BRANDEFENSE COUNTRY REPORT · ROMANIA 2026

Brandefense Romania Cyber Threat Landscape Report 2026

Identity offers, service recovery and the evidence boundaries of reported espionage

Odin by Brandefense
Research window: 1 January–22 November 2026, by post date
Version 1.0 · Public Research Edition · TLP:CLEAR · 8–22 November 2026

250
candidate domains across twelve sector groups

14
detailed advertisement dossiers with separate evidence limits

12
ransomware group labels in the Romanian listing population

18
actions with accountable owners and observable completion evidence

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Romania's digital and security context	10
03	National exposure: selected organisation domains	14
04	What the underground evidence shows	22
05	Official incidents and sector decisions	46
06	Hacktivism, DDoS and recent activity	80
07	Threat actors and evidence relationships	90
08	The fraud economy	102
09	Banking and financial services	108
10	Regulation and national response	112
11	Outlook	117
12	Action plan	121
A	Appendix A. Scope and evidence boundaries	127
B	Appendix B. Evidence register	130
C	Appendix C. Sources	132
D	Appendix D. Glossary	136
E	Appendix E. Further official findings and campaign context	138
	About this report	140

Board and executives	01 05 11 12
CISO	03 04 05 07
SOC and infrastructure	03 04 06 07
Fraud and customer teams	08 09 12
Legal and communications	05 06 10

About this edition

AI-assisted research and drafting. Source statements, criminal claims, observations and analyst assessments remain distinct. Appendix A explains the scope and confidence limits.

Romania's evidence calls for practical control of administrator access, sensitive documents, supplier dependencies and recovery, with a separate decision for every unverified claim.

773,764

Romania-tagged posts; not attacks

20

Romanian ransomware listings; criminal claims

250

selected candidate domains across twelve sectors

50/100 (B)

national Atlas headline for the selected portfolio

Contents and reading routes

The report connects leadership decisions to retained evidence. Each chapter opens with a question and closes with three takeaways. The appendices preserve source, population and terminology boundaries.

Chapter	Question	First reader
1 Executive summary	Which decisions should come first?	Leadership
2 Context	Which Romanian dependencies shape the response?	CISO
3 Organisation exposure	Which observations can be supported for the selected domains?	Infrastructure
4 Underground activity	What was advertised, and what is unverified?	Threat intelligence
5 Sector cases	What do official disclosures actually establish?	Service owners
6 DDoS and recent activity	What changed during 8–22 November?	Operations
7 Actors	Which attribution and relationship statements are supported?	Threat intelligence
8 Fraud	How can information become an unauthorised instruction?	Fraud and customer operations
9 Banking	Which controls require security, treasury and customer teams?	Financial services
10 Regulation	Which reporting clocks and exclusions apply?	Legal and compliance
11 Outlook	What would change the assessment?	Leadership
12 Action plan	Who acts over 30, 60 and 90 days?	All owners
Appendices A–E	What are the evidence limits, sources and definitions?	All readers

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

Observation means a post or measurement is held. **Claim** means its author asserts an outcome. **Official account** means an authority or organisation reports a finding within its stated scope. **Analyst inference** connects evidence to a decision.

An observed advertisement does not authenticate the advertised material. Official confirmation of an incident can leave the initial access, copying, population and actor unresolved.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow directly from Romania's retained evidence and verified public disclosures?

4

leadership decisions with named owners and completion evidence

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Romania's visible threat picture combines data and access advertisements, extortion listings and official reports of disrupted services. November brought new reporting about older espionage activity, recent access offers and privacy-enforcement findings. Ransompedia holds 20 Romanian listings in the window. None of these populations is a national incident count. Start with privileged-account validation, protect sensitive documents and supplier access, and prove that essential workflows can recover.

This report combines Brandefense Blackhole posts, Ransompedia listings, Atlas exposure and passive observations for selected domains, and source-checked public reporting. Each population has a distinct unit, date and limitation. The selected domains do not estimate national prevalence. [S1][S2][S3]

The requested window ends on 22 November. The evidence reflects what was available during research that day. It is not a completed end-of-day census. The closing period, 8–22 November, appears separately in Chapter 6.

1. Access advertisements need account evidence. The forum material includes government-themed portal access, remote-access offers and a November marketplace administrator offer. These establish advertising, without demonstrating working access, a completed transaction or a particular entry route. A seller's account label should trigger validation by the account owner. [S1]

2. Documents create a fraud problem before origin is resolved. Offers describe customer records, education-related payroll information, travel contracts and private legal-services documents. A claimed document count is not a count of people. Even authentic information would not establish that every named counterparty suffered an intrusion. [S1]

3. Ransomware visibility supports recovery preparation. Ransompedia records 20 Romanian listings under twelve group labels, compared with 17 in all of 2025. Qilin accounts for 7 of the current-window listings. The partial-year and full-year figures are not a matched-period growth rate. A listing remains a criminal claim. [S3]

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

4. Recent espionage reporting has an earlier chronology. ESET's 10 November research describes a government Exchange case beginning in December 2025, with activity in January 2026. SRI's 11 November account says it identified the attack in December, stopped it and identified no sensitive-data exfiltration. Preserve both sources' scope rather than resolving their differences without additional evidence. [S6][S7][S8]

5. Privacy findings widen the control agenda. Official enforcement notices describe remote-access weaknesses, unauthorised access by staff and handling errors alongside cyberattacks. The defensive programme therefore needs access governance, secure administration and process controls. External-attack counts alone would miss these lessons. [S33][S37][S39][S40]

6. Current credential listings require validation. 79 of 250 selected domains had a credential listed for sale when checked. The national Atlas headline is 50/100 (B). At least 356,395 device associations and 1,355,738 credential-record associations support separate validation tasks, without establishing current intrusion. [S2]

Four decisions for leaders

1. **Make account validation an owned service.** Confirm that credential and access alerts reach identity operations. Match each signal to active accounts, privileges and sessions. Escalate demonstrated unauthorised use; close historical or unmatched material with a recorded reason.
1. **Protect documents across supplier boundaries.** Identify who can export legal, customer, staff and payment information. Test supplier alerting, evidence preservation and revocation. Ask whether a legitimate document could support a fraudulent instruction even if its original source remains uncertain.
1. **Demonstrate independent recovery.** Restore an essential workflow using protected backups and separate recovery credentials. Require a service owner to accept the result. Include customer contact and supplier dependencies in the exercise.
1. **Use one factual timeline for reporting and communications.** Record discovery, awareness, service impact and subsequent findings separately. Give legal, privacy and communications teams the same facts. Preserve the distinction between a recent publication and a recent attack.

The year in numbers

The figures below describe separate populations. They must not be added together.

773,764

Romania-tagged posts in the requested post-date window [S1]

WHAT IT IS NOT

Attacks, affected people or unique incidents

41,379

Distinct posts in the retained report archive [S1]

WHAT IT IS NOT

The whole Romanian underground or a representative sample

256

Retained Romania-tagged forum posts [S1]

WHAT IT IS NOT

256 incidents or independently verified offers

14

Forum posts dated 8–22 November within that set [S1]

WHAT IT IS NOT

Fourteen new attacks

20

Romanian ransomware listings in the window [S3]

WHAT IT IS NOT

Confirmed encryption, data theft or distinct legal entities

17

Romanian listings in all of 2025 in the same snapshot [S3]

WHAT IT IS NOT

A matched-duration baseline

7 of 20

Listings carrying the Qilin label [S3]

WHAT IT IS NOT

A success rate or verified attribution of public incidents

250

Selected candidate domains in twelve sector groups [S2]

WHAT IT IS NOT

An official ranking, independent legal entities or national prevalence

50/100 (B)

National Atlas headline for the selected portfolio [S2]

WHAT IT IS NOT

A breach percentage, incident probability or sector ranking

94.8%

Internet penetration in DataReportal's October 2026 estimate [S5]

WHAT IT IS NOT

The share attacked or using secure services

94

Romania-associated payment cards appearing in clear text in retained posts [S4]

WHAT IT IS NOT

Card theft, validity, fraud losses or Brandefense's wider card coverage

KEY TAKEAWAYS

01

Validate accounts and documents before accepting an advertisement's claims.

02

Treat recovery, supplier notification and fraud prevention as linked business decisions.

03

Keep posts, listings, official cases and people in separate populations.

Report map

Start with the decision your role owns. Follow the evidence to its limitation, then use Chapter 12 to assign completion evidence.

Board and executives	Fund identity control and demonstrable recovery	01 05 11 12
CISO	Set priorities across accounts, suppliers and services	03 04 05 07
SOC and infrastructure	Validate access, mail and service evidence	03 04 06 07
Fraud and customer teams	Reject unauthorised instructions using genuine information	08 09 12
Legal and communications	Apply the correct clock and preserve uncertainty	05 06 10

CHAPTER 02

Romania's digital and security context

02

THIS CHAPTER ANSWERS

Which dependencies shape a proportionate Romanian response?

94.8%

estimated internet penetration in October 2026

2.1 Connectivity creates many identity boundaries 11

2.2 Shared services connect separate organisations 11

2.3 Elections and regional issues: maintain the attribution boundary 12

2.4 Use disclosure dates without rewriting the incident 12

2.5 Separate the national reporting roles 12

CHAPTER 02

Romania's digital and security context

IN SHORT

A highly connected population relies on shared identity, payment and public-service systems. The evidence spans customer records, supplier documents, remote access and government email. Service continuity and confidentiality need separate evidence. Cross-border research can inform controls without proving a Romanian victim. Map important services, administrators and suppliers together, and assign the reporting route before an incident starts.

2.1 Connectivity creates many identity boundaries

DataReportal estimates 17.8 million internet users and 94.8% penetration in October 2026. It reports 26.1 million cellular connections and 13.6 million social-media user identities. Connections and user identities are different units; neither is a count of unique customers. [S5]

For security planning, the important boundary is where a service accepts authority. A customer account, help-desk call, supplier login and administrator session require different checks. Knowing a person's details does not authorise a change to their recovery method or payment destination.

The marketplace and document offers in Chapter 4 make this distinction practical. They advertise information and access together. That does not establish either proposition. Defenders should ask separately whether a record is authentic, whether a login works, and whether any unauthorised action occurred.

2.2 Shared services connect separate organisations

Travel contracts, invoicing information and legal documents can pass through several organisations. A copy may sit with a supplier, customer, employee or external adviser. A seller's list of counterparties does not locate the original loss. [S1]

Map the service dependency before choosing a response. The application owner can identify exports and delegated users. Procurement can identify contractual evidence duties. The data-protection officer can assess personal-data consequences. The account owner can investigate sessions.

This is an analytical response model, not an assertion that the observed sellers share a supply chain. No common operator or common source links the separate offers merely because they describe similar records.

A retail parent group's 19 October notice confirmed malicious activity and precautionary shutdowns across brands in Europe and the United States. Stores stayed open; most Central and Southeastern European websites and apps were available again by then. The notice did not identify particular Romanian services or a Romanian compromise. Group ownership establishes a dependency question, not a confirmed local incident. [S86]

2.3 Elections and regional issues: maintain the attribution boundary

This report takes no position on the annulled November 2024 presidential election, the 2025 rerun, candidates, parties or government decisions. Those historical elections do not establish the cause, actor or motive of any 2026 incident examined here.

References to Russia, Moldova, Ukraine or Hungary serve source attribution or the stated comparator context. A Russian-language post does not establish nationality or state direction. Regional proximity does not establish a shared campaign.

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

ESET attributes Cereal to Turla with high confidence. SRI attributes the government-email attack to Turla in its own account. The April router operation also carries an official attribution. These are the sources' assessments, not new independent attributions by this report. [S6][S7][S9]

2.4 Use disclosure dates without rewriting the incident

A November notice can describe an older event, a completed investigation or a newly published assessment. The recent-activity section therefore identifies what became public during the closing period. It does not silently redate earlier intrusions.

In the Exchange case, ESET reports a December 2025 starting point and January 2026 activity. SRI says it identified the attack in December 2025. Their November publications are relevant to the window while the earlier chronology remains explicit. [S6][S7][S8]

An enforcement decision can likewise be issued after the conduct it examines. The publication date determines inclusion in the disclosure register. When an attack date is not given, the report does not invent one or place it in a monthly attack series.

2.5 Separate the national reporting roles

Romania's civilian cybersecurity framework designates DNSC as the competent national authority. The framework includes specific exclusions and a distinct treatment for financial entities subject to DORA. Privacy reporting remains a separate question. [S13][S14]

SRI's National Cyberint Centre supplies the official accounts of the reported government-email response and the April router operation. Police and prosecutors describe investigations and alleged conduct. ANSPDCP publishes privacy-enforcement findings. These sources answer different questions and their figures cannot form one national attack total. [S7][S9][S20]

Chapter 10 turns these distinctions into reporting decisions. An incident lead should know the relevant legal entity, service and supervisor before the first alert, with an alternate contact available outside office hours.

KEY TAKEAWAYS

01

Map service, supplier and identity dependencies before deciding containment.

02

Preserve the original event chronology when using recent publications.

03

Attribute state assessments to their sources and keep political positions outside the analysis.

CHAPTER 03

National exposure: selected organisation domains

THIS CHAPTER ANSWERS

Which observations can this edition support for the selected Romanian domains?

250

candidate domains across twelve sector groups

3.1 Universe card 15

3.2 Exposure observations and national Atlas headline 16

3.3 Passive email observations 19

3.4 DNS, TLS and homepage observations 20

3.5 Validate exposure through local evidence 21

CHAPTER 03

National exposure: selected organisation domains

IN SHORT

79 of 250 selected domains had a credential listed for sale when checked. The national Atlas headline is 50/100 (B). The portfolio records at least 356,395 device associations and 1,355,738 credential-record associations. These overlapping populations are not unique people or confirmed intrusions. Passive controls retain their assessed denominators. Assign owners to current-account validation, employee-device investigation and service recovery.

3.1 Universe card

Item	Boundary
Population	250 selected candidate domains in twelve sector groups
Selection	Public institutions, financial services, essential-service providers and significant private-sector organisations
Counting unit	Candidate domain; organisational independence and legal ownership are not established for every entry
Selection limit	Purposive portfolio, not an official top-company ranking or a representative national sample
Date	Exposure and passive observations dated 22 November 2026 [S2]
Publication	National Atlas headline and anonymous sector signal counts
Interpretation	Unknown observations are not zero values or evidence of a secure configuration

The sector population is shown below. Its size describes the selected portfolio, not a sector's share of the Romanian economy.

Sector	Candidate domains
Government	50
Banking and finance	30
Education	25
Manufacturing and industry	25

Sector	Candidate domains
Energy and utilities	20
Retail and holdings	20
Transport and logistics	20
Telecom and technology	15
Healthcare	10
Insurance	10
Hospitality and tourism	10
Media and entertainment	15
Total	250

The term organisation describes the selection purpose. The numerical denominator is the candidate domain. In c03, `orgs_listed_for_sale_now` counts candidate domains with current listings; it does not establish independent organisations. The download records `listing_count_unit` as `candidate_domains`. A group website can serve several entities, and a global corporate domain can include activity outside Romania. These limits apply before any sector comparison.

3.2 Exposure observations and national Atlas headline

79 of 250 selected domains had a credential listed for sale when checked. The national Atlas headline is 50/100 (B), describing the selected portfolio. It is not a breach percentage, incident probability or certification of effective controls. [S2]

The exposure snapshot is dated 22 November 2026. Annual mention context covers 23 November 2025–22 November 2026, while lookalike observations cover a recent 30-day interval. These signals are not all new 2026 events.

Only the national Atlas rating is published. Anonymous sector rows describe signal counts with their domain denominators. Group websites, shared services and global domains can include related entities or activity outside Romania.

The portfolio contains at least 356,395 device associations, including 11,551 employee-device associations, and 1,355,738 credential-record associations. These populations overlap and cannot be added together or read as unique people. [S2]

Device associations concern 222 domains, employee-device associations 180, and credential records 241. Document references concern 102 domains and total 568 observations. Candidate lookalikes concern 169 domains; they are not verified malicious infrastructure. [S2]

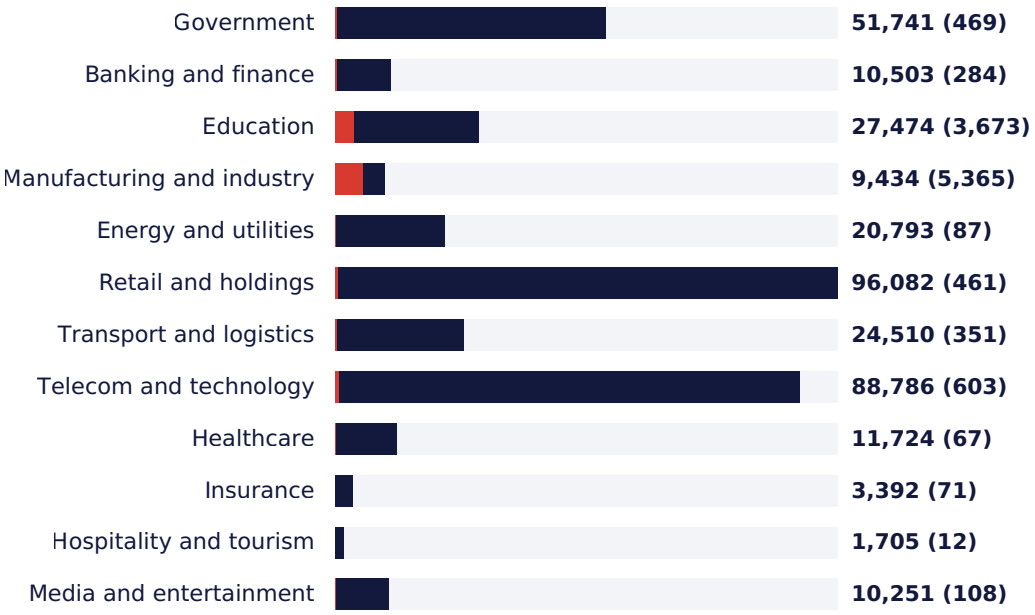
The table reports device associations as minimum observed counts. Credential records combine historical populations and do not establish valid passwords, current infection or Romanian-only users.

Sector	Domains	Current listings	Device associations	Credential records
Government	50	9	51,741	58,126
Banking and finance	30	9	10,503	63,106
Education	25	6	27,474	565,816
Manufacturing and industry	25	4	9,434	348,550
Energy and utilities	20	8	20,793	16,972
Retail and holdings	20	17	96,082	61,499
Transport and logistics	20	3	24,510	115,056
Telecom and technology	15	6	88,786	75,855
Healthcare	10	2	11,724	9,741
Insurance	10	3	3,392	19,146
Hospitality and tourism	10	5	1,705	4,469
Media and entertainment	15	7	10,251	17,402
Total	250	79	356,395	1,355,738

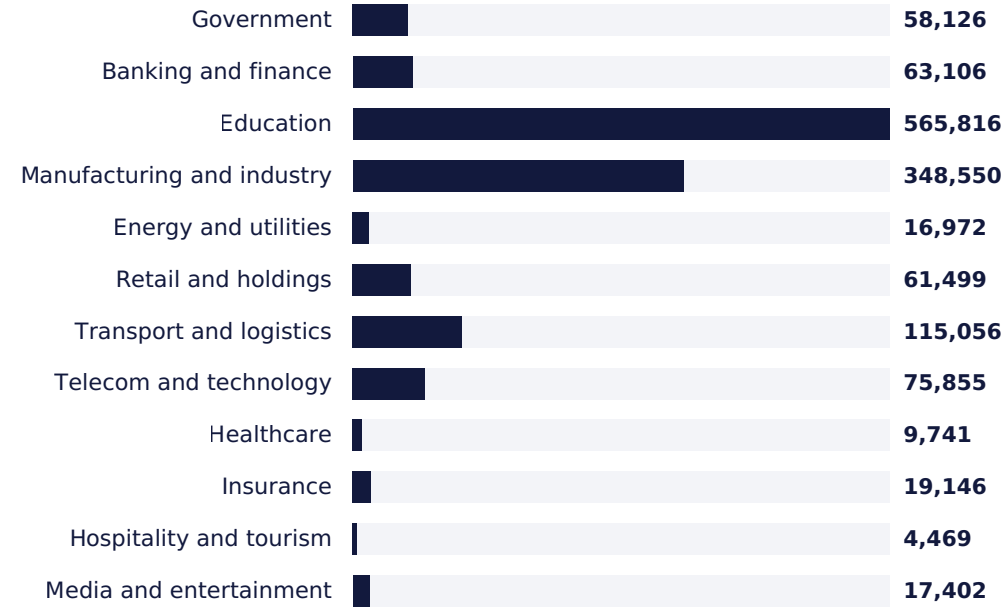
Device and credential associations retain separate sector denominators

Employee device associations Other device / credential associations

Device associations, at least (employee subset in parentheses)



Credential-record associations (separate scale)



Source: exposure observations for 250 selected candidate domains, 22 November 2026 [S2]. Cumulative associations may overlap and include historical material; not unique people, current intrusions or national prevalence.

79 of 250

selected domains with a current credential listing

50/100 (B)

national Atlas headline for the selected portfolio

A current credential offer should prompt account-specific investigation. It does not by itself establish a working password, successful intrusion, a completed sale or a particular number of affected employees.

Device associations require a different question: whose device, holding access to which service, at what time? Customer, student, employee and shared-service identities can use the same corporate domain. A domain association alone does not resolve ownership or present infection.

Historical credential records also require account validation. A record can be old, duplicated across sources, already remediated or associated with a customer. Do not make a disruptive account decision from a cumulative total alone.

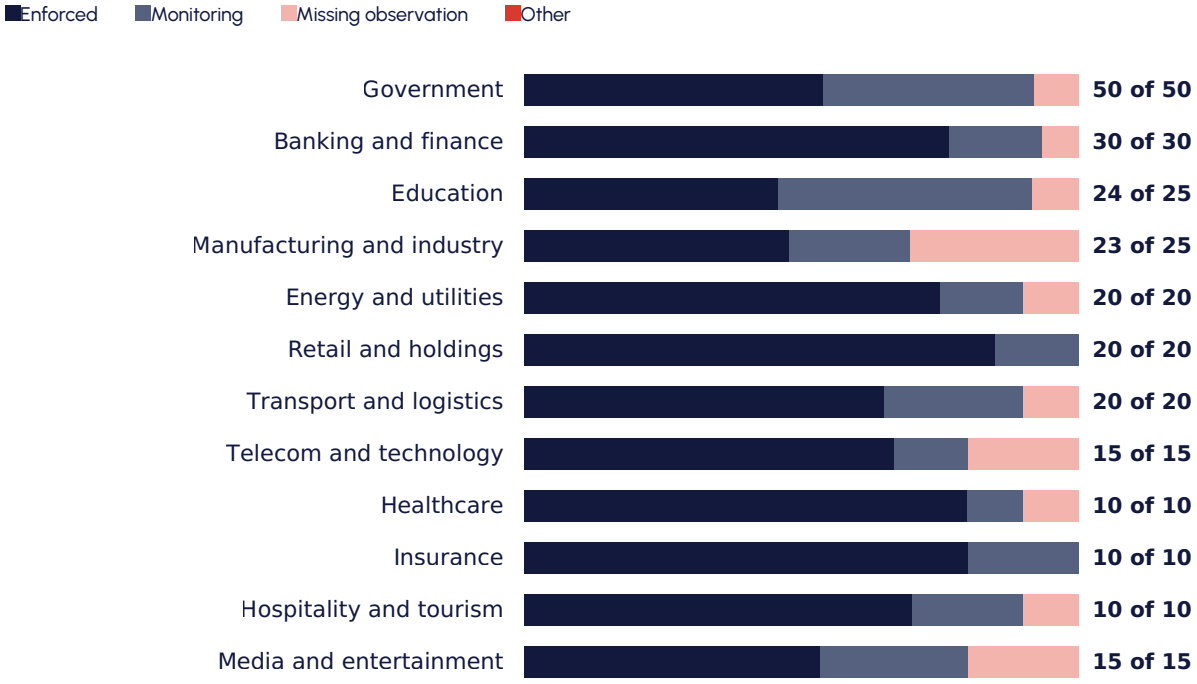
3.3 Passive email observations

The passive results below retain their own observation denominator. DMARC enforcement, an SPF record and a DKIM record answer different questions. A missing or unsuccessful observation is not interchangeable with a confirmed absent control. [S2][S18]

Passive observations are available for 247 of the 250 selected domains; 3 remain unassessed. [S2]

Observation	Count	Denominator
DMARC enforcement requested	158	247
DMARC monitoring	62	247
DMARC record not found	27	247
Other DMARC observation	0	247
SPF record found	239	247
DKIM record found	177	247

Email-policy observations retain the selected-sector denominators



Source: passive observations, 22 November 2026 [S2]. 250 candidate domains; 247 observed domains. Each sector retains its observation denominator. An absent observation does not confirm an absent control.

DMARC communicates the domain owner's requested treatment of messages that fail its authentication alignment checks. A monitoring policy does not request rejection. A quarantine or rejection policy does not guarantee that every receiver applies it or that impersonation stops. [S18]

The operational action is to identify legitimate senders, review authentication reports and stage enforcement with the email owner. Include outsourced payroll, customer support, invoicing and marketing. A policy change is complete when legitimate mail remains usable and the exception owner is known.

3.4 DNS, TLS and homepage observations

The 247 observed domains include 31 with a DNSSEC delegation observation. TLS results were available for 217 domains, of which 207 were valid at the check. Homepages were reachable for 187; HSTS was observed for 124. These denominators answer different questions. [S2]

Treat a published DNSSEC delegation observation as a delegation signal, rather than a full validation of every DNS answer. A DKIM record that was not found does not establish that the organisation never signs mail. A reachable homepage does not establish secure application authorisation.

TLS observations apply to the endpoint and date assessed. An unsuccessful observation can arise from service availability, certificate presentation or access limitations. Review the underlying service and its intended audience before choosing remediation.

Keep the service owner in the loop. Some domains deliberately carry no public application or outbound mail. Record that purpose and its approved configuration instead of forcing every domain into the same operational template.

3.5 Validate exposure through local evidence

Signal	First validation	Escalation trigger	Completion evidence
Credential offer	Match to an active account, privileges and remediation history	Demonstrated unauthorised authentication or valid privileged access	Session decision and account-owner sign-off
Device association	Confirm device and account relationship	Active infection or unexplained privileged session	Containment, session review and owner disposition
Document claim	Compare authorised internal records and access history	Verified sensitive records or an unauthorised export	Data scope, legal decision and access correction
Email-policy observation	Confirm sending services and domain purpose	Unapproved sender or a material authentication gap	Approved policy and tested legitimate delivery
Availability claim	Compare service telemetry and provider evidence	Confirmed disruption affecting a business workflow	Restoration accepted by the service owner

These are recommended validation steps. They are not a description of how Brandefense constructs a rating or collects its evidence.

KEY TAKEAWAYS

01

The portfolio denominator is 250 candidate domains, with ownership and independence limits.

02

The national Atlas headline describes this portfolio; passive observations retain separate denominators.

03

Validate accounts, devices, documents and service purpose separately before acting.

CHAPTER 04

What the underground evidence shows

THIS CHAPTER ANSWERS

What do Romanian data and access offers establish, and what must defenders validate?

14
detailed advertisement dossiers with separate evidence limits

4.1 Universe card 23
4.2 Volume, platforms and languages 23
4.3 How to read the dossiers 26
4.4 Case A: Government-themed access advertisements (B01) 27
4.5 Case B: Historical invoicing-data rectification (B02) 28
4.6 Case C: Betting-account lists and verification-bypass demand (B03) 29
4.7 Case D: Online-store customer-data claim (B04) 31
4.8 Case E: IT-services client and invoice-data claim (B05) 32
4.9 Case F: Digital-marketing and CRM claim (B06) 33
4.10 Case G: Citizen-photo data advertisement (B07) 34
4.11 Case H: Travel-contract publication claim (B08) 36
4.12 Case I: Retail customer-data offer in May (B09) 37
4.13 Case J: Education-related payroll-data claim (B10) 38
4.14 Case K: Retail customer-data offer in June (B11) 39
4.15 Case L: Private legal-services document offer (B12) 40
4.16 Case M: Online-marketplace administrative-access offer (B13) 42
4.17 Additional service offers and limits 43
4.18 Case N: Private-aviation identity-document and manifest offer (B24) 44

CHAPTER 04

What the underground evidence shows

IN SHORT

The retained forum material advertises access, customer records, documents and identity services. Some posts refer to older data; recent offers concern marketplace administration and legal-services documents. The dossiers below establish what was advertised, not the truth of the advertised access or volume. Validate account ownership, data freshness and authorised exports before deciding containment, customer protection or notification.

4.1 Universe card

Item	Boundary
Window	1 January–22 November 2026, by post date
Country-tagged population	773,764 posts [S1]
Retained archive	41,379 distinct posts [S1]
Forum population	256 retained country-tagged posts across eleven months
Recent forum population	14 posts dated 8–22 November
Case unit	An editorial dossier can contain several advertisements or replies
Evidence limit	Observed text does not authenticate a database, working account or sale

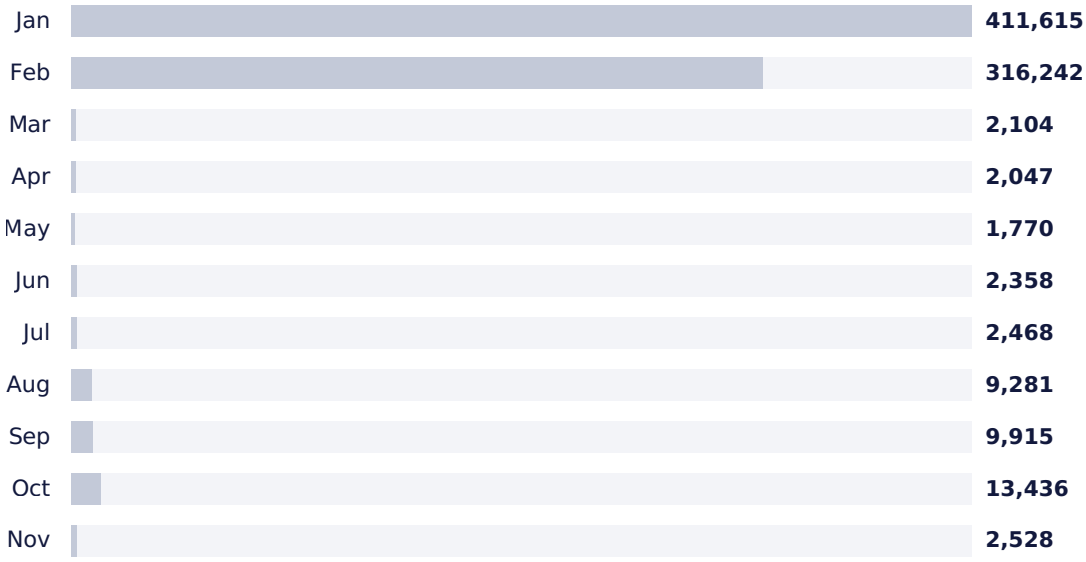
Country tags describe how the material relates to the country. A multi-country service catalogue or list of payment markets is not verified targeting of Romania. Replies, reposts, advertisements and claimed datasets are different objects.

4.2 Volume, platforms and languages

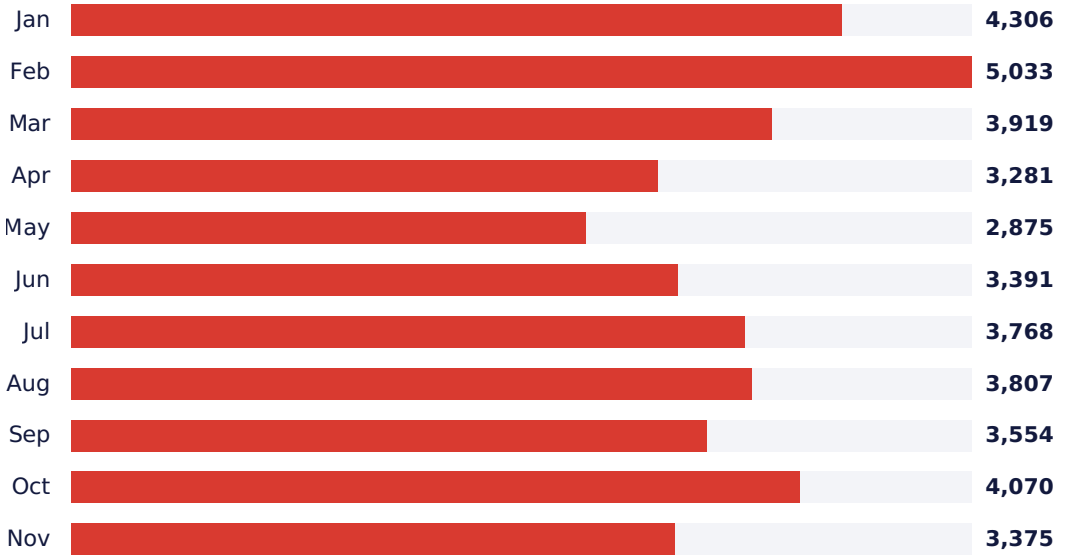
The country-tagged population is 773,764 posts. January accounts for 411,615, or 53.2%. The retained report archive contains 41,379 distinct posts. These are visibility measures, not an incident series. The retained population does not cover every tagged post. [S1]

Monthly post volumes describe visibility rather than an attack trend

Country-tagged posts



Retained archive (separate scale)



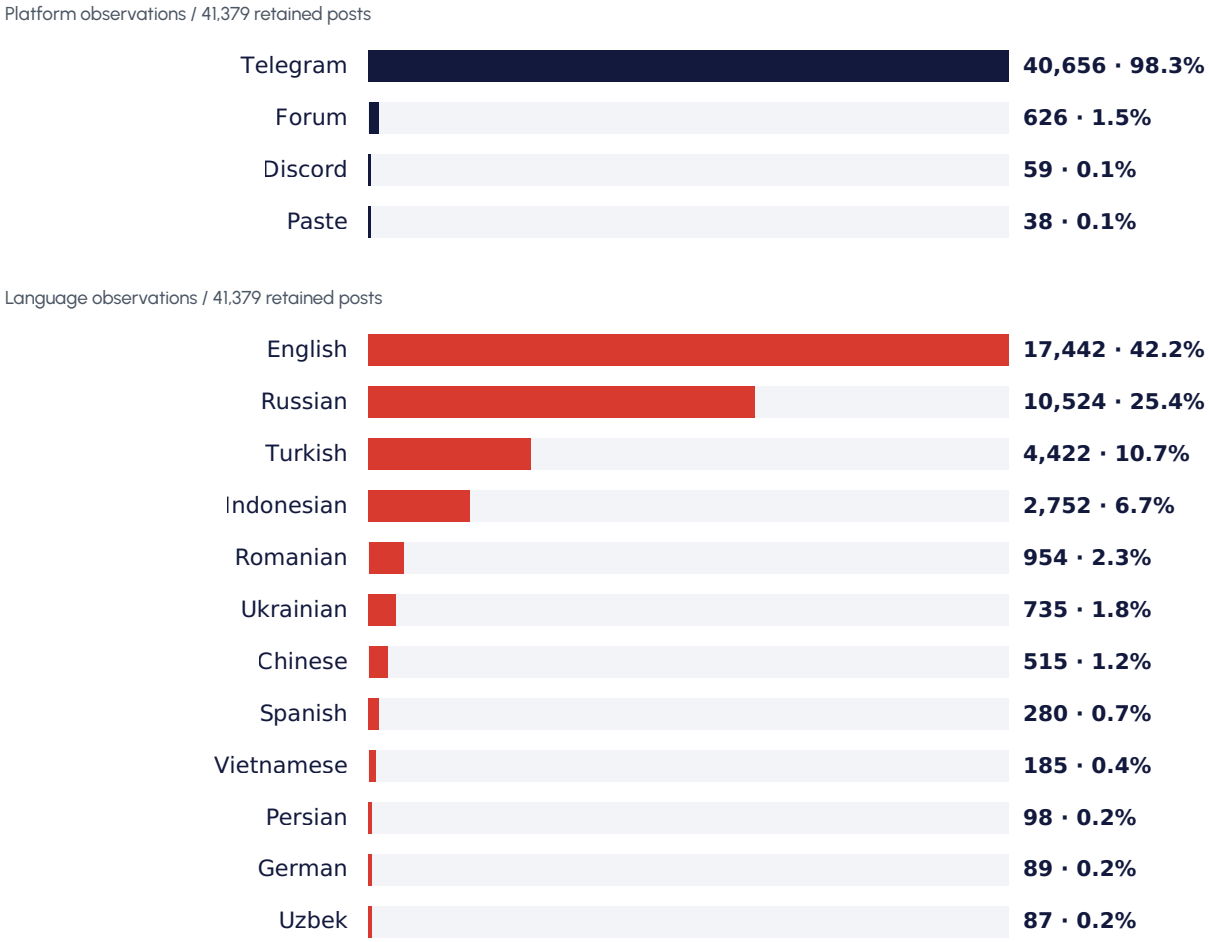
Source: Brandefense Blackhole, Romania-tagged posts and retained archive, 1 January–22 November 2026; closing day partial. Posts are not attacks or unique incidents [S1].

View	Label	Posts	Archive denominator
Platform	forum	626	41,379
Platform	discord	59	41,379
Platform	telegram	40,656	41,379
Platform	paste	38	41,379
Language	EN	17,442	41,379

View	Label	Posts	Archive denominator
Language	RU	10,524	41,379
Language	TR	4,422	41,379
Language	ID	2,752	41,379
Language	RO	954	41,379
Language	UK	735	41,379
Language	ZH	515	41,379
Language	ES	280	41,379

Language observations can overlap; their row counts are not added as distinct posts. Platform figures describe the retained archive, rather than the full country-tagged population. [S1]

Platform and language observations retain separate post denominators



Language labels can overlap; platforms and languages are separate views of the retained archive. Source: Brandefense Blackhole, Romania-tagged posts and retained archive, 1 January–22 November 2026; closing day partial. Posts are not attacks or unique incidents [S1].

The archive and national tagged view have different coverage. They are not presented as nested populations. Repetition, advertising and unequal visibility prevent interpreting a post-volume change as a change in national incident prevalence.

Additional country-tagged forum themes describe post content rather than verified incidents



Base: 256 retained country-tagged forum posts; themes describe post content, not verified incidents. Source: Brandefense Blackhole, Romania-tagged posts and retained archive, 1 January–22 November 2026; closing day partial. Posts are not attacks or unique incidents [S1].

4.3 How to read the dossiers

Each case keeps its claim, chronology, held evidence, alternatives and response together. A reply expressing interest is not independent validation. Similar wording is not proof of the same file or operator. A source-provided date remains a claim unless independently corroborated.

The observed activity includes access sales, database advertising, identity documents, consumer-account services and historical data recirculation. These themes describe content. They do not partition Romania's incidents or measure criminal revenue. [S1]

4.4 Case A: Government-themed access advertisements (B01)

A

CASE A

Government-themed access advertisements

Evidence card B01 | 1 Jan 2026 | Forum | Government

Unverified advertisement

CLAIM	Two posts offer unspecified Romanian government portal access. Similar wording appears under two aliases. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-01-01, 2026-06-01. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	Copied advertising or a fictitious offer can explain similar wording. Text similarity does not establish identity or access.
LIMIT	No portal, account, working access, screenshots, completed sale or common operator established. The second post does not establish another intrusion.
RESPONSE	Review government-service privileged access and valid-session evidence before disruptive action.
DECISION	Record a service-owner disposition. If no account or system can be matched, retain the uncertainty rather than naming a national platform.

Bottom line

No portal, account, working access, screenshots, completed sale or common operator established. The second post does not establish another intrusion.

Evidence card B01 — 1 Jan 2026

renquix | Forum | Forum | EN

ORIGINAL

Selling romanian gov portal access

Held

Two posts offer unspecified Romanian government portal access. Similar wording appears under two aliases.

Not established

No portal, account, working access, screenshots, completed sale or common operator established. The second post does not establish another intrusion.

4.5 Case B: Historical invoicing-data recirculation (B02)

CASE B

B

Historical invoicing-data recirculation

Evidence card B02 | 21 Jan 2026 | Forum | Business services

Unverified advertisement

CLAIM	Posts recirculate claimed invoicing/customer databases, with descriptions referring to 2023 or 2024. Claimed counts differ. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-01-21, 2026-01-23, 2026-03-22. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	An older export can explain a recent post. A recent label does not automatically refresh the data.
LIMIT	These statements do not date a new 2026 intrusion; the different figures and claims do not establish the same file. Samples were not independently validated.
RESPONSE	Check whether affected identities and secrets were already remediated; validate freshness before response.

DECISION	Check password and token changes since the claimed data period. A historical customer list can still support impersonation even when old passwords no longer work.

Bottom line

These statements do not date a new 2026 intrusion; the different figures and claims do not establish the same file. Samples were not independently validated.

Evidence card B02 21 Jan 2026

EchoEcho Forum Forum EN

ORIGINAL

SQL dump (2.08GB sql files) 04.2024 clients - 209K lines

Held

Posts recirculate claimed invoicing/customer databases, with descriptions referring to 2023 or 2024. Claimed counts differ.

Not established

These statements do not date a new 2026 intrusion; the different figures and claims do not establish the same file. Samples were not independently validated.

4.6 Case C: Betting-account lists and verification-bypass demand (B03)

C

CASE C

Betting-account lists and verification-bypass demand

Evidence card B03 16 Feb 2026 Forum Consumer services

Unverified advertisement

CLAIM	A country-themed betting-account list and requests or offers for verification and account-checking tools appear during the year. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-01-24, 2026-02-12, 2026-02-16, 2026-09-24, 2026-10-11. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	A buying request can express interest without an available product. An advertised tool may fail against the current service.

LIMIT	Requests do not establish available capability. No access test, working bypass, new platform intrusion or completed fraud is established.
RESPONSE	Monitor automated sign-ins, enrolment changes and account recovery. Test verification against replayed documents.
DECISION	Test recovery and enrolment decisions using authorised exercises. Successful identity checks require more than recognition of personal details.

Bottom line

Requests do not establish available capability. No access test, working bypass, new platform intrusion or completed fraud is established.

Evidence card B03 — 16 Feb 2026

Reddington66 Forum Forum EN

ORIGINAL

want to buy a kyc bypass

Held

A country-themed betting-account list and requests or offers for verification and account-checking tools appear during the year.

Not established

Requests do not establish available capability. No access test, working bypass, new platform intrusion or completed fraud is established.

4.7 Case D: Online-store customer-data claim (B04)

CASE D

D

Online-store customer-data claim

Evidence card B04 | 4 Mar 2026 | Forum | Retail

Unverified advertisement

CLAIM	A March post describes a Romanian online-store database with customer and company information. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-03-04. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	The material could come from a historical export or a supplier. The seller description does not locate the original loss.
LIMIT	The record does not establish origin, current access, data completeness or the advertised compromise mechanism.
RESPONSE	Review account and database access, preserve logs, and assess notification only against validated records.
DECISION	Ask application owners to reconcile exports, delegated users and data-retention periods. Do not infer payment-card exposure from the phrase full customer data.

Bottom line

The record does not establish origin, current access, data completeness or the advertised compromise mechanism.

Evidence card B04 4 Mar 2026

Eliphas Forum Forum EN

ORIGINAL

Romanian online store with full customer data

Held

A March post describes a Romanian online-store database with customer and company information.

Not established

The record does not establish origin, current access, data completeness or the advertised compromise mechanism.

4.8 Case E: IT-services client and invoice-data claim (B05)

E

CASE E

IT-services client and invoice-data claim

Evidence card B05 2 Apr 2026 Forum Technology

Unverified advertisement

CLAIM	An April post advertises more than 300,000 client records, employees and invoices, 1.95 GB; a reply asks to see it. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-04-02, 2026-04-02. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	An export can combine several table types. Invoices and customer records have different units, even in an authentic file.
LIMIT	Claimed rows are not unique victims. The reply is not independent confirmation or evidence of transfer.
RESPONSE	Check service-provider access, invoice changes and partner contact verification.
DECISION	Treat a familiar invoice as context, not payment authority. Verify changed beneficiary details through a previously trusted contact.

Bottom line

Claimed rows are not unique victims. The reply is not independent confirmation or evidence of transfer.

Evidence card B05 2 Apr 2026

xorcat Forum Forum EN

ORIGINAL

Records: 300,000+ client records, employees, invoices

Held

An April post advertises more than 300,000 client records, employees and invoices, 1.95 GB; a reply asks to see it.

Not established

Claimed rows are not unique victims. The reply is not independent confirmation or evidence of transfer.

4.9 Case F: Digital-marketing and CRM claim (B06)

CASE F

F

Digital-marketing and CRM claim

Evidence card B06 | 7 Apr 2026 | Forum | Business services

Unverified advertisement

CLAIM	April posts advertise a digital-marketing platform database and CRM or messaging-service information; one claims 40,000+ rows. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-04-04, 2026-04-07. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	A commercial export or partner copy could explain the material. A dispute between aliases does not settle provenance.
LIMIT	A post accuses another alias of reposting. This is an actor claim, not proof of authorship, file identity or operator linkage. Access validity and the origin of the advertised material remain unverified.
RESPONSE	Rotate validated exposed integration secrets, review authorisations and preserve messaging-service logs.

DECISION	The response boundary is the validated integration and its permissions. An organisation-wide reset requires evidence beyond a database advertisement.

Bottom line

A post accuses another alias of reposting. This is an actor claim, not proof of authorship, file identity or operator linkage. Access validity and the origin of the advertised material remain unverified.

Evidence card B06 7 Apr 2026

xorcat Forum Forum EN

ORIGINAL

Records: 40,000+ rows

Held

April posts advertise a digital-marketing platform database and CRM or messaging-service information; one claims 40,000+ rows.

Not established

A post accuses another alias of reposting. This is an actor claim, not proof of authorship, file identity or operator linkage. Access validity and the origin of the advertised material remain unverified.

4.10 Case G: Citizen-photo data advertisement (B07)

G

CASE G

Citizen-photo data advertisement

Evidence card B07 | 20 Mar 2026 | Forum | Identity services

Unverified advertisement

CLAIM	A March offer claims a database of 8,000 Romanian citizens with photographs. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-03-20. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	A collection could combine several sources. Calling people citizens does not establish a state-system origin.

LIMIT	The title is an advertisement. Source system, population, consent, completeness and acquisition date are not established.
RESPONSE	Review identity recovery against known personal details and document-image replay; avoid assuming a national-register incident.
DECISION	Review account recovery, document-image replay and excessive lookup permissions. Protect individuals without presenting the advertised total as a verified affected population.

Bottom line

The title is an advertisement. Source system, population, consent, completeness and acquisition date are not established.

Evidence card B07 — 20 Mar 2026

fent888 Forum Forum EN

ORIGINAL

Romania Database 8k Citizens + Photo

Held

A March offer claims a database of 8,000 Romanian citizens with photographs.

Not established

The title is an advertisement. Source system, population, consent, completeness and acquisition date are not established.

4.11 Case H: Travel-contract publication claim (B08)

CASE H

H

Travel-contract publication claim

Evidence card B08 | 24 Apr 2026 | Forum | Hospitality and tourism

Unverified advertisement

CLAIM	An April post claims travel-services contracts and threatens further releases of rooming lists and reservations. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-04-24. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	A document can legitimately exist with several counterparties. Mentioning a hotel does not establish access to its systems.
LIMIT	The follow-up discussion provides no independent confirmation. Document authenticity and scope remain unverified.
RESPONSE	Review travel-partner document sharing and revoke access only after validating a match.
DECISION	Protect reservations, guest communications and payment instructions separately. Changes should be confirmed through a known channel, not the contact supplied in a suspect message.

Bottom line

The follow-up discussion provides no independent confirmation. Document authenticity and scope remain unverified.

Evidence card B08 — 24 Apr 2026

johnapp | Forum | Forum | EN

ORIGINAL

leaks of confidential contracts with other chain hotels

Held

An April post claims travel-services contracts and threatens further releases of rooming lists and reservations.

Not established

The follow-up discussion provides no independent confirmation. Document authenticity and scope remain unverified.

4.12 Case I: Retail customer-data offer in May (B09)

CASE I

Retail customer-data offer in May

Evidence card B09 | 7 May 2026 | Forum | Retail

Unverified advertisement

CLAIM	A seller advertises 86,283 lines for USD 300, assigning the data a 4 May 2026 date. The same alias cross-posts, bumps and receives a reply. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-05-07, 2026-05-07, 2026-05-07, 2026-05-12. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	Repeated posts can represent one offer. An asking price does not establish realised value or the number of buyers.
LIMIT	The actor-supplied date is not independently verified. Cross-posts do not establish separate intrusions or completed sales.
RESPONSE	Review customer-data exports and account access. Validate a sample through authorised internal records before notification.
DECISION	Compare any validated data with permitted export paths. Preserve the difference between an advertised line count and unique customers.

Bottom line

The actor-supplied date is not independently verified. Cross-posts do not establish separate intrusions or completed sales.

Evidence card B09 7 May 2026

moxzey Forum Forum EN

ORIGINAL

Total lines:86.283

Held

A seller advertises 86,283 lines for USD 300, assigning the data a 4 May 2026 date. The same alias cross-posts, bumps and receives a reply.

Not established

The actor-supplied date is not independently verified. Cross-posts do not establish separate intrusions or completed sales.

4.13 Case J: Education-related payroll-data claim (B10)

J

CASE J

Education-related payroll-data claim

Evidence card B10 | 24 May 2026 | Forum | Education

Unverified advertisement

CLAIM	A May thread and quoted reply advertise 331K teacher-related records and administrative credentials. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-05-24, 2026-05-24. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	An administrative export can contain repeated positions or entries. The claimed count does not establish distinct people or nationwide access.
LIMIT	The source system, national coverage, record count and current access remain unverified. Working credentials are not established.
RESPONSE	Review payroll-provider privileges and staff identity logs; validate any matching account before resetting wider populations.

DECISION	Check supplier and internal administrator permissions separately. Validate the source system and account before expanding the response.

Bottom line

The source system, national coverage, record count and current access remain unverified. Working credentials are not established.

Evidence card B10 24 May 2026

somewhere Forum Forum EN

ORIGINAL

331K TEACHERS + ADMIN CREDS PLAINTEXT

Held

A May thread and quoted reply advertise 331K teacher-related records and administrative credentials.

Not established

The source system, national coverage, record count and current access remain unverified. Working credentials are not established.

4.14 Case K: Retail customer-data offer in June (B11)

K

CASE K

Retail customer-data offer in June

Evidence card B11 20 Jun 2026 Forum Retail

Unverified advertisement

CLAIM	A June post claims 453,009 customer-data lines and assigns a 19 June 2026 breach date. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-06-20. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	A historical export, a subset or fabricated material remain alternatives. Credible fields do not authenticate the whole advertised volume.
LIMIT	The claimed breach date is not independent evidence. Listed data fields and sample rows do not verify the whole advertised database or the origin.

RESPONSE	Check unusual exports and customer record access, then assess personal-data reporting from validated facts.
DECISION	Use application evidence to establish the scope and awareness timeline. A sample match supports investigation before it supports adopting every seller claim.

Bottom line

The claimed breach date is not independent evidence. Listed data fields and sample rows do not verify the whole advertised database or the origin.

Evidence card B11 20 Jun 2026

tempp991 Forum Forum EN

ORIGINAL

Total lines: 453.009

Held

A June post claims 453,009 customer-data lines and assigns a 19 June 2026 breach date.

Not established

The claimed breach date is not independent evidence. Listed data fields and sample rows do not verify the whole advertised database or the origin.

4.15 Case L: Private legal-services document offer (B12)

L

CASE L

Private legal-services document offer

Evidence card B12 | 10 Nov 2026 | Forum | Professional services

Unverified advertisement

CLAIM	The same alias posts a legal-services document claim on 5 November and offers 21,000 documents on 10 November. Claimed material includes client, property, corporate and identity documents. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-11-05, 2026-11-10. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.

ALTERNATIVE	One document can contain several individuals and counterparties. A list of names does not establish separate losses at every organisation.
LIMIT	Advertised counterparties are not evidence of their own intrusion. No file, volume or provenance was independently verified.
RESPONSE	Review third-party document sharing, identity checks and unusual downloads; validate a match through authorised records.
DECISION	The relevant controls include confidential sharing, bulk downloads and changes to legal or payment instructions. Preserve privileged material through approved incident channels.

Bottom line

Advertised counterparties are not evidence of their own intrusion. No file, volume or provenance was independently verified.

Evidence card B12 — 10 Nov 2026

ternny | Forum | Forum | EN

ORIGINAL

It is for sale 21,000 private and confidential documents

Held

The same alias posts a legal-services document claim on 5 November and offers 21,000 documents on 10 November. Claimed material includes client, property, corporate and identity documents.

Not established

Advertised counterparties are not evidence of their own intrusion. No file, volume or provenance was independently verified.

4.16 Case M: Online-marketplace administrative-access offer (B13)

CASE M

M

Online-marketplace administrative-access offer

Evidence card B13 | 10 Nov 2026 | Forum | Retail

Unverified advertisement

CLAIM	On 10 November a seller advertises administrative panel access to a Romanian marketplace, including orders, customers, delivery information and bank details. [S1]
CHRONOLOGY	The dossier contains posts dated 2026-11-10. These are publication dates, not independently established intrusion dates.
WHAT IS HELD	The retained source text establishes the advertisement and its wording. The advertised access and data remain unverified.
ALTERNATIVE	A screenshot or description could show stale or limited access. A claim about bank details does not establish payment-card-number exposure.
LIMIT	The seller did not provide proof in the retained public post. Access validity, exfiltration, victim acknowledgement, number of people and completed sale remain unknown.
RESPONSE	Validate administrator sessions and privileges; preserve logs and review recent exports and payment-detail changes.
DECISION	Administrator session evidence is more useful than an immediate public attribution. Separate customer-data access, payment-setting changes and any confirmed copying.

Bottom line

The seller did not provide proof in the retained public post. Access validity, exfiltration, victim acknowledgement, number of people and completed sale remain unknown.

Evidence card B13 10 Nov 2026

NorthDivision Forum Forum EN

ORIGINAL

Selling actual admin panel access into [retail platform]

Held

On 10 November a seller advertises administrative panel access to a Romanian marketplace, including orders, customers, delivery information and bank details.

Not established

The seller did not provide proof in the retained public post. Access validity, exfiltration, victim acknowledgement, number of people and completed sale remain unknown.

4.17 Additional service offers and limits

An April offer describes remote access associated with Romania. It does not establish a particular victim or valid credentials. In November, another advertisement offers vehicle-data lookups at USD 10 per 1,000 lookups. Neither establishes unauthorised access to an official register. [S1]

The practical control for a comparable lookup service is to verify bulk-query authority and unusual use. For remote access, review account ownership, MFA, device trust and recent sessions. A vendor product name in an advertisement is not evidence that its software vulnerability was used.

No retained advertisement has been matched to the official cases in Chapter 5 solely because the sector or country is similar. The report therefore draws no relationship between those populations without a concrete shared element.

Late-October bot announcements also advertise small-site databases. Their stated volumes do not establish data origin, affected people or separate confirmed intrusions. Validate ownership and record freshness through authorised internal evidence before escalating a public claim. [S1]

A fashion-retailer offer dated 2026-01-02 advertises 84,792 lines for USD 200 while claiming a 2026-01-29 breach date. The dates conflict. The text does not resolve the chronology or establish data origin, access or a completed sale. Preserve the conflict without inferring either a dated intrusion or fabrication. [S1]

An October post also claims publication of an unnamed website database. The available description does not establish its content, population or origin. It is another unverified publication claim, rather than a confirmed incident or a measured affected population. [S1]

A 9 January monitoring relay described an auction for a Romanian online shop's WordPress administration panel and shell access. The retained material establishes that the offer was relayed, while working access, a directly held seller offer and the referenced screenshot remain unverified. [S1]

Posts dated 20 September and 5 October repeated a claim to offer one million Romanian mobile-contact records with basic identity fields. The repeated wording supports one advertised dataset theme. It does not validate the row count, unique people, provenance or a new breach of a Romanian organisation. [S1]

Two retained forum records dated 11 April advertised a database associated with an unnamed Romanian retail website. The offer claimed 48,183 rows, basic identity and contact fields, and a breach date of 9 April. A 26 April entry was a thread bump. These records establish circulation of one offer; the data's authenticity, provenance, affected-person count and claimed intrusion date remain unverified. [S1]

4.18 Case N: Private-aviation identity-document and manifest offer (B24)

N

CASE N

Private-aviation identity-document and manifest offer

Evidence card B24 | 4 Sep 2026 | Telegram | Transport and services

Unverified advertisement

CLAIM	On 4 September, a marketplace post claimed to offer identity documents and flight manifests associated with an unnamed private-aviation operator. It advertised 2,600 passenger identity documents, a further 100 crew passports and 6,000 files totalling 2 GB. These are claimed files and documents, not validated distinct people. A 20 September post repeated substantial parts of the offer. [S1]
CHRONOLOGY	The posts are dated 2026-09-04 and 2026-09-20. They do not establish initial access or document acquisition dates.
WHAT IS HELD	The two retained posts establish that the claim circulated. The later wording does not establish a second intrusion or a completed sale.
LIMIT AND ALTERNATIVE	The advertised six-year population does not date an intrusion. Document authenticity, validity, provenance and any connection to the operator's live systems remain unverified. Older material, third-party handling records or misleading advertising remain possible.
RESPONSE	Verify provenance and authorised document exports before defining affected individuals. Review passenger-handling and third-party access records, then assess targeted impersonation risk for any legitimate affected population.

Bottom line

The advertised six-year population does not date an intrusion. Document authenticity, validity, provenance and any connection to the operator's live systems remain unverified. Older material, third-party handling records or misleading advertising remain possible.

Evidence card B24 4 Sep 2026

Escanors Marketplace Telegram Telegram EN

ORIGINAL

We have 2,600 passports/national ids/residential permits

Held

An offer dated 4 September claims 2,600 passenger identity documents, 100 crew passports and 6,000 files totalling 2 GB. A repost dated 20 September does not establish another intrusion or completed transfer.

Not established

The advertised six-year population does not date an intrusion. Document authenticity, validity, provenance and any connection to the operator's live systems remain unverified. Older material, third-party handling records or misleading advertising remain possible.

KEY TAKEAWAYS

01

Fourteen dossiers describe advertised propositions, rather than confirmed intrusions.

02

Keep historical data, access validity, file identity and completed sales as separate questions.

03

Validate administrator sessions, document exports and supplier permissions through authorised internal evidence.

CHAPTER 05

Official incidents and sector decisions

05

THIS CHAPTER ANSWERS

Which official disclosures change the response, and which questions remain unresolved?

5.1 Sector decision table 47
5.2 Case O: Business IT disruption at an energy transport operator 48
5.3 Case P: Ransomware disrupts land-administration applications 49
5.4 Case Q: Public-funding procurement application unavailable 50
5.5 Case R: Ransomware triggers service isolation in detention administration 51
5.6 Case S: DNSC reports suspected denial of service against its website 52
5.7 Case T: Incident affects an auxiliary investor service 53
5.8 Case U: Communications operator investigates internal-network incident 54
5.9 Case V: Regulator identifies missing MFA in a hospitality ransomware case 55
5.10 Case W: Regulator orders stronger remote access and logging at an energy-services firm 56
5.11 Case X: Regulator sanctions a credit provider after an IT attack 57
5.12 Case Y: Real personal data expands the impact of a test-server attack 58
5.13 Case Z: Administrator credentials obtained through phishing 59
5.14 Case AA: Two application failures in a telecommunications enforcement decision 60
5.15 Case AB: Bank employee accessed customer statements outside assigned duties 61
5.16 Case AC: Incorrect notification processing exposes banking customer data 62
5.17 Case AD: DDoS interrupts visa and consular platforms 63
5.18 Case AE: Possible interference with refrigeration controllers 64
5.19 Case AF: Malware prompts municipal fiscal-website isolation 65
5.20 Case AG: Waste-services customer portal suspended and rebuilt 66
5.21 Case AH: Surveillance images exposed without authentication 67
5.22 Case AI: April disclosure of earlier military-email access 68
5.23 Case AJ: Ransomware response at a Romanian bank 69
5.24 Case AK: Defacement interrupts a university faculty website 70
5.25 Case AL: Account-opening portal exposed customer documents 71
5.26 Case AM: Bookseller outage and November reopening 72
5.27 Case AN: University academic and administrative services disrupted 73
5.28 Case AO: Government document portal restricted after privacy reports 74
5.29 Case AP: Municipal finance office disclosed repeated attacks 75
5.30 Case AQ: Municipal websites investigated after loss of availability 76
5.31 Case AR: Municipal online-payment outage and planned replacement 77
5.32 Case AS: Repeated defacement of a transport-sector public website 78
5.33 Recovery does not settle every evidence question 78

31

detailed official-account dossiers, separate from underground offers

CHAPTER 05

Official incidents and sector decisions

IN SHORT

Official accounts describe business IT disruption, public-application outages, ransomware and privacy-control failures. Several statements explicitly preserve operational or database boundaries. Those exclusions matter, but preliminary findings can change. The cases below separate incident dates from publication dates and internal errors from external attacks. Build recovery around the business workflow, then assign data-scope, identity and notification decisions to separate owners.

5.1 Sector decision table

Sector	Evidence	Interpretation boundary	First owner
Public services	Application and service-isolation accounts	Restored access does not settle confidentiality	Service owner and incident lead
Energy	Business IT disruption and privacy findings	Business-system impact does not establish operational-control access	IT and operations
Financial services	Auxiliary application and employee-access findings	Customer data and settlement integrity require separate checks	Security, operations and privacy
Telecom	Internal-network incident and application-control failures	Continued customer service does not settle every data question	Service assurance
Technology	Personal data on a test server	A non-production label does not remove privacy consequences	Engineering and data owner
Hospitality	Ransomware and remote-access findings	Recent enforcement need not mean a recent attack	Business owner and infrastructure

The detailed cases below are editorial dossiers. Some contain a sequence of updates or several findings. Their count does not represent unique national incidents. [S20][S21][S22][S23][S24][S25][S26][S27]

5.2 Case O: Business IT disruption at an energy transport operator

CASE O

Business IT disruption at an energy transport operator

Energy

Official account; scope as stated

OFFICIAL ACCOUNT	The company reported an attack on business IT and temporary website unavailability. It said operational SCADA and telecommunications were unaffected and transport continued normally. [S20]
CHRONOLOGY	Published 2026-02-04. The source dates the incident or detection 2026-02-03. That date does not necessarily establish initial access.
UNRESOLVED	Initial access, responsible actor, data exfiltration and ransomware family are not established by the filing.
DECISION TEST	Can finance and public communications operate while business IT is isolated?
RESPONSE	Test business-system recovery and isolation from operational systems. Validate supplier and administrative access.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

Initial access, responsible actor, data exfiltration and ransomware family are not established by the filing.

5.3 Case P: Ransomware disrupts land-administration applications

CASE P

P

Ransomware disrupts land-administration applications

Public administration

Official account; scope as stated

OFFICIAL ACCOUNT	The government said ransomware encrypted and deleted part of the application-hosting virtual infrastructure. It said the central cadastral database was unaffected and no evidence showed access to those records. [S21]
CHRONOLOGY	Published 2026-07-27. The source dates the incident or detection 2026-07-14. That date does not necessarily establish initial access.
SOURCE STATUS	The media-published copy is DNSC's preliminary annex dated 22 July 2026. DNSC says its online publication was unauthorised and it was not the final report. [S75][S115]
UNRESOLVED	The preliminary annex separately supports ancillary account-directory extraction and damage to virtual infrastructure. It does not support the relay claim that the core land registry was wiped. The full affected-person population remains unquantified. [S75][S76]
DECISION TEST	Does an intact authoritative database remain usable when applications and identity services are unavailable?
RESPONSE	Restore applications and identity dependencies in a tested sequence. Validate integrity of authoritative records separately.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The statement did not establish the full impact on other user data. Restoration timing remained unsettled. The media-published DNSC annex is preliminary; its publication was unauthorised and it is not the final report.

5.4 Case Q: Public-funding procurement application unavailable

CASE Q

Public-funding procurement application unavailable

Public administration

Official account; scope as stated

OFFICIAL ACCOUNT	The ministry announced a cyber incident affecting a procurement application used by private beneficiaries of Cohesion Policy projects. The application could not be accessed. It said the application was not used for recovery-plan projects. [S22][S61]
CHRONOLOGY	Published 2026-07-16. The source dates the incident or detection 2026-07-15. That date does not necessarily establish initial access.
UNRESOLVED	The notice did not establish data theft, actor, malware family, attack start or initial access.
DECISION TEST	Can beneficiaries prove timely submissions if the normal application is unavailable?
RESPONSE	Map procurement deadlines and alternate submission channels. Preserve application and identity logs.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The notice did not establish data theft, actor, malware family, attack start or initial access.

The regional programme authority later dated the interruption from 15 July and announced restoration on 18 August. It described migration to the Government Cloud and deadline extensions under Order 1143/2026. Restoration is an update to this case, not another incident. [S61]

5.5 Case R: Ransomware triggers service isolation in detention administration

CASE R

R

Ransomware triggers service isolation in detention administration

Public administration

Official account; scope as stated

OFFICIAL ACCOUNT	The institution reported ransomware on workstations and servers. It paused selected digital services and isolated systems. Next-day preliminary checks said important databases and backups were unaffected while other databases were partly affected. [S23][S24]
CHRONOLOGY	Published 2026-07-29. The source dates the incident or detection 2026-07-29. That date does not necessarily establish initial access.
UNRESOLVED	The next-day statement said entry method was unknown. Preliminary findings do not establish final scope.
DECISION TEST	Can essential contact workflows continue without the normal digital platform?
RESPONSE	Exercise site isolation, continuity of essential contacts and restoration from independently verified backups.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The next-day statement said entry method was unknown. Preliminary findings do not establish final scope.

5.6 Case S: DNSC reports suspected denial of service against its website

CASE S

S

DNSC reports suspected denial of service against its website

Public administration

Official account; scope as stated

OFFICIAL ACCOUNT	DNSC reported temporary website access difficulties and unusually high request volume from multiple sources. It described DDoS as a possibility and said protective measures stabilised the website. [S25]
CHRONOLOGY	Published 2026-09-08. The source dates the incident or detection 2026-09-08. That date does not necessarily establish initial access.
UNRESOLVED	The notice did not establish a responsible actor or intrusion into internal systems.
DECISION TEST	Can users distinguish an unavailable website from an unavailable national response service?
RESPONSE	Exercise traffic escalation, supplier coordination and an independent incident-communications channel.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The notice did not establish a responsible actor or intrusion into internal systems.

5.7 Case T: Incident affects an auxiliary investor service

T

CASE T

Incident affects an auxiliary investor service

Financial services

Official account; scope as stated

OFFICIAL ACCOUNT	A capital-market infrastructure operator reported an attack on an auxiliary online investor application. It said critical settlement and registry functions continued normally and holdings or settled-transaction information were not accessed or altered. [S26]
CHRONOLOGY	Published 2026-10-16. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	This communiqué gives no attack date, affected-person count or detailed personal-data categories. Do not infer that publication date equals attack date.
DECISION TEST	Can the organisation verify market-function integrity while separately investigating investor-data access?
RESPONSE	Separate investor identity support from settlement integrity checks. Tie phishing advice to validated affected data.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

This communiqué gives no attack date, affected-person count or detailed personal-data categories. Do not infer that publication date equals attack date.

5.8 Case U: Communications operator investigates internal-network incident

CASE U

U

Communications operator investigates internal-network incident

Telecommunications

Official account; scope as stated

OFFICIAL ACCOUNT	The company reported an incident detected at 06:30 with preliminary ransomware characteristics. It suspended email preventively. Company and DNSC statements said customer services continued with no indications then of impact. [S27]
CHRONOLOGY	Published 2026-10-19. The source dates the incident or detection 2026-10-19. That date does not necessarily establish initial access.
UNRESOLVED	Data impact, final malware determination and entry method remained under investigation.
DECISION TEST	Can staff coordinate containment when ordinary email has been suspended?
RESPONSE	Exercise separate internal messaging and customer-service continuity. Validate restoration and incident notices.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

Data impact, final malware determination and entry method remained under investigation.

5.9 Case V: Regulator identifies missing MFA in a hospitality ransomware case

CASE V

V

Regulator identifies missing MFA in a hospitality ransomware case

Hospitality

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP said ransomware exploited a remote connection without multi-factor authentication. Customer and employee personal data were accessed without authorisation. The authority imposed a EUR 5,000 fine. [S33]
CHRONOLOGY	Published 2026-11-17. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	October investigation completed. No attack date, affected-person count or responsible actor given. This is a recent publication, not a dated November intrusion.
DECISION TEST	Does the remote-access inventory include supplier and emergency administration?
RESPONSE	Require MFA on every remote administrative path and verify session records after changes.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

October investigation completed. No attack date, affected-person count or responsible actor given. This is a recent publication, not a dated November intrusion.

5.10 Case W: Regulator orders stronger remote access and logging at an energy-services firm

CASE W

W

Regulator orders stronger remote access and logging at an energy-services firm

Energy and industrial services

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP found personal-data disclosure and unauthorised access following an IT attack. It imposed a EUR 8,000 fine and required access logging and secure remote access with VPN and MFA. [S34]
CHRONOLOGY	Published 2026-11-13. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	No attack date, actor or affected-person count. Data categories do not quantify affected individuals.
DECISION TEST	Can the team reconstruct which privileged identity accessed which information?
RESPONSE	Verify privileged-access logs, retention and protected remote connections with operational evidence.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

No attack date, actor or affected-person count. Data categories do not quantify affected individuals.

5.11 Case X: Regulator sanctions a credit provider after an IT attack

X

CASE X

Regulator sanctions a credit provider after an IT attack

Financial services

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP reported an IT attack affecting confidentiality, integrity and security of personal data. It imposed a EUR 10,000 fine after an October investigation. [S35]
CHRONOLOGY	Published 2026-11-11. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	The notice does not establish intrusion date, attack family, perpetrator or numerical victim total.
DECISION TEST	Do technical recovery records support the same data scope used in customer communications?
RESPONSE	Reconcile customer, employee and partner data access with incident notification and tested recovery evidence.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The notice does not establish intrusion date, attack family, perpetrator or numerical victim total.

5.12 Case Y: Real personal data expands the impact of a test-server attack

CASE Y

Y

Real personal data expands the impact of a test-server attack

Technology

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP found an attack on a software testing server exposed personal data. It said using real data during testing worsened impact, imposed a EUR 6,000 fine and required fictitious test data. [S36]
CHRONOLOGY	Published 2026-10-16. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	No actor, intrusion date or affected-person count. A test environment can carry production-data consequences.
DECISION TEST	Can testing meet its purpose without real customer or employee records?
RESPONSE	Replace personal production records in development environments. Verify isolation and access control.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

No actor, intrusion date or affected-person count. A test environment can carry production-data consequences.

5.13 Case Z: Administrator credentials obtained through phishing

CASE Z

Z

Administrator credentials obtained through phishing

Business services

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP found that phishing obtained credentials for a user with administrator rights. Client personal data were accessed without authorisation. The authority imposed a EUR 3,000 fine. [S37]
CHRONOLOGY	Published 2026-08-19. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	The notice does not quantify clients or date the intrusion. One privileged identity does not establish compromise of every account.
DECISION TEST	Can responders revoke active sessions and delegated access as well as reset a password?
RESPONSE	Review privileged sessions and recovery paths. Rehearse revoking both credentials and active sessions.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The notice does not quantify clients or date the intrusion. One privileged identity does not establish compromise of every account.

5.14 Case AA: Two application failures in a telecommunications enforcement decision

CASE AA

AA

Two application failures in a telecommunications enforcement decision

Telecommunications

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP described an application synchronisation error that exposed other customers' invoices and a separate attack on a ticketing platform. It imposed two fines totalling EUR 100,000. [S38]
CHRONOLOGY	Published 2026-07-17. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	No fresh 2026 attack date for the ticketing case. The invoice error and externally attacked application have different causes.
DECISION TEST	Does a legitimate login remain restricted to its own customer records in every connected application?
RESPONSE	Test authorisation across linked applications. Protect ticketing administration with restricted multifactor access.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

No fresh 2026 attack date for the ticketing case. The invoice error and externally attacked application have different causes.

5.15 Case AB: Bank employee accessed customer statements outside assigned duties

AB

CASE AB

Bank employee accessed customer statements outside assigned duties

Banking

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP found an employee accessed customer-account statements without authorisation at a third party's request. It imposed a EUR 5,000 fine and required measures against personal-use access. [S40]
CHRONOLOGY	Published 2026-07-02. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	The notice does not establish an external attack or sector-wide prevalence rate.
DECISION TEST	Can an investigator distinguish legitimate support work from curiosity or third-party requests?
RESPONSE	Review exceptional employee access, evidence of business purpose and unexplained customer-record lookups.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The notice does not establish an external attack or sector-wide prevalence rate.

5.16 Case AC: Incorrect notification processing exposes banking customer data

CASE AC

AC

Incorrect notification processing exposes banking customer data

Banking

Official account; scope as stated

OFFICIAL ACCOUNT	ANSPDCP found that manual file processing caused insurance-renewal notices to reach wrong recipients. It imposed EUR 10,000 for security shortcomings and EUR 2,000 for delayed breach notification. [S39]
CHRONOLOGY	Published 2026-05-29. The underlying attack date is not established. This dossier is counted by disclosure, not as a newly dated attack.
UNRESOLVED	The decision does not describe external hacking or quantify affected people. It explicitly records delayed notification beyond 72 hours.
DECISION TEST	Can the team detect a recipient mismatch and start its privacy assessment promptly?
RESPONSE	Test recipient matching before bulk delivery. Record when breach-notification deadlines begin.
COMPLETION EVIDENCE	Record the relevant service and data owner, the validation performed, remaining uncertainty and the decision taken. Close the exercise only when the owner accepts its evidence.

Bottom line

The decision does not describe external hacking or quantify affected people. It explicitly records delayed notification beyond 72 hours.

5.17 Case AD: DDoS interrupts visa and consular platforms

AD

CASE AD

DDoS interrupts visa and consular platforms

Public administration

Source-qualified account

SOURCE ACCOUNT	The ministry said DDoS slowed two citizen-service platforms and caused short outages. It said all its digital systems returned to normal and no sensitive information was accessed. [S62]
CHRONOLOGY	Published 2026-03-14. The source dates the incident or observations 2026-03-13/14.
UNRESOLVED	Attack duration, actor and traffic volume were not established.
DECISION TEST	Can citizens use an alternate channel while the public platform is unavailable?
RESPONSE	Exercise DDoS failover and alternate citizen communications; separate availability evidence from intrusion claims.

Bottom line

Attack duration, actor and traffic volume were not established.

5.18 Case AE: Possible interference with refrigeration controllers

CASE AE

AE

Possible interference with refrigeration controllers

Retail and food distribution

Source-qualified account

SOURCE ACCOUNT	Six stores of one unnamed chain reported abnormal refrigeration temperatures. DNSC treated the reports as possible cyber incidents alongside a European wave. [S63][S81]
CHRONOLOGY	Published 2026-11-03. The source dates the incident or observations 2026-11-02.
UNRESOLVED	A cyber mechanism for the Romanian stores, losses, responsible actor and retailer identity were not established. Six stores are not six confirmed attacks.
DECISION TEST	Can operations distinguish a configuration fault from unauthorised remote changes without losing safe control?
RESPONSE	Remove controller management from direct internet access, secure supplier access, check firmware, setpoints, defrost programmes and alarms.

Bottom line

A cyber mechanism for the Romanian stores, losses, responsible actor and retailer identity were not established. Six stores are not six confirmed attacks.

5.19 Case AF: Malware prompts municipal fiscal-website isolation

CASE AF

AF

Malware prompts municipal fiscal-website isolation

Public administration

Source-qualified account

SOURCE ACCOUNT	The municipality was quoted saying a trojan affected the fiscal website server and it was disconnected while specialists investigated and restored service. [S64]
CHRONOLOGY	Published 2026-07-20. The source dates the incident or observations 2026-07-20.
UNRESOLVED	Original official post, wider-system impact, data access, actor and restoration date were not established by the read source.
DECISION TEST	Does the team have a dated restoration record beyond the first isolation announcement?
RESPONSE	Document isolation and safe restoration; test citizen-service continuity and investigate server access paths.

Bottom line

Original official post, wider-system impact, data access, actor and restoration date were not established by the read source.

5.20 Case AG: Waste-services customer portal suspended and rebuilt

CASE AG

AG

Waste-services customer portal suspended and rebuilt

Utilities and environmental services

Source-qualified account

SOURCE ACCOUNT	The company confirmed a 7 October portal security incident and possible unauthorised access to customer data. It suspended the portal and invalidated passwords, then restored access 2 November after infrastructure rebuilding, remediation and external audit. The company said waste services were unaffected. [S65][S66]
CHRONOLOGY	Published 2026-11-02. The source dates the incident or observations 2026-10-07.
UNRESOLVED	Whether records were copied, exact affected-account count, actor and initial access remained under investigation. The original notice has no explicit publication date; 2 November is a dated restoration disclosure.
DECISION TEST	Can service restoration be accepted while the copying investigation remains open?
RESPONSE	Revoke old credentials, test rebuilt services, communicate through verified channels and monitor follow-on fraud.

Bottom line

Whether records were copied, exact affected-account count, actor and initial access remained under investigation. The original notice has no explicit publication date; 2 November is a dated restoration disclosure.

5.21 Case AH: Surveillance images exposed without authentication

CASE AH

AH

Surveillance images exposed without authentication

Public administration and education

Source-qualified account

SOURCE ACCOUNT	Reporters found municipal CCTV images indexed without authentication in September–October. The municipality said it had disabled external access, reset passwords, updated software and closed exposed ports; it disputed personal-data compromise. A separate childcare authority said an image alone does not establish its provenance or a breach and promised checks. [S68][S69]
CHRONOLOGY	Published 2026-11-09. The municipal observations were made in September–October; the separate childcare reply is dated 2026-11-02. These dates do not establish an intrusion start.
UNRESOLVED	Exposure duration, access by others and exact childcare-camera provenance were unresolved. No attacker or state attribution was established.
DECISION TEST	Can administrators demonstrate effective authentication and justify external viewing permissions?
RESPONSE	Inventory cameras, restrict external access, verify authentication and retention, inspect access logs, and document notification decisions.

Bottom line

Exposure duration, access by others and exact childcare-camera provenance were unresolved. No attacker or state attribution was established.

5.22 Case AI: April disclosure of earlier military-email access

CASE AI

AI

April disclosure of earlier military-email access

Defence email

Earlier incident; April disclosure

SOURCE ACCOUNT	Reuters reported at least 67 military email accounts affected. The official response, quoted by national radio, described dozens of accounts accessed and 30 unsuccessful attempts. It said the incident was detected in March 2025 and isolated within 24 hours. [S73][S74]
CHRONOLOGY	The disclosure is dated 2026-04-15. The response dates detection to March 2025 and describes centralisation of cyber responsibility in March 2026. The broader regional campaign period does not establish a new Romanian intrusion in 2026.
BOUNDARY	The response said the accounts held unclassified administrative or public information. Reuters' reporting records disagreement about the specific Fancy Bear attribution. No evidence links this disclosure to the separate Turla government-email case.
RESPONSE	Treat administrative email as sensitive to intelligence collection. Validate access, enforce MFA and revoke relevant sessions when unauthorised use is confirmed. Preserve the official information-classification statement without treating unclassified as consequence-free.

Bottom line

Romanian detection dated March 2025; attribution disputed

5.23 Case AJ: Ransomware response at a Romanian bank

CASE AJ

AJ

Ransomware response at a Romanian bank

Banking and finance

Quoted official account

SOURCE ACCOUNT	DNSC said it was notified on 2 August of ransomware at the bank and was assisting mitigation and investigation at its request. [S77][S78]
CHRONOLOGY	Published 2026-08-04. The underlying attack date is not established. The notification date is 2026-08-02. These dates do not establish initial access.
BOUNDARY	The statement does not establish affected systems, customer-data theft, service impact, ransom or actor. A later extortion listing remains a separate claim; its date must not replace the official notification date.
RESPONSE	Exercise bank-service recovery, protect privileged access and prepare evidence-based supervisory and customer notifications.

Bottom line

The statement does not establish affected systems, customer-data theft, service impact, ransom or actor. A later extortion listing remains a separate claim; its date must not replace the official notification date.

5.24 Case AK: Defacement interrupts a university faculty website

AK

CASE AK

Defacement interrupts a university faculty website

Education

Quoted official account

SOURCE ACCOUNT	The faculty dean confirmed that the public website interface was affected. The site was disconnected for log analysis and removal of infected files while a technical audit assessed impact. [S79]
CHRONOLOGY	Published 2026-02-13. The source dates the incident or detection to 2026-02-13. These dates do not establish initial access.
BOUNDARY	The article describes a defacement message, but the quoted official finding is preliminary. It does not establish theft of student records or independently confirm the actor signature or precise entry method.
RESPONSE	Isolate affected web services, preserve logs, review administrative access and verify the clean deployment before reopening.

Bottom line

The article describes a defacement message, but the quoted official finding is preliminary. It does not establish theft of student records or independently confirm the actor signature or precise entry method.

5.25 Case AL: Account-opening portal exposed customer documents

CASE AL

AL

Account-opening portal exposed customer documents

Banking and finance

Quoted official account

SOURCE ACCOUNT	The investment-services firm's 20 November update confirmed unauthorised access to its account-opening portal server, allowing access to the database and documents. Monitoring detected the incident and the server was isolated. [S80][S96]
CHRONOLOGY	Published 2026-11-20. The source dates the incident or detection to 2026-10-30. These dates do not establish initial access.
BOUNDARY	The firm said the incident stayed within the application and client assets remained protected. Affected-person totals, exact data copied and the access method were not established; impact assessment and notification were continuing.
RESPONSE	Keep onboarding separate from trading and custody, verify document access logs and complete risk-based customer notifications.

Bottom line

The firm said the incident stayed within the application and client assets remained protected. Affected-person totals, exact data copied and the access method were not established; impact assessment and notification were continuing.

5.26 Case AM: Bookseller outage and November reopening

CASE AM

AM

Bookseller outage and November reopening

Retail and holdings

Quoted official account

SOURCE ACCOUNT	The bookseller's notice said a security incident reported on 22 October disrupted services; it isolated systems, notified authorities and engaged external specialists. Online shopping, loyalty, invoices and vouchers were affected. A company email reported by Mobilissimo confirmed the online shop reopened on 18 November. [S82][S83]
CHRONOLOGY	Published 2026-10-29. The source dates the incident or detection to 2026-10-22. These dates do not establish initial access.
BOUNDARY	The initial company notice said it had no indication of customer data being accessed or extracted while investigation continued. The reopening email does not establish complete restoration of every service or a final forensic result.
RESPONSE	Test dependencies between online sales, store invoicing, loyalty and gift cards; communicate recovery by service and reset reused passwords.

Bottom line

The initial company notice said it had no indication of customer data being accessed or extracted while investigation continued. The reopening email does not establish complete restoration of every service or a final forensic result.

5.27 Case AN: University academic and administrative services disrupted

CASE AN

AN

University academic and administrative services disrupted

Education and research

Quoted official account

SOURCE ACCOUNT	University management announced a cyber incident affecting IT infrastructure and digital services used for academic and administrative work. It said DNSC, ANSPDCP and DIICOT were notified and specialists were working on gradual service restoration. [S84][S97]
CHRONOLOGY	National coverage was published 2026-07-29, following the management announcement and local report dated 2026-07-28. The underlying attack date is not established. These dates do not establish initial access.
BOUNDARY	The statement did not name an actor, establish ransomware, quantify data theft or give the initial compromise date. An extortion listing's claimed volume and Qilin label remain separate allegations.
RESPONSE	Segment academic, administrative and identity systems; rehearse phased restoration and preserve evidence for the notified authorities.

Bottom line

The statement did not name an actor, establish ransomware, quantify data theft or give the initial compromise date. An extortion listing's claimed volume and Qilin label remain separate allegations.

5.28 Case AO: Government document portal restricted after privacy reports

CASE AO

AO

Government document portal restricted after privacy reports

Government and public administration

Quoted official account

SOURCE ACCOUNT	After reports that published documents exposed identity numbers and home addresses, the government said it ordered another document check, restricted public access where necessary and reviewed document ingestion and publication. [S85]
CHRONOLOGY	Published 2026-09-25. The source dates the incident or detection to 2026-09-25. These dates do not establish initial access.
BOUNDARY	This was a publication and privacy-control issue; the response did not establish external intrusion, a GDPR ruling or the number of affected people. The platform's overall size is not an affected-person count.
RESPONSE	Review document redaction and publication approval, remove excessive identifiers and check access to already published files.

Bottom line

This was a publication and privacy-control issue; the response did not establish external intrusion, a GDPR ruling or the number of affected people. The platform's overall size is not an affected-person count.

5.29 Case AP: Municipal finance office disclosed repeated attacks

CASE AP

AP

Municipal finance office disclosed repeated attacks

Government and public administration

Quoted official account

SOURCE ACCOUNT	The finance director told a 29 October council meeting that an attack occurred on 27 August and recurred daily for one week. She said authorities were informed and requested stronger antivirus and firewall protection. [S87]
CHRONOLOGY	Published 2026-10-30. The source dates the incident or detection to 2026-08-27. These dates do not establish initial access.
BOUNDARY	The statement does not establish the entry method, data access, actor, ransom or financial loss. Requested database protection is not proof that the database was accessed.
RESPONSE	Review repeat-event logs, separate public fiscal services from database administration and validate protective changes.

Bottom line

The statement does not establish the entry method, data access, actor, ransom or financial loss. Requested database protection is not proof that the database was accessed.

5.30 Case AQ: Municipal websites investigated after loss of availability

CASE AQ

AQ

Municipal websites investigated after loss of availability

Government and public administration

Quoted official account

SOURCE ACCOUNT	Police said they were conducting preliminary checks after reports that several municipal websites had become unavailable. The police statement described a possible cyberattack and said the institutions had not yet filed official complaints. [S88]
CHRONOLOGY	Published 2026-07-10. The underlying attack date is not established. These dates do not establish initial access.
BOUNDARY	The cause, actor, technical mechanism and data impact were unresolved. Website unavailability and an investigation do not confirm intrusion or ransomware.
RESPONSE	Coordinate hosting-provider logs and outage communications before assigning a cause.

Bottom line

The cause, actor, technical mechanism and data impact were unresolved. Website unavailability and an investigation do not confirm intrusion or ransomware.

5.31 Case AR: Municipal online-payment outage and planned replacement

CASE AR

AR

Municipal online-payment outage and planned replacement

Government and public administration

Quoted official account

SOURCE ACCOUNT	The municipality said online payments were unavailable following an internationally reported cyber incident affecting the platform. On 16 November it announced a replacement payment system planned for 23 November, with two testing days. [S89][S90]
CHRONOLOGY	Published 2026-10-22. The source dates the incident or detection to 2026-10-22. These dates do not establish initial access.
BOUNDARY	No local intrusion, malware, exploited CVE or data loss is established. The November notice also referred to a national payment-platform access problem; do not repeat the October fallback as continuously available. The planned 23 November launch is after cut-off, not observed restoration.
RESPONSE	Test local and national payment fallbacks, publish precise service status and validate replacement access before reopening.

Bottom line

No local intrusion, malware, exploited CVE or data loss is established. The November notice also referred to a national payment-platform access problem; do not repeat the October fallback as continuously available. The planned 23 November launch is after cut-off, not observed restoration.

5.32 Case AS: Repeated defacement of a transport-sector public website

CASE AS

AS

Repeated defacement of a transport-sector public website

Government and public administration

Quoted official account

SOURCE ACCOUNT	The director confirmed a second website attack within two weeks, said both events were reported to DNSC and described work with an IT service provider to restore access. The public site displayed a defacement message. [S98]
CHRONOLOGY	Published 2026-07-03. The source dates the incident or detection to 2026-07-03. These dates do not establish initial access.
BOUNDARY	The director said databases were unaffected and reports had backups and another public repository. Three-to-four-hour recovery was a forecast, not observed completion. A displayed handle does not identify the attacker or prove interference with transport operations.
RESPONSE	Repair the route used for repeat access, preserve web logs and keep public documents available through an independent repository.

Bottom line

The director said databases were unaffected and reports had backups and another public repository. Three-to-four-hour recovery was a forecast, not observed completion. A displayed handle does not identify the attacker or prove interference with transport operations.

5.33 Recovery does not settle every evidence question

The case set separates business IT, public-facing applications, internal networks, authoritative records and operational systems. These are distinct surfaces. A statement that one remained operational should be retained exactly without being expanded into a claim that no other data was affected.

Likewise, an official security finding does not authenticate an unrelated market advertisement. A genuine document may have several legitimate holders. A similar sector and nearby dates do not establish a common incident or operator.

The service owner should accept restoration. The identity owner should decide account and session containment. The data owner and privacy team should establish affected records and notification. One team's closure does not automatically close the others' questions.

KEY TAKEAWAYS

01

Preserve every official exclusion within its actual scope and date.

02

A recovered application can still leave data-access and notification questions open.

03

Give service restoration, identity containment and privacy decisions separate completion evidence.

CHAPTER 06

Hacktivism, DDoS and recent activity

06

THIS CHAPTER ANSWERS

What separates an availability claim from established impact, and what became visible during 8–22 November?

8–22 November

recent activity within the full reporting window

6.1 Availability and access answer different questions 81
6.2 Retained claims in their own words 81
6.3 Claim versus official account 85
6.4 Timeline of disclosures and claims 86
6.5 Recent activity: 8–22 November 87
6.6 Communicate the fact that is established 88

CHAPTER 06

Hacktivism, DDoS and recent activity

IN SHORT

Official accounts distinguish short public-service outages and suspected DDoS from intrusion or data access. The closing period brought two notable forum offers, espionage reporting, privacy decisions and fraud warnings. Several recent publications concern older events. Verify service impact through operational evidence, preserve the original chronology, and prepare an independent communications route before the next claim.

6.1 Availability and access answer different questions

The foreign ministry reported DDoS-related slowdown and short outages affecting two citizen-service platforms on 13–14 March. It said services returned to normal and no sensitive information was accessed. No actor or traffic volume was established in that statement. [S62]

On 8 September, DNSC described temporary website access difficulties and unusually high requests from multiple sources. It considered DDoS a possibility and said protections stabilised the site. This does not establish an intrusion into internal systems or a responsible group. [S25]

These accounts support service-specific continuity planning. They do not validate every politically framed claim or connect the two events. A screenshot of an unavailable page can record a moment without establishing duration, cause or business impact.

6.2 Retained claims in their own words

On 11 March, 313 Team posted government-themed website claims. One Arabic excerpt says the attack will continue for two hours. This is prospective actor wording, not a measurement of a completed outage. It is not matched to the foreign ministry's 13–14 March account. [S1][S62]

Evidence card B14 — 11 Mar 2026

313 Team | Telegram | Telegram | AR

ORIGINAL

سيستمر الهجوم لساعتين.

TRANSLATION

The attack will continue for two hours.

Held
The account stated a duration for a government-themed website claim.

Not established
The duration and impact were not independently measured. Arabic wording is prospective.

DDoSia Project posts carrying a NoName057(16) signature described Romanian targets during 16–21 March. They named several sectors, including public services, transport, energy and finance. Later summer posts repeated Romanian targeting claims. Their target lists and availability links do not establish sustained disruption or internal access. [S1]

Evidence card B15 — 17 Mar 2026

DDoSia Project | Telegram | Telegram | RU

ORIGINAL

Продолжаем [...] атаковать Румынию

TRANSLATION

We continue [...] to attack Romania.

Held
A March campaign post lists public-service targets and bears a NoName057(16) signature.

Not established
No independent outage, business disruption or operator identity was established.

Evidence card B19 — 1 Aug 2026

NoName-labelled account | Telegram | Telegram | EN

ORIGINAL

Continuing our "tour" of Romania

Held
An August post lists several Romanian public-service websites as targets.

Not established
The list does not establish sustained downtime or internal service impact.

The BD Anonymous claim dated 28 July concerns a public-service-themed website. It does not establish an independently measured outage. [S1]

Evidence card B18 — 28 Jul 2026

BD Anonymous | Telegram | Telegram | EN

ORIGINAL

We have successfully took down

Held
The account claimed disruption of a government-themed website.

Not established
The quotation is the actor's wording. No outage was independently established.

A ServerKillers-labelled relay dated 12 September gives an alleged duration for public-service website disruption. The duration remains a relayed claim; no common operator or measured outage is established. [S1]

Evidence card B20 — 12 Sep 2026

ServerKillers-labelled relay | Telegram | Telegram | EN

ORIGINAL

Duration: 5 hours.

Held
A September relay states a duration for government-themed disruption claims.

Not established
The duration is a relayed assertion; no common operator or measured outage was established.

Other retained claims concern a car-wash interface, surveillance access and an April administrative panel. Interface language, a screenshot and a declaration of access do not establish device ownership, location, control or physical effects. None is linked to the possible November refrigeration incidents. [S1][S63]

Evidence card B16 17 Mar 2026

DDoSia Project | Telegram | Telegram | EN

ORIGINAL

The interface is entirely in Romanian.

Held
The post describes alleged access to a car-wash control interface.

Not established
Interface language does not establish location, working control or physical effects.

Evidence card B17 30 Oct 2026

RBL Leviathan Ghost | Telegram | Telegram | EN

ORIGINAL

Team1914 | Romania CCTV Access

Held
A post carries a Team1914-labelled Romanian surveillance-access claim.

Not established
No device, session, owner or relationship between operators was validated.

Evidence card B21 7 Apr 2026

Access-claim account | Telegram | Telegram | RU

ORIGINAL

Был получен полный доступ к системе

TRANSLATION

Full access to the system was obtained.

Held
An April post claims administrative access to a Romanian service platform.

Not established
The wording is an actor assertion. No access, archive or later transfer was validated.

Some August relays on a NoName-labelled account carry Darkstorm signatures. This establishes a labelled relay, not a common operator or formal alliance. The material supplies no independent measure of sustained Romanian service disruption. [S1]

Posts dated 30 and 31 July also claim access to manufacturing control interfaces. Recipe, temperature and force labels do not establish ownership, working control or production effects. These claims are not linked to the later refrigeration reports. Validate management access and physical-process evidence with the equipment owner. [S1]

Evidence card B22 30 Jul 2026

NoName-labelled account Telegram Telegram EN

ORIGINAL

Recipes. Vacuum. Temperatures. Cycle management.

Held
A 30 July post describes alleged access to a manufacturing control interface.

Not established
No working access, equipment ownership or location, control action or production effect was independently validated.

Evidence card B23 31 Jul 2026

NoName-labelled account Telegram Telegram EN

ORIGINAL

Recipes, temperatures, closing force

Held
A 31 July post describes alleged access to another manufacturing control interface.

Not established
No working access, equipment ownership or location, control action or production effect was independently validated.

Summer claims repeatedly listed logistics and maritime-service websites, including booking and authentication pages. Treat them as alleged web-service disruption: a target list does not establish access to cargo systems, interrupted port operations or modified transactions. [S1]

On 17 September, a ServerKillers-labelled relay claimed that a Romanian financial-sector public website was unavailable for three hours. No independent outage measurement is retained. The claim does not establish access to financial systems, interrupted transactions or customer-data exposure. [S1]

6.3 Claim versus official account

The panel below keeps the questions separate. It is a decision aid, not a reconciliation of incompatible measurements.

Question	Criminal or public claim	Official or source account	Decision boundary
Is an administrator account usable?	November marketplace access advertisement [S1]	No matching confirmation established in the cited evidence	Validate sessions; do not authenticate the seller's claim
Was a public service disrupted?	An outage can be amplified as an attack claim	Foreign ministry describes short March outages and restored service [S62]	Preserve the ministry's stated scope
Was DNSC's internal network accessed?	Public-site difficulty could be presented as wider impact	DNSC describes website difficulty and possible DDoS [S25]	No internal-system conclusion follows
Were sensitive emails exported?	Research describes collection capability	SRI says no sensitive-data exfiltration was identified [S7]; ESET describes observed tool behaviour [S6] [S8]	Keep each proposition attached to its source

6.4 Timeline of disclosures and claims

4 Feb 2026	**Energy transport operator** Business IT incident reported; operational-system exclusion retained [S20]
13 Feb 2026	**Source account** Defacement interrupts a university faculty website [S79]
14 Mar 2026	**Foreign ministry** DDoS-related slowdown and short outages reported for 13–14 March [S62]
8 Apr 2026	**SRI** Participation in the router-network disruption announced [S9]
3 Jul 2026	**Source account** Repeated defacement of a transport-sector public website [S98]
10 Jul 2026	**Source account** Municipal websites investigated after loss of availability [S88]
16 Jul 2026	**Public-funding ministry** Procurement application unavailable after a cyber incident [S22]
27 Jul 2026	**Government** Ransomware and recovery account for public administrative applications [S21]
29 Jul 2026	**Detention administration** Ransomware, service suspension and system isolation reported [S23]
29 Jul 2026	**Source account** University academic and administrative services disrupted [S84][S97]
4 Aug 2026	**Source account** Ransomware response at a Romanian bank [S77][S78]
18 Aug 2026	**Regional programme authority** Procurement application restored; earlier interruption retained [S61]
8 Sep 2026	**DNSC** Temporary website difficulty; possible DDoS [S25]
25 Sep 2026	**Source account** Government document portal restricted after privacy reports [S85]
16 Oct 2026	**Capital-market operator** Incident in an auxiliary investor application disclosed [S26]
19 Oct 2026	**National reporting** Communications operator and DNSC describe an internal-network incident [S27]
22 Oct 2026	**Source account** Municipal online-payment outage and planned replacement [S89][S90]

29 Oct 2026	**Source account** Bookseller outage and November reopening [S82][S83]
30 Oct 2026	**Source account** Municipal finance office disclosed repeated attacks [S87]
3 Nov 2026	**National radio** Possible refrigeration incidents reported at six stores [S63]
10 Nov 2026	**NorthDivision** Marketplace administrator access advertised, unverified [S1]
10 Nov 2026	**ternny** Private legal-services documents advertised, unverified [S1]
10 Nov 2026	**ESET research** Government-email toolset research published; earlier activity dates retained [S6][S8]
11 Nov 2026	**SRI** December 2025 detection and response described [S7]
17 Nov 2026	**ANSPDCP** Hospitality ransomware enforcement finding published [S33]
18 Nov 2026	**DNSC warning reported** Mobile-operator and institution impersonation warning [S28]
20 Nov 2026	**Source account** Account-opening portal exposed customer documents [S80][S96]
21 Nov 2026	**Police** January–September investment-fraud study published [S29]

6.5 Recent activity: 8–22 November

The retained country-tagged forum set contains 14 posts during this period. The strongest access and document propositions are the 10 November marketplace offer and the legal-services offer. They remain unverified. Their full case boundaries appear in Cases L and M. [S1]

The legal-services dossier also contains a 5 November post by the same alias. That earlier post falls outside the recent interval while remaining relevant to the dossier's chronology. The November publications do not establish when any documents were acquired.

ANSPDCP's 11, 13 and 17 November decisions describe a credit provider, an energy-services firm and a hospitality operator. These are recent enforcement publications. Their attack dates are not given and they must not become three newly dated November intrusions. [S33][S34][S35]

The 18 November impersonation warning describes a sequence using a mobile-provider identity followed by an institutional pretext. The practical response is to stop the caller-led process and verify through an independently obtained official channel. [S28]

The police study published on 21 November covers investment-fraud complaints from January through September. It updates a historical reporting population. The study is useful for fraud controls while remaining distinct from current forum advertisements. [S29]

On 18 November a BNR speaker described a cyber stress exercise, including primary banking systems, communications and adverse social-media effects. It is an exercise scenario, not evidence that Romanian banks suffered that combined event. [S59]

Two multi-country catalogues dated 16 November also advertise shell access and include Romanian sites. They do not establish ownership, current access or a new Romanian intrusion. Treat each reference as an ownership and session-validation lead, rather than accepting the catalogue as confirmed access. [S1]

An investment-services firm's 20 November update confirmed database and document access through its account-opening portal after an incident dated 30 October. The firm said client assets remained protected while notifications and impact assessment continued. Publication does not move the initial incident into November. [S80]

A bookseller's company email reported reopening on 18 November after the October disruption. This supports recovery of a specific sales channel. It does not establish complete restoration of every service or a final data-scope finding. [S83]

A municipal 16 November notice planned a replacement online-payment service for 23 November. The latter date is after cut-off and is not observed restoration. The notice also acknowledged access problems at a national payment platform. An alternate channel described as available in October cannot be assumed continuously available. [S90]

Police explicitly denied a radar cyberattack on 17 November, describing technical evaluations instead. That denial is a control against adopting a circulating allegation, not another attack in the case total. Verify the source statement before escalating an availability headline. [S95]

6.6 Communicate the fact that is established

A useful first update states the affected service, the known interruption, the investigation boundary and the next update time. Say whether an access allegation, observed outage, unauthorised access or data disclosure is established. Keep the service owner's language precise.

An alternate status channel should remain usable if ordinary email or the main website is unavailable. Rehearse customer instructions without requiring the failed service for identity verification. Keep old contact routes available to challenge a suspicious change request.

For operational systems, include the physical-process owner. A public application outage and an abnormal refrigeration setpoint require different evidence and recovery tests. Neither establishes an actor merely because another country reported a similar event. [S63]

KEY TAKEAWAYS

01

Verify service impact separately from an actor's announcement or access offer.

02

Recent publication dates can describe older attacks, completed investigations or exercises.

03

Rehearse independent communications and service-specific recovery before the next claim.

CHAPTER 07

Threat actors and evidence relationships

THIS CHAPTER ANSWERS

Which actor propositions are supported, and which relationships must remain unconnected?

12

ransomware group labels in the Romanian listing population

7.1 Relationship map 91
7.2 Turla and Cereal: preserve two accounts 93
7.3 Behaviour matrix from the published research 94
7.4 APT28 and the router operation 95
7.5 Ransomware: listing labels and regional visibility 97
7.6 Criminal personas and common-operator claims 99
7.7 DDoS claimants and branding boundaries 100
7.8 Translate actor knowledge into a local decision 101

CHAPTER 07

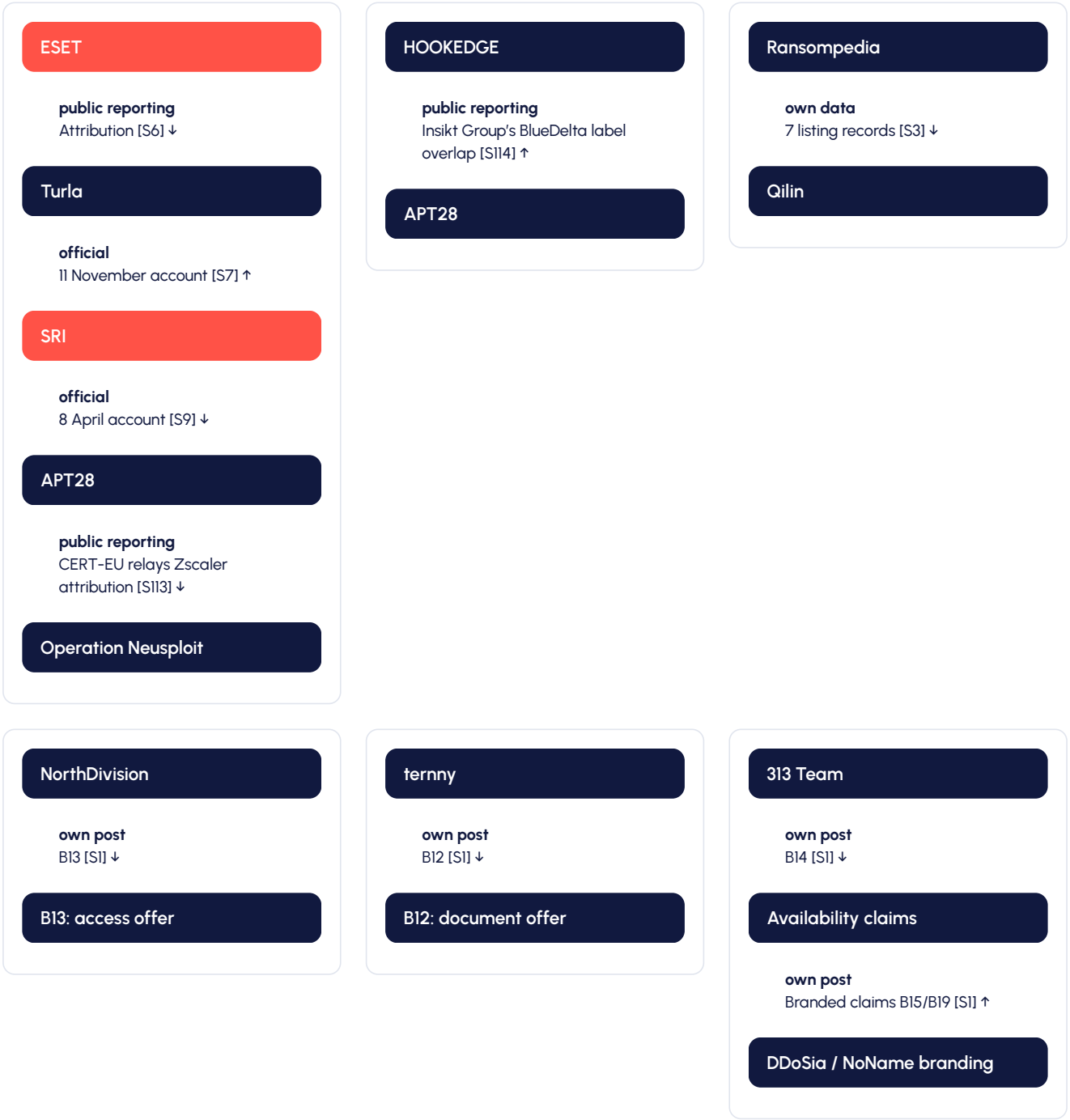
Threat actors and evidence relationships

IN SHORT

The evidence supports source-attributed espionage accounts, ransomware listing labels and criminal advertisements. They are separate populations. ESET and SRI describe Turla-related activity with different evidentiary scopes. SRI also reports a router operation attributed to APT28. Listing labels and seller aliases do not connect those campaigns to Romanian advertisements or official outages. Choose defensive controls from documented behaviour and locally validated evidence.

7.1 Relationship map

Own post Relay Official statement Public reporting Our observation



Every edge states its evidence type. Ransompedia relationships are own-data listing observations. Vendor research, official attribution and retained advertisements have different evidentiary roles. The map does not establish an overarching criminal ecosystem or shared operator.

No concrete shared element connects the market dossiers to the reported government-email case. No operator link connects Turla, APT28, Qilin and the forum sellers in this report. Keeping those nodes unconnected is part of the assessment.

7.2 Turla and Cereal: preserve two accounts

Turla

Espionage account | Attribution by ESET and SRI; no new independent attribution

IN ROMANIA, 2026

2026-11-10
ESET research published

2026-11-11
SRI response published

CLAIMED TARGETS

Government email case with earlier activity dates

SEEN IN PUBLIC REPORTING

[S6] Vendor research

[S7] Official response

OUR ASSESSMENT

Inspect mail integrity and account evidence while preserving both sources' scope.

CONFIDENCE
Confidence applies to the stated proposition

ESET's 10 November research attributes Cereal to Turla with high confidence. It describes a Romanian government Exchange case from December 2025, with greater activity on 20 January 2026. ESET did not establish the initial access method. [S6][S8]

SRI's 11 November statement says its National Cyberint Centre identified the attack in December 2025, stopped it, remediated the email service and identified no sensitive-data exfiltration. It refers to systemic Microsoft operating-system vulnerabilities without naming a CVE. [S7]

These propositions should remain visible together. A collection capability does not establish a specific exported volume. An official no-exfiltration-found statement describes the investigation's finding, rather than a universal proof of absence. The report cannot resolve the sources' observation periods or scope differences.

The defensive consequence is to inspect mail-server integrity and privileged access together. Network blocklists alone would not answer the behaviours described in the research. Establish what telemetry would distinguish legitimate maintenance, unexpected code loading and unauthorised mail access.

7.3 Behaviour matrix from the published research

The table selects behaviours explicitly named in ESET's white paper. It does not assert that every technique occurred in Romania or that a local detection has been tested. [S8]

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Execution	Stealth	Collection
T1047 Windows Management Instrumentation	T1055.001 DLL injection	T1114.002 Remote email collection
	T1620 Reflective code loading	T1119 Automated collection

Selected behaviours named in ESET research; not a tested detector or a Romania-specific technique inventory. [S8] [S6]

Behaviour	ATT&CK ID	Research scope	Defender question
Windows Management Instrumentation	T1047	Queries described in the toolset research	Does administrative activity match an approved task?
DLL injection	T1055.001	Injection into a process described by ESET	Can endpoint telemetry explain unexpected module activity?
Reflective code loading	T1620	Loading into memory described for components	Are unusual loads correlated with identity and service events?
Remote email collection	T1114.002	Mailbox retrieval described in the research	Can mail access be traced to an authorised identity?
Automated collection	T1119	Email selection and staging behaviour	Are unusual mail exports or service actions reviewed?

A technique matrix is a map of described behaviour, not a production rule. A control owner should test any resulting analytic against authorised maintenance and known benign mail-processing components before using it operationally.

7.4 APT28 and the router operation

APT28

Source-attributed router and Office campaigns | SRI attributes the operation to APT28 and GRU

IN ROMANIA, 2026

2026-03-02
Neusploit official summary published

2026-04-08
SRI participation announced

CLAIMED TARGETS

Separate router and document-delivery campaigns described by cited sources

SEEN IN PUBLIC REPORTING

[S9] SRI account

[S10] Joint advisory

[S113] CERT-EU summary

[S114] Insikt Group research

OUR ASSESSMENT

Validate router configuration and remote-access evidence; no link to Turla is established.

CONFIDENCE
Confidence applies to the stated proposition

SRI announced participation in Operation Masquerade on 8 April. It described disruption of a router-based attack network, attributed the activity to APT28 and GRU, and said the activity included entities in Romania. [S9]

The FBI-led advisory describes altered router DNS settings and credential-interception risks. It names CVE-2023-50224 in the broader campaign. The advisory does not establish that this vulnerability was used against every Romanian entity or connect it to Cereal. [S10]

NVD describes an unauthenticated information-disclosure issue affecting TP-Link router installations. Its record and the vendor advisory require hardware-specific treatment. The vendor lists TL-WR841N V8–V12 as partially patched, including EU_V11_211209 and EU_V12_230317. These are not universal fixes for every hardware revision. [S11][S12]

Use the vendor's current model and region table. Replace unsupported devices where no suitable update exists, restrict management exposure and inspect unexpected DNS configuration changes. Do not infer a Romanian incident from owning a model that appears in an advisory.

CERT-EU's February Cyber Brief, published 2 March, relays Zscaler's Operation Neusploit research. It names Romania among the campaign's target countries and attributes the activity to APT28. The summary gives no Romanian victim count and does not connect the campaign to Cereal or the router operation. [S113]

The campaign concerns CVE-2026-21509. NVD describes a local Microsoft Office security-feature bypass. Microsoft's KB5002713 addresses it for Office 2016 MSI and explicitly excludes Click-to-Run. [S111][S112]

The CVE record covers the products below on both 32-bit and x64 systems. For LTSC and Microsoft 365 Apps, it refers to applicable security releases rather than one universal fixed build. [S116]

Affected product and versions	Corresponding fixed release
Office 2016 MSI: before 16.0.5539.1001	16.0.5539.1001; KB5002713; not Click-to-Run [S112][S116] [S118]
Office 2019 Click-to-Run, volume licensed: before 16.0.10417.20095	1808, build 16.0.10417.20095 [S116][S118][S119]
Office LTSC 2021: 16.0.1 up to the applicable security release	Volume licensed: 2108, build 14334.20522 [S116][S117]
Office LTSC 2024: 16.0.0 up to the applicable security release	Volume licensed: 2408, build 17932.20670 [S116][S117]
Microsoft 365 Apps for Enterprise: 16.0.1 up to the applicable security release	Select the channel and version below [S116][S117]

The LTSC builds above and Microsoft 365 Apps builds below are the 10 February 2026 releases that include the fix, not claims about the first fixed build. [S117]

Microsoft 365 Apps channel	Fixed release: version / build
Current Channel	2601 / 19628.20204
Monthly Enterprise Channel	2512 / 19530.20226; 2511 / 19426.20294; 2510 / 19328.20306
Semi-Annual Enterprise Channel	2508 / 19127.20532; 2502 / 18526.20714; 2408 / 17928.20776

Microsoft also describes service-side protection for Microsoft 365 Apps and Office 2021 or later, requiring an application restart. Office 2016 and 2019 require their security update. [S118]

Select the current update for the deployed edition, licensing type and channel. Treat the listed releases as historical patch references. Do not substitute an MSI package for Click-to-Run or a volume-licence build for retail. Then validate document controls and unexpected email access.

Insikt Group's HOOKEDGE research describes campaigns from late September 2025 to early April 2026, including Romanian targets. The vendor assesses the BlueDelta association with moderate confidence and describes overlap with the APT28 label. It reports macro-enabled Word delivery and a Windows backdoor. These findings do not establish a Romanian victim total or connect the activity to the other campaigns here. [S114]

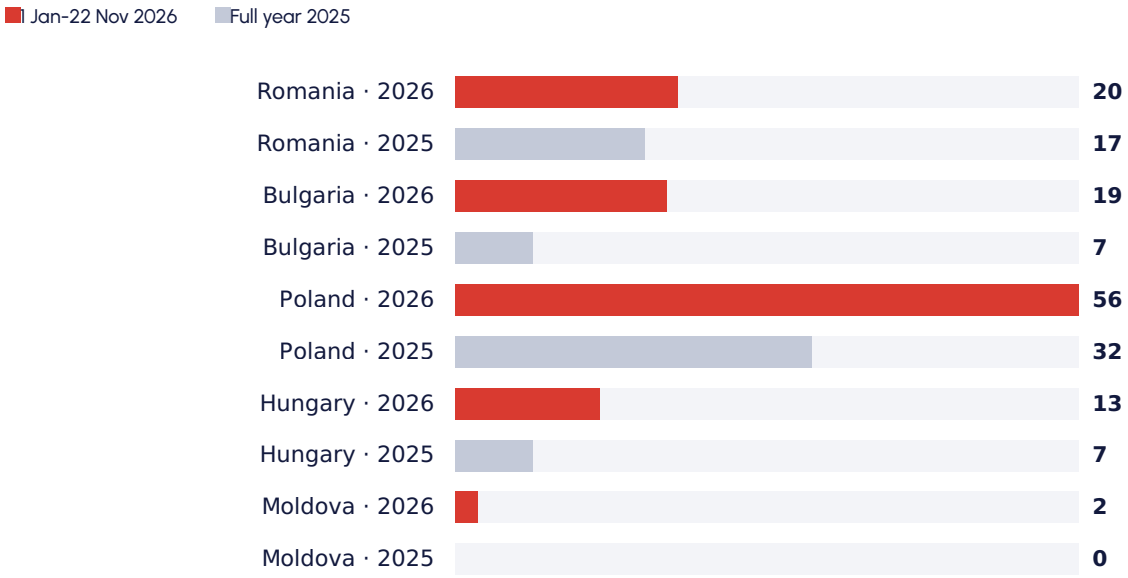
Block untrusted document macros according to approved policy. Review unexpected scheduled tasks and outbound use of legitimate web services with local endpoint evidence. A shared source label is not evidence that two Romanian incidents share infrastructure or operators.

7.5 Ransomware: listing labels and regional visibility

Ransompedia records 20 Romanian listings under twelve group labels. Qilin contributes 7, Lockbit5 and Thegentlemen contribute 2 each, and nine labels contribute 1 each. These are recorded listing labels, not an independent attribution of every officially disclosed incident. [S3]

The 20 listings concern 19 organisations. They remain claim records rather than confirmed intrusions. [S3]

Regional listing totals describe visibility rather than a country risk ranking



Source: Ransompedia country-associated listing claims [S3]. 2026: 1 January–22 November, closing day partial; 2025: full year. Unequal periods and source visibility; not a national security ranking or a matched-period growth rate.

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

Country	Window listings	All of 2025	Comparison limit
Romania	20	17	Partial year and full year differ
Bulgaria	19	7	Different economy and source visibility
Poland	56	32	Larger regional economy; no size adjustment
Hungary	13	7	Selected regional comparator
Moldova	2	0	Smaller population; zero is this source's visibility

The comparator choice reflects adjacency, regional dependencies and the Romanian-language context. The figures do not measure national reporting quality, losses, security maturity or attack probability. A listing can concern a repeated organisation or a group structure.

An April pharmaceutical-sector relay and July–August education-sector relays correspond to listing publications. This corroborates the visibility of the claims, not victim acknowledgement. The two education dates concern one organisation and do not establish two intrusions. [S1][S3]

A March law-enforcement-record relay has no matching new 2026 listing in the retained Romanian feed. A related older listing is dated 2024. It cannot confirm the freshness, origin or volume of the new relay. Keep the claim separate from a verified incident. [S1][S3]

Qilin

Ransomware listing label | No independent state attribution

IN ROMANIA, 2026

2026 window

7 Romanian listing records [S3]

CLAIMED TARGETS

Several sector labels; listed organisations are not named

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

Seven own-data listings do not establish seven unique intrusions. [S3]

CONFIDENCE

Confidence applies to the stated proposition

7.6 Criminal personas and common-operator claims

NorthDivision

Forum seller alias | State direction not established

IN ROMANIA, 2026

2026-11-10
Marketplace offer B13

CLAIMED TARGETS

Generic retail platform

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

An administrator-access advertisement is held; working access and sale remain unverified. [S1]

CONFIDENCE
Confidence applies to the stated proposition

ternny

Forum seller alias | State direction not established

IN ROMANIA, 2026

2026-11-05
Document claim

2026-11-10
Document offer B12

CLAIMED TARGETS

Generic private legal-services material

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

The posts do not validate files, counterparties, acquisition date or completed sale. [S1]

CONFIDENCE

Confidence applies to the stated proposition

Aliases identify the names used on retained posts. A persistent name can support continuity of advertising, while authorship, account control and common operation remain separate questions. Similar wording across aliases is insufficient to connect the January and June government-themed offers. [S1]

The legal-services dossier supports two observed posts under one alias. It does not establish the same underlying file, a completed sale or access to every named counterparty. The marketplace dossier supports an access advertisement, without independent authentication of the account.

7.7 DDoS claimants and branding boundaries

313 Team

DDoS claimant | No independent state attribution

IN ROMANIA, 2026

2026-03-11
Government-themed claim B14

CLAIMED TARGETS

Generic public-service websites

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

The two-hour wording is prospective; independent duration and impact are not established. [S1]

CONFIDENCE
Confidence applies to the stated proposition

DDoSia Project / NoName-labelled accounts

Campaign branding in retained posts | State direction and common operator identity not independently established

IN ROMANIA, 2026

2026-03
Romanian targeting claims B15

CLAIMED TARGETS

Public services, transport, energy and finance in source claims

2026-08-01
Public-service claim B19

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

Signatures and branding establish the wording observed, not the operator or operational outcome. [S1]

CONFIDENCE
Confidence applies to the stated proposition

The retained posts establish claims under the named brands. They do not independently establish state direction, common operator identity, access to internal systems or a relationship to the officially reported outages. A relay is kept distinct from an original claim. [S1]

7.8 Translate actor knowledge into a local decision

Use a campaign description to choose the evidence to examine. Email collection calls for mailbox and server-integrity evidence. Router manipulation calls for device ownership and configuration review. A listing calls for continuity and disclosure triage. An advertisement calls for account and data validation.

Avoid using a familiar actor name to fill a missing link. A known ransomware label does not establish encryption in a specific public incident. A state attribution in one official campaign does not transfer to a separate outage or seller.

KEY TAKEAWAYS

01
Attach every state attribution and actor proposition to its source.

02
Ransomware labels, forum aliases and officially reported campaigns remain separate.

03
Build controls from documented behaviour and local validation, rather than an assumed common operator.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How can personal information become an unauthorised instruction or transaction?

3

distinct validation questions: identity, authority and transaction

8.1 Information is not authority 103
8.2 Payment-card material: narrow scope 103
8.3 Accounts, verification and document reuse 104
8.4 Asking prices are not market value 104
8.5 Official campaign observations 104
8.6 Investor warnings and cross-border enforcement 106
8.7 Make the fraud hand-off practical 106

CHAPTER 08

The fraud economy

IN SHORT

Romanian advertisements combine identity information, accounts and access claims. Official warnings describe impersonation, investment fraud and abuse of social accounts. A genuine name, invoice or document can make a request credible without authorising it. The narrow payment-card population does not measure national fraud. Test account recovery, payee changes and customer contact against an adversary who already knows personal details.

8.1 Information is not authority

The retained offers describe customer, company, invoice, education and legal information. These records could support a persuasive approach if authentic. They do not authorise a recipient to change a payment destination, restore an account or disclose further documents. [S1]

Build a verification process around the requested action. A customer name can help locate a record, while a sensitive change should require independent proof of authority. Use a contact route established before the suspicious request and avoid the new number or address supplied in it.

The distinction matters for support teams as well as treasury. An account-recovery attacker can use a correct order reference or document description. Staff should know which facts are lookup information and which controls authorise a change.

8.2 Payment-card material: narrow scope

SCOPE OF THE CARD FIGURES

These figures cover only payment cards that appeared in clear text in dark-web posts collected for this report. Brandefense detects stolen cards through many other methods outside this report. The figures do not measure card theft, card validity or fraud loss.

The retained-post population contains 94 distinct Romania-associated cards in 107 posts. The observations do not establish that the cards remained valid or that a payment occurred. [S4]

The sample is not a basis for estimating all Romanian card exposure or recommending blanket reissuance. An issuer should validate account status, attempted transactions and its own fraud evidence before deciding customer action. A poster's claimed approval status is not confirmation of a successful payment.

8.3 Accounts, verification and document reuse

The consumer-account dossier includes requests for identity-verification bypass and account-checking tools. A request establishes demand, without demonstrating a working capability. The citizen-photo advertisement similarly does not identify the source system or prove a new loss from a state register. [S1]

For a service using identity documents, test recovery and enrolment against reused images and known personal details. Review exception handling, repeated attempts and changes to contact information. The completion evidence should demonstrate the authorisation decision, rather than merely record that a document was uploaded.

Avoid interpreting the language of a post as the nationality of its author. English and Russian can be market languages. Country references may describe supported customers or payment markets, rather than an intrusion location.

Other posts advertise or seek bank-linked accounts, account handovers and capacity to receive payments. Claimed recurring flows do not establish transfers, working access, bank-system intrusion or losses. Fraud teams should validate the account holder and payment authority separately from the advertiser's identity. [S1]

8.4 Asking prices are not market value

Observation	Quoted unit	Price	Limit
January fashion-retailer offer	Claimed dataset of 84,792 lines	USD 200	Post and claimed breach dates conflict; authenticity and sale unverified
May customer-data offer	Claimed dataset of 86,283 lines	USD 300	Asking price; authenticity and sale unverified
November vehicle lookup	1,000 lookups	USD 10	Service advertisement; source authority unverified

Source: retained advertisements [S1]. The offers concern different units and cannot support a common median price. Neither a visible price nor a reply establishes that money changed hands.

A low asking price does not prove fabrication. A high price does not prove quality or current access. Treat the advertised number, price and freshness as separate propositions requiring evidence.

8.5 Official campaign observations

The table follows the publication chronology. Its rows describe warnings or investigations, not a set of confirmed new attacks on those dates.

Published	Source account	Evidence boundary	Defensive decision
26 January	DNSC courier-themed SMS and messaging fraud warning reported [S54]	Warning, not a victim census	Verify delivery instructions in the known service
11 February	DNSC trademark-fee phishing warning reported [S56]	Payment pretext, not proof of a registrar intrusion	Check authority and invoice origin independently
17 April	Institutional-identity phishing warning reported [S55]	Use of an authority's name does not make it the attacker	Validate alleged official requests through a known channel
8 July	Police marketplace-account fraud investigation [S30]	Alleged conduct under investigation	Review account recovery and transaction communications
5 August	SRI warns of caller-identity spoofing [S31]	Displayed number does not authenticate a caller	Call back through independently verified contact information
9 August	Police vishing warning [S32]	Campaign warning, not a count of successful transfers	Reject caller-led remote access or payment instructions
18 November	DNSC warning about successive mobile-provider and institutional impersonation [S28]	Claimed authority is part of the pretext	Stop the sequence and verify separately
18 November	DIICOT social-account phishing investigation reported [S53]	Alleged activity dated September 2024–January 2025	Review recovery and warn contacts after verified account abuse
21 November	Police January–September investment-fraud study [S29]	Retrospective complaints, not November attack incidence	Train fraud and support teams on escalation and evidence

Police reported 1,624 complaints in the January–September investment-fraud study. It described more than RON 73.6 million in 1,346 situations and about EUR 8.5 million in 260 situations. Currency categories and situations must not be summed into a unique-victim count. [S29]

The study supports a business response: customers need a route to challenge a purported investment opportunity or transfer instruction before paying. After a suspected transfer, preserve the communication and transaction trail and use the financial institution's established fraud channel.

Additional dated warnings preserve the same distinction between a customer-targeting lure and an institutional intrusion.

Published	Source account	Evidence boundary	Defensive decision
2 April	Tax-authority impersonation calls use public names to request personal or banking information; a regional warning followed on 20 May [S91] [S92]	Identity pretext; no authority-system intrusion established	Verify the request using an independently obtained official channel
7 May	Digitalisation authority warns of SMS links to cloned citizen-payment pages [S101]	Warning, not proof of the legitimate platform's intrusion	Open the known service independently and verify payment authority
23 May	Energy supplier warns about invoice-payment phishing [S102]	Customer-targeting warning; supplier-network intrusion not established	Check invoice origin and payment changes through known contacts
4 August	Postal regulator describes delivery-fee, address, locker and messaging-account lures [S93]	Sector warning does not establish a courier intrusion	Reject caller-led account linking and verify through the known delivery service
24 August	A newsroom receives bank-impersonation emails [S103]	Media-observed lure; scale and bank-system intrusion unproved	Verify device-reset and authentication requests independently
5 October	A reader-submitted refund lure is described by a technology publication [S104]	Successful theft and merchant intrusion not established	Verify refunds inside the known merchant or payment service

8.6 Investor warnings and cross-border enforcement

ASF's investor-alert register contains dated warnings about unauthorised or misleading investment services. A warning is a due-diligence signal, not an attribution of every fraudulent message using a similar brand. Confirm the precise legal entity and authorised service through the regulator's current information. [S57]

A November police update describes alleged tax-platform fraud involving searches in Romania and an affected foreign service. It is relevant cross-border enforcement, not proof of Romanian customer-data exposure. Suspects and allegations remain subject to the investigation. [S52]

8.7 Make the fraud hand-off practical

Agree what information security sends to fraud operations: a validated account or record relationship, the possible action enabled, relevant dates and remaining uncertainty. Avoid sending a large unqualified volume as an instruction to block customers.

Customer operations should own warnings and trusted callbacks. Treasury should own beneficiary changes. Identity operations should own credentials and sessions. Privacy should assess affected records. The incident lead should reconcile these decisions without turning every signal into the same response.

KEY TAKEAWAYS

01

Genuine information does not establish authority for a sensitive change.

02

Card observations and asking prices retain narrow units and cannot measure national losses.

03

Join identity, fraud and customer operations around validated evidence and trusted contact routes.

CHAPTER 09

Banking and financial services

09

THIS CHAPTER ANSWERS

Which financial controls follow from the evidence without overstating exposure?

30

selected financial-domain candidates, not thirty independently verified banks

9.1 Population and limits 109
9.2 Employee authority needs evidence of business purpose 109
9.3 Processing errors and attacks need different remediation 110
9.4 Payment context is not payment authority 110
9.5 Customer services and critical market functions 110
9.6 The cyber stress scenario remains a scenario 111
9.7 Joint ownership and reporting 111

CHAPTER 09

Banking and financial services

IN SHORT

Financial services need separate controls for employees, customers, suppliers and transaction authority. The 30 financial-domain candidates contain at least 10,503 device associations and 63,106 credential-record associations. Official decisions describe unauthorised staff access, notification-processing errors and an IT attack. A November cyber stress discussion is an exercise, not a bank incident. Validate account access, protect payment changes and test customer service alongside technical recovery.

9.1 Population and limits

The financial group contains 30 candidate domains. It includes authorities, market infrastructure, payment and investment services as well as banks. It is not a census of licensed card issuers or thirty independent banks. Domain ownership and entity independence remain selection limits. [S2]

The financial portfolio contains at least 10,503 device associations, including 284 employee-device associations, and 63,106 credential-record associations. Current listings concern 9 of its 30 domains. These overlapping observations do not establish active customer accounts, fraud losses or confirmed intrusions. [S2]

The card observations include 26 cards under 7 financial labels. These labels do not establish licensed issuer status. Account and issuer validation must precede customer action. [S2][S4]

SCOPE OF THE CARD FIGURES

Any payment-card figures referenced here cover only cards appearing in clear text in the collected posts. Brandefense detects stolen cards through many other methods outside this report. Those figures do not measure card theft, validity or fraud loss.

The separate card population contains 94 cards in 107 posts, with the scope above. It is not the selected financial-domain exposure population. The financial-label card observations do not establish an incident in issuer infrastructure. [S4]

9.2 Employee authority needs evidence of business purpose

The 2 July ANSPDCP finding describes an employee accessing customer-account statements outside assigned duties at a third party's request. ANSPDCP's November decision also concerns access beyond staff authorisation. These are access-governance findings, not evidence of a common external campaign. [S40][S41]

Review unusual customer-record lookups alongside role, case assignment and business purpose. Privileged access is not automatically legitimate because the employee authenticated successfully. Keep an auditable explanation for exceptions and a route to investigate misuse without circulating customer records unnecessarily.

9.3 Processing errors and attacks need different remediation

The 29 May decision describes manual file processing that sent insurance-renewal information to wrong recipients. It includes a separate delayed-notification finding. The relevant controls include recipient matching, quality checks and prompt awareness assessment. A malware-only response would not address the cause. [S39]

The November credit-provider finding describes an IT attack and inadequate protection of personal data. Its scope should guide access review and recovery evidence. It does not establish every bank's exposure or provide a national financial-sector attack rate. [S35]

9.4 Payment context is not payment authority

Invoice and customer-data offers can make fraudulent instructions plausible. A correct reference, company name or balance should not authorise a new beneficiary. Use a previously agreed channel to verify changes, with a second owner for sensitive payments. [S1]

Customer recovery needs the same discipline. Changing the phone or email used for approval can move authority even when the account password remains unchanged. Test the institution's real workflow and evidence, rather than assuming that one authentication control protects every decision.

A 14 September monitoring relay alleged that Italian law-enforcement systems had been used to request customer information from a financial service, and included Romanian residents in a wider country list. No Romanian data subset was validated. This is a claim about an abused disclosure channel, without evidence here of intrusion into the financial service's systems. [S1]

9.5 Customer services and critical market functions

The auxiliary investor-application incident illustrates a useful distinction. The operator's statement preserves the functioning and integrity of critical settlement and registry services. The public-facing application and potential customer-data questions remain separate. [S26]

The practical exercise should require both owners to provide evidence: market operations for critical functions, and customer-service or privacy owners for account information. A statement about one surface must not silently close the investigation of the other.

The investment-services firm's later account-opening case makes the boundary concrete. Protected client assets do not establish that onboarding documents were inaccessible to an unauthorised party. The firm confirmed portal database and document access while retaining unresolved scope. Test onboarding, trading and custody boundaries separately, and give privacy assessment its own evidence. [S80]

9.6 The cyber stress scenario remains a scenario

The BNR discussion reported on 18 November describes a stress exercise combining loss of primary IT and a main communications channel, with adverse social-media effects. It considers how an operational event could become a liquidity concern. This is planning context, not a reported combined attack. [S59]

For an institution using a similar planning assumption, test payment access, customer contact, liquidity information and decision authority together. Record the minimum service that can operate, who approves exceptional transactions and how customers receive a trustworthy update.

9.7 Joint ownership and reporting

Decision	Accountable owner	Evidence of completion
Account and session containment	Identity and security operations	Validated scope and session decisions
Suspicious customer contact	Fraud and customer operations	Tested escalation and trusted callback
Sensitive payment change	Treasury or payment operations	Independent verification and approval record
Staff information access	Data owner and compliance	Business-purpose review and exception decisions
Service restoration	Business-service owner	Recovery test with customer workflow acceptance
Supervisory notification	Legal and designated reporting owner	Applicable regime, awareness time and submitted information recorded

DORA reporting, civilian cybersecurity duties and personal-data obligations require their own applicability decisions. The reporting team should retain one factual chronology while applying the correct route to each obligation. Chapter 10 sets out the distinctions. [S13][S14][S15][S60]

KEY TAKEAWAYS

01

Keep employee, customer, supplier and transaction-authority decisions separate.

02

Access misuse and processing errors need controls alongside external-attack detection.

03

Test customer communications, critical functions and supervisory reporting with the recovery exercise.

CHAPTER 10

Regulation and national response

10

THIS CHAPTER ANSWERS

Which duties apply, and how should an organisation avoid using the wrong reporting clock?

6 hours

maximum for the specified cross-border information report under Article 15(3)

10.1 Read the instrument and its amendment together 113
10.2 Civilian cybersecurity reporting clocks 113
10.3 Sanctions depend on the infringement 114
10.4 Personal-data reporting remains separate 115
10.5 DORA and financial reporting 115
10.6 Rehearse one incident with several obligations 115

CHAPTER 10

Regulation and national response

IN SHORT

Romania's civilian cybersecurity framework, GDPR and DORA have different scopes, triggers and recipients. The cybersecurity framework includes a specific cross-border information deadline alongside its early warning and incident notification. Financial entities require the DORA applicability distinction. Enforcement cases also show that processing errors can create notification duties. Identify the legal entity, applicable regime, awareness time and reporting owner before rehearsing the first report.

10.1 Read the instrument and its amendment together

Emergency Ordinance 155/2024 establishes Romania's civilian cybersecurity framework. Law 124/2025 approved it with amendments. The original ordinance and the promulgated amendment must be read together; an earlier summary can miss changed sanctions or management duties. [S13][S14]

Article 2 excludes specified defence, public-order, national-security and law-enforcement institutions and classified systems. Its treatment of entities subject to DORA is also distinct. These exclusions do not justify assuming that every public body or every financial-domain candidate follows the same route. [S13]

The legal team should record the actual entity and service classification, the competent authority and applicable implementing provisions. This chapter is an operational guide, not a substitute for that entity-specific legal assessment.

10.2 Civilian cybersecurity reporting clocks

The table summarises Article 15. Each time limit retains its own trigger. The reporting obligation is prompt, with the stated period as a maximum. [S13]

Trigger	Required stage	Maximum	Important distinction
Awareness of information enabling the national CSIRT to identify cross-border impact	Cross-border information report	6 hours	Specific Article 15(3) information duty
Awareness of a significant incident	Early warning	24 hours	Indicate suspected malicious conduct or cross-border impact where relevant
Awareness of a significant incident	Incident report	72 hours	Initial severity, impact and available indicators
National CSIRT request	Intermediate update	As requested	Separate from scheduled final reporting

Trigger	Required stage	Maximum	Important distinction
Incident report submitted	Final report	One month	Describe incident, likely cause, mitigation and cross-border impact
Incident ongoing at final-report stage	Progress report, followed by final report	Final within one month of handling the incident	Do not omit the continuing-incident path
Significant incident affecting trust services	Trust-service incident report	24 hours	Exception to the ordinary 72-hour incident-report stage

The ordinance identifies the national reporting platform for the civilian route. An organisation should establish access and an alternate reporting owner before an incident. A forum allegation alone does not automatically establish a significant incident; preserve the evaluation and awareness chronology. [S13]

10.3 Sanctions depend on the infringement

Law 124/2025 changes Article 60's sanction bands. The largest bands apply to specified infringements, not every late action or every incident. Turnover means the entity's worldwide annual turnover in the last financial year. [S14]

Entity or category	Specified sanction band	Boundary
Important entities, Article 60(2)(a) infringements	RON 5,000 to EUR 7,000,000 equivalent or 1.4% of worldwide annual turnover, whichever maximum is higher	Applies to the listed infringement letters
Essential entities, Article 60(2)(b) infringements	RON 10,000 to EUR 10,000,000 equivalent or 2% of worldwide annual turnover, whichever maximum is higher	Applies to the listed infringement letters
Important entities, Article 60(2)(c) infringements	RON 1,000–300,000	Separate listed infringements
Essential entities, Article 60(2)(d) infringements	RON 1,500–500,000	Separate listed infringements
Article 60(2)(e) category	RON 1,000–100,000	Separate listed infringements
Serious infringements under Article 60(2¹)	RON 3,000–600,000	Repeated-infringement increase and individualisation require the statutory conditions

Do not present a maximum fine as an incident-loss estimate. The management and reporting owner should instead demonstrate the classification decision, the required controls and the timeliness of its response.

10.4 Personal-data reporting remains separate

ANSPDCP's official FAQ states that a controller notifies the competent supervisory authority without undue delay and, where feasible, within 72 hours of awareness. The exception concerns a breach unlikely to create risk to individuals' rights and freedoms. [S15]

The May banking decision illustrates a separate delayed-notification finding alongside security shortcomings. The underlying cause was a processing error, rather than an established external attack. The incident lead must therefore pass misdelivery and access-control events to the privacy team as well as malware cases. [S39]

Record the awareness time, affected data, risk decision and information available at each stage. A supplier's ongoing investigation does not by itself answer the controller's own reporting question.

10.5 DORA and financial reporting

ASF's official presentation states that DORA applies from 17 January 2025. It describes reporting major ICT incidents to the relevant competent authority, and informing customers without undue delay where their financial interests are affected. [S60]

Article 2(3) of the Romanian civilian framework preserves only Articles 5–10 and 18 for financial entities subject to DORA. Do not apply the civilian Article 15 sequence to every bank without this scope check. Confirm the appropriate BNR or ASF supervisory route for the entity. [S13][S14]

Delegated Regulation 2025/301 distinguishes awareness from classification as major. Its initial stage is as early as possible, within 4 hours of major classification and no later than 24 hours after awareness. Later major classification has a specific 4-hour rule. [S67]

The intermediate report is due within 72 hours of the initial notification. The final report follows within one month of the latest intermediate report. The regulation includes weekend, holiday and entity-specific provisions; the reporting owner must check them rather than assuming a universal extension. [S67]

10.6 Rehearse one incident with several obligations

Give the exercise team an access alert, an unavailable customer service and uncertain personal-data copying. Ask it to identify the entity, classify significance, record awareness and select the relevant recipient. Do not wait for final attribution before evaluating a reporting duty.

Require a legal or reporting owner to explain each clock. Keep the facts consistent across privacy, cyber and financial notices, while preserving their different tests. Evidence of completion is a recorded decision and a usable reporting route, including an out-of-hours alternate.

KEY TAKEAWAYS

01

Check the entity and regime before choosing a reporting deadline.

02

Preserve the specific cross-border, trust-service and DORA distinctions.

03

Give reporting, privacy and communications owners one factual timeline with separate legal decisions.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which judgements follow from the evidence, and what would change them?

4

conditional scenarios with explicit decision triggers

11.1 Key judgements 118
11.2 What would change the assessment 119
11.3 Conditional planning scenarios 119
11.4 What the data cannot forecast 120

CHAPTER 11

Outlook

IN SHORT

The evidence supports preparation for identity abuse, supplier-document loss and service disruption. It does not support a national attack probability or a ranking of sectors by security. Recent publications can reveal older activity, while advertisements can recycle older data. Use conditional scenarios with measurable triggers, and change the response when a validated account, confirmed dataset or service impact changes the evidence.

11.1 Key judgements

Judgement	Confidence and basis	Limit	Owner's response
Administrator access deserves an owned validation process	High for the observed advertising and official access-control findings [S1][S37]	Working access is not established by an offer	Identity operations investigates privileges and sessions
Documents can support secondary fraud even when origin remains uncertain	Moderate analytical judgement from the kinds of records advertised [S1]	No realised loss is inferred from an advertisement	Fraud and data owners test authority and contact verification
Recovery must include applications and customer workflows	High for the reported outages and restoration boundaries [S21][S22][S26][S61]	One case does not estimate national recovery capability	Service owner accepts a demonstrated restore
Recent espionage reporting justifies mail-integrity review	High for the existence of the source accounts [S6][S7][S8]	Source periods and outcome scope differ	SOC and mail team identify local evidence requirements
Physical-process warnings deserve scoped validation	Moderate for reported possible refrigeration incidents [S63]	The Romanian cyber mechanism and losses remain unresolved	Operations verifies controllers, alarms and supplier access

Confidence attaches to the proposition, not a seller or actor as a whole. A high-confidence observation that an advertisement exists can coexist with low confidence in its contents.

11.2 What would change the assessment

New evidence	Assessment change	Decision
An advertised account matches active unauthorised sessions	Access allegation becomes a local identity incident	Contain the validated sessions and investigate related privileges
Authorised internal checks validate sensitive records	Data claim gains a concrete local basis	Establish scope and evaluate privacy and customer protection
Operator telemetry confirms business-service interruption	Availability claim gains measured operational impact	Activate continuity and provider escalation
A later official statement changes data or recovery scope	Earlier preliminary account needs updating	Reconcile communications, notification and control work
A concrete shared technical element connects campaigns	A specific relationship may become supportable	Document the edge and preserve the source attribution

A sample match would justify investigation before adoption of the seller's entire volume or acquisition-date claim. A negative finding in one source would not establish the absence of activity elsewhere.

11.3 Conditional planning scenarios

These are planning assumptions, not predictions or probabilities.

1. **If a new administrator offer matches a current account**, validate sessions and privilege changes immediately through the account owner. Escalate confirmed unauthorised activity to incident response and assess data access separately.
1. **If a supplier confirms a sensitive-document loss**, identify which internal records and customers are implicated. Challenge payment and legal instructions through trusted routes, and evaluate notification from the confirmed scope.
1. **If public-service access is disrupted**, activate the tested alternate workflow and independently usable status channel. Measure restoration through successful user tasks, without treating the outage as proof of data access.
1. **If physical-process settings change unexpectedly**, involve operations and the equipment owner. Preserve evidence safely, verify supplier access and restore tested configuration. Do not transfer an attribution from a similar foreign report.

11.4 What the data cannot forecast

Post volumes, source listings and a purposive portfolio cannot produce a national incident probability. Advertised record counts cannot forecast fraud losses. A source's no-impact statement cannot establish how every organisation using similar technology will fare.

The useful forward view is an evidence trigger linked to an owner. Review it after new disclosures, validate changes in the same unit, and preserve the difference between an update and another incident.

KEY TAKEAWAYS

01

Give every judgement a source boundary and a signal that would change it.

02

Use validated access, data and service evidence to trigger specific actions.

03

Reassess after later disclosures without turning updates into additional incidents.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who acts over 30, 60 and 90 days, and what demonstrates completion?

18

actions with accountable owners and observable completion evidence

12.1 The 30/60/90-day plan 122
12.2 Role ownership 124
12.3 Completion scorecard 124
12.4 How Brandefense can help 125

CHAPTER 12

Action plan

IN SHORT

Begin by ensuring account and access alerts reach the right team. Validate privileges, supplier permissions and sensitive-data flows before disruptive action. Then test email policy, remote administration, payment changes and minimum service. By day 90, demonstrate recovery and a reporting exercise that joins technical, customer and legal decisions. Close each action with evidence accepted by its business owner.

12.1 The 30/60/90-day plan

1Days 1–30

Confirm account and access alert delivery for owned services

OWNER
CISO and identity operations

COMPLETION EVIDENCE
Test alert received and assigned

Validate new credential and administrator offers against active accounts

OWNER
Identity operations

COMPLETION EVIDENCE
Account, session and disposition record

Identify sensitive-document holders and export permissions

OWNER
Data owners and procurement

COMPLETION EVIDENCE
Approved service and supplier map

Inventory remote administration, including suppliers and emergency access

OWNER
Infrastructure

COMPLETION EVIDENCE
Accountable owner for every approved path

Establish entity classification and all applicable reporting routes

OWNER
Legal and compliance

COMPLETION EVIDENCE
Signed applicability record and alternate reporter

Prepare an independent status and trusted customer-contact channel

OWNER
Communications and service owners

COMPLETION EVIDENCE
Channel tested without ordinary email or main website

2Days 31–60

Protect remote administration with suitable MFA and restricted permissions

OWNER

Infrastructure and identity

COMPLETION EVIDENCE

Authorised test and exception-owner record

Review privileged mailbox and server-integrity telemetry

OWNER

SOC and mail owner

COMPLETION EVIDENCE

Evidence sources and tested triage procedure

Stage email-policy enforcement with legitimate-sender validation

OWNER

Email owner

COMPLETION EVIDENCE

Approved policy and successful legitimate delivery

Test customer recovery against reused personal information

OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Exercise result and corrected exceptions

Require independent verification for sensitive payee changes

OWNER

Treasury and payment operations

COMPLETION EVIDENCE

Approved procedure and tested change request

Remove unnecessary real personal data from test environments

OWNER

Engineering and privacy

COMPLETION EVIDENCE

Data-owner acceptance and access review

Verify camera and controller exposure, authentication and supplier access

OWNER

Operations and infrastructure

COMPLETION EVIDENCE

Approved configuration and alarm review

3Days 61–90

Restore an essential workflow with protected backups and separate credentials

OWNER

Service owner and infrastructure

COMPLETION EVIDENCE

Recovery time, integrity and workflow acceptance

Rehearse supplier notification and personal-data scope decisions

OWNER

Procurement, privacy and incident lead

COMPLETION EVIDENCE

Timeline and decision evidence

Rehearse cyber, privacy and financial reporting where applicable

OWNER
Legal and reporting owners

COMPLETION EVIDENCE
Correct recipients, clocks and out-of-hours alternate

Exercise an outage alongside a public data or access claim

OWNER
CISO, communications and business owners

COMPLETION EVIDENCE
Separate service, identity and disclosure decisions

Report unresolved evidence and overdue control work to leadership

OWNER
CISO and executive sponsor

COMPLETION EVIDENCE
Accepted scorecard with owners and dated decisions

12.2 Role ownership

The CISO owns prioritisation and escalation. The business owner accepts minimum service and recovery. Identity operations validates accounts and sessions. Procurement and data owners establish supplier scope. Privacy and legal determine applicability and notification. Customer operations manages trusted communications.

SOC and infrastructure should identify the evidence that closes a technical question. A password reset is not proof that every session or delegated permission was revoked. A reachable homepage is not proof that the business workflow recovered. An actor's silence is not proof that data was not copied.

12.3 Completion scorecard

Measure	Target	Evidence
Alert delivery	In place by day 30	Successful routed test
New account or access signal	Named owner and recorded disposition	Account and session validation
Critical remote-administration paths	Owned and tested by day 60	MFA and privilege review
Sensitive payment changes	Independently verified by day 60	Approved procedure and exercise
Essential recovery workflow	Demonstrated by day 90	Business acceptance and recorded recovery time
Applicable reporting routes	Exercised by day 90	Awareness timeline, recipients and alternate owner
Material unresolved evidence	Visible to leadership by day 90	Owner, reason and next decision date

Treat a failed exercise as evidence for a dated corrective action. Do not label an incomplete test successful because a procedure exists or a meeting occurred.

12.4 How Brandefense can help

Brandefense provides threat intelligence, dark-web monitoring and attack-surface capabilities. Use the findings here to define the domains, brands, accounts and services that require monitoring, then connect relevant alerts to accountable response owners. Product visibility complements local validation and incident evidence. [S19]

Request a Brandefense demonstration focused on identity exposure, ransomware intelligence and the services your team needs to protect.

KEY TAKEAWAYS

01

Assign every priority a business owner and observable completion evidence.

02

Test supplier notification, payment verification and independent recovery together.

03

Close actions through demonstrated decisions and functioning services.

APPENDICES

Appendices

A–E

THIS CHAPTER ANSWERS

Which populations, dates and confidence limits govern the report?

4

evidence types kept separate throughout

Appendix A. Scope and evidence boundaries 127

Appendix B. Evidence register 130

Appendix C. Sources 132

Appendix D. Glossary 136

Appendix E. Further official findings and campaign context 138

Appendix A. Scope and evidence boundaries

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

A.1 Research contract

The report covers Romania, 1 January–22 November 2026 by post date. The requested endpoint is 22 November at the end of the UTC day. Research occurred before that day ended, so later material on the cut-off day may be absent.

Public disclosures are dated by publication, with incident and discovery dates retained separately when available. The recent-activity interval is 8–22 November. Material about an earlier event is included as a recent disclosure without moving the event into November.

The intended readers are security leadership, operational teams, identity and infrastructure owners, financial and customer-protection teams, and legal and communications functions. Decisions concern validation, containment, recovery, notification and prevention of secondary harm.

A.2 Posts and advertisements

Brandefense Blackhole supplies the retained post evidence. The report distinguishes the country-tagged population from the retained archive and the 256-post country-tagged forum set. The views have different coverage and are not presented as nested populations. [S1]

The retained archive contains 41,379 distinct posts. The country-tagged population is 773,764. A post may be an advertisement, a reply, a relay, a catalogue or a claimed incident. Those objects cannot be added as independent attacks.

Country references and languages do not establish targeting, nationality, state direction or victims. A claimed quantity does not establish unique people. A claim date does not establish acquisition or initial access. Authentic excerpts remain source statements with the same uncertainty as the surrounding case.

The report establishes no completed criminal transaction from a visible price or reply alone. Similar text does not establish the same dataset, original theft, common operator or transfer between sellers.

Selected-domain observations form a separate population and are not added to the publication totals above. A global corporate-domain reference does not by itself establish a Romanian event. [S1][S2]

A.3 Selected domains and exposure observations

The portfolio contains 250 candidate domains selected for institutional and sector significance. Domain independence, complete ownership and exclusively Romanian scope are not established for every candidate. [S2]

Results describe the selected domains, rather than national prevalence or an official business ranking. Group and global domains can serve several entities or populations. Passive observations retain their actual assessed denominators and unknown outcomes.

Atlas supplies the national headline of 50/100 (B) for the selected 250-domain portfolio. 79 domains had a credential listed for sale when checked. Only the national rating is published; sector tables contain anonymous signal counts. No sector or group Atlas rating is published. [S2]

Exposure and passive observations are dated 22 November 2026. Device counts are minimum observations; credential records may be historical and populations overlap. Financial-label card observations do not verify issuer status or establish the source of card exposure.

A.4 Payment-card material

Card figures cover only payment cards appearing in clear text in the retained dark-web posts. Brandefense detects stolen cards through many other methods outside this report. These observations do not measure national card theft, current validity or fraud losses. [S4]

Issuer, country, post and card populations are different units. They must not be combined with device or credential associations. Transaction validity and customer action require issuer-specific evidence.

A.5 Ransomware listings

Ransompedia supplies the listing population for Romania and the four comparators. Dates describe listing publication, not intrusion start. A listing is a criminal assertion and can concern a repeated organisation or a group structure. [S3]

The 2026 window and the full 2025 comparison have unequal durations. Different national economies, disclosure practices and source visibility prevent a country risk ranking or a matched-period growth rate.

The same label across countries does not establish a shared operator for every event. A feed label does not independently attribute an official incident unless a concrete relationship is established.

A.6 Vulnerability and technical research

The report checks CVE-2023-50224 against NVD and the vendor advisory. The cited hardware and fixed-release examples retain the vendor's regional and version boundaries. They do not establish the vulnerability used against a particular Romanian organisation. [S11][S12]

The Cereal behaviour matrix selects techniques from the cited white paper. It is descriptive research context, not a tested detection rule or evidence that every technique occurred in Romania. No working offensive code or victim-access details are included. [S8]

A.7 Public incidents and coverage limits

Official disclosures, regulator findings, original investigations and attributed campaign reporting support the public cases. An official account can be preliminary or preserve unresolved data scope. Quoted official statements are identified when the original notice itself could not be verified.

The report includes external attacks, access misuse, processing errors, possible operational incidents and context from enforcement. They remain distinct. 31 official-account dossiers do not mean 31 confirmed intrusions occurring in 2026.

Some official archive periods and original notices could not be verified. Coverage is limited to the referenced material and is not an exhaustive national incident census. Public absence claims are not drawn from inaccessible sources.

An organisation is named as an affected party only where official confirmation and wider reporting support the name. Other cases use generic roles. Identifying article links are withheld. If the source is the unnamed organisation itself, its URL is also withheld.

A.8 Confidence and neutrality

High confidence applies to a proposition directly supported by held evidence or a clear source account. It does not authenticate every statement inside an advertisement. **Moderate confidence** identifies an interpretation with meaningful unresolved alternatives. **Unverified** preserves a claim without adopting its contents.

State attributions are presented as the source's assessments. No attribution is inferred from language, a country tag, a nationality or a political slogan. The report takes no position on governments, elections, parties, foreign relations or territorial questions.

Conditional scenarios are planning assumptions. Their value lies in an owner and an observable trigger, rather than a claimed numerical probability.

Appendix B. Evidence register

The cards reproduce short authentic excerpts with victim and contact details removed. Their translations preserve the claim boundary. Post-card IDs are public references, not raw record identifiers.

Card	Date	Venue	Alias	Language	Chapter
B01	2026-01-01	Forum	renquix	EN	4
B02	2026-01-21	Forum	EchoEcho	EN	4
B03	2026-02-16	Forum	Reddington66	EN	4
B04	2026-03-04	Forum	Eliphas	EN	4
B05	2026-04-02	Forum	xorcat	EN	4
B06	2026-04-07	Forum	xorcat	EN	4
B07	2026-03-20	Forum	fent888	EN	4
B08	2026-04-24	Forum	johnapp	EN	4
B09	2026-05-07	Forum	moxzey	EN	4
B10	2026-05-24	Forum	somewhere	EN	4
B11	2026-06-20	Forum	tempp991	EN	4
B12	2026-11-10	Forum	ternny	EN	4
B13	2026-11-10	Forum	NorthDivision	EN	4
B14	2026-03-11	Telegram	313 Team	AR	6
B15	2026-03-17	Telegram	DDoSia Project	RU	6
B16	2026-03-17	Telegram	DDoSia Project	EN	6
B17	2026-10-30	Telegram	RBL Leviathan Ghost	EN	6
B18	2026-07-28	Telegram	BD Anonymous	EN	6
B19	2026-08-01	Telegram	NoName-labelled account	EN	6
B20	2026-09-12	Telegram	ServerKillers-labelled relay	EN	6
B21	2026-04-07	Telegram	Access-claim account	RU	6
B22	2026-07-30	Telegram	NoName-labelled account	EN	6

Card	Date	Venue	Alias	Language	Chapter
B23	2026-07-31	Telegram	NoName-labelled account	EN	6
B24	2026-09-04	Telegram	Escanors Market-place	EN	4

The case manifest contains 14 advertisement dossiers and 31 official-account dossiers. Cases can group updates and related claims. Their total of 45 is an editorial count, not unique attacks, victims or confirmed 2026 intrusions.

Appendix C. Sources

Own-data references describe Brandefense's retained evidence. Their publisher homepages do not independently reproduce the underlying counts. External sources were read for the propositions used; withheld links preserve the public naming boundary.

S1: Odin by Brandefense · Romania post evidence and aggregate observations · source · Verified on 2026-11-22.

S2: Odin by Brandefense · Atlas national rating, selected-domain exposure and passive observations · source · Verified on 2026-11-22.

S3: Ransompedia · Romanian and regional ransomware listing observations · source · Verified on 2026-11-22.

S4: Brandefense Blackhole · Payment-card aggregate in retained posts · source · Verified on 2026-11-22.

S5: DataReportal · Digital 2027: Romania; October 2026 data · source · Verified on 2026-11-22.

S6: ESET · Exchange for breakfast: Cereal research · source · Verified on 2026-11-22.

S7: SRI · Government-email incident response statement, 11 November 2026 · source · Verified on 2026-11-22.

S8: ESET · Cereal white paper, 10 November 2026 · source · Verified on 2026-11-22.

S9: SRI · Operation Masquerade participation statement, 8 April 2026 · source · Verified on 2026-11-22.

S10: FBI and international partners · Router DNS manipulation advisory, 7 April 2026 · source · Verified on 2026-11-22.

S11: NVD · CVE-2023-50224 record · source · Verified on 2026-11-22.

S12: TP-Link · CVE-2023-50224 hardware and firmware advisory · source · Verified on 2026-11-22.

S13: Official Gazette via EUR-Lex · Emergency Ordinance 155/2024, original official text · source · Verified on 2026-11-22.

S14: Romanian Senate · Promulgated Law 124/2025 approving Ordinance 155/2024 with amendments · source · Verified on 2026-11-22.

S15: ANSPDCP · Official FAQ: personal-data breach notification · source · Verified on 2026-11-22.

S18: RFC Editor · RFC 9989: DMARC · source · Verified on 2026-11-23.

S19: Brandefense · Product demonstration and capabilities · source · Verified on 2026-11-22.

S20: Official or attributed public source · CONPET business IT incident filing · source · Verified on 2026-11-22.

S21: Official or attributed public source · Government land-administration ransomware update · source · article URL withheld · Verified on 2026-11-22.

S22: Official or attributed public source · Public-funding procurement application notice · source · article URL withheld · Verified on 2026-11-22.

S23: Official or attributed public source · Detention-administration ransomware communiqué · source · article URL withheld · Verified on 2026-11-22.

S24: Official or attributed public source · Detention-administration next-day restoration update · source · article URL withheld · Verified on 2026-11-22.

S25: Official or attributed public source · DNSC website availability statement · source · Verified on 2026-11-22.

S26: Official or attributed public source · Capital-market auxiliary application communiqué · source · article URL withheld · Verified on 2026-11-22.

S27: Official or attributed public source · Communications operator and DNSC incident statements · source · article URL withheld · Verified on 2026-11-22.

S28: Official or attributed public source · DNSC two-call impersonation warning · source · Verified on 2026-11-22.

S29: Official or attributed public source · Police investment-fraud study January-September · source · Verified on 2026-11-22.

S30: Official or attributed public source · Police marketplace-account fraud investigation · source · Verified on 2026-11-22.

S31: SRI · SRI caller-identity spoofing warning · source · Verified on 2026-11-22.

S32: Official or attributed public source · Police vishing warning · source · Verified on 2026-11-22.

S33: ANSPDCP · ANSPDCP hospitality ransomware decision · source · article URL withheld · Verified on 2026-11-22.

S34: ANSPDCP · ANSPDCP petroleum-services security decision · source · article URL withheld · Verified on 2026-11-23.

S35: ANSPDCP · ANSPDCP credit-provider security decision · source · article URL withheld · Verified on 2026-11-22.

S36: ANSPDCP · ANSPDCP software test-server decision · source · article URL withheld · Verified on 2026-11-22.

S37: ANSPDCP · ANSPDCP administrator-phishing decision · source · article URL withheld · Verified on 2026-11-22.

S38: ANSPDCP · ANSPDCP telecommunications applications decision · source · article URL withheld · Verified on 2026-11-22.

S39: ANSPDCP · ANSPDCP banking notification-processing decision · source · article URL withheld · Verified on 2026-11-22.

S40: ANSPDCP · ANSPDCP banking insider-access decision · source · article URL withheld · Verified on 2026-11-22.

S41: ANSPDCP · ANSPDCP banking access-rights decision · source · article URL withheld · Verified on 2026-11-23.

S42: ANSPDCP · ANSPDCP retail account-validation decision · source · article URL withheld · Verified on 2026-11-22.

S43: ANSPDCP · ANSPDCP automotive supplier-managed application decision · source · article URL withheld · Verified on 2026-11-22.

S44: ANSPDCP · ANSPDCP professional-services security decision · source · article URL withheld · Verified on 2026-11-22.

S45: ANSPDCP · ANSPDCP industrial-services security decision · source · article URL withheld · Verified on 2026-11-22.

S46: ANSPDCP · ANSPDCP cross-border business-services decision · source · article URL withheld · Verified on 2026-11-22.

S47: ANSPDCP · ANSPDCP hospitality application decision · source · article URL withheld · Verified on 2026-11-22.

S48: ANSPDCP · ANSPDCP manufacturing access-control decision · source · article URL withheld · Verified on 2026-11-22.

S49: ANSPDCP · ANSPDCP consumer-products security decision · source · article URL withheld · Verified on 2026-11-22.

S50: ANSPDCP · ANSPDCP customer-services security decision · source · article URL withheld · Verified on 2026-11-22.

S51: ANSPDCP · ANSPDCP retail administrator-account decision · source · article URL withheld · Verified on 2026-11-22.

S52: Official or attributed public source · Police cross-border tax-platform fraud update · source · article URL withheld · Verified on 2026-11-22.

S53: Official or attributed public source · DIICOT social-account phishing investigation reported · source · Verified on 2026-11-22.

S54: Official or attributed public source · DNSC courier-themed fraud warning reported · source · Verified on 2026-11-22.

S55: Official or attributed public source · DNSC institutional-impersonation phishing warning reported · source · Verified on 2026-11-22.

S56: Official or attributed public source · DNSC trademark-fee phishing warning reported · source · Verified on 2026-11-22.

S57: ASF · ASF investor alert register · source · Verified on 2026-11-22.

S58: ANSPDCP · ANSPDCP complete news index · source · Verified on 2026-11-22.

S59: Official or attributed public source · BNR deputy governor on cyber stress and liquidity transmission · source · Verified on 2026-11-22.

S60: ASF · ASF official DORA presentation · source · Verified on 2026-11-22.

S61: Official or attributed public source · Official regional authority announces procurement-application restoration · source · Verified on 2026-11-22.

S62: Official or attributed public source · Foreign ministry official DDoS statement · source · Verified on 2026-11-22.

S63: Official or attributed public source · DNSC possible refrigeration-controller incident via national radio · source · Verified on 2026-11-22.

S64: Official or attributed public source · Municipal fiscal website malware statement reported nationally · source · article URL withheld · Verified on 2026-11-22.

S65: Official or attributed public source · Waste-services operator customer-portal incident notice · Source URL withheld to protect the organisation · Verified on 2026-11-22.

S66: Official or attributed public source · Waste-services operator restores portal · Source URL withheld to protect the organisation · Verified on 2026-11-22.

S67: ASF · Delegated Regulation 2025/301, official ASF mirror · source · Verified on 2026-11-23.

S68: Official or attributed public source · Original reporting on publicly exposed surveillance images · source · article URL withheld · Verified on 2026-11-22.

S69: Official or attributed public source · Childcare authority response to exposure inquiry · source · article URL withheld · Verified on 2026-11-22.

S71: Official or attributed public source · Spanish interior ministry confirms LeakBase operation and Romanian participation · source · Verified on 2026-11-22.

S72: Official or attributed public source · Paris prosecutor confirms SocksEscort operation and Romanian participation · source · Verified on 2026-11-22.

S73: Reuters via Investing.com · Reuters investigation of reported military-email access, syndicated body · source · Article URL withheld; Reuters byline syndication read; original domain unavailable · Verified on 2026-11-22.

S74: Official or attributed public source · Military-email response to reporting · source · Article URL withheld; official response quoted by national radio · Verified on 2026-11-22.

S75: Official or attributed public source · Media-published copy of DNSC preliminary annex dated 22 July 2026 · source. Preliminary findings; publication lacked DNSC authorisation; not a final report (S115) · Publication status verified on 2026-11-23.

S76: Official or attributed public source · Land-administration initial official incident statement · source · Verified on 2026-11-22.

S77: Official or attributed public source · DNSC bank-ransomware statement quoted in original financial reporting · source · article URL withheld · Verified on 2026-11-22.

S78: Official or attributed public source · Independent national coverage of bank-ransomware response · source · article URL withheld · Verified on 2026-11-22.

S79: Official or attributed public source · Faculty website incident confirmed in dean interview · source · article URL withheld · Verified on 2026-11-22.

S80: Official or attributed public source · Investment-services firm update confirms account-opening database access · source · Verified on 2026-11-23.

S81: Official or attributed public source · DNSC explains abnormal temperatures in six Romanian stores · source · Verified on 2026-11-22.

S82: Official or attributed public source · Bookseller customer notice on security disruption · source · Verified on 2026-11-22.

S83: Official or attributed public source · Bookseller reopening confirmed in customer email · source · Verified on 2026-11-22.

S84: Official or attributed public source · University management statement on infrastructure disruption · source · Verified on 2026-11-22.

S85: Official or attributed public source · Government response to personal identifiers in published documents · source · Verified on 2026-11-22.

S86: Official or attributed public source · Retail group update on malicious network activity and restoration · Source URL withheld to protect the organisation · Verified on 2026-11-22.

S87: Official or attributed public source · Municipal fiscal director discloses repeated attacks to council · source · Verified on 2026-11-22.

S88: Official or attributed public source · Police preliminary checks after municipal website outages · source · Verified on 2026-11-22.

S89: Official or attributed public source · Municipal statement on unavailable online payments · source · Verified on 2026-11-22.

S90: Official or attributed public source · Municipality announces planned payment-system replacement · Source URL withheld to protect the organisation · Verified on 2026-11-22.

S91: Official or attributed public source · Tax authority warns of inspector-impersonation calls · source · Verified on 2026-11-22.

S92: Official or attributed public source · Regional tax authority repeats vishing warning · source · Verified on 2026-11-22.

S93: Official or attributed public source · Postal regulator warns of parcel and WhatsApp lures · source · Verified on 2026-11-22.

S95: Official or attributed public source · Police denies cyberattack explanation for radar withdrawals · source · Verified on 2026-11-22.

S96: Official or attributed public source · Independent report on investment-services onboarding interruption · source · Verified on 2026-11-23.

S97: Official or attributed public source · Original local report reproduces university statement · source · Verified on 2026-11-22.

S98: Official or attributed public source · Transport-sector official account of repeated website attacks · source · Verified on 2026-11-22.

S99: Official or attributed public source · Fleet-platform founder describes earlier DDoS and response · source · Verified on 2026-11-22.

S100: Official or attributed public source · Supplier case study on fleet-platform availability incident · Source URL withheld to protect the organisation · Verified on 2026-11-22.

S101: Official or attributed public source · Digitalisation authority warns of cloned payment-platform SMS · source · Verified on 2026-11-22.

S102: Official or attributed public source · Energy supplier warns about invoice phishing · Source URL withheld to protect the organisation · Verified on 2026-11-22.

S103: Official or attributed public source · Newsroom receives bank-impersonation emails · source · Verified on 2026-11-22.

S104: Official or attributed public source · Reader-submitted refund lure targeting online shoppers · source · Verified on 2026-11-22.

S106: Official or attributed public source · Annual-report account of defence-manufacturer payment diversion · source · Verified on 2026-11-22.

S111: Official or attributed public source · NVD record for the Office security-feature bypass · source · Verified on 2026-11-22.

S112: Official or attributed public source · Microsoft Office 2016 MSI security update KB5002713 · source · Edition-specific update; not for Click-to-Run · Verified on 2026-11-23.

S113: Official or attributed public source · CERT-EU Cyber Brief for February 2026, published 2 March · source · Neusploit summary relays Zscaler research · Verified on 2026-11-22.

S114: Official or attributed public source · Insikt Group research on BlueDelta and HOOKEDGE · source · Source attribution and activity-period limits retained · Verified on 2026-11-23.

S115: DNSC via AGERPRES · DNSC clarification on preliminary annex publication, 2 September 2026 · source · Preliminary annex, not an authorised final report · Verified on 2026-11-23.

S116: CVE Program / Microsoft · CVE record for Office affected products and version boundaries · source · Verified on 2026-11-23.

S117: Microsoft · Office security releases including the CVE-2026-21509 fix · source · Verified on 2026-11-23.

S118: Microsoft · MSRC January 2026 security guidance for CVE-2026-21509 · source · Verified on 2026-11-23.

S119: Microsoft · Update history for Office 2016 C2R and Office 2019 · source · Verified on 2026-11-23.

Appendix D. Glossary

Term	Plain meaning
Access advertisement	A claim that an account or service can be accessed; it does not establish working access
Credential record	A record associated with authentication information; not necessarily a current account or valid password
Device association	An observed relationship between a device and a domain; ownership and current infection need validation
Combolist	A collection of account identifiers and passwords, potentially drawn from several older sources
CRM	Customer relationship management: systems holding customer interactions and related business records
CSIRT	A team responsible for coordinating responses to cybersecurity incidents
DDoS	Distributed denial of service: activity intended to make a service unavailable through traffic or resource pressure
DKIM	DomainKeys Identified Mail: domain-based signing of email
DMARC	Domain-based email authentication alignment, reporting and requested message treatment [S18]
DNSSEC	DNS security extensions that support authentication of DNS data; a delegation observation is not full end-to-end validation
DORA	The EU digital operational resilience framework for the financial sector [S60]
HSTS	HTTP Strict Transport Security: a web policy asking browsers to use HTTPS
ICT	Information and communication technology
KYC	Know your customer: identity and related customer-verification processes
MFA	Multifactor authentication: authentication using more than one distinct factor
NIS2	The EU cybersecurity directive reflected in national implementation frameworks
Phishing	Deceptive communication intended to obtain information, access or an unauthorised action
Ransomware listing	A criminal publication naming an alleged victim; separate from confirmation of encryption or theft

Term	Plain meaning
RTO	Recovery time objective: the maximum interruption the business plan allows for a service
SCADA	Supervisory control and data acquisition: systems used to monitor and control industrial processes
SOHO router	Small-office or home-office network router [S10]
SPF	Sender Policy Framework: a domain's published authorisation for sending hosts
TLS	Transport Layer Security: protection for a communication connection; not proof of endpoint security
Vishing	Voice-based phishing using a telephone or similar voice channel

Appendix E. Further official findings and campaign context

These additional entries preserve distinct control lessons. The dates are publication dates. An enforcement notice can describe an older incident or conduct, and some findings establish no external attacker.

Published	Source finding	Classification boundary	Defensive implication
13 January	Hospitality application incident; investigation concluded in 2025 [S47]	Publication does not establish a 2026 attack	Review application access and processor assurance
19 January	Employee medical spreadsheet distributed internally with inadequate access protection [S48]	No external attack or 2026 event date established	Restrict sensitive staff-data circulation
4 February	Authentication and account-reset weakness exposed an employee directory across EU users [S46]	Investigation concluded in December 2025	Test account recovery and population scope
25 March	Attack on a supplier-administered automotive application; records published [S43]	No 2026 attack date established by publication	Verify supplier safeguards and evidence access
3 April	Professional-services IT attack affected confidentiality and availability [S44]	No common incident established with similarly worded decisions	Give access monitoring an owner
30 April	Industrial-services attack exposed staff and correspondent records [S45]	Attack timing and a link to other cases unresolved	Inspect data flows and access records
18 June	Mobile-account validation weakness exposed another person's invoices and delivery data [S42]	Authorisation failure; no external attacker established	Test record-level authorisation and notification
28 August	Consumer-products attack affected identity and contact information [S49]	Attack date not stated	Verify access monitoring and protected logs
2 October	Customer-services security finding includes personnel, payroll and banking information [S50]	Attack date not stated	Include staff and supplier records in scope

Published	Source finding	Classification boundary	Defensive implication
30 October	Retail administrator-account attack exposed internal identifiers and authentication information [S51]	Attack date not stated	Protect administrative access and inspect sessions
November	Bank worker exceeded authorised access to customer information [S41]	Insider-access finding, not a common external campaign	Review business purpose and access exceptions

The ANSPDCP news index includes other privacy, procedural and institutional notices. They are not all cyber incidents. The index's 54 notices must not become a national attack count. [S58]

In March, official foreign law-enforcement accounts identify Romanian participation in operations concerning LeakBase and SocksEscort. These are international enforcement observations. They do not establish Romanian victim or device totals, and the report does not combine different global counts. [S71][S72]

A 4 May fleet-service disclosure describes DDoS in autumn 2025. The supplier said a distinct component remained operational. This is historical disclosure and service-boundary context, not a fresh 2026 attack or a count of affected vehicles. [S99][S100]

An August account quoting DNSC's 2025 annual report describes a manufacturer's email and payment-diversion incident. It belongs to the earlier year. It reinforces independent verification of changed payment instructions without entering the current-year occurrence count. [S106]

About this report

Odin by Brandefense prepared this country research package with AI assistance. It combines retained own-data observations with source-qualified public accounts. The English edition is the master; the Romanian edition carries an AI translation notice and preserves the numbers, evidence IDs and directives.

The report belongs to Brandefense Country Report · Romania 2026. It does not estimate national attack prevalence, authenticate criminal advertisements or independently attribute state activity. Its purpose is to connect defensible evidence to accountable security decisions.

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