BRANDEFENSE COUNTRY REPORT · FRANCE 2026

Brandefense France Cyber Threat Landscape Report 2026

Identity-led data theft, supplier incidents and disruption of connected services

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

120 of 249
assessed domains with a current credential-market listing

7,757
retained forum records, a partial observation population

295
French extortion listings, distributed across many group names

20
actions with an owner, trigger and completion evidence

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	France's digital and security context	10
03	National exposure: the selected domain universe	14
04	What the retained dark-web posts show	25
05	Incidents and claims by sector	42
06	Hacktivism, DDoS and industrial disruption	55
07	Threat actors and campaigns	60
08	The fraud economy	71
09	Banking and finance deep dive	76
10	Regulatory and national response	81
11	Outlook and conditional scenarios	86
12	Action plan	90
A	Appendix A. Scope, method and confidence	97
B	Appendix B. Evidence register	100
C	Appendix C. Sources	101
D	Appendix D. Glossary	105
	About this report	107

Board and CISO	01 05 11 12
SOC and response	04 06 07 12
Identity and applications	03 05 07 12
Operations and safety	05 06 12
Fraud and finance	08 09 12
Legal and procurement	05 10 12

About this edition

AI-assisted research and drafting. Observations, actor claims, official disclosures and analyst interpretations remain distinct. Appendix A explains the scope and confidence of each evidence population.

French organisations face a connected problem: stolen identities can expose records, supplier incidents can reach many customers, and remote access can affect physical operations.

Contents and reading routes

The twelve chapters connect evidence to decisions. Read the summary first, then follow the route that matches your responsibility.

Chapter	Question	First reader
1. Executive summary	Which decisions deserve immediate ownership?	Board and CISO
2. Digital context	Which dependencies shape the threat picture?	Leadership
3. Organisation exposure	What does the selected universe establish?	Infrastructure
4. Dark-web evidence	What is offered and what remains a claim?	Intelligence
5. Sector cases	Which disclosed mechanisms change priorities?	Service owners
6. Hacktivism and disruption	What separates publicity from demonstrated impact?	Operations
7. Actors and campaigns	Which relationships and attributions are supported?	Intelligence
8. Fraud economy	How can personal information support deception?	Fraud teams
9. Banking and finance	Which access and payment controls need joint ownership?	Finance and identity
10. Regulatory response	Which obligations apply at the cut-off?	Legal and compliance
11. Outlook	Which signals would change the assessment?	Leadership
12. Action plan	Who acts and what demonstrates completion?	All owners

Leadership route: Chapters 1, 5 and 10–12. **Operations route:** Chapters 4, 6, 7 and 12. **Identity and fraud route:** Chapters 3, 8, 9 and 12.

Observed means retained material or a recorded measurement. **Claimed** means a poster or listing asserts an event or capability. **Officially reported** means a controller or authority describes an event within its stated scope.

An analyst interpretation connects evidence to a decision. It cannot establish missing facts about access, affected people, attribution, a completed sale or financial loss.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow from France's evidence through the cut-off?

4

decisions with an owner and a completion test

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

France's evidence connects data theft, identity abuse and service disruption. Ransompedia records 295 France-labelled listings in the window, against 182 in all of 2025. Official investigations describe stolen accounts, excessive access and supplier dependencies. The November disclosures also include attacks against refrigeration controllers. Current credential listings concern 120 of 249 assessed domains; the national Atlas headline is 63. Prioritise account and export controls, supplier notification, independent recovery and safe industrial remote access.

This report combines retained Brandefense post material, Ransompedia listings, passive observations and source-checked reporting. The figures describe different populations. A post is not an incident, a listing is not confirmation, and a selected organisation universe does not estimate national prevalence [S1][S2][S3][S4].

1. Identity controls must constrain data use after authentication. ANSSI's tax-administration investigation identifies legitimate credentials, insufficient separation and detection gaps. Its October operational update again describes the reuse of stolen secrets to reach data-bearing applications. MFA matters, but permissions, sessions and exports also need controls [S7][S8].

2. Ransomware visibility supports recovery investment across sectors. The 295 France-labelled listings compare with 457 for Germany, 286 for Italy, 221 for Spain and 46 for Belgium. Qilin accounts for 48 France-labelled listings and The Gentlemen for 44. These are records of public claims, not confirmed incidents or national risk rankings [S3].

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

3. Suppliers can turn one incident into many notification decisions. A postal-services provider disclosed a September incident during November. Reporting quotes the provider on names and postal addresses and gives an affected population of 22 million recipients. The provider's scale does not establish which other systems were accessed [S12][S13].

4. Physical operations require a separate response track. The French C4 assessment reports changes to refrigeration-controller settings at about 700 distribution sites during 11–12 October. It reports fires in at least 15 cases. Its attribu-
tion to an Iranian cyber unit is the authorities' assessment, not an attribution derived from this report's posts [S10].

5. Publication dates can hide earlier incident dates. CERT-FR's 12 November update describes October incidents and continuing investigations. The regulator's January sanctions address earlier events. Neither should be counted as a new November or January intrusion solely because the notice appeared then [S7][S14][S15].

Four decisions for leaders

1. **Constrain valid accounts before bulk extraction occurs.** Assign identity and application owners to review privileged, supplier and partner access. Test whether a legitimate low-privilege user can retrieve another user's records. Escalate unexpected bulk access with account, session and export context.
1. **Test notification with suppliers that handle sensitive records.** Require a named incident contact, a rapid initial alert and successive scope updates. Exercise a case where the supplier knows an incident occurred but cannot yet enumerate the affected customers.
1. **Prove recovery and industrial safety independently.** Restore a critical business service with separate recovery credentials. For connected equipment, verify remote-access isolation, local operating procedures and safe restoration with the operational owner.
1. **Join fraud, legal and communications decisions.** Prepare messages that state what is known, what is still being investigated and what affected people can do. Never treat knowledge of personal details as proof that a caller may authorise a payment.

The year in numbers

Each number has its own unit and observation period.

295

France-labelled ransomware listings dated within the report window [S3]

WHAT IT IS NOT

Confirmed attacks, distinct victims or total national ransomware activity

182

France-labelled listings in all of 2025 in the same snapshot [S3]

WHAT IT IS NOT

A comparison over an equal duration

48 / 44

France-labelled listings under Qilin and The Gentlemen [S3]

WHAT IT IS NOT

Attribution of every intrusion to a single operator

7,757

Retained forum records [S1]

WHAT IT IS NOT

A whole-window national post total or unique incidents

162 of 237

Observed domains showing a DMARC reject or quarantine policy [S2]

WHAT IT IS NOT

Verified protection for every sender or a national adoption rate

63

National Atlas headline for 249 assessed domains [S2]

WHAT IT IS NOT

National prevalence or a sector rating

120 of 249

Assessed domains with a current credential listing [S2]

WHAT IT IS NOT

Confirmed intrusions or completed sales

250

Candidate domains across twelve selected sector cells [S2]

WHAT IT IS NOT

A representative national sample or an official organisation ranking

About 700

Distribution sites in the authorities' refrigeration-controller account [S10]

WHAT IT IS NOT

A count independently verified by Brandefense

At least 15

Cases involving fires reported in that official account [S10]

WHAT IT IS NOT

A measure of all physical consequences

64 / 5

Newly reported data-security events / those concerning ministries or supervised bodies in the October update [S7]

WHAT IT IS NOT

Sixty-four independently confirmed new ministry incidents

22 million

Recipients in reporting on the postal-services provider disclosure [S13]

WHAT IT IS NOT

A population added to other leaks to count unique affected French residents

KEY TAKEAWAYS

01

Protect the use of valid accounts as well as the sign-in process.

02

Treat supplier data, recovery and industrial safety as distinct operational responsibilities.

03

Keep listing counts, official incident estimates and affected-person figures separate.

Report map

Start with the decision you own, then follow its evidence, limit and completion test.

Board and CISO	Which dependencies justify investment now?	01 05 11 12
SOC and response	When does a claim require an investigation?	04 06 07 12
Identity and applications	Can valid access retrieve too much data?	03 05 07 12
Operations and safety	Can remote equipment be isolated safely?	05 06 12
Fraud and finance	What can a convincing caller actually authorise?	08 09 12
Legal and procurement	Who must notify whom and when?	05 10 12

Evidence track	What it answers	Boundary
Underground posts	What people advertise, request or announce	Authenticity, recency and outcomes need separate proof
Ransomware listings	What appears in the listing snapshot	Publication can follow intrusion and can repeat an organisation
Passive observations	What selected public configurations show	No demonstration of successful intrusion or control effectiveness
Official disclosures	What a controller or authority reports	Estimates and investigations may change
Technical advisories	Which products and versions need action	An advisory does not establish exploitation at a French organisation

CHAPTER 02

France's digital and security context

THIS CHAPTER ANSWERS

Which national dependencies should shape defensive planning?

95.7%

internet penetration in the late-2026 digital snapshot

2.1 A connected population and repeated identity touchpoints 11
2.2 Public services concentrate data and delegated access 11
2.3 Supplier reach is a service property 12
2.4 Connected operations add a safety dimension 12
2.5 Political framing and state attribution 12
2.6 The institutional response has several tracks 13

CHAPTER 02

France's digital and security context

IN SHORT

France combines widespread digital-service use with large identity stores, connected suppliers and remotely managed equipment. Those features create different failure paths. A valid account may expose records without a software exploit. A supplier incident may require many customer assessments. A controller change may affect physical operations. Map identity, data and service dependencies together before choosing a defensive priority.

2.1 A connected population and repeated identity touchpoints

DataReportal's Digital 2027 France edition presents late-2026 estimates of 63.9 million internet users and 95.7% penetration. It reports 77.4 million mobile connections and 53.5 million social-media user identities in October. Connections and platform identities are not unique people [S5].

The security implication is about repeated interactions. One person may use tax, employment, health, retail, telecom and banking services. Each service can hold accurate information that later makes an impersonation more convincing. None of those details should independently authorise a sensitive action.

The same logic applies inside organisations. An employee can use a partner application, an outsourced support platform and a shared identity provider during one workflow. The business process crosses boundaries that an isolated server inventory may miss.

Map the workflow from the person to the application, the application to its data and the data to each supplier. Identify which party can reset access, export records, alter payment instructions or change a physical process. Those are operational decisions, not just inventory fields.

2.2 Public services concentrate data and delegated access

The official incidents span tax records, education, employment, benefits and administrative services [S6][S7][S8]. Their common defensive question is how a valid identity is permitted to use information. The evidence does not establish that one actor conducted all these incidents.

An application can authenticate a user correctly and still expose too much information. The problem may lie in excessive permissions, an object-level authorisation error or insufficient scrutiny of automated retrieval. A password reset alone does not repair those conditions.

This is why the report links identity controls to application owners. Security teams need the business meaning of an export, a lookup and a record identifier. Without that context, a large but legitimate business operation can resemble abuse, and abusive retrieval can look routine.

2.3 Supplier reach is a service property

The postal-services provider disclosure illustrates how many organisations can depend on one processing service [S12][S13]. A controller may need to assess its own records even when it has no evidence of intrusion into its systems. Supplier and customer investigations can proceed on different timelines.

A useful dependency register records the data held, authorised access, subcontractors, recovery arrangements and incident contacts. Contractual assurances need a practical test. Can the supplier identify which customer datasets were affected, and can the customer make a notification decision before the investigation ends?

This report does not infer that every organisation using a supplier was affected. Nor does it treat a supplier's broad user base as the incident's affected population. Those are different numbers with different purposes.

2.4 Connected operations add a safety dimension

The refrigeration-controller incident makes physical operations part of the landscape [S10]. Operational teams need to know who may change settings, how remote access is controlled, and which independent alarms detect an unsafe state.

Information-security recovery and physical recovery are not interchangeable. Restoring a controller configuration does not automatically establish that food, equipment or facilities are safe. Operational owners must decide when service can resume and what evidence they require.

The same principle applies to energy, water, logistics and manufacturing. The report uses those sectors for defensive planning. It does not claim that every sector suffered the same mechanism or that a public controller interface establishes unauthorised access.

2.5 Political framing and state attribution

The report records political motives only when a source states them and when they help explain the evidence. Actor slogans do not establish causation, sponsorship or the truth of a grievance. Loaded descriptions and slurs are omitted.

The French authorities' November attribution is presented as their assessment [S10][S11]. It is not extended to unrelated data sellers, DDoS announcements or ransomware groups. Similar timing and shared political language do not establish a common operator.

The analysis takes no position on territorial questions, domestic political disputes, elections, government decisions or foreign relations. Its recommendations concern security evidence and operational responsibilities.

2.6 The institutional response has several tracks

ANSSI's operational updates describe assistance to ministries and coordination of technical crisis communications [S6][S7]. CNIL's decisions concern personal-data obligations and security controls [S14][S15][S16][S17]. Police and judicial investigations have a separate evidential and procedural role.

These tracks overlap but answer different questions. A technical report can describe an intrusion route without establishing criminal liability. A regulatory decision can concern an older incident. An investigation announcement can report allegations that have not been tried.

The practical response is to maintain current contacts and a shared evidence timeline. Record discovery, awareness, containment, initial notification and subsequent updates separately. Chapter 10 explains the legal boundaries; Chapter 12 assigns operational ownership.

KEY TAKEAWAYS

01

Map the people, applications, records and suppliers involved in each critical workflow.

02

Give physical operating safety its own restoration decision.

03

Keep official attributions, regulatory findings and criminal allegations within their source's scope.

CHAPTER 03

National exposure: the selected domain universe

THIS CHAPTER ANSWERS

Which measured signals warrant account, endpoint or service validation?

120 of 249

assessed domains with a current credential-market listing

3.1 Universe card 15
3.2 Current listings and the national headline 16
3.3 Device and credential associations 18
3.4 Documents, similar domains and mentions 20
3.5 Email-policy and certificate observations 21
3.6 DNS, TLS and homepage observations 23
3.7 Ownership and completion evidence 24

CHAPTER 03

National exposure: the selected domain universe

IN SHORT

120 of 249 assessed domains had a credential listed for sale when checked. The national Atlas headline is 63, describing the assessed part of the selected 250-domain portfolio. One selected domain lacks exposure results. The portfolio records at least 1,051,618 device associations and 480,908,523 credential records. These overlapping observations are not confirmed intrusions. Assign current listings, employee-device signals and configuration findings to their relevant owners for validation.

3.1 Universe card

The selection describes prominent institutions and services. It is not an official top-organisation ranking, and several domains belong to related corporate groups [S2].

Item	Definition
Selected population	250 candidate domains across twelve sector groups
Selection	Purposive selection of public services, finance, infrastructure, major businesses, education and health institutions
Unit	A selected primary service domain; not necessarily an independent legal entity
Corporate overlap	Parent companies, subsidiaries, brands or distinct services may appear separately
Exposure population	249 assessed domains; one selected domain has no exposure result
Passive population	237 observed domains; 13 selected domains remain outside that denominator
Exposure snapshot	21 November 2026
Similar-domain observation window	19 October–18 November 2026
Mention and passive snapshots	22 November 2026
Sector reporting	Observed signal counts
Public output	Anonymous aggregates and the national Atlas headline
Inference boundary	No estimate of national prevalence, security effectiveness or a typical organisation

Legal-entity and ownership validation remains necessary before an independent-organisation ranking. A recognisable domain and a reachable service do not establish that every selected entry is independent.

3.2 Current listings and the national headline

120 of 249 assessed domains had a credential listed for sale when checked. The selected universe contains 250 domains, with one unavailable exposure record. Missing data are not an observed zero [S2].

The national Atlas headline is **63 on a 0–100 scale**. Higher values indicate greater observed exposure. It describes this assessed portfolio, not every organisation in France. Only the national headline is published; sector and organisation ratings are withheld.

63

national Atlas headline for 249 assessed domains

Selected, exposure and passive populations retain separate denominators

Selected domains are shown in each row label. Exposure and passive fractions use selected domains; current credential listings use exposure-assessed domains and are shown in coral.

	Selected	Exposure observed	Passive observed	Current listing
Government (50)	50/50	50/50	49/50	19/50
Banking and finance (30)	30/30	30/30	27/30	16/30
Education (30)	30/30	30/30	26/30	18/30
Manufacturing and industry (30)	30/30	30/30	30/30	11/30
Energy and utilities (20)	20/20	20/20	20/20	6/20
Retail and holdings (20)	20/20	19/20	20/20	14/19
Transport and logistics (20)	20/20	20/20	19/20	9/20
Telecom and technology (10)	10/10	10/10	10/10	9/10
Healthcare (10)	10/10	10/10	7/10	1/10
Insurance (10)	10/10	10/10	10/10	5/10
Hospitality and tourism (10)	10/10	10/10	10/10	6/10
Media and entertainment (10)	10/10	10/10	9/10	6/10

Source: exposure observations for 249 assessed domains among 250 selected candidates, 21 November 2026. Cumulative associations can overlap; they do not establish unique people, confirmed intrusions or national prevalence [S2].

Sector	Selected	Exposure assessed	Passive observed	Domains with a current credential listing
Government	50	50	49	19
Banking and finance	30	30	27	16
Education	30	30	26	18
Manufacturing and industry	30	30	30	11
Energy and utilities	20	20	20	6
Retail and holdings	20	19	20	14
Transport and logistics	20	20	19	9
Telecom and technology	10	10	10	9

Sector	Selected	Exposure assessed	Passive observed	Domains with a current credential listing
Healthcare	10	10	7	1
Insurance	10	10	10	5
Hospitality and tourism	10	10	10	6
Media and entertainment	10	10	9	6
Total	250	249	237	120

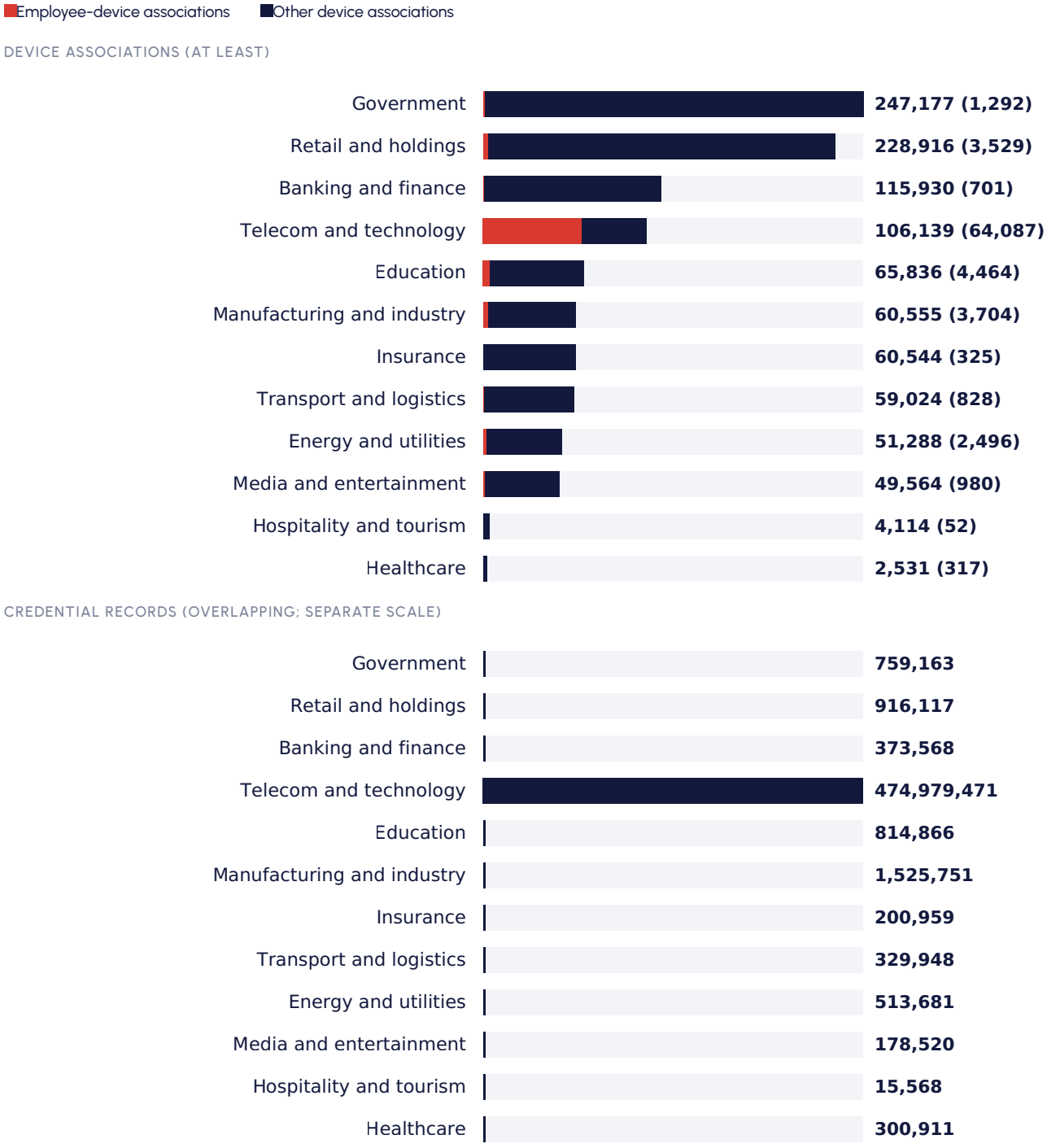
A current listing establishes that a credential associated with a domain is advertised. It does not establish account validity, completed sales, affected people or an intrusion into the organisation. Validate the account and service against authorised records before deciding on a response.

In the downloadable charts, `domains_with_current_credential_listing` counts domains with advertised associated credentials. The field does not establish that an organisation or organisational access is offered for sale.

3.3 Device and credential associations

Device associations occur at 236 assessed domains and credential records at 243. The portfolio contains at least 1,051,618 device associations, including 82,775 employee-classified associations. The employee count sits within the device view and must not be added to it [S2].

Sector device and credential populations require different validation



Source: exposure observations for 249 assessed domains among 250 selected candidates, 21 November 2026. Cumulative associations can overlap; they do not establish unique people, confirmed intrusions or national prevalence [S2].

Sector	Assessed	Devices, at least	Employee devices	Credential records
Government	50	247,177	1,292	759,163
Banking and finance	30	115,930	701	373,568
Education	30	65,836	4,464	814,866

Sector	Assessed	Devices, at least	Employee devices	Credential records
Manufacturing and industry	30	60,555	3,704	1,525,751
Energy and utilities	20	51,288	2,496	513,681
Retail and holdings	19	228,916	3,529	916,117
Transport and logistics	20	59,024	828	329,948
Telecom and technology	10	106,139	64,087	474,979,471
Healthcare	10	2,531	317	300,911
Insurance	10	60,544	325	200,959
Hospitality and tourism	10	4,114	52	15,568
Media and entertainment	10	49,564	980	178,520
Total	249	1,051,618	82,775	480,908,523

Credential records comprise 170,231,515 breach-database records, 21,992,886 stealer-log records and 288,684,122 combolist records. Their sum is 480,908,523.

A combolist is a compiled list of account identifiers and passwords that may combine or repeat older material [S77]. These records can overlap across domains and do not count unique active accounts.

Telecom and technology contributes 474,979,471 credential-record associations, or 98.8% of the portfolio total. Customer-facing domain use and repeated historical material are plausible contributors. This concentration does not establish the same share of affected people or confirmed intrusions [S2].

A device associated with a customer-facing service is not automatically an endpoint owned by that service. Employee classification also requires context, especially where staff, students or customers share a domain. Establish freshness, ownership and previous remediation before disruptive action.

3.4 Documents, similar domains and mentions

Sector	Assessed	Currently listed	Document associations
Government	50	19	2,807
Banking and finance	30	16	327
Education	30	18	418
Manufacturing and industry	30	11	1,675

Sector	Assessed	Currently listed	Document associations
Energy and utilities	20	6	1,089
Retail and holdings	19	14	532
Transport and logistics	20	9	487
Telecom and technology	10	9	2,549
Healthcare	10	1	75
Insurance	10	5	55
Hospitality and tourism	10	6	19
Media and entertainment	10	6	171
Total	249	120	10,204

Document associations occur at 210 assessed domains, totalling 10,204. An association does not establish confidentiality, unlawful disclosure or adversary access. Public documents and repeated material remain plausible explanations [S2].

The similar-domain view dated 19 October–18 November 2026 contains 171,947 candidates across 229 assessed domains. These are candidates for ownership and usage review, not confirmed phishing sites. Similar names can identify related, authorised or unrelated services.

Dark-chat mentions occur at 125 assessed domains and dark-web mentions at 96 over the annual window ending 22 November 2026. They can reflect news, links, customers or advertising. Mention presence does not independently demonstrate hostile activity [S2].

Counts in these tables are not additive. A domain can have devices, credentials, listings and documents simultaneously. A large sector sum also does not describe the typical organisation in that sector.

3.5 Email-policy and certificate observations

Passive observations cover 237 selected domains. DMARC reject policies occur at 107 and quarantine policies at 55. Together, 162 domains, or 68.4%, publish either policy. Another 65 publish monitoring policies and 10 have no policy observed [S2].

Published policy does not prove that every sender is configured correctly or every receiver follows the requested treatment. Review the effective policy for the actual sending domain and validate outbound messages before changing policy [S27].

Mail policy and certificate counts use the passive population

	DMARC reject / quarantine	SPF	DNSSEC	Valid TLS
Government	27/49	48/49	11/49	47/49
Banking and finance	23/27	26/27	5/27	20/27
Education	8/26	24/26	3/26	22/26
Manufacturing and industry	25/30	29/30	9/30	29/30
Energy and utilities	17/20	20/20	4/20	19/20
Retail and holdings	16/20	20/20	0/20	19/20
Transport and logistics	14/19	18/19	5/19	17/19
Telecom and technology	8/10	9/10	2/10	10/10
Healthcare	5/7	7/7	1/7	5/7
Insurance	8/10	10/10	0/10	10/10
Hospitality and tourism	4/10	7/10	3/10	9/10
Media and entertainment	7/9	8/9	0/9	9/9

Source: passive observations for 237 domains, 22 November 2026. HSTS uses 184 recorded homepages. Unsuccessful validation and unresolved TLS remain distinct; policies do not establish message-level enforcement [S2].

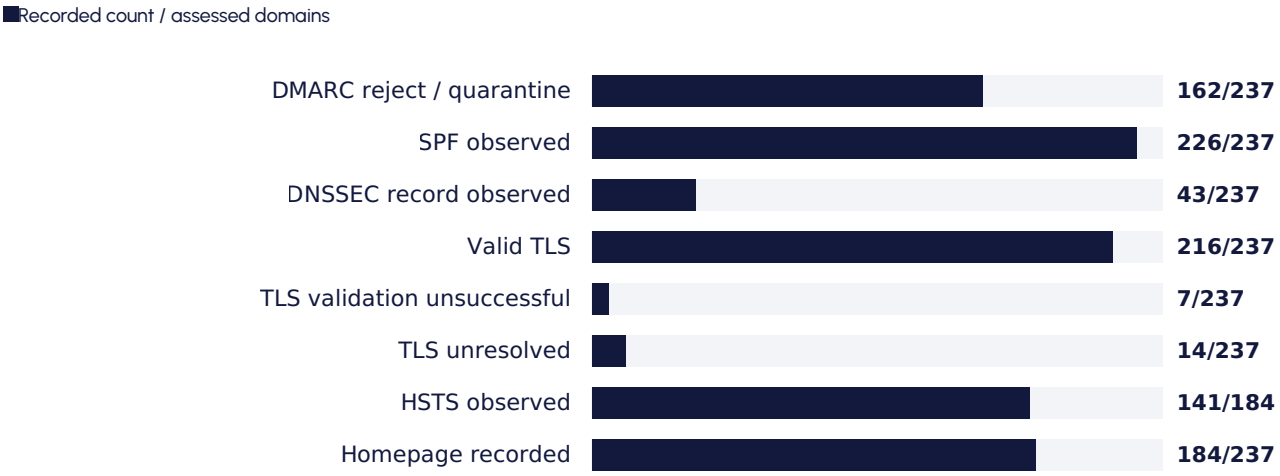
Sector	Observed	Reject or quarantine	SPF observed	Valid certificate
Government	49	27	48	47
Banking and finance	27	23	26	20
Education	26	8	24	22
Manufacturing and industry	30	25	29	29
Energy and utilities	20	17	20	19
Retail and holdings	20	16	20	19
Transport and logistics	19	14	18	17
Telecom and technology	10	8	9	10
Healthcare	7	5	7	5

Sector	Observed	Reject or quarantine	SPF observed	Valid certificate
Insurance	10	8	10	10
Hospitality and tourism	10	4	7	9
Media and entertainment	9	7	8	9
Total	237	162	226	216

SPF is observed for 226 domains. Presence does not establish that every authorised sender is included or all other senders are rejected. Failure to observe a DKIM record likewise does not establish absent signing; actual message headers provide the appropriate check [S2][S27].

3.6 DNS, TLS and homepage observations

Passive results preserve inconclusive certificate and homepage observations



Source: passive observations for 237 domains, 22 November 2026. HSTS uses 184 recorded homepages. Unsuccessful validation and unresolved TLS remain distinct; policies do not establish message-level enforcement [S2].

Observation	Count	Assessed population
DNSSEC delegation record observed	43	237 observed domains
Certificate check valid	216	237 observed domains
Certificate validation unsuccessful	7	237 observed domains
Certificate check unresolved	14	237 observed domains
Homepage response recorded	184	237 observed domains
Homepage observation inconclusive	53	237 observed domains
HSTS observed	141	184 recorded homepages

The certificate outcomes sum to 237, while recorded and inconclusive homepage outcomes also sum to 237. Inconclusive results are not counted as absent security headers or confirmed defects [S2].

A valid certificate does not establish application security. A DNSSEC-related record does not demonstrate validation for every application. HSTS describes the recorded response, not every subdomain or user journey [S27].

3.7 Ownership and completion evidence

Give identity operations the current-account validation queue, endpoint teams the employee-device queue, and fraud teams the relevant customer-account signals. Assign document sensitivity to its data owner and similar-domain use to the brand and service owner.

Close each item with an active, historical, unrelated or unresolved disposition and supporting date. Escalate corroborated unauthorised activity through the organisation's response process. The national headline cannot replace evidence about the particular account, device or service.

KEY TAKEAWAYS

01

Validate current listings at 120 of 249 assessed domains without declaring confirmed intrusions.

02

Keep device, credential, document and passive populations separate.

03

Assign each credible signal to its operational owner and record a dated disposition.

CHAPTER 04

What the retained dark-web posts show

04

THIS CHAPTER ANSWERS

Which advertised offers support a validation task, and which conclusions remain unavailable?

7,757

retained forum records, a partial observation population

4.1 Universe card 26
4.2 Platforms, languages and the closing fortnight 27
4.3 Advertised objects and defensive meaning 28
4.4 Six case studies 29
4.5 Four further caution cards 38
4.6 Relationships, prices and claims 40
4.7 Additional claims kept separate 40

CHAPTER 04

What the retained dark-web posts show

IN SHORT

The retained population contains 7,757 forum records, including 432 dated in the closing fortnight. Selected offers concern privileged access, healthcare, identity-labelled records, telecom data, a claimed supplier series and engineering files. Dates and authenticity remain uncertain for some material. These examples do not establish a national crime mix or verified new incidents. Validate provenance, current access and the actual data fields before choosing a response.

4.1 Universe card

The country-tag snapshot contains 841,760 records dated within the nominal window. That is a tagged-record count, not a count of malicious posts, targeting, victims or incidents. The retained forum population contains 7,757 record IDs, including 432 dated 9–22 November [S1]. It is a subset of the 7,758 forum records in the country-tag snapshot: October retains 1,849 of 1,850 tagged forum records, leaving one tagged October entry unretained.

Item	Definition
Country-tag population	841,760 records associated with France in the window
Retained forum population	7,757 record IDs, including discussion and replies
Closing fortnight	432 retained record IDs dated 9–22 November
Time interpretation	Recorded publication date; the final calendar day is partial
Country boundary	A country association does not establish targeting or victim geography
Repetition boundary	Retained IDs can represent the same underlying message
Date uncertainty	Some publication dates conflict with other retained dates; theft and first circulation are not dated by this count
Validation boundary	Advertised access, files, card status and affected populations remain untested
Analytical use	Selected case narratives and defensive questions, without a national crime-family prevalence estimate

Country-tagged records and retained forums describe different populations

Records in each observation population



Source: Brandefense retained France-related material, 1 January–22 November 2026; final day partial. Country-tagged records and retained forums are separate populations; the closing fortnight is a subset of retained forums. Posts are not incident counts [S1].

The country-tag volume does not supply a national relevant-crime range. News, discussion and unrelated geographic associations can contribute. The retained cases cannot establish the distribution of criminal activity across the broader population.

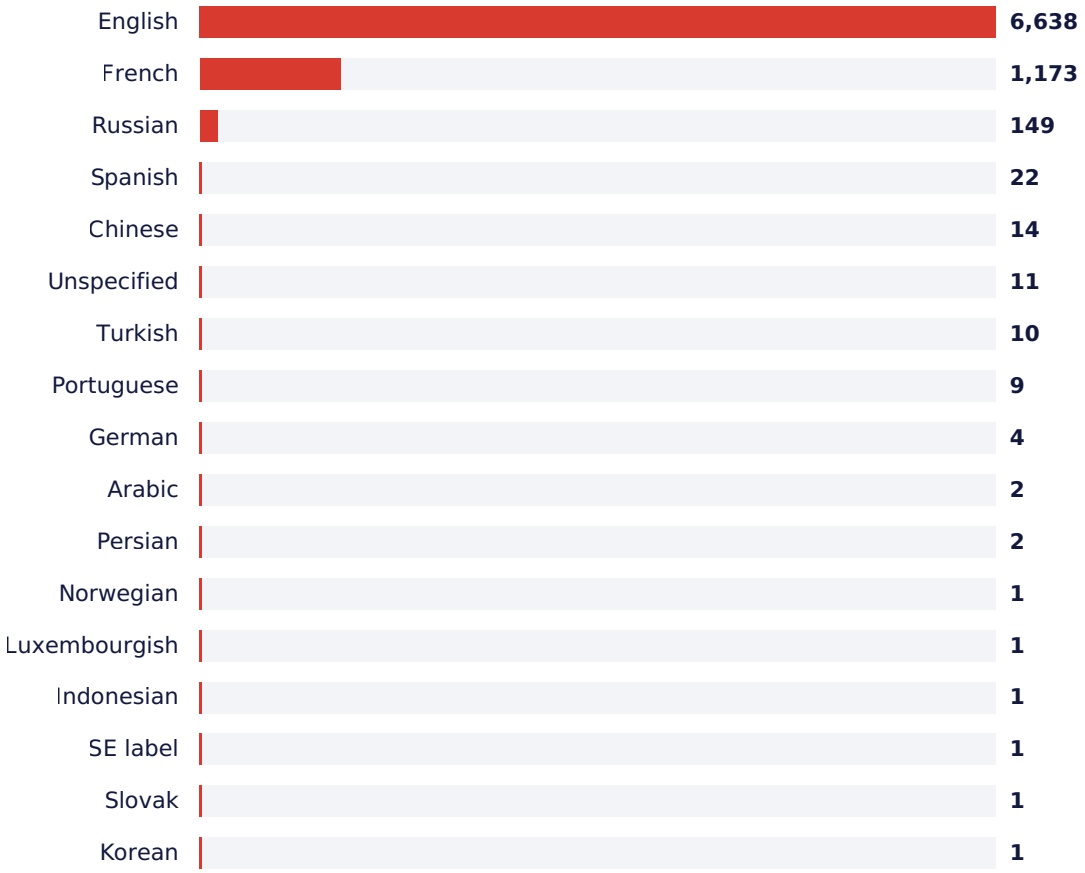
4.2 Platforms, languages and the closing fortnight

The tagged snapshot records 833,822 Telegram records, 7,758 forum records, 109 Discord records, 71 paste records and 0 onion-source records. Of the 7,758 tagged forum records, 7,757 are in the retained forum population, leaving one tagged October entry unretained (1,849 of 1,850) [S1].

The retained population carries 6,638 English labels, 1,173 French labels and 149 Russian labels. Other or unspecified labels account for 80 instances. Labels overlap and do not form a partition of 7,757 records [S1].

Language labels overlap and describe the retained forums only

Language labels in 7,757 retained forum records; labels overlap



Source: Brandefense retained France-related material, 1 January–22 November 2026; final day partial. Country-tagged records and retained forums are separate populations; the closing fortnight is a subset of retained forums. Posts are not incident counts [S1].

Language labels cannot establish a seller's nationality, location or state affiliation. A reply may challenge a claim, ask for access or contribute no new evidence. Neither a reply nor a relisting should automatically become another incident.

The 432 closing-fortnight records add a dated forum observation population. They do not establish the date of theft, the first appearance of an offer or complete coverage of French criminal activity. Recent public disclosures remain a separate evidence track in Chapter 6.

A 15 November local-service supplier claim says several claimed reachable assets were never downloaded. A 21 November construction-sector offer advertises privileged access. Neither establishes current access or copied data. A 10 November hospitality-data offer describes older extraction, illustrating why recent advertising is not a new-incident count [S1].

4.3 Advertised objects and defensive meaning

The examples below are qualitative. Their selection does not estimate the relative size of French criminal markets [S1].

Advertised object	Example	What is observed	What is not established
Privileged access	Cultural-organisation offer	Broad administrative capabilities and a stated asking price	Current access, control of every named system or a sale
Health data and optional access	Large healthcare bundle	Files, secrets and corporate access advertised as distinct objects	One original source, unique patients or valid access
Identity-labelled records	Competing institutional labels and totals	Sales claims and a participant's attribution challenge	A confirmed intrusion into the institution named by a seller
Telecom customer records	Several offers and an explicit repost	Identity, contact and bank-related fields marketed	New theft, a common operator or unique customers
Shared business platform	Several releases with the same series label	The poster explicitly asserts a common platform relationship	A verified platform-wide cause or every customer affected
Project documents	Contractor archive with customer-project folders	Files advertised under customer and project labels	Intrusion into downstream customers or industrial systems

4.4 Six case studies

A

CASE A

A broad privileged-access offer

Evidence card B01 | 19 Mar 2026 | Leak forum | Access

Unverified access claim

CLAIM

An alias offered access to a cultural organisation, describing identity administration, virtual infrastructure, cloud administration, email and endpoint security. Its asking price was 2.5K USD [S1].

OBSERVATION

Two near-identical advertisements under the same alias share a long privilege inventory. B01 preserves the price, while B02 preserves the endpoint-security claim.

WHAT WE CAN ESTABLISH

The same venue identity advertised a similar offer twice. That is not evidence of a second intrusion or a second operator.

ALTERNATIVES

A genuine access seller, a reseller, copied promotion or fabrication. The advertised capability list does not distinguish them.

LIMITS	Access was not tested and the victim organisation is not established. The public alias is generalised because the original contains unsuitable framing.
RESPONSE	Where an internal match exists, review privileged identity, virtual infrastructure and security administration together. Validate recovery access independently of the claimed administrative estate.

Bottom line

Validate privileged access and recovery before treating a capability list as fact.

Evidence card B01 — 19 Mar 2026

Persona A | Leak forum | Forum | English

ORIGINAL

Price: 2.5K USD

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The seller offered purported live access spanning identity administration, virtual servers, email and endpoint security. The stated price is an asking price, not evidence of a completed transaction.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B02 — 19 Mar 2026

Persona A | Leak forum | Forum | English

ORIGINAL

Full access to the EDR Security Center

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

A second near-identical post under the same alias advertised control of endpoint-security administration. It supports a relisting observation, not an independent compromise or a second operator.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Persona A

Original alias generalised

Forum identity advertising access | Not established

IN FRANCE, 2026

19 Mar

Recorded date of similar privileged-access advertisements, B01–B02

CLAIMED TARGETS

A cultural organisation, as claimed

IN THEIR WORDS

"Full access to the EDR Security Center" B02

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

Two similar advertisements under one venue identity. Access, sale and victim identity are unverified. No public corroboration is cited in this edition.

CONFIDENCE
High that the advertisements are retained; capability and chronology uncertain

B

CASE B

Health files and corporate access priced separately

Evidence card B03 | 17 Jun 2026 | Leak forum | Healthcare

Unverified data and access claim

CLAIM	A seller advertised 533 GB and 1,167,076 files, describing health documents, source code, certificates and credentials. Corporate access was offered for an additional payment [S1].
OBSERVATION	The advertisement separates a data bundle from a purported access capability. A file count and a live-access offer are different objects.
WHAT WE CAN ESTABLISH	The seller made those claims. Neither the files, the source institutions, the stated volumes nor the access were independently authenticated.
ALTERNATIVES	A mixture of historical files, data from several parties, a reseller's archive, padded material or a genuine recent extraction.
LIMITS	The file total is not a patient count. This offer is not linked to the separate official medical-software disclosures in Chapter 5.
RESPONSE	Validate document exposure, certificates or other secrets, and current access as separate investigations. Involve the data owner before inferring what a health-related file actually contains.

Bottom line

Files, patient populations and current access require separate validation.

Evidence card B03 — 17 Jun 2026

Zab26 | Leak forum | Forum | English

ORIGINAL

I can include corporate access if you pay extra.

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The seller claimed 533 GB across 1,167,076 files, including health documents and credentials, and offered corporate access separately. Neither access validity, completeness nor the asserted counts were independently tested.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

CASE C

C

Identity-service labels and incompatible totals

Evidence card B04 | 7 Jan 2026 | Leak forum | Identity services

Attribution disputed

CLAIM	Two advertisements used related identity-service labels but claimed 127 million and 13 million records. A participant separately challenged an institutional attribution [S1].
OBSERVATION	B04 records the challenge; B05 and B06 preserve the competing sales statements. A counterclaim is also an unverified participant statement.
WHAT WE CAN ESTABLISH	A common theme and conflicting descriptions. The posts do not establish identical files, a common operator or the actual institution of origin.
ALTERNATIVES	Rebranding of older information, merged sources, different subsets, repeated records or a genuine dataset with misleading promotion.
LIMITS	The two totals cannot be reconciled or added. A large count is not automatically impossible, because its unit may be rows rather than people.
RESPONSE	Verify source attribution and field relevance privately. Treat static identity details as insufficient authority for account recovery, without presenting the seller's institutional label as confirmation.

Bottom line

A common institutional label does not establish the original source.

Evidence card B04 — 7 Jan 2026

suicid | Leak forum | Forum | English

ORIGINAL

its attributed name may simply be false

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

A forum participant disputed the attribution of a purported identity-service dataset and warned that an exfiltrator could label data with a more prominent organisation's name. This is a participant's assessment, not an official determination.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B05 — 17 Apr 2026

RubiconH4ck | Leak forum | Forum | English

ORIGINAL

the price is $4K negotiable

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

A seller offered a dataset labelled as municipal identity-service data, claiming 127 million records dated 2025. The post provides a sale claim and field list, not proof that the named service was the source.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B06 — 12 Sep 2026

lauraallen | Leak forum | Forum | English

ORIGINAL

13 Million

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

Another advertisement used the same institutional label but claimed 13 million records. The differing totals cannot be reconciled from the retained posts and must not be added together.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

CASE D

D

Telecom data and explicit recirculation

Evidence card B07 | 9 Jan 2026 | Leak forum | Telecom

Claims and explicit repost

CLAIM	Separate advertisements described telecom-customer records and bank-account details. One claimed 150,782 lines; another described an 80.9 GB archive. A third explicitly called its material a repost of late-2025 data [S1].
OBSERVATION	B07, B08 and B09 are grouped by sector, not by a proven common incident. B09's historical wording is the poster's own description.

WHAT WE CAN ESTABLISH	Telecom-related information was marketed and one author described republication. That does not independently authenticate the file's age or origin.
ALTERNATIVES	Old customer records, information from another service, overlapping archives, copied advertising or a separate recent incident.
LIMITS	Different aliases and archive sizes cannot be converted into a count of unique incidents or customers. No link is asserted to the earlier telecom event behind the January sanction.
RESPONSE	Validate freshness and overlap before an account response. Customer operations should expect persuasive calls that know the person's provider, identity or bank details.

Bottom line

Validate age and overlap before counting a new incident.

Evidence card B07 9 Jan 2026

near | Leak forum | Forum | French

ORIGINAL

Après plusieurs demandes, voici 150 000 IBAN provenant de [victim domain].

TRANSLATION

After several requests, here are 150,000 IBANs from [victim domain].

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation. English translation shown; the original is French.

Held

The poster claimed to share 150,782 lines combining customer identity and contact fields with bank-account details. This describes the advertised bundle; the records and source were not authenticated.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B08 4 May 2026

OverSec | Leak forum | Forum | English

ORIGINAL

We have the honor of unveiling our first claim

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

A seller attributed an 80.9 GB JSONL dataset to a telecommunications provider and inserted a May 2026 date in the advertisement. The post date and internal dataset date are separate, unverified fields.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B09 9 May 2026

NormalLeVrai | Leak forum | Forum | English

ORIGINAL

I'm just reposting 27.471.090 clients dating from the end of 2025.

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The author explicitly described this as a repost of a late-2025 customer archive. It belongs in 2026 circulation coverage, without counting it as a newly established 2026 intrusion.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

A forum reply described one advertised telecom collection as 2024 material. This is a counterclaim about provenance, not an independently established acquisition date [S1].

CASE E

E

A claimed shared-platform release series

Evidence card B10 | 3 Sep 2026 | Leak forum | Supplier services

Claimed series: attribution corrected

CLAIM	A venue alias presented several equipment-sector releases as part of a common CRM-platform series. One post explicitly corrected a mistaken company attribution [S1].
OBSERVATION	B10 and B13 preserve the asserted series, B11 preserves the correction, and B12 preserves an advertised file total. This supports the poster's claimed relationship, not a verified root cause.
WHAT WE CAN ESTABLISH	The alias used a common label and changed an attribution. The organisation named in error should not become an additional victim in a chart.
ALTERNATIVES	A genuine common supplier event, copied platform branding, unrelated customer exports or a mixture of genuine and misattributed material.
LIMITS	Archive sizes and file totals are unverified. Same alias means a venue identity, not a proven individual or a platform-wide intrusion.
RESPONSE	Track each customer's actual exposure and corrections separately. Investigate the common dependency only where independent supplier or customer evidence supports it.

Bottom line

Preserve corrections and validate each customer dependency separately.

Evidence card B10 — 3 Sep 2026

updap | Leak forum | Forum | English

ORIGINAL

This leak is part of a many leaks

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The post explicitly placed the claimed 44 GB release in a named shared-platform series. This is evidence of the poster's series label, not independent verification that the platform or each customer was accessed without authorisation.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B11 — 3 Sep 2026

updap | Leak forum | Forum | English

ORIGINAL

Old thread is deleted.

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The author corrected a company attribution and said a previous thread had been deleted. Retain the correction alongside the claimed 22.25 GB release; the earlier named organisation should not be treated as an additional victim.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B12 — 3 Sep 2026

updap | Leak forum | Forum | English

ORIGINAL

Files: 323 388

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

Another post under the same alias advertised 13.48 GB and 323,388 files for an equipment-rental business, using the same shared-platform series label. Counts are seller assertions and may include duplicates or attachments.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B13 — 28 Sep 2026

updap | Leak forum | Forum | English

ORIGINAL

Size: 200 GB

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The same venue alias advertised a 200 GB release for an equipment supplier, again explicitly describing it as part of the shared-platform series. Common branding alone does not establish a shared intrusion mechanism.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

F

CASE F

Contractor files are not industrial-system access

Evidence card B14 | 4 Jan 2026 | Leak forum | Engineering

Unverified project-file sale

CLAIM

A seller advertised roughly 340 GB of engineering-contractor files and listed purported project folders for customers in construction and energy. It also said the material was offered on another forum [S1].

OBSERVATION	The advertisement contains customer-project labels and a cross-venue assertion. Neither authenticates the underlying files or establishes who originally obtained them.
WHAT WE CAN ESTABLISH	A contractor-file sale claim. A folder name does not establish intrusion into the customer named on that folder.
ALTERNATIVES	A historical contractor archive, an export taken from a project-sharing service, copied promotion or a genuine current disclosure.
LIMITS	Intrusion freshness is unresolved. The offer does not establish access to plants, controllers or operational systems.
RESPONSE	Review contractor document access, export permissions and retention. Keep confidentiality investigations separate from industrial-safety incidents unless technical evidence connects them.

Bottom line

Project folders do not establish access to customers or industrial systems.

Evidence card B14 — 4 Jan 2026

Angel_Batista | Leak forum | Forum | English

ORIGINAL

This data is also sold on the other breach by me

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held

The seller advertised roughly 340 GB of contractor files, with purported customer-project folders in energy and construction. Folder names and claimed volumes do not establish compromise of the customers or of industrial control systems.

Not established

Authenticity, current access, original source, unique affected people and a completed sale are not established.

4.5 Four further caution cards

A purported insider-assisted public-platform access offer supplies no validated access proof. Its role description is generalised. The claim is not confirmation that an insider exists [S1].

A separate advertisement groups email addresses by public-service domains while showing fields associated with another membership context. An employee's address appearing in a dataset does not establish intrusion into the employer's network [S1].

Evidence card B15 30 Jan 2026

kazutlg Leak forum Forum English

ORIGINAL

With the help of my insider, we propose a full access on government panel

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held
The seller claimed insider-assisted panel access and on-demand personal financial information. The retained narrative supplies no validated access evidence or official confirmation; include only as an unverified access-market claim.

Not established
Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B16 20 Feb 2026

HexDex Leak forum Forum English

ORIGINAL

Totally 8861 Unique Email agents

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held
The poster grouped addresses by government mail domains. Visible field names include sporting-membership and licence data; a government email suffix does not prove an intrusion into government networks. The stated subtotals also must not be added to the purported unique total.

Not established
Authenticity, current access, original source, unique affected people and a completed sale are not established.

A professional-registry advertisement itself mentions public or administrative contact fields. It should not be presented as a patient-data breach without provenance checks. Another offer claims household support records spanning roughly 2012–2026; historical span and unverified family counts matter [S1].

Evidence card B17 23 Jun 2026

Edric Leak forum Forum English

ORIGINAL

Public or administrative contact fields (where applicable)

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held
The post described a professional registry with roughly 12 million entries, institutional identifiers and administrative fields. The source text itself mentions public contacts. Without provenance checks this must not be presented as a confirmed patient-data breach.

Not established
Authenticity, current access, original source, unique affected people and a completed sale are not established.

Evidence card B18 4 Mar 2026

HexDex Leak forum Forum English

ORIGINAL

over the period from ~2012 to 2026.

Note. Recorded publication date; chronology remains uncertain. The excerpt is a claim, not confirmation.

Held
The seller claimed information on 659,658 families and 1,462,485 people, spanning a long historical period. These are unvalidated seller counts, not established numbers of affected people or new 2026 records.

Not established
Authenticity, current access, original source, unique affected people and a completed sale are not established.

These examples illustrate attribution, unit and age problems that matter more than the headline size of an advertisement. They do not establish that every disputed offer is false.

4.6 Relationships, prices and claims

A shared long phrase can support a relationship between advertisements. It does not prove file identity, theft authorship or a completed transfer. A seller saying that material appears elsewhere is a claim about cross-venue circulation until independently corroborated.

The 2.5K USD and negotiable $4K examples are asking prices [S1]. They are not a French price index, a value of the data, a paid amount or an estimate of business loss.

The appropriate response is a validation task with a clear closure criterion. Record whether the data matches, whether the account remains active, whether sessions need revocation and whether the source has been verified. Unmatched or historical material still needs a documented disposition.

4.7 Additional claims kept separate

The wider retained material includes the following unverified claims. They broaden the defensive questions without establishing additional confirmed victims or shared operators [S1].

Claimed object	What was advertised	What remains unresolved	Defensive question
Property-services files	A self-described hacktivist persona advertised property images, contracts and identity or contact fields	Declared motive and freshness are the poster's assertions; no files or access validated	Which property and customer records can external users export?
Company-register material	Privileged transfer access and a large representative-record collection	Described fields may overlap public registry information	Can provenance distinguish confidential records from public data?
Furnishing software	Customer, order, accounting, email and credential-hash material	Seller scope and current validity unverified	Which software accounts span commerce and accounting?
Cultural-media service	Profiles, access links, billing and audit records	Advertised object is broader than a customer list, but remains unverified	Can links and sessions be revoked independently?
Retail-labelled collection	A seller label paired with employment-style fields	Schema does not clearly support the advertised retail origin	Does the internal schema actually match?
Mobile-service-labelled collection	Lead, call, team and source-site fields	These fields may describe lead generation rather than subscriber systems	Which processor or campaign holds the matching fields?
French contact compilation	An explicit claim of aggregation from multiple databases	Aggregation does not establish a common original intrusion	Can repeated records and historic provenance be recognised privately?

Claimed object	What was advertised	What remains unresolved	Defensive question
Sports and housing applications	An author alleged a shared content-management weakness at two different services	Neither the flaw nor either access outcome was independently validated	Do authorised internal checks find a common supplier dependency?
Mobile subscriber material	Subscriber, device-unlock, billing and possibly active-token material	Tokens and origin untested; a row is not necessarily a customer	Can old tokens and billing links be revoked?
Insurer-related material	Employee access, data and an extortion demand	Access and deadline remain the claimant's assertions	Are employee sessions and third-party exports visible together?
Aerospace supplier files	Orders, shipping, enterprise-software records and internal files	No engineering-system or operational access demonstrated	Which commercial accounts expose supplier project context?
Cloud-provider access	A purported parent account with broad downstream reach	Claimed provider-wide populations do not establish access to each customer	Can administrative delegation and tenant boundaries be independently checked?

A separate advertisement offered caller-identity and messaging services with French destination support. It is a fraud-enablement signal, not evidence of a French organisation's intrusion. None of these observations authorises testing third-party systems or contacting a seller [S1].

KEY TAKEAWAYS

01

Use the retained forums for specific validation questions, not a national threat-rate estimate.

02

Keep source, age, record units and access validity separate in every advertisement.

03

A common label or customer folder does not establish a common operator or downstream intrusion.

CHAPTER 05

Incidents and claims by sector

THIS CHAPTER ANSWERS

Which sector cases establish a mechanism that defenders can test?

10

sector and service contexts with different evidence boundaries

5.1 How to read the selected cases 43
5.2 Public administration: identity and application access 44
5.3 Other administrative services: distinct events, not one giant breach 46
5.4 Education and research: dates and data age matter 48
5.5 Health: provider scope and claimed totals 49
5.6 Postal services, suppliers and availability 50
5.7 Banking, identity services and tourism 51
5.8 Professional services and third-party scripts 52
5.9 Additional supplier and customer-service disclosures 52
5.10 The remaining recent claims 52
5.11 Additional disclosures and their boundaries 53

CHAPTER 05

Incidents and claims by sector

IN SHORT

Official disclosures describe account misuse, excessive access, software weaknesses, supplier incidents and physical disruption. They also preserve important exclusions. Account files are not people, support records do not establish wider data exposure, and a protected private-message history is not a general messaging failure. Use each case's actual mechanism and data scope to choose a proportionate response.

5.1 How to read the selected cases

Cases below distinguish an organisation's statement, an authority's investigation, reporting that quotes a statement, and unverified market material. Publication in the window does not establish that the underlying incident began in 2026.

The selected cases also include monitor-only claims and items still being assessed. A recorded action does not make a claim true. No total in this chapter should be interpreted as a census of French incidents or unique affected people.

Sector or service	Evidence in this edition	Boundary	First response
Public administration	Account misuse, object-level weaknesses and data extraction in official reports	Several services and dates; no common actor inferred	Validate access, permissions and exports [S6][S7][S8]
Education and research	Personnel, pupil, directory and legacy payroll-related disclosures	Historical and current records can overlap	Review delegated access and retained data [S6][S34] [S38][S39]
Health	Medical-software and radiology-provider incidents	Administrative notes differ from a complete medical record	Identify supplier-held fields and active remote access [S36][S51]
Banking and finance	Financial-data access and fraudulent transactions reported separately	Financial records do not establish intrusion at every bank	Join identity validation and payment controls [S35][S49] [S50][S78]
Postal and business services	DDoS updates and a separate recipient-data incident	Availability and confidentiality are different cases	Exercise continuity and processor notification [S12] [S13][S31]
Retail and food production	Official refrigeration-controller findings	Site effects are authority-reported	Verify remote access and independent safety alarms [S10]
Tourism and leisure	Reservation-file disclosure quoted in reporting	Booking files are not unique travellers	Harden partner access and booking-related communications [S41]

Sector or service	Evidence in this edition	Boundary	First response
Sports and associations	Member-platform and permit-portal incidents	Different organisations and populations	Review membership exports and account access [S32] [S6][S7]
Professional and technology services	Internal-system disclosure and a third-party script incident	Possible exposure differs from established data theft	Review dependencies and session activity [S52][S53]
Energy and connected infrastructure	Concurrent hydroelectric targeting in an official account	Different impact from refrigeration	Involve operational and safety owners [S10]

5.2 Public administration: identity and application access

CASE G

Tax records across separate access perimeters

Public administration

Official investigation

DISCLOSURE

ANSSI published its investigation on 29 September after activity between May and August. It separates a fiscal-service perimeter from a cadastral-data perimeter [S8].

ESTABLISHED

The official investigation describes stolen legitimate credentials, sensitive applications exposed across trust boundaries, and detection gaps. It identifies lateral access from another administration as part of the sequence.

UNITS

The September operational report gives approximately 353,000 individual fiscal users, 252,000 professional fiscal users and 434,000 cadastral users. They are different populations with unknown overlap [S6].

ALTERNATIVES AND LIMITS

The figures cannot be added to count unique residents. A later advertisement does not independently establish further access or a new extraction.

RESPONSE

Test whether a valid external or partner account can cross its intended boundary. Correlate authentication with application activity and record exports, including systems omitted from routine monitoring.

Bottom line

Constrain data use after valid sign-in across trust boundaries.

The important distinction is between a legitimate credential and a legitimate action. The official account says the credentials were valid. It does not say that the resulting retrieval was authorised by the affected data owners [S8].

CASE H

H Professional-directory data after second-factor validation

Public administration

Official account; second factor validated

DISCLOSURE	The 12 November update records an advertisement on 8 October and dates extraction to 26 September. The offer concerned more than 60,000 staff and professional records [S7].
ESTABLISHED	The official account says an agent's account was misused with validation of the SMS second factor. It describes account revocation and further investigation.
ALTERNATIVES AND LIMITS	The account does not establish exactly how the second factor was obtained or approved. It does not establish an attack on every staff account.
RESPONSE	Review MFA approval and recovery paths, sessions and directory access. Do not close the case merely because a password was changed.

Bottom line

Review sessions and recovery paths as well as passwords.

This case is separate from the older jobseeker-data event behind the January sanction. Staff-directory records, jobseekers and historical sanction populations must not be merged [S7][S15].

CASE I

I Holiday-support data through partner access and authorisation weakness

Public administration

Official account; files not people

DISCLOSURE	The October update says a data sale prompted detection on 9 October. It dates automated extraction to 8–10 October [S7].
ESTABLISHED	The official account combines stolen partner credentials without MFA and an object-level authorisation weakness. It reports nearly 1.2 million files, including benefit information and children's identities.
EXCLUSIONS	The source says bank data and passwords were not involved. Files are not unique people, and a household may appear through more than one record.
LIMITS	The service was offline pending safeguards in the account. That is not a statement that every application operated by the broader organisation was affected.

RESPONSE

Test record-level permissions with an approved partner test account. Review automated retrieval, require strong authentication and verify safeguards before reopening the affected service.

Bottom line

Test object-level permissions and partner access before reopening.

5.3 Other administrative services: distinct events, not one giant breach

The official operational reports describe the following additional services. The table preserves provisional wording and mixed units [S6][S7].

Service role	Incident or disclosure context	What the source states	Limit
Administrative library portal	October; published 12 November	Stolen technical accounts may have exposed data concerning about 100 users; privilege escalation was blocked	Investigation continued
Permit-exam registration	4 October; published 12 November	Object-level weakness exposed more than 1,000 people's data, including minors	Separate from the January federation incident
Aid-administration portals	August; updated in November	Two portals experienced data extraction and received corrections	No link established to the agency's other incidents
Training-payment portal	30 September; claimed in October	Misused account and a vulnerability; 30,500 users affected	Separate portal and incident
Public-service application A	August; published in September	Professional-account misuse exposed contact data	Contact records are not unique people
Public-service support application	Late June–July; published in September	Subcontractor incident concerned 136 users and 213 support requests	Wider operational-data exposure not established
Customs messaging and exchange service	August linkage; published in September	Three staff mailboxes and an associated exchange service	No assertion of all customs systems affected
Environmental technical-control portal	September operational report	Account misuse and a portal weakness permitted enumeration of 22,000 agents or authorised bodies	Mixed unit, not a distinct-person count
Shared ministerial workspace	Detected in August	More than 300 accounts and accessible mailbox or file contents	Content scope remained under analysis
Youth-service portal	Claim notified in September	Report records a 275,000-user exposure claim	Investigation and scope remained provisional

Service role	Incident or disclosure context	What the source states	Limit
Housing-related application B	Claim notified in August	Unverified data-extraction claim	Scope and access route remained unconfirmed
Public-service application C	September report	Incident still being assessed	No established extraction, route or population
Parliamentary correspondence application	September report	Possible correspondence extraction	Conditional, with no confirmed population
Charging-session analytics	September report	102,000 charging sessions and about 100 technical accounts extracted	Neither unit is an individual vehicle owner
Urban-planning platform	Claim notified in August	Claimed extraction and suspected analytics-instance route	Origin and dates remained under investigation
Government innovation analytics	September report	118 application user accounts affected	Restricted application scope, not the whole agency
Government analytics services	September report	Two instances affected; extracted material already public	Application access still matters despite public data
Professional-qualification portal	August; published in September	Analytics-instance exploitation and user-record extraction	No distinct-person total supplied
Agricultural training platform	Early September claim	Claimed data concerning 5,265 people	Investigation continued

Some applications share a product family or a broad technical weakness. That does not establish one operator or identical data sensitivity. A public-data instance and a benefits application can need different notification assessments despite a similar access route.

The September report records mass exploitation affecting nine ministerial analytics instances and identifies CVE-2026-72898 [S6]. The vulnerability and vendor fixes were separately checked [S21][S22]. Those technical facts do not validate every large advertisement that mentions the same product.

The November report also gives a useful prevented-access example. Stolen VPN certificates were identified, but MFA prevented the connection and investigators found no other malicious activity. That should be counted as a blocked attempt within the official account, not a successful VPN intrusion [S7].

January reporting quoted a social-contribution agency on misuse of partner credentials against a hiring-declaration service. It gave 12 million potentially affected employees. The original notice was not directly read here, so the case remains an attributed report with a verification limit [S33].

5.4 Education and research: dates and data age matter

A March ministry notice reports extraction of data concerning about 243,000 personnel after an external account was impersonated. It describes identity and contact fields, absence periods without medical details, and work-contact information for tutors. The source does not establish exposure of complete health records [S38].

An April notice concerns pupil information in an auxiliary account-administration service. The incident dates to late 2025 and the exact affected population remained under assessment. It must not be converted into a verified multi-million-person 2026 incident [S39].

The summer operational account concerns incidents across 25 of 30 education authorities. It describes valid credentials, privileged accounts, additional access and data extraction. The November update reports continuing remediation and no newly observed data breach since the September report within that case's scope [S7].

These disclosures are not automatically independent populations. A staff record can appear in a personnel application, a directory and a later advertisement. The report therefore retains separate case entries without adding their headline figures.

February technology reporting quotes a research organisation's statement concerning people paid before January 2007. The disclosed data age is material. The incident does not establish that current research systems or every current employee were affected [S34].

A June government messaging statement describes one misused account and possible exposure of public-room messages and profile data concerning 73,467 agents. It says encrypted private-message history remained protected. This is separate from the later summer messaging-account incident [S42].

Education reporting quotes a January notice from a public agronomy institution describing system and mail disruption, with possible data impact still being assessed [S59]. Cybersecurity reporting quotes another institution on September extraction from an internship application, excluding passwords, login details and bank data [S60].

For defenders, historical retention is a current control issue. An old payroll-related dataset may still contain useful identity information. Review why it remains accessible, who can retrieve it and whether its retention is still justified.

5.5 Health: provider scope and claimed totals

J

CASE J

Medical software disclosed in February, detected in the prior year

Healthcare

Official disclosure of earlier incident

DISCLOSURE	Technology reporting quotes a medical-software provider's 26 February statement on detection in late 2025. It attributes unlawful access or extraction of patient-related data to the provider's account [S36].
ESTABLISHED	The reporting quotes the provider as identifying 1,500 affected physician users. Reporting discusses a much larger patient population, which is a separate unit and evidential statement [S36].
DATA SCOPE	Administrative unstructured note fields can contain sensitive information. That is different from saying that complete structured medical records, prescriptions and laboratory results were extracted.
LIMITS	Publication is within this report's window; the underlying incident began earlier. Physician users cannot be multiplied into a verified patient total.
RESPONSE	Ask the provider which fields and customers were affected. Assess unstructured note fields as well as structured clinical tables, and preserve the disclosure's date distinction.

Bottom line

Preserve data fields, units and the distinction between incident and disclosure.

A 27 February broadcaster report attributes an affected population of nearly 15 million people to the ministry responsible for health. This is an attributed ministry figure, separate from the provider's physician-user count and from claims about complete clinical records [S75].

K

CASE K

Radiology access and a later market advertisement

Healthcare

Provider update: claim larger than current estimate

DISCLOSURE	A radiology-software provider issued an initial statement on 8 November and an update on 18 November. The update describes a claim posted on the evening of 17 November [S51].

ESTABLISHED	The provider says initial analysis suggests correspondence with the earlier incident, while the precise perimeter remains under investigation. It attributes the incident to fraudulent use of customer credentials for remote access.
CLAIM BOUNDARY	The provider says its current assessment places the affected population significantly below the criminal claim. This report does not adopt the advertised 18-million-person figure.
LIMITS	The provider says it detected no further intrusion or leak after containment. That statement does not independently validate every data field in the advertisement.
RESPONSE	Affected providers should identify actual patient data, review remote-access credentials and sessions, and coordinate individual risk assessments. Unnamed downstream notices are not automatically the same incident.

Bottom line

Match actual patient data and current remote access without adopting seller totals.

Several recent monitor entries concern medical-imaging organisations or older patient datasets. Their source relationships differ. A notice that does not name the software provider should remain unlinked until stronger evidence establishes the dependency [S54].

CNIL's September hospital sanction concerns an older patient-data incident. It is useful control evidence, but it does not add a newly occurring 2026 hospital intrusion to this chapter [S55].

5.6 Postal services, suppliers and availability

CASE L

L

A business-mailing provider's September incident disclosed in November

Business services

Company and prosecutor quoted in reporting

DISCLOSURE	November reporting quotes the organisation and the Paris prosecutor concerning a September incident at a business-mailing provider. The reported population is 22 million recipients [S12][S13].
ESTABLISHED	The reported exposed fields are names and postal addresses. Reporting quotes the provider as excluding bank details and saying client organisations were informed.

LIMITS	Recipients are not the provider's corporate customers. The provider's document-processing activity does not establish that all document contents were extracted.
ALTERNATIVES	A customer's downstream notice may describe this supplier incident without a separate intrusion into that customer's systems. Such notices do not establish separate incidents where the supplier dependency is explicitly established.
RESPONSE	Controllers should identify whether their recipient records were involved, make their own risk assessment and prepare for convincing postal or digital impersonation. Preserve successive supplier scope updates.

Bottom line

One supplier event can require many separate controller decisions.

National reporting quotes a postal-service provider on renewed online disruption on 1 January and describes a preceding DDoS incident in December 2025. It quotes the provider as reporting no data leak. This availability incident is not evidence of, or an explanation for, the September recipient-data case [S31].

5.7 Banking, identity services and tourism

A February official notice says stolen credentials were used to access a financial-data service from late January. It estimates that about 1.2 million accounts may be concerned. The source explicitly says the user's tax identifier was not consulted [S35].

Financial-data services and accounts at banks are different attack surfaces. A data incident can expose account identifiers without establishing that the account holder's bank systems were accessed. Chapter 9 develops the associated fraud and verification questions.

An April identity-document portal update says 11.7 million individual accounts could be affected, subject to continuing technical findings. The source distinguished identity and contact data from attachments and biometric material excluded at that stage. The conditional wording should remain in every summary [S40].

A tourism group's May disclosure, as quoted by national reporting, concerns 1.6 million booking files. A criminal claim used a larger population and a different unit. The organisation's reported exclusion of bank data does not make booking details harmless, but the files cannot be called unique travellers [S41].

The November cooperative-bank incident is discussed separately in Chapter 9. The bank's 4 November statement reported fraudulent transactions and delayed transfers while stating that customer holdings were unaffected [S49]. Its 18 November filing attributed the attack to an external provider's platform, identified the bank's own account as affected and estimated an earnings impact of about 100 million euros [S78]. It is not an extension of the financial-data service incident [S49][S50][S78].

5.8 Professional services and third-party scripts

A market-research group's November statement confirms an internal-system incident, a complaint and an external investigation. Its statement says operations were unaffected, while the possible scope for customers, projects and partners remained under assessment. It does not establish a confirmed theft total or an actor [S52].

Separately, a researcher reported malicious JavaScript delivered through an international experimentation platform to 178 organisations on 16 November. Some French companies appear in that research. The number is global, and script delivery does not establish that every visitor lost information [S53].

The useful response is to inventory third-party scripts, identify who can change them and review relevant browser-session or application evidence. This report does not treat a researcher-listed brand as an officially confirmed French victim.

5.9 Additional supplier and customer-service disclosures

An energy supplier's October notice concerns unusual access to a commercial partner's platform, with a France-only customer scope. It says its own information systems and bank data were unaffected. This is a customer-data and partner-access case, not an industrial-control incident [S57].

A vocational-training agency's September notice concerns potential extraction involving about 1.7 million people through an external accommodation-management tool. Its own systems and services were described as unaffected. The precise scope remained under investigation, with bank and social-security information apparently excluded [S58].

The two cases demonstrate why a supplier assessment should follow the actual data and service. The identity of a large parent organisation does not establish that every service, industrial operation or legal entity in the group was affected.

5.10 The remaining recent claims

The closing-period sweep retains additional advertisements and monitor reports by role. Their authenticity, geography or original disclosure remained insufficiently established for named case treatment [S54].

Cluster	Examples retained	Status boundary	Defender's next question
Retail and consumer services	Electronics, outdoor equipment, meal delivery, specialist retailers and home projects	Claims or notices reproduced by a monitor; exact original scope varies	Does an authentic notice or internal match confirm the source?
Professional software	Recruitment, business applications, tourism software and web services	Some reports quote company notices; originals were not independently read in this edition	Which service and customer records were actually involved?

Cluster	Examples retained	Status boundary	Defender's next question
Membership and education	Tutoring, sport, associations and a community platform	Claimed rows can include historical members	Are the records current and are duplicates understood?
Housing and property	Rental matching, alleged property-company data and renovation enquiries	Some claims have conflicting provenance	Does the sample match the claimed organisation?
Public and municipal services	Waste-service email and a municipal extortion claim	Possible supplier consultation differs from confirmed extraction	Is there operator confirmation and a verified dependency?
Extortion claims	Measurement equipment, engineering, food, optical and pharmaceutical brands	Country assignment or feed correspondence remained unresolved for several entries	Is the exact legal entity and country supported?
Older or disputed material	Reconstructed hospital files, renewed membership claims and historical community data	Repost or disputed attribution, not established new intrusion	What evidence establishes age and original source?

This section summarises selected unresolved reports; it is not an itemised incident register. These items are not counted as confirmed incidents. The open questions concern source verification, entity matching and recency, rather than an assumption that every claim is false.

5.11 Additional disclosures and their boundaries

The following entries retain further source-checked disclosures. Reports quoting an organisation remain attributed reports when its original notice was not directly available. These rows are not added to a national incident or affected-person total.

Service role	Disclosure and evidence	Boundary and response
University alumni platform	April regional reporting quotes police and the university on 127,400 accessed records [S63]	Original university release not read; records are not distinct people. Validate alumni-platform permissions.
University publishing shop	September local reporting describes a malicious payment-page script and 1,332 purchasers contacted [S64]	Potential exposure may extend back to 2023; no fraudulent-payment total established. Review scripts and payment dependencies.
Research institute	August technology reporting quotes the institute's notice on data exposure after an external intrusion [S65]	Exfiltration remained unconfirmed in the quoted notice. Keep exposure separate from established theft.
Business-software provider	Original statement identifies 13 instances with contact/email extraction, five involving documents, and a separate three-instance account-impersonation scenario [S66]	Exact original publication day unresolved; do not add scenarios or infer all customers' infrastructure affected. Review each tenant and its sessions.

Service role	Disclosure and evidence	Boundary and response
Integration-service external operator	January technology reporting quotes the agency director on a supplier-side incident [S67]	Direct original not read; neither direct agency-server intrusion nor the seller's population is adopted. Preserve supplier and controller boundaries.
Hospital imaging viewer	November cybersecurity reporting quotes the hospital on supplier-linked patient-data exposure and continued imaging activity [S68]	The quoted notice excludes medical results and financial/billing data. Product link not independently established here; no affected total adopted. Review legacy supplier retention.
Student support appointments	March technology reporting quotes the issuer on 774,000 people over ten years: 139,000 with attachments and 635,000 with limited appointment, identity or contact fields [S69]	Disjoint subsets equal the reported total; these are not all current students. Review attachment retention and appointment-service access.
Regulated-owner information	March News-agency reporting quotes an authority on extraction through an enterprise account [S70]	Central system reportedly not reached; no population total or direct original notice read. Validate authorised business accounts separately.
Health-prevention document orders	August News-agency reporting quotes the agency on about 80,000 people's contact data in an outsourced platform [S71]	Health data excluded; do not infer access to core public-health systems. Review processor-held contact records.
Primary-school administration	March technology reporting quotes a notice on access to user information and pupil, family and teacher contact details [S72]	No affected total adopted from the reporting. Check account scope and family-data retention.
Admissions administration module	April original discloses October 2025 extraction affecting about 705,000 candidates from completed 2023/2025 sessions [S73]	Historical regional module, not current 2026 applications. Review legitimate staff access and anonymisation.
School-sport licensing	March technology reporting quotes the federation on November 2025 extraction and later publication; account and image-link countermeasures described [S74]	No official population or photo total adopted; the quoted initial analysis excluded financial and disability fields. Revoke residual links as well as accounts.

KEY TAKEAWAYS

01

Preserve incident dates, publication dates, data fields and units in every sector case.

02

Test valid-account permissions and supplier dependencies against the disclosed mechanisms.

03

Keep provisional and monitor-only claims visible without promoting them to confirmed national incidents.

CHAPTER 06

Hacktivism, DDoS and industrial disruption

06

THIS CHAPTER ANSWERS

What separates a public claim from demonstrated service or physical impact?

2

response tracks: digital availability and operational safety

6.1 Timeline and evidence levels 56

6.2 The refrigeration case: official impact versus public publicity 57

6.3 DDoS evidence needs service context 57

6.4 Industrial interface claims require a different boundary 58

6.5 Recent activity: 9–22 November 58

6.6 Lessons for operations and communications 59

CHAPTER 06

Hacktivism, DDoS and industrial disruption

IN SHORT

An announcement, an outage and an unsafe operating state require different evidence. The official October refrigeration case reports physical effects and a November state attribution. DDoS posts and interface screenshots do not establish comparable impact. Preserve the operator's service measurements, keep attribution tied to its source, and give industrial safety owners authority over isolation and restoration.

6.1 Timeline and evidence levels

The timeline distinguishes incident dates from disclosure dates. An official publication can update an earlier event without establishing a new attack on the publication day.

12 Aug 2026	**Tax-administration investigation** First exfiltration perimeter was publicly claimed; the later official investigation describes the route [S8].
1 Sep 2026	**State-services response** ANSSI says the reinforced response capacity was requested on this date [S6][S7].
26 Sep 2026	**Employment-service staff data** The October update dates the data extraction to this day [S7].
4 Oct 2026	**Administrative permit service** The operational update describes an object-level authorisation weakness and exposed records [S7].
8 Oct 2026	**Staff-data advertisement** The official account distinguishes the advertising date from the earlier extraction [S7].
9 Oct 2026	**Holiday-support platform** A data sale prompted detection; the reported extraction period spans 8–10 October [S7].
11 Oct 2026	**Refrigeration-controller incident** The authorities date the settings changes to the night of 11–12 October [S10].
9 Nov 2026	**French C4 assessment** An attribution report describes the earlier controller incident and its physical effects [S10].
12 Nov 2026	**CERT-FR operational update** October cases and continuing remediation are published [S7].
14 Nov 2026	**Postal-services disclosure** France 24 quotes company confirmation of a September incident [S12].
18 Nov 2026	**CNIL security decision** An anonymised sanction describes password storage, shared access and retention [S16].

The timeline does not imply that the same actor carried out these events. It places different evidence types in one chronology so that defenders can choose the appropriate validation task.

6.2 The refrigeration case: official impact versus public publicity

The C4 report says about 700 French distribution sites had refrigeration controllers affected during the October incident. It describes changed defrost settings, significant merchandise losses and fires in at least 15 cases. Those are reported official findings [S10].

The report separately mentions concurrent targeting of equipment at small hydroelectric installations, with moderate effects. It does not state that those installations had the same impact as the refrigeration sites. The two populations should not be added into one verified national equipment total [S10].

Point	Public claim or publicity	Official account	What remains unresolved here
Occurrence	Public-facing channels relayed the refrigeration event, according to C4	C4 reports controller settings changed on 11–12 October [S10]	This report holds no operator telemetry
Scale	Public claims cannot independently measure affected facilities	About 700 distribution sites in the official account [S10]	No separate Brandefense site census
Physical effects	A screenshot cannot demonstrate a fire or merchandise loss	Official report describes losses and at least 15 fire cases [S10]	No independent reconstruction of each site's consequences
Attribution	Alias use and political messaging are insufficient on their own	C4 attributes the activity to Shahid Kaveh within the Iranian cyber structure [S10] [S11]	The attribution is the authorities', not derived from our market posts
Response	A claimed recovery or channel announcement does not establish safety	Operators and authorities describe the incident within their own scope	Safe restoration requires each operator's evidence

The panel compares different kinds of evidence. It supplies no ratio between a claimant's figure and the official account. The official attribution and the physical consequences also answer different questions: who the source assesses was responsible, and what it reports happened.

6.3 DDoS evidence needs service context

A DDoS announcement establishes that a persona made a claim. An external reachability screenshot may show that one request failed. Neither establishes the duration, geographical scope or business impact of an interruption.

Operators should preserve their own availability measurements and mitigation-provider records. A service can block requests from a region or change protection settings while continuing to serve customers elsewhere. That possibility should not be converted into a claim that every reported outage was harmless.

The response question is practical: did customers lose a critical function, for how long, and through which dependency? Service-level evidence can guide mitigation and communication without settling the claimant's identity.

6.4 Industrial interface claims require a different boundary

A pictured industrial interface may be genuine, stale, simulated or copied from another source. It does not establish that the poster can change a setting. Even demonstrated access would not by itself establish a physical consequence.

The official refrigeration case provides stronger evidence because the authorities describe changed settings and reported consequences [S10]. That does not validate unrelated claims about pumps, water systems, factories or transport controls.

Give each industrial claim to the responsible operational owner. Validate asset ownership privately, review remote-access sessions and compare the current configuration with the approved operating state. Avoid reproducing third-party interfaces, addresses or credentials in public communications.

6.5 Recent activity: 9–22 November

The closing fortnight brought several different developments. The 9 November attribution report concerns an October physical incident. The 12 November operational update concerns October data events and continuing remediation. The postal-services disclosure concerns a September incident [S7][S10][S12][S13].

On 9 November, CNIL also announced the local-authority sanctions. On 18 November it published the password-storage decision and CERT-FR issued the NGINX alert. Regulatory findings and vulnerability warnings are relevant recent activity, but they are not additional confirmed intrusions [S16][S17][S23].

On 17 November, the lower chamber adopted the amended resilience and cybersecurity bill at first reading. This legislative step belongs in recent activity, while its status remains distinct from an effective national law [S61].

The recent section therefore tracks what changed in defender knowledge during the fortnight. It does not label every item as an attack that occurred during those days. This distinction is essential when planning staffing, customer notices and remediation urgency.

The 20–21 November tourism-software coverage supplies a recent availability case. In a direct trade-press interview, the provider's CEO described unlawful access, a precautionary shutdown of connected booking platforms and progressive recovery. Data leakage remained unresolved; illicit bookings were a feared risk, not an established outcome. The provider said it did not host bank data [S76].

6.6 Lessons for operations and communications

Trigger	First owner	Evidence to preserve	Initial decision
Public service named in an announcement	SOC and service owner	Claim, timestamps and actual service metrics	Increase readiness and validate customer impact
Confirmed digital interruption	Operations and provider	Availability, traffic and mitigation records	Activate agreed mitigation and factual status updates
Claimed industrial access	Operational security	Private ownership match and remote-access records	Assess exposure with the equipment owner
Unauthorised controller change	Operations and safety	Approved settings, actual process state and independent alarms	Isolate safely and control restoration
New state attribution	Intelligence and communications	Exact source, assessed actor and confidence	Update attribution language without extending it to unrelated cases

Public communications should separate service availability, data confidentiality and physical safety. A service being restored does not establish that no information was taken. Equally, a data offer does not establish a sustained outage.

KEY TAKEAWAYS

01

Match the strength of each impact claim to operator or official evidence.

02

Separate digital availability from physical safety and restoration.

03

Treat the closing fortnight as an update to knowledge, with incident dates stated separately.

CHAPTER 07

Threat actors and campaigns

07

THIS CHAPTER ANSWERS

Which actor relationships and campaign mechanisms are supported?

295

French extortion listings, distributed across many group names

7.1 Reading the relationship map 61
7.2 Ransomware and extortion 62
7.3 The official industrial attribution 65
7.4 Official espionage reporting: Turla 67
7.5 Identity-led campaigns without a common-actor claim 68
7.6 Technique mapping for defenders 68
7.7 Technical advisories are a separate campaign signal 69
7.8 A separate small-business persistence case 70

CHAPTER 07

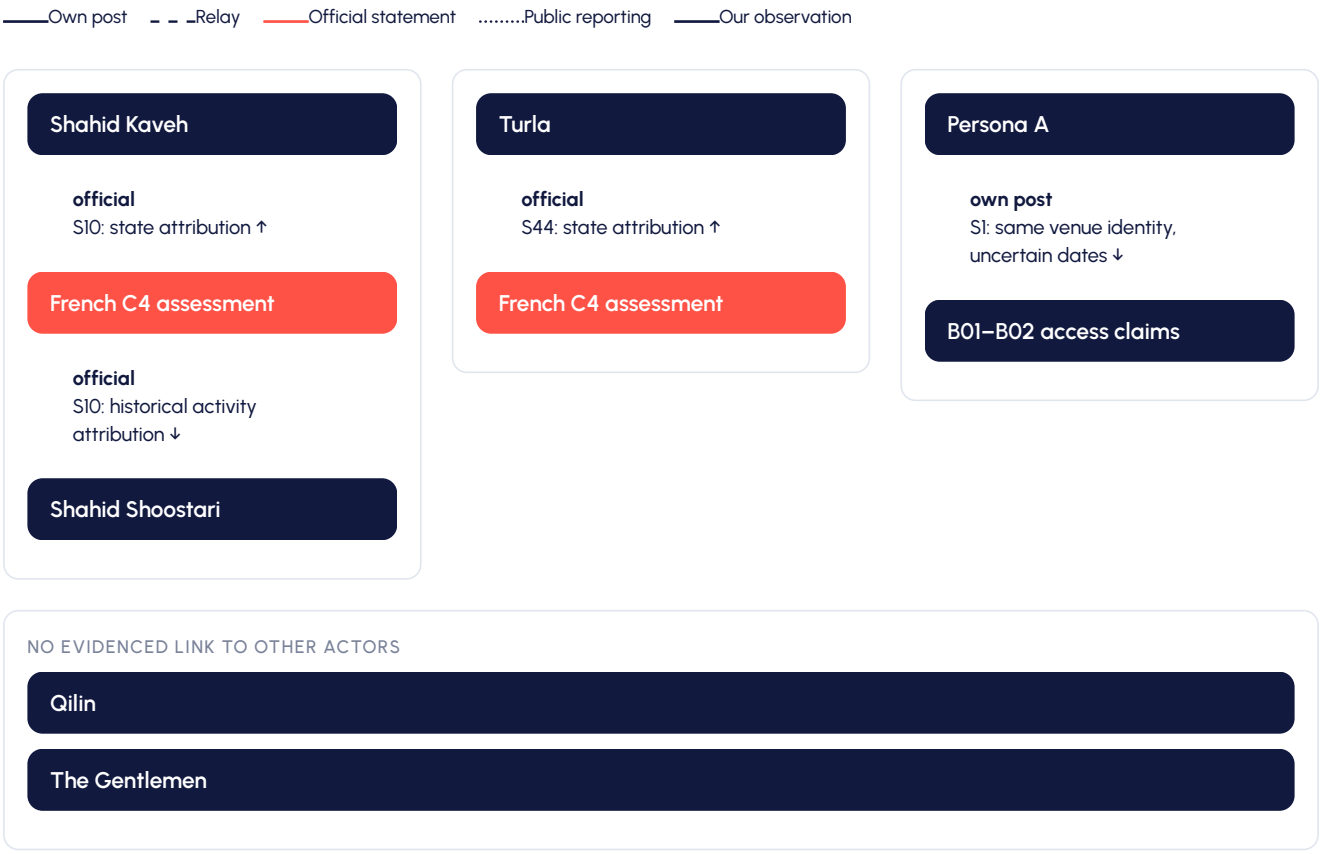
Threat actors and campaigns

IN SHORT

Extortion brands are prominent in the listing data, while the official industrial case supplies a separate state-attribution track. Data sellers and access advertisers remain unverified personas unless stronger evidence exists. Similar wording, timing or political framing does not establish shared control. Keep attribution attached to its source and make recovery depend on the observed mechanism, rather than a group name.

7.1 Reading the relationship map

The map shows official attribution links and one persona-to-post relationship. The extortion listing brands appear as unconnected nodes. Each edge carries its evidence type. A reused alias does not establish a unique person, and an advertised target does not establish access.



No evidence here connects the extortion brands, the state-attributed industrial activity and the separate market personas into one organisation. Any planning relationship between stolen data and downstream fraud is labelled as an analytical model.

7.2 Ransomware and extortion

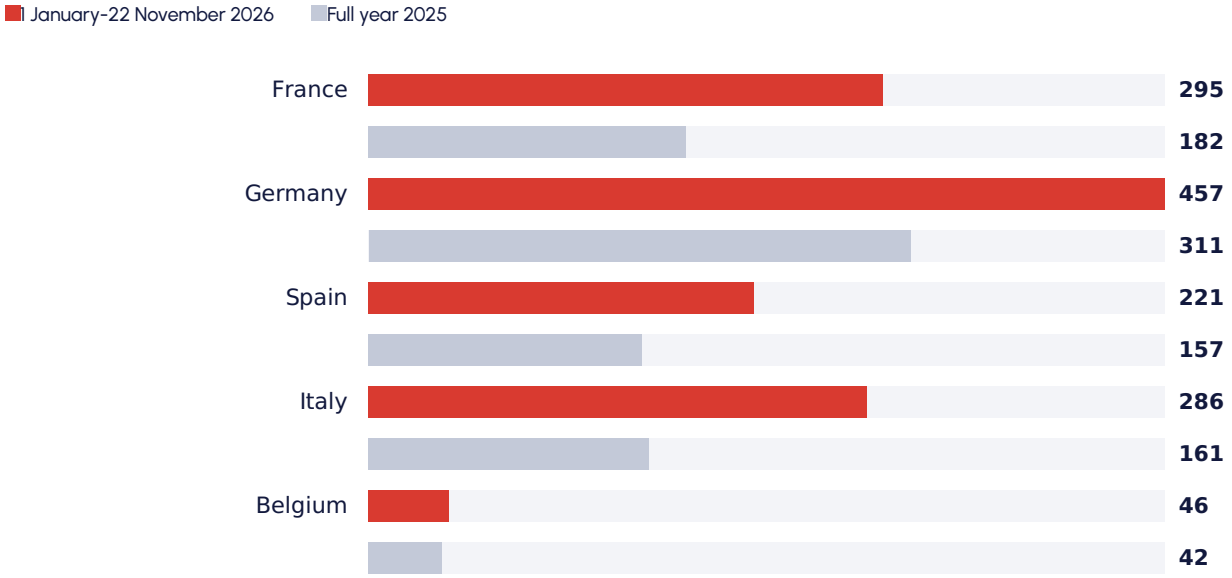
Ransompedia records 295 France-labelled listings dated within the report window. In the same snapshot, the full-year 2025 French total is 182. The observation periods differ, and the larger partial-year number does not quantify a change in national ransomware incidence [S3].

As a separate, non-comparable official baseline, ANSSI's 2025 threat panorama records 1,366 handled or reported security incidents in 2025 against 1,361 in 2024 [S79]. Within that official series, reported data-exfiltration incidents rose from 130 in 2024 to 196 in 2025 [S79].

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

The following comparison uses the same current window for France and four regional peers. The selection covers neighbouring industrial and service economies, with Belgium adding French-language and institutional connections. Listing visibility is not adjusted for population, economic size or disclosure practice.

France has 295 listings; the four peer counts describe visibility rather than national risk



Source: Brandefense Ransompedia country-labelled listings. 2026: 1 January-22 November; 2025: full year. Unmatched periods; listing dates are not incident dates or national risk rankings [S3].

Country	Window listings	All of 2025	Interpretation
France	295	182	The country in scope
Germany	457	311	Adjacent large industrial economy
Spain	221	157	Adjacent large EU economy
Italy	286	161	Large industrial and financial economy
Belgium	46	42	Adjacent economy with French-language connections

Qilin and The Gentlemen together account for 92 of the 295 France-labelled listings, or 31.2%. Other brands account for 203, or 68.8%. The distribution spans multiple listing labels and several extortion brands; it does not establish separate people behind every brand.

Listing brand	France-labelled listings	Share
Qilin	48	16.3%
The Gentlemen	44	14.9%
Coinbasecartel	13	4.4%
Lapsus$	12	4.1%
Other names	178	60.3%
Total	295	100.0%

These names are preserved as listing labels. A familiar historical brand does not establish continuity of operators, malware or access methods. Country and sector labels also need case-level corroboration before an organisation is described as affected.

Qilin

Agenda

Ransomware and extortion listing brand | Financially framed extortion claims

IN FRANCE, 2026

2026

48 French listings in the report window

CLAIMED TARGETS

Organisations described in public listing claims

SEEN IN PUBLIC REPORTING

[S3] Ransompedia records 48 French listings under this label

OUR ASSESSMENT

A frequent listing label. The count establishes public claims, without confirming encryption, theft or a unique operator. Plan recovery and data-response decisions independently of brand.

CONFIDENCE

High for the retained listing count; incident outcomes unverified

The Gentlemen

Ransomware and extortion listing brand | Financially framed extortion claims

IN FRANCE, 2026

2026

44 French listings in the report window

CLAIMED TARGETS

Organisations described in public listing claims

SEEN IN PUBLIC REPORTING

[S3] Ransompedia records 44 French listings under this label

OUR ASSESSMENT

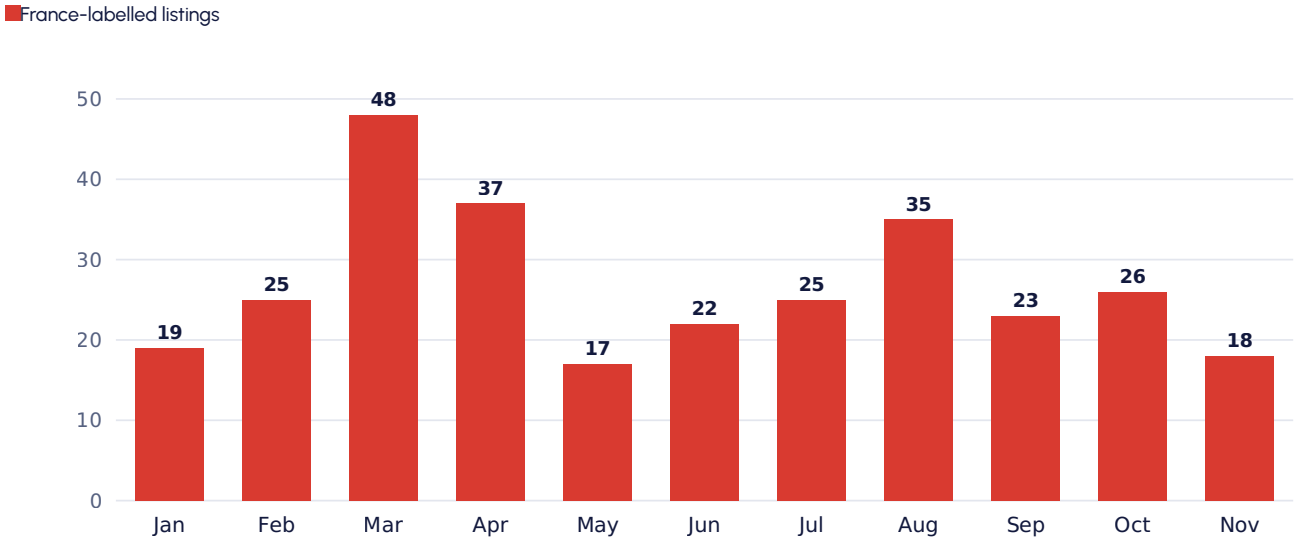
The second-largest French listing label in this snapshot. No access route is inferred from the group name.

CONFIDENCE

High for the retained listing count; incident outcomes unverified

French monthly counts range from 17 in May to 48 in March. November contributes 18 listings through the cut-off and is a partial month. A chart of listing dates cannot identify when the intrusions occurred or whether the same organisation appears more than once [S3].

France-labelled listings appear throughout the window, with November still partial



Source: Brandefense Ransompedia country-labelled listings. 2026: 1 January–22 November; 2025: full year. Unmatched periods; listing dates are not incident dates or national risk rankings [S3].

The most frequent feed sector labels include consulting, government and administration, technology, retail, construction and manufacturing. They are labels on claims. They neither reconcile directly with the selected organisation sectors nor demonstrate that one sector has weaker controls.

For response planning, separate data publication from service recovery. A restoration exercise can demonstrate continuity while leaving a confidentiality problem unresolved. An extortion communication should therefore involve recovery, privacy, legal and communications owners together.

7.3 The official industrial attribution

On 9 November, CERT-FR published the French C4 assessment of attacks affecting French interests. It attributes the October refrigeration-controller attack to the Shahid Kaveh unit within the Iranian Revolutionary Guards' electronic and cyber structure. That is the source's attribution [S10][S11].

The assessment also describes Shahid Shoostari, which it associates with the names Emennet Pasargad and Iliyanet. The French cases it discusses for that unit concern earlier years. Their inclusion in a 2026 publication does not make them new 2026 incidents [S10].

Shahid Kaveh

Public-facing aliases as attributed by C4

Industrial activity attributed by the French authorities | Attributed by French C4 to the Iranian Revolutionary Guards cyber structure

IN FRANCE, 2026

11–12 Oct
Refrigeration-controller incident in the French official account

9 Nov
C4 publishes its attribution

CLAIMED TARGETS

Refrigeration and other connected industrial equipment, as described by C4

SEEN IN PUBLIC REPORTING

[S10] C4 reports changed settings, merchandise loss and fire cases

[S11] French diplomatic authority publishes an attribution statement

OUR ASSESSMENT

Attribution belongs to the official sources. Validate industrial remote access, configuration authority and safe restoration; do not extend this attribution to unrelated claims.

CONFIDENCE
Officially attributed; no independent Brandefense attribution

Shahid Shoostari

Emennet Pasargad; Iliyanet, per C4

Earlier activity described in a 2026 official report | Attributed by French C4 to the Iranian cyber structure

IN FRANCE, 2026

9 Nov
C4 describes earlier French cases and the unit relationship

CLAIMED TARGETS

Earlier media and display-service cases described by the source

SEEN IN PUBLIC REPORTING

[S10] The official report discusses events from earlier years

OUR ASSESSMENT

A 2026 attribution publication does not make those historical cases new 2026 incidents. No relationship to the separate forum sellers is established.

CONFIDENCE

Source attribution; historical event dating preserved

The official account links several public-facing aliases to Shahid Kaveh. This report preserves that relationship only as an official attribution. It does not use an alias, a language clue or a repost alone to attribute another French event to that unit.

The defensive consequence is independent of the political assessment. Operators should know which remote paths can change physical settings, which alarms are independent, and who can authorise safe restoration. Chapter 6 separates that confirmed official account from unverified interface claims.

7.4 Official espionage reporting: Turla

On 13 July, CERT-FR published a C4 assessment reporting the targeting and unauthorised access of French entities using the Turla intrusion set. It attributes the activity to the Russian FSB's 16th Centre [S44].

The source identifies strategic government, diplomatic, defence, justice and technology contexts. Its historical account extends back to at least 2004. This publication does not establish that every described operation occurred during this report's 2026 window.

Turla

Intrusion set named by French C4

Espionage activity attributed by the French authorities | Attributed by French C4 to the Russian FSB 16th Centre

IN FRANCE, 2026

13 Jul

CERT-FR publishes targeting and attribution assessment

CLAIMED TARGETS

Strategic government, diplomatic, defence, justice and technology contexts, as reported

SEEN IN PUBLIC REPORTING

[S44] C4 reports targeting and unauthorised access of French entities

OUR ASSESSMENT

The historical campaign spans earlier years. Do not assign every described operation to 2026 or extend the state attribution to unrelated Russian-language material.

CONFIDENCE
Official source attribution; individual event dates not fully specified

The attribution is the French authorities' assessment. It is not extended to unrelated Russian-language posts, DDoS claims or extortion labels. Language alone cannot establish a state sponsor.

For defenders, maintain an investigation track for persistent access to strategic services. A market offer and a state-linked campaign report can justify different questions even when both mention the same broad sector.

Beyond the July Turla advisory, ANSSI's 2025 threat panorama reports sustained state-linked espionage against French institutional, diplomatic and industrial interests, primarily involving intrusion sets linked by the agency to Russia and China [S79][S80]. Because this edition profiles only actors with a dedicated 2026 French campaign advisory or retained corpus evidence, other state-linked intrusion sets are not profiled separately here.

7.5 Identity-led campaigns without a common-actor claim

The tax investigation, employment-service staff-data incident and holiday-support platform case all involve legitimate account access in the official account [S7][S8]. They do not establish one actor or one initial-access route.

The tax report describes stolen credentials and exposure across trust boundaries. The staff-data case says a second factor was validated. The holiday-support case combines partner credentials and an object-level authorisation weakness. A universal statement that MFA alone would have prevented every case would exceed this evidence.

The response should therefore cover several stages: account protection, recovery procedures, session review, role permissions, object-level checks and export monitoring. A control at one stage should not conceal a missing control at another.

7.6 Technique mapping for defenders

This is an analyst mapping of publicly described behaviour to ATT&CK concepts. It is not a claim that the authorities used these labels or that every technique was present in every incident [S29].

ANALYST MAPPING OF SOURCE-DESCRIBED BEHAVIOUR TO MITRE TECHNIQUES

Initial Access	Impair Process Control
T1078 Valid Accounts	T0836 Modify Parameter

Analyst mapping of source-described behaviour, not a source's original technique matrix. S7, S8, S10 and S29. [S10]

Behaviour in source	Technique concept	Source boundary	Defender's question
Use of legitimate stolen credentials	T1078, Valid Accounts	Described in the tax and operational reports [S7][S8]	Can an apparently valid session reach sensitive records without scrutiny?
Changes to industrial process settings	T0836, Modify Parameter	The official refrigeration account reports setting changes [S10]	Would an independent alarm detect an unsafe state?

The first concept concerns enterprise access. The second belongs to industrial systems. Their shared presence in a planning matrix does not imply one intrusion chain or a relationship between the actors.

For identity abuse, evidence should connect the user, session, application action and retrieved records. For controller changes, evidence should connect the authorised operator, approved configuration and independently observed process state. Those are different hunt surfaces.

7.7 Technical advisories are a separate campaign signal

The 18 November CERT-FR NGINX alert identifies two HTTP/2 vulnerabilities. NVD and F5 describe denial of service and possible code execution under stated conditions. Neither source establishes exploitation at a French organisation in this report [S23][S24][S25][S26].

The Metabase record and vendor advisory establish a critical SQL-injection issue and available fixes. The vendor reports active exploitation, but that statement does not establish that any particular French market advertisement resulted from the flaw [S21][S22].

Product and CVE	Affected scope checked	Fixed versions or branch action	Response boundary
Metabase, CVE-2026-72898	Six vendor-listed affected ranges, reproduced below	Recommended patches below; x denotes the edition	Use the vendor's exact branch guidance; review prior activity and connected secrets [S21][S22]
NGINX Open Source, CVE-2026-123633	F5 lists 1.19.7–1.30.6 and 1.31.0–1.31.8 with the relevant HTTP/2 configuration	1.30.7 or 1.31.9	Review the full product table for other packaged products [S24][S26]
NGINX Open Source, CVE-2026-123007	F5 lists 1.9.5–1.30.6 and 1.31.0–1.31.8 with HTTP/2	1.30.7 or 1.31.9	A patch action is not proof that earlier unauthorised activity is absent [S25][S26]

Metabase's affected ranges and recommended patches are reproduced separately as listed by the vendor [S22].

Affected range	Recommended patch
>= x.58.0, < x.58.23	x.58.24
>= x.59.0, < x.59.20	x.59.21
>= x.60.0, < x.60.16	x.60.17
>= x.61.0, < x.61.10	x.61.11
>= x.62.0, < x.62.8	x.62.9
>= x.63.0, < x.63.3	x.63.5

For NGINX Plus, the two vendor tables give different branch fixes. The patch reference deliberately limits the numerical summary to Open Source. Owners of Plus and embedded products should use the applicable vendor row, rather than translating the Open Source version into a different product [S26].

CERT-FR recommends disabling HTTP/2 as an interim measure while awaiting patches [S23]. Owners should test the operational effect and verify the resulting configuration. This report supplies no exploit, production test command or claim of validated mitigation at a third party.

7.8 A separate small-business persistence case

Cato CTRL's 16 June research describes Poisson activity from 30 March–1 May against French individuals and an automotive small business. It reports credential theft and independent remote-access paths surviving command infrastructure disruption. Its victim descriptions are internally inconsistent, so no population total is adopted [S62].

The lesson is to inspect endpoints, authorised remote tools and persistence before declaring containment. The source does not establish a link to this report's sellers or ransomware groups [S62].

KEY TAKEAWAYS

01

Keep extortion labels, criminal personas and official state attributions on separate evidence tracks.

02

Map the observed mechanism to an investigation that the relevant owner can perform.

03

Verify affected branches and prior activity without treating an advisory as a confirmed French incident.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How can exposed personal information become a convincing fraudulent request?

4

mechanism sections covering five official campaign examples

8.1 Data offers and downstream fraud are different observations 72
8.2 Payment-card material in posts: a narrow view 72
8.3 False assistance after a data breach 73
8.4 Tax-refund and false-authority pretexts 73
8.5 Messaging-device pairing and account trust 73
8.6 Crypto-service information and physical threats 74
8.7 Enforcement as a separate evidence track 74
8.8 Prices and advertised services 74

CHAPTER 08

The fraud economy

IN SHORT

Accurate personal details can support impersonation without giving a criminal control of a bank or public service. Five official warnings describe false deletion assistance, tax refunds, judicial summons, messaging-device pairing and crypto-service impersonation. Payment-card material in posts supplies only a narrow additional view. Treat identity facts as potentially known, verify requests through a trusted independent channel, and test sensitive transactions rather than relying on recognition alone.

8.1 Data offers and downstream fraud are different observations

An advertisement establishes that information or access is being marketed. It does not establish that a buyer obtained it, that the data is genuine, or that a later fraud used those records. The report does not draw a common-operator link from a seller to a fraud campaign without supporting evidence [S1].

The connection is useful as an analytical model. If accurate customer or administrative information becomes available, a caller can use it to make a pretext more credible. The validation question is whether the organisation's process still requires independent authority for the requested action.

The relevant facts can differ by service. A tax-related message may quote an administrative context. A booking message may quote a real reservation. A banking caller may know the institution and the account holder's identity. Familiar details should not substitute for verification of the request.

8.2 Payment-card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

This section presents a limited view of France-associated payment-card observations. These figures do not measure national card theft, active cards, completed transactions or fraud losses.

The aggregate contains 11 distinct France-associated cards in 5 retained records. Of these, 1 is issuer-associated and 10 are country-only. These disjoint categories sum to 11 [S4]. Its limits also apply when discussed in the banking chapter or method appendix. An absence in this narrow view cannot establish that a bank, issuer or customer population had no exposure.

A poster's claim that a card is active or a payment succeeded remains a claim. Card validity and completed payments are not established. Fraud-response decisions require an issuer's own validation and transaction evidence.

8.3 False assistance after a data breach

CNIL's 24 June warning describes unsolicited organisations claiming to help people whose information has appeared in a breach. Some messages use genuine personal details and offer assistance to remove information from the internet. CNIL says these approaches do not come from, or operate in partnership with, the regulator [S43].

The mechanism matters because it reuses the victim's awareness of an earlier incident. A person expecting protective advice can be approached with a service that appears to solve the same problem. The warning is not evidence that every unsolicited offer uses stolen data.

Controllers should prepare a recognisable official support channel in their own breach notice. Explain what the organisation will ask for and how a person can verify contact. Avoid directing individuals to an unverified intermediary simply because it knows accurate details.

8.4 Tax-refund and false-authority pretexts

Cybermalveillance.gouv.fr's tax-refund warning describes emails, SMS and calls directing people to false pages for personal, tax-login and bank information. It was published on 15 July 2026 and updated on 8 September 2026 [S46].

The practical test is whether the recipient can verify the request through the service they normally use, rather than through a link or telephone number supplied in the message. A real refund season does not authenticate an individual message.

On 11 August, the Gendarmerie warned of a rise in false judicial summons seeking an alleged settlement payment. The article discusses earlier arrests, including a 2023 operation. That historical enforcement material is not a newly completed 2026 takedown [S47].

The report omits threatening wording and personal material from these messages. The relevant mechanism is impersonated authority combined with pressure to pay. Finance and customer-service teams should recognise the request pattern without reproducing the intimidation.

8.5 Messaging-device pairing and account trust

Cybermalveillance.gouv.fr's warning about false contest votes, published on 27 October 2026 and updated on 3 November 2026, describes links that persuade messaging users to connect an additional device. The account's contacts can then receive messages that appear to come from someone they know. This abuses a legitimate account function; it does not establish a messaging-software vulnerability [S56].

A separate CERT-FR alert, published on 20 March 2026 and updated on 18 June 2026, describes sensitive messaging accounts being accessed through legitimate account or pairing functions and impersonated support. Its scope extends beyond a claim about one commercial messenger. It does not establish that users' phones or encryption protocols were defeated [S37].

The response should review linked devices, recovery paths and suspicious support approaches. For organisations using messaging in sensitive workflows, determine which requests require verification outside the conversation. An existing conversation and a familiar account are not sufficient authority for a payment or access change.

8.6 Crypto-service information and physical threats

Cybermalveillance.gouv.fr's warning about crypto-asset services describes impersonation of employees, anti-fraud services or law enforcement following personal-data disclosures. It also records a Paris J3-directed investigation. It was published on 22 January 2026 and updated on 8 June 2026 [S45].

The warning describes a broader risk than a password leak alone. Account-service information can identify people for tailored demands. The report does not repeat personal details or infer that every service user faces the same level of threat.

Security, fraud, privacy and relevant physical-security owners should agree an escalation route for credible threats. A customer-facing message should explain how to verify contact and seek assistance without suggesting that a caller's knowledge establishes legitimate authority.

8.7 Enforcement as a separate evidence track

On 8 October, the Gendarmerie's judicial-police publication described the closure of three sites used to distribute stolen intimate material. It reports an investigation directed by Paris J3, two suspects arrested in France and a population exceeding 17,000 victims across countries [S48].

The multinational victim figure is not a count of French victims. Arrests are not convictions, and the enforcement announcement does not establish that every account-advertising persona in the corpus belonged to that operation.

The case shows why account security also has a privacy and personal-safety dimension. Organisations should preserve evidence, support affected people and avoid publishing identifiers or sensitive content merely to demonstrate that a claim exists.

8.8 Prices and advertised services

Asking prices in retained posts are properties of those advertisements [S1]. They do not establish a market price, the authenticity of an offer, a completed transaction or the value of the underlying information.

When an offer mixes record counts, account access and service promises, the units should remain separate. A low price does not demonstrate fabrication, and a high price does not demonstrate quality. Triage should begin with provenance, recency and internal relevance.

KEY TAKEAWAYS

01

Treat accurate personal details as insufficient authority for a sensitive request.

02

Keep the link from advertised data to downstream fraud labelled as an analytical model unless proven.

03

Review messaging, recovery and support channels alongside payment controls.

CHAPTER 09

Banking and finance deep dive

09

THIS CHAPTER ANSWERS

Which financial decisions require identity, supplier and transaction evidence together?

3

distinct surfaces: customer identity, financial-data access and payment operations

9.1 The selected banking universe 77

9.2 Financial records do not establish access to every bank 78

9.3 Fraudulent transactions and service interruption 78

9.4 A joint validation table 79

9.5 DORA and operational evidence 79

9.6 Priorities for financial teams 79

CHAPTER 09

Banking and finance deep dive

IN SHORT

Financial risk in this edition comes from several different surfaces. An official notice about a financial-data service concerns data access. A cooperative bank disclosed fraudulent transactions and delayed transfers. Card material in retained posts has a much narrower scope. Current credential listings concern 16 of 30 assessed financial-service domains. Join identity and fraud decisions, verify payment authority independently, and test critical financial-service dependencies.

9.1 The selected banking universe

The selection includes thirty banking, payment, investment and financial-infrastructure domains, all with exposure observations [S2]. It is not a list of thirty independent licensed deposit-taking banks. Related entities and different services can appear separately.

16 of 30 assessed financial-service domains had a credential listed for sale when checked. Device associations total at least 115,930, including 701 employee-classified associations. Neither population independently establishes intrusion into a bank.

Signal	Selected banking and finance population
Exposure-assessed domains	30
Current credential listings	16 domains
Device associations, at least	115,930
Employee-device associations	701
Credential records	373,568
Document associations	327
Passive-observed domains	27
DMARC reject or quarantine	23 of 27

Source: exposure and passive observations [S2]. No banking or individual exposure rating is published.

The limited card figures do not count active cards, successful payments or bank intrusions [S4]. A bank without an attributed card in this view cannot be described as unexposed.

A credential associated with a bank domain may concern staff, a customer email service or another account context. Validate current listings with identity operations and customer fraud teams. Review employee-classified devices with the endpoint owner before inferring who owns every other associated device.

9.2 Financial records do not establish access to every bank

The February official notice describes access to a financial-data service after a public official's credentials were stolen. It says the access began in late January and that about 1.2 million accounts may be concerned. The stated fields include account identifiers, account-holder identity and address [S35].

The notice explicitly says the tax identifier was not consulted. That exclusion takes precedence over broader secondary reporting. An accurate financial-information summary should not add an identifier that the primary source excludes.

This is a financial-data access case. It does not establish that each associated bank was intruded upon, that account balances were changed, or that the same number of distinct people was affected. One person can hold several accounts.

The defensive implication is about persuasive contact. A caller who knows a customer's bank or account identifier may sound credible. Banks and payment firms should test whether customer verification still relies on information that is no longer reasonably secret.

9.3 Fraudulent transactions and service interruption

Crédit Mutuel Arkéa's 4 November statement confirms an attack that enabled fraudulent transactions. It describes temporary suspension of some transactions, progressive resumption and delayed execution of some transfers. The bank says customer holdings were unaffected, without specifying an entry route in that initial statement [S49].

Reuters' 5 November follow-up reports a bank-estimated amount of around 100 million euros [S50]. In its 18 November regulatory filing, the bank states that the attack came through an external provider's platform and affected the bank's own account [S78]. The filing estimates an earnings impact of about 100 million euros, which remains an attributed incident-level estimate rather than a national cyber-loss statistic or a customer-loss total [S50][S78].

These dated disclosures distinguish the initial 4 November customer-reassurance notice from the 18 November filing on the external provider route and own-account scope [S49][S78]. The public filing does not identify the external provider, so no provider name or software flaw is added here.

The response lesson is to separate transaction integrity, customer holdings and service availability. A bank can temporarily delay legitimate transfers as a containment measure while investigating fraudulent movements. Those outcomes need different communications and evidence.

9.4 A joint validation table

External or internal signal	What it can support	What it cannot establish alone	First accountable owner
Financial-data disclosure naming account identifiers	Increased readiness for convincing impersonation	Intrusion at every associated bank	Fraud and customer operations
Credential or access advertisement	Account and session validation	A working login or bank-wide incident	Identity and response
Card-related post within this report's narrow scope	Issuer-side validation where independently justified	Active card, successful transaction or fraud loss	Card fraud operations
Unexpected payment instruction	Independent verification and transaction review	Legitimate authority because the sender knows customer details	Finance and fraud
Supplier incident	Scope, dependency and reporting assessment	Intrusion into the customer's own systems	Procurement, response and privacy
Transfer delay during containment	Service-impact and communications assessment	Loss of customer holdings	Service operations and communications

9.5 DORA and operational evidence

DORA applies to financial entities within its scope from 17 January 2025. ACPR's material identifies ICT risk management, incident reporting, resilience testing and ICT third-party risk as its core areas [S19]. These duties require legal applicability and current reporting-channel checks.

A financial entity should map its critical functions to the actual ICT providers, data flows and recovery paths. A supplier register is useful only if the institution can connect an incident notice to a specific service and business decision.

Test whether the same incident record can support technical response, supervisory classification, privacy assessment and customer communications. The facts can be shared while the legal tests remain distinct. A generic 72-hour statement should not replace instrument-specific reporting analysis.

9.6 Priorities for financial teams

Validate access. Match an external signal to an active account and review relevant sessions before choosing a disruptive response. Historical or unmatched material needs a documented disposition rather than an automatic mass reset.

Verify instructions. Require independent authority for a new beneficiary, changed bank details or an exceptional transfer. A convincing narrative, known contact details and an existing message thread can all be part of the deception.

Protect service continuity. Rehearse how containment affects transfers, customer access and dependent institutions. Agree who can suspend a function, how alternatives are communicated and what evidence permits resumption.

Exercise suppliers. Ask a critical provider to send an initial incident alert with uncertain scope. Measure whether financial, privacy and response teams can reach a documented decision without waiting for a final report.

KEY TAKEAWAYS

01

Separate financial-data access, payment integrity and service availability.

02

Keep bank-estimated loss figures and narrow card observations within their actual scope.

03

Join identity, fraud and supplier evidence before deciding who must act.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which rules and official findings should change current operations?

3

distinct decisions: protect data, assess notification and document remediation

10.1 Duties that already apply 82
10.2 NIS2: first-reading adoption is not an effective date 83
10.3 January sanctions concern earlier incidents 83
10.4 November findings make shared access a current issue 84
10.5 Coordination and evidence preservation 84
10.6 What CISOs should do now 85

CHAPTER 10

Regulatory and national response

IN SHORT

Personal-data security duties already apply. Financial entities also face DORA within its scope. ANSSI still presents the French NIS2 framework as a transposition process and its reference document as a working text. Recent CNIL decisions concern authentication, supplier access, logging and retention. Assign a legal owner to each applicable instrument, and test notification with incident response and suppliers.

10.1 Duties that already apply

The table separates existing duties from preparation for a future national framework. It is an operational summary, not legal advice.

Instrument	Scope and status	Operational requirement	Evidence to retain
GDPR Article 32	Controllers and processors within scope	Security measures appropriate to risk	Access decisions, testing, detection and recovery records [S18]
GDPR Article 33	Personal-data breach notification to the authority, unless the breach is unlikely to result in a risk to individuals' rights and freedoms	Notify without undue delay and, where feasible, within 72 hours of awareness	Awareness timeline, risk assessment, notification and updates [S18]
GDPR Article 34	Communication to individuals when the breach is likely to create a high risk, subject to its exceptions	Communicate without undue delay in clear language	Decision, affected population, message and practical advice [S18]
GDPR Article 33(2)	Processor becoming aware of a personal-data breach	Notify the controller without undue delay	Supplier alert, initial scope and subsequent changes [S18]
DORA	Financial entities within its scope; applicable since 17 January 2025	ICT risk management, incident reporting, resilience testing and ICT third-party risk	Classification decisions, reports, tests and contractual information [S19]
French NIS2 preparation	ANSSI describes ongoing transposition and a working reference document	Prepare scope and controls; verify enacted requirements before treating drafts as duties	Applicability analysis and current official text [S20]

The 72-hour period is not a universal deadline for every cyber event. Article 33 requires authority notification unless the breach is unlikely to result in a risk to individuals' rights and freedoms. A controller should document the decision even when notification is not required [S18].

Individuals' communications use a different test. High risk to their rights and freedoms matters, and the message must explain the nature, likely consequences and protective measures. A generic reassurance or a helpdesk telephone number does not necessarily provide the required substance [S14][S18].

Suppliers should not wait for a complete forensic report before giving the controller an initial alert. Early information can be incomplete and still support the controller's assessment. Record what was known at each decision point and update the assessment when the facts change [S18].

10.2 NIS2: first-reading adoption is not an effective date

At the cut-off, ANSSI's page describes the national transposition process and invites future essential and important entities to begin preparation. It says the Référentiel Cyber France has been available since 17 March 2026 as a working document [S20].

The legislative record shows that the lower chamber adopted an amended bill at first reading on 17 November 2026. The official record still presents a bill, not a promulgated law. This is a material closing-fortnight development [S61].

The ANSSI page describes its reference document as non-mandatory by default. This report therefore does not turn a working version into an enacted national obligation. Nor does it assume that a company's sector alone determines its legal classification.

The preparation task is still concrete. Identify potentially covered legal entities, critical services, management accountability, reporting contacts and third-party dependencies. Compare existing controls with the official reference text, while legal counsel verifies the actual requirements and transition provisions that apply.

A control programme can proceed while the legal timetable changes. Identity protection, incident handling and supplier management already have evidence in the incidents described here. Their business case does not depend on presenting a draft as law.

10.3 January sanctions concern earlier incidents

CNIL's 14 January announcement describes fines of 27 million euros and 15 million euros against two telecom entities. It concerns an October 2024 incident involving data attached to 24 million subscription contracts. Contracts are not unique people, and the sanction is not a new 2026 intrusion [S14].

CNIL identified weaknesses in remote-access authentication and detection of abnormal behaviour. It also found problems with the information given to affected people. For the mobile entity, its decision additionally addressed excessive retention [S14].

The operational lesson is that an access-control programme needs evidence at several levels. A configured remote-access service, a deployed detection tool and a sent notice do not independently establish that the controls met their purpose.

The regulator's 29 January employment-service announcement concerns an incident in the first quarter of 2024. CNIL describes social engineering of partner-adviser accounts, overly broad permissions and insufficient logging [S15].

CNIL also says that adequate measures had largely been identified in advance but had not been implemented. That finding supports a board-level closure test: a risk register or impact assessment should identify who verifies that the promised control actually works [S15].

10.4 November findings make shared access a current issue

On 9 November, CNIL announced ten simplified sanctions involving local authorities and a public establishment. The findings include inadequate administrator authentication, persistent supplier access, shared accounts, ineffective logging, weak segmentation and obsolete systems [S17].

The fines ranged from 3,000 to 20,000 euros under that procedure. Those amounts are not a general GDPR maximum, a price for non-compliance, or proof that all ten bodies suffered a new intrusion during November [S17].

The regulator also addressed security authorisation for administrative systems and impact assessments for video-surveillance processing. Those findings should remain within their stated legal context. A security team should involve the appropriate administrative and privacy owners rather than applying one generic compliance checklist [S17].

On 18 November, CNIL announced a 5-million-euro sanction against an unnamed company. It described customer passwords held in plain text, shared staff credentials and excessive retention. The regulator deliberately withheld the company's name; this report does the same [S16].

The decision supports immediate checks of password storage and individual accountability. It does not establish a newly disclosed theft of customer passwords. An inspection finding and a confirmed intrusion remain different evidence categories.

10.5 Coordination and evidence preservation

ANSSI's operational updates describe technical assistance, remediation and central crisis communication for the state-services campaign [S6][S7]. Those activities do not replace a controller's privacy assessment or a judicial investigation.

Create a shared incident timeline with separate fields for discovery, awareness, containment, restoration, notification and later confirmation. Assign an evidence owner who can explain why each timestamp exists. Avoid substituting the date of a press article for the date the organisation became aware.

Preserve the facts needed for several audiences. Technical responders need account, session, application and export evidence. Privacy teams need the data categories and risk to individuals. Service owners need continuity and recovery evidence. Investigators may need a preserved chain of custody.

The communications owner should maintain a versioned statement of what is known. An actor's number should remain labelled as an actor's number until independently supported. Corrections should state which measure changed, rather than silently replacing a figure.

10.6 What CISOs should do now

Decision	Accountable owner	First test	Completion evidence
Map current obligations	Legal and compliance	Classify a realistic supplier incident under each applicable instrument	Approved duty and contact matrix
Validate claimed remediation	CISO and audit	Choose a previously accepted risk and demonstrate the promised control	Technical result and business sign-off
Exercise notification	Privacy and response	Run the clock from first awareness with incomplete supplier information	Decision log and usable draft notification
Test communications	Communications and privacy	Ask an unfamiliar reader what the notice says they should do	Revised plain-language notice
Review retention	Data owners	Identify unnecessary historical exports and expired records	Approved deletion evidence and exception register

KEY TAKEAWAYS

01

Apply current data-security and financial-resilience duties while verifying the national NIS2 timetable.

02

Treat regulatory decisions as control evidence within their actual incident dates.

03

Test notification, individual accountability and remediation rather than relying on policy documents alone.

CHAPTER 11

Outlook and conditional scenarios

11

THIS CHAPTER ANSWERS

Which judgements guide planning, and what would change them?

5

judgements with a stated limit and a change signal

11.1 Key judgements 87
11.2 What would change the assessment 88
11.3 Conditional scenarios 88
11.4 Avoiding false certainty 89

CHAPTER 11

Outlook and conditional scenarios

IN SHORT

Identity-led data retrieval, supplier concentration and recovery remain practical priorities. Public listings also support continuity planning across sectors. The industrial-controller incident requires a safety response beyond ordinary IT restoration. These are conditional planning judgements, not attack probabilities. Review them when validated account activity, new official findings or measured operational effects change the evidence.

11.1 Key judgements

Confidence applies to each proposition, not to an actor or a whole chapter. A well-supported control priority can coexist with uncertainty about who performed a particular intrusion.

Judgement	Confidence and basis	Limit	Change signal
Valid-account data use deserves immediate attention	High for the control priority; repeated mechanisms in official investigations [S7][S8][S9]	Does not establish the dominant route across all French incidents	Newly verified cases show a different route or controls prevent the same retrieval pattern
Supplier notification deserves joint exercises	High for dependency management; the postal-services disclosure and official supplier findings [S12][S13][S17]	No national supplier-incident prevalence estimate	A processor cannot identify customer scope or an exercise misses a duty
Recovery investment remains justified	High for preparedness; 295 France-labelled listings in this window [S3]	Claims do not verify encryption, business losses or unique victims	Confirmed interruption or a failed restoration test changes service priorities
Industrial remote access needs safety ownership	High for the specific need; the authorities report physical effects [S10]	Does not establish the same exposure at every industrial operator	Unauthorised setting changes or unsafe alarms require operational escalation
New advertisements will require freshness checks	Moderate as a planning judgement; retained claims and official warnings about republication [S1][S9]	An advertisement date is not a theft date	Matching current records, sessions or independent disclosures establish recency

A low-volume channel can still matter if it advertises valid access. Conversely, a high-volume country tag can carry repeated promotion or international lists. The information's ability to change a decision matters more than the count alone.

11.2 What would change the assessment

Account evidence. A match to an active privileged account, an unusual session and an unexplained export would justify incident escalation. A historical password that was already invalidated would support a different, documented disposition.

Supplier evidence. A processor's initial notice may broaden or narrow as investigation proceeds. A change in data categories matters more than a larger headline population if it introduces financial, health or minor-related information.

Operational evidence. A public claim about equipment does not establish a physical effect. An unauthorised configuration change, an independent alarm or an operator-confirmed interruption would change the assessment and the response owner.

Attribution evidence. A shared slogan or simultaneous announcement does not establish shared control. A new official attribution or a substantiated technical relationship should update the actor map with its source and confidence.

Coverage evidence. Account and ownership validation can change priorities within the assessed exposure portfolio. The selected domains do not become a national sample, and historical records do not establish current access.

11.3 Conditional scenarios

These scenarios are planning assumptions. They carry no numerical probability, promised outcome or estimate of national financial loss.

Scenario	Trigger to watch	Initial response	Evidence for closure
A newly advertised dataset concerns active customers	Internal matching confirms current records or an official notice confirms the source	Preserve the claim, scope affected data and investigate access	Account, application and notification dispositions
A partner account retrieves unusually broad records	Export and lookup behaviour departs from its authorised business task	Limit access, preserve sessions and involve the application owner	Reproduced authorisation boundary and explained export activity
A critical supplier reports an uncertain incident	Initial notice identifies a relevant service but not the affected population	Convene privacy, procurement and service owners	Successive scope updates and a recorded notification decision
A political announcement names a public service	Claim is followed by operator-confirmed interruption	Activate service mitigation and factual status communications	Service metrics and provider incident record
Remote settings change on connected equipment	Operator confirms an unauthorised or unsafe state	Isolate remote access under the safety plan	Safe operating state, reviewed access and owner-approved restoration

11.4 Avoiding false certainty

The same advertisement can support several explanations: an original seller, a reseller, copied promotion, mixed historical records or fabrication. The correct next step is to seek evidence that distinguishes those explanations.

An official incident report may also remain provisional. Its statement that an investigation continues is material. Preserve that limit in the summary, the case card and the recommended action, especially when an actor advertises a larger figure.

The report's conclusions should be reviewed when new evidence arrives, not only at the next annual edition. An account-validation result or a supplier update can change an operational decision faster than a national trend chart.

KEY TAKEAWAYS

01

Attach confidence to a specific proposition and record its limits.

02

Use observable triggers to change response, ownership and urgency.

03

Keep scenarios conditional until account, service or official evidence supports a stronger conclusion.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who acts over the next three months, and what demonstrates progress?

20

actions with an owner, trigger and completion evidence

12.1 The 30/60/90-day lanes 91

12.2 What completion means 94

12.3 By role 94

12.4 How Brandefense can help 95

CHAPTER 12

Action plan

IN SHORT

Start with access that can retrieve sensitive records or alter essential operations. Then test suppliers, restoration and fraud decisions. Finish with independent validation and removal of obsolete access. The plan contains 20 actions across 30, 60 and 90 days. Assign each action to a business owner and require evidence of the resulting behaviour, rather than counting policies or tools.

12.1 The 30/60/90-day lanes

The time periods are proposed planning intervals, not legal deadlines. An active incident or applicable notification duty takes priority.

Act immediately for exposed, affected deployments or an applicable vulnerability with reported exploitation. Infrastructure and application owners should patch or apply vendor-supported interim measures and investigate prior activity [S22][S23]. Record deployed-version evidence, remediation evidence and the investigation disposition. The 60-day advisory row covers broader inventory reconciliation.

30 days		
Review every current credential or access claim that matches your organisation; distinguish active, historical and unmatched signals	OWNER Identity and response	COMPLETION EVIDENCE A disposition with account validity, session review and escalation decision
Enforce strong authentication for privileged, remote, supplier and partner access where business risk warrants it	OWNER Identity and service owners	COMPLETION EVIDENCE Tested sign-in, recovery and emergency-access paths
Remove broad lookup permissions that exceed the user's business role	OWNER Application and data owners	COMPLETION EVIDENCE A valid test user cannot retrieve another user's unauthorised records

Alert on unexpected bulk retrieval with account and application context

OWNER

SOC and application owners

COMPLETION EVIDENCE

An authorised simulation produces a usable alert and response record

Confirm incident contacts and initial-alert terms for processors holding sensitive records

OWNER

Procurement and privacy

COMPLETION EVIDENCE

Successful contact test and agreed scope-update process

Review industrial remote access and safe local operating procedures

OWNER

Operations and safety

COMPLETION EVIDENCE

Approved access map, isolation test and safe fallback procedure

260 days

Investigate matched active credentials beyond password reset; review sessions and devices where justified

OWNER

Identity and endpoint response

COMPLETION EVIDENCE

Session revocation, device assessment and documented closure

Replace shared supplier administration with individually attributable, approved access

OWNER

Infrastructure and suppliers

COMPLETION EVIDENCE

Named accounts, time-limited approvals and reviewed activity records

Test object-level authorisation on sensitive applications under an approved assessment

OWNER

Application security

COMPLETION EVIDENCE

Failed unauthorised retrieval and retested corrections

Restrict exports to necessary data and authorised business purposes

OWNER

Data owners

COMPLETION EVIDENCE

Export inventory, access decision and a test of unusual retrieval

Restore a critical service using protected backups and separate recovery credentials

OWNER

Infrastructure and service owner

COMPLETION EVIDENCE

Recovery time, integrity check and business acceptance

Exercise a supplier incident while affected-person scope remains uncertain

OWNER

Privacy, response and procurement

COMPLETION EVIDENCE

Awareness timeline, initial decision and revised scope assessment

Reconcile the wider application inventory with relevant advisories and deployed branches; the immediate trigger above takes priority

OWNER

Infrastructure and application owners

COMPLETION EVIDENCE

Inventory coverage, deployed-version evidence and tracked remediation decisions

Rehearse a convincing caller who knows accurate customer details

OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Independent verification blocks an unauthorised payment or account change

Test service disruption communications and upstream mitigation contacts

OWNER

Operations and communications

COMPLETION EVIDENCE

Measured activation time, tested alternate channel and factual status statement

390 days

Remove obsolete partner, emergency and migration access after business review

OWNER

Identity and business owners

COMPLETION EVIDENCE

Approved removals and justified, time-limited exceptions

Validate logging from identity to application and data export

OWNER

SOC and assurance

COMPLETION EVIDENCE

A complete reconstructed test timeline with accountable users

Reduce unnecessary historical records and uncontrolled exports

OWNER

Privacy and data owners

COMPLETION EVIDENCE

Approved deletion evidence and tested retention exceptions

Re-test industrial configuration recovery with independent safety monitoring

OWNER

Operations and safety

COMPLETION EVIDENCE

Safe restoration, alarm validation and supplier access review

Report unresolved exceptions and test outcomes to management

OWNER

CISO and assurance

COMPLETION EVIDENCE

Decision record with owner, due date, residual risk and validation method

12.2 What completion means

A deployment record is an input, not a result. Strong authentication should be tested through normal access, account recovery and emergency procedures. If an alternative path bypasses the control, the business owner should understand and approve that residual risk.

An alert should reach someone who can act. Test whether it contains the account, application, business purpose and retrieval context needed for a decision. A generated event that nobody owns does not close the detection action.

A restoration test should demonstrate the business service, not just the recovery of a file. Check data integrity, dependencies, credentials, customer-facing functions and the authority to resume operations. Record what the test did not cover.

An industrial test requires operational approval and safe conditions. Use a controlled exercise rather than changing production settings solely to demonstrate a security point. The safety owner determines the acceptable test and restoration evidence.

12.3 By role

Role	First question	Useful evidence	Escalation trigger
CISO	Which service has the largest unresolved dependency?	Tested access and recovery results	Repeated failed control or unowned exception
SOC	Can we connect a valid session to unexpected retrieval?	Account, application and export timeline	Unexplained sensitive access or bulk extraction
Identity	Is the advertised account active and still trusted?	Account state, sessions and recovery paths	Active privileged access or corroborated unauthorised use
Application owner	What can a valid low-privilege user retrieve?	Object-level and export tests	Data outside the approved business scope
Fraud	Which facts does a persuasive caller already know?	Tested verification and transfer controls	Sensitive action based only on known personal details
Privacy and legal	When did awareness arise and what risk follows?	Versioned scope and notification decisions	Relevant risk or high risk under the applicable duty

Role	First question	Useful evidence	Escalation trigger
Procurement	Can the supplier provide an initial alert and successive scope?	Tested contacts and incident terms	Unreachable owner or missed critical information
Operations and safety	Can remote access be isolated without creating a hazard?	Approved safe fallback and restoration test	Unauthorised settings or a confirmed unsafe state

12.4 How Brandefense can help

Use external intelligence to create a validation task with an owner. A dataset offer, credential listing or brand-impersonation signal becomes useful when it is connected to the organisation's accounts, records, applications and response process.

Brandefense can support discussion of those external signals and their business context. Intelligence alone cannot determine whether a customer's account is active, a supplier's notice starts a duty, or a physical process is safe to restart. Those decisions need the organisation's evidence and accountable owners.

For a discussion of monitoring and response priorities, use the Brandefense demo request [S28]. The report's recommended first step is to bring a critical-service map and one concrete validation question.

KEY TAKEAWAYS

01

Assign every action to an accountable owner and a measurable completion test.

02

Validate access, notification and recovery through realistic exercises.

03

Escalate corroborated account abuse and unsafe operational states without waiting for an annual trend update.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Scope, method and confidence · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

79
sources

Appendix A. Scope, method and confidence 97
Appendix B. Evidence register 100
Appendix C. Sources 101
Appendix D. Glossary 105

Appendix A. Scope, method and confidence

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

A.1 Window and source populations

The nominal observation window runs from 1 January through the cut-off of 22 November 2026. Post evidence uses recorded publication time. A listing date, an incident date, discovery, public disclosure and a regulator's decision are different events.

The last calendar day and November's monthly totals are partial at observation. Recent activity means information published or updated during 9–22 November, with the underlying incident date stated separately where known.

The report combines four own-source populations: retained dark-web posts, public ransomware listings, selected-domain exposure and passive observations and narrow payment-card aggregates [S1][S2][S3][S4]. Public disclosures and technical sources provide separate corroboration or context.

No source population is added to another to estimate unique people, organisations or attacks. A post may advertise an older event, a listing may repeat a victim, and a service domain may belong to a group already represented elsewhere.

A.2 Retained posts and evidence cards

The 7,757 retained forum records support selected observations about advertisements, requests and discussion. They include 432 dated in the closing fortnight. They form a subset of the 7,758 tagged forum records in the 841,760-record country-tag snapshot, with one tagged October entry unretained (1,849 of 1,850). Neither population establishes unique incidents, national targeting or verified malicious activity [S1].

Some recorded dates remain inconsistent, so the report does not infer when theft occurred, when an offer first appeared or a reliable interval between advertisements. Dates on the evidence cards are recorded publication dates, with uncertainty stated on each card.

Quotations demonstrate statements made, not their truth. No advertised access, card or dataset was tested, and no criminal contact or purchase was made.

The larger retained population should not be read as an exhaustively adjudicated incident register. The public incident coverage is also limited by source availability and by items whose original disclosure remains unresolved.

A.3 Selected-domain observations

The universe contains 250 candidate service domains. Atlas exposure observations cover 249, and passive observations cover 237. Selection is purposive; related legal entities and services can appear separately. Ownership and independence require validation before an independent-organisation ranking [S2].

The national Atlas headline is 63 on a 0–100 scale for the assessed portfolio. Only the national headline is published. Sector tables contain observed signal counts, with no sector or organisation ratings.

Exposure observations were read on 21 November 2026. The similar-domain view covers 19 October–18 November 2026. Annual mention and passive observations end on 22 November 2026. Device totals are lower bounds; credential, device, document and mention associations can overlap and do not independently establish current access or confirmed intrusions.

Passive observations describe public email policies, DNS, certificates and homepages. They do not demonstrate control effectiveness. Inconclusive results remain separate from observed absences or unsuccessful certificate validation.

A.4 Ransomware listings

Ransompedia supplies public listing records associated with France and the four peer countries. The window total uses listing publication dates. The prior-year comparison covers all of 2025 and therefore has a different duration [S3].

A listing is a claim. It does not independently establish encryption, data theft, a unique victim, a particular access route or financial loss. Feed country and sector labels require case-level corroboration before a victim is named.

Country assignments are the feed's classifications. Some entity matches remain unresolved; the comparison does not independently establish where every affected service or person is located.

A.5 Payment-card scope

The limited card view contains 11 France-associated cards in 5 retained records. Of these, 1 is issuer-associated and 10 are country-only; the categories are disjoint [S4].

These figures do not measure national card theft, valid cards, successful payments or fraud losses.

A.6 Public incidents and naming

Chapter 5 presents selected cases and their evidence boundaries, distinguishing official disclosures, attributed reporting and unverified claims. Section 5.10 summarises selected unresolved reports. These tables are not an itemised incident register and do not treat every retained item as a distinct attack.

An organisation is named as an affected party only when official confirmation and wider reporting support the name in the public naming register. Other roles remain generic. Source titles and article paths that would identify a withheld party are withheld, with the publisher's root cited instead.

Public-source coverage is incomplete, and some original notices remain unavailable.

A.7 Confidence and attribution

High confidence applies to a narrow proposition directly supported by retained evidence or a clear primary source. It does not validate an advertisement's content merely because the advertisement is held.

Moderate confidence applies to an interpretation supported by relevant evidence but with material alternatives. A planning assumption remains conditional and includes a signal that would change it.

Unverified marks claims whose authenticity, current access, origin or impact is not established. A counterclaim and a denial are also attributed to their sources. An absence of corroboration establishes neither fabrication nor the absence of an incident.

State attributions remain those of the named official or research source. No attribution is extended through language, political framing or simultaneous announcements alone. An analytical model is labelled wherever it connects observations without a concrete actor relationship.

A.8 Technical and regulatory boundaries

Every CVE named in this edition was checked against NVD and the relevant vendor advisory [S21][S22][S24][S25][S26]. Product-specific affected and fixed branches must be read in their own context. An advisory is not a confirmed French incident.

Regulatory summaries distinguish current obligations, proposals, legislative stages and enforcement of older incidents [S14][S15][S16][S17][S18][S19][S20][S61]. They are planning aids. Applicability and notification decisions require the organisation's facts and current legal review.

Appendix B. Evidence register

The cards preserve recorded publication dates, with chronology uncertainty stated on each card. B07 preserves a French original with a labelled English translation; the other selected originals are English [S1].

Card	Recorded date	Venue	Alias	Chapter
B01	2026-03-19	Forum	Persona A	4
B02	2026-03-19	Forum	Persona A	4
B03	2026-06-17	Forum	Zab26	4
B04	2026-01-07	Forum	suicid	4
B05	2026-04-17	Forum	RubiconH4ck	4
B06	2026-09-12	Forum	lauraallen	4
B07	2026-01-09	Forum	near	4
B08	2026-05-04	Forum	OverSec	4
B09	2026-05-09	Forum	NormalLeVrai	4
B10	2026-09-03	Forum	updap	4
B11	2026-09-03	Forum	updap	4
B12	2026-09-03	Forum	updap	4
B13	2026-09-28	Forum	updap	4
B14	2026-01-04	Forum	Angel_Batista	4
B15	2026-01-30	Forum	kazutlg	4
B16	2026-02-20	Forum	HexDex	4
B17	2026-06-23	Forum	Edric	4
B18	2026-03-04	Forum	HexDex	4

Appendix C. Sources

Source numbers that do not appear were retired during review and are not cited. Every external entry records a source read and its verification date. Withheld article paths are preserved privately; public citations retain the publisher root.

S1: Brandefense Blackhole records associated with France and retained forum evidence, 1 January–22 November 2026. Own retained evidence; public aggregates and redacted cards accompany this edition. · verified on 2026-11-22.

S2: Atlas selected-domain exposure snapshot, 21 November 2026; mention and passive observations, 22 November 2026. Own retained evidence; public aggregates accompany this edition. · verified on 2026-11-22.

S3: Ransompedia listing snapshot, France and four regional peers. Own retained evidence; public aggregates and redacted cards accompany this edition. · verified on 2026-11-22.

S4: Brandefense payment-card aggregates for the narrow retained-post view. Own retained evidence; public aggregates accompany this edition. · verified on 2026-11-22.

S5: DataReportal, Digital 2027: France, late-2026 observations. https://datareportal.com/reports/digital-2027-france · verified on 2026-11-22.

S6: CERT-FR, September operational update, 30 September 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-006.pdf · verified on 2026-11-22.

S7: CERT-FR, October operational update, published 12 November 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-010.pdf · verified on 2026-11-22.

S8: ANSSI, investigation of a tax-administration data incident, 29 September 2026; title withheld. https://cyber.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S9: CERT-FR, lessons from application data breaches, 20 October 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-008.pdf · verified on 2026-11-22.

S10: CERT-FR, French C4 attribution and industrial-controller incident, 9 November 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-009.pdf · verified on 2026-11-22.

S11: French diplomatic authority, attribution statement, 9 November 2026. https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/declaration-d-attribution-a-l-iran-de-cyberattaques-visant-la-france · verified on 2026-11-22.

S12: France 24, company confirmation of a business-mailing provider incident, 14 November 2026; title withheld. https://www.france24.com/ (article URL withheld) · verified on 2026-11-22.

S13: RFI, postal-services provider incident, 16 November 2026; title withheld. https://www.rfi.fr/ (article URL withheld) · verified on 2026-11-22.

S14: CNIL, mobile and fixed-line operators security sanctions, 14 January 2026; title withheld. https://www.cnil.fr/ (article URL withheld) · verified on 2026-11-22.

S15: CNIL, employment-service security sanction, 29 January 2026; title withheld. https://www.cnil.fr/ (article URL withheld) · verified on 2026-11-22.

S16: CNIL, anonymised password-storage and retention sanction, 18 November 2026. https://www.cnil.fr/fr/conservation-des-mots-de-passe-sanction-5-millions-deuros · verified on 2026-11-22.

S17: CNIL, local-authority cybersecurity sanctions, 9 November 2026. https://www.cnil.fr/fr/sanctions-cybersecurite-collectivites-territoriales · verified on 2026-11-22.

S18: CNIL, GDPR text, Articles 32–34. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4 · verified on 2026-11-22.

S19: ACPR, Digital Operational Resilience Act and supervisory information. https://acpr.banque-france.fr/fr/reglementation/focus-sur-la-reglementation/transverse/digital-operational-resilience-act-dora · verified on 2026-11-22.

S20: ANSSI, NIS2 transposition and working reference document. https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/ · verified on 2026-11-22.

S21: NVD, CVE-2026-72898. https://nvd.nist.gov/vuln/detail/cve-2026-72898 · verified on 2026-11-22.

S22: Metabase, security advisory and affected/fixed branches. https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf · verified on 2026-11-22.

S23: CERT-FR, NGINX alert, 18 November 2026. https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-017/ · verified on 2026-11-22.

S24: NVD, CVE-2026-123633. https://nvd.nist.gov/vuln/detail/cve-2026-123633 · verified on 2026-11-22.

S25: NVD, CVE-2026-123007. https://nvd.nist.gov/vuln/detail/cve-2026-123007 · verified on 2026-11-22.

S26: F5, security advisories for the two NGINX HTTP/2 vulnerabilities. https://my.f5.com/manage/s/article/K000163928 ; https://my.f5.com/manage/s/article/K000163926 · verified on 2026-11-22.

S27: IETF protocol documents for DMARC, SPF, DNSSEC, TLS, DKIM and HSTS. https://www.rfc-editor.org/info/rfc9989/ ; https://www.rfc-editor.org/rfc/rfc7208 ; https://www.rfc-editor.org/rfc/rfc4035 ; https://www.rfc-editor.org/rfc/rfc9846 ; https://www.rfc-editor.org/rfc/rfc6376 ; https://www.rfc-editor.org/rfc/rfc6797 · verified on 2026-11-22.

S28: Brandefense, public demo request page. https://brandefense.io/request-a-demo/ · verified on 2026-11-22.

S29: MITRE ATT&CK, Valid Accounts and Modify Parameter. https://attack.mitre.org/techniques/T1078/ ; https://attack.mitre.org/techniques/T0836/ · verified on 2026-11-22.

S31: National press, postal-group statement quoted on renewed January disruption; title withheld. https://www.leparisien.fr/ (article URL withheld) · content verified on 2026-11-22; reference availability varies.

S32: Technology press, sports-federation member-platform statement quoted, January 2026; title withheld. https://www.01net.com/ (article URL withheld) · content verified on 2026-11-22.

S33: Franceinfo, social-contribution agency statement quoted, 20 January 2026; title withheld. https://www.franceinfo.fr/ (article URL withheld) · verified on 2026-11-22.

S34: Technology press, research-organisation historical payroll-data statement quoted, February 2026; title withheld. https://next.ink/ (article URL withheld) · content verified on 2026-11-22.

S35: Finance ministry, financial-data service incident, 18 February 2026; title withheld. https://presse.economie.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S36: Technology press, medical-software provider statement quoted, February 2026; title withheld. https://www.zdnet.fr/ (article URL withheld) · content verified on 2026-11-22.

S37: CERT-FR, messaging-account campaign alert, 20 March 2026; updated 18 June. https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-003/ · verified on 2026-11-22.

S38: Education authority, personnel-data incident, 24 March 2026; title withheld. https://www.education.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S39: Education authority, pupil-data incident, April 2026; title withheld. https://www.education.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S40: Interior authority, identity-document portal update, 21 April 2026; title withheld. https://www.interieur.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S41: Franceinfo, tourism reservation disclosure quoted, 16 May 2026; title withheld. https://www.franceinfo.fr/ (article URL withheld) · verified on 2026-11-22.

S42: Government digital directorate, messaging-account incident, 8 June 2026; title withheld. https://www.numerique.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S43: CNIL, false assistance after personal-data breaches, 24 June 2026. https://www.cnil.fr/fr/vigilance-accompagnement-violation-de-donnees · verified on 2026-11-22.

S44: CERT-FR, Turla targeting and attribution, 13 July 2026. https://cert.cyber.gouv.fr/cti/CERTFR-2026-CTI-004/ · verified on 2026-11-22.

S45: Cybermalveillance.gouv.fr, crypto-service disclosure and impersonation warning; published 22 January 2026; updated 8 June 2026. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-secteur-crypto-actifs-202601 · verified on 2026-11-22.

S46: Cybermalveillance.gouv.fr, tax-refund phishing warning; published 15 July 2026; updated 8 September 2026. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/remboursement-impot-hameconnage · verified on 2026-11-22.

S47: Gendarmerie, false judicial summons warning, 11 August 2026. https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2026/prevention-mefiez-vous-des-escroqueries-a-la-fausse-convocation · verified on 2026-11-22.

S48: Gendarmerie, J3-directed international site disruption, 8 October 2026. https://www.gendarmerie.interieur.gouv.fr/unpj/actualites/plus-de-17-000-victimes-dont-des-mineures-trois-sites-de-diffusion-de-contenus-intimes-voles-fermes · verified on 2026-11-22.

S49: Crédit Mutuel Arkéa, fraudulent-transactions statement, 4 November 2026. https://www.cm-arkea.com/arkea/banque/upload/docs/application/pdf/2026-11/04112026_-_communique_-_le_credit_mutuel_arkea_annonce_avoir_ete_victime_dune_cyberattaque__2026-11-04_15-40-19_385.pdf · verified on 2026-11-22.

S50: Reuters, Crédit Mutuel Arkéa attributed loss estimate, 5 November 2026. https://www.reuters.com/legal/government/french-bank-credit-mutuel-arkea-says-100-million-missing-after-cyberattack-2026-11-05/ · verified on 2026-11-22.

S51: Shared publishing platform, radiology-software provider statement on earlier incident and later sale claim, November 2026; title withheld. https://fr.linkedin.com/ (article URL withheld) · content verified on 2026-11-22; reference availability varies.

S52: Press-release service, market-research group internal-system incident statement, November 2026; title withheld. https://www.globenewswire.com/ (article URL withheld) · content verified on 2026-11-22; reference availability varies.

S53: Report URI, international third-party script incident, 16 November 2026; title withheld. https://blog.report-uri.com/ (article URL withheld) · verified on 2026-11-22.

S54: French-language monitor, closing-period claims and follow-ups; article URLs withheld. https://frenchbreaches.com/ (article URL withheld) · verified on 2026-11-22.

S55: CNIL, private-hospital sanction for an earlier incident, 3 September 2026; title withheld. https://www.cnil.fr/ (article URL withheld) · verified on 2026-11-22.

S56: Cybermalveillance.gouv.fr, false contest-vote messaging campaign; published 27 October 2026; updated 3 November 2026. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/vigilance-faux-vote-whatsapp · Verified on 23 November 2026.

S57: Energy supplier, commercial-partner incident, 27 October 2026; title withheld. https://www.bleepingcomputer.com/ (article URL withheld) · verified on 2026-11-22.

S58: Vocational-training agency, external accommodation-tool incident, 21 September 2026; title withheld. https://www.01net.com/ (article URL withheld) · verified on 2026-11-22.

S59: Education press, public agronomy institution disruption notice quoted, January 2026; title withheld. https://etudiant.lefigaro.fr/ (article URL withheld) · content verified on 2026-11-22; reference availability varies.

S60: Cybersecurity press, public agronomy school internship-record extraction notice quoted; title withheld. https://www.cyberattaque.org/ (article URL withheld) · content verified on 2026-11-22.

S61: French legislative records, amended resilience and cybersecurity bill, first reading 17 November 2026. https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731#AN1 ; https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/ · verified on 2026-11-22.

S62: Cato CTRL, Operation Poisson, 16 June 2026. https://www.catonetworks.com/blog/cato-ctrl-operation-poisson-analyzing-a-cybercriminals-entire-operation/ · verified on 2026-11-22.

S63: Regional public broadcaster, alumni-platform disclosure, April 2026; title withheld. https://france3-regions.franceinfo.fr/ (article URL withheld) · verified on 2026-11-22.

S64: Local press, university web-shop script incident, September 2026; title withheld. https://www.toutmontbeliard.com/ (article URL withheld) · verified on 2026-11-22.

S65: Technology press, research institute exposure statement quoted, August 2026; title withheld. https://next.ink/ (article URL withheld) · content verified on 2026-11-22.

S66: Business-software provider, original multi-instance statement; title withheld. https://fr.linkedin.com/ (article URL withheld) · verified on 2026-11-22.

S67: Technology press, external-operator disclosure, January 2026; title withheld. https://www.01net.com/ (article URL withheld) · verified on 2026-11-22.

S68: Cybersecurity press, hospital imaging-supplier notice quoted, November 2026; title withheld. https://www.cyberattaque.org/ (article URL withheld) · content verified on 2026-11-22.

S69: Technology press, student-support appointment-platform notice quoted, March 2026; title withheld. https://www.01net.com/ (article URL withheld) · content verified on 2026-11-22.

S70: News-agency reporting, regulated-owner records disclosure, March 2026; title withheld. https://www.tf1info.fr/ (article URL withheld) · verified on 2026-11-22.

S71: News-agency reporting, health-prevention document-platform disclosure, August 2026; title withheld. https://www.tf1info.fr/ (article URL withheld) · verified on 2026-11-22.

S72: Technology press, primary-school administration notice quoted, March 2026; title withheld. https://next.ink/ (article URL withheld) · content verified on 2026-11-22.

S73: Higher-education authority, admissions-module notice, 23 April 2026; title withheld. https://www.enseignementsup-recherche.gouv.fr/ (article URL withheld) · verified on 2026-11-22.

S74: Technology press, school-sport historical extraction notice quoted, March 2026; title withheld. https://www.01net.com/ (article URL withheld) · content verified on 2026-11-22.

S75: Public broadcaster, health-ministry population statement, 27 February 2026; title withheld. https://www.franceinfo.fr/ (article URL withheld) · verified on 2026-11-22.

S76: Tourism trade press, provider CEO interview and recovery update, 20–21 November 2026; title withheld. https://www.lechotouristique.com/ (article URL withheld) · verified on 2026-11-22.

S77: Credential-security research, combolist definition and historical-data repetition. https://spycloud.com/blog/plot-twist-combolists-are-still-a-threat/ · verified on 2026-11-22.

S78: Crédit Mutuel Arkéa, Amendment No. 2 to the 2025 Universal Registration Document, 18 November 2026. https://www.cm-arkea.com/arkea/banque/upload/docs/application/pdf/2026-11/cma_amendement_semestriel_2025_fr_n2_20261118.pdf · Verified on 23 November 2026.

S79: ANSSI and CERT-FR, Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002), 11 March 2026. https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf · Verified on 23 November 2026.

S80: ANSSI, Panorama de la cybermenace 2025 presentation, 11 March 2026. https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/ · Verified on 23 November 2026.

Appendix D. Glossary

Term	Plain meaning
C4	Centre de Coordination des Crises Cyber, France's interministerial body for cyber-threat analysis [S10].
Credential	An authentication secret or related account information. Its appearance does not establish current validity.
Combolist	A compiled list of account identifiers and passwords that may combine or repeat older material. Its appearance does not establish current validity [S77].
Session	An authenticated interaction that may continue beyond the initial sign-in.
MFA	Authentication requiring more than one factor. Its strength also depends on recovery and approval paths.
Object-level authorisation	The check that a user may access the particular record requested, beyond being signed in.
Infostealer	Malicious software designed to collect information such as login secrets and session data.
Ransomware listing	A public claim associated with extortion; it does not independently confirm encryption or theft.
Controller	The party deciding the purposes and means of personal-data processing.
Processor	A party processing personal data for a controller, within that relationship's scope.
DMARC	A domain owner's published message-authentication handling preference and reporting policy.
SPF	A published statement identifying permitted sending infrastructure for a mail identity.
DKIM	DomainKeys Identified Mail uses cryptographic signatures to associate a signing domain with an email message [S27].
HSTS	HTTP Strict Transport Security is a website policy directing browsers to use secure connections to that site [S27].
DNSSEC	DNS security extensions supporting validation of signed DNS information.
TLS	A protocol protecting communications in transit; a certificate result does not assess an application.

Term	Plain meaning
DORA	The EU financial-sector digital operational resilience framework, within its defined scope.
ReCyF	The French cybersecurity reference document presented by ANSSI as a working text at the cut-off.

Definitions follow the technical, research and legal sources cited in the relevant chapters [S9][S10][S18][S19][S20][S27][S77].

About this report

Odin by Brandefense prepared this country edition for security leaders and operational teams. It supports evidence-led validation, continuity and incident decisions. It does not authenticate criminal offers, estimate national prevalence or replace an organisation's investigation.

The French edition is translated from the English master. The English edition prevails where meaning differs. Publication and any subsequent update require the applicable review and release process.

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