BRANDEFENSE COUNTRY REPORT · SWEDEN 2026

Brandefense Sweden Cyber Threat Landscape Report 2026

Identity, supplier exposure and continuity across digital and physical services

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

192 of 250
selected domains published a reject or quarantine DMARC policy

7
claim dossiers, illustrated by authentic redacted excerpts

24
claimant labels in Sweden's ransomware-listing population

23 of 25
selected finance domains publish reject or quarantine DMARC policies

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Sweden's digital and institutional context	10
03	National exposure: a selected portfolio	14
04	Underground observations and claim cases	22
05	Incidents and disclosures by sector	37
06	Hacktivism, availability and operational systems	49
07	Threat actors, listing labels and attributed campaigns	53
08	Fraud, information trading and secondary harm	60
09	Banking, financial leads and payment continuity	64
10	Regulation and national response	68
11	Outlook and conditional scenarios	72
12	Action plan and completion evidence	76
A	Appendix A. Scope and evidence boundaries	82
B	Appendix B. Evidence register	85
C	Appendix C. Sources	86
D	Appendix D. Glossary	90
	About this report	91

Board and executives	01 05 10 11 12
CISO and service owners	03 04 05 10 12
SOC and intelligence	04 06 07 12 B
Fraud and customer operations	05 08 09 12
Privacy, legal and communications	05 06 10 12

About this edition

Prepared with AI assistance. Evidence and limits accompany the findings.

Sweden's documented incidents connect identity misuse, supplier-held information and service continuity. Defenders should validate each exposure and preserve the distinction between claims and confirmed effects.

62

Swedish-labelled ransomware listings; criminal claims, not confirmed intrusions

775,020

Sweden-associated posts observed in the requested window; not an incident count

50/100

National Atlas headline; 242 assessed domains in the selected portfolio

22

case dossiers: 7 claim cases and 15 public-event dossiers

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions should leaders make first?
2 Context	Which dependencies and authority changes affect response?
3 Selected-domain exposure	Which configuration observations need owner validation?
4 Underground observations	What do advertisements, requests and relays establish?
5 Incidents by sector	What did organisations and authorities confirm or report?
6 Availability and operational systems	How do claims differ from service and physical effects?
7 Actors and campaigns	Which relationships and attributions have source support?
8 Fraud	How can information support a deceptive request?
9 Banking	Which observations concern a bank, a customer or a dependency?
10 Regulation	Which entity, trigger, recipient and clock apply?
11 Outlook	Which conditional signals change the assessment?
12 Action plan	Who acts and what demonstrates completion?
Appendices A–D	Scope, evidence, sources and definitions

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which evidence supports immediate decisions for Swedish organisations?

62

Swedish-labelled ransomware listings in the requested window

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Sweden's evidence supports identity validation, supplier-data response and service continuity as distinct priorities. Ransompedia records 62 Swedish-labelled listings, each a criminal claim. Public disclosures show mailbox access, customer information exposure and deliberate service shutdowns. 73 of 242 assessed domains had a credential listed for sale. The national Atlas headline is 50/100. The recent-activity period brings several scope-sensitive customer notices. Validate owned accounts, exercise critical dependencies and assign separate owners to operational recovery and risk to people.

The requested window is 1 January–22 November 2026 by post time. Recent activity covers 8–22 November. Publication counts and recent material were checked after the UTC cut-off on 23 November. The report is a dated snapshot, not a complete census of incidents. Publication dates do not establish intrusion dates.

1. Listing counts justify readiness without establishing a national attack total. The 62 Swedish-labelled ransomware listings use 24 claimant labels. The leading three account for 30 listings, or 48.4%. Country associations and repeat appearances limit any unique-organisation interpretation. A listing does not confirm encryption, theft or payment. [S2]

2. Identity response extends beyond changing a password. The regional-healthcare case distinguishes 99 affected staff mailbox credentials from 44 mailboxes in which messages were read. CERT-SE's November warning describes several phishing campaigns against Swedish organisations. Relevant accounts require validation of sign-ins, sessions and rights, with exposure of mailbox contents assessed separately. [S18][S33]

3. Supplier and customer populations need their own denominators. Lyko's formal notice distinguishes 36,000 Swedish customers from 60,000 across markets. Universeum's recent disclosure concerns a late-October supplier event. Cabonline's notice raises journey-data questions. These populations overlap in unknown ways and are not added into a Swedish total. [S28][S30][S29]

4. Current listings require account validation. 73 of 242 assessed domains had a credential listed for sale. The assessed portfolio's national Atlas headline is 50/100. Exposure remains unknown for 8 selected domains. Separately, 192 of 250 domains publish reject or quarantine DMARC policy. These observations are not confirmed intrusions or national prevalence. [S4][S3]

5. Service and physical effects require different evidence. Official refrigeration warnings concern connected operational equipment. A manufacturing disclosure concerns precautionary shutdown and production interruption. A website claim alone establishes neither operational control nor data theft. Assign engineering and business owners alongside technical incident response. [S25][S27]

Four decisions for leaders

1. **Validate identity evidence.** Confirm owned accounts, current use and prior remediation; contain verified access, relevant sessions and authentication changes (§3–4, §12).
2. **Exercise supplier scope changes.** Require data categories, affected service and revised notices; assess harm to people separately from technical restoration (§5, §8–10).
3. **Demonstrate safe continuity.** Test a minimum service and a safe operational fallback, including supplier maintenance and identity dependencies (§6, §9, §12).
4. **Assign each reporting clock.** Identify the legal entity, trigger and recipient; record awareness and classification separately, with backup submission access (§10, §12).

The year in numbers

775,020

Observed Sweden-associated posts [S1]

WHAT IT DOES NOT MEASURE

Verified Swedish incidents or unique victims

727,150

January and February posts within that population [S1]

WHAT IT DOES NOT MEASURE

Two months of confirmed attack growth

62

Swedish-labelled ransomware listings [S2]

WHAT IT DOES NOT MEASURE

Unique organisations or confirmed intrusions

47

Swedish-labelled listings for all of 2025 [S2]

WHAT IT DOES NOT MEASURE

A matched observation period

24

Claimant labels in the 2026 listing population [S2]

WHAT IT DOES NOT MEASURE

Verified distinct operators

250

Selected domains with configuration observations [S3]

WHAT IT DOES NOT MEASURE

All Swedish organisations or independent legal entities

73 of 242

Assessed domains with a credential listed for sale [S4]

WHAT IT DOES NOT MEASURE

Tested credentials or confirmed intrusions

50/100

National Atlas headline for the assessed portfolio [S4]

WHAT IT DOES NOT MEASURE

A breach percentage or national prevalence estimate

192 of 250

Domains publishing reject or quarantine DMARC policy [S3]

WHAT IT DOES NOT MEASURE

Verified message delivery or fraud prevention

22

Seven claim dossiers and fifteen public-event dossiers

WHAT IT DOES NOT MEASURE

A deduplicated national incident count

KEY TAKEAWAYS

01

Validate claims before disruptive containment.

02

Preserve supplier, customer and service-impact boundaries.

03

Require completion evidence for identity, continuity and notification decisions.

Report map

Twelve chapters, five reader paths. Follow the decision that matches your responsibility; keep the evidence boundary with the finding.

Board and executives	Resource continuity and require completion evidence	01 05 10 11 12
CISO and service owners	Prioritise owned exposures and dependencies	03 04 05 10 12
SOC and intelligence	Distinguish observation, claim and attribution	04 06 07 12 B
Fraud and customer operations	Prevent contextual deception and secondary harm	05 08 09 12
Privacy, legal and communications	Determine scope, clocks and careful wording	05 06 10 12

The evidence labels are **observation**, **actor claim**, **official account**, **attributed reporting** and **analyst inference**. An advertisement can be directly observed while its asserted contents remain unverified. A confirmed incident can leave attribution and the full affected population unresolved.

CHAPTER 02

Sweden's digital and institutional context

02

THIS CHAPTER ANSWERS

Which dependencies change the response to an incident in Sweden?

1 July 2026

CERT-SE joined NCSC within FRA

2.1 Digital convenience creates continuity dependencies 11
2.2 Two institutional changes have different dates 11
2.3 Suppliers create several kinds of exposure 12
2.4 Political themes are source statements 12
2.5 Give each clock an owner 12

CHAPTER 02

Sweden's digital and institutional context

IN SHORT

Sweden's digital services connect identity, suppliers, payments and physical operations. The important distinction is which dependency failed and what evidence confirms the effect. Institutional responsibilities also changed during the year: CERT-SE became part of NCSC within FRA on 1 July. Use current reporting routes, preserve the dates behind historical disclosures, and test the business service alongside its technical recovery.

2.1 Digital convenience creates continuity dependencies

The Riksbank describes Sweden's payment market as almost entirely digital. Its 2026 report identifies disruption of electricity and data communications as vulnerabilities alongside cyberattacks. This is the central bank's resilience assessment, not a finding that payments are generally unsafe. [S7]

For a CISO, the practical unit is the service chain. A purchase can depend on a merchant, network, payment provider, identity service and customer device. A fault at one point does not establish access to every participant. Map the minimum service that can continue when a dependency is unavailable.

Treat alternative payment and customer-support arrangements as operational controls. Establish who can authorise them, which records they need and how transactions are reconciled after recovery. These are planning recommendations, not assertions that any named organisation lacked a fallback.

2.2 Two institutional changes have different dates

MSB became Myndigheten för civilt försvar, the Swedish Civil Defence and Resilience Agency, on 1 January 2026. Legacy branding and web addresses can therefore remain on valid official material. A retained MSB label does not by itself make a notice obsolete. [S6]

NCSC is part of FRA. On 1 July 2026, information-security and cybersecurity functions from the civil-defence agency were integrated into NCSC, including CERT-SE. The centre describes collaboration with defence, police, telecommunications and security authorities. The report does not treat this collaboration as attribution of an incident. [S5]

Keep the issuer, publication date and current contact route in the incident record. Advice issued before July can remain relevant, while the reporting destination and organisational description have changed. Confirm the applicable portal before an exercise, rather than discovering an obsolete route during an outage.

2.3 Suppliers create several kinds of exposure

A supplier may hold a copy of customer information, provide privileged support or operate the service itself. Those relationships produce different response duties. A stolen marketing export does not establish access to a payment system. A service shutdown can be precautionary even when information access remains uncertain.

Ask each critical supplier to identify the legal entity, service, data categories, access rights and evidence available to customers. Require a route for revised scope notices. Initial counts can change as an investigation distinguishes records, accounts, contacts and people.

The incident dossiers in Chapter 5 retain those distinctions. They do not add overlapping customer populations into a Swedish affected-person total. A foreign supplier can affect Swedish users without creating a separate intrusion at a Swedish customer.

2.4 Political themes are source statements

Claims invoking NATO accession, Russia, Israel and Gaza, Quran-burning incidents or elections require particular care. An actor's cited theme does not establish causation, nationality, state direction or a verified technical outcome. This report takes no position on government decisions, political parties, religion or foreign policy.

Official attributions remain the issuing authority's assessment. The wording does not become the authors' independent attribution merely because several publications repeat it. Language, a flag or an alias is insufficient to assign an operator to a country.

A political calendar can inform readiness when a source documents a relevant threat. It does not justify inventing a campaign or attributing an election outcome to cyber activity. Security teams should protect accounts and service continuity consistently across affiliations.

2.5 Give each clock an owner

The cybersecurity law entered into force on 15 January 2026. Its significant-incident duties differ from GDPR personal-data reporting and financial-sector DORA reporting. Chapter 10 sets out the distinct clocks and responsible functions. [S8][S10][S11]

Use one factual incident record with separate reporting decisions. Record awareness, service effect, affected data, supplier statements, confidence and the next update time. Legal and privacy teams should assess the relevant trigger while technical teams preserve evidence and contain validated access.

KEY TAKEAWAYS

01

Restore the business service as well as the application.

02

Use the current authority route while preserving the original notice date.

03

Attribute political and state-linked assessments to their sources and keep response decisions evidence-led.

CHAPTER 03

National exposure: a selected portfolio

03

THIS CHAPTER ANSWERS

Which measured control observations require validation by asset owners?

192 of 250

selected domains published a reject or quarantine DMARC policy

3.1 Universe card 15

3.2 Mail-domain policies by sector 16

3.3 Other configuration observations retain their denominators 17

3.4 Current listings lead the exposure decision 17

3.5 Turn observations into owned decisions 20

CHAPTER 03

National exposure: a selected portfolio

IN SHORT

73 of 242 assessed domains had a credential listed for sale when checked. The assessed portfolio's national Atlas headline is 50/100; 8 selected domains have unknown exposure. Configuration observations cover 250 domains, of which 192 publish reject or quarantine DMARC policy. These are separate signals, not confirmed intrusions or national prevalence. Validate current accounts, investigate relevant employee devices and review mail configuration with the responsible owners.

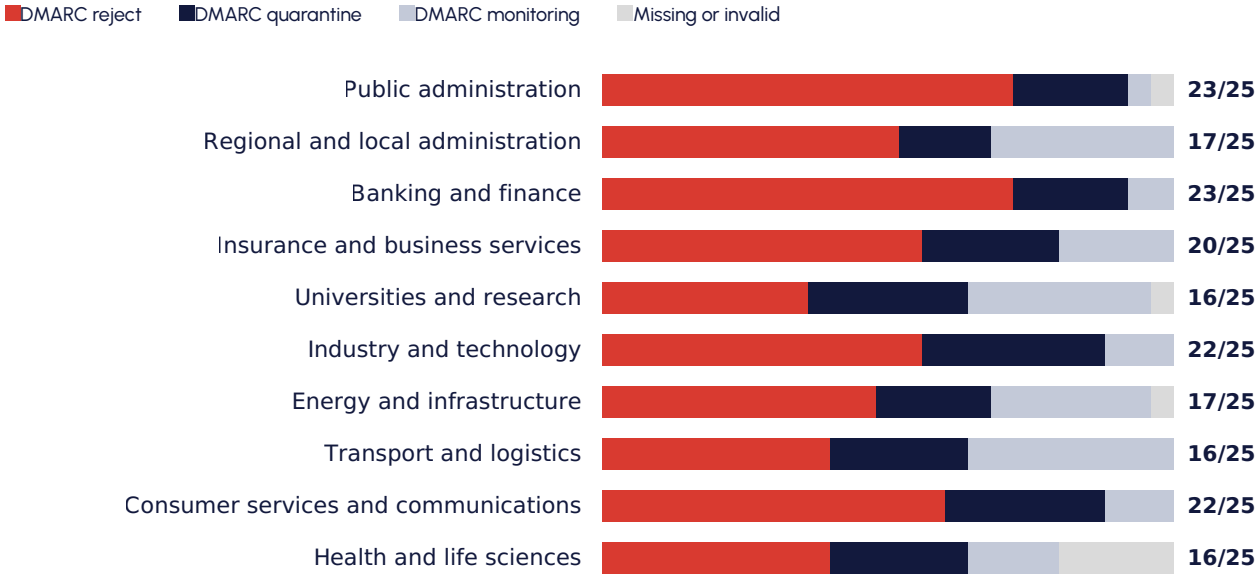
3.1 Universe card

Item	Scope
Selection	250 purposively selected organisations and their candidate domains; no revenue ranking or national prevalence estimate
Sectors	10 cells, each containing 25 selected entries
Unit	Domain observation; legal ownership and entity independence remain unvalidated
Configuration snapshot	22 November 2026; a configuration view, not a year-long intrusion count
Exposure data	242 assessed domains; 8 selected domains remain unknown; cumulative device, credential and document associations, current listings and a 30-day similar-name view [S4]
Interpretation	Missing observations do not establish a missing security control

The selection spans public services, finance, education, industry, infrastructure, transport and consumer services. Its size does not make it a random sample. Related services can share operators; a domain association does not establish a distinct independent legal entity. [S3]

3.2 Mail-domain policies by sector

Most selected domains publish an enforcing DMARC policy, with sector differences



Source: configuration observations for 250 selected domains [S3]. Published policies do not establish successful message delivery or prevented fraud.

Sector	Domains	Reject or quarantine	Monitoring	Missing or invalid
Public administration	25	23	1	1
Regional and local administration	25	17	8	0
Banking and finance	25	23	2	0
Insurance and business services	25	20	5	0
Universities and research	25	16	8	1
Industry and technology	25	22	3	0
Energy and infrastructure	25	17	7	1
Transport and logistics	25	16	9	0
Consumer services and communications	25	22	3	0

Sector	Domains	Reject or quarantine	Monitoring	Missing or invalid
Health and life sciences	25	16	4	5
ALL	250	192	50	8

Source: Brandefense configuration observations [S3]. Reject and quarantine together account for 192 of 250 domains, or 76.8%. A published policy does not establish that every legitimate message aligns or that every receiving service enforces it. No sector exposure rating is published.

3.3 Other configuration observations retain their denominators

Observation	Count	Boundary
SPF record present	243 of 250	Presence alone does not establish correct authorisation or alignment
DKIM-related record observed	210 of 250	Non-observation does not establish that the domain does not sign mail
DNSSEC delegation record present	130 of 250	Does not establish full chain validation
TLS certificate validation succeeded	243 of 250	4 validation failures and 3 unavailable results need owner review
Domains with available HSTS results	222 of 250	Results for other selected domains remain unavailable
HSTS observed	178 of 222	Does not establish complete coverage or control effectiveness

These are configuration observations rather than measured control effectiveness. The results do not establish complete coverage of subdomains, services or client connections. Non-observation does not establish a year-long exposure or successful attack. [S3]

3.4 Current listings lead the exposure decision

73 of 242 assessed domains had a credential listed for sale when checked. Exposure observations are available for 242 of the 250 selected domains; the other 8 remain unknown. The national Atlas headline for the assessed portfolio is 50/100. Only this national rating is published. [S4]

The headline supports prioritisation within the assessed portfolio. It is neither a breach percentage nor a probability of future intrusion. Sector tables show measured signal counts and their assessed denominators, without sector or organisation ratings.

Sector	Assessed domains	Domains with credentials listed for sale	Domains with employee-device associations	Domains with document associations
Public administration	24	5	9	16
Regional and local administration	25	2	24	23
Banking and finance	24	7	12	17
Insurance and business services	22	4	10	13
Universities and research	25	8	24	23
Industry and technology	25	7	23	24
Energy and infrastructure	24	4	11	9
Transport and logistics	24	12	11	9
Consumer services and communications	25	19	22	20
Health and life sciences	24	5	20	12
Total	242	73	166	166

In `c03_exposure_signals.csv`, `orgs_listed_for_sale_now` counts assessed domains with a credential listed for sale. The same domain count appears as `current_listing_domains` in `c04_sector_exposure.csv`. Neither field establishes independent organisations or organisations offered for sale. [S4]

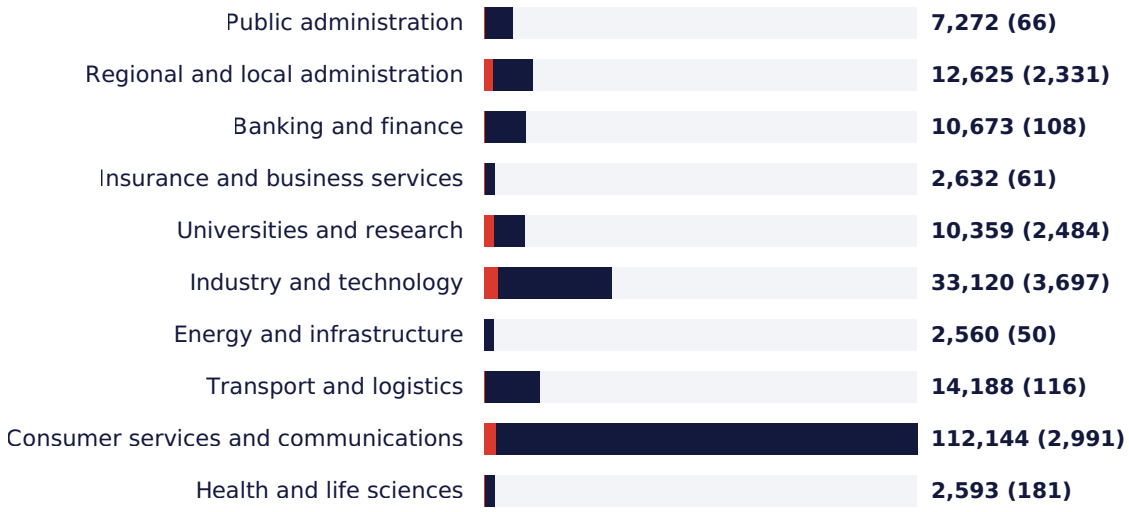
A current listing records an offer, not a completed sale, tested secret or confirmed intrusion. Validate account ownership, freshness, privileges, current use and prior remediation. Customer, student and employee associations require different response owners.

Device and credential totals below describe cumulative associations, rather than a 2026 incident population. The employee view sits within the device population and must not be added to it. Records can overlap across sources and domains. [S4]

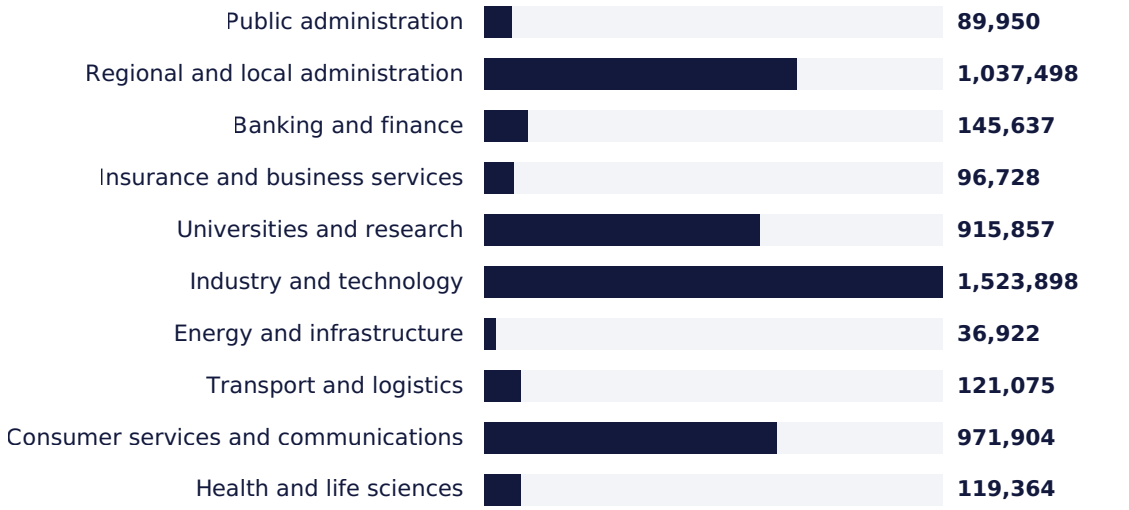
Device and credential associations require separate validation within the assessed portfolio

Employee device associations Other device associations

Device associations, at least (employee subset in parentheses)



Credential-record associations (separate scale)



Source: Brandefense exposure observations for 242 assessed domains out of 250 selected domains [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector	Assessed domains	Devices, at least	Employee devices	Credential records
Public administration	24	7,272	66	89,950
Regional and local administration	25	12,625	2,331	1,037,498
Banking and finance	24	10,673	108	145,637
Insurance and business services	22	2,632	61	96,728
Universities and research	25	10,359	2,484	915,857
Industry and technology	25	33,120	3,697	1,523,898

Sector	Assessed domains	Devices, at least	Employee devices	Credential records
Energy and infrastructure	24	2,560	50	36,922
Transport and logistics	24	14,188	116	121,075
Consumer services and communications	25	112,144	2,991	971,904
Health and life sciences	24	2,593	181	119,364
Total	242	208,166	12,085	5,058,833

The assessed portfolio contains at least 208,166 device associations and 5,058,833 credential-record associations. These are not distinct people, confirmed infected company-owned endpoints or proof that an organisation's own infrastructure supplied the material. Investigate corroborated employee endpoints and relevant sessions together.

Document observations total 2,885 across 166 assessed domains. A document association does not establish confidentiality, unlawful acquisition or adversary access. Similar-name observations total 15,469 across 183 domains in the preceding 30-day view. Similarity does not establish malicious use or ownership. [S4]

The configuration portfolio covers 250 domains, while exposure covers 242. Compare only observations with their stated denominator. Missing exposure values are not zeros, and the national rating is not a national prevalence estimate.

An organisation receiving a relevant account alert should validate account ownership, age, privileges, current use and prior remediation. For valid current access, examine sessions and authentication changes as well as passwords. Customer, student and employee associations need appropriate owners; a domain alone cannot distinguish those people.

Separate research published by QiAnXin XLab on 17 June reported at least 4,300 AryStinger-infected legacy routers worldwide and placed 6.40% of the infected routers it observed in Sweden. This is the researcher's device observation, not Brandefense's selected portfolio, a count of Swedish organisations or a national infection rate. The researchers could not quantify the NAS variant. Infrastructure owners should identify unsupported gateways, review applicable vendor guidance and investigate relevant signs of unauthorised control. No named Swedish organisation or operator attribution is established here. [S78]

3.5 Turn observations into owned decisions

Messaging teams should validate legitimate senders before changing policy. Test alignment for essential services and retain exceptions with owners and expiry dates. Infrastructure teams should investigate failed certificate validation and confirm the intended endpoint before remediation.

Keep configuration review separate from incident declaration. A missing record is a reason to check the owned service, rather than a conclusion that information was stolen. Record the result, remediation and next check for each validated finding.

KEY TAKEAWAYS

01

The selected-domain denominator is 250, not all Swedish organisations.

02

Configuration observations describe visible configuration rather than attack outcomes.

03

Current listings, devices and documents require separate validation; missing exposure remains unknown.

CHAPTER 04

Underground observations and claim cases

04

THIS CHAPTER ANSWERS

What do retained advertisements establish about Swedish-associated information?

7

claim dossiers, illustrated by authentic redacted excerpts

4.1 Universe card 23

Monthly observed publication volume 24

Publication channels and languages 25

4.2 Seven claims and the decisions they support 26

4.3 Historical material and relays 34

4.4 Recent activity and analytical limits 35

4.5 Additional retained claims 35

CHAPTER 04

Underground observations and claim cases

IN SHORT

The retained material contains credential offers, requests for identity and vehicle information, advertised business records and recirculated historical claims. Seven cases show different response questions. Recent examples are publication events, not proof of newly stolen data. A Swedish label does not establish provenance or residency. Validate relevant claims against owned accounts and data before declaring an incident or recommending disruptive action.

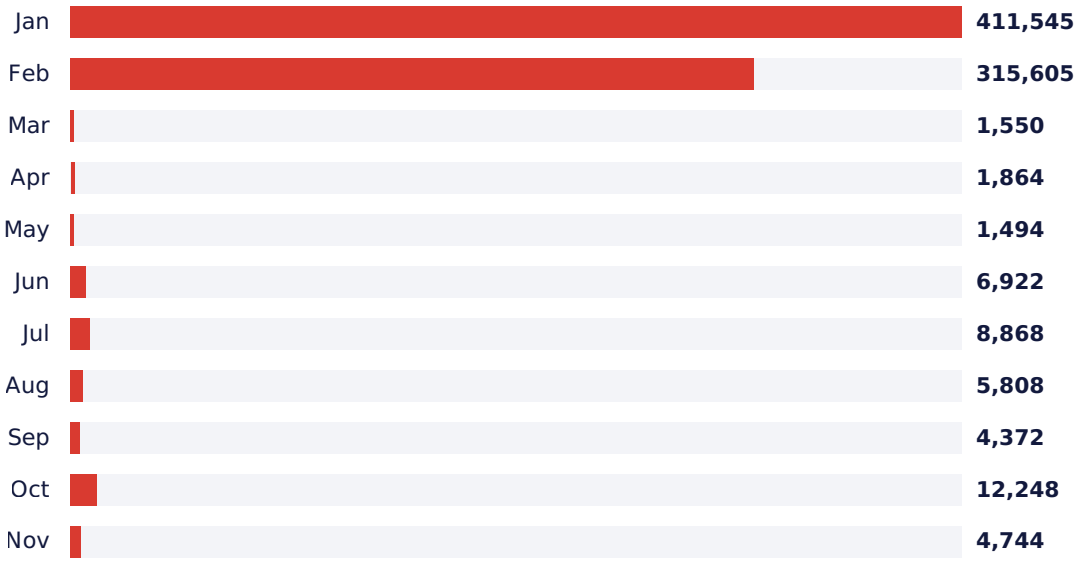
4.1 Universe card

Item	Scope
Window	1 January–22 November 2026, by post time
Retained corpus	49,045 distinct posts across the report's evidence sets
Sweden-tagged forum material	484 retained posts; not all criminal offers or verified Swedish incidents
Recent country-associated material	3,018 retained posts dated 8–22 November; overlapping the corpus above
Recent Sweden-tagged forum material	42 posts within the recent population
Illustrations	Authentic quotations with victim identifiers and contact details removed
Limits	Country association, record freshness, validity, possession and completed transactions are not established by advertising

Source: Odin by Brandefense [S1]. The retained corpus and the wider observed publication population are different units. Missing material does not establish absence of activity. The report does not estimate a national crime-family prevalence from the illustrated cases.

Monthly observed publication volume

January and February account for most observed country-associated posts



Source: Brandefense Blackhole, observed Sweden-associated posts, 1 January-22 November 2026; November partial [S1]. Posts are not confirmed incidents; language associations can overlap.

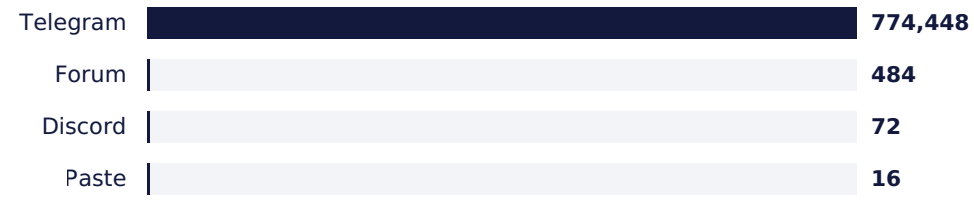
Month	Posts	Month	Posts
January	411,545	July	8,868
February	315,605	August	5,808
March	1,550	September	4,372
April	1,864	October	12,248
May	1,494	November through cut-off	4,744
June	6,922	Total	775,020

January and February account for 727,150 posts, or 93.8%. Observed promotion and repeated advertising can dominate country-associated volume. This is not evidence of a corresponding intrusion peak or a matched-month threat trend. [S1]

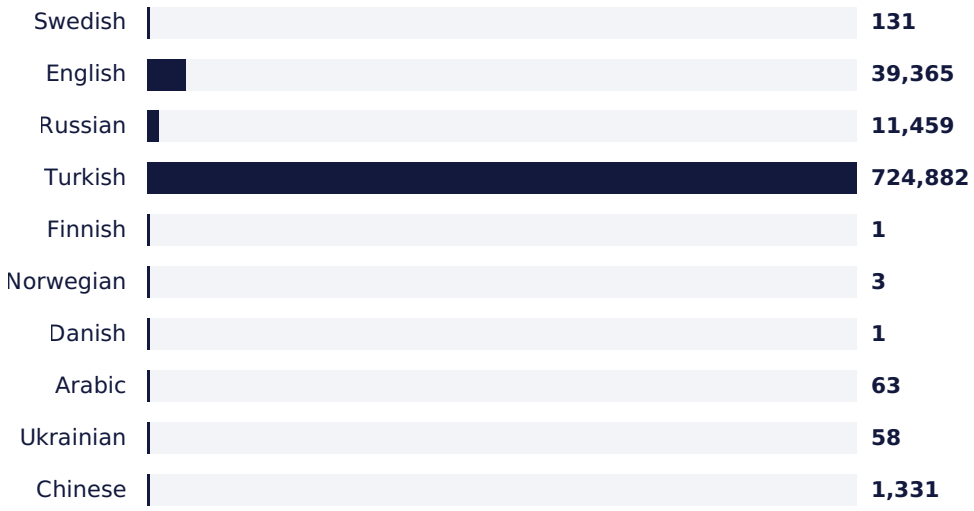
Publication channels and languages

Publication channels and language associations describe visibility rather than attack prevalence

Platform



Language



Source: Brandefense Blackhole, observed Sweden-associated posts, 1 January–22 November 2026; November partial [S1]. Posts are not confirmed incidents; language associations can overlap.

Channel	Associated posts
Telegram	774,448
Forum	484
Discord	72
Paste	16

Language association	Posts
Swedish	131
English	39,365
Russian	11,459

Language association	Posts
Turkish	724,882
Finnish	1
Norwegian	3
Danish	1
Arabic	63
Ukrainian	58
Chinese	1,331

Most language associations are Turkish (724,882 posts); this describes publication visibility and does not establish Swedish targeting, origin or actor nationality. [S1]

Language associations can overlap, and channel counts describe publications rather than attacks or distinct operators. Country association does not establish targeting, residence or provenance. The January–February concentration remains a publication-volume observation. [S1]

4.2 Seven claims and the decisions they support

A

CASE A

Country-labelled credentials, including a November offer

Evidence card B01 | 30 Jan 2026 | Forum thread | Cross-sector information

Claim unverified

CLAIM	A 30 January advertisement describes a Sweden-labelled email/password collection of 17 K++ lines. A 19 November post advertises 30 K++ lines using similar wording. These are the sellers' quantities and freshness claims. [S1]
BOUNDARY AND ALTERNATIVES	The posts establish advertising, not working credentials, unique accounts or two distinct stolen datasets. Similar phrasing does not verify the same file, a common operator or a later capture date.
RESPONSE	Validate an owned account against current status, sign-ins and previous remediation. If current use is confirmed, address relevant sessions and authentication methods as well as passwords. Do not impose a national password-reset conclusion from advertised line counts.

Bottom line

Validate an owned account against current status, sign-ins and previous remediation.

Evidence card B01 30 Jan 2026

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

ORIGINAL

Database : Sweden Type : Email , Password Condition: Fresh,HQ Combo: 17 K++ Line

Note. The word fresh is the advertiser's description. Publication does not establish when credentials were captured.

Held
An advertisement labels an email/password collection as Swedish and claims 17 K++ lines.

Not established
Authenticity, unique accounts, password validity, collection date, original source or completed transfer.

Evidence card B07 19 Nov 2026

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

ORIGINAL

Database : Sweden Type : Email , Password Condition: Fresh,HQ Combo: 30 K++ Line

Note. A recent advertisement can contain old material. Its post date and purported collection date are different.

Held
A 19 November advertisement claims a Sweden-labelled email/password collection of 30 K++ lines.

Not established
Fresh capture, working passwords, unique people, original source, overlap with earlier offers or completed transfer.

CASE B

B

Demand for Swedish personal identity numbers

Evidence card B02 | 15 Feb 2026 | Forum thread | Cross-sector information

Claim unverified

CLAIM	A 15 February forum post requests a Swedish database containing personal identity numbers. It is a request to acquire information, rather than an assertion that the requester already possesses it. [S1]
BOUNDARY AND ALTERNATIVES	No purchase, theft, victim population or source organisation is established. A personnummer request does not demonstrate access to a public register or an ability to authenticate as another person.
RESPONSE	Test customer-support and account-recovery procedures against callers who know genuine identity details. Treat such details as context, rather than sufficient authority to disclose information or approve a consequential change.

Bottom line

Test customer-support and account-recovery procedures against callers who know genuine identity details.

Evidence card B02 — 15 Feb 2026

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

ORIGINAL

Looking for any type of database from Sweden that includes Swedish personnummer / personal ID number / Social security number.

Note. This is demand, not a successful purchase or data-theft disclosure.

Held
A buyer requests Swedish personal identity numbers and refers to earlier advertised datasets.

Not established
Any acquisition, database access, number of affected people, original provenance or a new intrusion.

CASE C

C

A stealer label and a geographic assertion

Evidence card B04 | 23 Apr 2026 | Forum thread | Cross-sector information

Claim unverified

CLAIM	An April advertisement labels a dataset as Vidar Stealer material and gives SE as source geography. It advertises credentials and autofill information. The malware and geography labels are the poster's assertions. [S1]
BOUNDARY AND ALTERNATIVES	The retained post does not validate malware-family attribution, device ownership, capture date, working sessions or a Swedish organisation intrusion. A device-location claim is not a service-nationality determination.
RESPONSE	If an authorised alert matches an owned endpoint or account, investigate the endpoint and associated credentials together. Review session exposure and prior containment before deciding which secrets to rotate.

Bottom line

If an authorised alert matches an owned endpoint or account, investigate the endpoint and associated credentials together.

Evidence card B04 — 23 Apr 2026

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

ORIGINAL

Malware Family . Vidar Stealer [...] Source Geo ..... SE [...] Credentials .... Yes [...] Autofill Data .. Yes

Note. These are the poster's dataset labels. Device geography and service nationality are separate propositions.

Held

A forum post labels an advertised stealer dataset as Vidar and gives SE as source geography.

Not established

Malware-family attribution, device ownership, capture time, working credentials, session access or use against any Swedish organisation.

CASE D

D

Automotive-service customer and invoice data

Evidence card B05 | 5 Sep 2026 | Forum thread | Cross-sector information

Claim unverified

CLAIM	A September offer describes a Swedish automotive-service database with customer, order, invoice and storage information. The record categories suggest business context that could make a later request credible. The advertisement alone does not establish such misuse. [S1]
BOUNDARY AND ALTERNATIVES	Origin, authenticity, source-system access and affected customer count remain unverified. A supplier copy, older export or misleading description could produce similar advertising. No completed sale is established.
RESPONSE	Validate any relevant alert with the data custodian. Authenticate invoice-account changes and collection or delivery requests through a known channel. Do not let knowledge of a real order replace identity verification.

Bottom line

Validate any relevant alert with the data custodian.

Evidence card B05 — 5 Sep 2026

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

ORIGINAL

Swedish tire and rubber-repair shop database [...] Customer, order, invoice, and tire storage data

Note. Organisation names, locations, sample rows and system identifiers are withheld.

Held

A post offers a purported automotive-service database and describes linked customer and business records.

Not established

Provenance, authorisation, authenticity, affected customer count, source-system access or a completed sale.

CASE E

E

Recent demand for vehicle information

Evidence card B06 | 18 Nov 2026 | Forum thread | Cross-sector information

Claim unverified

CLAIM	An 18 November forum request seeks vehicle database information by VIN. The original post names a manufacturer and another data service; those identities are withheld because the request does not establish an incident at either. [S1]
BOUNDARY AND ALTERNATIVES	The request establishes interest. It does not establish availability, possession, access, a seller response or a purchase. Vehicle data can also have legitimate public, commercial or historical sources.
RESPONSE	An asset owner should check the actual data categories and service rights if a relevant alert emerges. Fraud teams should assess the specific transaction at risk, rather than declare a manufacturer intrusion from a buyer's request.

Bottom line

An asset owner should check the actual data categories and service rights if a relevant alert emerges.

Evidence card B06 — 18 Nov 2026

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

ORIGINAL

[...] WIll buy db for [vehicle manufacturer] and [vehicle database] vehicle data per VIN [...]

Note. A request is evidence of interest in information, not evidence that the information is available.

Held

A forum request seeks vehicle-related database material on 18 November.

Not established

Possession, seller response, database access, a successful purchase or a new incident at a manufacturer.

CASE F

F

Recent Swedish-labelled identity leads

Evidence card B13 | 17 Nov 2026 | Forum thread | Cross-sector information

Claim unverified

CLAIM	A 17 November forum advertisement offers leads described as fresh for Sweden and other countries, with a total claim of 200k. The fields include names, personal identity numbers, addresses and contact information. [S1]
BOUNDARY AND ALTERNATIVES	The advertised total is not a verified Swedish-person count. The post does not establish freshness, authenticity, source organisation, lawful provenance, completed sale or a connection to any recent company disclosure.
RESPONSE	Prepare customer-support staff for requests containing plausible personal details. Validate a relevant data alert against authorised records and earlier disclosures. Keep the response proportionate to the categories and actual misuse established.

Bottom line

Prepare customer-support staff for requests containing plausible personal details.

Evidence card B13 — 17 Nov 2026

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

ORIGINAL

Selling fresh leads for Sweden and other countries. Total count 200k. [...] Person Nr [...] Source: Financial company.

Note. The financial-company origin is the seller's assertion. Sample rows and personal identifiers are withheld.

Held

A 17 November seller advertises 200k leads labelled Sweden and other countries, including personal identity and contact fields.

Not established

Unique people, freshness, working contact details, provenance, consent, any financial company relationship or completed sale.

U

CASE U

Advertised financial-services access

Evidence card B16 | 14 Apr 2026 | Forum thread | Financial services

Claim unverified

CLAIM	One forum post dated 14 April advertises two Swedish financial-services access offers: remote monitoring and management (RMM) with claimed enterprise-administrator privileges, and SSH remote login with claimed domain-user privileges. These are the seller's capability descriptions. [S1]
BOUNDARY AND ALTERNATIVES	The post does not verify either access path, privilege, present usability or target identity. It does not establish licensed-bank status, two separate organisations, a completed sale, data theft or ransomware deployment. The offers may overlap or misdescribe the underlying asset.
RESPONSE	If an authorised alert can be matched to owned infrastructure, the remote-access owner and SOC should examine account privileges, approved management tools and authentication history. Preserve evidence, revoke unauthorised sessions and credentials, and check persistence before closing the alert. Neither a generic sector label nor a seller's privilege claim justifies declaring an institutional intrusion.

Bottom line

Validate owned remote-access paths, privileges and sessions before declaring an intrusion.

Evidence card B16 — 14 Apr 2026

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

ORIGINAL

[RMM (vendor redacted)] Financial Services - Sweden ([revenue redacted]) [...] Privilege ..... Enterprise Admin [...] [SSH] Financial Services - Sweden ([revenue redacted]) [...] Privilege ..... Domain User [...]

TRANSLATION

[RMM (vendor redacted)] Financial Services - Sweden ([revenue redacted]) [...] Privilege ..... Enterprise Admin [...] [SSH] Financial Services - Sweden ([revenue redacted]) [...] Privilege ..... Domain User [...]

Note. The offers may overlap. Publication does not establish exploitation, data theft or ransomware deployment; identifying vendor and revenue details are redacted.

Held

One post advertises two Swedish financial-services access offers, through RMM with claimed enterprise-administrator privileges and SSH with claimed domain-user privileges.

Not established

Verified access, privilege, usability, target identity, licensed-bank status, two separate organisations or a completed sale.

4.3 Historical material and relays

Evidence card B09 — 8 Apr 2026

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

ORIGINAL

Source Code [software supplier] Data Breach [...] in November, 2025

Note. The post belongs to the 2026 publication window; its alleged underlying event belongs to 2025.

Held
An April forum post repeats a software supplier source-code claim that it dates to November 2025.

Not established
A new 2026 intrusion, code authenticity, source-system access or validation of the poster's attribution.

Evidence card B11 — 8 Mar 2026

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

ORIGINAL

[...] [the supplier] [...] was the victim of a ransomware attack.

Note. The quoted statement is the poster's account. Public confirmation must be established separately.

Held
A post quotes a thread about an earlier supplier incident and advertised data.

Not established
A new 2026 intrusion, the poster's claimed affected population, file identity, freshness or current access.

Evidence card B10 — 30 Apr 2026

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

ORIGINAL

The attackers claim they have access to the company's source code, cloud infrastructure, and various keys.

Note. A relay is not independent confirmation of the original actor's claims.

Held
An April forum relay repeats claims about source code, employee information and cloud-related material at a pharmaceutical organisation.

Not established
Current access, key validity, source, completeness, attribution or any operational or patient-data effect.

B09 dates its own alleged software event to November 2025. B11 quotes a supplier narrative about an earlier year. Both posts belong to this report's publication window; neither establishes a new 2026 intrusion. Public regulatory decisions about prior-year incidents remain a separate source population.

B10 is a forum relay of pharmaceutical source-code and cloud-material claims. Repetition is not independent verification. The report does not validate keys, current access, employee populations or patient-data effects from that relay. [S1]

4.4 Recent activity and analytical limits

The 17 November lead advertisement, 18 November vehicle-data request and 19 November credential offer are recent publications with different evidential meanings. A request is demand; an offer asserts availability. Neither establishes a completed transfer or the capture date.

A 9 November multi-country broker-lead advertisement also includes Sweden. It does not establish a Swedish financial institution intrusion or verified balances. Chapter 9 separates financial lead lists from bank-system and customer-account access. [S1]

Evidence card B14 — 9 Nov 2026

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

ORIGINAL

Quantity : (38K) Country: MIXED TIER-1/2/3 (Sweden, Norway, Netherlands etc.)

Note. The claimed total applies to a mixed-country list. It must not be reported as 38K Swedish people.

Held
A 9 November post advertises 38K broker-themed leads across several countries and includes Sweden.

Not established
The Swedish share, source relationships, unique people, current balances, deposit validity or completed transfer.

The examples provide response distinctions, not a case-success scorecard. No file identity, common operator or criminal transaction chain is established by similar wording. Missing or unresolved material remains a coverage limit rather than a finding of no incident.

4.5 Additional retained claims

An early-year post offers a retail/e-commerce database; later thread activity repeats the offer. Publication and later discussion do not establish new thefts, working customer accounts or a completed transaction. Data ownership, freshness and any matching prior disclosure require separate validation. [S1]

Other retained offers describe Swedish-labelled credential lists, community or business databases, financial-depositor leads and identity-document material. Some assert large inventories or repeat older quotations. Their advertised totals cannot be added into a count of Swedish people, and none supplies independent evidence of the source organisation, acquisition date or current usability. Replies requesting a new link or praising a seller do not corroborate the underlying claim. [S1]

A separate thread points to an alleged industrial-automation dataset; another advertises corporate decision-maker information with a claimed source at a different company. A pointer, supplier name or familiar customer name does not verify data possession or an intrusion at any named body. [S1]

KEY TAKEAWAYS

01

An advertisement verifies publication, not the advertised asset.

02

Requests, offers, relays and historical reposts need different interpretations.

03

Recent post dates do not establish fresh theft or a link to recent company disclosures.

CHAPTER 05

Incidents and disclosures by sector

THIS CHAPTER ANSWERS

What did organisations and authorities establish, and what follows for the service owner?

15

case dossiers; their populations overlap and must not be added

5.1 Read the chronology before the headline 38

5.2 Dated case dossiers 39

5.3 Other events retain their own evidence type 46

5.4 Recent activity: 8–22 November 2026 47

5.5 Vulnerability advice is not an incident count 47

CHAPTER 05

Incidents and disclosures by sector

IN SHORT

The case dossiers distinguish mailbox access, supplier-held information, operational disruption and scope updates. They preserve the difference between an event date and a public disclosure. Fifteen dossiers illustrate decisions; they are not a national incident total. The recent-activity period, 8–22 November, includes customer notices and supplier incidents. Use each case's established facts to choose the response, then validate the corresponding dependency in your own service.

5.1 Read the chronology before the headline

A disclosure in November may describe an October supplier event or earlier historical bookings. Several controllers can report one supplier incident. Conversely, two mailbox events in one sector can remain separate until technical evidence links them. The dossiers below preserve those units.

Sector	Observed consequence	First response owner
Healthcare	Staff mailbox access and phishing relays	Identity, privacy and clinical-service leadership
Education	Shared-platform information theft and precautionary restrictions	Platform owner and data-protection officer
Municipal services	Interrupted IT and later employee-data findings	Municipal incident commander and service owners
Retail and visitor services	Customer contact information and contextual fraud risk	Customer operations and privacy
Transport	Reservation, journey and account information at providers	Supplier manager and traveller-support function
Manufacturing and facilities	Production pause or connected-controller concerns	Engineering, safety and business continuity

5.2 Dated case dossiers

CASE G

G

Regional healthcare mailboxes

Healthcare

March disclosure; activity spans two years

ESTABLISHED ACCOUNT	On 5 March, Region Värmland reported credential exposure affecting 99 staff mailboxes. Mail had been read in 44 mailboxes at least once between October 2025 and February 2026. Access was disabled. [S18][S53]
BOUNDARY	The figures count staff mailboxes, not patients, messages or separate intrusions. The period overlaps the previous year. The statement did not establish access to other systems.
RESPONSE	Review sign-ins, delegated rights, forwarding rules and active sessions for validated affected accounts. Separately assess personal information held inside each mailbox. A reset alone does not establish that all access has ended.

Bottom line

Review sign-ins, delegated rights, forwarding rules and active sessions for validated affected accounts.

CASE H

H

An IT supplier distinguishes affected environments

Technology suppliers

Company account reported by the press

ESTABLISHED ACCOUNT	An IT supplier's account, as reported, described access to non-production systems. It reported no indications of effects on production environments or customer services. [S54]
BOUNDARY	The original company incident notice is not currently available. This report therefore relies on attributed reporting and withholds the supplier name.
RESPONSE	Ask which environment, data copy and credential were involved. Review separation of development secrets and production access. Do not infer a customer intrusion merely because an application name appears in supplier material.

Bottom line

Ask which environment, data copy and credential were involved.

CASE I

I Municipal IT and service continuity

Local government

Official disruption notices

ESTABLISHED ACCOUNT	A municipal notice described an IT attack, restricted IT access and crisis arrangements, and warned of potential personal-data leakage. [S20][S56]
BOUNDARY	The notices do not establish the full scope of affected services or information.
RESPONSE	Identify identity, connectivity and hosting dependencies. Exercise minimum citizen services without normal IT and preserve each controller's data-risk decision.

Bottom line

Identify identity, connectivity and hosting dependencies.

CASE J

J Learning-platform theft and multiple controller reports

Higher education

Supplier event; customer responses

ESTABLISHED ACCOUNT	IMY reported 51 personal-data incident notifications associated with Canvas by 8 May. CERT-SE described the platform supplier's confirmation of information theft and temporary access restrictions at Swedish institutions. [S21] [S57][S69][S77]
BOUNDARY	51 is a count of notifications received at that point. It is not 51 separate supplier intrusions, a final number of institutions or a count of affected students. An actor's global record claim is not substituted for the authority's unit.
RESPONSE	Map the institution's actual data categories and tenant relationship. Rehearse teaching, assessment and student communications during a precautionary restriction. Reopening should consider both service operation and the continuing privacy assessment.

Bottom line

Map the institution's actual data categories and tenant relationship.

CASE K

K

Ryde customer accounts across four countries

Transport services

Confirmed scope: country segment unknown

ESTABLISHED ACCOUNT	Ryde said it discovered an intrusion on 2 August and stopped it shortly afterwards. Its notice described contact information, dates of birth, partial card details and payment histories. Reporting placed the 4.5 million accounts across Sweden, Norway, Finland and Germany. [S22][S60]
BOUNDARY	The total is not a Swedish affected-person count. The company excluded full card numbers and ride-location history. Partial payment details do not establish usable card credentials or fraudulent transactions.
RESPONSE	Warn customers about messages using genuine account or payment context. Validate the information actually disclosed before recommending card or account action. Keep the country segment unknown unless the controller supplies it.

Bottom line

Warn customers about messages using genuine account or payment context.

CASE L

L

An IT supplier's internal systems and controlled reopening

Technology supply chain

Official incident and recovery account

ESTABLISHED ACCOUNT	The supplier's incident information describes unauthorised access to internal IT systems, a temporary shutdown and staged reopening. [S23][S61]
BOUNDARY	Restored services do not demonstrate that every customer-data assessment or supplier relationship is closed.
RESPONSE	Ask the supplier about the actual service and account used by your organisation. Agree evidence for reopening and a route for later scope changes. Keep technical restoration and customer-information review as separate milestones.

Bottom line

Ask the supplier about the actual service and account used by your organisation.

CASE M

M Municipal employee information and later scope changes

Local government

Official notices; scope update

ESTABLISHED ACCOUNT	A municipality's notice described sensitive employee information being copied to an external location after an IT intrusion. [S24][S62]
BOUNDARY	Record age does not establish repeated intrusions.
RESPONSE	Treat sensitive employment categories as a dedicated harm assessment. Identify the affected people and authorised support route without reproducing their details. Preserve the chronology of changing scope and assess notification separately from service recovery.

Bottom line

Treat sensitive employment categories as a dedicated harm assessment.

CASE N

N Lyko narrows the customer population

Retail

12 November event; 18 November update

ESTABLISHED ACCOUNT	Lyko's formal 18 November release described detection on 12 November and containment within an hour. It reported 36,000 customers in Sweden within 60,000 across its markets. Order information was involved for 95 customers. [S28][S65]
BOUNDARY	The company excluded payment information, passwords and personal identity numbers, and reported no operational impact. Earlier media figures are not added to the later formal scope. The 95 are not an additional verified unique-person population.
RESPONSE	Use the current controller notice when advising customers. Name and contact information can support convincing impersonation even when passwords are excluded. Review unusual account-recovery or order-change requests through a known independent channel.

Bottom line

Use the current controller notice when advising customers.

CASE O

O ■ Cabonline booking information at a supplier

Transport and supported travel

Supplier access confirmed; onward sharing unresolved

ESTABLISHED ACCOUNT	Cabonline's November notice described unauthorised access at an external booking supplier. Some contact, booking, pickup and destination information and payment-related information could be involved. The company said the access route was closed. [S29][S66][S70]
BOUNDARY	The company distinguished payment-related information from access to bank accounts or the ability to make unauthorised payments. Potential onward sharing remained under investigation; no completed sharing was established in the notice. Do not infer a protected-identity total.
RESPONSE	Assess journey information for personal-safety consequences as well as phishing. Customer-service and public-service travel owners should coordinate a safe support route. Preserve actual data categories and the supplier's updates rather than issuing a blanket payment-risk claim.

Bottom line

Assess journey information for personal-safety consequences as well as phishing.

CASE P

P ■ Universeum guests and a booking supplier

Visitor services

20 November disclosure; late-October event

ESTABLISHED ACCOUNT	Universeum's 20 November release described a late-October attack against its booking-system supplier. The organisation said an unauthorised party accessed information about roughly 280,000 guests, including names, email addresses, telephone numbers and dates of birth. It excluded personal identity numbers and payment-card information. [S30][S67]
BOUNDARY	The release said bookings and passes remained valid and no fraudulent use was known at publication. This is a recent disclosure of an earlier event. It is not linked here to another Gothenburg disclosure by location or timing alone.
RESPONSE	Prepare a visitor-facing explanation of which information can support deceptive contact. Check messages about bookings or passes through the established service. Supplier recovery and customer reassurance should use the same verified scope.

Bottom line

Prepare a visitor-facing explanation of which information can support deceptive contact.

CASE Q

Q Gothia Towers distinguishes forms from ticket information

Hospitality and exhibitions

18 November detection; investigation ongoing

ESTABLISHED ACCOUNT	Svenska Mässan Gothia Towers reported detection on 18 November in a limited external web environment. Its 20 November statement described about 14,000 customers potentially affected through form information. About 500 of those customers also had order information and user details entered when buying exhibition tickets leaked. [S31][S68]
BOUNDARY	The ticket customers are an explicit subset of the potentially affected customers. The categories carry different certainty and are not added together. The company excluded personal identity numbers and payment information, said other systems were unaffected and retained an ongoing-investigation qualification.
RESPONSE	Preserve the distinction between possible exposure and established leakage in customer notices. Where ticket-account details were involved, require a password change and review account sign-ins. Validate the web environment's effective permissions and logs. Treat changed investigation scope as an update obligation rather than evidence of a second intrusion.

Bottom line

Preserve the distinction between possible exposure and established leakage in customer notices. Where ticket-account details were involved, require a password change and review account sign-ins.

CASE R

R Airline reservation information and historical bookings

Air transport

Attributed company notice; source organisation withheld

ESTABLISHED ACCOUNT	Reporting described an airline notice about reservation references and flight-related information that might have been disclosed through an external reservation provider. [S63][S26]
BOUNDARY	The notice mainly concerns historical bookings and completed journeys. The investigation and intrusion period remained unresolved here. It does not establish a Swedish-resident population, active passenger accounts or access to flight-control systems.

RESPONSE	Ask which reservation fields were exposed and whether live bookings need protection. Review reservation-service account rights and unusual lookups. Do not merge this disclosure with a different airline's payment-page incident without concrete evidence.

Bottom line

Ask which reservation fields were exposed and whether live bookings need protection.

S

CASE S

Production shutdown after an intrusion

Manufacturing

Company spokesperson as reported

ESTABLISHED ACCOUNT	A manufacturer's spokesperson said in reporting that systems were shut down for isolation after an intrusion and production was paused. [S64][S27]
BOUNDARY	The cited account does not establish encryption, an actor or a data-theft quantity. Discovery and disclosure are different events. A defensive shutdown is not automatically attacker control of machinery.
RESPONSE	Exercise a safe production pause and the evidence required for restart. Separate enterprise IT restoration from industrial safety checks, scheduling and order reconciliation. Name the person authorised to approve each step.

Bottom line

Exercise a safe production pause and the evidence required for restart.

T

CASE T

Refrigeration incidents require physical verification

Retail and operational technology

Official campaign warning

ESTABLISHED ACCOUNT	NCSC's 2 November statement acknowledged incidents affecting grocery refrigeration systems and contact with affected organisations. Its advice concerned internet exposure, supported equipment and layered protection. A 5 November notice placed related events in a wider European context. [S25] [S17]
BOUNDARY	The official account does not supply a Swedish national victim total or a common actor for every incident. A public controller image does not by itself verify current access or physical harm. Do not infer other critical-infrastructure effects.

RESPONSE	Have engineering confirm settings and safe local operation. Remove unnecessary public access, control supplier maintenance paths and preserve the change history. Agree isolation and fallback procedures before a controller must be disconnected.

Bottom line

Have engineering confirm settings and safe local operation.

CASE V

V

Trezor shipping records and a revised international population

Official statement

Consumer services and fulfilment

ESTABLISHED ACCOUNT	Trezor's 13 August disclosure concerned its shipping provider ShipMonk and customers across several markets, explicitly including Sweden. The initial 13,689 customers comprised 11,742 with contact and shipping information exposed and 1,947 with partial name, city and email information. The latter group also included older orders. [S79][S80]
SCOPE UPDATE	The 4 September update added roughly 67,000 US customers with order records from November 2019–August 2021; the updated FAQ gives 80,689 customers overall. These are international populations, with no verified Swedish count. Trezor said its systems and devices were unaffected. [S79]
RESPONSE	Treat exposed delivery details as a phishing and personal-safety issue. Never provide a wallet backup in response to a message or website request. Supplier managers should seek evidence of deletion for retained historical copies; a policy or earlier assurance alone does not prove deletion.

Bottom line

Separate Swedish scope, device security and the continuing harm from delivery details.

5.3 Other events retain their own evidence type

An organisation reported an intrusion affecting internal documents, including some personal information, without reported effects on its customer system. [S19][S55]

Another organisation's mailbox was used to send phishing messages; it reported no indication of wider system effects. [S58]

A services company reported a summer incident and subsequent employee-data leakage. The source describes administrative information and a shutdown; the leak-site label remains a separate assertion. These disclosures do not establish the same actor, entry route or data population. [S59]

A separate November regional-healthcare notice described a staff mailbox sending unpaid-invoice lures. The authority said IT had isolated the event and found no indication of effects on other staff or systems at publication. [S32]

5.4 Recent activity: 8–22 November 2026

The table distinguishes when information became public from the timing and certainty of the underlying event. November is not compared with a complete prior month as a growth measure.

Date of notice	Activity or update	What remains distinct
November	Healthcare staff mailbox used for invoice lures	Separate incident; no wider-system effect indicated at publication [S32]
17 November	CERT-SE warns of several phishing campaigns	Campaign warning, not a national victim count [S33]
18 November	Lyko gives a formal scope update	Detection on 12 November; Sweden and all-market populations separated [S28]
19 November	Cabonline supplier-related booking notice	Journey-data risk and onward-sharing uncertainty [S29]
20 November	Rail reservation abuse under police investigation	No evidence of railway-control access; purpose and offender unresolved [S41]
20 November	Universeum supplier disclosure	Late-October event; no relationship inferred from geography [S30]
20 November	Gothia Towers external-web notice	Possible form exposure versus reported ticket-information leakage [S31]

The recent period also contains three Swedish-labelled ransomware listings. Their publication dates do not establish when an intrusion began or independently confirm any dossier above. [S2]

5.5 Vulnerability advice is not an incident count

CERT-SE's October PHP warning and the vendor advisories support immediate applicability checks. Both identifiers below were checked against NVD. Their existence does not establish exploitation at a Swedish organisation. [S13][S14][S15][S16]

Identifier	Affected scope	Minimum fixes for this flaw	Response
CVE-2026-109618	Earlier releases in the listed PHP branches; unsupported older branches need vendor-supported fixes or migration	PHP 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12	Identify applicable deployments, update and investigate relevant signs of access
CVE-2026-109619	Earlier releases in the listed PHP branches; actual exposure depends on deployment and request handling	PHP 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12	Use supported vendor guidance; temporary measures are not equivalent to a complete fix

These are the October minimum fixes for two named vulnerabilities, not a recommendation to deploy an outdated release. The vendor published later security releases on 19 November. Deploy the current supported security release appropriate to the environment. If immediate updating is impossible, assess isolation with the service owner. [S14]

KEY TAKEAWAYS

01
Preserve event, discovery and disclosure dates as different facts.

02
Keep supplier events, customer notifications and people as different units.

03
Address customer and personal-safety consequences alongside technical recovery.

CHAPTER 06

Hacktivism, availability and operational systems

THIS CHAPTER ANSWERS

How do claims differ from a verified service or physical effect?

3

separate questions: claim, service effect and operational effect

6.1 A chronology of statements, not an attack counter 50

6.2 Keep claims and official accounts alongside each other 51

6.3 Verify the task the user needs 52

6.4 Political neutrality in incident communications 52

CHAPTER 06

Hacktivism, availability and operational systems

IN SHORT

A public claim, a responding website and a functioning physical process are different evidence. Official refrigeration warnings justify operational checks without supplying a common actor or a national victim count. A prior-year heating attempt disclosed in 2026 must retain its earlier event date. Keep the service timeline separate from actor messaging, and give engineering responsibility for verifying safe settings and local control.

6.1 A chronology of statements, not an attack counter

15 Apr 2026	**Government account as reported by AP** An unsuccessful heating-operator attempt in 2025 was disclosed; source attribution remains the minister's [S38]
14 Sep 2026	**NCSC and partner assessment** No major information or cyberattacks affecting election conduct were reported in the stated assessment [S39]
2 Oct 2026	**NCSC** Warning of phishing messages impersonating NCSC and FRA; agency branding does not authenticate a message [S42]
2 Nov 2026	**NCSC** Refrigeration incidents acknowledged; organisations urged to review connected equipment [S25]
5 Nov 2026	**NCSC** Wider European refrigeration warning; no national incident count supplied [S17]
17 Nov 2026	**CERT-SE** Several phishing campaigns against Swedish organisations observed [S33]

The entries use publication dates. The heating-operator entry concerns a 2025 attempt, rather than a 2026 attack. The election entry is an official assessment with a defined subject, rather than proof that no accounts were targeted.

A 22 April Spanish-language relay says a video was reuploaded. Its surrounding account refers to a heating event in 2025. The excerpt establishes circulation of a claim, not video authenticity, a new 2026 attack, actor identity or independent state attribution. [S1]

Evidence card B15 — 22 Apr 2026

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

ORIGINAL

[…] volvimos a subir el video del ataque […]

TRANSLATION

[…] we reuploaded the attack video […]

Note. The 2026 post adds evidence of claim circulation. It does not change the alleged underlying event year, 2025, or independently corroborate an actor attribution.

Held
A Spanish-language relay links a reupload claim to a Swedish minister's discussion of a 2025 heating-plant event and refers to NoName057(16).

Not established
Video authenticity, independent examination of the footage, target-system access, actor identity, state attribution or a new 2026 incident.

6.2 Keep claims and official accounts alongside each other

Question	Actor or public assertion	Official or reported account	Defensible conclusion
Was physical harm established?	Images or claims can assert control	NCSC acknowledged refrigeration incidents without a complete national impact total [S25]	Verify local settings, process history and safety consequences
Who was responsible?	An alias can claim responsibility	The heating attribution is the minister's account of a prior-year attempt [S38]	Do not transfer that attribution to another event
Did an outage expose data?	A claimant may assert several outcomes	Manufacturing reporting describes a shutdown and production effect [S27]	Availability and information access require separate evidence
Did election conduct suffer a major attack?	Political messaging can allege interference	NCSC's post-election statement reported no major attacks affecting conduct in its assessment [S39]	Preserve that bounded official assessment without claiming universal absence

No attacker-to-authority numerical ratio is calculated. The statements describe different units and levels of verification. This report does not turn politically framed language into a verified cause of a service interruption.

6.3 Verify the task the user needs

For a public service, monitor whether people can complete the critical task, not only whether the homepage answers. Identity, payment or document delivery can remain unavailable while a landing page works. Preserve service monitoring, provider mitigation records and customer-support reports together.

For operational equipment, verify the physical process with authorised engineering staff. A remote-access change can require a different response from a network outage. Confirm safe local control, restoration authority and supplier access before reconnecting equipment.

Do not infer success or failure of every defensive control from an incident announcement. Protective isolation can itself interrupt a service. Communications should distinguish attacker effects from deliberate containment where the evidence supports that distinction.

6.4 Political neutrality in incident communications

Repeat only the minimal actor claim needed to explain the defensive question. Remove slurs, calls to harm, religious insults and slogans. Preserve official state attribution as a source assessment. Do not describe NATO accession, religious incidents or government decisions as a proven attack cause without specific source evidence.

A retained forum post solicits technical help against a hosting company and asserts that it serves a Swedish political website. The Swedish link is indirect; the host's corporate and infrastructure geography remain uncertain. The post establishes incitement, not an attempted or successful intrusion. Personal details and inflammatory allegations are withheld, and it is not counted as a confirmed Swedish incident. [S1]

An actor's chosen target list does not establish hostility by a population, political party or country. Readiness should follow a relevant threat and the service dependency. Keep public updates factual, time-bounded and useful to users.

KEY TAKEAWAYS

01
Verify service and physical effects separately from claims.

02
Preserve the earlier event date in a later disclosure.

03
Use factual status messages without adopting actor rhetoric or political explanations.

CHAPTER 07

Threat actors, listing labels and attributed campaigns

THIS CHAPTER ANSWERS

Which relationships are supported by which evidence?

24

claimant labels in Sweden's ransomware-listing population

7.1 The relationship map records evidence links 54

7.2 Ransomware listings and regional context 55

7.3 International advisory attributions remain attributed 57

7.4 Claims need proposition-specific confidence 59

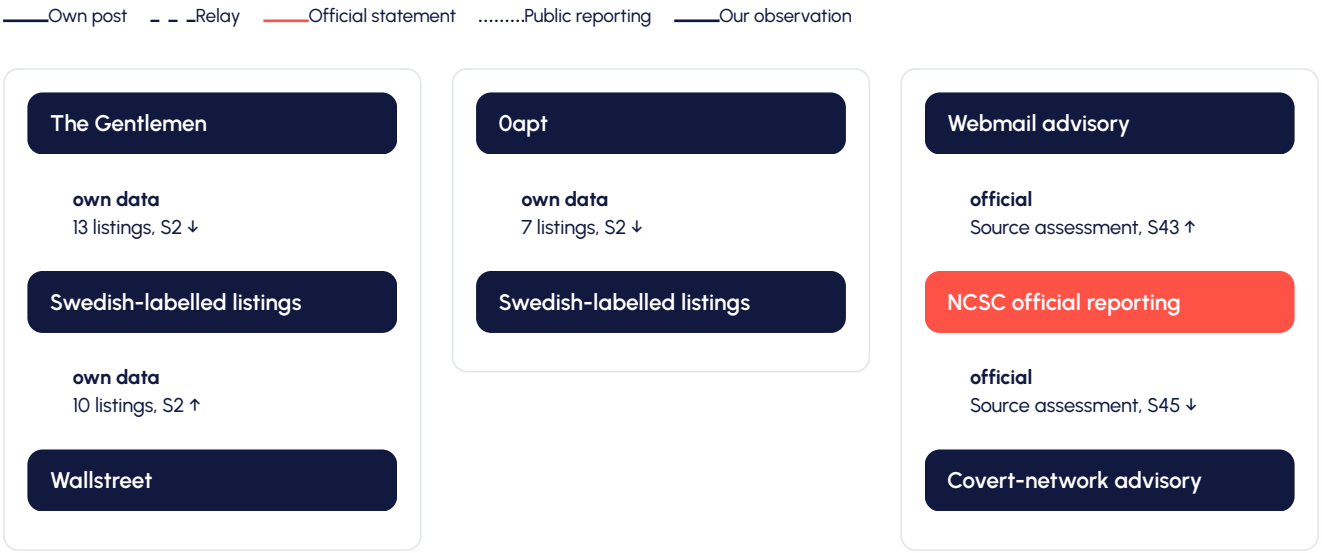
CHAPTER 07

Threat actors, listing labels and attributed campaigns

IN SHORT

Ransompedia records 24 claimant labels in 62 Swedish-labelled listings. The leading three labels account for 30 listings. These are recorded assertions, not verified operators, code families or completed intrusions. Official international advisories describe other campaigns with their own attributions and scope. Keep each relationship tied to its source, and prioritise the access or service behaviour that defenders can validate.

7.1 The relationship map records evidence links



NO EVIDENCED LINK TO OTHER ACTORS

The map joins listing labels to the retained listing population as **own data**. It joins official campaign assessments to their issuing source. It does not draw a shared-operator edge between a criminal advertisement, a refrigeration event and an international advisory merely because they concern Sweden.

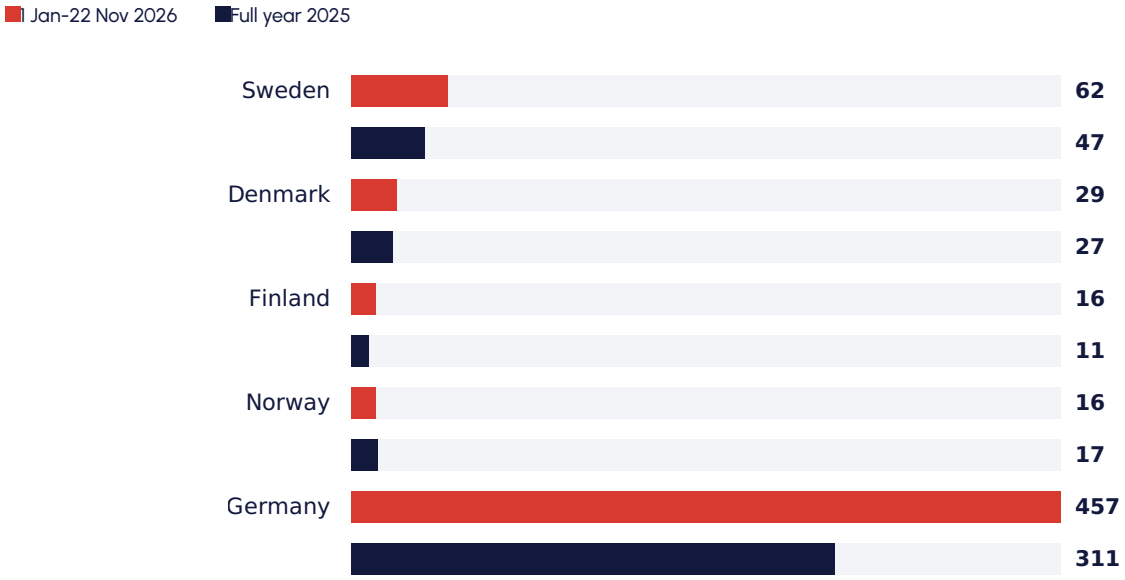
No common operator is established across those populations. Any wider criminal-service chain would be an **analytical model**, not an observed transaction or affiliation. Post similarity alone would not establish a transfer of data or access.

7.2 Ransomware listings and regional context

Denmark, Finland and Norway provide Nordic service context. Germany supplies a larger Baltic Sea industrial comparison.

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

Swedish-labelled listings require recovery readiness across several sectors



Source: Brandefense Ransompedia, 1 January-22 November 2026 versus full-year 2025 [S2]. Unequal periods; country-labelled claims, not unique victims, confirmed intrusions or a national security ranking.

Country	2026 window listings	Full-year 2025 listings	Interpretation
Sweden	62	47	Partial-year listing population
Denmark	29	27	Separate country-labelled population
Finland	16	11	Separate country-labelled population
Norway	16	17	Separate country-labelled population
Germany	457	311	Larger, separate listing population

Source: Ransompedia [S2]. The periods are not matched years. Differences are not population-adjusted attack rates, defensive effectiveness or a ranking of national security. Country labels may describe a group, subsidiary or cross-border activity.

The Swedish population includes repeat appearances of an organisation and a cross-border naming issue. The count remains 62 listings, rather than a revised claim about unique Swedish organisations. Manufacturing has 11 listings, consulting 8 and health 7; these source sectors do not establish national incident rates. [S2]

The Gentlemen, Wallstreet and 0apt account for 13, 10 and 7 listings respectively. Together that is 30 of 62, or 48.4%. The other 32 listings use other labels. A label does not establish a unique affiliate, technical method, successful encryption or completed payment. [S2]

The Gentlemen

Label in the retained listing population

Ransomware/extortion listing label | No state attribution established here

IN SWEDEN, 2026

2026 window

13 Swedish-labelled listings, S2

CLAIMED TARGETS

Listed organisations; identities withheld and country association qualified

SEEN IN PUBLIC REPORTING

[S2] 13 listings recorded in Ransompedia

OUR ASSESSMENT

A listing verifies an extortion assertion. It does not establish a unique operator, code lineage, encryption, data authenticity or payment. Validate an owned alert and prepare recovery independently of branding.

CONFIDENCE

High for the recorded count; individual claims unverified

Wallstreet

Label in the retained listing population

Ransomware/extortion listing label | No state attribution established here

IN SWEDEN, 2026

2026 window

10 Swedish-labelled listings, S2

CLAIMED TARGETS

Listed organisations; identities withheld and country association qualified

SEEN IN PUBLIC REPORTING

[S2] 10 listings recorded in Ransompedia

OUR ASSESSMENT

A listing verifies an extortion assertion. It does not establish a unique operator, code lineage, encryption, data authenticity or payment. Validate an owned alert and prepare recovery independently of branding.

CONFIDENCE
High for the recorded count; individual claims unverified

0apt

Label in the retained listing population

Ransomware/extortion listing label | No state attribution established here

IN SWEDEN, 2026

2026 window
7 Swedish-labelled listings, S2

CLAIMED TARGETS

Listed organisations; identities withheld and country association qualified

SEEN IN PUBLIC REPORTING

[S2] 7 listings recorded in Ransompedia

OUR ASSESSMENT

A listing verifies an extortion assertion. It does not establish a unique operator, code lineage, encryption, data authenticity or payment. Validate an owned alert and prepare recovery independently of branding.

CONFIDENCE
High for the recorded count; individual claims unverified

7.3 International advisory attributions remain attributed

NCSC's July webmail advisory relays a joint assessment led by NSA with partner agencies. It describes probable Russia-linked actors and vulnerable Zimbra webmail. The source does not provide a Swedish victim count or establish that every exposed deployment was accessed. [S43]

A separate July router advisory concerns network-device protection and source-attributed Russian-state targeting. An April advisory describes what the issuing agencies call China-nexus covert networks. Neither creates a named Swedish victim or attributes the unrelated cases in Chapter 5. [S44][S45]

Joint webmail advisory

Official international campaign advisory | Attribution remains the cited agencies' assessment

IN SWEDEN, 2026

2026

Official advisory, S43

CLAIMED TARGETS

Source-defined international population; no Swedish victim inferred

SEEN IN PUBLIC REPORTING

[S43] NCSC official supporting advisory

OUR ASSESSMENT

NCSC relays the issuing agencies' probable Russia-linked assessment. No Swedish victim count or link to the report's other incidents is established.

CONFIDENCE

High for the official statement; no independent operator attribution

Covert-network advisory

Official international campaign advisory | Attribution remains the cited agencies' assessment

IN SWEDEN, 2026

2026

Official advisory, S45

CLAIMED TARGETS

Source-defined international population; no Swedish victim inferred

SEEN IN PUBLIC REPORTING

[S45] NCSC official supporting advisory

OUR ASSESSMENT

The issuing agencies use China-nexus attribution. This is source attribution and international campaign context, not evidence of a named Swedish infection.

CONFIDENCE

High for the official statement; no independent operator attribution

The report does not add technique identifiers where the cited passage lacks an explicit mapping. The operational priorities remain supported software, controlled management access, useful device logs and strong remote authentication. An advisory is a reason to assess an applicable asset, not evidence of that asset's infection.

7.4 Claims need proposition-specific confidence

Confidence can be high that a post or listing exists, while confidence in the offered asset remains unresolved. Similarly, a company can confirm information access while the perpetrator remains unknown. Keep those propositions separate in actor cards, case headings and management briefings.

An alias can change, and a listing service can display several labels. Do not infer a person's identity, location, ideology or state connection from the name alone. Source attribution and technical linkage need their own evidence.

KEY TAKEAWAYS

01

Listing labels count claims rather than verified operators.

02

International advisories retain their source's attribution and geographic limits.

03

Link evidence populations only when a concrete relationship supports the edge.

CHAPTER 08

Fraud, information trading and secondary harm

THIS CHAPTER ANSWERS

How can information support a convincing request without proving an intrusion?

132

distinct Sweden-labelled card-number records; narrow retained-post scope only

8.1 Context is not authentication 61

8.2 Recruitment and advertised information services 61

8.3 Payment-card material: a narrow observation 62

8.4 Police warnings show different paths to deception 63

8.5 Prepare support for people, not only systems 63

CHAPTER 08

Fraud, information trading and secondary harm

IN SHORT

Identity and contact information can make a false request credible without giving the caller legitimate authority. The retained posts show lead advertising, information demand and recruitment claims. Police reporting supplies separate evidence of impersonation tactics. Neither population establishes a common operator or national fraud loss. Verify consequential requests independently and connect customer support, fraud and privacy decisions when information is exposed.

8.1 Context is not authentication

A caller who knows a booking, invoice, name or personal identity number may sound convincing. These facts do not prove control of the relevant account or authority to change a payment. Cases D, O and P identify different information categories that require proportionate review.

The model connecting information to later impersonation is an **analytical model**. This report does not establish that a particular retained seller supplied a particular fraud campaign. The public warnings below stand on their own evidence.

8.2 Recruitment and advertised information services

Evidence card B08 — 24 May 2026

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

ORIGINAL

ГЕО: Польша Чехия Румыния Норвегия Швеция

TRANSLATION

Geography: Poland, Czechia, Romania, Norway, Sweden.

Note. The excerpt removes contact details and avoids amplifying derogatory language.

Held
A Russian-language recruitment post includes Sweden among advertised geographic markets.

Not established
A Swedish victim, successful fraud, active local workers, nationality or a common operator with other posts.

Evidence card B12 — 7 Nov 2026

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

ORIGINAL

This High quality phone database you can use for Spam [...] Sweden-100k

Note. The post precedes the recent-activity window. Similar titles and quantities elsewhere do not establish the same file or operator.

Held
A 7 November post advertises country-labelled phone lists and claims 100k entries for Sweden.

Not established
Authenticity, unique subscribers, collection date, origin, lawful provenance, delivery or actual spam activity.

The Russian-language recruitment excerpt includes Sweden among several geographic markets. It establishes an advertisement, not active local workers, successful fraud or a Swedish victim. A language choice does not establish nationality or state direction. [S1]

A phone-list advertisement published on 7 November claims a Swedish quantity of 100k within a multi-country offer. It precedes the recent period. The quantity, authenticity, subscribers, origin and delivery are unverified; it is not a telecom-provider incident count. [S1]

A personal-identity request is also not proof of bypassing know-your-customer controls. Check the claimed capability separately from the account or transaction involved. The report does not estimate illicit-account availability from advertisements.

Additional advertisements and requests include Nordic social accounts, mailbox access, identity-verification services, caller-identity manipulation and payment-mule recruitment. A phishing-panel advertisement imitates a music service and claims several credential or approval stages; it does not establish compromise of that service. A multinational gambling-data offer includes Sweden without a verified Swedish share. These are different claimed inputs to deception, not evidence of a shared operator or completed fraud chain. Defenders should review suspicious account recovery, caller-directed approvals and unusual payment changes against their own evidence. [S1]

A contact-lookup bot advertisement separately claims a large multinational inventory and includes Sweden. It does not establish a breach of the caller-identification service it references, the origin of the records or a verified Swedish-person total. A participant also challenges the plausibility of fields in a gambling-data sample; that criticism is an unverified forum assessment, rather than independent proof that the advertised dataset is genuine or fabricated. [S1]

An additional 19 August advertisement offered country-labelled identity data, including purported Swedish ID-linked records. It establishes advertising, not possession, authenticity, valid identifiers or a fresh organisational intrusion. [S1]

8.3 Payment-card material: a narrow observation

SCOPE OF THE CARD FIGURES

These figures describe a limited observed publication population. They do not estimate Swedish card theft, fraud losses or payment validity.

The retained posts contained 132 distinct card-number records labelled Sweden, with 141 appearances in 135 posts. No named issuer is established. The country label, actual issuance, stolen status and payment validity remain unverified. These are observed records in a narrow post population, rather than confirmed stolen Swedish cards. [S1]

No recommendation to cancel a card follows from this count alone. An issuer or customer receiving a relevant validated alert should use its established fraud-response process and the specific information exposed. No personal or operational payment details are published here.

8.4 Police warnings show different paths to deception

Publication	Documented pattern	Defensive implication
28 January	A false rental-car text leads to a caller impersonating a bank [S35]	End the contact and reach the real institution independently
24 April	Text messages impersonate traffic-fine requests and demand linked payment [S34]	Verify the purported official demand outside the message
September	Criminals impersonate real creditworthy firms through newly created web identities and unpaid orders [S52]	Confirm the business, contact and delivery instructions through independent records
2 October	NCSC warns that its and FRA's names are used in false official messages [S42]	Branding and a threatened deadline do not authenticate a request
12 November	Police describe delivery-pretext calls passed to false bank staff [S71]	A transfer between callers is not independent verification
12 November	A payment-card impersonation investigation describes deceptive messages and a callback route [S72]	Review the requested card-enrolment action, rather than trusting the claimed alert

The police sources describe warnings or investigations at their stated dates. Allegations remain allegations; an arrest or charge is not a conviction. The report does not add their case amounts into a national loss estimate.

8.5 Prepare support for people, not only systems

A warning should identify the information actually involved, the action a recipient can take and a safe way to ask for help. Avoid directing people to supply sensitive records through an unverified channel. Where travel or health context is involved, assess personal-safety consequences with the appropriate owner.

Technical restoration and fraud protection have different closure tests. A restored booking service does not remove a caller's knowledge of older journeys. Review unusual changes to payments, contact details or account recovery while preserving normal access for legitimate users.

KEY TAKEAWAYS

01

Genuine personal details do not authorise a consequential request.

02

Keep the narrow card-post observation separate from stolen-card and fraud-loss claims.

03

Prepare safe customer support and independent verification for the secondary phase.

CHAPTER 09

Banking, financial leads and payment continuity

THIS CHAPTER ANSWERS

Which financial observations concern an institution, a customer or a payment dependency?

23 of 25

selected finance domains publish reject or quarantine DMARC policies

9.1 Selected finance domains are not a licensed-bank census 65

9.2 A bank-themed lead is not a bank-system finding 66

9.3 Customer action and provider access require separate evidence 66

9.4 External payment-page information exposure is another unit 67

9.5 Continuity includes the merchant and the customer 67

CHAPTER 09

Banking, financial leads and payment continuity

IN SHORT

Financial lead advertising does not establish access to a bank's systems or customers' money. The selected finance-domain cell supplies exposure associations alongside bounded configuration observations. Police warnings concern deception and consequential customer actions. Separate institutional access, customer impersonation and payment-service continuity, then assign each a validation and response owner.

9.1 Selected finance domains are not a licensed-bank census

The finance cell contains 25 selected domains, not every licensed bank, financial entity or independent Swedish legal person. 23 publish reject or quarantine DMARC policy, and 2 publish monitoring policy. These are public configuration observations, not a sector exposure rating. [S3]

SPF records are present for 24 domains, DKIM-related records observed for 22 and DNSSEC delegation records for 16. TLS validation succeeded for 24; one result is unavailable. HSTS was observed for all 22 finance domains with available HSTS results; results for the remaining 3 selected domains are unavailable. No universal finance-sector conclusion follows. [S3]

Question	Available observation	Response owner
Does the selected domain publish enforcing DMARC?	23 of 25	Messaging and domain owner
Is an institution's current credential offered?	7 of 24 assessed finance domains had a current listing [S4]	Identity owner after an authorised alert
Are device associations connected to current access?	At least 10,673 device associations; current access unverified [S4]	Endpoint and identity teams
Does a lead offer establish customer account access?	No validated relationship established	Fraud and customer protection
Can payment services continue during a dependency outage?	No institution-specific assurance from this report	Payments and continuity owners

9.2 A bank-themed lead is not a bank-system finding

Evidence card B03 — 31 Mar 2026

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

ORIGINAL

We are selling specific bank leads for all popular destinations in EU + America (+ some Asia)

Note. The post quotes 170 EUR per 1k specific bank leads. It does not establish that a bank supplied the information.

Held
A seller advertises financial leads and includes a Swedish bank-themed example among several countries.

Not established
Source, consent, validity, current bank relationship, account access, available balance or completed sale.

The advertisement offers bank-themed leads across several countries and includes a Swedish example. It quotes 170 EUR per 1k leads. That is an advertised asking price and unit, not a completed sale, account value or verified bank relationship. [S1]

A lead may be a contact record, older marketing material, a misleading description or information from another source. The report does not establish that a bank supplied the data, that the named person holds an account or that a balance can be accessed.

B14's recent multi-country broker advertisement retains the same limits. Do not link a financial-themed list to an unrelated airline payment incident or the private selected-domain portfolio without specific evidence. [S1]

Case U in Chapter 4 concerns advertised institutional remote access, whereas B03 concerns financial contact leads. The former asserts a technical capability and the latter offers records. Neither is independently validated, and neither establishes a licensed bank intrusion. Route a relevant access alert to the infrastructure owner and SOC; route lead-list misuse to fraud and privacy teams. [S1]

9.3 Customer action and provider access require separate evidence

Police warnings show messages leading recipients to a purported bank, sometimes through a callback or call transfer. The relevant question is what the customer is being asked to approve. Knowing genuine personal facts, an invoice amount or a service name does not authenticate that request. [S35][S71][S72]

Institutions should provide an independent contact route and a safe way to verify card enrolment or payment changes. Review customer-reported events with the actual transaction and authentication evidence. Do not infer bank infrastructure access from a customer being deceived.

9.4 External payment-page information exposure is another unit

Reporting described an airline's warning that malicious code on supplier-hosted web pages may have exposed card information for some customers, including in Sweden. [S40]

This is attributed company reporting with an international population, not a count of Swedish stolen cards from the retained post dataset. The supplier was not named in the cited account. No relationship with the reservation case or a particular web-technology supplier is established here.

9.5 Continuity includes the merchant and the customer

The Riksbank's assessment connects payments to electricity and communications. Test the loss of a dependency without assuming a malicious cause. Include the merchant, customer-support route, reconciliation and resumption decision in the exercise. [S7]

Exposure observations cover 24 of the 25 selected finance domains; one remains unknown. The bank-domain subset contains 11 assessed domains. It includes 6 with a current listing and 71 employee-device associations. These observations do not establish institutional intrusion. [S4]

The narrower bank view contains at least 5,032 device associations not identified as employee devices. Ownership and current access remain unverified. The payment-card material establishes no verified issuer attribution, so it supplies no validated card-to-bank relationship or issuer ranking. Maintain separate identity, endpoint and customer-fraud validation queues. [S1][S4]

KEY TAKEAWAYS

01

Financial themes and lead prices do not establish bank-system access.

02

Keep finance-domain configuration observations within their selected denominator.

03

Validate customer actions and payment dependencies separately from institution exposure.

CHAPTER 10

Regulation and national response

10

THIS CHAPTER ANSWERS

Which trigger, recipient and deadline apply to this incident?

15 January 2026

Sweden's Cybersecurity Act entered into force

10.1 Start with the applicable legal entity 69
10.2 Keep the reporting clocks distinct 69
10.3 Privacy duties follow the information and the risk 70
10.4 DORA exceptions require an explicit decision 71
10.5 Sanctions are exposure, not a forecast fine 71

CHAPTER 10

Regulation and national response

IN SHORT

Sweden's Cybersecurity Act, GDPR and DORA ask different questions about the same event. A significant service incident, a personal-data breach and a major financial-sector ICT incident can overlap without sharing a single clock. Current guidance directs cybersecurity-law reports to NCSC. Establish legal scope, reporting authority and backup access to each reporting route before an incident; record awareness and classification times separately.

10.1 Start with the applicable legal entity

The Cybersecurity Act, Cybersäkerhetslag (2025:1506), entered into force on 15 January 2026. Applicability depends on the statutory definitions, activities and exceptions. A sector label in this report is not a determination that every selected organisation falls within the law. [S8]

Legal and compliance owners should document the entity, activity, size or other inclusion basis, supervision and relevant exclusions. Section 10 of Chapter 1 addresses equivalent security or incident-reporting requirements under other legislation. Do not assume either universal duplication or a universal financial-sector exemption. [S8]

Management must also understand its responsibilities. Chapter 2 requires appropriate and proportionate security measures and training for management. A reporting checklist alone does not demonstrate implementation. Record which executive accepts residual risk and which service owner supplies evidence that the measures work. [S8]

10.2 Keep the reporting clocks distinct

The table gives the principal triggers and sequence. It is an operational reading guide, not a legal opinion on an individual incident.

Regime	Trigger	Principal timing	Recipient
Cybersecurity Act	A significant incident for an in-scope operator	Early information within 24 hours of awareness; incident notification within 72 hours, or 24 hours for trust-service providers	NCSC through the current reporting route [S8][S9]
Cybersecurity Act follow-up	The same reported incident	Final report within one month after the incident notification; a progress report if ongoing, followed by a final report within one month after handling ends	Same designated authority [S8]

Regime	Trigger	Principal timing	Recipient
GDPR	A personal-data breach, unless risk to people's rights and freedoms is unlikely	Notify the competent supervisory authority within 72 hours of awareness where feasible; explain delay	IMY or other competent data-protection authority [S10]
DORA	A major ICT-related incident at an in-scope financial entity	Initial report as early as possible, within 4 hours of major classification and normally no later than 24 hours after awareness	Relevant financial supervisor; Swedish reporting guidance from Finansinspektionen [S11][S12]
DORA follow-up	The same major ICT incident	Intermediate report within 72 hours of initial notification, even if incident status or handling is unchanged. Updated intermediate report without undue delay and, in any case, when regular activities recover. Final report within one month of the intermediate or latest updated intermediate report	Financial supervisor [S11]

The cybersecurity law also provides for an intermediate report when the authority requests one. A significant incident includes serious actual or potential service disruption or financial damage, or considerable harm to other people or organisations. Assess the applicable criteria rather than waiting for certainty about an attacker. [S8]

PTS states that cybersecurity-law reports go to NCSC and are forwarded to the relevant supervisory authority. Its guidance distinguishes this route from eIDAS reports for trust services, which go to PTS. A single portal assumption can therefore send a correct report to the wrong recipient. [S9]

10.3 Privacy duties follow the information and the risk

IMY's guidance requires an assessment of the consequences for people. Where notification is required, incomplete facts can be supplemented. A controller should document the incident and its rationale even when it concludes that notification is not required. [S10]

Communication to affected people has a different trigger: likely high risk to their rights and freedoms. The default is communication without undue delay. A criminal listing does not automatically establish that trigger; a supplier's confirmed data loss can require urgent assessment even before the full population is known. [S10]

Maintain a distinction between controller and processor. Ask who determines the processing purpose, who holds the relevant copy and when each party became aware. Contractual notice commitments support the response but do not replace statutory duties.

10.4 DORA exceptions require an explicit decision

If major classification occurs after the initial 24-hour awareness period, the initial notification is due within 4 hours of that classification. Record why the classification changed and preserve the supporting times. Do not silently replace awareness with the date of a later public statement. [S11]

The regulation allows specified weekend and bank-holiday timing relief, with exceptions for initial and intermediate reports by credit institutions and other listed entities. Supervisors can also exclude certain significant entities. Do not assume that a bank can wait until the next working day. Check Article 5 and the entity's supervisory position. [S11]

Finansinspektionen's October guide describes delegated portal permissions and the three reporting stages. Confirm that authorised staff can submit a report while normal identity or communications services are unavailable. Retain the receipt and the link between successive reports. [S12]

10.5 Sanctions are exposure, not a forecast fine

Chapter 4 of the Cybersecurity Act sets a minimum administrative fee of SEK 5,000. For essential private operators, the maximum is the greater of 2% of preceding global annual turnover or the SEK equivalent of EUR 10,000,000. [S8]

For important private operators, the corresponding maximum is the greater of 1.4% or EUR 7,000,000. The maximum for public operators is SEK 10,000,000. These statutory amounts are not a prediction of a fine for any case in this report. [S8]

The useful board question is whether scope, controls, training, reporting access and decision records can be demonstrated. Do not infer a legal violation from a missing configuration observation, an underground advertisement or a precautionary service shutdown.

KEY TAKEAWAYS

01

Record awareness, significant-incident assessment and major classification separately.

02

Verify the current recipient and an authorised backup reporting route.

03

Legal scope and risk to people require an owned decision, not a conclusion from a listing.

CHAPTER 11

Outlook and conditional scenarios

11

THIS CHAPTER ANSWERS

Which signals would change the priorities after the cut-off?

4

conditional planning scenarios, not probability estimates

11.1 Key judgements and their limits 73

11.2 Four planning assumptions 74

11.3 What would change this assessment 74

CHAPTER 11

Outlook and conditional scenarios

IN SHORT

The evidence supports preparing for identity misuse, supplier-data consequences, extortion and disruption of connected operations. It does not establish a national attack probability or a common operator behind the disclosed incidents. The scenarios below describe decisions if specified signals appear. Assign an owner to each trigger, keep alternatives visible and revise the assessment when organisation evidence changes.

11.1 Key judgements and their limits

The judgements describe propositions, rather than a blanket confidence score for Sweden or an actor.

Judgement	Confidence and basis	Limit	Decision
Supplier access and supplier-held data can create several customer responses	High for the documented cases in Chapter 5	Different suppliers and incident scopes; no common campaign established	Rehearse an update and notification process with critical suppliers
Identity misuse can turn a familiar sender into a phishing route	High for disclosed mailbox cases and the CERT-SE warning	The report cannot measure all successful phishing or every affected account	Validate sign-ins, sessions and message traces together
Extortion readiness remains justified across sectors	High that 62 Swedish-labelled listings were observed [S2]	Listings are claims; labels and repeated organisations limit geography and uniqueness	Demonstrate restoration and a decision process for data-theft claims
Connected equipment requires an operational response owner	High for the official refrigeration warnings	Neither nationwide impact nor a common operator is established	Verify exposure and safe local control with facilities and suppliers
Published post volume cannot predict future successful attacks	High for this evidential limitation	Visibility and repeated advertising affect the population	Use validated asset-specific evidence to choose containment

A high-confidence disclosure can still leave entry route, actor and population unresolved. Carry those unknowns into the response record. Avoid promoting a cautious case description into a stronger headline or management conclusion.

11.2 Four planning assumptions

Scenario A: relevant credential evidence appears

If a current owned account is validated, review sign-ins and privileges, revoke relevant sessions and rotate affected secrets. If the record is historical and already remediated, document that disposition. Neither outcome should be inferred from a seller's wording.

Scenario B: a supplier revises the affected-data scope

If newly confirmed categories include travel, health, children or protected-contact information, reassess harm to people and communication needs. If only an old public export is matched, narrow the assessment. Retain the supplier's successive statements rather than overwriting the first notice.

Scenario C: an operational controller behaves unexpectedly

If local records confirm changed settings or loss of safe control, activate engineering isolation and the agreed fallback. If the issue is a communications outage without manipulation evidence, preserve that distinction. A screenshot or political claim alone does not establish the physical outcome.

Scenario D: a public service receives an availability claim

If service monitoring confirms disruption, engage upstream mitigation and preserve the operational timeline. If no service effect is observed, retain the claim as unverified. Communications should state the measured service effect and the next update time, without reproducing hostile rhetoric.

11.3 What would change this assessment

Validated unauthorised use of an owned account would substantiate an identity incident. A verified supplier report naming the affected system and data would narrow the customer-impact assessment. A technical investigation linking incidents through concrete infrastructure or access evidence could support a campaign relationship.

Conversely, validated historical data, a corrected country label or a ruled-out system association would narrow the conclusion. These are expected forms of analytical revision. They do not require declaring the original unverified claim true or fabricated.

The recent-activity section highlights publication and disclosure within 8–22 November. It does not create a matched growth comparison between periods. New notices after the cut-off belong to a later update even if they describe earlier activity.

KEY TAKEAWAYS

01

Attach confidence to a proposition and preserve its unresolved parts.

02

Trigger containment with validated owned evidence.

03

Update scenarios when scope or attribution changes, while retaining earlier statements.

CHAPTER 12

Action plan and completion evidence

12

THIS CHAPTER ANSWERS

Who acts, under which condition, and what demonstrates completion?

30 / 60 / 90

review milestones; urgent containment starts immediately

12.1 Immediate actions and review milestones 77

12.2 What each role should ask 79

12.3 How Brandefense can help 80

CHAPTER 12

Action plan and completion evidence

IN SHORT

Start urgent validation, containment and applicable security updates immediately. The milestones below are assurance checkpoints, not permission to leave a known critical exposure open. Assign a technical owner and a business owner to each priority service. Completion means evidence that the relevant account, dependency or recovery route works as intended, with unresolved risks explicitly accepted and dated.

12.1 Immediate actions and review milestones

The lanes connect evidence to a response owner. Use the conditions to avoid disruptive actions based only on an advertisement.

1Immediate

Confirm authorised alert sources, monitored assets, accountable recipients and escalation; test a synthetic alert before relying on the handoff

OWNER
CISO, SOC and identity lead

COMPLETION EVIDENCE
Alert received, acknowledged and routed; missing coverage assigned an owner

Prioritise phishing-resistant authentication for privileged and high-risk access; test secure recovery and session revocation

OWNER
Identity and service owners

COMPLETION EVIDENCE
Approved sign-in and recovery exercise; unauthorised sessions lose access

Validate a relevant current-account alert; contain confirmed access and revoke associated sessions

OWNER
Identity lead and incident commander

COMPLETION EVIDENCE
Account disposition, sign-in review and recorded session revocation

Identify applicable critical or actively exploited flaws; update affected services or apply an approved isolation plan

OWNER
Application and infrastructure owners

COMPLETION EVIDENCE
Installed-version evidence and an independent service check

Check internet exposure of operational controllers and the safe isolation procedure

OWNER

Engineering and facilities

COMPLETION EVIDENCE

Approved connectivity inventory, access review and tested local control

2By day 30

Reconcile privileged, service and supplier accounts with accountable owners

OWNER

Identity and procurement

COMPLETION EVIDENCE

Reviewed ownership, rights and expiry records; unowned access removed

Confirm reporting scope, recipients, awareness recording and backup portal access

OWNER

Legal, privacy and compliance

COMPLETION EVIDENCE

Entity-specific decision record and a successful reporting-route exercise

Review external sender domains, legitimate mail flows and authentication policies

OWNER

Messaging team

COMPLETION EVIDENCE

Validated mail inventory, alignment observations and approved remediation

3By day 60

Restore a priority service in isolation, including identity and supplier dependencies

OWNER

Service owner and recovery lead

COMPLETION EVIDENCE

Approved recovery time and accepted data loss compared with measured restoration and reconciliation results; fallback tested

Exercise a supplier scope revision involving customer or employee information

OWNER

Procurement, privacy and customer operations

COMPLETION EVIDENCE

Timed supplier contact, category-specific risk decision and approved notice draft

Exercise an availability incident without assuming data theft

OWNER

Network and communications

COMPLETION EVIDENCE

Mitigation activation, measured service timeline and clear status messages

4By day 90

Re-test unresolved controls and close or explicitly accept each outstanding risk	
OWNER	COMPLETION EVIDENCE
CISO and business executives	Dated sign-off with residual risk, owner and next review date
Exercise a connected-equipment incident with engineering and suppliers	
OWNER	COMPLETION EVIDENCE
Facilities, engineering and safety	Safe-state demonstration, preserved settings and tested recovery authority
Review customer-support resistance to requests using genuine stolen details	
OWNER	COMPLETION EVIDENCE
Fraud and customer operations	Authorised exercise results and independent verification of consequential changes

A failed exercise is useful evidence when it produces an owned correction. Do not mark a control complete because a policy exists or a supplier replied. Demonstrate the behaviour needed during the incident.

If no authorised alert route exists, the CISO should arrange an internal or appropriate provider route and record dependent validation as unavailable until the handoff works. Continue immediate triage of credible evidence already received. Test recovery with an authorised impersonation scenario and a genuine user who has lost a factor.

12.2 What each role should ask

Board and executives. Which service must continue, what minimum operation is acceptable, and who can approve temporary restrictions? Ask for the last observed recovery result and the oldest unresolved dependency risk. A single portfolio number does not answer either question.

SOC and identity teams. Can an alert be tied to an owned account, valid access, current sessions or observed malicious changes? Preserve the difference between historical credentials and current access. Keep a clear route to endpoint, cloud and messaging owners.

Engineering and facilities. Who can change the controller, who notices unexpected settings and who can restore safe local operation? Test these questions with the maintenance provider. Keep safety decisions with authorised operational staff.

Privacy and legal. Which people and data categories may be affected, when did awareness occur and what facts remain missing? Preserve each reporting decision and subsequent revision. A technical recovery announcement does not close the personal-data assessment.

Procurement and supplier management. Can the supplier identify the affected tenant, data copy and support account? Require timely scope updates, evidence preservation and a customer escalation route. Distinguish a supplier's general statement from an assessment of your own service.

Fraud and customer operations. Which requests become more credible if a caller knows real booking, invoice or employment details? Verify consequential changes through an independent established route. Familiar information should provide context rather than authority.

12.3 How Brandefense can help

Brandefense can support teams in reviewing relevant threat intelligence, external exposure and impersonation observations. Agree the monitored brands, assets, alert recipients and validation process before treating a finding as an incident.

Use the report's evidence distinctions when discussing a service: posts describe publication, ransomware listings describe claims, and exposure observations require asset-owner validation. No service engagement removes the need for internal investigation, operational judgement or legal assessment.

Request a Brandefense demo to discuss the assets, decisions and response evidence that matter to your organisation.

KEY TAKEAWAYS

01

Begin urgent containment and security updates now, then verify them at the milestones.

02

Require observed completion evidence from both technical and business owners.

03

Close the incident's service, identity and people-related consequences separately.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Scope and evidence boundaries · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

80
sources

Appendix A. Scope and evidence boundaries 82
Appendix B. Evidence register 85
Appendix C. Sources 86
Appendix D. Glossary 90

Appendix A. Scope and evidence boundaries

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

A.1 Window and source types

The publication window is 1 January–22 November 2026 by post time, with 8–22 November highlighted separately. Public-source verification occurred on 22–23 November 2026. Publication counts and recent material were checked on 23 November, after the UTC cut-off. Notices can describe earlier events, and those dates remain explicit.

Sources comprise dark-web posts collected by Odin by Brandefense, ransomware listings, selected-domain Atlas exposure observations, a configuration snapshot, organisation disclosures, official advisories, regulatory decisions and press reporting. Each source establishes only its own proposition. [S1][S2][S3][S4]

A.2 Posts and observed volume

The observed country-associated post population is 775,020. January and February together contain 727,150, or 93.8%. Publication concentration does not measure successful attacks. Repeated promotion and international material can appear in country-associated observations. November is partial. [S1]

The retained evidence corpus is narrower than that publication population. It supports the cited excerpts and claim dispositions, rather than a complete census of everything published. Some source content remains unavailable. No national crime-family shares, unique-person totals or completed-sale estimate are inferred.

A.3 Selected organisations and configuration observations

The portfolio comprises 250 selected candidate domains in ten sector cells of 25. Selection is purposive and ownership and independence are unvalidated. The results do not estimate prevalence across Sweden. Mail-policy, certificate and HSTS observations retain their assessed denominators. [S3]

A published SPF or DKIM-related record is not proof of correct delivery. DNSSEC delegation presence is not complete validation. TLS and HSTS observations do not establish complete coverage or control effectiveness. Unknown results are not failures, and failed validation requires owner investigation before a cause is assigned.

A.4 Exposure and ratings

The national Atlas headline is 50/100 for 242 assessed domains from the selected 250-domain portfolio. The other 8 domains have unknown exposure. Sector and group exposure ratings are not published. Cumulative device, credential and document associations and current listings require asset-owner validation. [S4]

A.5 Ransomware listings

The 62 Swedish-labelled listings are public criminal assertions recorded in Ransompedia, rather than confirmed intrusions or unique organisations. Repeat appearances and cross-border labels remain relevant limitations. Prior-year figures cover the full year; the 2026 window is partial. [S2]

A.6 Payment-card scope

SCOPE OF THE CARD FIGURES

These figures describe a limited observed publication population. They do not estimate Swedish card theft, fraud losses or payment validity.

The 132 distinct Sweden-labelled records, with 141 appearances in 135 posts, do not establish actual issuance, stolen status or a named bank. They are separate from the externally reported airline payment-page population and cannot be added to it. [S1][S40]

A.7 Public incidents, historical events and exclusions

Fifteen public-event dossiers and seven claim cases illustrate supported decisions. A supplier incident can produce multiple controller notifications. An update can revise an earlier population. The report therefore does not present a deduplicated national incident total.

The public register also records campaign advisories and explicit exclusions. A foreign-subsidiary disclosure about a 2025 event does not establish a Swedish 2026 intrusion. A public transport-sector technical outage, healthcare-system outage and municipal-care disruption lack an established malicious cause in the cited sources. [S48][S49][S50][S51]

IMY issued regulatory decisions during 2026 concerning earlier attacks. These are regulatory outcomes, not new 2026 intrusions. [S37][S36]

An additional visitor-ticket supplier notice is retained as qualified scope context; original-page retrieval was unavailable, and the available official search passage does not independently verify a new supplier incident. A regional bus operator's board record describes manual continuity and says passenger traffic was unaffected. [S46][S47]

A.8 Confidence and naming

Confidence attaches to a proposition. Observation of an offer can be certain while possession remains unverified. A named victim appears only where official confirmation and broad reporting meet the naming rule. Other cases use roles broad enough to fit several organisations.

Where a source path identifies a withheld organisation, a press or official issuer root can be shown with an article-withheld notice. A withheld organisation's own domain is not printed; its public URL is empty. Source availability limits remain explicit rather than becoming false verification claims.

Appendix B. Evidence register

Authentic excerpts are shown inline. Post dates describe publication; no card establishes a completed transaction or a confirmed intrusion by itself.

Card	Date	Venue	Alias	Language	Section
B01	2026-01-30	Forum thread	Alias withheld	English	4
B02	2026-02-15	Forum thread	Alias withheld	English	4
B03	2026-03-31	Forum thread	Alias withheld	English	9
B04	2026-04-23	Forum thread	Alias withheld	English	4
B05	2026-09-05	Forum thread	Alias withheld	English	4
B06	2026-11-18	Forum thread	Alias withheld	English	4
B07	2026-11-19	Forum thread	Alias withheld	English	4
B08	2026-05-24	Forum thread	Alias withheld	Russian	8
B09	2026-04-08	Forum thread	Alias withheld	English	4
B10	2026-04-30	Forum relay	Alias withheld	English	4
B11	2026-03-08	Forum thread	Alias withheld	English	4
B12	2026-11-07	Forum thread	Alias withheld	English	8
B13	2026-11-17	Forum thread	Alias withheld	English	4
B14	2026-11-09	Forum thread	Alias withheld	English	4
B15	2026-04-22	Forum thread	Alias withheld	Spanish	6
B16	2026-04-14	Forum thread	Alias withheld	English	4

Appendix C. Sources

S1: Odin by Brandefense. Retained underground observations and publication counts. URL withheld; source mapping retained. Verified on 2026-11-23.

S2: Ransompedia. Country-labelled ransomware listings, requested window. URL withheld; source mapping retained. Verified on 2026-11-22.

S3: Odin by Brandefense. Configuration snapshot of 250 selected domains. URL withheld; source mapping retained. Verified on 2026-11-22.

S4: Brandefense Atlas exposure observations, 22 November 2026; national rating for 242 assessed selected domains, completed 22 November 2026. Own data; domain identities withheld.

S5: NCSC. Institutional remit and July 2026 transfer. https://www.ncsc.se/sv/om-centret/ Verified on 2026-11-22.

S6: Swedish Civil Defence and Resilience Agency. MSB became Myndigheten för civilt försvar. https://www.mcf.se/sv/om-oss/vart-uppdrag/msb-ar-myndigheten-for-civilt-forsvar/ Verified on 2026-11-22.

S7: Sveriges Riksbank. Payments Report 2026: summary and recommendations. https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-report-2026/summary-and-recommendations/ Verified on 2026-11-22.

S8: Sveriges riksdag. Cybersäkerhetslag (2025:1506). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/ Verified on 2026-11-22.

S9: PTS. Incident reporting under the Cybersecurity Act. https://www.pts.se/sakerhet-och-integritet/cybersakerhetslagen/incidentrapportera-enligt-cybersakerhetslagen/ Verified on 2026-11-22.

S10: IMY. Managing personal-data breaches. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsincidenter/hantering-av-personuppgiftsincidenter/ Verified on 2026-11-22.

S11: EUR-Lex. Delegated Regulation (EU) 2025/301, Article 5. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng Verified on 2026-11-23.

S12: Finansinspektionen. DORA incident-reporting guide, 14 October 2026. https://www.fi.se/globalassets/media/dokument/lathundar//lathund_dora_incidentrapportering_2026-10-14.pdf Verified on 2026-11-22.

S13: CERT-SE. Critical PHP vulnerabilities, updated 27 October 2026. https://cert.se/2026/10/kritiska-s%C3%A5rbarheter-i-php.html Verified on 2026-11-22.

S14: PHP project. Security releases and vendor advisories, 2026 archive. https://www.php.net/archive/2026.php Verified on 2026-11-22.

S15: NVD. CVE-2026-109618. https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Verified on 2026-11-22.

S16: NVD. CVE-2026-109619. https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Verified on 2026-11-22.

S17: NCSC. European refrigeration-system warning, 5 November 2026. https://www.ncsc.se/sv/aktuellt/eu-varnar-for-cyberincidenter/ Verified on 2026-11-22.

S18: Official organisation statement. Mailbox phishing (a regional healthcare authority). https://www.regionvarmland.se/regionvarmland/nyhetsarkiv/press/2026-03-05-region-varmland-drabbat-av-personuppgiftsincident Verified on 2026-11-22.

S19: Organisation statement; identity withheld. Intrusion affecting internal documents (an organisation). URL withheld; source mapping retained. Verified on 2026-11-22.

S20: Organisation statement; identity withheld. IT attack and service disruption (municipal services). URL withheld; source mapping retained. Verified on 2026-11-22.

S21: www.imy.se. Supplier data theft (higher-education customers of a shared learning platform). https://www.imy.se/nyheter/dataintrang-mot-laroplattformen-canvas/ Verified on 2026-11-22.

S22: Official organisation statement. Customer-data theft (a micromobility provider operating in Sweden). https://www.ryde-technology.com/security-incident-2026-08-02 Verified on 2026-11-22.

S23: Organisation statement; identity withheld. Internal-system access and precautionary shutdown (an IT services supplier). URL withheld; source mapping retained. Verified on 2026-11-22.

S24: Organisation statement; identity withheld. IT intrusion and sensitive employee-data theft (a municipality). URL withheld; source mapping retained. Verified on 2026-11-22.

S25: www.ncsc.se. Refrigeration manipulation (grocery retailers and food-distribution operations). https://www.ncsc.se/sv/aktuellt/cyberangrepp-mot-kylsystem/ Verified on 2026-11-22.

S26: www.svt.se. Booking-data access (an airline using an external reservations platform). https://www.svt.se/ (article URL withheld) Verified on 2026-11-22.

S27: www.svt.se. Intrusion and production shutdown (a manufacturer). https://www.svt.se/ (article URL withheld) Verified on 2026-11-22.

S28: Official organisation statement. Limited-system customer-data access (a beauty retailer). https://lyko.com/no/om-lyko/media/pressemeldinger/lyko-har-atgardat-dataintrang-i-en-avgransad-del-av-sitt-system Verified on 2026-11-22.

S29: Official organisation statement. Supplier booking-data access (a taxi service using an external booking supplier). https://www.cabonline.se/it-incident Verified on 2026-11-22.

S30: Official organisation statement. Supplier guest-data theft (a visitor attraction using an external bookings supplier). https://newsroom.notified.com/news/457193/personuppgiftsincident Verified on 2026-11-22.

S31: Official organisation statement. External web-environment intrusion (a hospitality and exhibition operator). https://svenskamassan.se/2026/11/information-om-dataintrang-hos-svenska-massan-gothia-towers/ Verified on 2026-11-24.

S32: Organisation statement; identity withheld. Staff mailbox phishing relay (a regional healthcare authority). URL withheld; source mapping retained. Verified on 2026-11-22.

S33: www.cert.se. Phishing campaign warning (Swedish organisations across sectors). https://www.cert.se/2026/11/uppmanar-till-okad-vaksamhet-natfiske.html Verified on 2026-11-22.

S34: polisen.se. Smishing using false traffic fines (members of the public). https://polisen.se/aktuellt/nyheter/nationell/2026/april/pagaende-vag-av-bedrageriforsok-via-sms/ Verified on 2026-11-22.

S35: polisen.se. SMS to phone social engineering (members of the public). https://polisen.se/aktuellt/nyheter/mitt/2026/januari/polisen-i-region-mitt-varnar-for-ett-nytt-bedragerimodus/ Verified on 2026-11-22.

S36: www.imy.se. Regulatory decision following a prior-year attack. https://www.imy.se/ (article URL withheld) Verified on 2026-11-22.

S37: www.imy.se. Regulatory decision following a prior-year attack. https://www.imy.se/ (article URL withheld) Verified on 2026-11-22.

S38: apnews.com. Attribution of prior-year unsuccessful destructive attempt (a heating operator). https://apnews.com/ (article URL withheld) Verified on 2026-11-22.

S39: www.ncsc.se. Official post-election assessment (election administration). https://www.ncsc.se/sv/aktuellt/inga-storre-informations--eller-cyberangrepp-mot-svenska-valet/ Verified on 2026-11-22.

S40: www.svt.se. Supplier website payment-data exposure (Swedish customers of an airline). https://www.svt.se/ (article URL withheld) Verified on 2026-11-22.

S41: www.aftonbladet.se. Reservation abuse under police investigation (a rail operator). https://www.aftonbladet.se/ (article URL withheld) Verified on 2026-11-22.

S42: www.ncsc.se. Authority-impersonation phishing (recipients of false official warnings). https://www.ncsc.se/sv/aktuellt/nationellt-cybersakerhetscenters-namn-anvands-i-natfiskekampanj/ Verified on 2026-11-22.

S43: www.ncsc.se. International campaign advisory (users of vulnerable webmail). https://www.ncsc.se/sv/aktuellt/co-seal-med-nsa-om-zimbra/ Verified on 2026-11-22.

S44: www.ncsc.se. International campaign advisory (critical-infrastructure network operators). https://www.ncsc.se/sv/aktuellt/nya-internationella-rad-mot-cyberangrepp-pa-sarbar-natverksutrustning/ Verified on 2026-11-24.

S45: www.ncsc.se. International campaign advisory (organisations using connected edge devices). https://www.ncsc.se/sv/aktuellt/nya-internationella-rad-for-att-forsvara-sig-mot-dolda-natverk-med-kopplingar-till-kina2/ Verified on 2026-11-22.

S46: Organisation statement; identity withheld. Supplier booking-data access (visitor attractions using a shared ticket supplier). URL withheld; source mapping retained. Verified on 2026-11-22.

S47: Organisation statement; identity withheld. IT shutdown with manual continuity (a regional bus operator). URL withheld; source mapping retained. Verified on 2026-11-22.

S48: www.maine.gov. Prior-year supplier breach notification (a foreign subsidiary of a Swedish-headquartered company). https://www.maine.gov/ (article URL withheld) Verified on 2026-11-22.

S49: www.cert.se. Technical outage (a public transport-sector body). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S50: www.cert.se. Supplier technical outage (regional healthcare organisations). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S51: www.cert.se. IT disruption (a municipality providing home care). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S52: polisen.se. Fraudulent supplier/customer identity (Swedish businesses). https://polisen.se/aktuellt/nyheter/syd/2026/september/fler-bedragerier-mot-foretag--polisen-varnar-for-metoden/ Verified on 2026-11-22.

S53: www.svt.se. Mailbox phishing (a regional healthcare authority). https://www.svt.se/nyheter/lokalt/varmland/natfiskeattack-mot-region-varmland-personuppgifter-har-lackt Verified on 2026-11-22.

S54: www.svt.se. Intrusion (an IT services supplier). https://www.svt.se/ (article URL withheld) Verified on 2026-11-22.

S55: Organisation statement; identity withheld. Intrusion affecting internal documents (an organisation). URL withheld; source mapping retained. Verified on 2026-11-22.

S56: www.cert.se. IT attack and service disruption (municipal services). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S57: www.cert.se. Supplier data theft (higher-education customers of a shared learning platform). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S58: www.cert.se. Mailbox phishing relay (a public-sector organisation). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S59: www.cert.se. Ransomware and employee-data theft (a services company). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S60: www.svt.se. Customer-data theft (a micromobility provider operating in Sweden). https://www.svt.se/nyheter/lokalt/norrbotten/ryde-utsatt-for-dataintrang-alla-kunder-drabbade Verified on 2026-11-22.

S61: techtidningen.se. Internal-system access and precautionary shutdown (an IT services supplier). https://techtidningen.se/ (article URL withheld) Verified on 2026-11-22.

S62: Organisation statement; identity withheld. IT intrusion and sensitive employee-data theft (a municipality). URL withheld; source mapping retained. Verified on 2026-11-22.

S63: www.cert.se. Booking-data access (an airline using an external reservations platform). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S64: www.cert.se. Intrusion and production shutdown (a manufacturer). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S65: www.aftonbladet.se. Limited-system customer-data access (a beauty retailer). https://www.aftonbladet.se/minekonomi/a/kMJBkk/lyko-hackat-kunduppgifter-lackta Verified on 2026-11-24.

S66: www.svt.se. Supplier booking-data access (a taxi service using an external booking supplier). https://www.svt.se/nyheter/inrikes/taxikunder-drabbade-av-dataintrang-bokningsuppgifter-kan-ha-lackt Verified on 2026-11-22.

S67: www.svt.se. Supplier guest-data theft (a visitor attraction using an external bookings supplier). https://www.svt.se/nyheter/lokalt/vast/dataintrang-hos-universeum-varnar-for-bedrageriforsok Verified on 2026-11-22.

S68: www.svt.se. External web-environment intrusion (a hospitality and exhibition operator). https://www.svt.se/nyheter/lokalt/vast/dataintrang-mot-gothia-towers Verified on 2026-11-22.

S69: www.cert.se. Supplier data theft (higher-education customers of a shared learning platform). https://www.cert.se/ (article URL withheld) Verified on 2026-11-24.

S70: Public-service customer statement; identity withheld. Supplier booking-data access (a taxi service using an external booking supplier). URL withheld; source mapping retained. Verified on 2026-11-22.

S71: Polismyndigheten. Delivery-pretext and bank-impersonation warning. https://polisen.se/aktuellt/nyheter/nord/2026/november/bedragare-kontaktar-aldre-om-falska-mobelleveranser/ Verified on 2026-11-22.

S72: Polismyndigheten. Payment-card impersonation investigation. https://polisen.se/aktuellt/nyheter/stockholm/2026/november/man-haktad-misstankt-for-tio-fall-av-grova-bedragerier-pa-gotland/ Verified on 2026-11-22.

S73: RFC Editor. DMARC protocol reference. https://www.rfc-editor.org/rfc/rfc7489.html Verified on 2026-11-22.

S74: RFC Editor. SPF protocol reference. https://www.rfc-editor.org/rfc/rfc7208.html Verified on 2026-11-22.

S75: RFC Editor. DKIM signatures. https://www.rfc-editor.org/rfc/rfc6376.html Verified on 2026-11-22.

S76: RFC Editor. HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html Verified on 2026-11-22.

S77: SVT. Swedish higher-education users affected by the Canvas incident. https://www.svt.se/nyheter/inrikes/flera-svenska-universitet-drabbade-i-hackerattack Verified on 2026-11-22.

S78: QiAnXin XLab. AryStinger research, 17 June 2026. https://blog.xlab.qianxin.com/arystinger-botnet-hijacks-legacy-routers-for-global-attacks-en/ Verified on 2026-11-24.

S79: Trezor. Recent customer data exposed in shipping provider incident; updated 4 September 2026. https://trezor.io/blog/news/recent-customer-data-exposed-in-shipping-provider-incident Verified on 2026-11-22.

S80: Protos. Trezor says 13,689 customers hit by data breach at shipping partner, 13 August 2026. https://protos.com/trezor-says-13689-customers-hit-by-data-breach-at-shipping-partner/ Verified on 2026-11-22.

Appendix D. Glossary

- **CSIRT.** A computer security incident response team that helps prevent and handle incidents. [S5]
- **DMARC.** A domain policy for handling and reporting mail that fails aligned authentication checks. [S73]
- **SPF.** A mechanism for a domain to authorise sending hosts. [S74]
- **DKIM.** A cryptographic mail signature associating a signing domain with a message. [S75]
- **HSTS.** A browser policy requiring secure connections to the specified site. [S76]
- **DORA.** The EU digital operational resilience framework for in-scope financial entities. [S11]
- **GDPR.** The EU personal-data protection regulation; its breach duties depend on the facts and risk. [S10]
- **NCSC / CERT-SE.** Sweden's national cybersecurity centre and national incident-response function; institutional dates are distinguished in Chapter 2.
- **Personnummer / VIN.** A Swedish personal identity number and a vehicle identification number, respectively; knowledge of either does not authenticate a requester.
- **Controller / processor.** The party deciding the processing purpose and means, and a party processing on its behalf; responsibilities require case-specific assessment.
- **DNSSEC / DS.** Signed DNS information and a delegation record; record presence alone does not establish complete validation.
- **TLS.** Technology protecting a connection.
- **Phishing-resistant MFA.** Authentication designed to prevent credentials being relayed through an impostor service; ordinary code or number confirmation is not automatically resistant.
- **KYC.** Know-your-customer identity checks; an advertised bypass remains a capability claim until validated.
- **Session.** Continuing authenticated access that can require revocation separately from a password change.
- **Post / listing / notification.** A message, a public extortion assertion and a report to an authority; they are different counting units.
- **National Atlas headline.** An exposure summary for the assessed portfolio; neither a breach percentage nor an incident probability.
- **Analytical model.** A proposed explanation or planning relationship that is not an observed transaction chain.
- **TLP:CLEAR.** Shareable without a TLP restriction; privacy and other applicable obligations still matter.

About this report

Prepared by Odin by Brandefense. Version 1.0 covers the window ending 22 November 2026 and highlights 8–22 November separately. Own-data follow-up was completed on 23 November. Evidence types, source dates and remaining unknowns accompany the findings. This is not a national census or assurance about an organisation's complete security state.

The Swedish edition translates the English master; the English edition prevails where they differ. Recommendations require validation against the reader's own assets, service requirements and legal obligations.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS

4.7 / 5

COVERAGE

3 pillars

CTI, DRPS, EASM

MONITORING

24 / 7

Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO