a current credential listing

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Belgium's digital and threat context	10
03	National exposure: selected organisations and domains	13
04	What we see on the dark web	22
05	Confirmed incidents and claims by sector	36
06	Hacktivism, disruption and operational systems	48
07	Threat actors and evidence relationships	52
08	The fraud economy	60
09	Banking and finance deep dive	65
10	Regulatory and national response	68
11	Outlook	73
12	Action plan	76
A	Appendix A. Method and limits	81
B	Appendix B. Evidence register	84
C	Appendix C. Sources	85
D	Appendix D. Glossary	88
	About this report	90

CISO and leadership	01 05 10 11 12
SOC and identity	03 04 07 09 A–B
Operations and procurement	02 05 06 12
Finance and customer protection	04 08 09
Privacy and communications	05 06 10 A–C

About this edition

AI-assisted research and drafting. Evidence labels and coverage limits apply throughout. The English edition prevails where translated editions differ.

Contents and reading guide

Chapter	Question
1 Executive summary	What should leaders decide first?
2 Context	Which dependencies shape the Belgian picture?
3 National exposure	What does the selected domain assessment establish?
4 Dark web	What was advertised, and what remains unverified?
5 Incidents	Which service and data outcomes were supported?
6 Disruption	How do claims differ from operational impact?
7 Actors	Which relationships are evidenced?
8 Fraud	How could exposed information support deception?
9 Banking	What should identity and fraud teams validate?
10 Regulation	Which duties and milestones apply?
11 Outlook	Which conditional scenarios deserve rehearsal?
12 Action plan	Who owns the next 30/60/90 days?
Appendices A–D	Scope, evidence register, sources and glossary

Leadership can start with Chapters 1, 5, 10 and 12. SOC and identity teams should read Chapters 3, 4, 7 and 9. Operations, procurement and customer-protection teams should use Chapters 5, 6 and 8.

Observed means a retained advertisement, listing or public statement exists. **Claimed** preserves what an advertiser says without validating its outcome. **Assessed** identifies a proportionate interpretation, its alternative explanation and the action it supports.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What matters most for Belgian organisations in 2026, and what should leadership do first?

4

decisions tied to identity, suppliers, operations and incident communication

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Belgium's evidence points to identity protection and service continuity. The CCB received 588 incident reports through 28 September. Ransomware sites carried 46 Belgian listings within the report window. Retained forum posts advertised customer data, identity material, access and fraud tools. Public incidents affected care, membership information, education and administrative services. These populations measure different things. Validate active identities, map supplier dependencies, restrict remote operational access and rehearse notification and recovery decisions.

The report combines underground observations, exposure data and verified public reporting. Brandefense Blackhole records 96,265 country-tagged posts across platforms. The retained content covers 1,025 distinct forum posts, including 480 country-tagged forum posts. These overlapping populations describe visibility, not national attack counts. [S1][S2][S3]

1. Identity protection has the strongest official support. In its 9 November assessment, the CCB described account-related incidents as around 30% of reported incidents during the first two quarters. Police reporting separately describes reused mailbox credentials, invoice alteration and bank-impersonation fraud. Neither source measures current exposure at every Belgian organisation. [S5][S31][S32]

2. Extortion claims span many group labels. Ransompedia recorded 46 accepted listings dated within the window, across 22 group labels. Qilin accounts for 9 and The Gentlemen for 7. The partial-year total exceeds the 42 recorded during all of 2025. This is not an annual growth rate or proof of 46 distinct intrusions. [S1]

3. Shared suppliers turn technical incidents into service decisions. Learning, healthcare and local-government cases show how a dependency can affect communication, availability and data assessment. A customer population is not an affected-victim count. Require a supplier-specific and customer-specific impact statement. [S8][S13][S22]

4. Advertising mixes old data, current claims and untested capabilities. One telecom advertisement points back to July 2025. A large citizen-data poster admits its source is unknown. Recent posts advertise support-ticket data, bank impersonation tools and a casino-themed customer list. They do not establish working access or completed transactions. [S3]

5. Operational recovery needs its own owner. November refrigeration disruption creates a different problem from a website outage. Public attribution remained disputed in the retained reporting. The immediate defensive question is how to control remote access and return equipment to a safe state. [S25][S26][S27]

6. Current listings require scoped identity validation. 63 of 250 selected organisation domains had a credential listed for sale when checked. The national Atlas headline is 48 out of 100. At least 296,591 device associations and 26,236,674 credential records describe overlapping exposure populations, not confirmed intrusions. [S2]

Four decisions for leaders

1. **Validate identities before prescribing disruptive response.** Ask identity and SOC leads to distinguish an old credential, an active account and a suspicious session. Keep a recorded disposition for each relevant finding.
2. **Map supplier dependencies to data and service impact.** Ask each critical provider for scoped notification terms and a tested alternative process. Rehearse an outage while the confidentiality assessment remains uncertain.
3. **Control remote operational access.** Give operations a verified access list, a safe local process and authority to restrict supplier access when needed. Test recovery without the ordinary remote route.
4. **Prepare clear notifications and recovery decisions.** Assign privacy, legal, communications and technical owners. Keep statutory clocks separate from internal planning targets and preserve uncertainty across French and Dutch notices.

The year in numbers

588

Incident reports received by CCB, 1 January–28 September 2026 [S4]

WHAT IT IS NOT

A full-year total, unique victims or a national prevalence estimate

46

Accepted Belgian ransomware listings within the report window [S1]

WHAT IT IS NOT

Confirmed encryption, distinct intrusions or measured loss

22

Group labels attached to those listings [S1]

WHAT IT IS NOT

Verified separate criminal organisations

1,025

Distinct retained forum posts across the collected sets [S3]

WHAT IT IS NOT

All posts concerning Belgium or unique incidents

480

Country-tagged forum posts within that retained population [S3]

WHAT IT IS NOT

An additional population to add to 1,025

31

Retained posts dated 9–22 November [S3]

WHAT IT IS NOT

Not verified new intrusions

250

Purposively selected candidate domains [S2]

WHAT IT IS NOT

A ranked economic census or a representative national sample

245

Candidate domains with a DNS response at the observation date [S2]

WHAT IT IS NOT

Validated independent legal entities or a security rating

63

Selected organisation domains with a current credential listing [S2]

WHAT IT IS NOT

Working access, active accounts or confirmed intrusions

48

National Atlas headline for the selected 250 domains [S2]

WHAT IT IS NOT

National prevalence or a sector rating

96,265

Country-tagged posts across platforms [S3]

WHAT IT IS NOT

Verified Belgian targeting, criminal relevance or national incidents

KEY TAKEAWAYS

01

Prioritise account validation and recoverable services.

02

Keep advertisements, listings and confirmed incidents as separate populations.

03

Give suppliers, operations and notification decisions named owners.

Report map

Start with the decision you own, then follow the evidence and its limits.

CISO and leadership	Fund identity, continuity and notification work	01 05 10 11 12
SOC and identity	Validate advertisements, sessions and current activity	03 04 07 09 A–B
Operations and procurement	Maintain safe services through a supplier incident	02 05 06 12
Finance and customer protection	Interrupt impersonation and payment changes	04 08 09
Privacy and communications	Preserve evidence scope and reporting duties	05 06 10 A–C

CHAPTER 02

Belgium's digital and threat context

THIS CHAPTER ANSWERS

Which features of Belgium matter for incident response, and which conclusions should defenders avoid?

588

incident reports received by the CCB through 28 September, not a national victim count

2.1 A digital dependency can cross several boundaries 11

2.2 Official reports point to identity and system exposure 11

2.3 Suppliers create service dependencies 12

2.4 Politically framed activity needs careful attribution 12

CHAPTER 02

Belgium's digital and threat context

IN SHORT

Belgium's public services, commercial platforms and suppliers share digital dependencies across organisational and national borders. The CCB received 588 incident reports through 28 September. Its November identity report puts account protection at the centre of the response. The cases in this report also show why a supplier interruption can become a customer-service problem. Identify the account, supplier and operational dependencies that your organisation needs to keep working.

2.1 A digital dependency can cross several boundaries

Belgium's official portal describes a federal state with three communities and three regions. Dutch, French and German are official languages. These are administrative facts, not explanations of security performance. [S6]

For a defender, the useful question is who controls a service and its data. A central contract may support several local administrations. A foreign platform may hold Belgian customer records. An incident at that platform does not establish an intrusion into every Belgian customer's own network.

The report therefore separates domestic organisational incidents, shared-service incidents and foreign-service context. It does not rank language communities, regions or administrations by security. The selected domain observations cannot support such comparisons.

Communications should follow the affected users. Prepare plain-language notices in the languages your service uses. Keep the scope, uncertainty and protective advice identical across editions. Translation must not turn a possible disclosure into a confirmed theft.

2.2 Official reports point to identity and system exposure

The CCB received 588 incident reports between 1 January and 28 September 2026, against 556 during all of 2025. Those periods differ. The comparison shows that the earlier full-year total was exceeded; it is not an annual growth rate. [S4]

The quarterly reports describe changing incident mixes. The first quarter recorded 154 cyber incidents; the second recorded 188 cyber incidents within a wider notification population. These figures are not interchangeable with all notifications. [S7][S8]

The third-quarter report highlights system intrusions and exposed vulnerabilities. The CCB's November identity assessment says account-related incidents represented around 30% of reported incidents during the first two quarters. Reporting populations and periods remain attached to each figure. [S9][S5]

This supports two parallel workstreams. Identity teams should verify sessions, recovery routes and privileged access. Infrastructure teams should know which exposed systems require urgent remediation. Neither team can close its work solely by completing the other's checklist.

2.3 Suppliers create service dependencies

The CCB's second-quarter report discusses software supply chains affecting Belgium. Public cases concern healthcare software, learning platforms and a digital-signature service used by local authorities. Their common feature is dependency, not evidence of one coordinated attacker. [S8][S13][S22]

For suppliers, the first useful deliverable is a customer-specific impact statement. For customers, it is a record of which data, accounts and processes depend on that supplier. A supplier's client count is not the number of clients whose data was taken.

Keep commercial continuity separate from confidentiality. A service can be unavailable because it was deliberately isolated. Another service can remain available while personal data is exposed. Chapter 5 records these outcomes separately.

2.4 Politically framed activity needs careful attribution

The CCB describes state-sponsored activity and geopolitical hacktivism as relevant threats. That assessment does not attribute every Belgian incident to a state. The public record for the refrigeration campaign illustrates why the distinction matters. [S8][S9][S26]

Reuters reported different ministerial assessments on 13 November. The interior minister described Iranian involvement as very likely; the foreign minister said the available information was insufficient for official attribution. An investigation was continuing. [S26]

This report makes no independent attribution for that campaign. It takes no position on government decisions, international disputes, language politics or historical relationships. Actor rhetoric does not establish motive, technical responsibility or impact.

EU institutions appear only as public context. A Brussels location, an EU-related brand or a multilingual post does not by itself make an incident part of Belgium's domestic organisational population.

KEY TAKEAWAYS

01

Attach each official figure to its own reporting population and period.

02

Map supplier dependencies to the service and data actually affected.

03

Preserve uncertainty when describing attribution or translating a notice.

CHAPTER 03

National exposure: selected organisations and domains

THIS CHAPTER ANSWERS

What do measured exposure signals mean for the selected organisations?

63 of 250

selected organisation domains had a credential listed for sale when checked

3.1 Universe card 14

3.2 Exposure signals by sector 14

3.3 Devices and credentials 17

3.4 How to handle a current identity finding 18

3.5 Email and web controls 19

CHAPTER 03

National exposure: selected organisations and domains

IN SHORT

63 of 250 selected organisation domains had a credential listed for sale when checked. The national Atlas headline is 48 out of 100. The portfolio records at least 296,591 device associations and 26,236,674 credential records. These overlapping observations do not establish unique people, active accounts or confirmed intrusions. Passive checks cover 245 of these domains. Validate current listings, investigate employee-associated devices and verify recovery routes.

3.1 Universe card

Attribute	Scope
Population	250 selected primary domains across ten sectors; 245 with passive observations
Unit	A primary domain; legal-entity independence and ownership are not established by DNS
Selection	Public-service and economic roles; a purposive portfolio, not a ranked national census
Exposure date	Cumulative device, credential, listing and document observations: 21 November 2026
Other periods	Mentions: previous 365 days through 22 November 2026; lookalikes: 30 days; passive observations: 22 November 2026
Overlap	Records can overlap across sources, domains, devices and people; totals are not unique-user counts
Interpretation	Findings describe selected domains, not national prevalence or every organisational asset

The national scope of this report does not make the portfolio representative. A domain may serve employees, students, customers or several operating units. Domain associations do not establish device ownership or enterprise-network intrusion. [S2]

3.2 Exposure signals by sector

The national Atlas headline for the selected 250 domains is 48 on a 0–100 scale. Higher values describe more observed external exposure in this portfolio. The table reports signal counts by sector. [S2]

Current listings, employee-device associations and document references describe different populations

Cells show domains with the signal out of 25 selected domains per sector. Current credential listings are shown in coral.

	Current listing	Listing history	Employee devices	Document references
Banking and finance	11/25	11/25	18/25	18/25
Government and public services	3/25	3/25	11/25	11/25
Local administration	2/25	2/25	23/25	18/25
Education and research	6/25	6/25	21/25	19/25
Health and care	2/25	2/25	19/25	13/25
Energy and utilities	2/25	2/25	16/25	9/25
Transport and logistics	8/25	8/25	18/25	13/25
Industry and business	2/25	2/25	20/25	20/25
Retail and consumer services	18/25	18/25	16/25	14/25
Telecom, technology and media	9/25	9/25	17/25	18/25

Source: exposure observations for 250 selected organisation domains, 21 November 2026. Cumulative, overlapping associations; not confirmed intrusions or national prevalence [S2].

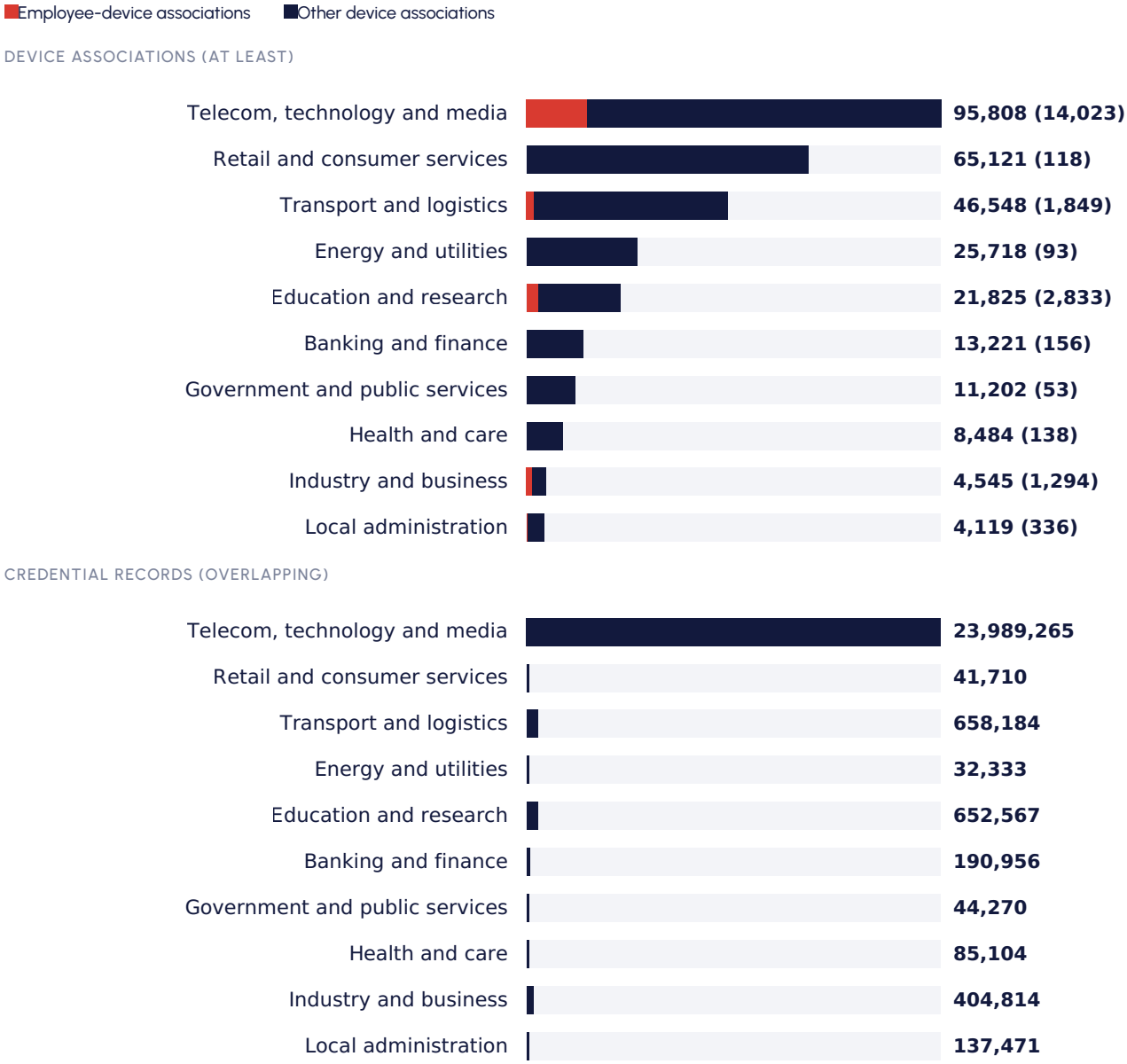
Sector	Domains	Current listings	Listing history	With employee devices	With documents
Banking and finance	25	11	11	18	18
Government and public services	25	3	3	11	11
Local administration	25	2	2	23	18
Education and research	25	6	6	21	19
Health and care	25	2	2	19	13
Energy and utilities	25	2	2	16	9

Sector	Domains	Current listings	Listing history	With employee devices	With documents
Transport and logistics	25	8	8	18	13
Industry and business	25	2	2	20	20
Retail and consumer services	25	18	18	16	14
Telecom, technology and media	25	9	9	17	18
All selected domains	250	63	63	179	153

The last two columns count domains with an employee-device association or exposed-document reference, not devices or documents. Every sector contains 25 selected domains. A current listing supports account validation; it does not establish that an account works. [S2]

3.3 Devices and credentials

Device and credential associations differ substantially across the selected sectors



Source: exposure observations for 250 selected organisation domains, 21 November 2026. Cumulative, overlapping associations; not confirmed intrusions or national prevalence [S2].

Sector	Domains	Devices, at least	Employee devices	Credential records
Banking and finance	25	13,221	156	190,956
Government and public services	25	11,202	53	44,270
Local administration	25	4,119	336	137,471

Sector	Domains	Devices, at least	Employee devices	Credential records
Education and research	25	21,825	2,833	652,567
Health and care	25	8,484	138	85,104
Energy and utilities	25	25,718	93	32,333
Transport and logistics	25	46,548	1,849	658,184
Industry and business	25	4,545	1,294	404,814
Retail and consumer services	25	65,121	118	41,710
Telecom, technology and media	25	95,808	14,023	23,989,265
All selected domains	250	296,591	20,893	26,236,674

The portfolio contains at least 296,591 device associations, including 20,893 classified as employee-related. Credential records comprise 9,869,372 breach-database records, 1,488,704 stealer-log records and 14,878,598 combolist records. These sources overlap; their total does not count unique accounts. [S2]

Some device totals are lower bounds. An employee classification is an investigative lead, not verified employment or device ownership. Shared educational and customer-facing domains need role validation before account response.

The portfolio also records 38,774 lookalike-domain candidates and 1,333 exposed-document references. Similarity does not establish malicious use; a document reference does not prove confidential data was disclosed. Dark-chat mentions occur for 39 domains and dark-web mentions for 31. Visibility does not establish hostility. [S2]

3.4 How to handle a current identity finding

Assign a finding to an accountable identity owner. Check whether the account exists, remains active and has already been remediated. Compare the finding's age with recent authentication and recovery activity.

If a suspicious current session is verified, revoke it and review persistence, registered authentication methods and mailbox changes. If the record is historical and inactive, document that disposition. Preserve evidence before deleting or resetting an account.

The 63 current credential listings concern the selected domain portfolio. Forum requests and capability advertisements are separate observations. Neither a current listing nor a buyer request establishes working access or a confirmed organisational intrusion. [S2][S3]

3.5 Email and web controls

Observation	Count	Denominator
DMARC reject or quarantine	188	245
DMARC monitoring policy	46	245
No valid DMARC policy observed	11	245
SPF observed	234	245
DKIM information observed	204	245
DS (delegation signer) record observed	65	245
TLS certificate validated	240	245
TLS certificate error	1	245
TLS outcome undetermined	4	245
Homepage response obtained	213	245
HSTS (HTTP Strict Transport Security) in obtained response	164	213
CSP (Content Security Policy) in obtained response	91	213

A published DMARC policy describes how receivers are asked to treat unauthenticated messages. A monitoring policy differs from enforcement. Even an enforcement policy is not proof that every legitimate sender is aligned or that every receiver applies it. [S2]

SPF and DKIM support email authentication, but their presence is not a complete mail-security assessment. Failure to observe a signing configuration does not prove that no valid signing configuration exists. Owners should validate their actual sending services.

A DS record observation is not end-to-end validation of DNSSEC. A successful TLS observation concerns the assessed host at that time. A failed or missing observation must be reviewed before it is described as an organisational configuration defect. [S2]

Homepage headers describe the captured response, rather than every application or path. An absent header can justify a configuration review; it cannot establish exploitability, sensitive-data exposure or a successful intrusion.

Email-control observations concern the selected domain population

	DMARC reject / quarantine	SPF	TLS
Banking and finance	23/25	25/25	25/25
Government and public services	21/25	20/25	24/25
Local administration	20/23	22/23	22/23
Education and research	13/24	23/24	24/24
Health and care	16/24	21/24	23/24
Energy and utilities	21/25	25/25	25/25
Transport and logistics	16/24	23/24	24/24
Industry and business	22/25	25/25	23/25
Retail and consumer services	19/25	25/25	25/25
Telecom, technology and media	17/25	25/25	25/25

Source: passive observations, 22 November 2026. Each cell shows observed/assessed domains; published policies do not establish enforcement for every message [S2].

Sector	Observed	DMARC reject/quarantine	SPF observed	TLS valid
Banking and finance	25	23	25	25
Government and public services	25	21	20	24
Local administration	23	20	22	22
Education and research	24	13	23	24
Health and care	24	16	21	23
Energy and utilities	25	21	25	25
Transport and logistics	24	16	23	24
Industry and business	25	22	25	23

Sector	Observed	DMARC reject/quarant-ine	SPF observed	TLS valid
Retail and consumer services	25	19	25	25
Telecom, technology and media	25	17	25	25

KEY TAKEAWAYS

01

Validate current listings and employee-device associations with their owners.

02

Keep overlapping records separate from people and confirmed intrusions.

03

Review passive controls against the assessed domain and date.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do retained advertisements establish about Belgian data, access and fraud demand?

1,025

distinct retained forum posts, with limited coverage beyond these venues

4.1 Universe card 23
4.2 Volume and language 25
4.3 The products advertised 27
4.4 Case studies 27
4.5 Additional evidence cards 33
4.6 Recent activity in the retained forums 35
4.7 What the forums add 35

CHAPTER 04

What we see on the dark web

IN SHORT

The retained forums show a market for customer records, identity images, access and fraud tools. Some advertisements explicitly refer to older incidents. Others acknowledge uncertain provenance or describe proposed data structures. The closing weeks add support-ticket, bank-template and casino-themed claims. The observed fact is the advertisement. Validate relevance, freshness and access through trusted organisational evidence before treating an offer as a current incident.

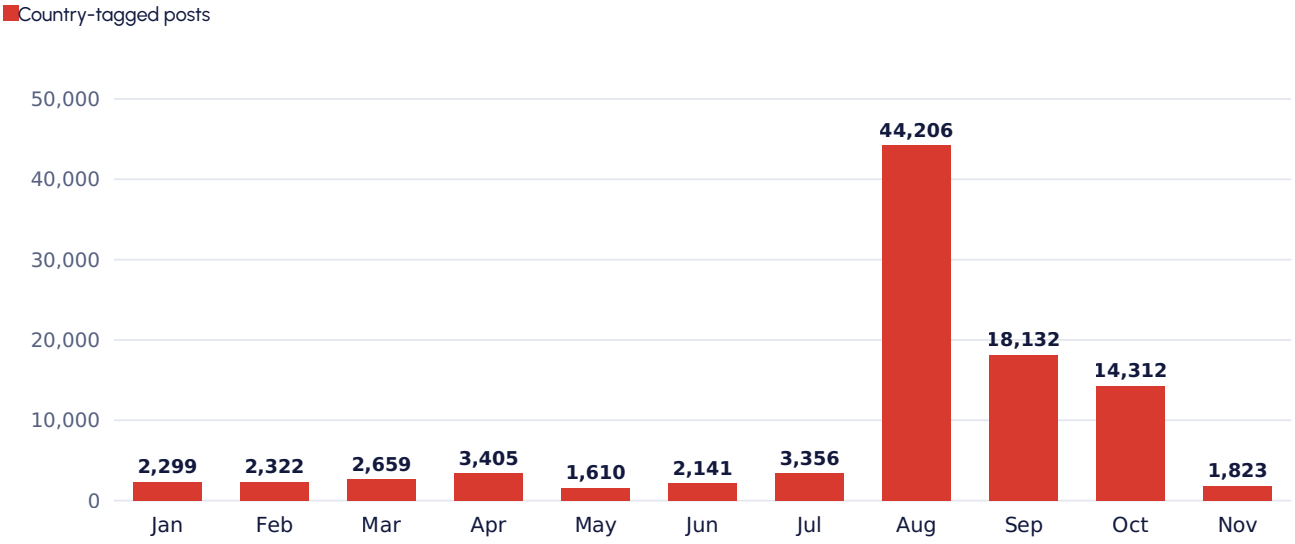
4.1 Universe card

Attribute	Scope
Period	Post dates 1 January–22 November 2026
Retained population	1,025 distinct posts in the retained forum material
Country-tagged subset	480 posts, included within the retained population
Recent subset	31 posts dated 9–22 November, also included within the retained population
Venue	Retained content is forum-based; tagged counts also cover other platforms
Unit	A post, not a unique file, seller, purchase, victim or incident
Coverage limit	Some advertised records remain unavailable; tagged totals and retained forum posts are separate populations

The forum and country-tagged populations overlap. Their totals must not be added together. Country labels and references to Belgium do not independently validate targeting, provenance or nationality of a victim. [S3]

Brandefense Blackhole records 96,265 country-tagged posts across platforms during the report window. A country tag does not establish Belgian targeting, criminal relevance or an incident. These counts include discussion and advertising; they are separate from the 1,025 retained forum posts. [S3]

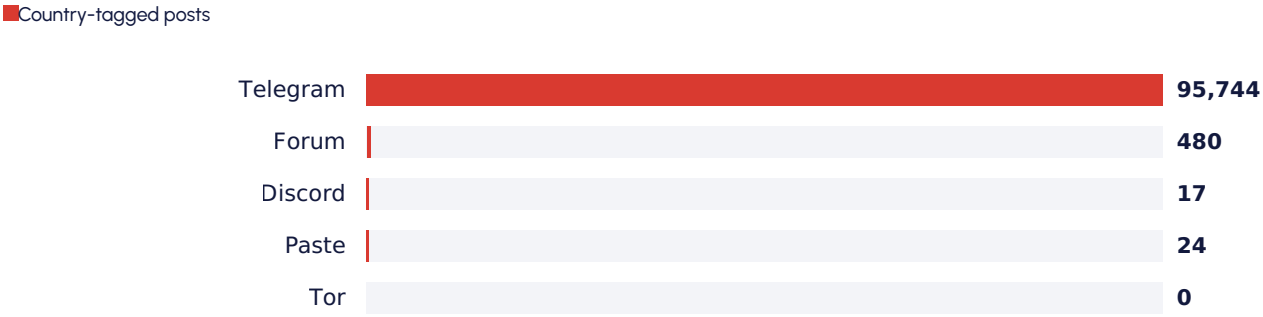
Country-tagged monthly counts measure recorded visibility, not attack frequency



Source: Brandefense Blackhole, 1 January-22 November 2026; November partial. Tagged posts and retained forum posts are separate populations, not confirmed incidents [S3].

Month	Country-tagged posts
2026-01	2,299
2026-02	2,322
2026-03	2,659
2026-04	3,405
2026-05	1,610
2026-06	2,141
2026-07	3,356
2026-08	44,206
2026-09	18,132
2026-10	14,312
2026-11	1,823

Tagged platform counts describe source visibility, not victims



Source: Brandefense Blackhole, 1 January-22 November 2026; November partial. Tagged posts and retained forum posts are separate populations, not confirmed incidents [S3].

Platform	Country-tagged posts
telegram	95,744
forum	480
discord	17
paste	24
tor	0

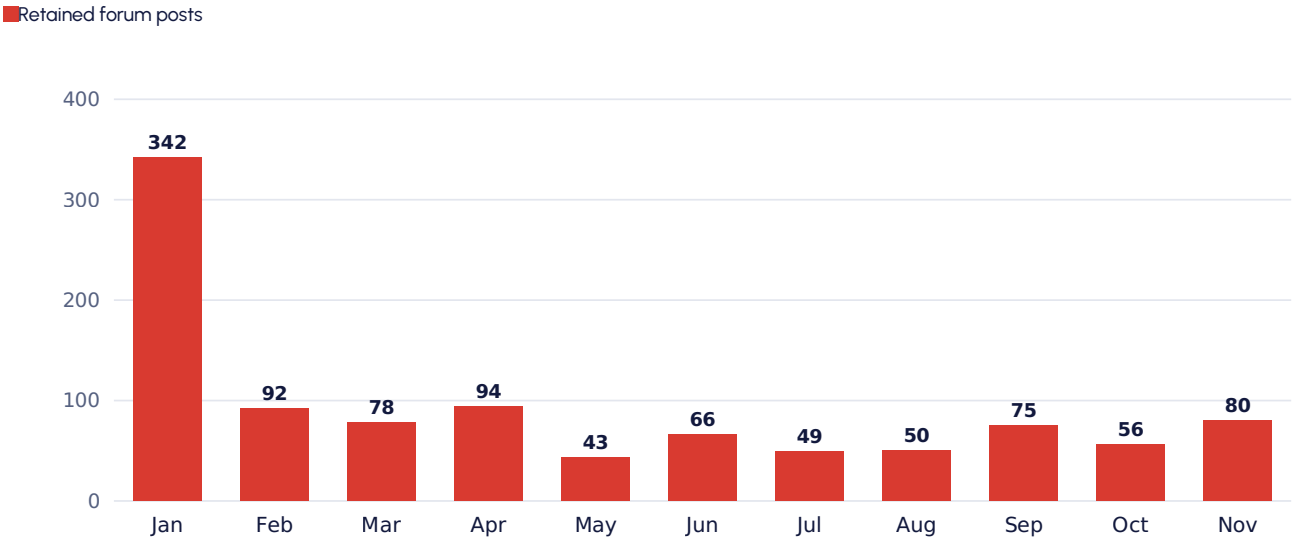
Telegram accounts for 95,744 of the 96,265 tagged posts. Retained case evidence comes from forums; the messaging population is represented here by counts. Those counts do not validate advertised claims or measure attack frequency. The forum content cannot establish crime-family shares across all platforms. [S3]

4.2 Volume and language

Month	Retained posts
2026-01	342
2026-02	92
2026-03	78
2026-04	94
2026-05	43
2026-06	66
2026-07	49
2026-08	50

Month	Retained posts
2026-09	75
2026-10	56
2026-11	80

The monthly figures describe retained forum posts, not national attack frequency



Source: Brandefense Blackhole, 1 January–22 November 2026; November partial. Tagged posts and retained forum posts are separate populations, not confirmed incidents [S3].

The monthly figures describe this retained population. They do not establish that Belgian threat activity rose or fell with the number of posts. Advertising, reposts, discussion and visibility can each affect the count. [S3]

Research covered English, French, Dutch and Russian reporting, with additional relevant regional context. The language of an advertisement does not establish the advertiser's nationality or the language of affected users.

4.3 The products advertised

Family	What the retained material shows	What it does not establish
Customer and citizen data	Telecom, training, legal-service and consumer-themed offers	Authenticity, unique people or fresh intrusion
Identity documents	Requests for Belgian identity images	A supplied document or successful onboarding
Access and sessions	Claims of administrative access and demand for cookies	Valid current access or a completed purchase
Bank-account identifiers	Advertised identifiers and asking prices	Account control or payment authority
Fraud tools	Bank-specific phishing-template advertisements	A working tool, deployed campaign or successful authentication interception

These are observed themes, not mutually exclusive incident categories or shares of a national underground economy. One advertisement may mention several products. A transaction is not established merely because a price is displayed. [S3]

4.4 Case studies

A

CASE A

A telecom advertisement points back to 2025

Evidence card B01 | 24 Jan 2026 | Leak forum | Telecommunications

Claim unverified

CLAIM	The advertiser offers a customer-data sample described as exceeding 300k people. It explicitly dates the underlying incident to July 2025.
CHRONOLOGY	The retained advertisement is dated 24 January 2026. Similar titles and later reuploads do not independently establish identical files.
ESTABLISHED	The advertisement and its historical reference are retained. The record count, source and authenticity are unverified.
ALTERNATIVE	Older material may be copied, relabelled or resold. A 2026 posting date does not establish a fresh intrusion.

RESPONSE	Validate affected accounts and prior remediation before describing a new incident. Prepare proportionate warnings if old personal details are circulating again. [S3]

Bottom line

A January advertisement states an older incident date and advertises a customer-data sample.

Evidence card B01 — 24 Jan 2026

kazutlg | Leak forum | Forum | English

ORIGINAL

At the end of July 2025, [a telecom operator] detected a cyberattack on one of its IT systems [...] Here is a sample from this parsed database containing over 300k individuals.

Held

A January advertisement states an older incident date and advertises a customer-data sample.

Not established

The number or authenticity of records, a new 2026 intrusion, or completed transactions.

CASE B

B A citizen-data poster admits the source is unknown

Evidence card B02 | 21 Jan 2026 | Leak forum | Citizen data

Claim unverified

CLAIM	A persona advertises 3.1M Belgian citizen records and suggests a public-service origin while admitting that the source is unknown.
CHRONOLOGY	The 21 January post drew a reply suggesting older social-network data. The original persona accepted that as a possibility.
ESTABLISHED	The uncertainty is visible in the discussion. Neither the original claim nor the reply validates the data source.
ALTERNATIVE	Historical social-media material, public-source collection and relabelled data remain plausible. The discussion does not establish that a government database was accessed.
RESPONSE	Require validated provenance and relevant samples before notifying a supposed source organisation. Do not use a large country-labelled count as the verification. [S3]

Bottom line

A forum post claims a large population dataset while acknowledging an unknown source.

Evidence card B02 — 21 Jan 2026

xmlrpc | Leak forum | Forum | English

ORIGINAL

Today, I leak data from 3.1M Belgian citizens. I don't have a source for this database [...] It's probably a government department scrape.

Held

A forum post claims a large population dataset while acknowledging an unknown source.

Not established

Government provenance, the size or uniqueness of a dataset, or a 2026 state-system intrusion.

CASE C

C

An autumn training-network offer may recirculate older material

Claim unverified

Evidence card B03 | 2 Oct 2026 | Leak forum | Education and training

CLAIM	The advertiser offers more than 700K people and +85 K IBAN, while also claiming to sell access. Those are different propositions.
CHRONOLOGY	The retained offer is dated 2 October. February replies and another October package refer to the same target topic. Public reporting separately describes republication. [S20]
ESTABLISHED	The advertisement is retained. Neither the number of distinct people nor current access is independently established.
ALTERNATIVE	An older package can be reposted or advertised by a different persona. Similar naming does not establish file identity or a separate October intrusion.
RESPONSE	Validate present account access separately from historical data exposure. Warn affected users about renewed impersonation when the organisation has established relevance. [S3]

Bottom line

An October advertisement makes both dataset and access claims. Earlier February replies reference the same target topic.

Evidence card B03 — 2 Oct 2026

yneov18 | Leak forum | Forum | English

ORIGINAL

I am selling the complete [vocational-training network] database from belgium containing more than 700K different people and +85 K IBAN [...] also selling the access.

Held

An October advertisement makes both dataset and access claims. Earlier February replies reference the same target topic.

Not established

The number of distinct people, valid current access, or a separate October intrusion.

CASE D

D

An access offer repeatedly describes proposed tables

Evidence card B04 | 8 Nov 2026 | Leak forum | Digital identity

Claim unverified

CLAIM	A seller claims administrative access to an identity-verification service, approximately 412k records and a price of USD 4,550.
CHRONOLOGY	The offer is dated 8 November. Its descriptions repeatedly call the contact, identity-check and recovery tables proposed.
ESTABLISHED	The schema descriptions and access assertion are retained. They do not show a validated account, tenant or database.
ALTERNATIVE	The structures could be hypothetical, copied or synthetic. Their wording raises questions without independently proving fabrication.
RESPONSE	Use trusted provider channels to validate a relevant tenant. Preserve administrative activity and recovery records before prescribing broad account resets. [S3]

Bottom line

The offer and its schema descriptions; the title claims roughly 412k records.

Evidence card B04 — 8 Nov 2026

DataJava | Leak forum | Forum | English

ORIGINAL

Access: full admin account in [identity-verification portal] [...] Proposed contact table [...] Proposed identity verification case table [...] Proposed account recovery case table [...] Price: $4,550

Held

The offer and its schema descriptions; the title claims roughly 412k records.

Not established

Valid access, actual stored records, the count, a successful sale or any supplier or identity-service incident.

CASE E

E

A phishing-panel advertisement names bank templates

Evidence card B05 | 20 Nov 2026 | Leak forum | Banking and identity fraud

Claim unverified

CLAIM	The SALTA3 advertisement markets templates for specific banks, including Belgian brands, and claims interactive authentication features.
CHRONOLOGY	The 20 November post falls within the closing two weeks. It is tool marketing, rather than a retained attack trace.
ESTABLISHED	The advertisement and claimed brand coverage exist. A bank brand in a template list is an impersonation theme, not evidence of bank-system access.
ALTERNATIVE	Features can be exaggerated or copied. The material does not establish working capability, deployment or successful authentication interception.
RESPONSE	Rehearse customer reporting and unusual device-enrolment or payment-approval handling. Review phishing-resistant authentication while preserving a clear distinction between marketing and observed attacks. [S3]

Bottom line

A 20 November advertisement markets bank-specific templates, including Belgian brands, and claims interactive features.

Evidence card B05 — 20 Nov 2026

0xcasper | Leak forum | Forum | English

ORIGINAL

SALTA3 is a live panel phishing kits customized to target specific banks [...] OTP/TAN/2FA support including QR Codes and PhotoTAN method.

Held

A 20 November advertisement markets bank-specific templates, including Belgian brands, and claims interactive features.

Not established

A working kit, successful MFA interception, active deployment, victims, bank-system access or payment losses.

CASE F

F

A supplier support-system claim includes tickets and attachments

Claim unverified

Evidence card B06 | 13 Nov 2026 | Leak forum | Business technology

CLAIM	A persona claims to hold all support tickets and attachments and advertises 6,028 users. Its claims about customers and earlier contact remain unverified.
CHRONOLOGY	The post is dated 13 November. No retained evidence independently establishes the claimed earlier contact with the supplier.
ESTABLISHED	The assertion is retained. It does not establish possession of every attachment or the impact on a particular customer.
ALTERNATIVE	The material could be partial, historical, copied or fabricated. A customer name inside advertising does not validate customer impact.
RESPONSE	Request a customer-specific supplier statement. Limit sensitive support attachments and review administrative access to portals that may hold operational details. [S3]

Bottom line

An actor claims support tickets and attachments; the post advertises 6028 users.

Evidence card B06 13 Nov 2026

updap | Leak forum | Forum | English

ORIGINAL

some random internet group has your every support ticket and every attachment [...] We urge your customers to review what they shared with you.

Held
An actor claims support tickets and attachments; the post advertises 6028 users.

Not established
That all tickets or attachments are held, affected customers, current access or technical impact.

4.5 Additional evidence cards

The remaining cards show identifier advertising, identity-image demand, session buying and a recent casino-themed offer. The original excerpts are retained advertisement text with identifying material removed. They are not instructions or validated product descriptions. [S3]

Evidence card B07 — 13 Apr 2026

[alias withheld] | Leak forum | Forum | English

ORIGINAL

I SELL 40K+ BELGIUM IBANS PRICE : 1000 IBANS = 1,75$ (USD) ALL IBANS = 70,19$ (USD)

Held
A seller advertises bank-account identifiers with a country label and asking prices.

Not established
Access to accounts, usable payment authorisation, a named bank incident, or a completed sale.

Evidence card B08 — 24 Feb 2026

Crazy88 | Leak forum | Forum | English

ORIGINAL

Hello i'm looking for a seller that can provide belgium ids i need a lot of them 500+

Held
A buying request for Belgian identity documents.

Not established
Any supplied document, completed purchase, successful identity verification or source breach.

Evidence card B09 — 3 Nov 2026

buylogs | Leak forum | Forum | English

ORIGINAL

I will buy requests from your logs EXPENSIVELY - cookies with active email [...] 250-2500 (fixed and percentage possible)

Held
A buying request names logistics platforms and active email cookies, with an asking range.

Not established
A seller response, purchased sessions, account validity, a completed sale or a platform breach.

Evidence card B10 — 21 Nov 2026

WSdatabase | Leak forum | Forum | English

ORIGINAL

Belgium Casino User Database 2026

Held
The 21 November advertisement and a displayed contact-data sample with claimed deposit fields.

Not established
The source casino, dataset freshness, deposit accuracy, current account access or a new intrusion.

An IBAN offer quotes USD 1.75 for 1,000 identifiers and USD 70.19 for the whole advertised package. The quantities are not an exact verified inventory. An IBAN is not authority to move money. [S3]

A logistics-session request displays a USD 250–2,500 range. It establishes demand and an asking range, rather than account validity or completed trade. The defensive relevance is session recovery and independent verification of payment changes. [S3]

4.6 Recent activity in the retained forums

Post date	Card	Advertisement	Boundary
2026-11-13	B06	Supplier support tickets and attachments	Customer names in a claim do not establish customer impact
2026-11-20	B05	Bank-specific phishing templates	Marketing is not proof of deployment or a bank-system incident
2026-11-21	B10	Casino-themed customer data	Similar September advertising does not establish identical files or a fresh incident

The identity-service offer in B04 is dated 8 November and falls outside the recent period. Its proximity to later notices does not link it to them. No shared operator or common incident is inferred. [S3]

A 22 November advertisement again offered bank-impersonation templates and claimed interactive authentication features. Another multinational commodity advertisement included Belgium in its price list. These observations do not establish working access, verified card validity or a new bank intrusion. [S3]

4.7 What the forums add

The forums make the wording and timing of claims visible. A population-data poster concedes uncertainty about provenance. A telecom advertiser supplies an older incident date. An access seller repeatedly describes its tables as proposed.

Those details help an investigator ask better questions. They do not settle authenticity. A title, row count or schema can be copied, partially true, outdated or fabricated. The report preserves those alternatives instead of treating all advertisements as equivalent breaches.

KEY TAKEAWAYS

01
Post dates identify advertising, not intrusion dates.

02
Validate provenance and working access separately.

03
Recent fraud-tool marketing supports preparation, not a claim of successful attacks.

CHAPTER 05

Confirmed incidents and claims by sector

05

THIS CHAPTER ANSWERS

Which outcomes were established, and which numbers still belong to a claimant?

3

separate questions: availability, data exposure and attribution

5.1 How to read the incident register 37

5.2 Healthcare and learning services 37

5.3 Municipal and shared public services 40

5.4 Membership, customer and operational data 42

5.5 Other recorded incidents and reported claims 43

5.6 Additional business, research and local-service cases 45

5.7 What these cases establish 47

CHAPTER 05

Confirmed incidents and claims by sector

IN SHORT

Belgium's public record covers interrupted healthcare, exposed membership information, education platforms, municipal systems and shared suppliers. Several organisations confirmed an incident while leaving the number of affected people unresolved. Restoration and data-loss assessments sometimes changed on different dates. The case cards preserve those distinctions. Use the closest operational example to test your own containment, customer notice and recovery decisions.

5.1 How to read the incident register

A confirmed incident does not confirm every criminal claim attached to it. The register separates direct organisational statements, official warnings, attributed reporting and underground advertisements. The cases below are selected dossiers, not a national census.

Some foreign services hold Belgian users' data. They belong in the dependency picture, but a worldwide user count is not a Belgian affected count. Repeated advertisements and related federation notices are not automatically independent incidents.

Names appear only when official confirmation and wider reporting support them. Other organisations have broad role labels. A role label protects identity; it must not conceal uncertainty about the event itself.

5.2 Healthcare and learning services

G

CASE G

A hospital isolates systems in January

Healthcare

Attributed public account

EVENT	A Belgian hospital network detected a serious IT disruption on 13 January. Its statement, quoted in reporting, described a precautionary shutdown across its campuses. [S10]
CHRONOLOGY	Scheduled care was interrupted and critical patients were transferred. The retained January account does not establish a ransom payment, a named attacker or the full data-loss scope.

ESTABLISHED	Clinical continuity depended on the ability to work with digital systems unavailable. A shutdown decision can protect systems while creating immediate operational costs.
ALTERNATIVES AND LIMITS	Service disruption alone cannot distinguish encryption, containment or another technical cause. Later criminal claims require their own evidence.
RESPONSE	Clinical leadership should rehearse manual documentation, patient transfers and communication with neighbouring providers. Record which systems must be restored before normal scheduling resumes.

Bottom line

Use the stated scope and preserve the unresolved questions.

H

CASE H

Basic-Fit confirms a cross-border customer-data incident

Consumer services

Attributed public account

EVENT	Safeonweb relayed company confirmation on 13 April that Belgian members were among those involved in a customer-data incident. Reuters also reported the company statement. [S11][S12]
CHRONOLOGY	The disclosure described information linked to members across several countries. The figure of about one million relates to the wider international population, not Belgium alone.
ESTABLISHED	Potentially affected data included contact, birth-date and bank information. The company said passwords and identity documents were not taken. [S11]
ALTERNATIVES AND LIMITS	A bank-account identifier is not evidence of access to the holder's bank account. The retained sources do not establish a Belgian affected-person count.
RESPONSE	Warn customers about messages that quote real membership details. Support teams should verify identity through a separate trusted process before changing contact or payment information.

Bottom line

Use the stated scope and preserve the unresolved questions.

CASE I

A learning-platform incident raises Belgian dependency questions

Education

Attributed public account

EVENT	Safeonweb's 6 May warning described a vendor-confirmed incident at an online learning platform used in Belgium. The vendor's confirmation was dated 1 May. [S13]
CLAIM	A criminal group advertised a worldwide population of 275 million users. Safeonweb explicitly described that number as unconfirmed. It is not a Belgian count.
ESTABLISHED	Possible data categories included names, email addresses, student identifiers and messages. The vendor reported no indication at that time of password, birth-date, official-ID or financial-data involvement.
ALTERNATIVES AND LIMITS	A platform-wide claim cannot establish which records were taken from a particular institution. Institutional notifications and service restoration answer different questions.
RESPONSE	Education providers should request a scoped impact statement, prepare student notices and review staff support workflows. Treat unexpected course-related messages as a customer-protection concern.

Bottom line

Use the stated scope and preserve the unresolved questions.

The CCB's second-quarter report also discusses a healthcare-software supplier incident relevant to Belgium. That establishes a dependency concern; it does not establish that every client hospital suffered data theft. [S8]

5.3 Municipal and shared public services

CASE J

J

Machelen's data-loss assessment changes after the initial incident

Local government

Attributed public account

EVENT	The municipality identified a cyber incident on 11 September. Its own update says that further analysis confirmed personal-data theft on 22 September. [S15][S16]
CHRONOLOGY	Digital services were affected. The captured municipal notice says service had become operational again, with possible delays, while the data-loss investigation continued.
ESTABLISHED	The incident date, confirmation date and restoration state are different facts. The initial uncertainty did not prevent the municipality from providing later updates.
CLAIM	A later extortion listing is recorded in the report's ransomware population. The listing does not independently establish the complete data set, attack method or identity of the intruder. [S1]
RESPONSE	Maintain an update page with dated changes. Give residents practical protective advice while explaining which data categories and affected people remain under investigation.

Bottom line

Use the stated scope and preserve the unresolved questions.

CASE L

L

A digital-signature supplier affects local-government workflows

Shared public services

Attributed public account

EVENT	Reporting on 26 October quoted a supplier's chief executive describing unauthorised access to a digital-signature service. Suspicious activity had been detected on 23 October. [S22]
CHRONOLOGY	The supplier took the service offline and restored it the following evening with restrictions. Customer-specific impact assessments were being prepared.

ESTABLISHED	The supplier said mainly metadata was involved and said fraudulent signatures had not been created. Those are attributed company statements, not an independent forensic conclusion.
ALTERNATIVES AND LIMITS	More than 120 local authorities used the module. That customer population is not an affected-authority count. A separate integration population must not be added to it.
RESPONSE	Ask for the impact on your own documents, identities and integrations. Review replaced access permissions and test payment notices through a known official channel.

Bottom line

Use the stated scope and preserve the unresolved questions.

M

CASE M

Federal tax services restore applications in stages

Government

Attributed public account

EVENT	SPF Finances/FOD Financiën confirmed a cyberattack on 28 October. Its recovery notice says it contained the incident within hours and temporarily took applications offline. [S23][S24]
CHRONOLOGY	Main services returned on 31 October. A withholding-tax function returned on 6 November, and e604 on 12 November. These are restoration milestones, not separate intrusions.
ESTABLISHED	The authority stated that its investigation found no data exfiltration and no attacker control of applications. Attribute that conclusion to the authority and its investigation. [S23]
ALTERNATIVES AND LIMITS	A preventive shutdown is a real availability impact. It does not prove data theft, and restoration alone would not establish its absence.
RESPONSE	Exercise staged recovery and communicate which functions remain unavailable. Keep technical containment, user impact and confidentiality findings in separate sections of the incident record.

Bottom line

Use the stated scope and preserve the unresolved questions.

5.4 Membership, customer and operational data

K

CASE K

A fitness-chain incident and a larger criminal headcount

Consumer services

Attributed public account

EVENT	A fitness-club chain acknowledged an incident affecting membership information. Reporting quoted its spokesperson describing records linked to at most 31 of its 85 Belgian clubs. [S18]
CLAIM	The widely repeated figure of 150,000 members was attributed to the people advertising the data. It must not become a company-confirmed affected count.
ESTABLISHED	The reported categories included identity, contact and membership details, and some bank-account identifiers. The company said passwords and health data were not involved. [S18]
ALTERNATIVES AND LIMITS	Clubs, members, prospects and advertised records are different units. Dividing a claimed headcount by the club count would not establish exposure per club.
RESPONSE	Notify the people identified by the company's investigation and prepare for tailored impersonation. Do not authenticate a caller merely because they know a membership or bank-account detail.

Bottom line

Use the stated scope and preserve the unresolved questions.

N

CASE N

Refrigeration disruption makes remote access an operational issue

Retail operations

Attributed public account

EVENT	Official warnings and public reporting describe a November incident affecting retail refrigeration. Changed operating conditions created consequences for stores and stock. [S25][S27]
CHRONOLOGY	Belgian disruption was reported on 2 November. Further technical advice and attributed statements followed. Different reports counted stores, equipment and suppliers' customer populations.

ESTABLISHED	Operations teams need to control remote access and retain the ability to restore safe settings. The public sources do not justify adding all reported equipment and store counts together.
ATTRIBUTION	Reuters reported conflicting ministerial assessments on 13 November. This report does not resolve that disagreement or independently attribute the campaign. [S26]
RESPONSE	Immediately remove direct public internet access to refrigeration management interfaces. Operations and security should coordinate safe continuity and protected remote maintenance, restrict accounts to approved needs, and rehearse a safe local mode. Verify safe settings and retain evidence that the interfaces are no longer directly reachable. [S25]

Bottom line

Use the stated scope and preserve the unresolved questions.

CASE O

A recent gift-voucher service notice

Consumer services

Attributed public account

EVENT	Safeonweb warned on 20 November about unauthorised access to a gift-voucher platform. Its notice relayed the company's finding and said the investigation was continuing. [S29]
ESTABLISHED	Names and email addresses may have been viewed. According to the company, passwords and payment-card data were not affected at that stage.
ALTERNATIVES AND LIMITS	The notice did not provide a Belgian affected-customer count. The ability to send convincing follow-up messages is a plausible risk, not proof that a particular scam already used these records.
RESPONSE	Customer teams should publish a short warning on the service's normal channels. Advise users to open the official app or website directly when checking an unexpected message.

Bottom line

Use the stated scope and preserve the unresolved questions.

5.5 Other recorded incidents and reported claims

These rows preserve additional incident coverage without treating every account in the press as a verified technical finding.

Period	Broad role	Evidence and limit	Defender implication
June	A sensitive public agency	Reporting described a mobile-management incident spanning 2025 and spring 2026; official confirmation and attribution were unresolved [S14]	Investigate management-plane access without assuming the internal intelligence network was reached
September	A sports federation	Reporting quoted confirmation of a membership-database incident; the complete scope was not independently established [S17]	Prepare membership notices and review outsourced administration
September	A related sports membership administration	A federation and its wing were discussed together; advertised record counts remain claims [S17]	Keep one campaign dossier when the evidence concerns related systems
October	A school group	A director confirmed an incident affecting pupils and staff; 3,550 plus 650 is 4,200 people in the reported population [S19]	Review staff access and support processes, including home-address sensitivity
October	A vocational-training network	Reporting described republication of data attributed to a February incident; 700,000 records and 85,000 bank details were reported figures [S20]	A repost can renew phishing risk without establishing a new intrusion
October	A public e-learning platform	Reporting described a service closure and a separate advertised data count [S21]	Treat availability and the data claim as separate validation tasks
November	An employee-benefits payment service	Official warning described possible account-data exposure; the company had not identified payment-system problems or suspicious transactions [S28]	Warn account holders without describing unverified payment loss
April	An online booking service	Safeonweb relayed possible reservation-data access and changed reservation PINs; the company said financial data was not accessed [S11]	No Belgian affected-user total was established

5.6 Additional business, research and local-service cases

R

CASE R

A research institute confirms copied data while services continue

Medical research

Attributed public account

OFFICIAL ACCOUNT	A specialist medical and research institute's notice describes unauthorised access to and copying from a database after detection on 12 October. The notice was updated on 10 November. [S49]
ESTABLISHED	The institute says most copied information was coded, with a smaller amount directly identifiable. Its current findings did not identify effects on other systems; care and teaching continued.
LIMITS	Coded data is not automatically anonymous. A separately reported notification headcount does not measure the entire copied database, and the report supplies no combined affected-person total.
RESPONSE	Research and privacy teams should assess coding and identification risk together. Identify who holds the linking information, document the affected projects and prepare proportionate participant communication.

Bottom line

Use the stated scope and preserve the unresolved questions.

S

CASE S

A professional body's contact population needs a precise denominator

Professional services

Attributed public account

OFFICIAL ACCOUNT	A professional legal body's 6 November update says it was informed of the incident on 29 October. It describes access involving an administrative application and advertised contact information. [S50]
ESTABLISHED	The update identifies approximately 27,500 contacts who are not lawyers, in addition to lawyer records. It does not give one total affected population.
LIMITS	The body says its analysis did not identify banking or special-category personal data in the affected population. This is the body's assessment, not an independent verification of every advertised file.

RESPONSE

Keep professional and external-contact populations separate. Warn recipients about messages using genuine contact details and validate the scope before reusing an advertiser's larger count.

Bottom line

Use the stated scope and preserve the unresolved questions.

The following additional cases widen the service picture. They do not all establish data theft or ransomware.

Period	Broad role	What the source supports	Limit
April	A municipality	The mayor described disruption and data theft; restoration was gradual [S53]	Original municipal statement not retained; no complete affected-person count
May	A chemical manufacturer	Its own clarification describes unauthorised access and says forensic work found no evidence of exfiltration or ransomware [S47]	Later publicity concerns the same May event
May	A recycling-park operator	Its follow-up scopes the incident to an external supplier computer; operations were isolated as a precaution [S48]	No indications of exfiltration in the stated investigation
July	A supermarket's external customer-data supplier	Reporting quotes a company statement about contact data on a separate supplier server [S51]	Do not generalise to payment systems or every customer
August	A furniture retailer	A spokesperson described short disruption and access to customer contact and order information [S52]	Criminal attribution remains a claim
October	A travel operator	A spokesperson confirmed a data incident and customer warning [S56]	The origin of personalised fraud messages remained unresolved
October, reported in November	A precious-metals dealer	Reporting quotes confirmation of customer-system access [S54]	A proposed connection to burglaries was not established
November	A municipal public website	A mayor described website access and possible staff-account exposure [S55]	No finding of citizen-data exposure or access to separate municipal services

A charging-account service supplies recent cross-border context. Its own FAQ describes an 8 November attack, discovery on 10 November and remediation on 12 November. It notified users on 18 November. A Belgian affected count is not established. [S46]

VRT reports more than 3.5 million European users; that population is not an affected-account count. [S71] The company identifies account and profile information, including password hashes, while excluding several other categories in its notice. Individual Belgian service providers should validate their own dependency and users. [S46]

5.7 What these cases establish

The strongest repeated pathway is a gap between the service boundary and the organisational boundary. Members use a platform, staff rely on a supplier and residents depend on an administrative application. Incident response must identify the actual dependency.

The cases also show why clear reporting matters. A confirmation can narrow a criminal claim without eliminating every risk. A restoration notice can help users resume work while the data investigation continues.

The report does not add customer counts, claimed records, organisations and store counts into one headline. Such a total would measure nothing consistent. Leaders should ask which service, data category and person requires action now.

KEY TAKEAWAYS

01

Keep restoration, data exposure and attribution as separate findings.

02

Supplier client populations are not affected-victim totals.

03

Reposted data can renew fraud risk without proving a new intrusion.

CHAPTER 06

Hacktivism, disruption and operational systems

06

THIS CHAPTER ANSWERS

What was observed, what was claimed, and how should services remain usable during disruption?

9–22 November

the recent-activity period, within the wider annual window

6.1 Timeline 49

6.2 Claim against public account 50

6.3 A website incident is not an equipment incident 50

6.4 Recent activity: 9–22 November 51

6.5 Decisions during a short disruption 51

CHAPTER 06

Hacktivism, disruption and operational systems

IN SHORT

The public record supports preparation for both website disruption and operational consequences. The CCB reported no hacktivist DDoS incidents in the first quarter and a limited return in the second. November refrigeration incidents show a different continuity problem. Actor statements and political explanations do not establish technical impact. Prepare status communications, service alternatives and controlled remote access before the next disruption.

6.1 Timeline

13 Jan 2026	**Hospital statement, as quoted in reporting** Precautionary system shutdown and interrupted care [S10]
22 Apr 2026	**CCB quarterly report** No hacktivist DDoS incidents reported for the first quarter [S7]
15 Jul 2026	**CCB quarterly report** A limited, one-day return of DDoS activity described for the second quarter [S8]
11 Sep 2026	**Municipal incident notice** Digital service interruption, followed by a later data-theft confirmation [S15]
28 Oct 2026	**Federal tax administration** Applications temporarily taken offline after an incident [S23]
2 Nov 2026	**Retail refrigeration reporting** Belgian equipment disruption reported [S25][S27]
9 Nov 2026	**CCB identity assessment** Account protection remains a priority [S5]
10 Nov 2026	**Medical research institute** Its incident statement is updated; this is not a new intrusion [S49]
12 Nov 2026	**Federal tax administration** e604 restoration update [S23]
13 Nov 2026	**Reuters** Differing ministerial assessments of refrigeration attribution [S26]
17 Nov 2026	**Safeonweb** Warning about fake pellet and firewood offers [S45]
18 Nov 2026	**Charging-account service** Users notified after earlier detection and remediation; Belgian affected count unavailable [S46]

20 Nov 2026 **Safeonweb**
Gift-voucher service warning relays ongoing investigation [S29]

An official row identifies the source of the account. It does not mean that the source independently verified every attacker statement mentioned in that account. A relay row identifies reporting rather than an original actor post.

6.2 Claim against public account

Point	Claim or interpretation	Official account	Assessment
Website availability	An actor may advertise a site as unavailable	CCB reports describe their own observed incident population [S7][S8]	A screenshot or a post does not establish outage duration or national impact
Tax-system shutdown	Unavailability may be described as successful access	The authority says applications were isolated and no exfiltration or application control was found [S23]	Attribute the findings to its investigation
Refrigeration responsibility	A state may be named in political commentary	Reuters records differing ministerial assessments and an ongoing investigation [S26]	Attribution remains unresolved in this report
Refrigeration scale	Equipment, stores and customers appear in different accounts	Official warnings describe the operational risk [S25] [S27]	Do not combine incompatible denominators

6.3 A website incident is not an equipment incident

A website can be unavailable while internal operations continue. An operational interface can change equipment behaviour while the corporate website remains online. Their telemetry, owners and recovery decisions differ.

For public websites, agree how traffic mitigation is requested and how legitimate users retain access. Preserve availability measurements and the time zone. Avoid statements that infer data access from a denial-of-service claim.

For refrigeration equipment, immediately remove direct public internet access to management interfaces. Operations and security should coordinate safe continuity and protected remote maintenance. Verify that management interfaces are no longer directly reachable. [S25]

For operational equipment, involve the team responsible for safe settings. Test what happens if the supplier's remote route is removed. Verify that the local recovery process remains safe and that emergency access is logged.

The refrigeration case does not establish that all connected household appliances face the same exposure. Safeonweb's public advice distinguishes general device protection from the particular commercial incidents. [S27]

6.4 Recent activity: 9–22 November

The recent window is an observation period, not a forecast. The CCB's 9 November identity report describes current defensive priorities using earlier reporting populations. Its publication date does not move those underlying incidents into November. [S5]

On 12 November, the tax administration's notice recorded another application restored after the October incident. On 13 November, Reuters recorded attribution uncertainty around refrigeration. Neither is a new independent attack count. [S23][S26]

Safeonweb's 20 November gift-voucher warning adds a customer-data concern. It reports possible disclosure and an ongoing investigation, with no Belgian headcount. Treat this as a trigger for scoped customer communication. [S29]

The recent underground evidence is assessed separately in Chapter 4. A new advertisement can concern old data. It can also promote a tool whose actual use has not been established. Post dates measure the advertisements, not their underlying incidents. [S3]

6.5 Decisions during a short disruption

Agree the minimum information needed to activate traffic protection, isolate a supplier integration or switch to a manual process. Waiting for attribution can prolong disruption without improving the initial containment decision.

Use one public status channel and update it with explicit timestamps. Say which services work, which do not and what users should do. Describe data access only when evidence supports it.

Preserve the distinction between a precaution and a finding. An organisation may isolate a system because it cannot yet rule out risk. That is not a statement that every connected system was affected.

KEY TAKEAWAYS

01
Measure service availability separately from criminal claims.

02
Operations teams must own safe equipment recovery.

03
Recent publication dates do not turn older incidents into new attacks.

CHAPTER 07

Threat actors and evidence relationships

THIS CHAPTER ANSWERS

Which actor labels are observed, and what relationship can each item actually support?

22

ransomware group labels in the retained Belgian listing population

7.1 How the evidence connects 53

7.2 Extortion: a distributed listing population 54

7.3 Advertising personas 58

7.4 Espionage and unresolved intrusion reporting 58

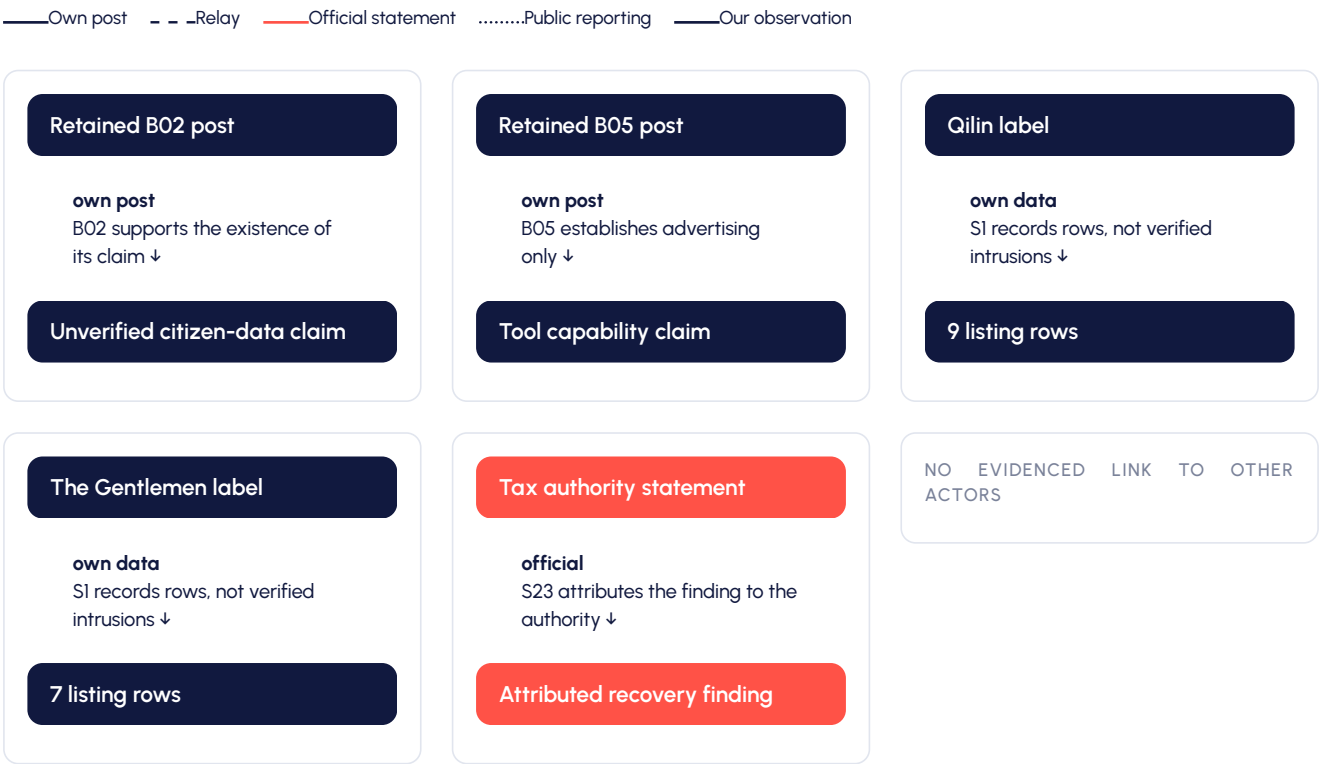
CHAPTER 07

Threat actors and evidence relationships

IN SHORT

The evidence contains extortion labels, advertising personas and campaigns described by authorities. These are different kinds of identity. A common sector, language or political theme does not link operators. The report's relationship map connects evidence to a proposition, rather than joining unrelated groups. Build the response around validated access, service impact and recovery needs; use attribution when it improves those decisions.

7.1 How the evidence connects



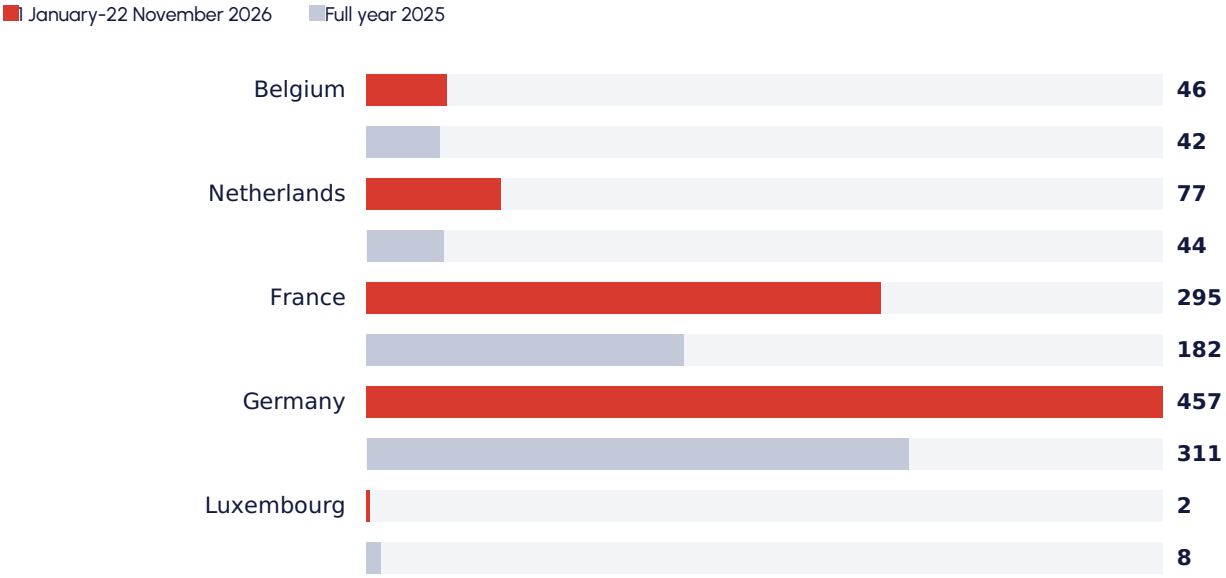
The map shows a retained advertisement supporting its own claim, a listing supporting an extortion assertion and public sources supporting a stated outcome. It does not infer a shared operator between those populations.

Matching titles can establish similar advertising. A repeated alias can establish use of that persona. Neither establishes identical files, a completed transfer or the identity of a person behind the account. No common criminal organisation is inferred from these similarities. [S3]

The relationship between reused credentials, account abuse and fraud is an analytical model of a possible pathway. The police describe that pathway in specific investigations. It does not mean the forum sellers in this report supplied those investigated campaigns. [S31][S32]

7.2 Extortion: a distributed listing population

Belgium has 46 listings in the partial-year window, with different totals across four regional peers



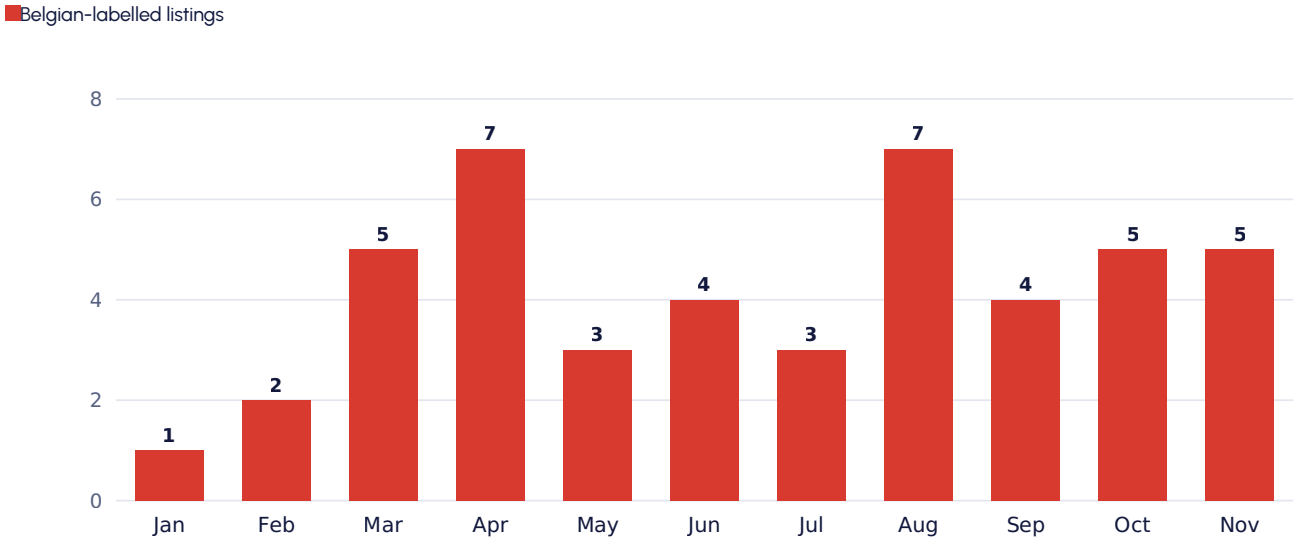
Unmatched periods; not a national risk ranking. Source: Brandefense Ransompedia accepted country-labelled listings, 1 January-22 November 2026; November partial. Listing dates are not incident dates [S1].

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

Country	2026 window	Full 2025	Comparison limit
Belgium	46	42	Listings, not confirmed intrusions
Netherlands	77	44	Neighbouring logistics and Dutch-language market
France	295	182	Neighbouring French-language and enterprise market
Germany	457	311	Neighbouring industrial and trading economy
Luxembourg	2	8	Neighbouring financial-services market with a small listing population

All 2026 figures cover the same report window. They are not adjusted for business population, economic size, reporting propensity or source visibility. The table cannot establish that a Belgian organisation is safer or more exposed than a peer. [S1]

Belgian listings appear throughout the year, rather than in one single month

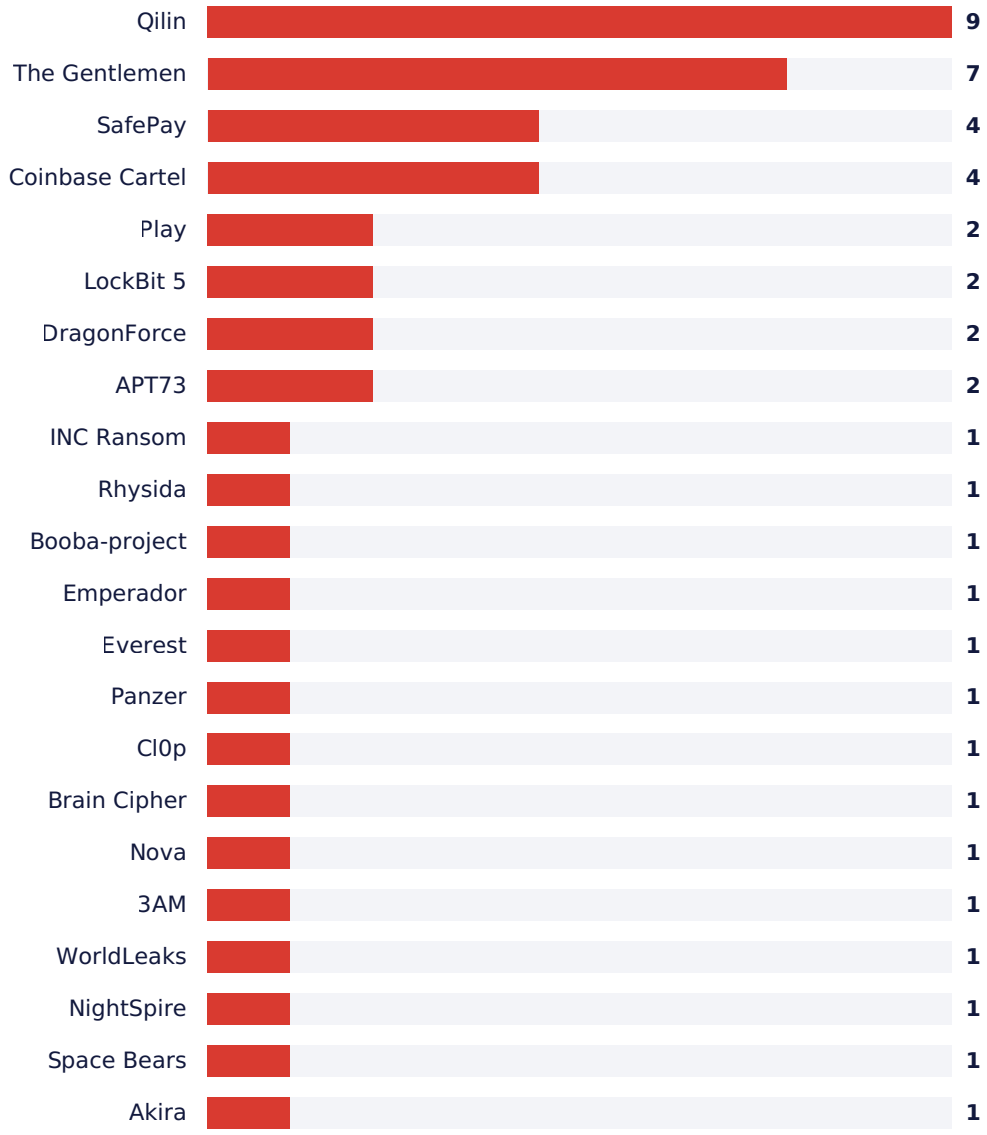


Source: Brandefense Ransompedia accepted country-labelled listings, 1 January–22 November 2026; November partial. Listing dates are not incident dates [S1].

The monthly listing counts are 1, 2, 5, 7, 3, 4, 3, 7, 4, 5 and 5 from January through the November cutoff. Their sum is 46. Partial November must not be compared with a full month as a trend forecast. [S1]

Four group labels account for 24 of the 46 Belgian listings





Source: Brandefense Ransompedia accepted country-labelled listings, 1 January–22 November 2026; November partial. Listing dates are not incident dates [S1].

Qilin has 9 listings, The Gentlemen 7, SafePay 4 and Coinbase Cartel 4. Together they account for 24 of 46 listings. The remaining 22 listings are distributed across 18 other labels. [S1]

Qilin

Extortion listing label | No state attribution made

IN BELGIUM, 2026

2026

9 · Belgian-labelled listings in the report window; not confirmed intrusions

CLAIMED TARGETS

Sector and country labels require validation; no victim list published

SEEN IN PUBLIC REPORTING

[S1] Retained listing aggregate, not independent actor attribution

OUR ASSESSMENT

Prepare recovery and validate any claim without relying on the actor label

CONFIDENCE

High confidence in the retained row count; intrusion outcomes unverified

The Gentlemen

Extortion listing label | No state attribution made

IN BELGIUM, 2026

2026

7 · Belgian-labelled listings in the report window; not confirmed intrusions

CLAIMED TARGETS

Sector and country labels require validation; no victim list published

SEEN IN PUBLIC REPORTING

[S1] Retained listing aggregate, not independent actor attribution

OUR ASSESSMENT

Prepare recovery and validate any claim without relying on the actor label

CONFIDENCE

High confidence in the retained row count; intrusion outcomes unverified

The country label is retained as a listing attribute, not accepted as proof of domestic legal jurisdiction. The listing population includes repeated brand descriptions and a foreign operating unit. Possible organisation overlaps remain distinct listing rows; no unique-victim total is asserted. [S1]

7.3 Advertising personas

Persona	Cards	Observed proposition	Limit
kazutlg	B01	Telecom-themed customer-data advertisement	Advertiser itself dates the incident to 2025
xmlrpc	B02	Citizen-data claim with admitted source uncertainty	Government provenance unverified
yneov18	B03	Training-network data and access claims	Current access and unique-person count unverified
DataJava	B04	Claimed identity-service administration	Proposed table descriptions do not validate access
0xcasper	B05	Bank-template phishing-panel marketing	Working capability and deployment unverified
updap	B06	Supplier support-ticket data claim	Customer impact and complete possession unverified

These are retained account aliases. They are not identified individuals, and their names do not authenticate an advertisement. An alias associated with one accurate item would not validate every later claim. [S3]

7.4 Espionage and unresolved intrusion reporting

The CCB discusses state-sponsored espionage as part of the threat environment. A reported incident at a sensitive public agency is not independently confirmed in the retained official record. The report therefore uses a broad role and attributes the account to reporting. [S8][S9][S14]

The CCB's third-quarter report describes isolated activity that it links to Russia, China and Iran. It also reports a Teams spear-phishing campaign observed in Belgium. These are the authority's assessments. [S9]

The public vendor and NVD records for two mobile-management vulnerabilities establish a product risk. They do not establish which vulnerability, actor or data outcome applied to that reported Belgian incident. [S41][S42][S43]

Record	Affected scope	Vendor's resolved versions	Boundary
CVE-2026-1281	NVD lists versions through 12.5.0.0 and specific later vulnerable builds including 12.5.1.0, 12.6.0.0, 12.6.1.0 and 12.7.0.0	See the release register below	Check the product branch and current vendor guidance
CVE-2026-1340	NVD lists affected EPMM versions through 12.7.0.0	See the release register below	No inference about an individual Belgian deployment

Ivanti EPMM fixed releases, as listed by the vendor [S41]:

`12.6.1.1, 12.7.0.1, 12.8.0.1`

Ivanti's advisory describes both as unauthenticated code-injection risks. Its product exclusions include Sentry and its cloud mobile-management product. A remediation decision must match the installed product and branch. The two NVD records were checked for this report. [S41][S42][S43]

No incident-specific ATT&CK matrix is supplied for the unconfirmed agency account. A generic technique mapping would risk turning product capability into an observed Belgian attack sequence.

KEY TAKEAWAYS

01
Group labels and personas are not verified operator identities.

02
Regional listing totals do not measure comparative attack probability.

03
Product vulnerabilities do not independently attribute a reported Belgian incident.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How could advertised data, documents and access support fraud, and where can defenders interrupt it?

2

police campaign cases with concrete response lessons

8.1 From correct details to a false instruction 61
8.2 Police campaign case cards 61
8.3 Identity images, sessions and onboarding 63
8.4 Payment-card material in posts: a narrow view 63
8.5 Prices are asking prices 63
8.6 Public campaign warnings throughout the year 64

CHAPTER 08

The fraud economy

IN SHORT

Retained advertisements offer identifiers, identity images, sessions and bank-themed tools. Police and Safeonweb describe practical fraud pathways involving impersonation, altered invoices and malicious applications. Those public campaigns are not attributed to the forum personas. Payment-card observations remain a very narrow view. Protect recovery, payment changes and customer communication through independent verification and a clear route for urgent fraud reports.

8.1 From correct details to a false instruction

Real personal information can make a fraudulent message credible. It cannot authenticate the sender. The training, membership and supplier cases explain why customer support and finance need protective controls even when passwords were reportedly unaffected. [S13][S18][S22]

The police's May warning describes criminals using previously leaked mailbox credentials, monitoring incoming messages and altering invoices. It attributes increasing automation to the observed fraud pattern. This report does not independently measure AI's share of that activity. [S31]

The decisive control is independent verification of the instruction. Use an already known contact route before accepting a changed beneficiary or emergency transfer. A familiar mailbox, accurate invoice amount or correct customer name is insufficient by itself.

8.2 Police campaign case cards

P

CASE P

An investigation targets a phishing-panel supplier

Fraud services

Attributed public account

OFFICIAL ACCOUNT	Federal Police announced an investigation on 22 April into a suspect alleged to create and sell phishing panels. The statement describes use of those tools in fraud across Belgium and other European countries. [S30]
CHRONOLOGY	The police described a January search and an April transfer of the suspect to Belgium. Those procedural dates differ from the announcement date.

ESTABLISHED	The statement supports a crime-service pathway: a supplier offers tools that other criminals can use. It does not connect that suspect to B05 or any persona in the retained forums.
LIMITS	An arrest and police allegations are not a conviction. Do not infer a national victim or loss total from this individual investigation.
RESPONSE	Make phishing-resistant authentication and payment verification part of the same fraud exercise. Record how a user can report an intercepted authentication interaction.

Bottom line

Use the stated scope and preserve the unresolved questions.

CASE Q

Q ■ Fake bank staff combine messaging, calls and remote access

Bank impersonation

Attributed public account

OFFICIAL ACCOUNT	A 2 July Federal Police statement describes an investigation involving dozens of Belgian victims and alleged proceeds exceeding EUR 500,000. The investigation was continuing. [S32]
CHRONOLOGY	Police say the investigation began in March and a principal suspect was arrested on 29 June. The July publication is not the start of every reported offence.
PATHWAY	The official account describes messages impersonating public bodies, a subsequent call from a fake bank employee and inducement to install remote-control software.
LIMITS	The proceeds figure is alleged, rather than a national fraud-loss estimate. No common operator with this report's underground advertisements is established.
RESPONSE	Customer teams should tell users to end unexpected calls and contact the bank independently. Fraud teams need an urgent escalation route for remote-access and new-beneficiary concerns.

Bottom line

Use the stated scope and preserve the unresolved questions.

8.3 Identity images, sessions and onboarding

The B08 request seeks more than 500 Belgian identity images. It establishes demand only. It does not establish a supplier response, a successful identity check or theft from a government registry. [S3]

The B09 request seeks active sessions associated with logistics services. Sessions can present a different response problem from a password alone. Review active sessions and recovery routes when the organisation has validated a relevant finding. [S3]

Do not turn document possession into sole identity proof. Onboarding and recovery teams should test the circumstances in which a real document image, contact address or old account identifier could be misused. Record an escalation route for uncertain cases.

8.4 Payment-card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

These limited observations do not estimate total card theft, active cards, bank-system intrusion or fraud loss.

The retained material associates 3 distinct payment-card numbers with Belgium, across 9 posts and 17 appearances. No named Belgian issuer attribution is established for these three cards. Repeated appearances are not additional cards. [S3]

These observations cannot establish whether a card remained active or whether any attempted payment succeeded. Issuers should use their own fraud evidence before recommending blocking or reissue. The card population must not be added to credential or customer-record counts.

8.5 Prices are asking prices

Product advertised	Displayed price	Evidence limit
Bank-account identifiers	USD 1.75 per 1,000; USD 70.19 for the advertised package	Quantity, provenance and payment authority unverified
Claimed identity-service administration	USD 4,550	Working access and advertised record population unverified
Logistics-related sessions	USD 250–2,500	A buying range, not a completed transaction

The prices describe the retained advertisements. They do not establish clearing prices, revenue, profitable activity or the size of a Belgian underground market. Differences in claimed scope prevent a simple price comparison. [S3]

8.6 Public campaign warnings throughout the year

Period	Official warning	Decision supported
January	High-profile invitation and sponsorship impersonation [S65]	Verify requests through an established business contact
February	Government sign-in impersonation [S62]	Open the official service directly
March	Fake compensation and recovery messages [S63]	Do not send identity documents to an unverified recovery contact
June	Hotel messages with accurate reservation details [S61]	Verify payment requests with the accommodation independently
September	Executive impersonation over collaboration software [S60]	Treat a familiar organisational identity as a claim to verify
September	Malicious-app and mobile card-relay fraud [S59]	Refuse unsolicited app installation and contact the bank separately
October	Messaging-account linking through fake voting requests [S64]	Verify unexpected requests even when they arrive from a known contact
November	Fake winter-fuel shops and advance-payment offers [S45]	Check seller identity and payment terms before ordering

These are prevention and campaign notices. They are not eight disjoint victim populations. The hotel warning, for example, does not establish that the earlier booking-platform incident supplied the information used in those messages. [S61]

KEY TAKEAWAYS

01

Correct personal information does not authenticate a payment request.

02

A tool advertisement is separate from an observed fraud campaign.

03

Card appearances and asking prices do not measure losses or completed trade.

CHAPTER 09

Banking and finance deep dive

09

THIS CHAPTER ANSWERS

Which identity and customer-protection signals should the banking portfolio validate first?

11 of 25

selected banking and finance domains had a current credential listing

9.1 What the evidence does and does not say 66

9.2 Separate the account, session and payment decision 66

9.3 Suppliers and regulatory coordination 67

CHAPTER 09

Banking and finance deep dive

IN SHORT

11 of 25 selected banking and finance domains had a current credential listing. The sector records at least 13,221 device associations, including 156 employee-classified associations, and 190,956 credential records. The three post-based cards have no named issuer attribution. These observations measure different populations. Coordinate identity, fraud and customer support around validated accounts, sessions and payment activity.

9.1 What the evidence does and does not say

Population	Available result	Interpretation
Selected banking and finance domains	25	Includes finance services; not a census of licensed card issuers
Device associations	At least 13,221; 156 employee-classified	Classification does not establish ownership or an enterprise intrusion
Credential records	190,956	Overlapping historical sources, not unique active accounts
Current credential listings	11 of 25 domains	Validate freshness, account validity and previous remediation
Issuer-domain subset	7 matched domains; 6 with current listings	86 employee and 4,306 non-employee device associations; a subset of the sector
Bank-template advertising	Observed in B05	An impersonation product claim, not a bank-system intrusion
Payment-card material	3 cards; 9 posts; 17 appearances	No named issuer attribution; no card-loss or bank-intrusion estimate

No retained card was attributed to a named issuer. This does not establish the absence of stolen cards. Non-employee associations do not independently establish customer ownership. [S2][S3]

9.2 Separate the account, session and payment decision

An exposed identifier can help personalise a call. A valid session can support account activity. A payment instruction can move funds only within the relevant authorisation process. Investigate those propositions separately rather than treating one as evidence of all three.

When fraud staff receive a report of remote-control software or an unexpected authentication request, route it quickly to account protection. Verify new beneficiaries and recovery changes through an independent known channel. Retain the decision and supporting activity records. [S32]

The B05 advertisement claims bank-specific templates and interactive authentication features. It does not prove that those features work or that any bank's controls were bypassed. Its practical use is to test the fraud team's response to an impersonation scenario. [S3]

9.3 Suppliers and regulatory coordination

DORA has applied since 17 January 2025 to a broad population of financial entities. The NBB describes supervision of ICT and cyber risk, including incident information, tests and third-party dependencies. [S38]

For each essential banking service, identify the identity provider, telecommunications route, core supplier and recovery dependency. A supplier's generic restoration message does not establish that your own service is safe, complete and reconciled.

Maintain one incident chronology and separate decisions for operational reporting, privacy, customer communication and fraud response. The presence of one reporting regime does not automatically close the assessment under another. [S36][S37][S38]

KEY TAKEAWAYS

01

Dispose of current listings through account validation.

02

Investigate identifiers, sessions and payment authorisation separately.

03

Keep issuer subsets, sector associations and post-based cards distinct.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which reporting duties and supervisory milestones should Belgian leaders already have operational?

18 April 2027

the conformity milestone addressed in the CCB's August communication

10.1 Rules that apply now 69
10.2 NIS2 conformity: evidence and remediation 70
10.3 Penalties and exclusions need the right scope 70
10.4 Personal-data notification is a separate decision 71
10.5 National crisis coordination 71

CHAPTER 10

Regulatory and national response

IN SHORT

Belgian NIS2 obligations are already in force. The April 2026 evidence checkpoint and the August supervisory communication require practical preparation, rather than a new-law waiting period. Personal-data incidents also require a separate assessment under GDPR. Financial entities must map the applicable DORA regime. Product manufacturers face CRA reporting duties from September. Assign an owner to each regime and rehearse the first notification before an incident.

10.1 Rules that apply now

The following table distinguishes the trigger, timing and supervisory context. It is a planning aid, not legal advice. The applicable authority and scope depend on the entity, activity and incident. [S33][S35][S36][S37][S38][S39]

Regime	Applies to	Timing	Responsible route
Belgian NIS2 law	In-scope essential and important entities; significant incidents affecting covered services	Without undue delay after becoming aware of a significant incident: early warning no later than 24 hours; incident notification no later than 72 hours. Final report within one month after notification unless ongoing (see below)	National CSIRT at CCB; trust-service providers have a 24-hour incident-notification exception
GDPR	Controllers with a personal-data breach, unless unlikely to create a risk to individuals' rights and freedoms	Without undue delay and, where feasible, within 72 hours of awareness	Competent data-protection authority; APD/GBA is not competent for every sector
DORA	Financial entities within the regulation's scope	Applicable since 17 January 2025; use the relevant incident classification and reporting process	Applicable financial supervisor and reporting channel
CRA reporting	Manufacturers of products with digital elements and reportable vulnerabilities or severe incidents	Duties began 11 September 2026. After becoming aware of an actively exploited vulnerability or severe incident: early warning within 24 hours and notification within 72 hours	European Single Reporting Platform, relevant CSIRT and ENISA

If the incident remains ongoing at the one-month milestone, provide a progress report then. Submit the final report within one month after definitive handling of the incident. [S36]

The CRA final-report clocks differ. For an actively exploited vulnerability, the CCB describes a deadline of 14 days after a corrective or mitigating measure becomes available. For a severe incident, it describes one month after the notification. [S39]

Do not apply a deadline from one regime to every incident. Notification to a supplier, insurer or police is not automatically a notification to the competent regulator. Keep an awareness timestamp and a separate decision record for each applicable duty.

10.2 NIS2 conformity: evidence and remediation

The law of 26 April 2024 entered into force on 18 October 2024. The CCB's April communication described evid-
ence expected from essential entities by 18 April 2026. The content depended on the conformity route chosen. [S33][S36]

For CyberFundamentals, the CCB described verification or an active path towards it, including a signed assessment agreement. For ISO/IEC 27001, it requested scope, applicability and internal-audit documentation. Direct inspection required self-assessment and supporting evidence. [S33]

The August communication addresses the 18 April 2027 milestone. Essential entities unable to demonstrate measures equivalent to Essential are asked for evidence equivalent to Important and a remediation plan towards Essential by 18 April 2028. [S34]

No remediation plan is required if, by 18 April 2027, the entity demonstrates Essential-equivalent measures or justifies a lower equivalent assurance level through its risk analysis. [S34]

The CCB explicitly says that this approach does not change the law's obligations or deadlines. Treat the communication as a supervisory requirement to document a credible route, not a blanket extension. Record the route, assessment scope, evidence owner and unresolved gaps. [S34]

10.3 Penalties and exclusions need the right scope

Article 59 distinguishes several breaches of the Belgian NIS2 law. For risk-management and incident-notification duties, it provides different bands for essential and important entities. Other failures have separate bands. [S36]

Provision	Statutory band	Scope reminder
Important entities	EUR 500 to EUR 7,000,000 or 1.4% of the undertaking's previous worldwide annual turnover, whichever is higher	Relevant risk-management or incident-notification duties
Essential entities	EUR 500 to EUR 10,000,000 or 2% of the undertaking's previous worldwide annual turnover, whichever is higher	Relevant risk-management or incident-notification duties
Repeat conduct	The administrative fine doubles for the same facts within three years	Requires the statutory repeat-conduct conditions
Public-administration sector	Article 62 excludes these entities from the administrative fines and measures under Articles 59–60	Assess applicable cybersecurity and notification duties separately [S36]

These are legal bands, not a prediction of a fine. The law also contains sector-specific exclusions and interaction with equivalent EU rules. Its financial-sector provisions must be read alongside DORA; a generic NIS2 checklist is insufficient. [S36][S38]

10.4 Personal-data notification is a separate decision

The APD/GBA directs controllers to its portal. Its guidance requires notification in a national language; technical annexes may also be in English. It identifies separate competent federal authorities for certain areas, including police information. [S37]

Prepare the portal account and authority assessment before an incident. Record what is known, what remains uncertain and when the next update will arrive. A missing final victim count is a reason to explain uncertainty, not to postpone every reporting decision.

The incident team should give privacy staff a concise impact statement. Include data categories, affected processing, possible recipients, protective measures and the evidence supporting each conclusion. Keep criminal record-count claims separate from the controller's own assessment.

10.5 National crisis coordination

The CCB describes a revised national cyber crisis framework. Its public guidance says the updated plan has applied since 7 May 2026 and coordinates competent authorities without replacing their mandates. Detailed operational content is not public. [S40]

An organisation should still know its own decision chain. Assign authority to isolate a service, request external support, activate manual operations and publish a status notice. Test those decisions with an unavailable supplier and an uncertain data-loss scenario.

KEY TAKEAWAYS

01

Keep NIS2, privacy, financial and product-reporting decisions distinct.

02

The CCB's remediation approach does not erase statutory deadlines.

03

Prepare notification access, evidence owners and crisis decisions before the first alert.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which planning assumptions are supported, and which signals would change them?

3

conditional scenarios for continuity, identity and supplier response

11.1 Key judgements 74

11.2 What would change the assessment 74

11.3 Conditional scenarios 75

CHAPTER 11

Outlook

IN SHORT

The strongest planning case is for identity protection, supplier assurance and recoverable services. Official reporting and the cases support those priorities, without establishing a probability of a future incident. Extortion listings remain distributed across many group labels. Recent operational disruption adds urgency to controlling remote access. Use the scenarios below to test decisions, then revise them when your own evidence changes.

11.1 Key judgements

Judgement	Confidence	Basis	Limit
Account protection deserves immediate attention	High for the priority	CCB identity assessment and police fraud reporting [S5] [S31][S32]	Does not measure exposure at an individual employer
Supplier failures can become local service problems	High for the pathway	Learning, health and signing-service cases [S8][S13] [S22]	Shared dependency does not mean every customer was affected
Extortion readiness should cover multiple actor labels	High for the visible listing mix	46 listings across 22 labels [S1]	Listings do not establish distinct intrusions or losses
Remote operational access warrants review	High for the control priority	Refrigeration disruption and official advice [S25][S27]	Does not establish the cause of every reported malfunction

Confidence belongs to these propositions. It does not certify an actor's honesty, a seller's whole catalogue or the authenticity of every record in a file.

11.2 What would change the assessment

A verified current privileged account would raise the urgency of an organisation's identity response. An old inactive credential with documented remediation would narrow it. The relevant evidence is account validity and recent activity, rather than the volume of advertisements.

A supplier's verified customer-specific impact report would narrow or widen the affected data population. A generic restoration statement would establish availability, while leaving confidentiality unresolved. Document both states independently.

An official investigation or reproducible technical evidence could change attribution for the refrigeration campaign. Repeated allegations, screenshots and political timing would not be enough on their own. Update the judgement only when the proposition itself gains support.

11.3 Conditional scenarios

These scenarios are planning assumptions. They are not forecasts of attack frequency, financial loss or likely perpetrators.

Scenario	Trigger	First decision	Completion evidence
A current identity is abused	An active account and suspicious session are verified	Identity lead revokes sessions and preserves access records	Account owner confirms recovery; access and recovery paths reviewed
A shared supplier isolates its platform	A service notice matches a documented dependency	Service owner activates the tested alternative and requests a scoped impact statement	Manual service works; affected records and reporting decisions documented
Remote equipment behaves unexpectedly	Operations validate a setting change or loss of control	Operations lead uses the safe local process and restricts remote access	Safe state confirmed; remote accounts and change history reviewed

KEY TAKEAWAYS

01

Treat scenarios as tests of decisions, not predictions.

02

Revise identity urgency using account validity and current activity.

03

Change attribution only when stronger evidence supports that proposition.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who should act first, and what evidence shows the work is finished?

30/60/90

days to validate identities, rehearse dependencies and verify recovery

12.1 The first 30/60/90 days 77

12.2 Responsibilities by role 79

12.3 How Brandefense can help 79

CHAPTER 12

Action plan

IN SHORT

Begin with facts your organisation can validate: active accounts, exposed services, supplier dependencies and restoration capability. Give each action an owner and a closure record. Extend the exercise to privacy, customer support, finance and operations. The aim is a service that can recover and a team that can explain what happened. Review progress against the evidence below at each leadership meeting.

12.1 The first 30/60/90 days

1Immediate

Remove direct public internet access to refrigeration management interfaces; coordinate safe continuity and protected remote maintenance

OWNER

Operations and security leads with maintenance providers

COMPLETION EVIDENCE

Reachability checks confirm no direct public access; safe settings and protected maintenance verified [S25]

230 days

If a current credential or session is linked to your service, verify the account, revoke suspicious sessions and review recovery routes

OWNER

Identity and SOC leads

COMPLETION EVIDENCE

Account disposition, activity review and recovery record

Identify internet-facing remote management and business-critical applications; prioritise vendor-confirmed urgent fixes

OWNER

Infrastructure lead

COMPLETION EVIDENCE

Owned inventory, patch evidence and documented exceptions

Map critical suppliers to data, administrative access and service processes

OWNER

Procurement and service owners

COMPLETION EVIDENCE

Dependency register with an incident contact and alternative process

Prepare one incident decision record covering notification triggers and awareness times

OWNER

Legal, privacy and incident lead

COMPLETION EVIDENCE

Tested access to required reporting channels and named deputies

360 days

Rehearse a supplier outage with uncertain customer-data impact

OWNER

Business continuity and privacy leads

COMPLETION EVIDENCE

A working alternative, draft user notice and separate regulatory decisions

Test payment-change verification using an already known contact channel

OWNER

Finance and fraud leads

COMPLETION EVIDENCE

Sampled callback records and handling for mismatched beneficiary details

Review remote equipment accounts and access paths with maintenance providers

OWNER

Operations lead

COMPLETION EVIDENCE

Approved access list, safe local process and change-review evidence

490 days

Restore one essential service from protected backups under realistic dependency constraints

OWNER

Recovery lead

COMPLETION EVIDENCE

Measured recovery result, data validation and closed exercise issues

Test detection of suspicious sessions, new authentication methods and unauthorised mailbox forwarding

OWNER

SOC and identity leads

COMPLETION EVIDENCE

Reviewed alerts, named response owner and retained exercise evidence

Present the conformity route, supplier gaps and exercise outcomes to management

OWNER

CISO

COMPLETION EVIDENCE

Signed decisions, funded remediation and dates for unresolved items

The horizons are organisational planning targets. They do not replace statutory reporting clocks, urgent containment or the immediate response to an active incident.

12.2 Responsibilities by role

Security leadership. Ask for evidence of recovery and identity control, rather than a list of purchased tools. Resolve ownership when an application, supplier and operational service cross several teams. Record accepted residual risks with an expiry date.

SOC and incident response. Start with the account, affected service and evidence type. Retain the original notification and a clear chronology. Verify the difference between a suspicious advertisement, a valid identity and an observed session before describing an outcome.

IT and infrastructure. Check that urgent updates reached the actual exposed system. A successful deployment task does not prove every appliance, bundled runtime or secondary server was covered. Keep recovery access separate from ordinary administration.

Privacy and communications. Draft short notices that say what is known, what remains uncertain and what users should do. Prepare French and Dutch versions together where relevant. Use a stable official channel for later updates.

Finance and customer protection. Verify new payment instructions independently. Train support teams for callers who quote genuine personal information. Real customer details make a fraud attempt more convincing; they do not authenticate the caller.

Operations and suppliers. Define a safe local mode before remote access is restricted. Agree who can change settings, approve emergency access and confirm restoration. Review the maintenance provider's access after staff or contract changes.

12.3 How Brandefense can help

Brandefense provides external threat intelligence and digital-risk monitoring. The service can support investigation of exposed credentials, leaked data and brand impersonation. An alert should enter the validation and response workflow described in this report. [S44]

Bring the domains, brands and services you are authorised to assess to a Brandefense demonstration. Ask how a finding reaches an accountable owner, how uncertainty is represented and what evidence closes the case. [S44]

KEY TAKEAWAYS

01

Give every action an owner and a verifiable completion record.

02

Test recovery with the supplier and identity dependencies unavailable.

03

Keep organisational planning targets separate from immediate incident and notification duties.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

How should a reader interpret the evidence without confusing its populations?

4

evidence types: observation, claim, public corroboration and assessment

Appendix A. Method and limits 81

Appendix B. Evidence register 84

Appendix C. Sources 85

Appendix D. Glossary 88

Appendix A. Method and limits

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

A.1 Window and timestamp meaning

The report covers 1 January–22 November 2026. Underground observations use post dates, not a presumed intrusion date. Own-source exposure observations date from 21 November; forum and passive observations date from 22 November. The current-day cutoff reflects information available at capture, rather than later hours of that date.

Recent activity is labelled 9–22 November. An official report published during that period can describe earlier events. A restoration update, republication and newly advertised historical file are not new intrusions by default.

A.2 Evidence populations

Population	Unit	Coverage boundary
Retained underground material	Distinct post	1,025 retained forum posts; tagged platform counts reported separately
Country-tagged forum subset	Post	480, included within the retained population
Ransomware material	Accepted listing row	46 Belgian-labelled rows; country and entity scope require caution
Domain inventory	Candidate primary domain	250 selected; 245 with a DNS response
Public incidents and campaigns	Evidence dossier	Organisational statements, official warnings and attributed reporting; not a national census
Payment-card material	Distinct card and appearances	3 cards, 17 appearances, 9 posts; no named issuer attribution

The public chart files contain aggregates. Public evidence cards retain short redacted excerpts without personal samples, victim identifiers or criminal contact routes. An actor alias identifies a forum persona, not a verified person.

A.3 Selected-domain observations

The domain set covers public services and broad economic roles. It is purposive and does not establish a ranked list of Belgium's largest independent organisations. DNS responses do not validate legal ownership, organisational independence or security performance.

Passive email and web observations concern the assessed domains at the observation date. Missing or unsuccessful observations remain distinct from established configuration findings.

Atlas covers all 250 selected domains. The national headline is 48 out of 100. Device, credential, document and current-listing observations were read on 21 November 2026. They are cumulative records, not exclusively 2026 events.

Mentions cover the previous 365 days through 22 November 2026; lookalikes cover 30 days. No organisation or sector rating is published. These observations do not establish active accounts, unique people or confirmed intrusions. [S2]

A.4 Ransomware comparisons

Ransomware leak-site listings are criminal assertions. A listing does not establish encryption, successful theft, payment, loss or unique legal-entity identity. Repeated brand descriptions and foreign units can complicate country comparisons.

The four regional peers share borders with Belgium and offer relevant logistics, language, industry or financial-services context. Raw listing totals are not adjusted national risk rates. Partial 2026 and full 2025 totals are kept explicitly separate.

A.5 Payment-card scope

These limited observations do not estimate total card theft, active cards, bank-system intrusion or fraud loss.

The 3 distinct cards were not attributed to named Belgian issuers. Seventeen appearances are not seventeen cards. The three cards are a single population; there is no additional named-bank population to add to them.

A.6 Public sources and naming

Public source categories include the national cyber authority, Safeonweb, the data-protection authority, police, organisational statements and reporting in relevant languages. Every factual source cited was read for its supporting passage. Verification dates record the review, not the incident date.

Named victims require official confirmation and wider reporting. Other organisations receive broad role labels. Where an article address identifies a withheld organisation, the public source register supplies the publisher's root with the article address withheld.

An unavailable original statement limits naming and corroboration. A reported quotation remains attributed to its speaker and publisher. It is not silently promoted to an independently verified forensic result.

A.7 Confidence and alternatives

High confidence can apply to the existence of a retained advertisement while confidence in its claimed contents remains low. The two propositions are different. Each case records what is held, what is unresolved and an alternative explanation.

Analytical models are labelled. Common language, geography, sector, political rhetoric or publication timing is insufficient to join actors. The report does not infer a shared operator from those similarities.

A.8 What the report excludes

The report does not provide a census of all Belgian cybercrime, a national affected-person total, financial-loss estimates or actor probabilities. Several public notices concern prevention or old events. They are not counted as new attacks merely because they were published in 2026.

For example, an October preventive website shutdown and a November hospital outage without indications of external attack are excluded as confirmed cyberattacks. Their existence illustrates why unavailability alone is insufficient. [S66][S67]

Legal statements are scoped to the cited authority and text. The report is not legal advice. Publication and regulatory dates are distinct from incident dates, and an administrative decision can concern an earlier year's conduct.

Appendix B. Evidence register

Card	Date	Venue	Alias	Language	Chapter
B01	2026-01-24	Leak forum	kazutlg	English	4
B02	2026-01-21	Leak forum	xmlrpc	English	4
B03	2026-10-02	Leak forum	yneov18	English	4
B04	2026-11-08	Leak forum	DataJava	English	4
B05	2026-11-20	Leak forum	0xcasper	English	4
B06	2026-11-13	Leak forum	updap	English	4
B07	2026-04-13	Leak forum	[alias withheld]	English	4
B08	2026-02-24	Leak forum	Crazy88	English	4
B09	2026-11-03	Leak forum	buylogs	English	4
B10	2026-11-21	Leak forum	WSdatabase	English	4

Cases A–F assess the retained forum propositions. Cases G–O and R–S assess public incident accounts. Cases P–Q assess official police campaign statements. They are case dossiers rather than mutually exclusive national incident units.

Appendix C. Sources

S1: Odin by Brandefense ransomware-listing aggregate. https://brandefense.io/. Verified on 2026-11-22. Retained report data; URL provides service context, not the underlying records.

S2: Atlas exposure ratings, Brandefense Blackhole domain associations and selected-domain passive observations. https://brandefense.io/. Verified on 2026-11-22. Retained report data; URL provides service context, not the underlying records.

S3: Brandefense Blackhole country-tagged post counts and retained forum and card-material observations. https://brandefense.io/. Verified on 2026-11-22. Retained report data; URL provides service context, not the underlying records.

S4: CCB, Figures show a steady rise in incidents. https://ccb.belgium.be/news/figures-show-steady-rise-incidents-ccb-urges-enterprises-act-immediately. Verified on 2026-11-22.

S5: CCB, The growing threat of identity compromise. https://ccb.belgium.be/news/growing-threat-identity-compromise. Verified on 2026-11-22.

S6: Belgian federal portal, Belgium, a federal state. https://www.belgium.be/en/about_belgium/government/federale_staat. Verified on 2026-11-22.

S7: CCB, Quarterly Cyber Threat Report Q1 2026. https://ccb.belgium.be/nl/open-media/1237/download?inline. Verified on 2026-11-22.

S8: CCB, Quarterly Cyber Threat Report Q2 2026. https://ccb.belgium.be/open-media/1427/download?inline. Verified on 2026-11-22.

S9: CCB, Quarterly Cyber Threat Report Q3 2026. https://ccb.belgium.be/open-media/1470/download?inline. Verified on 2026-11-22.

S10: Security Affairs, hospital service disruption and quoted statement. https://securityaffairs.com/ (article URL withheld). Verified on 2026-11-22.

S11: Safeonweb, company-confirmed fitness and booking-service incidents. https://safeonweb.be/nl/actueel/opgelet-klantgegevens-gelekt-bij-basic-fit-en-bookingcom. Verified on 2026-11-22.

S12: Reuters, Basic-Fit customer-data incident. https://www.reuters.com/business/basic-fit-says-data-breach-exposes-details-200000-members-netherlands-2026-04-13/. Verified on 2026-11-22.

S13: Safeonweb, learning-platform incident and phishing warning. https://safeonweb.be/ (article URL withheld). Verified on 2026-11-22.

S14: RTBF, reported mobile-management incident at a public agency. https://www.rtbf.be/ (article URL withheld). Verified on 2026-11-22.

S15: Machelen, municipal incident updates. https://www.machelen.be/cyberincident. Verified on 2026-11-22.

S16: VRT, municipal confirmation of personal-data theft. https://www.vrt.be/vrtnws/nl/2026/09/23/dan-toch-persoonsgegevens-gestolen-bij-cyberaanval-op-gemeentebe/. Verified on 2026-11-22.

S17: RTBF/Belga, sports membership incident accounts. https://www.rtbf.be/ (article URL withheld). Verified on 2026-11-22.

S18: RTBF, fitness-chain company statement and criminal claim. https://www.rtbf.be/ (article URL withheld). Verified on 2026-11-22.

S19: VRT, school-group incident and director statement. https://www.vrt.be/ (article URL withheld). Verified on 2026-11-22.

S20: VRT, vocational-training data republication. https://www.vrt.be/ (article URL withheld). Verified on 2026-11-22.

S21: L'Avenir, reported public e-learning platform incident. https://www.lavenir.net/ (article URL withheld). Verified on 2026-11-22.

S22: VRT, digital-signature supplier statement and customer-scope distinction. https://www.vrt.be/ (article URL withheld). Verified on 2026-11-22.

S23: SPF Finances/FOD Financiën, recovery updates. https://finances.belgium.be/fr/Actualites/eservices-disponibles-apres-cyberattaque. Verified on 2026-11-22.

S24: VRT, federal tax administration incident. https://www.vrt.be/vrtnws/nl/2026/10/28/cyberaanval-bij-fod-financien/. Verified on 2026-11-22.

S25: CCB, refrigeration-controller security advisory. https://ccb.belgium.be/advisories/warning-six-new-danfoss-vulnerabilities-refrigeration-controllers-risk-immediate-action. Verified on 2026-11-22.

S26: Reuters, differing ministerial assessments of refrigeration attribution. https://www.reuters.com/world/belgian-ministers-odds-over-irans-alleged-role-refrigerator-cyberattacks-2026-11-13/. Verified on 2026-11-22.

S27: Safeonweb, refrigeration incidents and connected-device advice. https://safeonweb.be/nl/actueel/na-de-incidenten-met-koelkasten-warenhuizen-kan-jouw-slimme-koelkast-een-eigen-leven-gaan. Verified on 2026-11-22.

S28: Safeonweb, possible benefits-service data exposure. https://safeonweb.be/ (article URL withheld). Verified on 2026-11-22.

S29: Safeonweb, possible gift-voucher customer-data exposure. https://safeonweb.be/ (article URL withheld). Verified on 2026-11-22.

S30: Federal Police, alleged phishing-panel supplier investigation. https://www.police.be/5998/fr/actualites/crime-as-a-service-arrestation-dun-fournisseur-de-panneaux-de-phishing. Verified on 2026-11-22.

S31: Federal Police, automated invoice-fraud warning. https://www.police.be/5998/fr/actualites/factures-falsifiees-la-police-judiciaire-federale-danvers-tire-la-sonnette-dalarme. Verified on 2026-11-22.

S32: Federal Police, phishing and fake-bank-employee investigation. https://www.police.be/5998/fr/actualites/un-chef-dune-bande-dhameconneurs-arrete-son-retour-de-dubai. Verified on 2026-11-22.

S33: CCB, NIS2 evidence milestone in April 2026. https://ccb.belgium.be/news/nis2-18-april-2026-deadline-what-essential-entities-must-have-place. Verified on 2026-11-22.

S34: CCB, New communication for NIS2 essential entities. https://ccb.belgium.be/news/new-communication-nis2-essential-entities. Verified on 2026-11-22.

S35: CCB, NIS2 Notifications – Howto?. https://ccb.belgium.be/cert/report-incident/nis2-notifications-howto. Verified on 2026-11-22.

S36: Justel, Belgian NIS2 law, consolidated text. https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel. Verified on 2026-11-22.

S37: APD/GBA, Notifier et gérer une violation de données. https://www.autoriteprotectiondonnees.be/professionnel/actions/violation-de-donnees-personnelles. Verified on 2026-11-22.

S38: National Bank of Belgium, ITA team and DORA. https://www.nbb.be/en/financial-supervision/digital-resilience-and-cyber-risk/ita-team. Verified on 2026-11-22.

S39: CCB, CRA reporting obligations take effect. https://ccb.belgium.be/news/cyber-resilience-act-european-reporting-obligations-take-effect. Verified on 2026-11-22.

S40: CCB, National Cyber Emergency Plan. https://ccb.belgium.be/vital-sectors/national-cyber-emergency-plan. Verified on 2026-11-22.

S41: Ivanti, EPMM security advisory and resolved versions. https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340. Verified on 2026-11-22.

S42: NVD, CVE-2026-1281. https://nvd.nist.gov/vuln/detail/CVE-2026-1281. Verified on 2026-11-22.

S43: NVD, CVE-2026-1340. https://nvd.nist.gov/vuln/detail/CVE-2026-1340. Verified on 2026-11-22.

S44: Brandefense, Request a demo. https://brandefense.io/request-a-demo/. Verified on 2026-11-22.

S45: Safeonweb, fake pellet and firewood offers. https://safeonweb.be/nl/actueel/pellets-brandhout-kopen-laat-je-niet-misleiden-door-valse-aanbiedingen. Verified on 2026-11-22.

S46: Charging-account service, company incident FAQ. https://help.chargemap.com/nl/articles/11583170. Verified on 2026-11-22.

S47: Chemical manufacturer, clarification of the May incident. https://www.christeyns.com/ (article URL withheld). Verified on 2026-11-22.

S48: Recycling operator, forensic follow-up. https://www.iok.be/ (article URL withheld). Verified on 2026-11-22.

S49: Medical research institute, statement updated in November. https://www.itg.be/ (article URL withheld). Verified on 2026-11-22.

S50: Professional legal body, scope update. https://www.avocats.be/ (article URL withheld). Verified on 2026-11-22.

S51: ITdaily, supermarket supplier incident. https://itdaily.be/ (article URL withheld). Verified on 2026-11-22.

S52: Wonen360, furniture-retailer company statement. https://www.wonen360.nl/ (article URL withheld). Verified on 2026-11-22.

S53: Télésambre, municipal incident and restoration reporting. https://www.telesambre.be/ (article URL withheld). Verified on 2026-11-22.

S54: La Libre, precious-metals customer-data incident. https://www.lalibre.be/ (article URL withheld). Verified on 2026-11-22.

S55: DH, municipal website incident and scope. https://www.dhnet.be/ (article URL withheld). Verified on 2026-11-22.

S56: HLN/VTM, travel-operator statement and customer messages. https://www.hln.be/ (article URL withheld). Verified on 2026-11-22.

S59: Safeonweb, malicious-app and NFC-relay warning. https://safeonweb.be/nl/actueel/pas-op-voor-frauduleuze-telefoontjes-waarin-je-wordt-gevraagd-een-app-te-installeren-en-je. Verified on 2026-11-22.

S60: Safeonweb, executive impersonation on Teams. https://safeonweb.be/nl/actueel/pas-op-voor-ceo-fraude-microsoft-teams. Verified on 2026-11-22.

S61: Safeonweb, false hotel and B&B reservation messages. https://safeonweb.be/nl/actueel/opgelet-voor-valse-whatsapp-berichten-over-hotel-en-bb-boekingen. Verified on 2026-11-22.

S62: Safeonweb, government sign-in impersonation. https://safeonweb.be/nl/actueel/phishing-naam-van-csam. Verified on 2026-11-22.

S63: Safeonweb, fraudulent compensation and recovery messages. https://safeonweb.be/nl/actueel/opgelet-voor-fake-dossier-voor-schadevergoeding-na-fraude. Verified on 2026-11-22.

S64: Safeonweb, false voting and account-linking messages. https://safeonweb.be/nl/actueel/opgelet-voor-valse-stemwedstrijden-whatsapp. Verified on 2026-11-22.

S65: Safeonweb, high-profile invitation impersonation. https://safeonweb.be/nl/actueel/opgepast-voor-berichten-die-van-het-koningshuis-lijken-te-komen. Verified on 2026-11-22.

S66: Safeonweb, preventive PHP patching outage. https://safeonweb.be/nl/actueel/php-crisis-waarom-waren-verschillende-websites-niet-bereikbaar. Verified on 2026-11-22.

S67: Numerikare/Belga, hospital outage without external-attack indications. https://www.numerikare.be/ (article URL withheld). Verified on 2026-11-22.

S68: IETF, RFC 6797: HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html. Verified on 2026-11-22.

S69: W3C, Content Security Policy Level 3, abstract. https://www.w3.org/TR/CSP3/. Verified on 2026-11-22.

S70: IETF, RFC 4034: Resource Records for the DNS Security Extensions, section 5. https://www.rfc-editor.org/rfc/rfc4034.html. Verified on 2026-11-22.

S71: VRT, charging-account service incident and European user population. https://www.vrt.be/vrtnws/nl/2026/11/18/charge-map-cyberaanval/. Verified on 2026-11-22.

Appendix D. Glossary

Term	Plain meaning
Account recovery	The process for restoring access after credentials or authentication methods are lost
Credential	Information used to authenticate, such as a password or authentication secret
Device association	A record linking a device-related observation to a domain; ownership requires validation
DMARC	An email policy that helps receivers assess messages using a domain's identity
DKIM	A digital email signature checked against a domain's published verification information
DNSSEC	A system for validating signed DNS information
DS record	A delegation signer record links a parent DNS zone to a child zone's signing key; observing it does not validate the full DNSSEC chain [S70]
HSTS	HTTP Strict Transport Security directs browsers to use HTTPS for a site; one observed header does not assess every application [S68]
CSP	Content Security Policy controls which resources a page may load or execute; one observed policy does not establish complete application security [S69]
Exfiltration	Unauthorised copying of data out of a system
Initial access broker	A seller who advertises access to organisational systems; each access claim needs validation
Metadata	Information describing another record, such as its title, author or processing time
NFC relay	Forwarding short-range card communications to another location during a fraudulent transaction
OAuth consent	Permission allowing an application to access specified resources under an account
Pseudonymisation	Replacing direct identifiers while keeping a possible route to linking records to people
Session	An authenticated interaction that may remain usable after the initial login

Term	Plain meaning
SPF	A DNS-published statement of authorised sending services for an email domain
TLS	The protocol used to protect network communication and authenticate a service

About this report

Prepared by Odin by Brandefense. Brandefense Country Report · Belgium 2026. Version 1.0, observation cutoff 22 November 2026. TLP:CLEAR.

The report keeps advertisements, listings, official accounts and assessment separate. It takes no political position and makes no independent state attribution. Recommendations describe actions an organisation should validate; they do not assert that a named organisation has failed to perform them.

French and Dutch editions are translated with AI from the English master. The English edition prevails where they differ. Independent publication review, rendering and release are separate steps.

© 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