BRANDEFENSE COUNTRY REPORT · ITALY 2026

Brandefense Italy Cyber Threat Landscape Report 2026

Service continuity, identity markets and evidence behind the claims

Odin by Brandefense
Research window: 22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · : 23 November 2026

132 of 250
candidate portfolio entries associated with credential offers when checked

802,371
Italy-tagged posts counted by publication time, rather than attacks

286
Italy-associated ransomware listing records in the reporting window

20
actions with owners and evidence of completion

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Italy's digital and operational context	10
03	National exposure: candidate portfolio entries	14
04	What we see on the dark web	19
05	Targeting examples and cases by sector	33
06	Hacktivism, DDoS and recent activity	46
07	Threat actors and evidence of relationships	54
08	The fraud economy	66
09	Banking and finance deep dive	71
10	Regulatory and national response	75
11	Outlook	80
12	Action plan	84
A	Appendix A. Sources, scope and confidence	91
B	Appendix B. Evidence register	94
C	Appendix C. Sources	96
D	Appendix D. Glossary	100
	About this report	102

Board and executives	01 05 11 12
CISO and security leads	03 04 05 10 12
SOC and intelligence	04 06 07 B
Fraud and customer protection	08 09 12
Legal and communications	05 06 10 12

About this edition

Prepared with AI assistance by Odin by Brandefense. Observations extend to the collection snapshot on 22 November, rather than the end of that day.

Italy's evidence calls for separate responses to interrupted services, identity-data offers and claims that have not been independently established.

802,371

Italy-tagged posts counted, rather than attacks

132 of 250

candidate portfolio entries associated with credential offers when checked

57/100

national Atlas headline for the selected portfolio

286

Italy-associated ransomware listing records, rather than confirmed intrusions

Contents and reading routes

Chapter	Question	Main reader
1 Executive summary	What should leaders decide first?	Board and CISO
2 Context	Which features of Italy's services shape the risk?	CISO and continuity
3 National exposure	What does the selected universe establish?	Identity and infrastructure
4 Dark web	What was actually advertised about Italy?	Threat intelligence
5 Sector cases	What happened and what should change?	Service owners
6 Hacktivism and DDoS	What did claimants say and authorities confirm?	SOC and communications
7 Threat actors	Which associations have supporting evidence?	Threat intelligence
8 Fraud economy	How do identity and payment workflows become targets?	Fraud and finance
9 Banking	Which customer and employee risks need separate owners?	Banking and treasury
10 Regulation	Which obligations apply to each entity?	Legal and response
11 Outlook	Which signals should change the plan?	Security leadership
12 Action plan	Who does what, and how is completion demonstrated?	All functions

Read Chapters 1, 5 and 12 for management decisions. Read Chapters 3, 4, 6 and 7 for operational evidence. Read Chapters 8-10 for fraud, banking and reporting obligations. Appendix A explains the populations and limits; Appendix B connects stable evidence references to the text.

Observation means a retained post, a measured public control or a source's published statement. **Claim** means an assertion by an actor or seller. **Assessment** means our interpretation, with the alternative and the evidence needed to change it. These labels apply to individual propositions, including within one incident.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What does Italy's evidence establish, and which decisions should leaders make first?

4

decisions linking continuity, identity, payments and incident reporting

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Italy's evidence combines confirmed service disruption, identity-data access and criminal claims with different levels of support. A university documented ransomware recovery; a recent retail disclosure confirmed contact-data access without establishing payment-data theft. Official Olympic-period reporting distinguishes attempted DDoS disruption from actual service effects. Treat those populations separately. Validate identity signals, test supplier-dependent recovery, confirm payment changes through known channels, and rehearse the reporting decision before the next incident.

1. Post volume and incident evidence answer different questions. The source counts 802,371 Italy-tagged posts. January and February contain 91.9% of that total. A separate retained corpus contains 16,613 distinct posts, including 839 Italy-tagged forum posts. The retained corpus is partial and nonrandom. These populations do not establish national attack volume or a criminal-family prevalence rate. [S1]

2. Extortion publications are broad, but individual assertions remain unverified. Ransompedia records 286 Italy-associated listing records across 59 group-name values. Qilin, The Gentlemen and Lockbit5 account for 95 records, or 33.2%. A listing is a claim; different records can name the same organisation, and unpublished cases are absent. [S2]

3. Confirmed interruption makes recovery a service-level decision. Sapienza's ransomware notice documents affected systems and recovery, while preserving unresolved information-exposure boundaries. Other source-backed cases describe supplier and healthcare interruption. A restored server is insufficient evidence that a business or clinical workflow is ready. Test the actual service. [S5][S25][S27]

4. Recent contact-data access needs precise customer advice. Unicoop Firenze confirmed access to some contact information while saying services continued. Its security information says payment-card data and passwords were not involved. The response should address credible impersonation, without converting contact-data access into a claim of banking-account access. [S7][S8]

5. Current credential offers need validation across the selected portfolio. When checked, credential offers were associated with 132 candidate entries in the 250-entry portfolio. The national Atlas headline is 57 out of 100. At least 759,724 device associations and 113,259,485 historical credential-record associations overlap. They do not establish unique users or confirmed intrusions. Passive-control measurements remain unavailable. [S3]

Four decisions for leaders

1. **Test the service through its suppliers.** Require a restoration exercise for one important service and its identity, hosting and communications dependencies. Record business usability as the completion criterion. The university, cloud and healthcare cases show why service recovery deserves a separate evidence trail (§5).
2. **Include sessions and recovery in identity response.** Route organisation-specific credentials and session evidence to the identity team. Check ownership, current validity, protection and earlier remediation before disruptive action. Revoke affected sessions when supported, and verify that recovery cannot recreate the access (§§3-4 and 12).
3. **Verify payment authority outside the requesting channel.** A plausible sender, familiar document, real conversation or convincing voice does not establish authority. Confirm new payees and changed instructions through independently known details. Test an urgent, confidential executive request against that process (§§8-9).
4. **Prepare reporting and communications records.** Legal needs an entity-specific reporting matrix, including when awareness starts each clock. Communications needs a statement separating claim, verified effect and action. Exercise both against a supplier outage accompanied by a data-sale claim (§§6, 10 and 12).

The year in numbers

802,371

Italy-tagged posts counted by publication time through the snapshot

WHAT IT IS NOT

Not attacks, victims or completed trades

16,613

Distinct retained posts in the partial combined corpus

WHAT IT IS NOT

Not a representative share of national cybercrime

839

Retained Italy-tagged forum posts

WHAT IT IS NOT

Not the entire country-tag count population

286

Italy-associated ransomware listing records

WHAT IT IS NOT

Not independently verified intrusions

270

Distinct victim-name values in those listing records

WHAT IT IS NOT

Not validated unique organisations or incidents

250

Candidate entries in the selected portfolio

WHAT IT IS NOT

Not validated independent organisations

42

Distinct Italy-associated payment cards in clear text in retained posts

WHAT IT IS NOT

Narrow post view, not theft prevalence or fraud loss (§8.6)

18

Case cards: underground assertions, source cases, campaigns and an exclusion

WHAT IT IS NOT

Not a national incident total

The first three rows use [S1], the listing rows use [S2], the candidate row uses [S3], and the narrow card observation uses [S4].

What these numbers cannot answer. Posts, listings, campaigns, affected-person estimates and notifications measure different things. They cannot be combined into a national attack total. More reports can reflect wider visibility as well as changing activity. The case studies support decisions without pretending those populations are interchangeable.

KEY TAKEAWAYS

01

Confirmed interruption and advertised data need different evidence and owners.

02

Identity response must cover sessions, recovery and payment authority.

03

Judge readiness through tested service outcomes and documented reporting decisions.

Report map

Twelve chapters, five reader paths. Start with your role's question, then use the case and evidence references to check the proposition supporting each decision.

Board and executives	Which service, identity and payment decisions need funding?	01 05 11 12
CISO and security leads	Which evidence changes our priorities?	03 04 05 10 12
SOC and intelligence	Is this a claim, a relay, or confirmed operational harm?	04 06 07 B
Fraud and customer protection	What can an attacker do with contact and identity data?	08 09 12
Legal and communications	Which facts can we state and which clocks apply?	05 06 10 12

01 Executive summary
Strongest findings and four decisions

02 Italy's digital and operational context
Digital services, suppliers and reporting visibility

03 National exposure: candidate portfolio entries
Selected-portfolio exposure signals

04 What we see on the dark web
Scope and meaning of underground observations

05 Targeting examples and cases by sector
Source-backed cases and a response by sector

06 Hacktivism, DDoS and recent activity
Disruption claims, official accounts and recent activity

07 Threat actors and evidence of relationships
Actor evidence and relationship limits

08 The fraud economy
Identity collection, account abuse and payment fraud

09 Banking and finance deep dive
Banking decisions across customer and employee populations

10 Regulatory and national response
NIS2, public-sector duties, GDPR and DORA

11 Outlook
Conditional scenarios and assessment changes

12 Action plan
Owned actions and completion evidence

CHAPTER 02

Italy's digital and operational context

02

THIS CHAPTER ANSWERS

Which characteristics of Italy's services explain the priorities in this report?

3

connected decisions: identity, continuity and supplier dependency

2.1 Follow the service behind the headline 11

2.2 Shared suppliers can create shared interruption 11

2.3 Important events attract visible claims 12

2.4 Reporting changes what authorities can see 12

2.5 Keep old incidents visible without redating them 12

CHAPTER 02

Italy's digital and operational context

IN SHORT

Citizens depend on digital public services, organisations depend on shared suppliers, and important events create visible availability targets. Italy's wider reporting framework also changes what authorities observe. These features explain why website claims, supplier outages and identity-data offers require different decisions. Map the services and approval processes that your organisation cannot operate without.

2.1 Follow the service behind the headline

The cases span education, infrastructure suppliers, healthcare, culture, retail and administration. They do not establish equal incident rates across sectors. They show different paths from a technical event to a service consequence. Unavailable student systems, encrypted supplier archives and contact-data access create different operational work. [S5][S24][S27][S7]

A service owner should first establish which function stopped or which information was accessed. The next question is who can verify it. A website check cannot establish the condition of an internal booking platform. Continued trading cannot establish that no personal information was accessed. Both observations can be accurate when they concern different assets.

The useful defensive unit is a business service with named dependencies. Identify its identity provider, hosting arrangement, support access, communications route and recovery source. Assign an owner who can judge business usability. This is a planning recommendation derived from the cases, rather than a national measurement of supplier concentration.

2.2 Shared suppliers can create shared interruption

ACN's August report describes encryption in a shared area at an ICT provider, affecting customers using it. The report associates the case with Titan. It does not publish a customer total or establish that every service was affected. The observation supports dependency-specific investigation, rather than a conclusion about all cloud providers. [S13]

Returning storage or servers to availability does not necessarily restore an application, authentication, transactions or reconciled records. Procurement and continuity teams should agree how those conditions will be tested. A supplier's update should allow each customer to determine whether its own service is affected.

Ask whether production access, backup administration and recovery approval depend on the same identities or control plane. The report does not assert that those arrangements caused a particular case. They are questions for an authorised design review and restoration exercise.

2.3 Important events attract visible claims

The Olympic period generated DDoS claims against event-related and diplomatic digital services. ACN distinguishes website effects from the event's regular operation. Its official account says no cyber incident affected regular competitions or associated essential services. That does not make every attempted disruption fictitious. It identifies the effect that was, and was not, observed. [S10]

Ticketing, accommodation, transport information, public communications and support services require separate checks. An organiser should know which supplier confirms each function and which channel remains usable when the main website is unavailable. A claimed list of websites cannot replace those service checks.

Political themes belong to the claimants or sources invoking them. The authors take no position on government decisions, migration, Russia/Ukraine, Israel/Gaza or other political disputes. Motive statements are relevant only when they help assess a claim, timing or communications. They do not establish technical responsibility.

2.4 Reporting changes what authorities can see

ACN's February account explains that operational NIS2 notification obligations widened visibility from January 2026. It cautions that increased visibility did not correspond to an equivalent increase in observed incident impacts. That statement concerns ACN's reporting population and period. It does not establish that underlying national threats rose or fell. [S10] For January–June 2026, ACN reports 2,171 cyber events, up 47% from the same period in 2025, and 1,072 incidents with confirmed impact. ACN notes that expanded NIS2 reporting visibility accounts for much of this rise, and these official totals remain separate from Brandefense post and listing counts. [S75]

The October operational summary reports 691 events and 394 incidents with confirmed impact. The headline figures are corroborated by ANSA's 20 November account. It also revises earlier observations. A monthly chart must use an identified publication vintage, because later investigation can change an earlier classification. First-publication and revised values should not silently become one series. [S49][S65]

For a board, more notifications can mean that the process is finding previously unseen events. To understand harm, ask about duration, affected services, information categories, recovery and recurrence. Count those outcomes separately from alerts and reports.

2.5 Keep old incidents visible without redating them

Some 2026 publications concern earlier activity. June rail-customer notices concern late-2025 activity. Several Garante decisions concern 2024 or 2025 incidents. They matter for notification, fraud and control lessons, but they are not fresh 2026 intrusions. [S45][S40][S41][S42]

The report distinguishes occurrence, claim, disclosure, follow-up and decision dates. A later recovery statement updates the same case. A criminal repost does not establish a new extraction. A regulator's decision is an enforcement observation, rather than evidence that the attack occurred on the decision date.

KEY TAKEAWAYS

01

Business services and dependencies are the useful unit for continuity decisions.

02

Event-related website claims do not establish interruption of the event.

03

Publication and reporting dates must remain separate from occurrence.

CHAPTER 03

National exposure: candidate portfolio entries

THIS CHAPTER ANSWERS

Which exposure signals in the selected portfolio need validation first?

132 of 250

candidate portfolio entries associated with credential offers when checked

3.1 Universe card 15

3.2 Sector signal counts 16

3.3 Devices, documents and lookalikes need different owners 17

3.4 Passive-control coverage 18

3.5 Turn signals into validation tasks 18

CHAPTER 03

National exposure: candidate portfolio entries

IN SHORT

When checked, credential offers were associated with 132 candidate entries in the 250-entry portfolio. The national Atlas headline is 57 out of 100. The portfolio records at least 759,724 device associations and 113,259,485 historical credential-record associations. These overlapping observations do not establish unique people or confirmed intrusions. Validate current listings, investigate employee-associated devices and route other account evidence to the appropriate service owner.

3.1 Universe card

Item	Definition
Population	250 candidate portfolio entries across twelve sectors
Selection	Purposive selection for public-service, economic or sector relevance; not a revenue ranking
Unit	One candidate primary domain per portfolio entry; ownership and organisational independence require validation
Exposure snapshot	21-22 November 2026; historical records are not limited to the report year
Initial observation	228 of 250 candidate domains returned public DNS data on 22 November 2026
Interpretation	Related organisations and shared services can have overlapping digital footprints
National Atlas headline	57 out of 100 for this selected portfolio
Passive controls	No usable DMARC, SPF, DKIM, DNSSEC, TLS or web-header assessment published
Generalisation	The list does not estimate national or sector prevalence

Brandefense Atlas provides the exposure rating; this report publishes the national headline only. The dated signal counts below describe the selected domains, rather than validated corporate boundaries. A higher rating describes greater observed exposure on the 0-100 scale. It does not quantify the probability of an attack. Domain associations do not establish users' nationality or location. [S3]

3.2 Sector signal counts

The table separates device associations, historical credential records and candidate entries associated with current credential offers. Its populations overlap. Device figures are minimum observed totals; a device or credential record can recur across related domains. No sector rating is published. [S3]

Sector	Candidate entries	Devices	Credentials	Entries associated with offers
Government	40	136,907	578,774	17
Banking and finance	25	83,725	1,662,877	14
Education	30	90,020	3,505,654	21
Healthcare	20	5,147	152,478	4
Insurance	10	13,037	109,972	5
Energy and utilities	20	53,735	308,222	9
Transport and logistics	20	56,248	157,468	13
Manufacturing and industry	25	24,414	431,897	9
Retail and consumer	20	64,048	120,737	14
Telecom and digital services	10	139,177	105,986,323	7
Media and sport	15	87,068	220,547	10
Tourism and hospitality	15	6,198	24,536	9
Total	**250**	**759,724**	**113,259,485**	**132**

Current credential offers are associated with 132 candidate portfolio entries; sector counts describe separate exposure signals

Columns use separate scales. Current credential offers are shown in coral as entries with offers / selected candidate entries; other cells show counts.

	Device associations (at least)	Historical credential records	Current credential offers
Government	136,907	578,774	17/40
Banking and finance	83,725	1,662,877	14/25
Education	90,020	3,505,654	21/30
Healthcare	5,147	152,478	4/20
Insurance	13,037	109,972	5/10
Energy and utilities	53,735	308,222	9/20
Transport and logistics	56,248	157,468	13/20
Manufacturing and industry	24,414	431,897	9/25
Retail and consumer	64,048	120,737	14/20
Telecom and digital services	139,177	105,986,323	7/10
Media and sport	87,068	220,547	10/15
Tourism and hospitality	6,198	24,536	9/15

Source: exposure associations for 250 selected candidate portfolio entries, 21-22 November 2026. Device figures are minimum totals; historical credential records overlap and do not establish unique accounts or confirmed intrusions. Passive controls are unavailable [S3].

The historical credential total comprises 29,686,862 breach-database records, 8,899,179 stealer-log records and 74,673,444 combolist records. These are record associations, not unique accounts, newly stolen passwords or a count of 2026 intrusions. Ownership, freshness and previous remediation require validation. [S3]

Stealer logs contain login details captured by information-stealing malware on infected devices. Combolists compile email-address or username and password pairs. These terms describe record types, not when credentials were stolen or whether they still work. [S69][S70]

3.3 Devices, documents and lookalikes need different owners

Of at least 759,724 device associations, 75,253 are employee-associated. The remaining 684,471 are outside that classification; they can concern customers, students or other users. Their ownership and current state are not established. A domain association does not identify an intrusion into the organisation's infrastructure. [S3]

The snapshot also records 2,976 exposed-document associations and 40,409 lookalike-domain observations. These are separate signals, not additional devices or verified phishing sites. A document association does not establish who published it, whether it remains sensitive or whether an unauthorised disclosure occurred. [S3]

A current listing describes a credential offer requiring account-level validation. It does not establish a completed sale, valid access or a confirmed internal intrusion. Send employee evidence to identity and endpoint teams, other account evidence to the relevant service owner, and document evidence to its information owner.

3.4 Passive-control coverage

The initial DNS observation covers 228 of the 250 candidate domains. It is not a hygiene assessment. No usable passive-control measurement is available in this edition, so no DMARC, SPF, DKIM, DNSSEC, TLS or web-header percentage is published. Missing measurements do not establish missing controls. [S3]

3.5 Turn signals into validation tasks

Signal	First validation	Completion evidence
Current credential offer	Establish account ownership and current relevance	Dated identity disposition
Employee-device association	Establish endpoint ownership, sessions and prior response	Endpoint and identity findings
Other device association	Identify the service relationship and relevant fraud evidence	Service or fraud disposition
Exposed-document association	Establish provenance, sensitivity and disclosure authority	Information-owner decision
Lookalike-domain observation	Establish ownership, content and impersonation evidence	Domain-investigation disposition

A national rating does not make these tasks interchangeable. Parent, subsidiary and provider overlap limits the independence of portfolio totals. Retain observation dates and account-level evidence before choosing disruptive remediation. Confirm the candidate domain and service before attributing any observation to a legal entity.

KEY TAKEAWAYS

01

Validate the credential offers associated with 132 of 250 candidate portfolio entries.

02

Device and historical credential associations are overlapping records, not confirmed intrusions.

03

Assign identity, service, information and domain evidence to the owners who can establish its current relevance.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do the retained posts establish about Italy-related underground advertising?

802,371

Italy-tagged posts counted by publication time, rather than attacks

4.1 Universe card 20
4.2 Monthly concentration needs explanation before interpretation 21
4.3 What the examples actually offer 22
4.4 Six own-source case cards 23
4.5 Recent and historical assertions require their own dates 29
4.6 Additional access and infrastructure claims 29
4.7 Turn an advertisement into a bounded validation task 31

CHAPTER 04

What we see on the dark web

IN SHORT

Italy-tagged volume is concentrated early in the year, but counts alone cannot explain the activity behind it. Retained forum examples show demand for data, identity-document offers, mail-access advertising and sector-labelled files. Several contain locked content or explicit historical dates. They establish advertisements and assertions, rather than valid access or fresh intrusion. Validate provenance, age and relevance before deciding that an organisation needs incident response.

4.1 Universe card

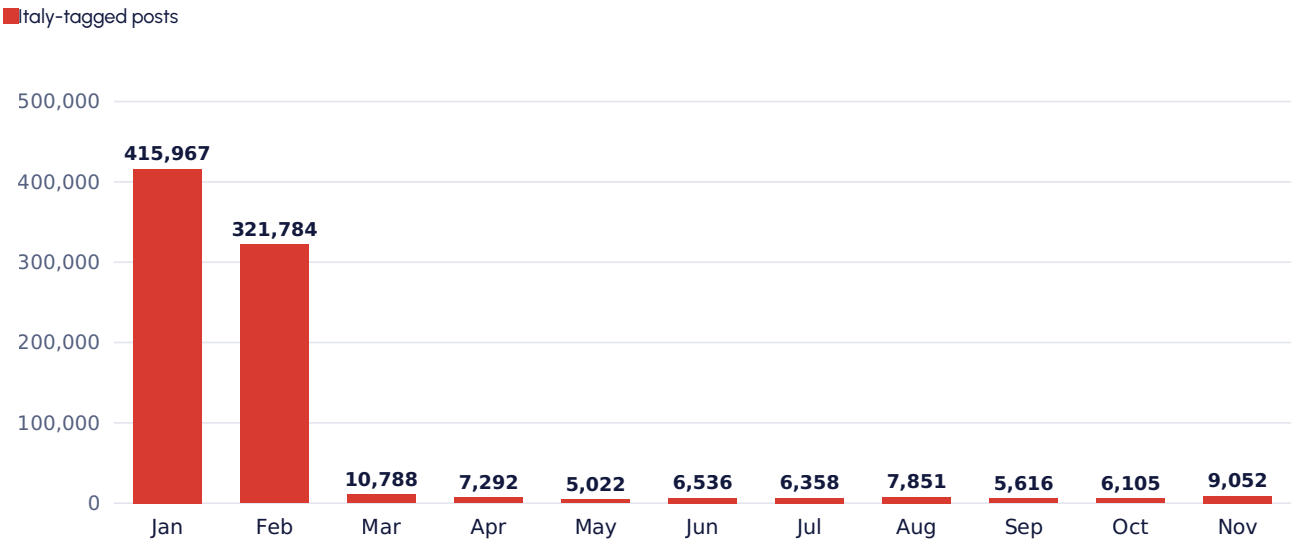
Item	Definition
Source	Underground and messaging observations held by Odin by Brandefense
Window	Publication time from 1 January to the 22 November collection snapshot
Country count	802,371 Italy-tagged posts; a country tag does not establish targeting
Retained material	16,613 distinct posts in a partial combined corpus, including 839 Italy-tagged forum posts (of which 195 are dated 9-22 November 2026)
Evidence cards	Seventeen redacted post excerpts with stable B references
Unit	Posts and advertisements, rather than verified intrusions, sales or unique people
Main limit	The retained text does not establish the contents of locked or advertised files

The source is [S1]. The count population and retained-text population are different. The report does not treat the latter as a representative sample of every tagged post or assume that forum themes explain messaging traffic. A selected excerpt illustrates a proposition, rather than its national frequency.

4.2 Monthly concentration needs explanation before interpretation

Month	Tagged posts	Reading
January	415,967	Publication count
February	321,784	Publication count
March	10,788	Publication count
April	7,292	Publication count
May	5,022	Publication count
June	6,536	Publication count
July	6,358	Publication count
August	7,851	Publication count
September	5,616	Publication count
October	6,105	Publication count
November	9,052	Partial period to collection snapshot
Total	**802,371**	**Posts, rather than attacks**

January and February contain most tagged posts; the series does not measure attacks



Source: Brandefense Italy-tagged publication counts, 1 January–22 November 2026; November ends at the collection snapshot. Tagged posts and the partial retained corpus are separate populations, not attacks [S1].

January and February contain 737,751 posts, or 91.9% of the total. That arithmetic does not identify a bot share, a successful-attack wave or an underlying threat trend. Repeated advertising, coverage differences and actual campaign activity are possible explanations requiring further evidence. Do not select one from volume alone. [S1]

The later months also cannot establish a reduction in national harm. Incidents can occur without underground publication, while advertising can continue after the underlying event. November is partial. The chart is useful for understanding the source's observed volume, rather than comparing national outcomes across unequal periods.

4.3 What the examples actually offer

Observed theme	Cards	Established proposition	Unresolved
Demand for Italy-labelled data	B01 · B03	Posters sought data and included Italy	Purchase, origin and validity
Financial-account advertising	B02	An advertisement listed banks across countries	Existence, ownership and use of accounts
Identity-document advertising	B04	Italy appeared in a multi-country offer	Authenticity and verification success
Bank-labelled logs	B05	A bot advertised a file under a banking label	Contents and service-side intrusion
Mail access	B06	An access advertisement had locked content	Current validity and account owners
Customer-name claim	B07	Uploader acknowledged poor data quality	Distinct people, source and currency
Healthcare-labelled files	B08	A mixed-format collection was associated with a provider	Authenticity, medical content and occurrence date
Retail database	B09	Seller advertised a dataset and samples	Origin, age and geographical composition
Recent media claim	B10	November post advertised locked material	Content, authenticity and fresh intrusion
Historical website data	B11	Post labelled the database as 2016	Authenticity and present relevance
Remote-access offer	B12	Separate advertisement claimed Italy-related business-service access	Current validity and control of access

A sector label supplies a validation question. It is not enough to identify an affected business process or declare data extraction. Locked content is a material limit because the advertised file cannot be assessed from its title. A sample offer is also an assertion until authorised evidence establishes what the sample contains.

4.4 Six own-source case cards

A

CASE A

Demand names Italy without establishing a victim

Evidence card B01 | 10 Feb 2026 | Forum | Cross-sector

Unverified advertisement

OBSERVATION	A February forum post requested French and Italian data for selected mail domains and asked for testing before purchase. A January solicitation separately included Italy among several markets. [S1]
ESTABLISHED	The retained posts establish demand and the requested geographical or service labels. They do not establish a purchase or a file's origin.
ALTERNATIVES	A buyer could seek older lists, user-side credentials, aggregated records or mislabelled material. No provider-side intrusion follows from the request.
RESPONSE	Compare the requested category with the organisation's identity and customer workflows. Escalate organisation-specific current evidence, rather than the country's appearance in a buyer's list.

Bottom line

Compare the requested category with the organisation's identity and customer workflows. Escalate organisation-specific current evidence, rather than the country's appearance in a buyer's list.

Evidence card B01 — 10 Feb 2026

kurkenluvsdh | Forum | Forum | English

ORIGINAL

Buying France + Italy Data [...] i ONLY need these domains [...] need tests before buy.

Held

A buyer requested data for selected Italian and French mail domains and asked to test it.

Not established

Any purchase, validity, source, or intrusion at a mail provider.

Evidence card B03 — 27 Jan 2026

exelo | Forum | Forum | English

ORIGINAL

[database solicitation removed] [...] IT ITALY [...]

Held

A forum persona sought databases and explicitly included Italy among several markets.

Not established

The origin, freshness, validity or later use of any data.

The request to test data is not evidence that testing happened or succeeded. This distinction matters when an alert converts a buyer's wish into a supposed available capability. Preserve the requested product and the outcome as different fields.

CASE B

B

Identity-document advertising includes Italy

Evidence card B04 | 19 Aug 2026 | Forum | Identity services

Unverified advertisement

OBSERVATION	An August advertisement listed Italy among countries in an identity-document offer. [S1]
ESTABLISHED	The post establishes a claimed product and intended verification use. It does not establish genuine documents, a completed sale or successful onboarding.
ALTERNATIVES	The material could be fabricated, obsolete, copied from another seller or genuine. The excerpt does not settle those alternatives.
RESPONSE	Test onboarding and recovery against plausible synthetic documents. Record the additional evidence required before a document alone can authorise an account or contact change.

Bottom line

Test onboarding and recovery against plausible synthetic documents. Record the additional evidence required before a document alone can authorise an account or contact change.

Evidence card B04 — 19 Aug 2026

Jaded | Forum | Forum | English

ORIGINAL

DIGITAL KYC Documents for your VERIFICATION NEEDS [...] Countries Listed Down Below: [...] Italy [...]

Held

An identity-document advertisement included Italy in a multi-country offer.

Not established

That documents were authentic, usable for verification, or actually sold.

The relevant defensive question is not whether the advertisement looks professional. It is which internal decision would accept the claimed material. That question remains useful even when authenticity is unresolved.

CASE C

C

A mail-access title hides the substantive content

Evidence card B06 | 20 Aug 2026 | Forum | Mail services

Unverified advertisement

OBSERVATION	An August forum post advertised Italian mail access, with substantive content locked. [S1]

ESTABLISHED	The advertisement exists. The report does not establish quantity, account ownership, current access or a provider intrusion.
ALTERNATIVES	A title can describe historical credentials, user-side data, copied advertising or active access. Locked content leaves the proposition unresolved.
RESPONSE	If organisation-specific evidence becomes available through authorised monitoring, validate the account, session state and previous remediation. Do not infer that an Italian mail provider was accessed.

Bottom line

If organisation-specific evidence becomes available through authorised monitoring, validate the account, session state and previous remediation. Do not infer that an Italian mail provider was accessed.

Evidence card B06 — 20 Aug 2026

MegaCloud | Forum | Forum | English

ORIGINAL

[quantity removed] Italy HQ MAIL Access [...] Content locked

Held
A forum post advertised Italian mail access; its substantive contents were locked.

Not established
The claimed quantity, access validity, account owners, or service-side compromise.

Evidence card B12 — 2 Apr 2026

Forum seller | Forum | Forum | English

ORIGINAL

country: Italy [...] access: RDWEB [...] price: [negotiation text removed]

Held
A forum seller advertised remote-web access associated with an Italian events-sector organisation.

Not established
That access worked, the organisation identity, entry route, data theft or a completed sale.

A credential and a session can support different response decisions. The advertisement alone establishes neither. Identity teams should receive the specific evidence and its limit, rather than a broad country-level compromise label.

CASE D

D

A bot's banking label does not identify extraction

Evidence card B05 | 4 Jun 2026 | Forum | Banking

Unverified advertisement

OBSERVATION	A June automated uploader advertised a file under a banking-log label. [S1]
ESTABLISHED	The label and publication are retained. No file contents, valid customer accounts or bank-system access are established by the excerpt.
ALTERNATIVES	A label could refer to user-side logs, an assembled list, older material or promotional misdescription. The source does not choose among them.

RESPONSE	Send any validated account-level evidence to the appropriate identity or fraud owner. Keep customer-device exposure separate from an allegation about banking infrastructure.

Bottom line

Send any validated account-level evidence to the appropriate identity or fraud owner. Keep customer-device exposure separate from an allegation about banking infrastructure.

Evidence card B05 — 4 Jun 2026

Forum bot · Forum · Forum · English

ORIGINAL

[bank label removed] Logs Txt Database [...] Content Type: Database Dump

Held
An automated forum uploader advertised a file under a banking-log label.

Not established
A breach of the bank, valid customer credentials, file provenance, or file contents.

Evidence card B02 — 18 Apr 2026

Jiskaa · Forum · Forum · English

ORIGINAL

ITALY · [bank names removed] [...]

Held
An advertisement listed Italian banks alongside banks, wallets and business accounts in other countries.

Not established
That accounts existed, belonged to the advertiser, or were used for fraud.

The adjacent account advertisement lists financial services in several countries. Its inclusion of Italian banks does not establish that the advertiser owned accounts or used them for fraud. These are different assertions even when they appear in the same market.

CASE E

E Retail data is advertised with samples

Evidence card B09 · 6 Aug 2026 · Forum · Retail

Unverified advertisement

OBSERVATION	An August seller advertised an Italy-labelled retail database and offered samples. [S1]
ESTABLISHED	The retained post establishes the advertisement. It does not establish the count, geographical composition, age, authenticity or completed sale.
ALTERNATIVES	The label could describe customers, leads, older records or material assembled outside the retailer. A claimed sample does not independently identify the source system.
RESPONSE	Assess provenance through authorised channels before matching an incident. Prepare customer-contact guidance if credible current information could support impersonation.

Bottom line

Assess provenance through authorised channels before matching an incident. Prepare customer-contact guidance if credible current information could support impersonation.

Evidence card B09	6 Aug 2026

wizard Forum Forum English

ORIGINAL

italian Database [retailer removed] [...] Total lines [volume removed] [...]

Held
A seller advertised an Italian-labelled retail database and offered samples.

Not established
The claimed count, geographical composition, data age, authenticity or completed sale.

Evidence card B07	28 Sep 2026

updap Forum Forum English

ORIGINAL

[provider and volume removed] (ONLY NAMES) [...] The data is bad but I'm still leaking [...]

Held
An uploader advertised customer-name data associated with a business-software provider and acknowledged poor data quality.

Not established
The number of distinct people, customer status, source, currency, or a successful intrusion.

A separate software-customer-name claim explicitly acknowledges poor data quality. It illustrates why advertised records should not automatically become affected people. Repeated names, incomplete fields and uncertain customer status require a defined denominator before publication.

CASE F

F

Healthcare-labelled files remain an unverified collection

Evidence card B08 · 18 Oct 2026 · Forum · Healthcare

Unverified advertisement

OBSERVATION	An October forum post associated a mixed-format file collection with a healthcare provider. [S1]
ESTABLISHED	The post describes file types and a provider association. It does not establish medical-record content, authenticity, theft or a fresh incident.
ALTERNATIVES	The collection could concern administrative material, an older event, mixed sources or an inaccurate label. No match to the confirmed healthcare case is assumed.
RESPONSE	Keep clinical continuity and information exposure as separate questions. A service owner should validate the claimed system and data category before a public statement or patient notification decision.

Bottom line

Keep clinical continuity and information exposure as separate questions. A service owner should validate the claimed system and data category before a public statement or patient notification decision.

Evidence card B08 — 18 Oct 2026

updap | Forum | Forum | English

ORIGINAL

[healthcare provider removed] [...] Format: Folders, XLS, PNG, ODS, ODT and others [...]

Held
A forum post associated a collection of mixed-format files with a healthcare provider.

Not established
That the files were medical records, had been stolen, were authentic, or reflected a new incident.

updap

Forum persona | Not assessed

IN ITALY, 2026

September
Posts a business-software names-only claim, B07

October
Posts a mixed-file healthcare offer, B08

CLAIMED TARGETS

Claims described by broad roles

SEEN IN PUBLIC REPORTING

[S1] Retained forum posts B07 and B08

OUR ASSESSMENT

A shared uploader alias links the posts. It does not establish file identity, common theft, authorship, or completed sales.

CONFIDENCE
High for the posting association; identity and underlying claims unverified

4.5 Recent and historical assertions require their own dates

The 11 November media-database advertisement falls inside the recent period, but its content was locked. It supports a recent publication observation, rather than a new intrusion. A February website-database post explicitly carries a 2016 date. It cannot establish a fresh 2026 incident. [S1]

Evidence card B10 — 11 Nov 2026

Linda2000 | Forum | Forum | English

ORIGINAL

[media organisation removed] Database Italy [...] Hidden Content [...]

Held
A November post advertised a database associated with a media organisation; the download was locked.

Not established
File contents, currency, authenticity, access validity or a new intrusion.

Evidence card B11 — 2 Feb 2026

Tanaka | Forum | Forum | English

ORIGINAL

Italy [website removed] WordPress Database [...] format: sql date: 2016 [...]

Held
A February forum post labelled an Italian website database with a 2016 date.

Not established
A new 2026 incident, current access, data authenticity or the meaning of the stated historical date.

Evidence card B12 — 2 Apr 2026

Forum seller | Forum | Forum | English

ORIGINAL

country: Italy [...] access: RDWEB [...] price: [negotiation text removed]

Held
A forum seller advertised remote-web access associated with an Italian events-sector organisation.

Not established
That access worked, the organisation identity, entry route, data theft or a completed sale.

A separate April offer advertises Italy-related RDWEB access. [S1] RDWEB means Remote Desktop Web Access, a web portal for remote desktop access. [S72] The service label does not establish that a seller controlled a working session. No concrete link connects that offer to the banking-log or mail advertisements. Keep each proposition separate, even when the same team would validate them. [S1]

4.6 Additional access and infrastructure claims

The further examples below remain unverified. No connection to an officially reported supplier incident is assumed, and no claimed access was tested. They broaden the triage questions beyond the six case studies. [S1]

Publication	Broad role	Advertised proposition	Validation question
January	Consumer retailer	Customer-identity database claim	Can provenance and the affected population be established?
January	Property services	Professional contact-list offer	What provenance and authorised use are supported?
January	Service-user records	Temporary-password and location-data assertions	Do any current accounts or systems actually match?
30 January	Automotive business	Administrative dashboard and business information	Does the claimed system and access belong to the organisation?
2 February	Financial institution	Information said to originate from staff systems	Is there supported staff-side evidence rather than a label?
February	Consumer services	Contact, membership and device-registration data assertions	Can provenance and current relevance be established?
February	Automotive services	A customer or service dataset advertisement	What evidence links the material to the claimed source?
January-February	Public services	Mailbox and administrative-panel access advertisements	Which accounts and actual privileges can be validated?
6 April	Industrial operator	Italy-related VPN and user access in a multi-country catalogue	Is any claimed account current and relevant?
April-May	Website operators	Webshell access offers	Does authorised evidence identify an affected asset?
26 April	Utility project	Project photographs, geographic layers and business records	What data is genuine, without inferring physical-control access?
14 May	Telecom-related software platform	Subscriber, provisioning and control-related assertions	Which asserted function can the service owner establish?
18 May	ICT supplier	Administrative access and alleged customer reach	Is customer access supported independently?

A utility's project documents do not establish control over physical processes. A supplier's alleged administrative access does not establish access to every customer. These distinctions belong in the first handoff, before a high-impact label becomes a public conclusion.

Evidence card B13 18 May 2026

Forum seller Forum Forum English

ORIGINAL

I'm selling full access Domain Admin for an Italian company named [supplier removed]. [...]

Held
An IT-supplier access offer also claimed onward access to customers.

Not established
Working access, customer exposure, data theft, a sale or any link to a separately reported supplier incident.

Evidence card B14 14 May 2026

Forum seller Forum Forum English

ORIGINAL

Data Exposed: [...] Subscriber PII [...] Mobile subscriber provisioning records [...]

Held
A post alleged exposure of subscriber and provisioning data and control capability at a telecom-related software platform.

Not established
Authenticity, working control, affected operators, service impact or current access.

Evidence card B15 26 Apr 2026

Forum seller Forum Forum English

ORIGINAL

Data Content: [...] field photos [...] GIS files [...] [project details removed]

Held
A seller advertised water-project survey, mapping and contractor-delivery material.

Not established
Authenticity, confidentiality, the origin of the files or access to operational control systems.

Evidence card B16 30 Jan 2026

Forum seller Forum Forum English

ORIGINAL

Admin dashboard includes [...] asking $5k [...]

Held
A seller offered automotive-sector administrative access and stated an asking price.

Not established
Working access, revenue, customer impact, payment compromise or a completed sale.

4.7 Turn an advertisement into a bounded validation task

A useful intelligence handoff states the claimed product, relevant organisation or role, date, source type and missing evidence. It identifies the team that can validate account, service or data relevance. The action should be proportionate to that proposition.

An account-specific signal can warrant prompt identity work. A generic multi-country offer may warrant monitoring rather than broad containment. A credible customer-data sample can justify preparatory fraud advice while the source remains uncertain. None of those decisions requires presenting the seller's assertion as an established national incident.

KEY TAKEAWAYS

01

Country tags and advertisements establish observations, rather than attacks or completed sales.

02

Locked, poor-quality and historical material needs explicit limits.

03

Route the specific proposition to the team that can validate its relevance.

CHAPTER 05

Targeting examples and cases by sector

05

THIS CHAPTER ANSWERS

Which events are supported, which remain claims, and what should each owner do first?

12

public-source references separating cases, campaigns and exclusions

5.1 Sector decisions 34

5.2 Source-backed case cards 37

5.3 Campaign cases and a documented exclusion 43

5.4 Close the loop with the owner 45

CHAPTER 05

Targeting examples and cases by sector

IN SHORT

Confirmed cases show interruption, unauthorised access and supplier consequences. Other stories remain claims, disputed interpretations or older incidents disclosed later. The cases preserve those distinctions, including when an organisation confirms an event but not data theft or actor identity. Assign an owner from the first-response table, then check the case's limit before taking action.

5.1 Sector decisions

The table links each issue to a validation step. It is a case-based guide, rather than a comparison of sector incident rates.

Education

EVIDENCE

Confirmed university ransomware and recovery notice

MEANING

Recovery and data-risk assessment need separate records

FIRST RESPONSE

Test student and administrative workflows after restoration

Cloud and ICT

EVIDENCE

Supplier interruption and shared-area encryption

MEANING

Customer workflows can depend on the affected resource

FIRST RESPONSE

Test a separate recovery route for that dependency

Healthcare

EVIDENCE

Incident, restoration and patient-notification accounts

MEANING

Restored care and administrative-data exposure need separate decisions

FIRST RESPONSE

Validate care and reconcile data scope and notifications

Retail

EVIDENCE

Confirmed member-contact access

MEANING

Continued trading and data exposure can coexist

FIRST RESPONSE

Verify unexpected customer contacts through known channels

Culture

EVIDENCE

Administrative incident with disputed wider claims

MEANING

IT disruption does not establish physical-security loss

FIRST RESPONSE

Confirm each claimed effect with the operator

Transport projects

EVIDENCE

Company-quoted response; works reportedly continued

MEANING

Office IT and physical works are different propositions

FIRST RESPONSE

Check business and engineering dependencies separately

Utilities

EVIDENCE

Restoration following business-function interruption

MEANING

Administrative effects do not establish supply interruption

FIRST RESPONSE

Obtain separate business and process-owner acceptance

Financial services

EVIDENCE

Official phishing campaigns and reported fraud

MEANING

Fraud can exploit legitimate approval workflows

FIRST RESPONSE

Confirm changed instructions outside the requesting channel

Public services

EVIDENCE

Official mailbox and identity-phishing notices

MEANING

Trusted senders and brands can be abused

FIRST RESPONSE

Review sessions and account-recovery changes

Schools

EVIDENCE

Threatening messages without established intrusion

MEANING

Communications-security still requires action

FIRST RESPONSE

Preserve messages and use the police liaison

5.2 Source-backed case cards

P references identify public-source case material. They are analyst paraphrases, rather than underground quotations. One case can contain differently supported propositions. Follow-up dates do not create additional incidents.

CASE G

University recovery confirmed after ransomware (P01)

Education

Source-confirmed incident; limits apply

CONFIRMATION	Sapienza Università di Roma confirms that ransomware began on 1 February 2026. Its April notice describes confidentiality and availability effects. [S5]
CHRONOLOGY	Early reporting described precautionary network shutdown and recovery with ACN. Closure occurred on 2 April and was communicated internally on 9 April. [S6][S5]

ESTABLISHED	About 400 physical and virtual servers were involved. University portals and student services were interrupted, and affected data were encrypted. [S5]
LIMITS	The university found no evidence that the specified data were stolen, publicly disseminated or used fraudulently. Its notice does not establish an actor. [S5]
RESPONSE	Separate restoration from personal-data assessment. Test student, finance and administrative workflows, verify records, and preserve a dated list of unresolved exposure questions.

Bottom line

Separate restoration from personal-data assessment. Test student, finance and administrative workflows, verify records, and preserve a dated list of unresolved exposure questions.

The case supports recovery work without a speculative actor narrative. Concurrent incidents elsewhere do not establish a common route or operator. Closure needs a tested service and an updated data-risk assessment, rather than an infrastructure ticket alone.

H

CASE H

A supplier incident reaches a public payment workflow (P02)

Cloud and public services

Source-confirmed incident; limits apply

CONFIRMATION	A cloud provider acknowledged a 23 March incident. Reporting linked the interruption to a municipal penalty-payment service. [S24][S25]
CHRONOLOGY	April coverage described payment difficulties and an investigation coordinated by prosecutors and entrusted to Polizia Postale. Payment deadlines were extended. [S25]
CLAIM	Qilin's association appears as a criminal claim in reporting. Acknowledgement of interruption does not independently establish attacker identity. [S24]
LIMITS	Initial statements did not establish extraction. Supplier and customer environments require separate examination.
RESPONSE	Identify the failed dependency and transactions awaiting reconciliation. Test an alternative route and verify customer access after restoration.

Bottom line

Identify the failed dependency and transactions awaiting reconciliation. Test an alternative route and verify customer access after restoration.

Customers need enough information to decide whether to suspend a workflow, offer a manual route or change a deadline. The supplier contract should identify who provides those facts and how updates reach customers during an outage.

CASE I

I A museum disputes broader interpretations (P03)

Culture

Source-confirmed incident; limits apply

CONFIRMATION	February reporting quoted a museum's account of an administrative IT incident. Visits and several visitor-facing functions were reported as continuing. [S23]
LATER REPORTING	April coverage described an attempted-extortion investigation and allegations about security information. The museum disputed evidence for those allegations. [S23]
ESTABLISHED LIMIT	The museum said collection movements cited in coverage were planned for building work. They should not become a demonstrated cyber consequence. [S23]
ALTERNATIVES	A real administrative incident, a claim about data possession and an inaccurate account of physical consequences can coexist.
RESPONSE	Confirm asset and service effects with the operator. Avoid amplifying physical-security details and distinguish unavailable IT from established information exposure.

Bottom line

Confirm asset and service effects with the operator. Avoid amplifying physical-security details and distinguish unavailable IT from established information exposure.

An investigation establishes that allegations are being examined. It does not establish every allegation in a report. This distinction also prevents communications teams from repeating an actor's intended pressure as their own conclusion.

CASE J

J A utility restores business functions (P04)

Utilities

Source-confirmed incident; limits apply

CONFIRMATION	Alto Calore's public statement dates an attack to 9 August. Its 16 September update announces a return to business operations with further work remaining. [S26]

ESTABLISHED LIMIT	The notice concerns business functions. It does not establish physical water-supply interruption or an actor identity.
ALTERNATIVES	Administrative systems and operational processes can have different recovery states. Wider reporting uses a different August date; this case preserves the official statement's date.
RESPONSE	Obtain separate business and process-owner acceptance. Check billing, customer records and work orders alongside operational communications.

Bottom line

Obtain separate business and process-owner acceptance. Check billing, customer records and work orders alongside operational communications.

Continuing physical operations does not remove business interruption. Restored administrative access does not establish that every record is complete. A recovery log should name the function, validation and owner accepting the result. [S26]

CASE K

K

Healthcare restores services and separates exposure questions (P05)

Healthcare

Source-confirmed incident; limits apply

CONFIRMATION	A regional healthcare group's Direction confirms a 31 August incident. Its early account describes unavailable IT, phones and email. [S27]
OPERATIONAL ACCOUNT	Rai reported disrupted appointments and manual work. Some activities continued, so the case does not establish that all care stopped. [S28]
FOLLOW-UP	A later Direction statement reports restored contacts, outpatient activity and operating rooms. It identifies INC Ransom and says no ransom was paid or negotiated. [S29]
EXPOSURE UPDATE	Rai's 17 November report describes patient letters dated 16 October confirming that some administrative information appeared online. It lists names, birth dates, care received, doctors and amounts paid. [S71]
LIMITS	Rai quotes the provider's data-protection officer describing a bounded part of the archive and individual postal notifications. The provider distinguishes administrative documents from clinical reports. B08's separate advertised-file claim remains unverified. [S71][S1]
RESPONSE	Validate safe care and reconcile paper and electronic records. Test communications independent of the affected environment. The privacy owner

should reconcile reported data exposure, the affected population and notification status.

Bottom line

Validate safe care and reconcile paper and electronic records. Test communications independent of the affected environment. The privacy owner should reconcile reported data exposure, the affected population and notification status.

Clinical continuity needs acceptance criteria that business-only plans can miss. Confirm record reconciliation, staff contacts and access to critical patient information. These are recommended checks, not allegations that the group failed to perform them.

A separate 16 November report quotes a regional health-service executive confirming abnormal booking-system activity reported on 5 November and countermeasures. Data-access scope and the relationship to wider booking faults remained under investigation. This is another disclosure, rather than evidence linking all booking problems to one intrusion or to Case K. [S64]

L

CASE L

Contact access without established payment-data theft (P06)

Retail

Source-confirmed incident; limits apply

CONFIRMATION	Unicoop Firenze confirmed access to a member-management system and some contact information. It said affected servers were isolated and authorities notified. [S7]
SERVICE STATUS	The statement says business services continued. Its security information says passwords, PINs, access codes and payment-card data were not involved. [S7][S8]
DENOMINATOR	Total membership is not a confirmed affected-person count. A membership headline cannot supply the missing incident denominator. [S9]
LIMITS	The notice does not establish a connection to separate refrigeration incidents or an international campaign.
RESPONSE	Warn about unexpected requests using familiar contact details. Confirm account or payment instructions through known channels, and update advice as scope changes.

Bottom line

Warn about unexpected requests using familiar contact details. Confirm account or payment instructions through known channels, and update advice as scope changes.

The 17 November notice belongs in recent activity. Its publication date does not establish first access. Customer operations should preserve that distinction when answering questions about which contacts need advice.

CASE M

M ■ Document reporting mixes different denominators (P07)

Business services

Source-confirmed incident; limits apply

CONFIRMATION	Journalists obtained company confirmation of an incident involving a contained number of people. Reporting associated material with a digital-services provider. [S31][S32]
OBSERVED MATERIAL	A publication described contracts and identity records in an archive. Those are journalists' observations, rather than company-confirmed affected-person totals. [S32]
LIMITS	Contracts and records can overlap. They cannot be added or converted into current bank-account totals. The reported extraction route remains unresolved.
ALTERNATIVES	Documents can originate from a service, partner, export or older process. A posted archive does not independently identify extraction.
RESPONSE	Check document categories and service relationships before notification decisions. Warn against requests invoking genuine contract details to obtain passwords or approval.

Bottom line

Check document categories and service relationships before notification decisions. Warn against requests invoking genuine contract details to obtain passwords or approval.

Documentary familiarity can make a fraudulent contact convincing without giving the caller legitimate authority. The response should identify what the caller could know, then protect the decision that information might influence.

CASE N

N ■ A project company separates IT response from works (P08)

Transport and construction

Source-confirmed incident; limits apply

CONFIRMATION	Reporting quotes a transport-project company describing isolation, specialist support and authority notification. It said operations and works were unaffected. [S30]
CHRONOLOGY	The reported occurrence was in October, with wider disclosure in November. Later disclosure does not create a new intrusion. [S30]

CLAIM	A criminal-group association and data volume were reported conditionally. The source did not establish them as findings.
LIMITS	Investigation is not final attribution. Office communications, engineering systems and physical works need separate evidence.
RESPONSE	Verify project-document access, contractor identities and approved engineering records. Obtain process-owner confirmation independently of office-system recovery.

Bottom line

Verify project-document access, contractor identities and approved engineering records. Obtain process-owner confirmation independently of office-system recovery.

CASE O

Shared storage creates a customer consequence (P09)

ICT services

Source-confirmed incident; limits apply

OFFICIAL REPORTING	ACN describes encryption in a shared area at an ICT provider, affecting customers using it. [S13]
ASSOCIATION	The report associates Titan with the incident. That source attribution does not cover every customer or the entire estate.
LIMITS	The passage supplies no customer total or precise occurrence date. It is not assumed to match another named case.
RESPONSE	Map the resource behind each important service. Test access separation, recovery access and customer-level acceptance through an authorised exercise.

Bottom line

Map the resource behind each important service. Test access separation, recovery access and customer-level acceptance through an authorised exercise.

5.3 Campaign cases and a documented exclusion

Useful coverage includes campaigns and exclusions. These references add decision value without manufacturing additional confirmed victims.

CASE P

P

Public mailboxes carry a credential lure (P10)

Public administration

Campaign reported

OFFICIAL OBSERVATION	CERT-AGID describes abused public mailboxes distributing document-themed messages to earlier correspondents, using a legitimate collaboration service. [S17]
ESTABLISHED	The source supports mailbox abuse and credential-seeking activity. It does not establish intrusion into the collaboration platform or every recipient organisation.
ALTERNATIVES	Familiar correspondence can reflect real history while the current message is fraudulent. Sender familiarity and destination trust are different decisions.
RESPONSE	Review sign-ins, sessions, forwarding and recovery changes. Warn correspondents separately and establish whether recipients entered credentials.

Bottom line

Review sign-ins, sessions, forwarding and recovery changes. Warn correspondents separately and establish whether recipients entered credentials.

CASE Q

Q

Identity packages create possible follow-on fraud (P11)

Identity and fraud

Campaign reported

OFFICIAL OBSERVATION	CERT-AGID describes benefit-themed smishing seeking identity, income and employment information. It distinguishes collection from possible later uses. [S18]
INTERPRETATION	The information could support further impersonation or credit applications. The source does not establish a loan or bank loss.
LIMITS	Document theft and an opened financial account are different populations. This report does not infer completed cash-out.
RESPONSE	Test onboarding and recovery with synthetic information assumed known to an attacker. Route genuine document exposure through fraud and identity processes.

Bottom line

Test onboarding and recovery with synthetic information assumed known to an attacker. Route genuine document exposure through fraud and identity processes.

CASE R

R

A technical outage is excluded (P12)

Public services

Excluded technical outage

OFFICIAL ACCOUNT	A parliamentary ministerial answer attributes the 6 May judicial-network disruption to a supplier's technical fault, rather than cyberattack or intrusion. [S46]
LIMIT	Unavailability and cyber intrusion are not synonymous. That answer does not resolve unrelated supplier incidents.
RESPONSE	Preserve a cause field and the evidence behind it. Record why an early cyber hypothesis was closed.

Bottom line

Preserve a cause field and the evidence behind it. Record why an early cyber hypothesis was closed.

5.4 Close the loop with the owner

For each case, the incident manager should state the affected function, current evidence and next validation. Use a dated status record rather than a permanent label copied from an early headline. Record whether the criminal claim was actually matched to the event.

The same discipline matters when evidence weakens a story. Maintenance, an older disclosure or a mistaken attribution should remain in the review record with an exclusion reason. Removing it from a threat total does not imply that no response work was needed.

KEY TAKEAWAYS

01

Confirm service effects, data scope and actor identity separately.

02

Follow-up notices update an existing case rather than creating an incident.

03

A documented exclusion strengthens coverage when its reason is explicit.

CHAPTER 06

Hacktivism, DDoS and recent activity

06

THIS CHAPTER ANSWERS

What did claimants say, what did authorities establish, and what changed near the cut-off?

9-22 Nov

recent period ending at the collection snapshot

6.1 Timeline of distinct evidence types 47
6.2 Olympic claims and official effects 48
6.3 Later waves need fresh evidence 49
6.4 Recent activity: 9-22 November 51
6.5 Physical controls need a process owner 52
6.6 Prepare a public line that survives new facts 53

CHAPTER 06

Hacktivism, DDoS and recent activity

IN SHORT

Olympic-period claims were visible, while ACN reported limited website effects and no impact on regular competitions or essential event services. Later accounts distinguish attempted disruption from intrusion. Recent disclosures add contact-data and document concerns; threatening messages remain separate from system access. Confirm the affected function, preserve external claims as claims, and prepare an alternative status channel.

6.1 Timeline of distinct evidence types

Dates below identify publications or explicitly dated events. Their descriptions retain that distinction. Actor claims, third-party relays and official accounts carry separate labels.

4 Feb 2026	**Foreign minister, reported by AP** Says attacks against diplomatic and Olympic-related sites were prevented; origin characterised by the minister
17 Feb 2026	**CSIRT Italia bulletin, republished regionally** Describes renewed business email compromise against Italian organisations
6 Jun 2026	**Spanish-language channel** Attributes Italian target claims to NoName057(16); no primary actor post or verified outage established
31 Aug 2026	**Healthcare Direction, reproduced by press** Confirms an incident; later notices distinguish restoration and data questions
8 Oct 2026	**Foreign ministry** Says website attack was mitigated without disruption; notice names no actor
12 Oct 2026	**BDAnonymousTeam** Claims activity against a government information website; effect unverified
22 Oct 2026	**BDAnonymousTeam** Claims activity against an airport website; effect unverified
29 Oct 2026	**Translated NoName057(16) posts** Repeat a defence-website assertion; no confirmed service effect
7 Nov 2026	**Press reporting** Reports a transport-project company's response; works said to continue
11 Nov 2026	**Press reporting** Describes threatening school messages; delivery does not establish system access
16 Nov 2026	**EU Council decision**

Adds NoName057(16) to a restrictive-measures annex; designation does not establish each Italian incident

16 Nov 2026	**Health executive quoted by Rai** Confirms earlier abnormal booking activity and countermeasures; access scope remains under investigation
17 Nov 2026	**Unicoop Firenze** Confirms some member-contact access; business services continue
17 Nov 2026	**Rai, quoting a healthcare data-protection officer** Reports administrative data online and patient letters dated 16 October; follow-up to the August incident
19 Nov 2026	**Company confirmation quoted by press** Describes a contained incident associated with document material
19 Nov 2026	**Interior minister, parliamentary statement** Reports a 2 November refrigeration cyberattack in Italy; responsibility and coordination unresolved [S74]
20 Nov 2026	**ACN October summary** Publishes operational observations and revisions of earlier months

A retained 11 November forum advertisement associates locked material with a media organisation (B10). It is recent publication evidence, not a verified recent intrusion. A separate buyer request for Italian corporate-bank logs establishes demand, rather than possession or a bank incident. [S1]

6.2 Olympic claims and official effects

AP reported the foreign minister's statement that attacks against diplomatic and Olympic-related sites were prevented. The minister characterised origin as Russian without supplying detailed technical attribution in that account. This report preserves his attribution; it does not independently assign a state operator. [S11]

ACN distinguishes website effects from regular event operation. In its February 2026 DDoS campaign summary, ACN reported temporary website unavailability for 6% of recorded events. It is not a success rate for every actor claim or a measure of all national DDoS. [S10]

Point	Claimant account	Official account	Assessment
Targeting	Posts and reports named diplomatic and event websites	Minister described attempts; ACN discusses event-related DDoS	Validate each service privately
Website effect	Claimants presented disruption as an achievement	ACN records temporary unavailability for a minority of DDoS events	Different populations cannot become a ratio
Event effect	Website claims attracted event-related attention	ACN says regular competitions and essential services were unaffected	Website effects do not establish event interruption
Attribution	The cited accounts do not identify a specific claimant alias	Minister characterised origin without detailed public technical basis	Preserve source attribution and unresolved operator identity
Data	Disruption claims did not establish access	The cited account does not establish theft from these claims	Assess separate data allegations on their own evidence

Check the exact service privately, obtain provider telemetry and confirm the user journey. State what was attempted, what users experienced and what action followed. A proportionate response does not require accepting unsupported actor numbers or publishing a broad affected-service list.

6.3 Later waves need fresh evidence

ACN reports renewed hacktivist DDoS late in May, with generally temporary unavailability or slowing. Its August account reports no particularly significant campaign in that month's national view. Neither observation establishes the absence of smaller activity. [S14][S13]

The foreign ministry's 8 October notice says an attack was mitigated without service disruption and checks were underway for diplomatic-consular sites. It does not name NoName057(16), Russia or a successful intrusion. Later reporting cannot retroactively supply an attribution absent from that notice. [S12]

A retained Spanish-language relay on 6 June attributes Italian target claims to NoName057(16). It establishes the relay, rather than a retained original actor post or a verified outage, duration or effect. It does not contradict ACN's narrower statement about particularly significant campaigns in another period. [S1]

Evidence card B17 — 6 Jun 2026

Channel relay | Spanish-language relay channel | Telegram | Spanish

ORIGINAL

Comenzamos el día con ciberataques a Italia [...]

TRANSLATION

We begin the day with cyberattacks on Italy [...]

Held
A Spanish-language relay attributed target claims against Italian public portals and other organisations to NoName057(16).

Not established
An original actor post, a verified outage, duration, cause, impact or the identity of an operator.

Retained October posts also carry a government-information-site claim and an airport-site claim under BDAnonymousTeam. Later translated NoName057(16) posts repeat a defence-website allegation. These are distinct assertions with no confirmed operational effects or common technical link established here. They do not expand the official 8 October ministry statement. [S1]

A name can recur, change administrators or be adopted by another poster. Reappearance alone cannot establish continuity of operator or infrastructure. Intelligence teams should retain the evidence behind each association rather than assuming every later post belongs to the same operation.

NoName057(16)

DDoS claimant | Pro-Russian, as described by the EU Council [S63]

IN ITALY, 2026

6 June
A Spanish-language channel relays Italian target claims, B17

16 November
EU Council adds the group to its cyber restrictive-measures list

CLAIMED TARGETS

Italian websites named in retained claims and relays

IN THEIR WORDS

"[Relay translation] We begin the day with cyberattacks on Italy [...]" B17

SEEN IN PUBLIC REPORTING

[S1] B17 retains a relay of claims, not an independently verified outage

[S63] Council Decision (CFSP) 2026/2546 adds the entity; the source's characterisation remains attributed

OUR ASSESSMENT

The retained relay establishes a claim, not a verified outage or operator identity. The Council designation does not establish responsibility for individual Italian incidents.

CONFIDENCE

High for the retained relay and published Council designation; responsibility and impact remain unverified for the relayed Italian claims

6.4 Recent activity: 9-22 November

The recent forum view uses the same Italy country-tag filter and retains 195 distinct posts dated 9-22 November 2026, forming a subset of the 839 retained Italy-tagged forum posts in §4.1. These are source publications, not verified incidents or necessarily new activity. The view does not establish complete national underground coverage. Validate the advertised account, dataset or service before escalating. [S1]

The forum observations include advertised tenant administration, business-contact lists and bank-themed phishing tools. [S1] A tenant is an organisation's managed environment within a cloud service. Tenant administration means managing that environment. [S73] The advertisements do not establish a current intrusion at a selected organisation. The contact-list offer describes scraped data; its origin and any completed sale remain unverified. [S1]

This period ends at the 22 November collection snapshot. Publication during it can concern an older event. The table therefore identifies what the recent source adds.

Observation	New information	Unresolved	Owner
Cooperative notice	Confirmed contact-data access and continued services	First access and final affected denominator	Privacy and customer operations
Health-booking disclosure	Executive confirmed earlier abnormal activity and countermeasures	Data scope and relation to wider booking faults	Health-service and privacy owners
Healthcare follow-up (P05)	Rai reports patient letters and bounded administrative data online	Complete exposure inventory and affected population	Privacy owner
EU Council decision	NoName057(16) added to a restrictive-measures annex	Responsibility for any particular Italian event	Legal and intelligence
Document-related reporting	Company confirmation alongside journalists' archive observations	Route, overlap and final population	Privacy and service owner
Refrigeration statement	Minister reports a 2 November attack on food-retail refrigeration [S74]	Responsibility, coordination and site-specific causes	Process owner and response
School-threat reporting	Threatening messages and investigation	Common actor and any system access	Security and police liaison

Observation	New information	Unresolved	Owner
October summary	Updated national operational snapshot	It does not measure completed November activity	Threat intelligence
Underground posts	Separate retained recent signal	Authenticity and connection to official cases	Intelligence and response

The 17 November healthcare follow-up updates Case K's August incident. Rai reports letters dated 16 October and the provider's distinction between administrative documents and clinical reports. This updates P05; it does not add a case. [S71]

The 16 November health-booking disclosure concerns activity reported earlier that month. The Council decision is a legal development, rather than an incident. Both belong in recent observation while retaining their own evidence types. [S63][S64]

The cooperative's 17 November notice belongs here. Earlier transport-project disclosures are preceding context. The 19 November refrigeration statement updates official evidence on an earlier event. Its recent publication does not change the event date. [S7][S30][S74]

Threatening messages require preservation, escalation and safe communications. Receipt does not establish access to school systems. Counts from different message rounds should not be added without evidence of distinct recipients. The report does not count the messages as confirmed school intrusions. [S36]

6.5 Physical controls need a process owner

A retained May post claimed access to an Italian flood-control interface. Neither working access nor physical effects were established. This claim is separate from the April utility-project data offer. [S1]

Early-November coverage discussed food-chain refrigeration and criminal claims. Parliamentary question preambles record concerns and reported events, rather than government technical findings. They cannot independently establish attacker, mechanism or scope. [S34]

On 19 November, the interior minister told Parliament that a cyberattack on 2 November affected food-retail refrigeration systems in Italy. He separately said attribution to coordinated hostile actors remained premature. His national account does not establish the cause of every individual reported malfunction. [S74]

A separate supermarket account illustrates the limit. Its manager reported temperature changes and manual intervention but could neither confirm nor exclude a cyberattack. That site is excluded from the confirmed cyber count. A changed physical reading still deserves investigation. [S35]

Separate safety from attribution. Use the safe manual or isolation procedure approved by the process owner. Preserve access and vendor-session records. Verify equipment state and product safety independently. Restoring a setting does not establish that exposed stock remained safe.

The report does not infer a common operator behind DDoS, threats, personal-data targeting and refrigeration cases. Similar timing or political messaging is insufficient. A common campaign needs a concrete supporting link checked against the particular events.

6.6 Prepare a public line that survives new facts

A useful first statement identifies the verified service condition, remaining uncertainty and action for users. It names the next update channel. If a claim is circulating, describe it as an external assertion without repeating unsupported scale.

Communications and the SOC should agree who verifies availability. Legal should assess notification from established facts. Providers should know which telemetry customers need. Test those handoffs while the main website and normal messaging route are unavailable.

KEY TAKEAWAYS

01

Availability claims need service-specific evidence and a defined denominator.

02

Recent disclosure does not establish recent intrusion.

03

Physical safety, response and attribution require distinct decisions.

CHAPTER 07

Threat actors and evidence of relationships

THIS CHAPTER ANSWERS

Which actors appear in the evidence, and what do those associations establish?

286

Italy-associated ransomware listing records in the reporting window

7.1 An evidence relationship is not a joint operation 55
7.2 Ransomware publications remain claims 59
7.3 Regional peers provide context, not a risk ranking 60
7.4 Publication timing differs from intrusion timing 61
7.5 Official case attribution stays with its source 62
7.6 Espionage context published in 2026 63
7.7 Web exploitation and phishing require different checks 64

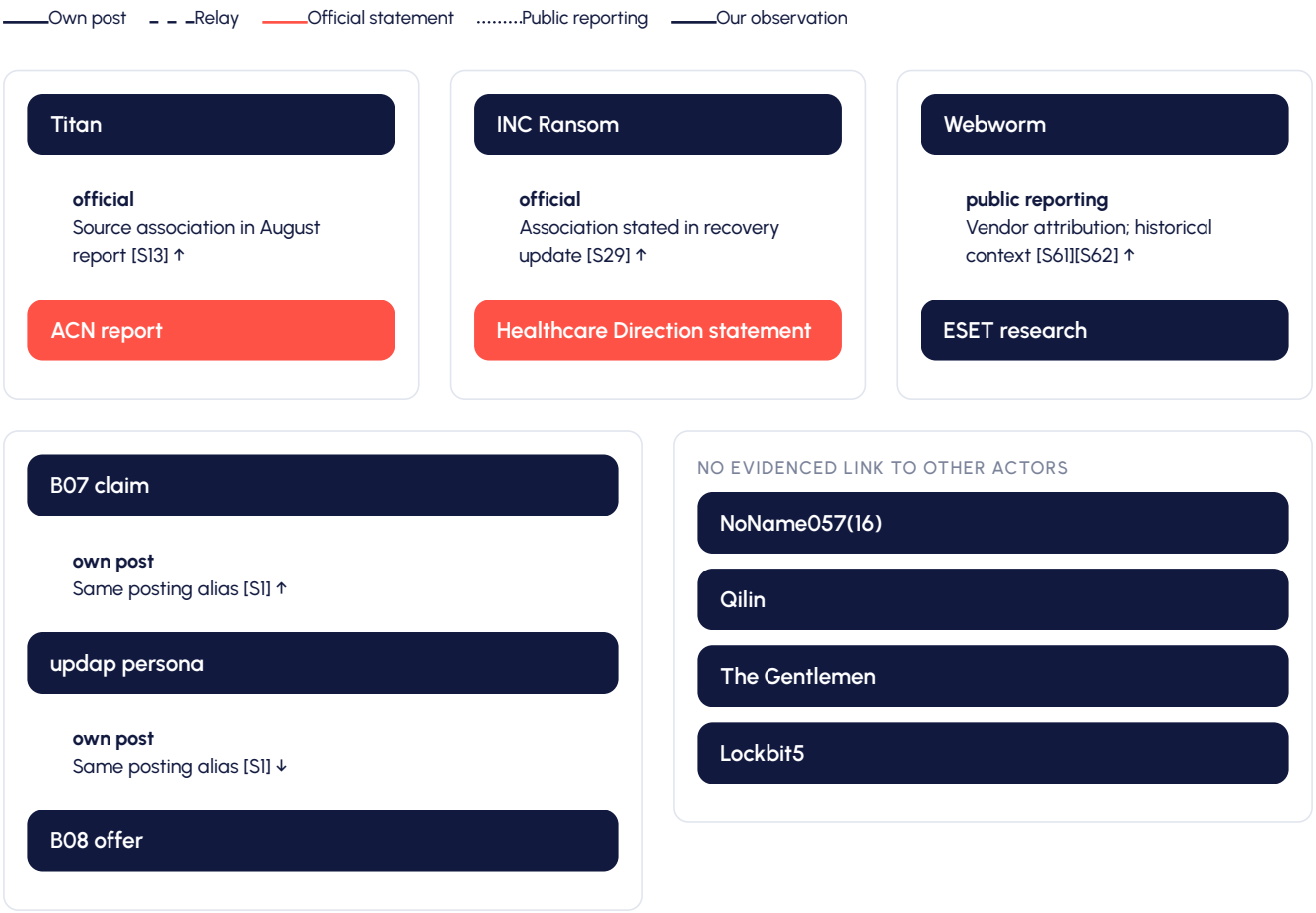
CHAPTER 07

Threat actors and evidence of relationships

IN SHORT

Ransompedia records a broad set of extortion brands naming Italy-associated organisations. Those are publication records, not independently verified intrusions. Hacktivist attribution remains tied to each claimant or cited official. Phishing notices often describe behaviour without identifying an operator. Use actor names to find relevant evidence, then validate the organisation-specific proposition before selecting a response.

7.1 An evidence relationship is not a joint operation



The relationship view connects a source to an observed claim, listing or reported case. Each edge states its evidence type. A connection to the same country, sector or political theme does not establish common ownership, a shared operator or cooperation between groups.

The network map above shows only source attributions and the shared posting alias linking B07 and B08. Where this report discusses fraud services as a possible sequence, that sequence is a separate analytical model identifying control decisions that could be abused. It does not assert that the same seller supplied documents, opened an account and moved money in a particular observed case. Concrete links would need their own evidence.

Qilin

Extortion listing label | Not assessed

IN ITALY, 2026

2026

35 Italy listings in the retained ransomware record

CLAIMED TARGETS

Organisations named by the listing source

SEEN IN PUBLIC REPORTING

[S2] 35 of 286 Italy listings

OUR ASSESSMENT

Counts describe public extortion claims. They do not establish encryption, loss, or the identity of an operator.

CONFIDENCE

High for retained listing counts

The Gentlemen

Extortion listing label | Not assessed

IN ITALY, 2026

2026

32 Italy listings; the source label is Thegentlemen

CLAIMED TARGETS

Organisations named by the listing source

SEEN IN PUBLIC REPORTING

[S2] 32 of 286 Italy listings

OUR ASSESSMENT

Keep each listing's verification separate from the reputation attached to a group name.

CONFIDENCE

High for retained listing counts

Lockbit5

Extortion listing label | Not assessed

IN ITALY, 2026

2026

28 Italy listings under this source label

CLAIMED TARGETS

Organisations named by the listing source

SEEN IN PUBLIC REPORTING

[S2] 28 of 286 Italy listings

OUR ASSESSMENT

The feed label is retained as a label. It does not independently establish continuity with another operation.

CONFIDENCE

High for retained listing counts

Titan

Ransomware association and listing label | Not assessed

IN ITALY, 2026

August

ACN associates an anonymous ICT-provider shared-storage incident with Titan

2026

11 Italy listings in the ransomware record

CLAIMED TARGETS

An unnamed provider and customer storage, according to ACN

SEEN IN PUBLIC REPORTING

[S13] ACN describes encryption affecting customer organisations using a shared area

[S2] 11 Italy listings

OUR ASSESSMENT

The source association does not establish that every listing relates to this incident or that the same operator controls another alias.

CONFIDENCE

High for the official description; wider links unestablished

INC Ransom

Source-attributed incident and listing label | Not assessed

IN ITALY, 2026

September

A healthcare provider's Direction identifies INC Ransom in a recovery update

2026

7 Italy listings in the ransomware record

CLAIMED TARGETS

A broadly described healthcare group in the Direction's account

SEEN IN PUBLIC REPORTING

[S29] Direction statement republished by local press

[S2] 7 Italy listings

OUR ASSESSMENT

Attribute the incident association to the Direction. Do not use a later forum offer to establish new theft or a second incident.

CONFIDENCE

High for the retained statement; archive contents and wider links unverified

7.2 Ransomware publications remain claims

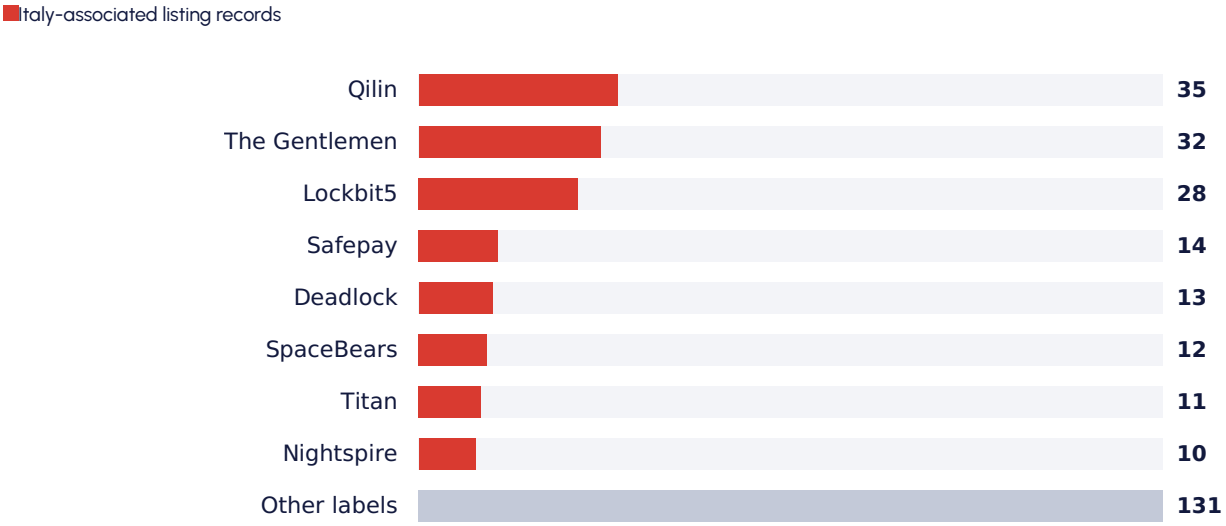
Ransompedia contains 286 Italy-associated listing records dated within the reporting window. They contain 270 distinct victim-name values and 59 group-name values. These are feed-record populations. Neither distinct name count is a verified count of organisations, operators or incidents. A publication can repeat an earlier assertion. [S2]

In the sector CSV, `distinct_feed_names` counts distinct victim-name values within each sector. Names can recur across sectors, so sector counts are non-additive and must not be summed. Use the global count of 270 for the full listing set. [S2]

The top three group labels account for 95 of 286 records, or 33.2%. The other records total 191, or 66.8%. This distribution describes the monitored publication set, rather than an allocation of Italy's ransomware harm. It cannot establish which group caused the most downtime or financial loss.

Group label	Listing records	Reading
Qilin	35	Actor-associated publication records
The Gentlemen	32	Actor-associated publication records
Lockbit5	28	Actor-associated publication records
Safepay	14	Actor-associated publication records
Deadlock	13	Actor-associated publication records
Space Bears	12	Actor-associated publication records
Titan	11	Actor-associated publication records
Nightspire	10	Actor-associated publication records
Other labels	131	Remaining monitored records
Total	**286**	**Not confirmed national intrusions**

Three group labels account for one third of Italy-associated listing records



Source: Brandefense Ransompedia Italy-associated listing records, 1 January–22 November 2026; November partial. Listing dates do not establish intrusion dates [S2].

In the source feed, The Gentlemen appears as Thegentlemen and Space Bears appears with a space, whereas some external reporting writes SpaceBears. The record-level response starts with a role and affected-service hypothesis, rather than an automatic breach statement. Check whether the named entity matches the organisation, whether a public confirmation exists and whether the material could concern an older event. Reconcile aliases privately before treating repeated names as distinct organisations.

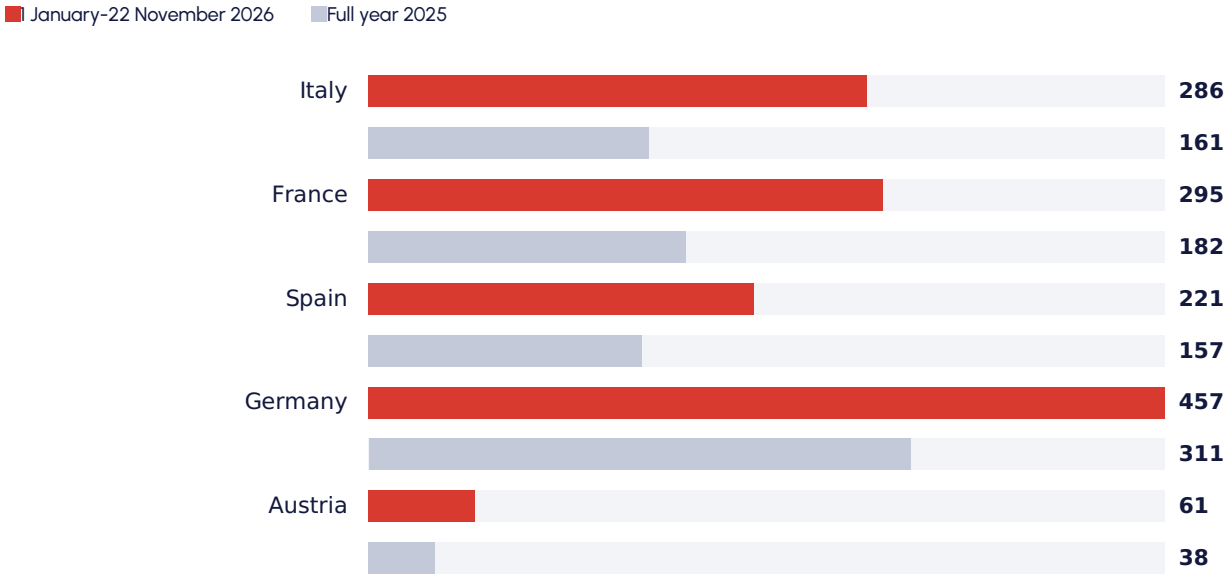
7.3 Regional peers provide context, not a risk ranking

France and Austria provide neighbouring service and cross-border context. Germany provides a large industrial economy comparison. Spain provides a Mediterranean European comparison. These are purposive peers, rather than matched national samples. Country labels and publication coverage require the same caution as the Italy set.

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

Country	2026 window	Full 2025	Interpretation
Italy	286	161	Country-associated listing records
France	295	182	Same source, different national population
Spain	221	157	Same source, different national population
Germany	457	311	Same source, different national population
Austria	61	38	Same source, different national population

Regional listing counts describe monitored publications rather than national incident prevalence



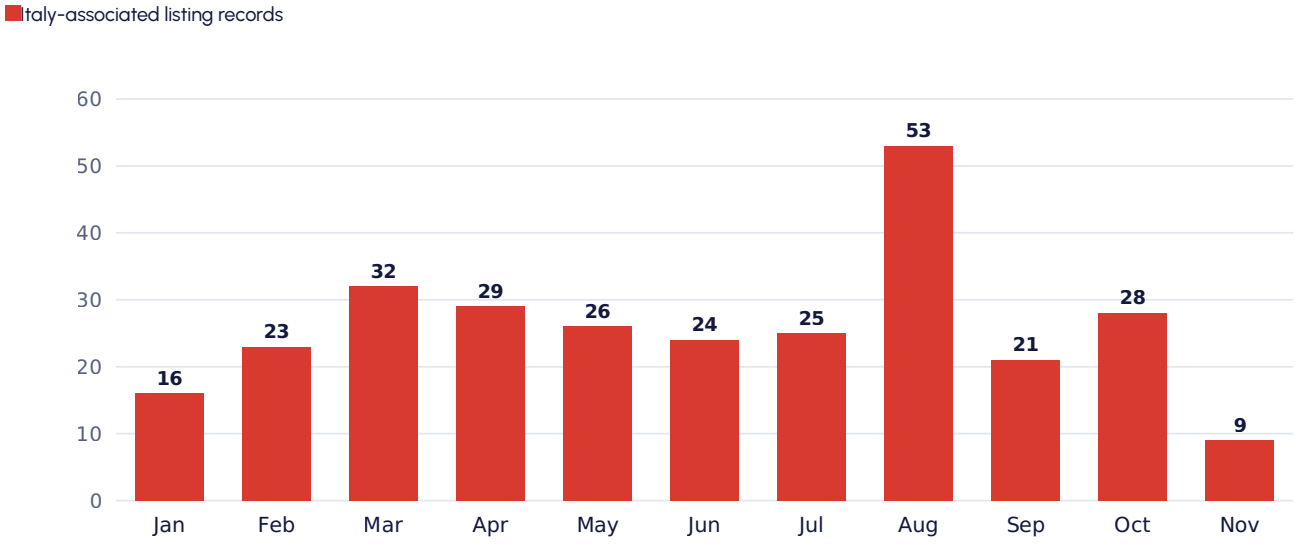
Unmatched periods and different country populations; not a national risk ranking. Source: Brandefense Ransompedia Italy-associated listing records, 1 January-22 November 2026; November partial. Listing dates do not establish intrusion dates [S2].

The 2026 period is incomplete; 2025 is a full year. The table therefore does not calculate growth rates. Different country populations, reporting practices and actor publishing choices also prevent a national security ranking. The useful question is which extortion brands and sector examples deserve monitoring for a specific organisation. [S2]

7.4 Publication timing differs from intrusion timing

The Italy listing series records 16 entries in January, 23 in February, 32 in March and 29 in April. It records 26 in May, 24 in June, 25 in July and 53 in August. September has 21, October 28 and the partial November window has 9. The total is 286. [S2]

August has the most listing publications; publication dates do not establish intrusion dates



Source: Brandefense Ransompedia Italy-associated listing records, 1 January–22 November 2026; November partial. Listing dates do not establish intrusion dates [S2].

August's 53 records are the largest monthly publication count in this source window. That observation does not establish an August peak in successful intrusion or a cause. Delayed publication, repeated allegations and changes in visibility are alternatives. Use the dates to prioritise review of the publications, not to forecast a seasonal attack probability.

7.5 Official case attribution stays with its source

A healthcare Direction identifies INC Ransom in its follow-up account. ACN associates Titan with an anonymous ICT-provider case. Reporting records Qilin's claim about the cloud case. These propositions have different support and must remain distinct from the wider Ransompedia group totals. [S29][S13][S24]

The report does not independently link every listing under a group label to the same technical operator. It also does not infer that one confirmed incident validates the group's other claims. For incident response, behaviour and affected assets matter more than importing a full profile without matching evidence.

No newly dated 2026 Italian state-linked intrusion is independently established by the limited material used here. That is a coverage statement, rather than a finding that Italy faced no espionage. Historical vendor reporting provides separate context below.

7.6 Espionage context published in 2026

Webworm

Espionage context published in 2026 | China-aligned, as described by ESET

IN ITALY, 2026

May

ESET publishes research on a 2025 campaign that included Italian government targeting

CLAIMED TARGETS

Government bodies in ESET's historical campaign account

SEEN IN PUBLIC REPORTING

[S61] ESET describes the targeting and attribution

[S62] Vendor technical analysis and technique table

OUR ASSESSMENT

ESET's recovery of an Italian government virtual-machine snapshot indicates 2025 access to virtualization management or snapshot storage, without resolving initial entry or establishing a newly dated 2026 Italian intrusion.

CONFIDENCE

As stated by ESET; no new national incident count inferred

ESET's May 2026 publication describes a 2025 campaign including Italian government targeting. ESET attributes it to a group it describes as China-aligned Webworm. Publication in 2026 does not establish a new Italian intrusion during this report's window. [S61]

In ESET's technical account, files recovered from an attacker-used cloud storage bucket included virtual-machine snapshots from an Italian government entity, capturing active machine state and configuration. That evidence indicates access to either the virtualization management plane or a snapshot storage repository, while leaving initial entry and wider network scope unresolved. The vendor-table examples below describe the historical campaign as a whole, rather than techniques independently observed in Italy in 2026. [S62]

TECHNIQUES NAMED IN THE SOURCE RESEARCH, BY TACTIC

Reconnaissance	Execution	Persistence	Command and Control	Exfiltration
T1595.002 Vulnerability scanning	T1059.003 Windows command shell	T1547.001 Registry run keys or startup folder	T1102.002 Bidirectional web-service communication	T1567.002 Exfiltration to cloud storage

Selected entries from ESET's campaign-wide technique table [S62]. This is historical context published in 2026, not a technique inventory observed at Italian organisations during the report window. [S62]

For defenders, snapshot exposure means isolating hypervisor administration, restricting access to backup and snapshot repositories, and rotating credentials or secrets stored inside captured machine states. Our 2026 review covered ACN and CERT-AGID publications, regional CSIRT bulletins, retained underground posts, and public reporting in four languages without finding an independently confirmed 2026 state-linked intrusion in Italy. That boundary reflects public-source visibility rather than an absence of espionage activity; do not assign historical techniques or vendor attribution to a new incident without matching evidence. [S61][S62]

7.7 Web exploitation and phishing require different checks

The January ClickFix bulletin describes abused Italian WordPress sites presenting deceptive verification screens that encourage manual actions. It identifies both known software weaknesses and inadequate administrative access protection as relevant in the observed campaigns. This is campaign-level guidance, not a finding about each candidate organisation. [S19]

A web team should inventory its actual components and supported versions before applying an advisory. A SOC should separately investigate whether a user interacted with the deceptive content and whether identity or endpoint evidence followed. Removing malicious web content and responding to a user's device are different tasks.

A September CSIRT bulletin reports exploitation of Joomla Content Editor for webshell deployment and defacement against organisations in Italy. That source does not establish an incident at any organisation in the selected universe. [S58]

The exact vendor version boundaries are retained below as a technical reference. Use a currently supported release containing the fix, then verify deployment and investigate relevant prior access. [S59][S60]

```
Product: Joomla Content Editor
Identifier: CVE-2026-48907
Affected: versions before 2.9.99.5
First fixed: 2.9.99.5
Wider hardening discussed by vendor: 2.9.99.6
```

The legacy patch notice distinguishes the specific fix from wider hardening in the subsequent release. NVD records the identifier. The first fixed release is a historical boundary, rather than a claim about the latest supported release at cut-off. [S59][S60]

A component inventory should identify the actual installation and owner. Remediation needs authorised verification and review of relevant earlier activity. A successful upgrade does not independently establish that no prior access occurred.

KEY TAKEAWAYS

01

Listing records and group labels measure publications, rather than verified intrusions or operators.

02

Keep each attribution attached to the source supporting that particular case.

03

Match a technical advisory to actual assets before turning it into remediation work.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How do identity information and trusted communications become tools for fraud?

4

decisions: identity proof, session trust, payment authority and customer warning

8.1 Identity information does not grant authority 67
8.2 Public-service themes reach payment information 67
8.3 Mailbox access makes a false payment request more plausible 68
8.4 A weekly campaign count is a campaign count 68
8.5 Police reports add outcomes but retain their own windows 68
8.6 Card material in posts: a narrow view 69
8.7 Prices and services describe offers, rather than transactions 69

CHAPTER 08

The fraud economy

IN SHORT

Official campaigns show requests for identity documents, credentials and payment information, often using familiar public-service or business themes. The documents sought can support further impersonation; the notices do not establish every later fraud. Underground offers add a separate view of demand and advertising. Check what information an attacker could know, protect the decision it could influence, and confirm payment instructions through independently known channels.

8.1 Identity information does not grant authority

A name, address, document image or contract detail can make a conversation credible. It does not establish that the caller owns an account or can approve a payment. The report's fraud recommendations focus on that decision boundary. Customer support, account recovery and finance should test what happens when an attacker already knows routine biographical information.

CERT-AGID's January benefit-themed notice describes collection of identity, income and employment documents. It presents later credit-related misuse as a possible purpose. That distinction matters: a document request is an observed collection attempt, whereas a successfully opened loan would need further evidence. [S18]

For defenders, the next step is to identify which workflow accepts the information as proof. A synthetic test can examine whether support reveals more information, changes a contact route or resets access after receiving plausible documents. Record the process decision and evidence required, without using genuine victims' data.

8.2 Public-service themes reach payment information

The January health-card renewal warning describes campaigns asking for personal data and, in some variants, card details under a delivery-fee pretext. The notice concerns impersonation, not evidence that the health-card service itself suffered an intrusion. The number of campaigns does not measure affected people or successful payments. [S16]

A separate January tax-themed notice describes a counterfeit SPID login. An April regional notice describes another digital-identity renewal lure. Those warnings support a customer-advice programme around familiar service themes. They do not establish that every recipient entered credentials or that an identity provider's infrastructure was accessed. [S15][S22]

A warning should tell people which decision to avoid and which route to use instead. Direct them to an independently known service channel. Avoid forwarding a screenshot containing a working malicious destination. The objective is to reduce a plausible request's authority, rather than to ask every user to recognise every visual detail.

8.3 Mailbox access makes a false payment request more plausible

The February business email compromise bulletin describes credential and one-time-code phishing followed by abuse of business correspondence and lookalike domains. The source is a campaign observation, not an estimate of Italian fraud losses. It supports checking more than the display name on a payment message. [S20]

A genuine invoice conversation can contain a fraudulent payment change. The relevant control is confirmation through a contact route established before the suspicious request. Finance should retain the confirmed payee, approver and callback evidence. An urgent or confidential request should enter the same process, including when it appears to come from an executive.

Identity response should also address the sender's environment. Review session history, recovery settings, delegated access and forwarding changes when a mailbox is implicated. A password reset alone may leave other access or trust relationships unresolved. Validate those conditions through an authorised incident process rather than assuming the bulletin establishes a particular customer's account remains active.

8.4 A weekly campaign count is a campaign count

CERT-AGID's 14-20 March review records 103 malicious campaigns: 66 directed at Italian targets and 37 generic campaigns affecting Italy. False penalty notices accounted for 24 Italy-directed phishing campaigns. Other themes included banking, payments and orders. These figures describe that weekly source population. [S21]

They do not supply a national annual incident total. Several messages can belong to one campaign, and one organisation can receive many messages without an established intrusion. The appropriate operational question is whether the organisation saw the theme, whether anyone interacted and what identity or payment action followed.

A SOC can connect that question to service-desk and fraud records. Preserve the suspected message, determine which account or workflow it touched, and assign closure. The reporting metric should distinguish blocked delivery, user interaction, entered credentials and confirmed misuse. Those are suggested internal categories, not inferred counts from the national notice.

8.5 Police reports add outcomes but retain their own windows

A June Carabinieri statement covers attempted and completed spoofing fraud from November 2025 through May 2026. It reports referrals to prosecutors and recovered funds. The mixed-year population cannot become a count of 2026 incidents. Investigative steps and allegations must remain distinct from convictions. [S38]

July reporting attributes a banking-impersonation investigation to Polizia Postale under a prosecutor's coordination. The source describes precautionary measures, not final judicial findings. The case supports a warning about fraudulent banking contact; it does not establish intrusion into the banks whose identities were invoked. [S39]

Historical enforcement adds another limit. A May Guardia di Finanza statement concerns alleged online fraud in 2022-2025. It belongs in response context, rather than the report's current-incident total. Date precision prevents a successful 2026 investigation from being misread as evidence of fresh 2026 attacks. [S57]

8.6 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

Any card figures in this report concern only payment cards that appeared in clear text in the dark-web posts collected for the report. Brandefense detects stolen cards through other methods outside this report. This view does not measure national card theft or fraud loss.

Within this narrow view, 42 distinct Italy-associated cards appeared in 38 retained posts. This does not establish that a card was active, that an issuer was intruded upon or that fraud occurred. No national theft or loss estimate follows from these observations. Country association does not establish cardholder residence or the location of fraud. Issuers should validate any relevant signal against their own authorisation and customer-protection evidence. [S4]

The operational distinction remains important even when a card-like record is observed. An advertised or printed status does not establish a completed transaction. Issuers should use their own authorisation and fraud evidence to determine whether a particular card needs intervention. Reissue decisions belong to issuer policy and validated risk.

8.7 Prices and services describe offers, rather than transactions

No comparable price series is published from the retained evidence. The report does not infer market value or completed transactions from isolated advertisements. Use the observed product and its validation limit to decide whether a follow-up is justified. [S1]

An automotive-dashboard offer carried a 5,000 USD asking price (B16). That is one advertised price, rather than a completed transaction or a market average. [S1]

A seller's asking price does not establish a completed sale, a buyer's identity or the value of genuine access. A multi-country advertisement can list Italy without identifying an Italian victim. The useful intelligence is the product asserted, the audience sought and the validation needed before an organisation acts.

Where identity, account and payment services appear together, any sequence connecting them remains an analytical model unless concrete evidence links the participants. Similar wording or adjacent posts can show a shared market theme without proving common operators. Avoid turning that model into a named criminal organisation.

KEY TAKEAWAYS

01

Familiar information can support impersonation without conferring authority.

02

Campaigns, document requests, completed fraud and recovered funds remain separate populations.

03

Protect payment changes and account recovery with independently verified approval.

CHAPTER 09

Banking and finance deep dive

THIS CHAPTER ANSWERS

Which banking risks concern employees, customers and payment authority, and who should validate each one?

3

different owners: identity, fraud and treasury

9.1 A measured portfolio with separate populations 72

9.2 A practical triage order 73

9.3 The payment-authority problem reaches senior staff 73

9.4 Separate customer advice from infrastructure claims 73

9.5 Card, account and transfer signals need different evidence 74

CHAPTER 09

Banking and finance deep dive

IN SHORT

Current credential offers are associated with 14 of 25 candidate banking and finance entries. Their domain associations include employee and other devices, alongside historical credentials. Validate current-account relevance, protect customer recovery and verify payment changes. Keep staff access, customer-device associations, card observations and authorised-payment fraud separate. Assign each signal to the team that can verify its current relevance before escalating.

9.1 A measured portfolio with separate populations

When checked, credential offers were associated with 14 of the 25 candidate banking and finance entries. Their domain associations total at least 83,725 devices, including 1,636 employee-associated devices, and 1,662,877 historical credential records. The remaining 82,089 device associations are outside the employee classification; ownership and freshness remain unverified. [S3]

A separate banking subset comprises 12 candidate entries within the 25-entry banking and finance portfolio. Device, credential and card observations do not establish the same person or event. The full portfolio and this subset have different denominators. No bank or sector rating is published. [S3][S4]

Banking subset	Observed count
Candidate entries	12
Entries with card observations	6
Entries associated with current credential offers	10
Employee-device associations	1,546
Other-device associations	60,912

These counts describe the 12-entry subset within the 25-entry candidate banking and finance portfolio. Device totals are minimum observations and can overlap. Card observations do not establish valid cards or completed fraud. [S3][S4]

An issuer should not infer a server intrusion from a customer's malware record. Conversely, apparently customer-side exposure can matter for fraud even when the bank's infrastructure is unaffected. Keep the technical hypothesis and the customer-protection decision separate so that neither team dismisses the other's relevant evidence.

9.2 A practical triage order

First identify whether the signal belongs to an active staff identity, a customer workflow or an unverified advertisement. Staff and privileged access should enter the identity process, including session and recovery checks. Customer evidence should reach fraud and support. A data-sale claim should reach intelligence and incident response for provenance assessment.

Then record what was validated. A disposition should state whether the identity belongs to the organisation, whether evidence is current enough to act on and which remediation already exists. An old password found in a historical list does not establish present access. A current advertisement also needs account-level verification.

Finally define escalation. An active privileged account, unexplained session or unauthorised recovery change deserves incident handling under local policy. An unverified bulk list may instead require monitoring and sample-provenance work through authorised channels. Neither response should be driven solely by an advertised record count.

9.3 The payment-authority problem reaches senior staff

Public reporting in September describes an alleged February fraud at a wealth-management institution using an executive message and a purported professional's voice. Reports give different unrecovered amounts after substantial recovery. This report does not treat the initial transfer figure as final loss or independently verify the reported AI component. [S56]

The naming and factual limits do not remove the decision lesson. A senior request needs the same payee and authority verification as another payment. Confidentiality and urgency should trigger the documented escalation path, rather than permission to skip confirmation. Treasury should know who can stop or recall a payment and how quickly that channel can be reached.

A useful exercise combines a genuine-looking conversation, plausible transaction documents and an unavailable executive. The completion evidence is whether staff used independently known contacts and recorded the required approvals. The exercise should also check whether a second approver independently verifies evidence rather than merely endorsing the first decision.

9.4 Separate customer advice from infrastructure claims

Recent contact and document disclosures can support tailored customer warnings without establishing stolen banking passwords. Explain that criminals might quote genuine information and ask for a new action. Tell customers to use their known app, branch or published service route to verify the request. Do not imply that knowing a contract number grants account access.

Where a company says payment information was not involved, retain that statement as the company's account. If evidence later changes, update the advice and record the basis. A provisional statement should be precise enough to survive that change: the known data categories, the current assessment and the next update route.

Contact-centre teams should have a response for callers worried by a public claim. It should distinguish an organisation-specific incident from a generic country advertisement. Support should avoid confirming additional identity details to an unexpected caller who already knows some accurate information.

9.5 Card, account and transfer signals need different evidence

Card authorisation evidence belongs to the issuer and merchant-payment process. Account recovery belongs to identity and fraud. A business transfer approved after deception belongs to treasury and the relevant fraud process. Joining those records can reveal a sequence, but it does not make them interchangeable units.

An internal review should retain the observed signal, affected service, proposed action and closure evidence. A single dashboard total labelled exposure can hide the distinction between an outdated credential, a current session and a completed payment. Use separate queues with a common escalation owner when evidence connects them.

For financial entities, DORA adds a reporting and resilience framework, discussed in Chapter 10. Its applicability and major-incident test should be checked for the entity and service. A supplier's incident is not automatically a major incident for every financial customer. [S54]

KEY TAKEAWAYS

01

Credential offers associated with 14 of 25 candidate financial entries require account validation.

02

Staff identities, customer fraud and treasury authority need separate validation owners.

03

A realistic payment exercise tests independent confirmation, stop channels and recovery escalation.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which rules apply to the entity, which facts start a clock, and who records the reporting decision?

4

frameworks with different scope and triggers

10.1 Start with applicability 76
10.2 NIS2: awareness and the applicable cohort matter 76
10.3 Public-sector duties require a separate scope check 77
10.4 GDPR separates notification from communication to individuals 77
10.5 DORA is a financial-sector framework 78
10.6 Enforcement lessons remain tied to older events 78
10.7 A designation is different from incident attribution 78
10.8 The reporting matrix should be usable during an outage 79

CHAPTER 10

Regulatory and national response

IN SHORT

Italy transposed NIS2 in 2024. Notification and control obligations depend on the entity's inclusion, cohort and applicable implementation. GDPR concerns personal-data risk; DORA governs relevant financial entities and major ICT incidents. Other public-sector duties also require scope checks. Build an entity-specific matrix, record awareness and assign a substitute reporter before an incident.

10.1 Start with applicability

The table is a reading guide to verified texts, rather than legal advice. The organisation's counsel should confirm current applicability, exclusions and implementing requirements. A country-tagged post alone does not establish a legally significant incident.

Framework	Applies to	Verified point	First action
Legislative Decree 138/2024	Essential and important entities within scope	Italy's NIS2 transposition entered into force on 16 October 2024	Confirm inclusion, entity and relevant services
NIS implementation	Listed entities and their applicable cohort	ACN's guide gives different 2026 and 2027 milestones by cohort	Preserve the inclusion communication and applicable determination
Law 90/2024	Specified public bodies and operators, with exclusions	Article 1 contains incident-reporting duties	Check scope and overlap with other regimes
GDPR	Controllers and processors handling personal data	Risk and high-risk assessments serve different notification decisions	Involve privacy counsel and document the assessment
DORA	Financial entities and arrangements within its scope	Applies from 17 January 2025; major ICT incidents require reporting	Confirm entity scope and competent authority

The source texts are [S50]-[S54]. They do not support one universal reporting clock for all Italian organisations. A multinational group should map legal entities and services, rather than assume its headquarters determines every obligation.

10.2 NIS2: awareness and the applicable cohort matter

Article 25 sets notification stages for significant incidents: pre-notification within 24 hours of awareness, notification within 72 hours, and a final report within one month after notification. It also addresses intermediate reporting, ongoing incidents and a particular trust-service rule. Notifications must be made without undue delay. [S50]

Covered entities notify CSIRT Italia. For significant incidents affecting trust services, Article 25 gives trust-service providers a 24-hour notification rule instead of the ordinary 72-hour notification stage. [S50]

ACN's 2026 guide distinguishes entities listed in 2025 from those listed in 2026. It gives January 2026 and January 2027 notification milestones respectively, with different baseline-control dates. Applicable determinations and an entity's inclusion communication remain necessary to interpret the exact start. Do not substitute a blanket national date. [S51]

The operational preparation is a documented awareness process. Identify who receives supplier reports, customer evidence and SOC findings. Preserve when the organisation learned facts relevant to significance. A later complete forensic account should update the record rather than erase the earlier decision or delay required reporting until all uncertainty disappears.

10.3 Public-sector duties require a separate scope check

Law 90/2024 Article 1 specifies public bodies and operators subject to reporting duties, with exclusions and overlap requiring examination. Its text includes notification stages measured from awareness. It also distinguishes repeated non-compliance within five years when describing the penalty provision. This is not an automatic first-delay fine. [S52]

Under the amended Article 1, use ACN's procedures for both reporting stages. Submit the initial report without delay and within 24 hours of awareness. Submit the complete notification within 72 hours of that same awareness time. Repeated non-compliance within five years attracts a 25,000-125,000 euro penalty under its stated conditions. Scope and exclusions still apply. [S67]

For a public service, identify whether the responsible body, an in-house company or a supplier holds each duty. The service contract should say who supplies incident facts and how quickly. Contractual notice does not replace the organisation's own legal assessment, and a supplier's report should not silently become its customer's completed notification.

A tabletop should test the handoff when the affected system normally holds contacts and evidence. The completion record should show the named reporter, substitute, authority, information available and next update. Legal should validate the matrix before the exercise, rather than while the clock is running.

10.4 GDPR separates notification from communication to individuals

Garante's guidance explains controller notification without undue delay and, where feasible, within 72 hours of awareness, unless risk to individuals is unlikely. Processors promptly inform controllers. Communication to affected individuals uses a high-risk assessment, with applicable exceptions. All personal-data breaches require documentation, including those not notified. [S53]

A June decision about an editorial mailbox illustrates that the regulator's Article 33 and Article 34 assessments can differ. It should not become a rule that every mailbox incident requires identical communications. The decision concerns historical activity and is used here for legal precision, rather than as a current incident. [S43]

Incident response should establish data categories, access, availability, affected services and uncertainty. Privacy counsel then records the risk decision and any update. Confirmed encryption, an unverified sale and a contact-data notice can create different questions; none should receive an automatic template conclusion.

10.5 DORA is a financial-sector framework

DORA applies from 17 January 2025. It covers ICT risk management, testing, incident management and third-party arrangements for entities within scope. Article 19 addresses reporting of major ICT-related incidents to the relevant competent authority. Its sector-specific relationship with NIS2 also requires an applicability check. [S54]

Entities covered by Banca d'Italia's published instructions submit reports through its INFOSTAT platform. Insurance operators should use IVASS's applicable DORA instructions and reporting arrangements. These source-specific routes do not replace an entity-by-entity authority check. [S66][S68]

This report does not import NIS2 or GDPR deadlines into DORA. The relevant financial entity should use its current regulatory matrix, classification process and competent-authority channel. An ICT supplier's incident needs assessment of actual or likely effects on that entity's services, rather than automatic classification from a headline.

10.6 Enforcement lessons remain tied to older events

A 2026 Garante telecom decision concerns incidents notified in February 2025 and support impersonation at retail outlets. Its security lesson concerns access and verification processes; the underlying activity must remain outside a 2026 occurrence total. Payment-related fields in that case also differ from clear-text card observations in posts. [S40]

Other decisions concern a consultancy's 2024 event, a company account of stolen VPN credentials in another historical incident, and legacy/shared-access issues at a healthcare software provider. They offer specific control lessons without establishing that those same routes caused the report's 2026 cases. [S41][S42][S44]

10.7 A designation is different from incident attribution

Council Decision (CFSP) 2026/2546, dated 16 November, adds NoName057(16) to a restrictive-measures annex. The Council's annex describes the group as pro-Russian. This report retains that as the Council's characterisation. The designation does not independently establish responsibility for each Italian event discussed here. [S63]

The decision is recorded as national-context evidence, rather than advice on sanctions implementation. Keep its legal status separate from a claim about a website or a particular operator.

10.8 The reporting matrix should be usable during an outage

Decision	Record	Owner
Is the entity and service within scope?	Applicable regime and exclusion rationale	Legal
When did relevant awareness occur?	Timestamp and supporting facts	Incident commander
What is known about impact?	Services, duration, data categories and uncertainty	Service and privacy owners
What stage is required?	Authority, channel, deadline and next update	Named reporter
What changes the assessment?	New evidence and scheduled review	Incident commander and legal

Keep a copy accessible through an approved route independent of the affected environment. Rehearse the substitute reporter and authority contact. After the exercise, fix missing facts and handoffs rather than merely recording that the meeting occurred.

KEY TAKEAWAYS

01

Scope and cohort come before selecting a reporting clock.

02

Personal-data notification and communication to individuals are separate decisions.

03

Preserve awareness, facts and legal rationale in a usable reporting record.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which developments should change Italy-focused defensive priorities after this snapshot?

5

conditional judgements with explicit change signals

11.1 Key judgements 81

11.2 What would change the assessment 82

11.3 Conditional scenarios for planning 82

11.4 What this report cannot forecast 83

CHAPTER 11

Outlook

IN SHORT

Plan from supported pathways: supplier interruption, identity and payment fraud, availability claims and vulnerable public services. The dataset does not measure the probability of a future attack or the effectiveness of a particular control. Each judgement below identifies the evidence that would change the decision. Review the signal, validate its relevance to your services, and update the plan when the evidence changes.

11.1 Key judgements

Judgement	Confidence	Basis and limit	Owner
Recovery independence deserves priority for important services	High for decision value	Several confirmed cases document interruption; no national prevalence estimate	Continuity and service owner
Contact and identity data can support credible impersonation	High for the mechanism	Official collection campaigns and recent disclosures; downstream misuse not established in every case	Fraud and support
A visible claim needs rapid service validation	High	Official and claimant accounts use different measures; timing alone cannot settle impact	SOC and communications
New organisation-specific session evidence warrants prompt identity review	Conditional	Depends on ownership, freshness and current account state	Identity and response
New critical-service intrusion reports could change sector priorities	Conditional	Current case coverage is partial; undisclosed incidents remain invisible	CISO and intelligence

Confidence attaches to each proposition, not to an actor or sector. High confidence in the need for a restoration test does not imply a quantified probability of ransomware. A conditional judgement becomes operational only when the specified evidence is relevant to the organisation.

11.2 What would change the assessment

Current interpretation	New evidence	Decision changed
A seller's dataset remains unverified	Authorised validation ties it to a current system or the organisation confirms access	Incident, privacy and customer-protection response
A website claim has unclear operational effect	Provider and service-owner records confirm sustained user impact	Mitigation capacity and continuity priorities
A supplier incident has a bounded dependency	Further supported customer or service effects appear	Dependency mapping and recovery scope
An identity record could be historical	Current session, active account or unauthorised recovery change is confirmed	Session revocation and incident escalation
A physical-control story has unclear cause	Operator readings and access evidence support unauthorised interference	Safety, isolation and specialist response
A case remains unattributed	A credible technical or official account publishes supporting links	Actor assessment and relevant hunts

A changed label should follow a changed evidential proposition. Record what was added and what remained unresolved. This prevents a dramatic new headline from replacing a more precise service or identity assessment without supporting facts.

11.3 Conditional scenarios for planning

Supplier interruption. If a critical supplier reports encryption or loss of a shared service, activate dependency mapping and the tested alternative route. Seek customer-specific impact and restoration evidence. The scenario does not assume every customer is affected or that the claimant's stolen-data figure is accurate.

Identity disclosure. If a newly observed dataset contains credible current customer or contract information, prepare fraud and support guidance while authorised validation continues. Do not wait for a complete attribution to protect an exposed workflow. Preserve uncertainty about origin and affected population in public statements.

Availability campaign. If actor channels publish a target list relevant to the organisation, check mitigation readiness and the alternative status channel. Validate actual user journeys and provider observations. Do not declare a sustained outage from a single failed website check or an actor's screenshot.

Payment impersonation. If a request changes payee details or invokes urgency and secrecy, use the independent confirmation process and escalation contact. A familiar sender, convincing voice or genuine document should not bypass that process. The signal is the requested authority change, not a guess about whether AI was used.

Physical-control concern. If process readings change unexpectedly or vendor access cannot be explained, use the approved safe-state procedure and preserve access evidence. The process owner decides operational safety. Intelligence assesses claims separately and should not delay safety action while seeking attribution.

11.4 What this report cannot forecast

The report cannot derive attack probability, financial loss or control effectiveness from post counts. An increase in listings can reflect publishing choices and visibility. A decline in observed posts can reflect source coverage. A newly public investigation can reveal older activity. These alternatives remain relevant after the snapshot.

The appropriate planning horizon is the next decision and its evidence. Maintain the owner, signal, action and closure record. Review it after a relevant disclosure, a supplier change or a restoration exercise. A fixed calendar alone should not decide whether the risk assessment changed.

KEY TAKEAWAYS

01

Plan around supported pathways and the service decisions they affect.

02

Every judgement needs a signal that could change it.

03

Post and listing counts do not supply forecasts of loss or attack probability.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who should do what in the next 90 days, and how will completion be demonstrated?

20

actions with owners and evidence of completion

12.1 The sequence 85

12.2 What counts as completion 87

12.3 First decisions by role 88

12.4 Avoid controls that solve the wrong proposition 89

12.5 How Brandefense can help 89

CHAPTER 12

Action plan

IN SHORT

Start with evidence intake, reporting ownership and a tested important service. Then address identity sessions, customer recovery, payment authority and supplier dependencies. Use current organisation-specific findings immediately; the schedule is not a reason to defer incident response. By day 90, give the board completion evidence and named owners for remaining gaps.

12.1 The sequence

The table proposes a sequence for programme work. A current material threat belongs in the organisation's incident process immediately. Deadlines here are suggested management targets, rather than claims about statutory timing.

1Days 1-30		
Confirm intake for relevant listings, session evidence and supplier notices	OWNER CISO and intelligence	COMPLETION EVIDENCE Source, queue and substitute owner recorded; one test alert received
Map one important service through identity, hosting, support and recovery dependencies	OWNER Service and continuity owners	COMPLETION EVIDENCE Approved map with external dependencies and contact routes
Name incident reporter, substitute and legal applicability owner	OWNER CISO and legal	COMPLETION EVIDENCE Reporting matrix approved for each relevant entity
Validate current organisation-specific identity evidence before disruptive action	OWNER Identity and response	COMPLETION EVIDENCE Dated disposition, ownership and remediation record
Review unexplained sessions, forwarding and recovery changes for implicated accounts	OWNER Messaging and SOC	COMPLETION EVIDENCE Investigation record and justified containment decisions

Confirm a usable public-status route independent of the main website

OWNER
Communications

COMPLETION EVIDENCE
Approved message template and tested alternative channel

Identify public-service software and apply supported security updates

OWNER
Infrastructure and web owners

COMPLETION EVIDENCE
Version inventory and authorised verification of remediation

2Days 31-60

Run a timed restoration of the important service, including customer workflow

OWNER
Infrastructure and service owner

COMPLETION EVIDENCE
Business acceptance and recovery-time comparison

Check recovery access independence from production identities

OWNER
Identity and continuity

COMPLETION EVIDENCE
Access review, approved recovery route and test result

Require independent confirmation of changed payees and payment instructions

OWNER
Finance and treasury

COMPLETION EVIDENCE
Procedure and authorised simulated request caught

Test customer recovery against an attacker with plausible personal information

OWNER
Fraud and support

COMPLETION EVIDENCE
Weaknesses recorded, corrected and retested

Prioritise phishing-resistant authentication for privileged and remote access

OWNER
Identity

COMPLETION EVIDENCE
Coverage and approved exception plan by user group

Inventory legitimate email senders before strengthening domain authentication

OWNER
Messaging

COMPLETION EVIDENCE
Sender owners, alignment evidence and staged change plan

Exercise website mitigation with the provider and real service checks

OWNER
Network and provider liaison

COMPLETION EVIDENCE
Mitigation record and verified user journey

Require customer-specific incident and recovery information from key suppliers

OWNER

Procurement and service owner

COMPLETION EVIDENCE

Contract or operating agreement with contacts and acceptance criteria

Review vendor access to physical-control systems with process owners

OWNER

Operations and safety

COMPLETION EVIDENCE

Approved access paths, monitoring and safe-state procedure

3Days 61-90

Reconcile offline and restored records in the service exercise

OWNER

Business and data owners

COMPLETION EVIDENCE

Exception list closed or assigned with dated acceptance

Run a reporting and communications tabletop with incomplete evidence

OWNER

Incident commander and legal

COMPLETION EVIDENCE

Awareness record, reporting rationale and timed updates

Test a senior payment request using plausible documents and urgency

OWNER

Finance and fraud

COMPLETION EVIDENCE

Independent approvals and stop-channel evidence

Report completed tests, exceptions and remaining owners to the board

OWNER

CISO

COMPLETION EVIDENCE

Evidence-linked board paper and dated follow-up decisions

12.2 What counts as completion

A policy document is useful only when the decision can be carried out. Evidence intake needs a tested alert. Restoration needs service-owner acceptance. A payment rule needs a simulated request that follows the approval path. A reporting matrix needs a timed exercise with incomplete facts.

The board should distinguish completed work from an accepted exception. An exception needs a reason, owner, compensating arrangement and review date. A supplier's promised improvement should remain open until its completion evidence arrives. Programme reporting should preserve that difference rather than treating all planned actions as closed.

Measure	Suggested completion criterion
Relevant evidence intake	A test reaches the accountable queue and substitute
Current identity evidence	Every retained organisation-specific item has a dated disposition
Service restoration	Business workflow passes within its approved recovery objective, or a fix is owned
Payment changes	Independent confirmation is demonstrated in an authorised test
Customer recovery	Synthetic impersonation attempts produce the approved outcome
Supplier recovery	Customer-specific facts and acceptance criteria are available
Incident reporting	Applicable entity, awareness record, reporter and update route are demonstrated
Communications	Claim, established effect and user action remain distinct

These are recommended acceptance criteria. They are not measurements of the current controls at the selected organisations. Each organisation should adapt them to its service criticality, policy and legal obligations.

12.3 First decisions by role

Role	First decision	Evidence to request
Board	Which service requires demonstrated recovery first?	Dependency map and business acceptance test
CISO	Who receives evidence and can escalate it?	Working intake and accountable queue
SOC	Which claim or signal can we validate now?	Provider, identity and service-owner records
Identity	Which account, session and recovery state is relevant?	Ownership, validity and authorised containment record
Fraud	Which customer decision can exposed information influence?	Recovery and contact-centre test results
Treasury	Who independently confirms payment authority?	Callback and approval evidence
Legal	Which entity and regime apply to the facts?	Applicability matrix and awareness chronology

Role	First decision	Evidence to request
Communications	What service state can be stated now?	Owner-verified status and next update route
Operations	Which physical state needs safe handling?	Process-owner readings and approved access paths

12.4 Avoid controls that solve the wrong proposition

Do not order a broad password reset solely because a seller advertised contact data. First establish whether credentials or sessions are implicated. Do not accept a restored website as proof that a critical workflow works. Test the workflow. Do not treat an actor's screenshot as final attribution or a complete impact assessment.

Similarly, a stronger email policy does not prevent every lookalike-domain message or a request from an already abused mailbox. Keep identity, payment and customer-process controls in the plan. The report's recommendations are complementary because the evidence describes more than one route to harm.

A physical-control concern requires a process owner, even when intelligence cannot confirm its actor. A legal reporting decision requires relevant facts and scope, even when forensic work continues. Align the owners around the decision they can verify, rather than waiting for one total narrative to settle everything.

12.5 How Brandefense can help

Brandefense can help teams relate external threat information to the domains, brands and services they manage. This report uses observed posts, public ransomware listings and verified reporting to identify questions requiring validation. It does not promise that every criminal assertion can be verified or that historical credentials remain usable.

Use a discussion with Brandefense to define the evidence your team needs, how it reaches accountable owners and which existing response process receives it. Bring service dependencies, identity boundaries and customer-fraud concerns. The useful outcome is an agreed evidence-to-action workflow, with clear limits and completion criteria.

Request a demo

KEY TAKEAWAYS

01

Establish working evidence intake and reporting ownership first.

02

Demonstrate recovery, independent payment approval and customer protection through tests.

03

Report completed evidence and owned exceptions, rather than policy completion alone.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

What evidence supports this edition, and where do the boundaries matter?

4

separate populations: posts, listings, candidate portfolio entries and reported cases

Appendix A. Sources, scope and confidence 91

Appendix B. Evidence register 94

Appendix C. Sources 96

Appendix D. Glossary 100

Appendix A. Sources, scope and confidence

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

A.1 Window and snapshot

The main window is 1 January-22 November 2026 by post publication time. Observations stop at the collection snapshot on 22 November, rather than the end of that day. The recent section covers 9-22 November to that snapshot. Incident occurrence and publication dates remain separate.

Official reports, regulator decisions and recovery statements can concern older events. Those items are labelled as historical or disclosure context. They do not become current intrusions because their statements were published in 2026. Follow-up notices update an existing case unless separate evidence establishes another event.

A.2 Own-source populations

Country-tag counts describe 802,371 posts. Retained forum material contains 839 Italy-tagged posts reviewed separately, including the 195-post recent subset for 9-22 November 2026. Seventeen selected excerpts illustrate demand, advertising and claims. The selected excerpts do not estimate the frequency of each theme across the complete tag-count population. [S1]

Ransompedia contributes country-associated listing records. Italy's 286 records and 270 distinct victim-name values are different units. Neither establishes a count of verified intrusions or a census of extortion. Group labels and publishing dates retain the source's meaning. Regional comparisons use the same source while preserving population and coverage limits. [S2]

The 250-entry candidate portfolio is selected for role. Its national Atlas headline is 57 out of 100. When checked, credential offers were associated with 132 candidate entries. Device and credential associations overlap. Domain response does not establish ownership or organisational independence. Passive-control measurements remain unavailable. [S3]

A.3 Public-source cases

The public sweep considered official cyber notices, public statements, reporting, regulator decisions and judicial-response material. Source passages used as facts were read. Direct statements, official documents reproduced elsewhere and company statements quoted by press retain different descriptions in the report.

Research considered Italian, English, Russian and Turkish material. The source view remains incomplete, particularly for some agency archives and organisation-specific coverage. This report does not claim a complete national census. An absent case is not evidence that no incident occurred.

Parliamentary questions require particular care. Their preambles can repeat allegations and press accounts. They are not automatically findings by the government or affected body. A ministerial answer is a different evidence type. The report preserves that distinction in the refrigeration discussion and technical-outage exclusion.

A.4 Cards and relationships

B references reproduce short redacted excerpts from retained posts. Omissions and removed identifiers appear in brackets. P references identify public-source case paraphrases, including campaign examples and an exclusion. A P reference is not an authentic actor quotation.

A shared posting alias supports a posting association. Similar titles, credit to another alias or overlapping fields do not establish file identity, authorship, common operators or a completed sale. Relationship maps label supporting evidence. Broader fraud sequences are analytical models unless a concrete link is shown.

A.5 Card material

Any card material is limited to payment cards appearing in clear text in posts collected for this report. Brandefense detects stolen cards through other methods outside this report. This population does not measure national card theft, active cards or fraud loss. Issuer action requires the issuer's own validation. [S4]

A.6 Confidence and alternatives

High confidence can describe a retained publication or an official statement's wording without validating the underlying criminal assertion. Medium confidence describes an interpretation with a supporting line and a stated alternative. Unverified means not independently established; it does not mean fabricated or confirmed.

A confirmed incident can retain unknown actor identity, extraction scope or initial access. A restored service can retain unresolved data questions. A claim can be relevant to monitoring without establishing intrusion. The report keeps those propositions separate in summaries, cards, figures and recommendations.

A.7 Naming and data protection

Victim names are used only where the package records official confirmation and wide reporting. Otherwise descriptions remain broad enough to fit several organisations. Source paths naming a withheld victim are replaced by publisher roots, with the article address withheld. Exact source mapping remains in the private evidence record.

Actor aliases appear only where needed to explain evidence. Contacts, personal information, victim identifiers and working offensive material are excluded. The report makes no claim that Brandefense sent a notification unless a dated record establishes it.

A.8 Comparing future editions

Future editions must state their own population, date and denominator. A candidate domain remains a candidate entry until validated by organisation-specific evidence. A new official confirmation updates the relevant case without changing the historical observation date.

Summary figures, tables, evidence cards and charts use the same snapshot populations across the English and Italian editions.

Appendix B. Evidence register

B.1 Retained post excerpts

These B references are redacted post evidence. Posting dates do not establish intrusion dates. Held and Not established statements in the cards define the supported proposition.

Card	Posted	Venue	Alias	Language	Chapter
B01	2026-02-10	Forum	kurkenluvsdh	English	4
B02	2026-04-18	Forum	Jiskaa	English	4
B03	2026-01-27	Forum	exelo	English	4
B04	2026-08-19	Forum	Jaded	English	4
B05	2026-06-04	Forum	Forum bot	English	4
B06	2026-08-20	Forum	MegaCloud	English	4
B07	2026-09-28	Forum	updap	English	4
B08	2026-10-18	Forum	updap	English	4
B09	2026-08-06	Forum	wizard	English	4
B10	2026-11-11	Forum	Linda2000	English	4
B11	2026-02-02	Forum	Tanaka	English	4
B12	2026-04-02	Forum	Forum seller	English	4
B13	2026-05-18	Forum	Forum seller	English	4
B14	2026-05-14	Forum	Forum seller	English	4
B15	2026-04-26	Forum	Forum seller	English	4
B16	2026-01-30	Forum	Forum seller	English	4
B17	2026-06-06	Spanish-language relay channel	Channel relay	Spanish	6

B.2 Public-source cases and exclusions

P references identify source-based analysis, rather than underground quotations. The date column distinguishes an event from a publication or follow-up where needed.

Reference	Date	Role	Evidence type	Chapter
P01	2026-02-01; follow-up 2026-04-09	University	Confirmed incident and recovery notice	5
P02	2026-03-23; April reporting	Cloud and municipal workflow	Company-acknowledged interruption and claim	5
P03	February; April reporting	Museum administration	Incident and disputed later allegations	5
P04	August; 2026-09-16 notice	Water utility	Official business-restoration statement	5
P05	2026-08-31; September notices; follow-up 2026-11-17	Healthcare group	Direction statements and privacy follow-up reported by press	5
P06	2026-11-17 notice	Consumer cooperative	Direct contact-access statement	5
P07	2026-11-19 reporting	Document service	Company confirmation quoted by press	5
P08	October event; November disclosure	Transport project	Company statement quoted by press	5
P09	August operational report	ICT provider	Anonymous official case account	5
P10	2026-01-27 notice	Public mail users	Official campaign observation	5
P11	2026-01-30 notice	Identity-document recipients	Official campaign observation	5
P12	2026-05-06; June answer	Judicial IT service	Technical outage excluded from cyber count	5

B.3 Counting the examples

The report contains eighteen case cards: six underground cases and twelve public-source references. The latter include nine incident-related cases, two campaign cases and one exclusion. An anonymous official case can still have an imprecise date. These are case-study counts, not a national incident total.

The private coverage record retains additional mentions, historical context and excluded candidates with reasons. A reported follow-up can share the same incident key as an earlier notice. A publication date alone is not sufficient to create a new incident entry.

Appendix C. Sources

Source numbers that do not appear were retired during review and are not cited.

S1: Odin by Brandefense, Italy-tagged post counts and retained forum observations, publication dates 1 January-22 November 2026, collection snapshot 22 November 2026. Own data; no public source address.

S2: Brandefense Ransompedia, Italy and regional comparison listing records, extracted 22 November 2026. Own data; no public source address.

S3: Brandefense Atlas exposure ratings, Blackhole domain associations, selected candidate-entry portfolio and initial public-domain observations, 21-22 November 2026. Passive-control measurements unavailable. Own data; no public source address.

S4: Odin by Brandefense, narrow card-material review of retained posts, 22 November 2026. Own data; no public source address.

S5: Sapienza Università di Roma, "Chiusura dell'incidente informatico dello scorso febbraio", 9 April 2026. https://www.uniroma1.it/it/node/538826. Verified on 22 November 2026.

S6: ANSA, "Attacco hacker all'università La Sapienza di Roma", 2 February 2026. https://www.ansa.it/amp/canale_legalita_scuola/notizie/mur/2026/02/02/attacco-hacker-alluniversita-la-sapienza-di-roma_5bce4cb1-c3a0-45bc-a888-8b8eed713b7c.html. Verified on 22 November 2026.

S7: Unicoop Firenze, official incident press note, 17 November 2026. https://www.coopfirenze.it/news-e-media/comunicati-stampa/nota-stampa. Verified on 22 November 2026.

S8: Unicoop Firenze, security information and incident questions. https://www.coopfirenze.it/news-e-media/sicurezza. Verified on 22 November 2026.

S9: ANSA, report of Unicoop Firenze's incident statement and membership context, 17 November 2026. https://www.ansa.it/toscana/notizie/2026/11/17/attacco-hacker-a-banca-dati-unicoop-firenze-coop-con-12-milioni-di-soci_9dbd5b8d-512c-4d76-bf30-171f84b4a9ac.html. Verified on 22 November 2026.

S10: ACN, Operational Summary febbraio 2026, official-authored report first published on 26 March 2026 and reproduced in its March 2026 revised file by Cybersecitalia. https://www.cybersecitalia.it/wp-content/uploads/2026/03/Operational_Summary_feb26_CLEAR_rev.pdf. Verified on 23 November 2026.

S11: Associated Press, "Italy averted Russian-linked cyberattacks targeting Winter Olympics websites, foreign minister says", 4 February 2026. https://apnews.com/article/italy-winter-olympics-us-cyberattacks-security-01b6af8e64606f31836c91faa6653d12. Verified on 22 November 2026.

S12: Foreign ministry, official notice on mitigated website attacks, 8 October 2026. https://www.esteri.it/it/sala_stampa/archivionotizie/comunicati/2026/10/la-farnesina-respinge-nuovi-tentativi-di-attacchi-informatici-al-proprio-sito-e-alle-infrastrutture-nazionali/. Verified on 22 November 2026.

S13: ACN, Operational Summary agosto 2026, official-authored report reproduced by Cybersecitalia. https://www.cybersecitalia.it/wp-content/uploads/2026/09/Operational_Summary_ago26_CLEAR.pdf. Verified on 22 November 2026.

S14: ACN, Operational Summary maggio 2026, official-authored report reproduced by Cybersecitalia. https://www.cybersecitalia.it/wp-content/uploads/2026/06/Operational_Summary_mag26_CLEAR.pdf. Verified on 22 November 2026.

S15: CERT-AGID, tax-brand impersonation seeking SPID credentials, 20 January 2026. https://cert-agid.gov.it/news/sfruttato-il-logo-di-ade-per-una-campagna-di-phishing-mirata-al-furto-di-credenziali-spid/. Verified on 22 November 2026.

S16: CERT-AGID, renewed health-card-expiry phishing campaigns, 22 January 2026. https://cert-agid.gov.it/news/ancora-una-campagna-di-phishing-su-scadenza-tessera-sanitaria-breve-sintesi-del-contesto/. Verified on 22 November 2026.

S17: CERT-AGID, public-administration mailbox abuse and credential phishing using a collaboration platform, 27 January 2026. https://cert-agid.gov.it/news/sfruttate-utenze-della-pa-compromesse-per-tentare-il-furto-di-credenziali-microsoft-365-tramite-figma/. Verified on 22 November 2026.

S18: CERT-AGID, benefit-themed smishing collecting income and employment information, 30 January 2026. https://cert-agid.gov.it/news/smishing-a-tema-inps-finiscono-nel-mirino-anche-i-dati-del-cud-e-le-informazioni-lavorative/. Verified on 22 November 2026.

S19: CSIRT Toscana, official republication of CSIRT-ITA bulletin on ClickFix and abused WordPress sites, 27 January 2026. https://csirt.regione.toscana.it/clickfix-portali-wordpress-vulnerabili-utilizzati-per-distribuire-codice-malevolo-bl01-260127-csirt-ita/. Verified on 22 November 2026.

S20: CSIRT Toscana, official republication of CSIRT-ITA business email compromise bulletin, 17 February 2026. https://csirt.regione.toscana.it/thread-hijacking-rilevate-attivita-malevole-che-utilizzano-tecniche-di-business-email-compromise-bl01-260217-csirt-ita/. Verified on 22 November 2026.

S21: CERT-AGID, weekly campaign review for 14-20 March 2026. https://cert-agid.gov.it/news/sintesi-riepilogativa-delle-campagne-malevole-nella-settimana-del-14-20-marzo/. Verified on 22 November 2026.

S22: CSIRT Umbria, digital-identity phishing warning, 23 April 2026. https://csirt.regione.umbria.it/novita/cybersecurity-alert-14/. Verified on 22 November 2026.

S23: ANSA, museum administrative incident and disputed later security allegations, 3 April 2026. Article URL withheld to protect victim identity. https://www.ansa.it/. Verified on 22 November 2026.

S24: Cybersecitalia, report quoting a cloud provider's incident acknowledgement, 27 March 2026. Article URL withheld to protect victim identity. https://www.cybersecitalia.it/. Verified on 22 November 2026.

S25: ANSA, cloud-provider interruption and municipal payment-service investigation, 1 April 2026. Article URL withheld to protect victim identity. https://www.ansa.it/. Verified on 22 November 2026.

S26: Alto Calore, "Siamo tornati", 16 September 2026. Wide-reporting checks include Tom's Hardware, 14 September, and Irpiniaoggi, 28 September. https://altocalore.it/siamo-tornati/. Verified on 22 November 2026.

S27: Nordestnews, healthcare Direction's incident statement reproduced on 3 September 2026. Article URL withheld to protect victim identity. https://www.nordestnews.it/. Verified on 22 November 2026.

S28: Rai, healthcare service interruption and manual-work reporting, September 2026. Article URL withheld to protect victim identity. https://www.rainews.it/. Verified on 22 November 2026.

S29: Trieste Cafe, healthcare Direction's recovery update reproduced on 10 September 2026. Article URL withheld to protect victim identity. https://www.triestecafe.it/. Verified on 22 November 2026.

S30: l'Adige, transport-project company incident statement and investigation, November 2026. Article URL withheld to protect victim identity. https://www.ladige.it/. Verified on 22 November 2026.

S31: Cybersecurity360, company-confirmed document-related incident and fraud-risk reporting, 19 November 2026. Article URL withheld to protect victim identity. https://www.cybersecurity360.it/. Verified on 22 November 2026.

S32: Fanpage, company confirmation and journalists' observations of contract and identity material, November 2026. Article URL withheld to protect victim identity. https://www.fanpage.it/. Verified on 22 November 2026.

S34: Camera dei deputati, parliamentary questions concerning reported refrigeration incidents. Preambles are questioners' statements. (article URL withheld). https://www.camera.it/ Verified on 22 November 2026.

S35: Rai, manager account of changed refrigeration temperatures without confirmation of cyber cause, 3 November 2026. Article URL withheld to protect victim identity. https://www.rainews.it/. Verified on 22 November 2026.

S36: L'Espresso, school-threat messages and the distinction from system intrusion, 13 November 2026. https://lespresso.it/c/innovazione/2026/11/13/attacchi-informatici-scuole-allarmi-bomba-educazione-digitale-in-italia/65911. Verified on 22 November 2026.

S38: Carabinieri, official digital-fraud investigation statement, 3 June 2026; underlying activity November 2025-May 2026. https://www.carabinieri.it/in-vostro-aiuto/informazioni/comunicati-stampa/truffe-digitali-operazione-nella-capitale-44-denunce-e-1-milione-di-euro-recuperato. Verified on 22 November 2026.

S39: ANSA, Polizia Postale banking-impersonation investigation under prosecutor coordination, 3 July 2026. https://www.ansa.it/puglia/notizie/2026/07/03/si-spacciavano-per-operatori-bancari-truffando-utenti-18-arresti_c2db0c8e-daef-4ca2-83c5-f5c8d4cb890f.html. Verified on 22 November 2026.

S40: Garante, 2026 decision concerning telecom incidents notified in February 2025 (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

S41: Garante, 2026 decision concerning an April 2024 consultancy incident (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

S42: Garante, 2026 decision concerning a historical engineering-consultancy incident (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

S43: Garante, 2026 decision on a historical editorial-mailbox incident and reporting duties (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

S44: Garante, 2026 decision on a historical healthcare-software incident (article URL withheld). https://www.garanteprivacy.it/ Verified on 22 November 2026.

S45: La Repubblica, rail-customer notification reporting concerning late-2025 activity, 26 June 2026. Article URL withheld to protect victim identity. https://www.repubblica.it/. Verified on 22 November 2026.

S46: Camera dei deputati, published ministerial answer on a supplier technical fault affecting judicial services, 26 June 2026. https://documenti.camera.it/leg19/resoconti/assemblea/html/sed0682/leg.19.sed0682.allegato_b.pdf. Verified on 22 November 2026.

S49: ACN, Operational Summary ottobre 2026, official-authored document published 20 November and read through its reproduced source text. https://media.agenziagiornalisticaopinione.it/2026/11/Operational_Summary_ott26_CLEAR.pdf. Verified on 22 November 2026.

S50: Gazzetta Ufficiale, Legislative Decree 138/2024, including Article 25; Italy's NIS2 transposition. https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/sg. Verified on 22 November 2026.

S51: ACN, Vademecum NIS, September 2026 edition, official-authored guide reproduced by Sistema FairPlay. https://www.sistemafairplay.it/pdf/news/VademecumNIS_2026_v1.pdf. Verified on 22 November 2026.

S52: Gazzetta Ufficiale, Law 90/2024, Article 1. https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.codiceRedazionale=24G00108&art.dataPubblicazioneGazzetta=2024-07-02&art.flagTipoArticolo=0&art.idArticolo=1&art.idGruppo=1&art.idSottoArticolo=1&art.idSottoArticolo1=10&art.progressivo=0&art.versione=1. Verified on 22 November 2026.

S53: Garante, official guidance on personal-data breach notification and communication. https://www.garanteprivacy.it/data-breach. Verified on 22 November 2026.

S54: EUR-Lex, Regulation (EU) 2022/2554, Digital Operational Resilience Act. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng. Verified on 22 November 2026.

S56: ANSA, report on alleged executive-payment fraud, prosecutor investigation and differing recovery figures, 25 September 2026. Article URL withheld to protect victim identity. https://www.ansa.it/. Verified on 22 November 2026.

S57: Guardia di Finanza, online-fraud enforcement statement concerning alleged 2022-2025 activity, 25 May 2026. https://www.gdf.gov.it/it/gdf-comunica/notizie-ed-eventi/comunicati-stampa/anno-2026/maggio/truffe-online-e-carte-di-credito-clonate. Verified on 22 November 2026.

S58: CSIRT Toscana, official republication of CSIRT-ITA bulletin on Joomla Content Editor exploitation and Italian defacement, 17 September 2026. https://csirt.regione.toscana.it/joomla-jce-rilevato-sfruttamento-cve-2026-48907-al-fine-di-distribuire-webshell-utilizzate-per-defacement-bl01-260917-csirt-ita/. Verified on 22 November 2026.

S59: Joomla Content Editor, vendor fix and legacy security-patch notices, June 2026. https://www.joomlacontenteditor.net/news/jce-pro-2-9-99-5-released and https://www.joomlacontenteditor.net/downloads/editor/security-patch/security-patch-for-jce-2-7-x-to-2-9-x. Verified on 22 November 2026.

S60: NIST National Vulnerability Database, CVE-2026-48907; official record checked for this review. https://nvd.nist.gov/vuln/detail/CVE-2026-48907. Verified on 22 November 2026.

S61: ESET, research press notice on Webworm European government targeting; 2026 publication concerning 2025 activity. https://www.eset.com/us/about/newsroom/research/eset-research-china-aligned-webworm-european-governments-targeted/. Verified on 22 November 2026.

S62: ESET WeLiveSecurity, "Webworm: New burrowing techniques"; historical campaign analysis and vendor technique table. https://www.welivesecurity.com/en/eset-research/webworm-new-burrowing-techniques/. Verified on 22 November 2026.

S63: Council of the European Union, Council Decision (CFSP) 2026/2546, dated 16 November 2026, restrictive-measures annex. https://publications.europa.eu/resource/cellar/c1d158d5-e1a2-11f1-aefc-01aa75ed71a1.0006.01/DOC_1. Verified on 22 November 2026.

S64: Rai, regional health executive's account of earlier booking-system abnormal activity and countermeasures, 16 November 2026. https://www.rainews.it/ (article URL withheld). Verified on 22 November 2026.

S65: ANSA, report corroborating ACN's October operational figures, 20 November 2026. https://www.ansa.it/sito/notizie/cronaca/2026/11/20/agenzia-cyber-ad-ottobre-rilevati-473-account-di-istituzioni-compromessi_cf5ebefa-c41a-43c7-9d2d-b1441db9abaa.html. Verified on 22 November 2026.

S66: Banca d'Italia, instructions for major ICT incidents and significant cyber threats under DORA. https://www.bancaditalia.it/compiti/vigilanza/dora-incidenti/index.html. Verified on 22 November 2026.

S67: Ministry of Economy and Finance, amended Law 90/2024 Article 1, in force from 10 October 2025. https://def.finanze.it/DocTribFrontend/executePrintArticolo.do?articolo=Articolo+1&codiceOrdinamento=0000000000000010000000000000

Appendix D. Glossary

- **Account recovery:** the process for regaining access after losing a password, device or other sign-in factor.
- **Actor claim:** an assertion by a seller or claimant that has not been independently established.
- **Affected population:** the people, accounts or organisations supported by the evidence for a particular event.
- **Business email compromise:** deception using business communications to obtain an unauthorised payment or another business action.
- **Candidate universe:** a selected list requiring further validation before measurements describe confirmed organisational boundaries.
- **Combolist:** a list of email-address or username and password pairs. [S70]
- **Country tag:** a label associating a post with a country; it does not establish hostile targeting.
- **Credential:** information used to sign in, such as a username and password.
- **DDoS:** distributed denial of service, using traffic from multiple sources to disrupt availability.
- **DMARC, SPF and DKIM:** email-authentication standards supporting checks on permitted senders and domain use.
- **DNSSEC:** signatures supporting verification of DNS information.
- **DORA:** the EU Digital Operational Resilience Act for entities and arrangements within its financial-sector scope.
- **Exposure rating:** a summary assessment that requires a defined source population and does not itself establish intrusion.
- **Exfiltration:** unauthorised removal of information; an advertisement alone does not establish it occurred.
- **GDPR:** the EU General Data Protection Regulation.
- **HSTS:** a website instruction telling supporting browsers to use encrypted HTTPS connections.
- **Identity proofing:** checking that a person is the person they claim to be.
- **Listing:** a published extortion or data claim, which can remain unverified or repeat earlier material.
- **MFA:** authentication using more than one factor.
- **NIS2:** the EU network and information security directive transposed in Italy through Legislative Decree 138/2024.
- **Phishing:** deceptive messages or pages seeking information, access or a harmful action.
- **Phishing-resistant authentication:** sign-in designed to bind authentication to the legitimate service rather than a copied page.
- **Ransomware:** malicious software used to restrict access to systems or information, commonly in an extortion attempt.
- **RDWEB:** Remote Desktop Web Access, a web portal for remote desktop access. [S72]
- **Recovery objective:** the business-approved target for restoring a service or limiting data loss.
- **Relay:** a third party repeating an actor's or another source's assertion.

- **Session:** an authenticated period of access that can remain relevant after a password changes.
- **Snapshot:** the point in time at which the observations for an edition stop.
- **SPID:** Italy's public digital-identity system.
- **Stealer log:** a record of login details captured by information-stealing malware on an infected device. [S69]
- **Tenant administration:** management of an organisation's environment within a cloud service. That environment is the tenant. [S73]
- **TLP:CLEAR:** information that may be shared without restriction under the Traffic Light Protocol, subject to other applicable duties.
- **TLS:** the protocol supporting encrypted network connections and server-certificate checks.
- **Webshell:** server-side code enabling unauthorised remote actions; the report provides no working example.

About this report

Prepared by Odin by Brandefense for the Brandefense Country Report · Italy 2026 series. Version 1.0 was first published on 22 November 2026 and revised on 23 November 2026; it records observations through the collection snapshot on 22 November 2026. The main post-time window begins on 1 January 2026. The recent section covers 9-22 November to that snapshot.

The report keeps observations, claims, source attribution and analyst interpretation separate. It does not estimate all cybercrime affecting Italy. Its recommendations describe work an organisation can validate; they do not assert that every organisation currently lacks those controls. The national Atlas headline describes the selected portfolio. Passive-control measurements remain unavailable in this edition.

The Italian edition is translated from the English master with AI assistance and carries the notice "Tradotto con l'IA". The English edition prevails where meanings differ.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO