BRANDEFENSE COUNTRY REPORT · NETHERLANDS 2026

Brandefense Netherlands Cyber Threat Landscape Report 2026

Identity theft, shared software and service continuity in a connected economy

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

84 of 250
selected entries had a credential listed for sale when checked

5,160
held posts in the stated scope, not a national attack count

77
accepted Netherlands ransomware listings in the research-window snapshot

21 of 25
selected finance domains with a published DMARC quarantine or reject policy

CONTENTS

Contents

01	Executive summary	04
	Report map	08
02	The Dutch digital and institutional context	09
03	Selected-domain exposure and public technical observations	12
04	What the retained underground posts establish	20
05	Confirmed incidents, supplier dependencies and recent activity	35
06	Connected systems, disruption and operational continuity	46
07	Actors, campaigns and the limits of attribution	50
08	The fraud economy and harm after disclosure	61
09	Banking and finance: separate the institution, customer and supplier	68
10	Regulation and the national response	72
11	Outlook: decisions that change when the evidence changes	76
12	A 90-day plan with evidence of completion	80
A	Appendix A. Scope, evidence and interpretation	88
B	Appendix B. Post evidence register	91
C	Appendix C. Sources	93
D	Appendix D. Glossary	98
	About this report	100

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

About this edition

Prepared by Odin by Brandefense from Brandefense Blackhole, Ransompedia, Atlas, public technical observations and verified public reporting. Analysis and first drafts by AI agents; analyst review is required before release. Scope and limitations appear in Appendix A.

The Netherlands' documented cases connect identity, shared software and service continuity, requiring separate decisions about access, data, physical operations and reporting.

5,160

held posts, not unique incidents [S1]

77

accepted ransomware listing claims, not confirmed breaches [S3]

249

observed candidate domains from a selected list of 250 [S2]

24

post evidence cards with explicit proposition limits [S1]

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What should Dutch organisations decide first after the incidents and campaigns documented in 2026?

4

decisions linking identity, suppliers, continuity and incident reporting

Four decisions for leaders 06

The year in numbers 06

CHAPTER 01

Executive summary

IN SHORT

Dutch disclosures show how customer records, shared software and trusted accounts connect security failures to everyday services. The consequences include interrupted healthcare interfaces, stolen association records and threats to people after bank-data theft. Official reporting also describes espionage against individual accounts and connected equipment. Ransomware listings add a separate view of criminal claims. Start with account recovery, supplier access and service dependencies, then rehearse the reporting decisions each incident requires.

This report combines different evidence populations. Brandefense Blackhole contributes Netherlands-associated posts and narrowly scoped card observations. Ransompedia contributes accepted leak-site listings. Atlas exposure associations and public technical observations describe a selected candidate-domain list. Company statements, authorities and technical researchers establish specific events and supply context. These populations have different units, windows and limitations. They are not added into a national attack total. [S1][S2][S3][S4]

1. Customer-data theft requires more than password recovery. The confirmed Odido case connects an impersonated colleague, internal access and later publication of customer information. Police reporting on Revolut links stolen identifying data to attempted violence. The defensive objective therefore includes account security, customer communications and a route for personal-safety concerns. The cases do not establish one common operator or a national rate of harm. [S15][S75]

2. A shared supplier can change many organisations' working day. ChipSoft, the Canvas learning platform and AllUnited illustrate different dependencies: patient interfaces, teaching systems and association administration. A supplier notice does not establish identical impact at every customer. Each dependent organisation must establish its own affected data, service state and reporting obligations. Chapters 5 and 12 turn that distinction into supplier questions and restoration evidence. [S44][S49][S68]

3. A successful patch does not settle earlier access. NCSC documented exploitation of mobile-management systems in the Netherlands. Its account distinguishes observed intrusion from subsequent remediation. The lesson is to test two propositions separately: whether the weakness is closed and whether an attacker already obtained access. A patch record answers the first question; investigation and containment answer the second. [S21]

4. Espionage includes personal accounts and small connected assets. AIVD and MIVD described Russian-state-linked messaging and camera campaigns, while AIVD reported Dutch victims of an Iranian-actor malware campaign. These are the agencies' attributions. They do not justify assigning every criminal claim, foreign-language post or vulnerable device to a state. Protect messaging recovery and connected equipment alongside corporate systems. [S36][S58][S61]

5. November changed the operational priorities before this cutoff. AllUnited's updates, an international malware disruption, a third-party browser-script incident and the Revolut investigation require different responses. A contemporaneous cloud-service outage also affected continuity, but NCSC reported no indication of a hack. The recent-activity section separates disclosure, enforcement, dependency and prevention rather than calling every item an attack. [S68][S71][S74][S75][S73]

6. Exposure signals need distinct validation owners. Across 250 selected entries, 84 had a credential listed for sale when checked. The national Atlas headline is 50 out of 100. Device associations total at least 312,644, including 16,435 employee-device associations; credential records total 4,736,932. These overlapping records support account and endpoint validation, not a national incident estimate. [S2]

Four decisions for leaders

1. **Make account recovery an authorised process.** Require an independently verified route for password, MFA and messaging-recovery changes. Review active sessions and linked devices when a relevant signal appears. A convincing caller must not be able to create a new trusted route merely by knowing internal vocabulary (§6–§7).
1. **Ask suppliers for data and service scope separately.** Identify the tenant, interface, exported data and restoration dependencies involved. Require a named contact, a usable notice and evidence supporting reconnection. A system returning to service does not establish that stolen information has disappeared (§5).
1. **Check connected controls and browser dependencies.** Review remote administration of cooling, cameras and other physical systems. Separately review third-party scripts that execute in customer browsers. Assign an operational owner who can isolate the dependency without guessing its business impact (§5.8, §6).
1. **Exercise the reporting clocks that actually apply.** Map the Cyberbeveiligingswet, GDPR and financial-sector requirements to the organisation. Record awareness, classification, decisions and recipients in one incident record. A generic instruction to report everything within 72 hours does not capture these different duties (§10).

The year in numbers

250

Purposively selected candidate domains across 12 sector cells

WHAT IT IS NOT

Not 250 independent Dutch organisations or a national prevalence sample

84 of 250

Selected entries with a credential listed for sale when checked

WHAT IT IS NOT

Not working accounts or confirmed intrusions [S2]

50 of 100

National Atlas headline for the selected portfolio

WHAT IT IS NOT

Not sector ratings or national prevalence [S2]

77

Accepted Netherlands ransomware listings in the retained research-window snapshot

WHAT IT IS NOT

Not 77 independently confirmed breaches or unique victims [S3]

478

Associations included in AllUnited's collective AP notification reported on 18 November

WHAT IT IS NOT

Not a final victim total or number of people affected [S68]

178

Organisations worldwide in Report URI's third-party-script research

WHAT IT IS NOT

Not 178 Dutch victims [S29]

15 August 2026

Commencement date stated in the Cyberbeveiligingsbesluit

WHAT IT IS NOT

Not the deadline for every separate incident-reporting obligation [S10]

5,160

Held Netherlands-associated posts within the research scope

WHAT IT IS NOT

Not unique offers, transactions or attacks [S1]

249 of 250

Domains covered by passive observations; component availability differs

WHAT IT IS NOT

Not a validated ranking of organisational security [S2]

36

Cards seen in clear text in the retained posts

WHAT IT IS NOT

Not national card theft or fraud losses [S4]

SCOPE OF THE CARD FIGURES

Card figures cover only payment cards visible in clear text in the retained posts. Brandefense detects stolen cards through other methods outside this report. These observations do not measure national card theft, active cards, issuer prevalence or fraud losses.

Board readers can follow Chapters 1, 5, 10 and 12. Security teams should also read the exposure scope, source cards and actor distinctions. Fraud owners should connect Chapters 8 and 9 to customer operations. The report map provides the full routes.

Report map

Twelve chapters, five reading paths. Each chapter opens with the question it answers; Chapters 2–12 close with three takeaways.

Board and executives	Which decisions need ownership, resources and evidence of completion?	01 05 10 11 12
CISO and service owners	Which signals, dependencies and technical controls affect our response?	03 04 05 06 10 12
SOC and threat intelligence	What is established, what remains a claim and which campaign mappings apply?	04 06 07 12 A B
Fraud and customer operations	How can information support convincing approaches, and how do we verify consequential requests?	04 08 09 12
Privacy, legal and communications	What scope and clocks apply, and how do we communicate uncertainty?	05 08 10 12 A

01 Executive summary
What leaders should decide first

02 Context
Why recovery, shared data and institutional roles matter

03 Selected-domain exposure
What bounded public observations can support

04 Underground posts
Which claims merit validation and which are excluded

05 Incidents
What organisations and authorities established, including recent activity

06 Connected systems
How to verify disruption and protect the physical or dependent service

07 Actors
Which attributions and relationships the sources support

08 Fraud economy
How records and advertised services connect to fraud and personal-safety response

09 Banking and finance
How institution, customer and supplier evidence differ

10 Regulation
Which triggers, recipients and clocks require decisions

11 Outlook
Which signals would change the assessment

12 Action plan
Who does what and how completion is demonstrated

CHAPTER 02

The Dutch digital and institutional context

02

THIS CHAPTER ANSWERS

Which features of the evidence change how Dutch organisations should prepare?

12

sector cells in the selected candidate-domain universe, each containing at least five domains

2.1 Digital work makes identity and recovery operational decisions 10

2.2 Shared data needs a service map, not just a supplier list 10

2.3 The technical contact point changed during the year 11

2.4 New legislation does not replace existing reporting decisions 11

2.5 Political context needs attribution, not a causal story 11

CHAPTER 02

The Dutch digital and institutional context

IN SHORT

The evidence crosses customers, employers, associations, service suppliers and public authorities. A stolen account can expose data held for another organisation, while isolating a supplier can interrupt work without proving every customer was breached. Dutch institutions also changed in 2026, including the strengthened NCSC and commencement of the Cyberbeveiligingswet. Build an inventory that connects data, services and accountable owners, then map the rules that apply to each relationship.

2.1 Digital work makes identity and recovery operational decisions

CBS published its company ICT chapter in February 2026 using 2025 data. For companies with at least ten workers, 82% of personnel used internet, 80% of companies supported remote working, and 61% of personnel had remote access to documents or software. These are adoption figures, not 2026 attack measurements. [S6]

The security consequence is a planning judgement. Remote work depends on an employee being able to regain access when a device, password or second factor fails. Recovery therefore deserves the same design attention as normal sign-in. The trusted caller, support ticket and emergency exception are part of the control system.

This matters for continuity as well as intrusion prevention. A process that prevents fraud but leaves legitimate staff unable to work creates pressure for informal bypasses. Measure both outcomes in an authorised exercise: whether the impersonator is stopped and whether the real user is restored through the approved route.

2.2 Shared data needs a service map, not just a supplier list

The confirmed cases in Chapter 5 involve different kinds of shared system. Their common management problem is deciding who holds the relevant data and who can safely restore the service. This is our synthesis of those cases, not evidence that every Dutch supplier has the same weakness.

A conventional procurement list can identify the legal counterparty while missing an operational dependency. A local team may rely on a federation connection, learning-platform integration or patient-facing portal administered through that counterparty. The incident owner needs the relationship between these components, including who can suspend and reconnect them.

The most useful map has two views. The data view identifies information categories, authorised recipients, exports and retention responsibilities. The service view identifies the process that stops when a connection is disabled, its fallback and the evidence needed to resume it. Each view answers questions the other cannot.

A provider can restore an interface before it resolves the complete data-loss scope. Conversely, a limited data incident can produce a broad precautionary shutdown. Communications should explain both states separately. Customers need to know whether they can use a service and whether they must take protective action concerning their information.

2.3 The technical contact point changed during the year

An NCSC release dated 6 January says the Digital Trust Center merged into NCSC from 1 January 2026. It describes a strengthened national contact point for organisations' digital resilience. That organisational change should not be read as automatically changing every entity's legal duties. [S5]

A CISO should distinguish advice, technical coordination, statutory notification and criminal reporting. These activities can support one incident, but contacting one body does not by itself discharge every obligation. The reporting map should identify the purpose of each contact, the information needed and who maintains the record.

2.4 New legislation does not replace existing reporting decisions

The national summary states that the Cyberbeveiligingswet and Wet weerbaarheid kritieke entiteiten entered into force on 15 August 2026. It identifies registration, care and significant-incident obligations, together with management training. Chapter 10 distinguishes the cyber law's duties from privacy and financial-sector reporting. [S8]

For groups operating through several entities, one technical incident can create more than one reporting relationship. The response plan should preserve a common factual chronology while allowing different legal assessments. This avoids both duplicate speculation and a mistaken assumption that a group-level notice covers every entity.

2.5 Political context needs attribution, not a causal story

This report uses AIVD and MIVD statements to describe state-linked activity. It does not infer responsibility from an alias, a language or the national location of an infrastructure provider. The concrete campaign evidence appears in Chapters 6 and 7. [S36][S58][S61][S62]

KEY TAKEAWAYS

01

Account recovery belongs in the same control design as sign-in.

02

Map data and service dependencies separately so that restoration does not obscure exposure.

03

Establish institutional contacts and legal coverage before the next incident starts.

CHAPTER 03

Selected-domain exposure and public technical observations

THIS CHAPTER ANSWERS

Which exposure observations should owners validate first across the selected Dutch portfolio?

84 of 250

selected entries had a credential listed for sale when checked

3.1 Universe card 13
3.2 Exposure signals by sector 14
3.3 Email authentication needs an authorised-sender inventory 16
3.4 Web continuity and security observations answer different questions 17
3.5 Listings, lookalikes, documents and mentions need different validation 19
3.6 Turn the observation into an accountable task 19

CHAPTER 03

Selected-domain exposure and public technical observations

IN SHORT

Across the selected portfolio, 84 of 250 entries had a credential listed for sale when checked. The national Atlas headline is 50 out of 100. At least 312,644 device associations and 4,736,932 credential records support separate validation tasks. These overlapping observations describe selected domains, including brands and groups, rather than independent organisations or national prevalence. Validate current accounts, investigate employee-device signals and assign owners to confirmed mail-policy gaps.

3.1 Universe card

Item	Definition
Population	250 candidate domains selected for public-service, commercial or systemic relevance
Sector cells	Government 40; finance 25; insurance 15; education 25; health 25; energy 20; transport 25; telecom and technology 25; industry 20; retail 15; hospitality 10; media 5
Unit	A selected primary domain associated with an institution, operating brand or group
Interpretation	One domain is not necessarily one independent legal entity or organisation
Selection	Purposive, not random and not an official national ranking
Exposure snapshot	Device, credential, document and listing observations read on 21 November 2026; cumulative records, not new 2026 incidents
Other windows	Mention observations cover 365 days to 22 November 2026; lookalike observations cover 19 October–18 November 2026
Passive snapshot	Public technical observations for 249 of 250 candidates at the cutoff; each control uses its own denominator
Overlap	Records can overlap across sources, domains and people; brands and parent groups can overlap across entries
Scope	External exposure associations plus public mail, DNS, certificate and web-header observations where available
National Atlas headline	50 out of 100 for this selected portfolio; no sector or organisation ratings are published

[S2]

The list is a starting point for owners to ask specific questions. It is not evidence that every entry has the same responsibilities, traffic, data sensitivity or operational independence. A transport operator's public domain and a group brand can have very different relationships to the systems that deliver their services.

A regulator's registration population is also different from this report's finance cell. DNB's bank register includes Dutch-licensed institutions and foreign institutions operating through passporting. The selected finance cell additionally includes other financial activities. It must not be described as 25 licensed Dutch banks or 25 card issuers. [S7]

3.2 Exposure signals by sector

The national Atlas headline is 50 on a scale from 0 to 100. Higher values indicate greater observed external exposure, not an estimated probability of intrusion. It describes this selected portfolio and does not estimate Dutch national prevalence. The table reports how many selected entries have each observed signal; device and document columns count entries, not individual records.

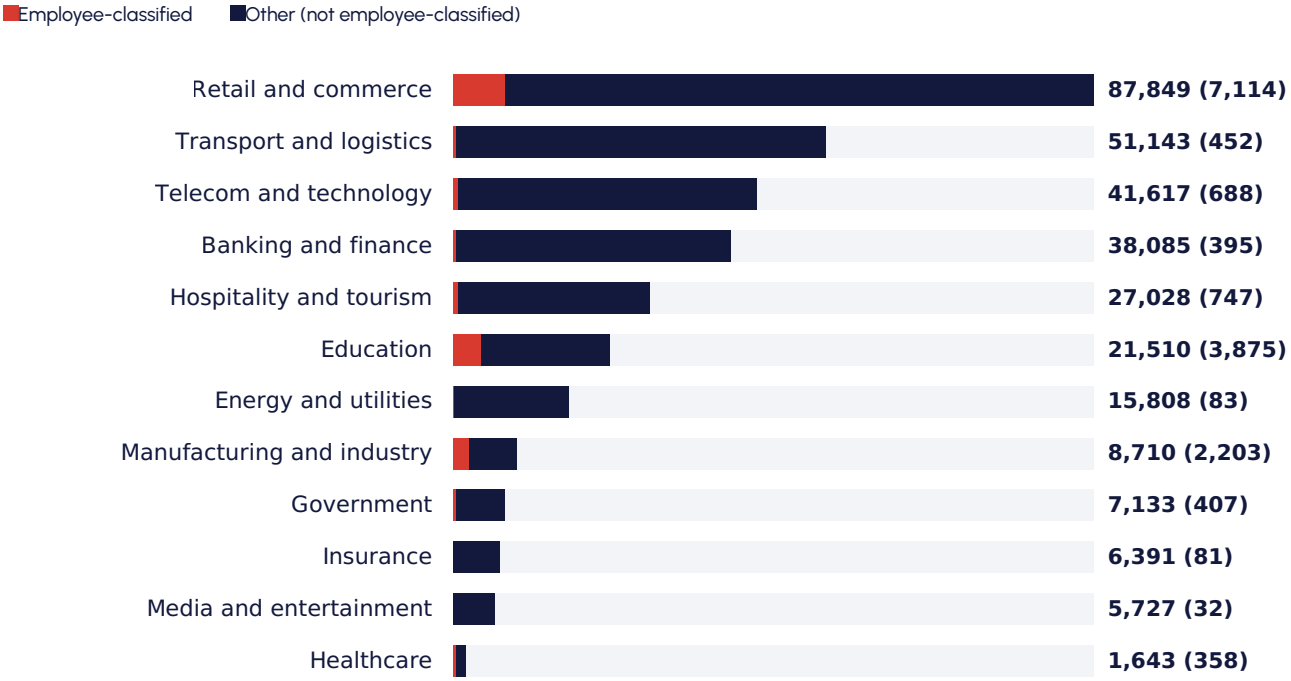
Sector	Candidates	Current listings	Employee devices	Documents
Banking and finance	25	11	16	13
Education	25	12	22	23
Energy and utilities	20	10	12	11
Government	40	5	35	33
Healthcare	25	2	21	13
Hospitality and tourism	10	10	8	5
Insurance	15	3	10	10
Manufacturing and industry	20	4	14	13
Media and entertainment	5	2	4	2
Retail and commerce	15	9	12	11
Telecom and technology	25	9	15	19
Transport and logistics	25	7	21	17
All selected domains	**250**	**84**	**190**	**170**

[S2]

All ten hospitality entries have a current credential listing; government has five across 40 selected entries. Those counts support account validation within the selected portfolio. They do not establish whether a credential works, whether MFA protects it or whether an institution suffered an intrusion.

The device and credential volumes describe a different population from the entry counts above.

Retail and transport carry the largest device-association totals in the selected portfolio



Source: Brandefense exposure associations, 250 selected candidate domains, read 21 November 2026. Records are cumulative and can overlap [S2].

Sector	Device associations	Employee subset	Credential records
Banking and finance	38,085	395	178,904
Education	21,510	3,875	1,287,262
Energy and utilities	15,808	83	88,963
Government	7,133	407	424,906
Healthcare	1,643	358	276,856
Hospitality and tourism	27,028	747	163,266
Insurance	6,391	81	120,004
Manufacturing and industry	8,710	2,203	438,927
Media and entertainment	5,727	32	9,451
Retail and commerce	87,849	7,114	1,173,918
Telecom and technology	41,617	688	341,992

Sector	Device associations	Employee subset	Credential records
Transport and logistics	51,143	452	232,483
All selected domains	**312,644**	**16,435**	**4,736,932**

[S2]

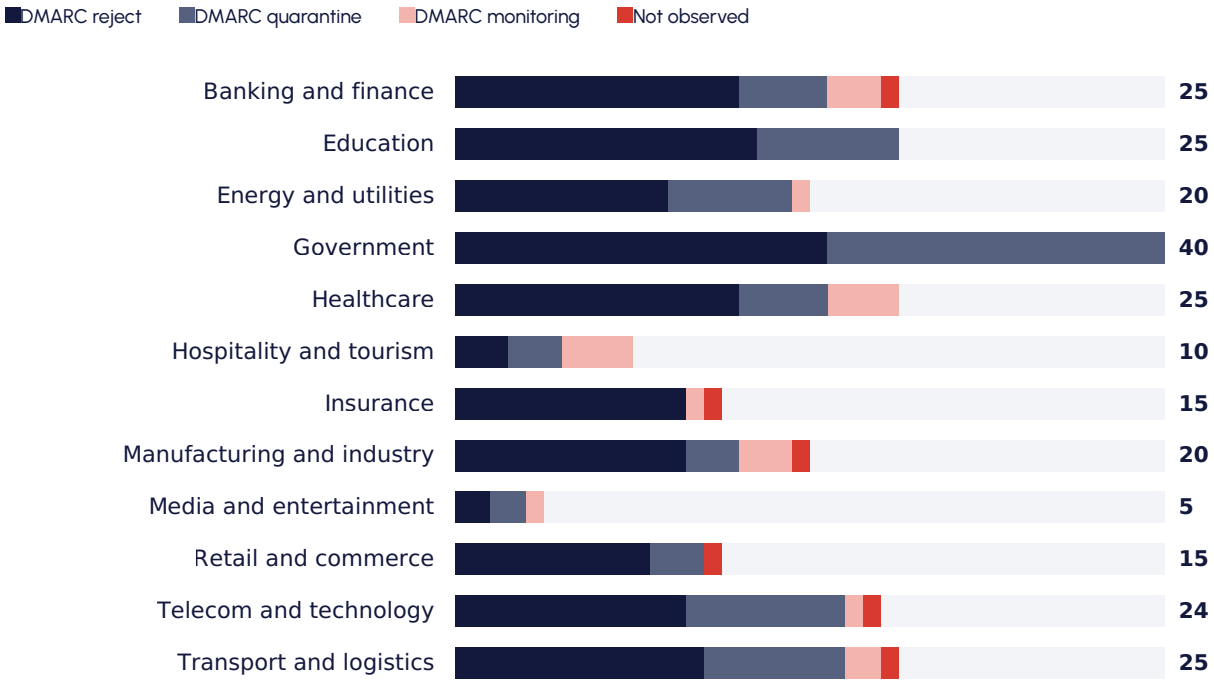
Device totals are lower bounds. Employee-device associations are included in the device total, rather than added to it. A device associated with a customer-facing service can belong to a customer or another external user. The association alone does not establish access to the institution's internal systems.

Credential records comprise 2,263,427 breach-database records, 454,417 stealer-log records and 2,019,088 credential-combination records. These populations can overlap and contain historical material. Retail contributes 7,114 employee-device associations and education 3,875; account ownership still needs validation, including student and customer accounts. [S2]

The denominator is part of the result. Exposure observations cover 250 selected entries, while the passive snapshot covers 249. The unavailable passive candidate is not treated as a failed control. A result for one population cannot silently become the denominator for another.

3.3 Email authentication needs an authorised-sender inventory

DMARC counts show published enforcement across the selected sector cells



Source: public technical observations for 249 selected domains at the cutoff. Each control uses its own observation denominator [S2].

Of 249 observed domains, 151 publish reject, 72 quarantine and 20 monitoring policies; a policy was not observed for six. Enforcement therefore appears on 223 observed domains. All selected government and education domains publish enforcement, while six of ten hospitality domains do. These are selected-domain results, not sector prevalence. [S2]

For this report, published quarantine or reject policies are the DMARC enforcement observation. Monitoring is a different state. [S85] An enforcement policy does not establish that every legitimate sender is correctly configured, that recipients always apply it, or that other forms of impersonation are prevented.

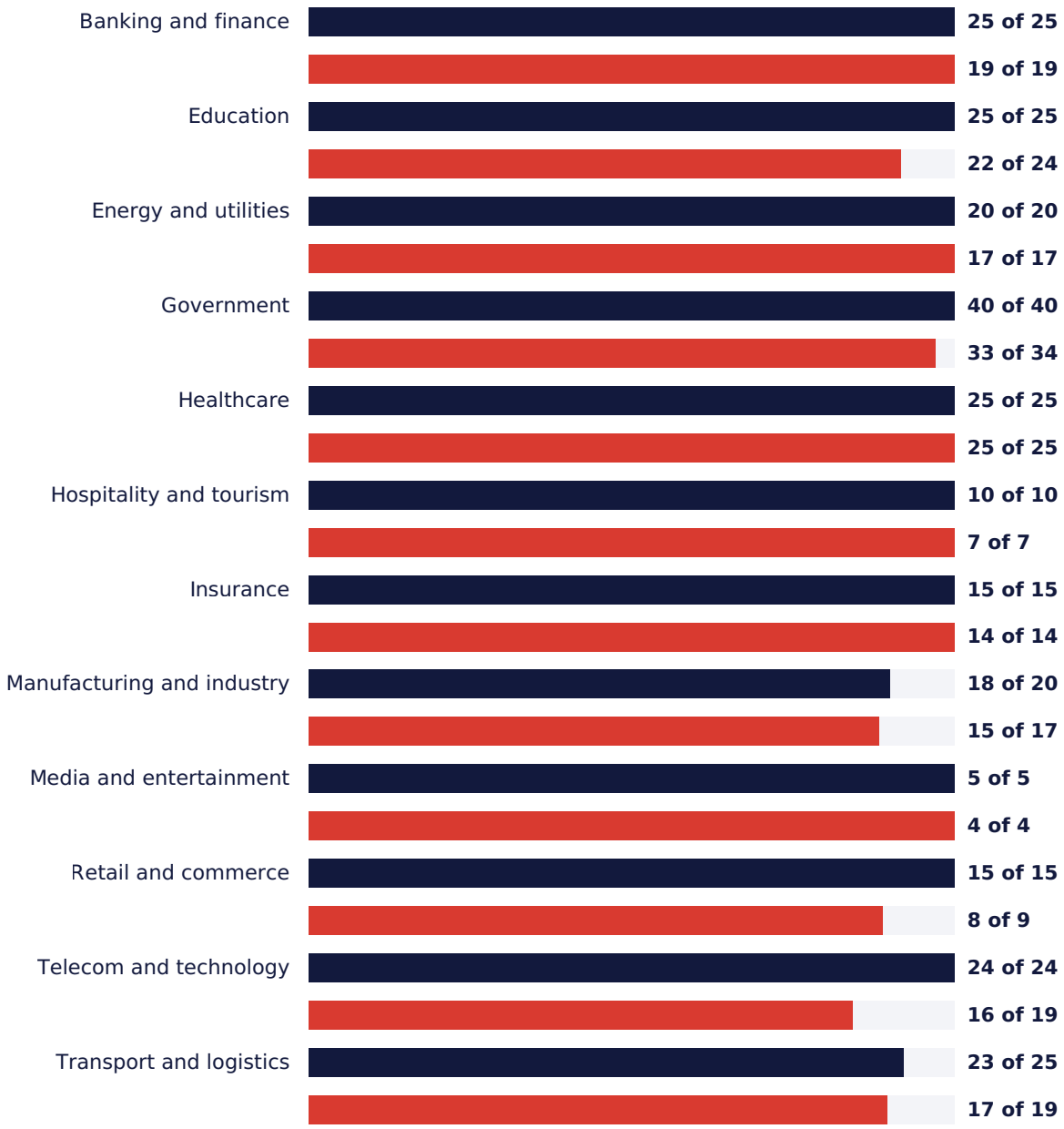
The decision for a messaging owner is consequently more specific than changing a policy label. Identify the services authorised to send on the domain's behalf and establish which are aligned. Agree a test and a rollback route before expanding enforcement. A control that rejects legitimate service messages can damage the business process it protects.

The incident response implication is equally specific. A customer who receives a convincing message can be facing a lookalike name, an affected legitimate account or a phone-based approach. Strong direct-domain authentication does not make such reports irrelevant. Preserve the message and refer it to the correct investigation route.

3.4 Web continuity and security observations answer different questions

TLS and HSTS observations use the domains on which each result was available





Source: public technical observations for 249 selected domains at the cutoff. Each control uses its own observation denominator [S2].

The snapshot contains 245 valid TLS results, 2 unsuccessful results and 2 inconclusive results. The latter categories do not establish a specific certificate defect. Of 208 observed homepages, 197 carry HSTS. SPF appears for 238 observed domains, DKIM for 215, and a DS record for 182. [S2]

Certificate validity is relevant to whether a user can establish the intended encrypted connection. A result should distinguish an observed invalid certificate from a domain for which a usable result was unavailable. The owner should confirm the relevant service and certificate chain before treating the result as a production defect.

HSTS is a browser instruction concerning future HTTPS use. [S88] Its observation on a reachable homepage does not describe every application, subdomain or first-time visit. A homepage header should not be presented as a complete assessment of transport security across an organisation.

DKIM not observed does not establish that the domain never signs mail. SPF concerns authorisation of sending hosts, not proof that every message is legitimate. [S86][S87]

DNSSEC terminology also needs precision. A DS record observed at a delegation is not, by itself, proof that the complete chain of trust validates. If a delegation result is included, keep the observation and the validation conclusion separate. A network owner can confirm the intended configuration through the normal change process.

3.5 Listings, lookalikes, documents and mentions need different validation

The 84 current listings describe credentials offered when checked, not unique people or confirmed intrusions. Validate ownership, age, account status and session activity through authorised incident handling. Historical records can remain visible after remediation, while a current advertisement does not establish that access still works.

The snapshot also contains 36,644 lookalike-domain observations and 1,888 exposed-document associations. Similar names can be unrelated to a brand, and publicly available documents can be intentionally published. Neither total is a confirmed phishing-site or confidential-file count. Brand and data owners should establish relevance, authorisation and sensitivity before acting. [S2]

Mention observations describe discussion and circulation, rather than validated access or a common operator. Review the underlying context and corroborating evidence before connecting a mention to an incident. Keep these observations separate from ransomware listings and the post populations in Chapter 4.

3.6 Turn the observation into an accountable task

A practical issue register should identify the domain, observed condition, responsible service, validation result and decision. Validated items can be corrected or recorded as approved exceptions. Unresolved ownership should be escalated rather than silently treated as an unaffected domain.

KEY TAKEAWAYS

01

The candidate-domain list is a purposive view with brand and group overlap.

02

Each control needs its own usable observation denominator and owner validation.

03

Validate current listings and employee-device signals without treating associations as confirmed intrusions.

CHAPTER 04

What the retained underground posts establish

THIS CHAPTER ANSWERS

Which Netherlands-associated offers deserve investigation, and what does a post leave unresolved?

5,160

held posts in the stated scope, not a national attack count

4.1 Universe card 21
4.2 Volume, platforms and language 22
4.3 Themes in the held subset 24
4.4 Six focused post cases 25
4.5 Reposts and education claims need dates and contents 30
4.6 Credential announcements and demand signals 32
4.7 Examples excluded from Dutch incident conclusions 33

CHAPTER 04

What the retained underground posts establish

IN SHORT

The retained posts advertise customer data, claimed access, identity material and financial accounts. Their value comes from a proposition an owner can check, not from the country label alone. Reposts, multi-country material and unsupported provenance limit interpretation. Read each evidence card with its qualifications. Validate the relevant data, account or service before deciding on incident response, public comment or customer protection.

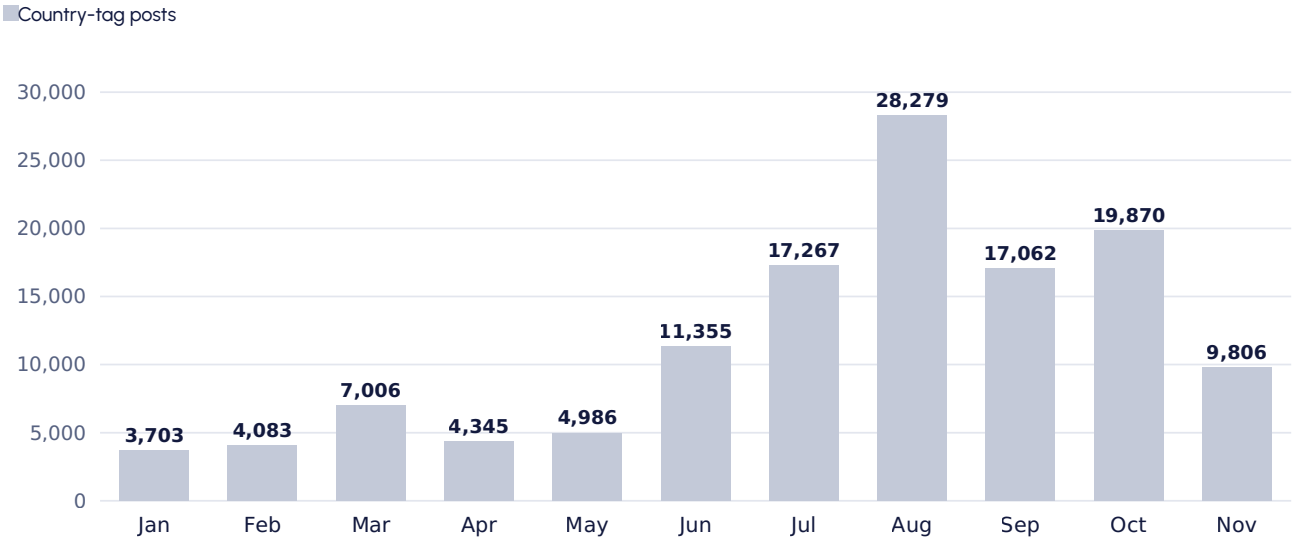
4.1 Universe card

Item	Definition
Window	1 January–22 November 2026, ending at the cutoff snapshot
Country association	Material concerning, mentioning or claiming a connection to the Netherlands
Held population	5,160 retained posts; 329 fall in the recent 8–22 November window
Country-tag population	127,762 posts in the tag totals; 3,286 held posts carry that tag
Theme and language base	The 3,286 held country-tag posts; not the entire tagged population
Platform base	The 5,160 held-post union
Unit	A post, not a unique seller, dataset, transaction or incident
Limit	Incidental references and country-labelled products do not establish Dutch victimisation

[S1]

4.2 Volume, platforms and language

Country-tag totals describe monthly post volume; November is incomplete

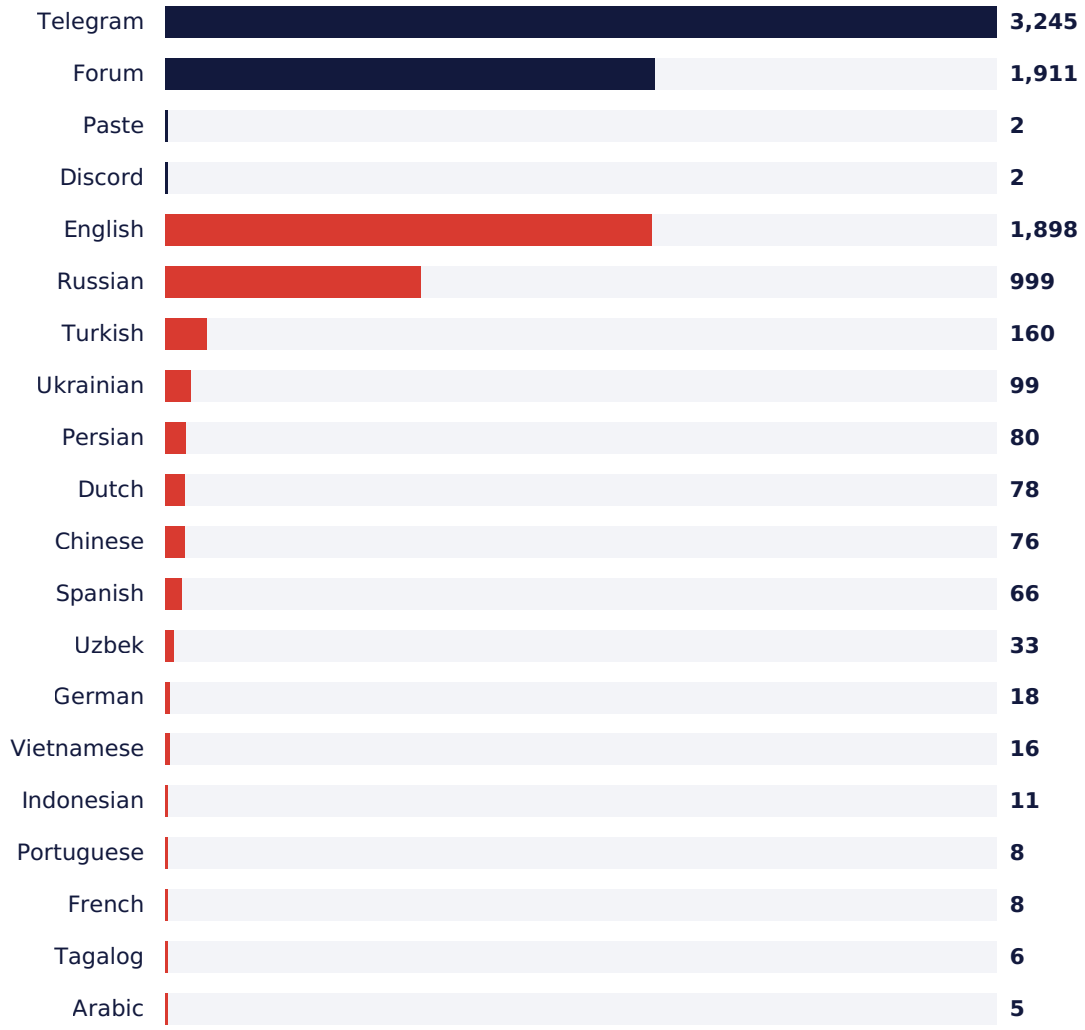


Source: Brandefense Blackhole, 1 January–22 November 2026; November partial [S1].

Tag totals range from 3,703 in January to 28,279 in August; November is partial. The held subset is not a complete monthly census. The difference between these populations is not a count of non-criminal posts, and the tag series is not a measured attack trend. [S1]

Platforms and languages describe the held subset rather than the Dutch population

5,160 held posts 3,286 held country-tag posts; languages can overlap



Source: Brandefense Blackhole, 1 January–22 November 2026; November partial [S1].

Dimension	Held result	Base and limit
Telegram	3,245	Of 5,160 held posts
Forums	1,911	Of 5,160 held posts
Paste / Discord	2 / 2	Of 5,160 held posts
English	1,898	Of 3,286 held country-tag posts
Russian	999	Same base; language does not establish nationality
Turkish / Dutch	160 / 78	Same base; language assignments can overlap

[S1]

4.3 Themes in the held subset

Themes describe advertised activity in 3,286 held tag posts; categories overlap



Base: 3,286 held country-tag posts; categories can overlap. Source: Brandefense Blackhole, 1 January–22 November 2026; November partial [S1].

Theme	Posts	Theme	Posts
Financial-account trading	1,000	Identity and verification	432
Phishing and fraud	443	Card material	431
Data and database offers	343	Malware/vulnerability references	198
Credential combinations	83	Access offers	76
Stealer-log references	50	DDoS/hacktivist references	14
Ransomware references	5		

[S1]

Categories can overlap, and incidental country mentions remain possible. They cannot be added into unique incidents or extrapolated into a Dutch market total. An advertised product is also not necessarily the source of a breach. A bank-branded contact list can originate with a partner, public material or an unrelated older dataset.

4.4 Six focused post cases

A

CASE A

A telecom-labelled identity-data offer

Evidence card B01 | 19 Feb 2026 | Forum thread | Telecommunications

Claim unverified

CLAIM	A 19 February seller advertises a Dutch telecom-labelled dataset, 5.8 million records and 1.3 million identity-document scans. The fields include identifying, contact and financial information.
ESTABLISHED	The advertisement exists. Its figures are the seller's, not a confirmed affected population. This report does not link the offer to a named confirmed telecom incident.
ALTERNATIVES AND LIMITS	Genuine material, aggregation, recycled data or misdescription remain possible. Origin, age, unique people, document availability and any sale are unverified.
RESPONSE	Ask the authorised data owner to assess a credible lead. Customer operations should verify identity through an established route rather than the caller's knowledge of basic details.

Bottom line

Validate the claimed fields and affected accounts before treating an advertisement as a fresh incident.

Evidence card B01 — 19 Feb 2026

Data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

[Dutch telecom provider] DATALEAK NL 5.8 MIL & 1.3 MIL ID/PASSPORT SCANS [...] -Full Name -Address -DOB -Phonen -[email field] -IBAN -BSN [...] [contact removed]

Note. Advertised volumes vary across later posts. The figures are seller claims, not a confirmed affected population.

Held

An offer naming a Dutch telecom provider, with claimed identity fields and volumes.

Not established

Authenticity, origin, capture date, number of unique people, document availability, any sale or confirmed breach.

CASE B

B

Patient tables and purported administrative access

Evidence card B02 | 8 Nov 2026 | Forum thread | Healthcare

Claim unverified

CLAIM	On 8 November a seller advertises three linked tables covering patient contacts, appointment requests and billing accounts, purported administrative access and a USD 4,650 asking price.
ESTABLISHED	The post describes an offer. Console images do not independently establish the named service relationship, valid access, dataset size or clinical impact.
ALTERNATIVES AND LIMITS	An unrelated service, a partial export, old access or fabricated evidence remain possible. No sale or successful control of a healthcare service is established.
RESPONSE	Validate the service and data relationship before making a patient-impact statement. Involve the relevant data owner and incident team without assuming the advertiser's technical description is accurate.

Bottom line

Check the service relationship and account evidence; patient-themed tables do not establish clinical impact.

Evidence card B02 — 8 Nov 2026

Healthcare-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

The file I'm selling came out of [healthcare service domain]. It covers Patient Contacts, Patient Appointment Requests and Patient Billing Accounts and is split across 3 tables. [...] Price: $4,650 [...] [contact removed]

Held

A seller advertises three linked patient-data tables, purported administrative access and a stated asking price on 8 November.

Not established

The named service/company relationship, legitimacy of the console images, source, access validity, dataset size, clinical impact or any sale.

CASE C

C

An online-retail export with wallet fields

Evidence card B03 | 18 Oct 2026 | Forum thread | Retail

Claim unverified

CLAIM	An 18 October Netherlands-labelled post advertises contact, account, order and wallet-related fields with purported sample rows.
ESTABLISHED	The field list and advertisement are visible. A wallet-balance field does not establish usable wallet access or a complete customer dataset.
ALTERNATIVES AND LIMITS	Public or partner data, older exports and synthetic records remain alternatives. The post does not establish unique customers, freshness or retailer-side origin. No link to the confirmed retail incident in Chapter 5 is established.
RESPONSE	Compare a credible lead through authorised channels with known schemas and older incidents. Keep payment-account access as a separate proposition requiring separate evidence.

Bottom line

Wallet-related field names do not establish the ability to move funds.

Evidence card B03 — 18 Oct 2026

Retail-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

[online retailer] Netherlands [...] user_id,full_name, email, contact_phone, street_address, city, postal_code [...] orders_count [...] wallet_balance_minor [...] [sample rows removed]

Held

A Netherlands-labelled retail-data post advertises contact, account, order and wallet-related fields and includes purported sample rows.

Not established

Source, authenticity, completeness, number of unique customers, freshness, wallet access, or whether the data came from the retailer.

CASE D

D

Software-sector RDWEB access

Evidence card B04 | 3 Apr 2026 | Forum thread | Software services

Claim unverified

CLAIM	A 3 April offer describes Netherlands, software solutions and RDWEB access, with revenue unknown and price open to offers.

ESTABLISHED	An access offer exists. The visible description establishes neither organisation identity nor a working session or privilege level.
ALTERNATIVES AND LIMITS	Stale, partial, unauthorised or fabricated access remain possible. The entry route and any sale are unknown.
RESPONSE	Review owned remote-administration gateways, authorised users and current access signals. Recommending strong authentication does not establish that the unnamed target lacked it.

Bottom line

Validate the advertised access and authorisation before escalating an anonymous country label.

Evidence card B04 — 3 Apr 2026

Access seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

Country: Netherlands Revenue: Unknown Industry: Software Solutions access: RDWEB price: $$$ open for offers [...] [contact removed]

Held

An offer explicitly describes Netherlands, software solutions and RDWEB access, with price open to offers.

Not established

Organisation identity, authorisation, whether access works, privilege level, freshness, entry route or any sale.

CASE E

E

Forex contact leads with financial fields

Evidence card B05 | 30 Jul 2026 | Forum thread | Financial leads

Claim unverified

CLAIM	A 30 July post advertises a Dutch-labelled 230,000-row forex contact list for USD 350, with contact, currency and deposit-related fields.
ESTABLISHED	The seller labels and prices a proposed product. The fields do not establish actual balances or an underlying broker's data loss.
ALTERNATIVES AND LIMITS	Marketing aggregation, older records or inaccurate labels remain possible. Unique people, authenticity, provenance and completed sale are unresolved. The later crypto offer in Chapter 8 is not established as the same file.
RESPONSE	Fraud teams should expect approaches tailored to apparent financial interests, while validating a specific dataset before attributing its source.

Bottom line

Contact and deposit-themed fields can support impersonation; provenance and balances remain unverified.

Evidence card B05 — 30 Jul 2026

Lead-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

Netherland Forex Consumer Database 230k Price $350 [...] COUNTRY CURRENCY EMAIL NAME PHONE DEPOSITES AMOUNT [...] [sample rows removed]

Held

An offer labels a 230k-row forex consumer list as Dutch and quotes $350 and financial/contact fields.

Not established

Record authenticity, underlying broker, capture date, unique people, lawful provenance, balances or completed sale.

CASE F

F

A Netherlands-labelled camera credential list

Evidence card B06 | 23 Aug 2026 | Forum thread | Connected cameras

Claim unverified

CLAIM	An August thread advertises credentials and snapshot links for 474 cameras said to be in the Netherlands.
ESTABLISHED	The post establishes a claim with a count. It does not establish locations, ownership, current reachability or working credentials.
ALTERNATIVES AND LIMITS	Old, wrongly located or invalid records remain possible. Neither physical impact nor industrial-control access is established. The post is not linked to the official camera campaign in Chapter 7.
RESPONSE	An owner with a credible asset-specific signal should validate it and review remote administration. Do not infer a national control-system incident from an unverified list.

Bottom line

A camera-credential advertisement is not evidence of industrial control or physical impact.

Evidence card B06 — 23 Aug 2026

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

ORIGINAL

474 cameras in Netherlands IP:PORT,USER,PASS with snapshot links [...]

Held
A forum thread claims a Netherlands camera-credential list with snapshot links and a count of 474.

Not established
Camera locations/ownership, current reachability, valid credentials, physical impact or any industrial-control compromise.

4.5 Reposts and education claims need dates and contents

B07 relays a technology-company database allegation; repetition of a similar theme does not establish a new intrusion. B24 explicitly dates its underlying source-code allegation to October 2025, although the post is from August 2026. Treat circulation date and intrusion date separately. [S1]

Evidence card B07 — 1 Jun 2026

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

ORIGINAL

Today i am leaking [technology company domain] ~154 DB's. [...] The files will be in .SQL extensions [...] The compromised data are: - Disk Encryption keys - users - software, and etc. - devices [...]

Note. A similar database theme appears in earlier retained posts. Repetition does not establish a new incident.

Held
A forum poster relays a technology-company database claim with a purported file count and data categories.

Not established
Authenticity, first publication, capture date, key validity, affected systems or a new 2026 intrusion.

Evidence card B24 — 21 Aug 2026

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

ORIGINAL

Today I have uploaded [software company] Data Breach for you to download [...] In October 2025, [software company] suffered a data breach and had their source code [...] [links removed]

Note. The post dates the alleged incident to October 2025. It is evidence of later circulation, not a new 2026 event.

Held
A August 2026 forum post recirculates a software-company source-code allegation that it explicitly dates to October 2025.

Not established
Authenticity, original publication, contents, a new 2026 incident or relationship to other source-code offers.

Education-themed material also varies. B08 advertises material under a university source-code/leak title without establishing the files' contents. B09 labels education records as relevant to 2023. B10 describes professional directory fields that do not independently establish an intrusion. None can simply be added to the confirmed Canvas case. [S1]

Evidence card B08 — 31 Jan 2026

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

ORIGINAL

Today I have uploaded [university domain] data breach for you to download [...] [data-description label] Tree Download [...] [links removed]

Note. The visible post does not establish what the underlying files contain.

Held
A forum thread names a Dutch university and advertises material under a source-code/leak title.

Not established
Underlying file contents, exfiltration, source-code authenticity, compromise date or affected users.

Evidence card B09 — 1 Feb 2026

Education-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

Data includes: ID;Voor-naam;Voorlet-ters;Tussenvoegsel;Naam;GeboorteDatum [...] BIC;IBAN [...] OuderEmail [...] BSNouder [...] Records: 1.338.803 [...] Relevance: 2023 [...] [sample rows removed]

Note. The seller labels the material as relevant to 2023. A 2026 posting date is not a new incident date.

Held
A 2026 forum offer advertises education-related personal and parent/account fields while explicitly describing the data as relevant to 2023.

Not established
Origin, authenticity, unique people, correspondence between the advertised record/email counts or a new 2026 breach.

Evidence card B10 — 10 May 2026

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

ORIGINAL

BEWARE OF FAKE CLAIMS/FAKE ACCOUNTS [...] Target: [research organisation] Type: Academic / Research In-stitution User Database Fields: UID, Email, Title, Initials, Prefix, Surname, Function, Telephone, Discipline, Organ-isation, Department, Address [...] [sample rows re-moved]

Held
A post advertises a research-organisation-labelled directory with professional contact fields.

Not established
The title volume, whether fields come from a public directory, source, currency or an intrusion.

A Netherlands-and-Belgium retail offer in B11 creates another boundary. Its advertised table fields do not establish usable payment tokens or the allocation of unique customers between countries. Country labels and field names support a question for investigation, not the answer. [S1]

Evidence card B11 — 3 May 2026

Retail-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

[online retailer] [~530k Netherlands and Belgium exports] [...] The dataset is organized into six main sections [...] user_id, account_ref, email, phone_mask [...] order_id, user_id, order_date [...] payment_id, order_id, payment_token [...] [contact removed]

Held
A seller advertises a Netherlands-and-Belgium retail export with account, order and payment-related table fields.

Not established
Authenticity, token usability, unique Dutch customers, country allocation, source or compromise date.

4.6 Credential announcements and demand signals

B12 announces a 328-line credential-combination file naming a marketplace. B13 announces two webmail-related lines. Neither establishes valid accounts, theft method or a breach of the named service. B14 is a buyer's request for multi-country logs and cookies; demand does not establish supply or working sessions. [S1]

Evidence card B12 11 Aug 2026

Automated uploader (alias withheld) Forum thread Forum English

ORIGINAL

[marketplace domain]-results Uploaded by [automated uploader] […] Total Lines: 328 Content Type: Email / Password Combo Date Uploaded: 2026-08-11 […] [credential sample removed]

Held
An automated forum uploader announces a 328-line file naming a Dutch marketplace service.

Not established
Credential validity, age, unique accounts, original theft method or service-side compromise.

Evidence card B13 26 Jun 2026

Automated uploader (alias withheld) Forum thread Forum English

ORIGINAL

[webmail domain] Uploaded by [automated uploader] […] Total Lines: 2 Content Type: URL / Email / Password Combo Date Uploaded: 2026-06-26 […] [credential sample removed]

Held
An automated forum uploader announces two URL/username/password lines naming a Dutch webmail login.

Not established
Validity, age, account ownership, theft method, unique people or breach of the mail provider.

Evidence card B14 2 Sep 2026

Log buyer (alias withheld) Forum thread Forum English

ORIGINAL

Buying [marketplace] logs. I pay well and on time. […] Interested in the following GEOs: […] Netherlands […] If anyone can recommend reliable suppliers of [marketplace] logs,cookies, I'll also reward you financially. […] [contact removed]

Held
A buyer explicitly seeks marketplace logs/cookies for multiple countries, including Netherlands.

Not established
Supply, any acquired logs, valid sessions, affected users or provider compromise.

4.7 Examples excluded from Dutch incident conclusions

B22 has a Netherlands-labelled title but an incoherent identifier fragment; the country association is not established. B23 describes an overseas consultancy as Dutch-led, which does not establish a Dutch victim. Both remain visible to explain the boundary and are excluded from Dutch incident conclusions. [S1]

Evidence card B22 — 2 May 2026

Forum poster (alias withheld) | Forum thread | Forum

Indonesian original; English retained translation quoted

ORIGINAL

DATABASE [technology company] (NETHERLANDS) [...] NIK (National Identification Number) [...] [sample identifiers removed]

Note. The excerpt is a retained English translation of an Indonesian-language post. The country association is not established and is excluded from Dutch incident claims.

Held

A forum title associates a technology-company name with Netherlands; the visible sample is an identifier-only NIK-labelled fragment.

Not established

Relationship of those identifiers to the named company, data origin, any Dutch population or any compromise.

Evidence card B23 — 9 Nov 2026

Access seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

Target Organization: [overseas consultancy] [...] [nationality descriptor removed] [...] based in [location outside Netherlands] [...] Environment: [file-transfer platform] Teams Dashboard [...] Access Parameters: Active verified session. [...] Available Assets: 112.8 GB [...] Fixed Price: $400 USD [...] [contact removed]

Note. An overseas organisation being described as Dutch-led does not establish a Netherlands incident. This item is excluded from that count.

Held

A 9 November access offer describes a UAE-based consultancy as Dutch-led and advertises a cloud session and files.

Not established

Access validity, any Dutch victim/data, lawful ownership, data scope or successful sale.

Staff should route suspicious material through authorised security processes rather than contact sellers or casually obtain sensitive files. The police's November warning discourages participation in criminal trading platforms. It is prevention context, not a count of breached users. Public cards omit contact routes, personal records and working indicators. [S70]

KEY TAKEAWAYS

01

A post establishes an offer or claim before it establishes an incident.

02

Route each proposition to the owner who can validate the relevant data, account or service.

03

Reposts, mixed-country offers and unsupported country labels require explicit limits and dispositions.

CHAPTER 05

Confirmed incidents, supplier dependencies and recent activity

THIS CHAPTER ANSWERS

What did organisations or authorities establish, and which decisions remain specific to each affected service?

12

developed incident and campaign cases across Chapters 5, 6 and 8

5.1 What counts as confirmation 36
5.2 Telecommunications: the account and the customer record 37
5.3 Public administration: exploitation, access and containment 38
5.4 Healthcare: restoring a connection is a clinical decision too 40
5.5 Travel and hospitality: a genuine booking can support a false payment request 41
5.6 Education: the supplier event and the university response 42
5.7 Retail, websites and other unresolved boundaries 43
5.8 Recent activity: 8–22 November 43

CHAPTER 05

Confirmed incidents, supplier dependencies and recent activity

IN SHORT

The confirmed evidence includes customer-data theft, public-sector access, healthcare and education dependencies, association software and exposed controls. Each case has a different scope and recovery problem. An investigation, supplier statement or published attacker claim does not establish every downstream effect. Read the confirmed account and unresolved questions separately. Establish your own data and service impact before adopting another organisation's incident description or reconnecting a shared interface.

5.1 What counts as confirmation

A confirmed incident here requires a statement by the organisation or an authority establishing an attack or unauthorised access. A criminal post or listing alone remains a claim. Naming additionally requires official confirmation and broad reporting; generic descriptions remain appropriate where that condition is not established.

The developed cases are not a national incident count. A campaign can contain several affected organisations, and an update can describe the same event months later. Supplier incidents can produce several customer notices. The chapter therefore states relationships and dates without adding them into a unique-victim total.

The cases also separate containment from harm. Disconnecting a system establishes a defensive action. It does not prove the system was encrypted, that all connected customers lost data, or that no data had already left. Each conclusion requires its own supporting evidence.

5.2 Telecommunications: the account and the customer record

CASE G

G

Odido customer-contact data

Telecommunications

Company and police reporting

WHAT WAS CONFIRMED	Odido's 12 February notice described unauthorised access to a customer-contact system. It said operations were unaffected and specified information outside the initial scope. NOS reported an initial figure of 6.2 million accounts, which must not be read as unique people. [S13][S35]
LATER ACCOUNT	The company's updated FAQ dates the activity to 5–6 February and attributes it to ShinyHunters. Police described a caller impersonating an IT colleague and later publication of data concerning more than six million customers. The attribution remains the company's. [S14][S15]
WHAT REMAINS UNRESOLVED HERE	This report does not reconstruct every step of the intrusion, reconcile all later population figures or establish which individual records remain usable. The initial disclosure and later updates answer different questions.
RESPONSE	Rehearse support verification and prepare for follow-up fraud using genuine customer details. Do not rely on the secrecy of basic account information as proof of identity.

Bottom line

Protect customer communications and recovery processes as well as passwords.

The regulatory investigation is discussed in Chapter 10. It should not be treated as a concluded liability finding or as independent proof of every criminal claim.

5.3 Public administration: exploitation, access and containment

CASE H

H

Mobile-management exploitation and the AP/Rvdr examples

Public administration

Official campaign confirmation

CAMPAIGN	NCSC confirmed exploitation of Ivanti EPMM at multiple Dutch organisations and described observed database copying or exfiltration in its updates. Its later timeline includes successful Dutch exploitation from 29 January and earlier activity identified retrospectively. [S31][S21]
NAMED EXAMPLES	A government letter confirmed exploitation at the Autoriteit Persoonsgegevens and Raad voor de rechtspraak. It specified unauthorised viewing of AP staff work contact information. Rvdr made a provisional breach notification; AP's detailed fields cannot be assigned automatically to every Rvdr employee. [S32][S33]
LIMIT	These examples sit within the campaign. They are not added again as a separate national campaign total. Product use alone does not establish that another organisation was breached.
RESPONSE	Confirm remediation, investigate prior access and assess administrative credentials or trust relationships that could outlive the original weakness.

Bottom line

Closing a weakness and investigating earlier access are separate completion tests.

CASE I

I

Ministry of Finance system access

Central government

Ministry confirmed access

WHAT WAS CONFIRMED	The ministry detected unauthorised access on 19 March and blocked access on 23 March. Its notice concerned systems supporting several policy-department processes. It said tax, customs and benefits services to citizens and businesses were unaffected. [S37][S38]
LIMIT	The initial statement did not establish an attacker, entry method, stolen-data scope or final set of affected systems. Those gaps should not be filled with facts from other government incidents.

RESPONSE	Define which processes depend on the isolated systems, keep an operational fallback and preserve the evidence supporting any statement about unaffected services.

Bottom line

Separate affected policy systems from unaffected public services in communications.

CASE J

J

Epe file theft and changing scope

Local government

Municipality reported theft

WHAT WAS CONFIRMED	Epe's rolling account dates entry to 10 March, downloading of nearly 552,000 files to 12 March and the first public notice to 14 March. Its later investigation said almost all residents' personal data was probably stolen. It listed 845 valid identity-document copies. [S41]
CHRONOLOGY AND LIMIT	Earlier reporting used a different identity-document figure. A valid-copy count is not interchangeable with all copies or affected people. The municipality's dated statement about non-appearance on known leak sites does not prove deletion or prevent later misuse. [S42]
RESPONSE	Keep scope definitions and update dates explicit, prioritise sensitive-document guidance and make the route for residents' questions usable.

Bottom line

Preserve the meaning and date of changing scope figures.

A file count is an investigation measure, not a count of individuals. One person can appear in several records, while one file can contain several people. The public notice should explain what the organisation can establish about affected people rather than leaving users to divide files by population.

A separate police phishing incident. On 25 March police described rapid detection and interruption of phishing-related access. Its initial account said citizen data and investigative information had not been visible or accessible. The source framed the apparent impact as limited and under investigation. This is separate from the police's 2024 incident. [S39][S40]

5.4 Healthcare: restoring a connection is a clinical decision too

CASE K

K

ChipSoft ransomware and customer interfaces

Healthcare software

Supplier and CERT confirmation

WHAT WAS CONFIRMED	Z-CERT's 17 April update dates ransomware to 7 April and confirms theft of personal and medical patient data at some Dutch customers. It distinguished affected hosted interfaces from self-managed or third-party-managed software deployments outside that scope. [S44][S45]
RECOVERY	ChipSoft's timeline described phased restoration and near-complete reconnection of patient portals by 12 May, with recovery continuing in June. Its statement about data destruction relied on assurances attributed to its security experts; this report cannot guarantee all copies disappeared. [S18]
LIMIT	A customer connection being disabled or restored does not, by itself, establish the data-theft scope at that customer. No actor is named by the cited primary accounts.
RESPONSE	Require both clinical continuity approval and security approval before reconnecting a shared service, with an agreed rollback and patient-communication route.

Bottom line

Restore each dependency with its owner; deletion assurances do not establish that every copy disappeared.

5.5 Travel and hospitality: a genuine booking can support a false payment request

L

CASE L

Booking.com guest-information access

Travel technology

Controller filing confirmation

WHAT WAS CONFIRMED	Booking Holdings' later filing confirms unauthorised third-party access to certain guests' booking information in April, remediation and cooperation with authorities. Reporting dated 13 April described customer notices and reservation PIN resets. The Dutch-resident subset was not established. [S46] [S47]
LIMIT	This is not evidence that every booking, hotel or Dutch traveller was affected. The report does not establish a common cause with the separate hotel-sector investigation below.
RESPONSE	Give customers an independent way to verify payment requests and check the trust placed in reservation details during support interactions.

Bottom line

Treat booking knowledge as a phishing risk, not authority to request payment.

R

CASE R

A rail-pass disclosure with a 2025 intrusion date

Rail-pass services

2026 disclosure; 2025 event

WHAT WAS CONFIRMED	Eurail's first disclosure was dated 10 January 2026. [S105] Its February update described database copying and later sale-related material. A company notice filed with a regulator dates file transfer to 26 December 2025. This is a 2026 disclosure, not a new 2026 intrusion. [S103][S104]
LIMIT	Ordinary direct purchasers and DiscoverEU participants have different data categories. Broader programme-specific fields must not be assigned to every purchaser. No Dutch-resident total is established here.
RESPONSE	Identify which service and customer category a notice concerns before issuing advice. Keep the event date, disclosure date and subsequent circulation separate in the response record.

Bottom line

Keep ordinary customers, programme participants, event dates and disclosure dates distinct.

A person may use one customer-facing brand without knowing which programme holds their information. Support staff need a way to identify the relevant service relationship through an established channel. Guidance should follow that relationship rather than the most extensive field list reported for any customer category.

A separate June investigation concerned hotel guests receiving targeted reservation or payment messages. NOS reported an industry estimate of at least 100 Dutch hotels, while the cause and complete scope remained unresolved. The industry participant's own page described an inventory effort. Neither establishes that the participant itself was the affected supplier. [S53][S54]

5.6 Education: the supplier event and the university response

CASE M

M

Canvas and university continuity

Education technology

University reported supplier incident

WHAT WAS CONFIRMED	UvA's rolling notice records formal supplier notification by 7 May, with names, email addresses and possible IDs involved according to supplier information. It described seven universities. Connections were suspended on 8 May, and UvA restored Canvas on 13 May. [S49][S50]
LIMIT	One university's notice is not permission to name every affected institution or assign identical scope to each. A supplier's assurance about deletion is not independently established deletion of every copy.
RESPONSE	Test an alternative teaching and submission route, define safe reconnection criteria and reconcile information handled through the temporary process.

Bottom line

A shared platform creates separate customer scope and restoration decisions.

Education continuity needs a decision about deadlines as well as technical access. If teaching material, assessment or submissions depend on a shared platform, faculty owners should know who can approve alternatives and communicate them. Security cannot resolve those academic decisions by restoring a login page alone.

5.7 Retail, websites and other unresolved boundaries

Ahold Delhaize's 19 October update described malicious activity and precautionary suspension of some websites or apps, while stores remained open. Its quarterly report estimated fourth-quarter sales and operating-income impacts. The 4 November report estimated fourth-quarter sales reduction of EUR 200–250 million and operating-income reduction of EUR 75–100 million. These are group estimates, not final or Dutch-only losses. No actor attribution is adopted. [S19][S20]

A retail webshop controller also disclosed a September customer-data incident. Its name is withheld here. The notice supports the bounded incident description, not a conclusion about the controller's wider estate. [S30]

Dustin's September chronology confirms internal-system access, temporary shutdown and staged restoration. Its later FAQ describes affected administrative/support data and limited business-contact or user information for certain managed-service customers. Separate reporting relays claims about Dutch customers; those customer-specific claims are not official confirmation of intrusions into their own networks. [S101][S102]

For websites more broadly, the AP warned in August of exploited WordPress vulnerabilities, breach notifications and inadequate communication about risks. It did not provide a count of operators. This cannot be added to another campaign's global infected-site total or treated as one measured national wave. [S60]

A reported internal-folder incident at an air-transport group remains generic here. A press account quoted the company acknowledging unauthorised access and describing no identified sensitive data or customer-service effect at that stage. A separate group's responsibility claim is not adopted. The precise incident day and complete scope remain unresolved. [S64]

These examples justify checking web administration, privileged access and customer notification. They do not establish a shared actor or a single intrusion path. NCSC's October food-sector notice specifically said it saw no reason at that time to assume the incidents it discussed were related. [S63]

5.8 Recent activity: 8–22 November

The recent window contains events that require different operational responses. Dates below distinguish the underlying event from its public update. An update is not counted as another intrusion, and a prevention exercise is not counted as a criminal victim incident.

CASE O

AllUnited and association-level scope

Association administration

Company confirmed theft

WHAT WAS CONFIRMED

AllUnited says data were stolen on 9 November and a software flaw was fixed after discovery. Its 18 November update reported a collective AP notification for 478 associations. A 20 November update still listed disabled federation interfaces. [S68]

LIMIT	The 478 figure counts participating associations in that collective notification. It is not a final number of affected people, all customers or all notifications. Interface status does not establish that every named federation was breached. Earlier press figures describe earlier reporting. [S69]
RESPONSE	Each association should establish the records it entrusted to the service, its own communication decision and which interfaces it can safely use.

Bottom line

Notification participants are not a final victim count; validate each association's scope.

CASE Q

A third-party script enters the customer browser

Browser dependencies

Supplier incident: local reach unresolved

WHAT WAS CONFIRMED	The experimentation-platform provider's advisory, updated 19 November, confirms exploitation on 16 November of a signup-flow flaw, account impersonation and malicious JavaScript injection. It said fewer than 5% of customers were affected and remediation occurred that day. [S74]
EXTERNAL OBSERVATION	Report URI described 178 organisations worldwide in its research. That is a global research count, not a Dutch victim count. Customer names are withheld pending the required confirmation; the cited evidence does not justify identifying Dutch customers here. [S29]
RESPONSE	Identify scripts executing in customer browsers, the accounts allowed to change them and a tested way to disable an affected dependency.

Bottom line

Global affected-site figures do not establish a Dutch victim total.

A browser dependency can sit outside the team that patches the main application. Security ownership should follow the ability to change executable content, including marketing or experimentation administration. The relevant exercise is whether the organisation can locate the dependency, revoke its administrative access and disable it without losing essential customer functions.

Public date	Item	Interpretation and immediate decision
9 November	Police warning about criminal online platforms [S70]	Prevention context; route suspicious material through authorised security processes
12 November	Operation Endgame update [S71][S72]	International enforcement; examine relevant notifications and prior compromise, as discussed in §7.5

Public date	Item	Interpretation and immediate decision
12 November	Supplier-related survey-data reporting [S94]	Company investigation as reported; email addresses are not unique people
13 November	Cloud-mail service disruption described by NCSC [S73]	Continuity event; no indication of a hack in that account; test independent communications
16 November	RDI GPS investigation notice [S98]	Event on 9 November; cause unresolved, separate from network-intrusion conclusions
18–20 November	AllUnited scope and interface updates [S68]	An update to the 9 November incident; establish association-specific data and service status
19 November	Revolut investigation reported by police [S75]	September theft with later public reporting; personal-safety and fraud response in Case P (§8.3)
21 November	Police simulated-webshop campaign [S77]	Prevention exercise, not customer losses from a criminal breach

A separate 12 November report quoted a consumer brand investigating supplier-related exposure of 128,000 email addresses and other survey data. The extent of viewing, copying or misuse remained unclear. Names remain withheld here. This is not established as part of the later browser-script incident. [S94]

RDI's 16 November notice adds a different boundary. It concerns aircraft GPS disruption on 9 November, 18:15–18:30. The authority said secondary systems protected aviation safety. Its investigation did not establish deliberate interference, origin or responsibility. This is not evidence of an intrusion into an airport's systems. [S98]

The cloud-mail account is an availability event without an established malicious cause. Its relevance here is continuity, rather than a new attack count. [S73]

KEY TAKEAWAYS

01

Confirm data impact and service impact separately for each organisation and supplier.

02

Rolling updates, campaign examples and collective notices cannot be added into a unique-victim total.

03

Recent activity makes association scope, browser dependencies and independent communications immediate exercise priorities.

CHAPTER 06

Connected systems, disruption and operational continuity

THIS CHAPTER ANSWERS

Which disruption claims require technical verification, and when does a connected system become an operational priority?

2 November

NCSC's notice confirming cooling-system cyberattacks affecting the Netherlands

6.1 A timeline with explicit evidence types 47
6.2 Cooling installations and remote changes 48
6.3 A camera list is not an industrial-control incident 49
6.4 DigiD availability and the boundary of the held posts 49
6.5 Continuity exercises should include security tooling 49

CHAPTER 06

Connected systems, disruption and operational continuity

IN SHORT

The strongest connected-control evidence here is an official cooling-system notice. It is different from a camera credential-list claim, a website availability allegation or a cloud outage. These events require different proof and different owners. Establish whether a physical process is affected, preserve local evidence and isolate unsafe remote access through an authorised decision. Prepare independent communications before the normal collaboration service becomes unavailable.

6.1 A timeline with explicit evidence types

9 Mar 2026	**AIVD and MIVD** Describe a messaging-account campaign and Dutch government victims; attribution belongs to the agencies [S36]
1 Apr 2026	**NCSC** Warns of malicious software-package activity; Dutch victim numbers are not established [S43]
28 May 2026	**Police and NCSC** Describe an international botnet disruption involving infrastructure hosted in the Netherlands [S52]
30 Jun 2026	**AIVD and MIVD** Describe recovery-key phishing as an evolution of the messaging campaign [S57]
10 Jul 2026	**AIVD and MIVD** Confirm hacked cameras on Dutch military-logistics routes, without identifying owners [S58]
23 Aug 2026	**Credential-list advertiser** Advertises camera-related material; authenticity, location and access remain unverified (B06)
7 Oct 2026	**Parliamentary answer** Describes recurring DigiD DDoS attempts and increased availability impact during 2026 [S96]
13 Oct 2026	**NCSC** Sees no reason at that time to assume the food-sector incidents it discusses are related [S63]
2 Nov 2026	**NCSC** Confirms cooling-system cyberattacks across Europe, including the Netherlands [S66]
12 Nov 2026	**Police** Announces further Operation Endgame disruption; international and Dutch-location figures require separate reading [S71]
13 Nov 2026	**NCSC** Describes a cloud-mail outage, without an indication of a hack in its account [S73]

16 Nov 2026 **RDI**
Reports investigation of 9 November GPS disruption; cause and responsibility unresolved [S98]

16 Nov 2026 **Provider advisory and technical research**
Browser-script incident confirmed; research count is global and customer identities remain withheld [S74][S29]

6.2 Cooling installations and remote changes

CASE N

N

Cooling installations and remote changes

Cooling installations

Official campaign notice

WHAT WAS CONFIRMED

NCSC's 2 November notice describes cyberattacks on cooling installations in several European countries, including the Netherlands. It identifies weak or default passwords as enabling remote setting changes and recommends removing direct internet exposure. [S66]

OTHER REPORTING

An Anadolu report, citing NOS, gave at least 17 Dutch businesses. That is a dated press account, not a count supplied by NCSC. The evidence here does not establish one vendor, one actor or measured spoilage at every site. [S67]

RESPONSE

Identify remote-administration paths and their owners. Check physical readings, restrict unsafe access and preserve a local recovery option before making a public statement about impact.

Bottom line

Coordinate remote-access restrictions with the owner responsible for the physical process.

Point	Inference to avoid	Supported boundary	Operator's decision
Scope	Every product from one supplier was affected	No complete vendor population established	Identify the actual remote-control dependency
Control	A screen establishes physical harm	Local process evidence still required	Check readings and local records
Attribution	One actor coordinated every event	No common operator established here	Contain the verified access without guessing responsibility
Population	A press estimate is a national census	NCSC supplies no Dutch total	Establish the organisation's own installation scope

[S66][S67]

An emergency decision should not depend on discovering who installed the connection. Facilities, refrigeration contractors, IT and business operations should agree who can disable access, who checks the equipment and how emergency maintenance continues. Record those roles before the incident rather than negotiating them while a process drifts.

6.3 A camera list is not an industrial-control incident

The camera-related post in Case F is underground evidence of an advertisement. It does not establish the country of every listed device, working access, ownership, authenticity or a change to a physical process. It must not be promoted into a verified industrial-control campaign. [S1]

6.4 DigiD availability and the boundary of the held posts

A parliamentary answer received on 7 October confirms daily DDoS attempts against DigiD and increased availability impact during 2026. It describes increasingly complex, targeted attacks. National reporting quoted Logius confirming another attack on 30 October. These are supporting events within a recurring campaign, not separate data-breach counts. [S96][S97]

For a service depending on digital authentication, the fallback should specify what the user can still do when sign-in is unavailable. A service-status message should explain the affected function and next update. An availability event alone does not establish theft of authentication data.

The theme table includes DDoS or hacktivist references, but the held material did not establish a Dutch DDoS campaign or a verified industrial-control claim. That is a limitation of this evidence, not proof that Dutch organisations experienced no such activity. [S1]

Website non-response alone would not establish cause, duration or operational impact. An actor can publish a claim at the same time a site is unavailable for another reason. Defenders should compare their own service telemetry, supplier status and incident evidence before adopting the actor's description.

6.5 Continuity exercises should include security tooling

The recent cloud-service outage in §5.8 shows why security depends on ordinary service availability. An incident team should know which alerts, administrative approvals and communications rely on the same service. A fallback that shares the failed identity or messaging dependency can fail at the same moment.

KEY TAKEAWAYS

01

Verify the physical process and remote-access owner before concluding an operational impact.

02

Keep underground camera claims separate from official espionage and cooling-system evidence.

03

Test communications and security decisions while the normal cloud service is unavailable.

CHAPTER 07

Actors, campaigns and the limits of attribution

07

THIS CHAPTER ANSWERS

Which actors are supported by the evidence, and which relationships should defenders avoid inferring?

77

accepted Netherlands ransomware listings in the research-window snapshot

7.1 A relationship map with evidence on every line 51

7.2 Ransomware listings and regional context 52

7.3 ShinyHunters and company-specific attribution 54

7.4 Three official campaign strands 55

7.5 Enforcement changes infrastructure, not the history of stolen data 59

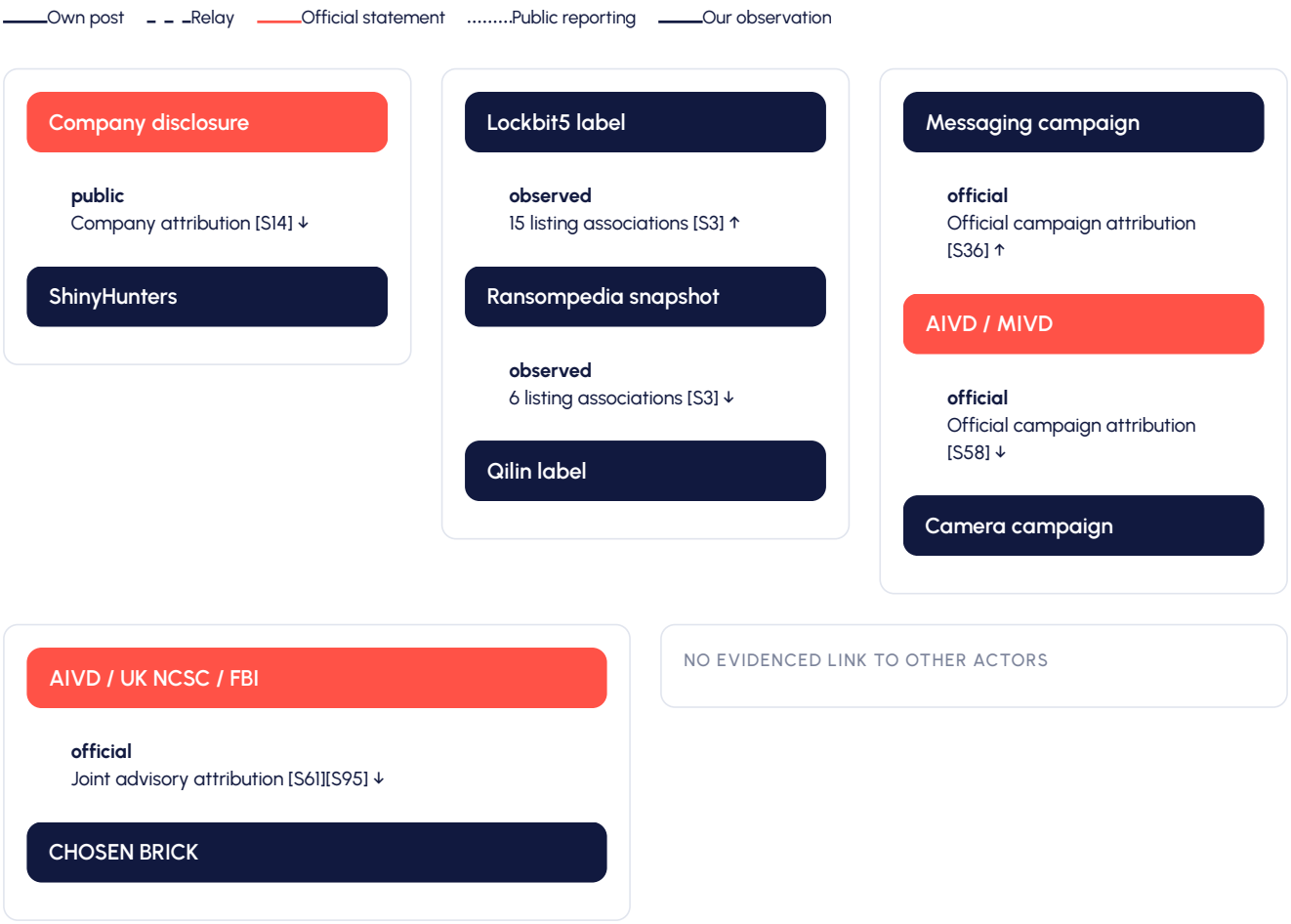
CHAPTER 07

Actors, campaigns and the limits of attribution

IN SHORT

Criminal listings, company attributions and intelligence-agency assessments answer different questions. Lockbit5 leads the retained Dutch ransomware listings; ShinyHunters is named in Odido's company account. Official campaign reporting separately covers messaging, cameras and targeted malware. These strands are not one network. Use the evidence-labelled map to preserve those boundaries, then prioritise recovery, account protection and the specific assets the campaigns describe.

7.1 A relationship map with evidence on every line

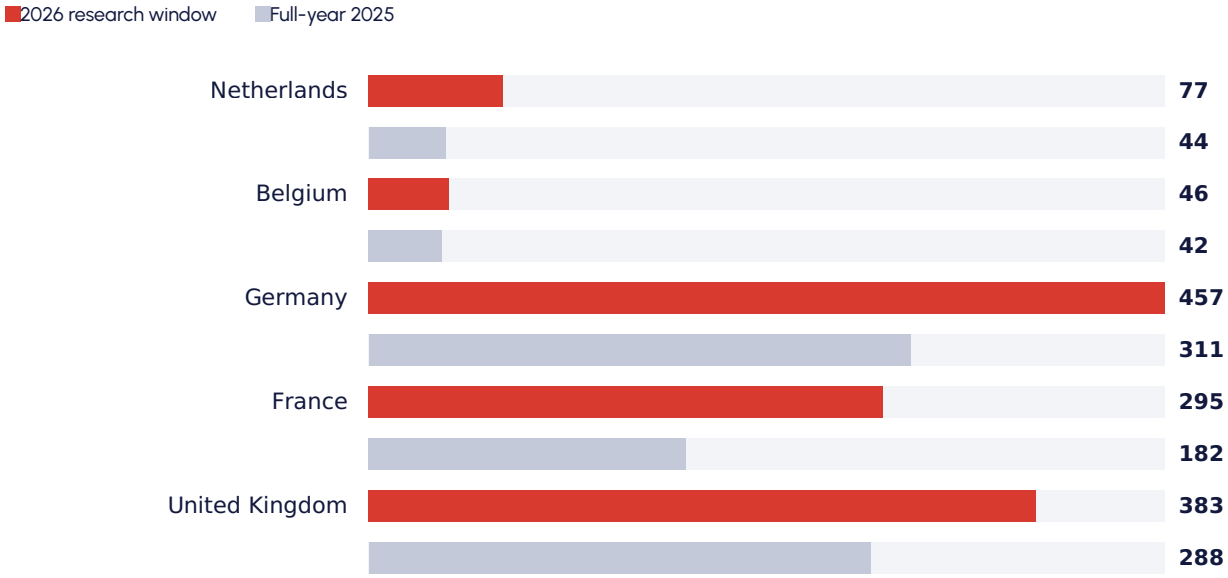


A line represents a documented relationship of the type shown. An official campaign attribution, a company's account, an actor's advertisement and a shared post are not equivalent evidence. An association does not establish a common operator, and an isolated node is preferable to an invented connection.

This report does not join the profiled ransomware brands, underground advertisers and state-linked campaigns into one organisation. Shared country interest or similar terminology does not establish coordination. Where a specific incident lacks an established actor, its defensive analysis remains useful without an attribution.

7.2 Ransomware listings and regional context

Netherlands listings exceed the prior annual total, with unmatched periods and no national risk ranking



Source: Brandefense Ransompedia accepted listings. 2026: 1 January–22 November; 2025: full year. Unmatched periods; not a national risk ranking [S3].

Country	Accepted listings in the 2026 research window	Full-year 2025 listings
Netherlands	77	44
Belgium	46	42
Germany	457	311
France	295	182
United Kingdom	383	288

[S3]

The 2026 column is partial-year and ends at the retained cutoff snapshot. The 2025 column covers a full year. The Dutch partial total is already above the previous annual total, but this is not a matched-period growth rate. The table also provides no population adjustment or probability of compromise.

Belgium, Germany and France provide nearby EU context; the United Kingdom adds a nearby non-EU comparison. Different economic size, disclosure, sector composition and criminal listing behaviour can affect counts. These figures are therefore descriptive comparators, not a league table of national security performance.

Group label as held	Dutch listings	Interpretation
Lockbit5	15	Most frequent label in this snapshot
Thegentlemen	9	Second by held Dutch listings
Qilin	6	Six listing claims, not six independently established intrusions
INC Ransom	4	Listing population only
DragonForce	4	Listing population only
Other labels	39	The remainder across multiple brands

[S3]

Lockbit5

Listing label in the retained snapshot

Ransomware and extortion listing alias | No state attribution established here

IN THE NETHERLANDS, 2026

2026 window

15 Netherlands listings under this label

CLAIMED TARGETS

Organisations associated with Netherlands listings; identities withheld

SEEN IN PUBLIC REPORTING

[S3] Ransompedia snapshot records 15 listings under the Lockbit5 label

OUR ASSESSMENT

The label is the most frequent in this Netherlands snapshot. It does not establish code lineage, a shared affiliate, encryption, payment or the accuracy of every country association. Prepare recovery and evidence preservation independently of branding.

CONFIDENCE

High for the retained listing count; individual claims unverified

Qilin

Listing label in the retained snapshot

Ransomware and extortion listing alias | No state attribution established here

IN THE NETHERLANDS, 2026

2026 window

6 Netherlands listings under this label

CLAIMED TARGETS

Organisations associated with Netherlands listings; identities withheld

SEEN IN PUBLIC REPORTING

[S3] Ransompedia snapshot records 6 Netherlands listings under Qilin

OUR ASSESSMENT

A listing creates a validation task, not a verified intrusion finding. Check incident records and supplier notices before linking an organisation to a new event. Listing volume does not identify a particular access route or defensive weakness.

CONFIDENCE

High for the retained listing count; access route and impact unresolved

7.3 ShinyHunters and company-specific attribution

ShinyHunters

Extortion attribution in company reporting | Attribution by Odido; not independently established by this report

IN THE NETHERLANDS, 2026

5–6 February

Dates given by Odido for its customer-system incident

7 September

Police described IT-colleague impersonation and subsequent publication of data

CLAIMED TARGETS

The publicly confirmed customer-contact incident; no wider victim list inferred

SEEN IN PUBLIC REPORTING

[S14] Odido attributes its February incident to ShinyHunters

[S15] Police describe the phone pretext, data theft and extortion demand

OUR ASSESSMENT

Validate the caller and the requested action separately. A familiar voice or internal jargon does not authorise a login, code disclosure or customer export. A retained advertisement does not establish the poster is the operator named by the company.

CONFIDENCE

High for the published company attribution; operator identity not independently verified

Odido's updated account names ShinyHunters. The Ransompedia snapshot separately contains two Dutch listings under a Shinyhunters label. These are different records with different meanings. This report does not infer that every related customer-data disclosure or supplier incident belongs to that group. [S14][S3]

7.4 Three official campaign strands

Messaging accounts and recovery secrets

AIVD and MIVD's March notice describes Dutch government employees as targets and victims of a campaign they attribute to Russian state hackers. It concerns individual accounts, verification or PIN codes and linked devices. The notice rejects a platform-wide compromise of Signal or WhatsApp. [S36]

Their June update describes phishing for Signal backup recovery keys as an evolution of the activity. It should not automatically be counted as a second distinct victim event. The agencies' account establishes campaign development, while individual totals and intrusion dates remain unavailable here. [S57]

Messaging-account campaign

Campaign described by AIVD and MIVD

State-attributed account-access campaign | Russian state hackers, according to AIVD and MIVD

IN THE NETHERLANDS, 2026

9 March
Authorities reported Dutch government staff among targets and victims

30 June
Authorities warned about phishing for backup recovery keys

CLAIMED TARGETS

Messaging accounts, with individual identities withheld

SEEN IN PUBLIC REPORTING

[S36] AIVD and MIVD describe verification-code and linked-device abuse

[S57] AIVD and MIVD describe backup recovery-key phishing

OUR ASSESSMENT

The account-recovery and linked-device paths deserve explicit review. These notices do not establish a defect in the messaging platforms themselves. Restrict sensitive work to approved channels and investigate unauthorised device links with the account owner.

CONFIDENCE
Official attribution as stated; no independent actor attribution

A response should also consider earlier conversations and connected devices. Changing one secret does not establish that the attacker never read prior material or that every linked session is removed. Users need a supported checklist and a confidential reporting route, especially where disclosure could expose sensitive relationships.

Cameras and logistics visibility

The agencies' July account attributes a European camera-espionage campaign to Russian state actors. It confirms a small number of hacked cameras on Dutch military-logistics routes, without publishing the owners or an exact count. This report does not identify their locations. [S58]

IP-camera espionage campaign

Campaign described by AIVD and MIVD

State-attributed camera-access campaign | Russian state actors, according to AIVD and MIVD

IN THE NETHERLANDS, 2026

10 July

Authorities reported a small number of affected Dutch cameras

CLAIMED TARGETS

Privately operated cameras near military-logistics routes; owners and locations withheld

SEEN IN PUBLIC REPORTING

[S58] AIVD and MIVD describe structured camera espionage in Europe and Dutch cases

OUR ASSESSMENT

Camera access can reveal operational patterns without access to a military network. Inventory ownership, remote administration and support dependencies. The separate underground camera-list advertisement is not linked to this campaign by the retained evidence.

CONFIDENCE

Official attribution and Dutch case confirmation as stated; no exact domestic count

A practical inventory should cover administration and data access rather than only ownership of the building. A facilities contractor may manage the camera, while another team decides what it records. The response plan should make those responsibilities explicit and retain a local method of checking whether access is authorised.

Targeted malware against people

AIVD's September account, based on joint work with UK services, describes Iranian cyberactors using CHOSEN BRICK against critics in the West and confirms Dutch victims were informed. This is the source agencies' attribution, not this report's independent attribution or a judgement about the targeted people. [S61]

CHOSEN BRICK campaign

Name used in the joint advisory

State-attributed malware campaign | Iranian cyberactors, according to AIVD and partner agencies

IN THE NETHERLANDS, 2026

15 September

Joint advisory published; underlying Netherlands targeting dates from at least 2025

CLAIMED TARGETS

Individuals described by the agencies as dissidents, activists and journalists; identities withheld

SEEN IN PUBLIC REPORTING

[S61] AIVD says Dutch victims were informed

[S95] Joint advisory describes the malware and campaign techniques

OUR ASSESSMENT

Provide a safe reporting route for people with heightened exposure, and isolate suspicious files for authorised analysis. The matrix describes campaign behaviour and capabilities. It does not establish that every technique occurred against each Dutch victim.

CONFIDENCE

Official attribution as stated; victim counts and individual dates withheld

TECHNIQUES LISTED IN THE JOINT AGENCY ADVISORY, BY TACTIC

Initial access	Execution	Persistence	Collection	Exfiltration	Impact
T1566.003 Spearphishing via Service	T1204.002 Malicious File	T1547.001 Registry Run Keys / Startup Folder	T1113 Screen Capture	T1041 Exfiltration Over C2 Channel	T1485 Data Destruction

CHOSEN BRICK technique IDs are explicitly listed in the joint advisory [S95]. The selected rows describe campaign behaviour or capabilities, not proof of every technique against Dutch victims. Messaging and camera notices are not assigned unsupported technique IDs. [S95]

The joint advisory supplies the technique mapping shown in the widget. It is a campaign behaviour and capability mapping. It does not prove that every listed technique was used against every Dutch victim or establish victim identities. [S95]

China-related assessments and historical context

An April AIVD notice endorses advice concerning covert networks used by Chinese hacking groups against Dutch and allied interests. An October MIVD/AIVD notice addresses edge-device espionage and a multi-year pattern, alongside an expectation of more activity. Neither supplies a new, complete Dutch victim list. [S48][S62]

The 2025 annual reports, published in April 2026, also discuss earlier messaging access, Dutch hosting-provider intrusions and North Korean IT-worker-related threats. Their publication belongs in this year's context; the underlying 2025 activity does not become a new 2026 incident merely through publication. [S90][S91]

A July Zimbra advisory supplies another useful boundary. AIVD described a campaign against Western organisations but explicitly said that incident had no Dutch victims. It can inform product readiness without being counted as a domestic compromise. [S59]

Software packages and the development environment

NCSC's April notice describes malicious package versions following Trivy access, CanisterWorm spread and a separate axios incident. It notes indications of exfiltration without enumerating Dutch victims. Keep these events distinct when reviewing build credentials, package trust and the services developers can reach. [S43]

7.5 Enforcement changes infrastructure, not the history of stolen data

Announced	Official action	What the figures describe
4 March	International action took a stolen-data forum offline [S89]	Criminal-market disruption, not a newly measured Dutch breach total
21 May	Police described taking a criminally oriented VPN service offline with French authorities [S51]	33 associated servers dismantled and 83 intelligence packages; international enforcement
28 May	Police/NCSC botnet action [S52]	At least 17 million infected devices globally and 200 infrastructure servers in the Netherlands
18 June	SocGholish-related disruption, linked by police to EvilCorp [S55]	14,971 websites cleaned internationally; infrastructure and credential figures are not Dutch victim counts
24 June	Infostealer infrastructure and credential recovery [S56]	More than 24 million logins from at least 384,000 systems in an international action
28 October	Action against a hosting company described by police as supporting criminal services [S65]	Infrastructure enforcement, without a census of breached Dutch customers
12 November	Further Operation Endgame action [S71][S72]	Dutch-location and international figures require separate treatment

For the November action, police reported 14 Gootloader servers removed in the Netherlands and six Dutch servers within a 120-server CastleRAT action. Its StealC figure included 80 servers removed by Dutch police. The latter does not establish their location. Recovered personal-data items were international. [S71][S72]

Do not add the June and November totals as independent unique victims or records. Their periods and infrastructure relationships can overlap. More importantly, dismantling a server does not revoke every stolen credential or remove every implant already delivered.

KEY TAKEAWAYS

01

Keep criminal claims, company attribution and agency assessments distinct on every map and card.

02

Ransomware comparisons describe listings with explicit periods, not national risk.

03

Infrastructure takedowns still require organisations to validate credentials, access and earlier compromise.

CHAPTER 08

The fraud economy and harm after disclosure

THIS CHAPTER ANSWERS

How can an advertised identity or stolen record become a fraud or personal-safety problem?

36

distinct payment cards visible in clear text in the retained posts, with no issuer attribution

8.1 Accounts and identity as advertised products 62

8.2 Real information can make a false request convincing 65

8.3 Personal safety after data theft 66

8.4 Clear-text cards: a narrow observation 67

8.5 Police prevention activity is evidence of a response, not a loss total 67

CHAPTER 08

The fraud economy and harm after disclosure

IN SHORT

The held posts advertise financial accounts, identity material, contact lists and claimed access. They establish offers, not completed transactions or a measured fraud market. Official reporting adds a more serious consequence: stolen bank-customer information linked to attempted violence. Keep fraud controls, privacy communications and personal-safety escalation connected. Validate the affected information, verify payment instructions independently and give people a clear route for suspicious approaches.

8.1 Accounts and identity as advertised products

Within the 3,286 held country-tag posts assessed for themes, financial-account trading appears in 1,000 posts. Identity or verification material appears in 432, and phishing or fraud in 443. Categories overlap and country mentions can be incidental. These counts cannot be extrapolated into Dutch transactions or losses. [S1]

A financial brand in an advertisement can describe the product the seller wants to exploit, rather than the source of a breach. An account-opening offer does not establish that an account passed that institution's checks. A contact list grouped by bank does not establish that the bank supplied the list.

A 20 November post advertises a multi-country phishing panel naming a Dutch issuer and claiming interactive login-code features. It does not establish deployment, effectiveness or a successful bypass. A separate 8 November offer describes 265,000 Dutch crypto leads; it is not established as the forex file in Case E. [S1]

A 22 November post repeats the kit-advertising language. Repetition does not establish deployment, effectiveness, a successful bypass or a common operator. [S1]

Evidence card B15 — 20 Nov 2026

Phishing-kit seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

[phishing-panel brand] is a live panel phishing kits customized to target specific banks [...] Netherlands [card issuer] [...] Multi-Country Targeting [...] Mobile and desktop interfaces [...] Live Chat (with victim) [...] OTP/TAN/2FA support [...] [contact removed]

Note. A 22 November post repeats the kit-advertising language. Repetition establishes circulation, not deployment, bypass success or a common operator.

Held
A 20 November seller advertises a multi-country phishing panel naming a Dutch card issuer and claiming interactive login-code support.

Not established
Operational deployment, effectiveness, victimisation, exact mechanism, bypass success or compromise of any issuer.

Evidence card B16 — 8 Nov 2026

Lead-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

Format: Country + Email + Name + Currency + Phone + Deposits Amount. [...] Premium Dataset [265K] NETHERLANDS CRYPTO LEADS [VIP DATA] [...] [contact removed]

Note. The advertised cryptocurrency leads are not established as the same file as the forex offer in B05.

Held
A 8 November post advertises a 265k Dutch crypto lead dataset and its claimed fields.

Not established
Origin, currency, authenticity, unique people or relation to the 230k forex list.

B17 advertises bank-labelled leads alongside other countries. B18 promotes a claimed virtual-camera verification bypass. B19 asks USD 200 for an advertised bank account, or USD 250 with an associated exchange account. None establishes supplied accounts, legitimate identities, usable funds or completed sales. Do not treat advertised support for verification as a proven bypass. [S1]

Evidence card B17 — 18 Jul 2026

Lead-data seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

SMS & E-Mail leads DBs on sale. [bank] NL leads, [bank] DE Leads [...] Various countries Leads phone partial email [...] Banking customers leads Dbs - various countries [...]

Held
A recurring sales text offers Netherlands-labelled bank leads alongside other financial datasets.

Not established
Bank-side origin, capture date, unique people, data validity, operator identity or a separate breach per repost.

Evidence card B18 — 13 Sep 2026

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

ORIGINAL

Netherlands Bank kyc bypass | KYC Bypass with Virtual Camera on Android [...] For free and Paid KYC Bypass Methods [...] [bank] Netherlands Virtual Camera [...] [links removed]

Held
A forum promotion claims virtual-camera methods for Dutch-bank identity verification.

Not established
Whether a method exists or works, any successful account opening, victim counts or any bank breach.

Evidence card B19 — 15 Apr 2026

Account seller (alias withheld) | Forum thread | Forum | English

ORIGINAL

[Dutch bank] [...] on your own phone. Price: 200$ (with exchange on same name = 250$) [...] account verified on your own phone [...] NL IBAN - Docs + Selfie [...] Ideal payments [...] [contact removed]

Held
A seller advertises a verified Dutch bank account, documents/selfie and payment functionality at stated asking prices.

Not established
Whether accounts can be supplied, ownership, identity legitimacy, active balances, completed sales or misuse at the bank.

Two recent posts require a different reading. B20 presents a business-bank account while soliciting work; the text does not establish criminal intent. B21 asks to buy a cryptocurrency-service database, without establishing that the database exists. Neither is counted as a fraud or victim incident. [S1]

Evidence card B20 — 15 Nov 2026

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

ORIGINAL

I have a small company in netherland named zzp. I have [bank] Business. i can create and more. I m opened for any ideea, any kind of work [...] [contact removed]

Note. The post does not establish criminal intent. It is not counted as a fraud incident.

Held
A 15 November poster presents a Dutch business-bank account while soliciting work or proposals.

Not established
Criminal intent, account availability, identity, transfers, fraud or any bank breach.

Evidence card B21 — 10 Nov 2026

Database buyer (alias withheld) | Forum thread | Forum | English

ORIGINAL

im looking to buy the [cryptocurrency service] databse [...] [contact removed]

Note. A purchase request does not establish that any database exists.

Held
A 10 November forum user asks to buy a database labelled with a cryptocurrency-service name.

Not established
Whether any database exists, its age, source, sale or compromise.

Prices in individual advertisements are asking prices. The retained evidence does not establish payment, delivery or the value of a national market. A high quoted dataset price can be an advertising claim; a free file can still justify a serious investigation if it contains verified current information.

8.2 Real information can make a false request convincing

A message quoting a person's real membership, booking or customer relationship can appear trustworthy. The confirmed incidents in Chapter 5 explain why the secrecy of such details is an unsafe verification principle. This is a defensive interpretation, not proof that every disclosed record was used in fraud.

Payment confirmation should therefore use a route established independently of the incoming request. A person should not verify a changed bank instruction by calling the number printed on the suspicious message. Business processes should specify which known record or official channel supplies the contact route.

Communications should make the safe route easy to find. A warning that merely says be vigilant leaves the user to improvise. State where to check a payment request, which information the organisation will not request through unsolicited contact and how to report an approach without forwarding sensitive data widely.

8.3 Personal safety after data theft

P

CASE P

Revolut data theft and attempted violence

Banking customers

Police-reported investigation

WHAT WAS CONFIRMED	A 19 November police notice describes September theft of identifying information concerning hundreds of European Revolut customers, including Dutch victims. It links the investigation to thwarted violence and arrests. Individual victims and identifying locations are not reproduced here. [S75]
REPORTED DETAIL	NOS quoted the bank giving 36 affected Dutch customers and described impersonation of an Italian authority. That figure is attributed reporting, not a Dutch count supplied in the police notice. It must not be combined with other account or record totals. [S76]
LIMIT	A public disclosure date is not the intrusion date. This report does not reconstruct the complete criminal chain or infer that every person whose data was taken faced the same threat.
RESPONSE	Include a route for credible safety concerns in customer incident handling, with trained escalation to appropriate authorities and controlled access to sensitive reports.

Bottom line

Connect fraud, privacy and personal-safety support without assuming an industry-wide rate.

The important operational lesson is the handoff. A customer report about an approach can arrive at a fraud desk, a privacy mailbox or ordinary support. These teams need a way to recognise a credible immediate concern and pass it to the accountable response owner without circulating details beyond those who need them.

A bank should keep the affected person's practical needs separate from public attribution. The customer may need advice before the organisation can describe the entire incident. Establish a known contact route, record what the person reports and avoid asking them to investigate the threatening party themselves.

8.4 Clear-text cards: a narrow observation

SCOPE OF THE CARD FIGURES

Card figures cover only payment cards visible in clear text in the retained posts. Brandefense detects stolen cards through other methods outside this report. These observations do not measure national card theft, active cards, issuer prevalence or fraud losses.

The retained result contains 36 distinct cards, 66 appearances and 43 posts. The brand labels are 30 Visa, five Mastercard and one Amex. No issuer is attributed. Repeated appearances are not additional distinct cards, and a brand label is not a named bank. [S4]

The appropriate operational action depends on authorised validation. A payment or fraud team should use a trusted compromise-reporting route, identify the relevant cards within its remit and apply issuer policy. A small public aggregate does not establish that an institution outside that result has no exposure.

8.5 Police prevention activity is evidence of a response, not a loss total

The police's January ticket-fraud notice describes a simulated shop exercise running across late 2025 and early 2026. Its 3,432 purchase attempts were interactions with a prevention exercise, not measured criminal theft. A separate January warning concerned fraudulent emails impersonating police and seeking a response, money or information. [S78][S79]

On 21 November police reported a simulated collectible-card webshop campaign launched in September. The notice's 5,312 advertisement clicks describe campaign interaction. They are not 5,312 victims, completed fraudulent payments or a loss estimate. [S77]

KEY TAKEAWAYS

01

Advertised accounts and identity material are offers, not established transactions or national losses.

02

Customer response should connect fraud, privacy and credible personal-safety concerns.

03

Clear-text card counts and prevention-exercise interactions each require their own narrow denominator.

CHAPTER 09

Banking and finance: separate the institution, customer and supplier

THIS CHAPTER ANSWERS

Which financial-sector conclusions follow from the observed domains and customer incidents?

21 of 25

selected finance domains with a published DMARC quarantine or reject policy

9.1 The financial population 69

9.2 Three different locations of risk 70

9.3 What to validate first 71

9.4 Reporting and customer response share one chronology 71

CHAPTER 09

Banking and finance: separate the institution, customer and supplier

IN SHORT

The finance cell contains banks, payment businesses and trading firms. It is not a list of 25 licensed issuers. Public technical observations show mail and web settings, while the Revolut case concerns a specific customer-data incident. Exposure associations cover the finance cell; the narrow card result has no issuer attribution. Validate institutional scope first, then test recovery, payment changes and the supplier paths holding customer information.

9.1 The financial population

The selected finance cell contains 25 candidate domains, with passive observations for all 25. It is broader than a bank or card-issuer cohort. DNB's register distinguishes licensed institutions and foreign passporting, and cannot be replaced by this report's selection. No individual bank exposure ranking is published. [S2][S7]

21 of 25

selected finance domains with DMARC quarantine or reject observed

25 of 25

selected finance domains with valid TLS results in this snapshot

19 of 19

observed finance homepages carrying HSTS; 6 other candidate homepages outside that denominator

0

issuer attributions in the narrow clear-text card result, not zero issuer exposure

SCOPE OF THE CARD FIGURES

Card figures cover only payment cards visible in clear text in the retained posts. Brandefense detects stolen cards through other methods outside this report. These observations do not measure national card theft, active cards, issuer prevalence or fraud losses.

[S2][S4]

Observation	Result	Limit
DMARC reject / quarantine	16 / 5	Published policy, not a measured phishing-success rate

Observation	Result	Limit
Monitoring policy / policy not observed	3 / 1	Owner validation needed before changing legitimate mail flows
SPF / DKIM observed	23 / 23	Record observation does not establish every message's authentication result
DS record observed	18	Does not establish complete DNSSEC validation
Valid TLS result	25	Describes the observed endpoint and snapshot
Homepage / HSTS observed	19 / 19	HSTS interpretation uses 19 homepages, not all 25 candidates
Device associations / employee subset	38,085 / 395	Overlapping observations, not confirmed internal intrusions
Credential records / current listings	178,904 / 11	Records and selected entries are different populations
Attributed card issuers	None in this result	No issuer comparison or join to the finance domain cell

[S2][S4]

The finance cell covers 25 selected entries, including an issuer-domain subset of nine entries. No issuer-attributed card appears in this narrow result. That absence does not establish zero card exposure. The broader finance cell has at least 38,085 device associations, including 395 employee-device associations, and 178,904 credential records. [S2][S4]

9.2 Three different locations of risk

Institutional access. The security team should assess the organisation's own privileged accounts, recovery procedures and externally reachable systems. A customer-facing brand in a fraud post does not by itself establish access to those systems. Conversely, a well-configured public domain does not establish that internal account recovery is safe.

Customer information and accounts. The fraud team should test decisions that can change the destination of money, create trusted access or disclose sensitive information. The customer can face a convincing approach using real details without the attacker holding the institution's current password. Independent confirmation should focus on authority for the requested action.

Supplier and service access. Customer information can sit with a provider or be released through a process that trusts an external request. The bank needs the relevant service, permitted users and update route. A supplier's security statement should not replace the institution's own assessment of data, customer communications and regulatory duties.

Case P illustrates why these responsibilities should meet. The disclosed incident and later police investigation require a response to affected customers, not only a technical statement about the bank's public website. That response still needs evidence specific to the person's circumstances; one case cannot establish an industry-wide rate.

9.3 What to validate first

For recovery, test a caller who knows accurate customer or employee details but cannot use the established trusted route. The authorised exercise should establish whether the process permits a high-impact change and which evidence supports the decision. Include a genuine user who has lost a factor, so the approved exception remains workable.

For payments, test a changed beneficiary, supplier account or payroll instruction through the relevant business process. Security can define technical safeguards, but finance and customer operations must own the decision to accept the instruction. Completion evidence should include a caught test and a record of authorised exceptions.

9.4 Reporting and customer response share one chronology

Financial reporting, privacy assessment and customer communications should use one factual chronology while preserving their separate legal tests. DORA and GDPR have different triggers and reporting requirements, as Chapter 10 explains. An early record should preserve what was known when each decision was made.

KEY TAKEAWAYS

01

The selected finance domains are not a licensed-bank or issuer census.

02

Institution, customer and supplier risks need different evidence and accountable owners.

03

Test recovery, payment changes and reporting together while keeping their legal decisions distinct.

CHAPTER 10

Regulation and the national response

THIS CHAPTER ANSWERS

Which reporting clock applies, who receives the notice and what should the incident owner record?

15 August 2026

commencement date confirmed by the Cyberbeveiligingsbesluit

10.1 What applies and what needs an entity-specific decision 73
10.2 The Cyberbeveiligingswet significant-incident sequence 73
10.3 Privacy notification is a separate risk decision 74
10.4 Financial ICT incidents have another clock 74
10.5 Investigations and public response are not concluded findings 75
10.6 Four things to establish now 75

CHAPTER 10

Regulation and the national response

IN SHORT

The Cyberbeveiligingswet is in force, while privacy and financial-sector obligations have their own triggers and clocks. A significant cyber incident, a personal-data breach and a major financial ICT incident are different legal assessments. One event can require several decisions. Establish scope and reporting recipients before the incident, then preserve awareness, classification, notices and updates in one chronology with a named owner and alternate.

10.1 What applies and what needs an entity-specific decision

The national summary and commencement order establish 15 August 2026 as the start date for the Cyberbeveiligingswet framework. Organisations should use the enacted text and applicable sector criteria rather than an older forecast of implementation. The related critical-entity framework should not be assumed to have identical incident-reporting tests. [S8][S10]

Framework	Decision required	Recipient and caution
Cyberbeveiligingswet	Determine whether the entity and service fall within scope; registration, care and significant-incident duties apply as specified	Designated CSIRT and competent supervisor; use the applicable sector rules [S8][S9][S84]
GDPR Articles 33–34	Controller assesses the breach and risk; processor informs its controller	Relevant supervisory authority and, where required, affected people; clocks and tests differ [S11]
DORA incident reporting	In-scope financial entity assesses whether the ICT incident is major	Relevant financial authority; the technical standard supplies notification and update clocks [S12]

The Cyberbeveiligingswet specifies ceilings of EUR 10 million or 2% for essential entities, and EUR 7 million or 1.4% for important entities, whichever is higher. The percentages concern the undertaking's total worldwide annual turnover in the preceding financial year. These ceilings concern specified contraventions, not fines imposed in the cases here. [S9]

10.2 The Cyberbeveiligingswet significant-incident sequence

NCTV describes a significant incident by serious actual or possible service disruption or financial loss, or considerable material or immaterial harm to others. Sector criteria vary. Its reporting route uses MijnNCSC for the designated CSIRT and competent supervisor. Certain entities have different deadlines. [S84]

Cbw stage	General clock stated by NCTV
Early warning	Within 24 hours of awareness of a significant incident
Incident notification	Within 72 hours of that awareness
Final report	Within one month after the incident notification

[S84]

Early reporting should distinguish facts from estimates. The reporter should be able to state the affected service, known effects, uncertainty and the next update route. A notice can be timely without pretending that the complete root cause or final impact is already known.

10.3 Privacy notification is a separate risk decision

Under GDPR, controllers notify the supervisory authority without undue delay and, where feasible, within 72 hours of awareness, unless risk to people is unlikely. Processors notify the controller without undue delay. Article 34 requires communication to affected people without undue delay where high risk is likely, subject to exceptions. [S11]

This means the supplier's notice and the controller's authority notification are different events. Contract terms should give the controller information it can use, including what is confirmed and what remains unresolved. Waiting for the supplier's final investigation can prevent the controller from making its own timely assessment.

Communications to people should explain their practical options. An affected customer needs to know what information could support a suspicious approach and how to verify contact. Avoid presenting a generic password change as a complete response where the exposure concerns identity documents, booking details or other information that cannot simply be reset.

10.4 Financial ICT incidents have another clock

Article 5 supplies the financial reporting sequence:

Stage	Clock
Initial	As early as possible, within four hours of major classification and no later than 24 hours after awareness
Late classification	If classification follows the 24-hour point, four hours after major classification
Intermediate	Within 72 hours after the initial notice
Final	Within one month after the intermediate report or latest update

For initial notifications and intermediate reports, credit institutions, central counterparties, trading-venue operators and financial entities designated essential or important cannot use the weekend or bank-holiday deferral. Article 5(5) does not exclude final reports from that deferral. [S12]

The privacy and financial reports can share facts without sharing a legal conclusion. One record should support them, while the decision log shows which test each reporter applied. This is more reliable than creating unrelated timelines that later disagree on when the organisation knew what happened.

10.5 Investigations and public response are not concluded findings

The RDI/AP investigation announced in March concerned the Odido incident. Its July update and ACM's announcement distinguish security, duty-of-care and retention remits. These are investigations and supervisory responsibilities, not final findings that every alleged failure or attacker figure was established. [S16][S17][S34]

A board exercise should test the route from technical evidence to each decision. Ask who approves the notice, who can submit it, who updates affected people and who records the reasons for withholding a notification where the legal test is not met. Completion evidence is the timed decision record, not simply attendance at the exercise.

10.6 Four things to establish now

1. **Coverage.** Identify applicable entities and services, including critical supplier relationships, and resolve legal uncertainty before an incident.
2. **Ownership.** Name the reporter and alternate for every relevant CSIRT, supervisor, privacy authority and criminal-reporting route.
3. **Chronology.** Preserve detection, awareness, classification, notification and update times in one record with their supporting facts.
4. **Usable notices.** Prepare templates that separate confirmed information, estimates, consequences, action and next update. Test them with a supplier and customer-facing team.

This chapter is a planning aid. The accountable organisation should confirm its own coverage, sector criteria and reporting channel against the current authoritative text. The 90-day plan includes the exercise and its evidence, while an actual material incident enters the response process immediately.

KEY TAKEAWAYS

01

The cyber, privacy and financial reporting tests require separate decisions.

02

Record awareness and classification explicitly, with the right reporter and alternate.

03

Supplier terms and exercises should support timely, usable notices rather than wait for final certainty.

CHAPTER 11

Outlook: decisions that change when the evidence changes

11

THIS CHAPTER ANSWERS

What should organisations prepare for next, and which signals would justify changing the plan?

5

conditional judgements with an owner-relevant signal

11.1 Five judgements 77

11.2 Evidence that would change the assessment 78

11.3 Conditional scenarios for an exercise 78

CHAPTER 11

Outlook: decisions that change when the evidence changes

IN SHORT

Prepare for recurrence of the mechanisms established here: account impersonation, supplier data loss, exposed administration and service dependency. The evidence does not support a forecast of every actor's next target or a national attack rate. Each judgement below names its basis, limitation and signal. Assign an owner to review those signals monthly, and change priorities when the relevant evidence changes.

11.1 Five judgements

Judgement	Confidence	Basis, limit and signal
If customer records remain usable for identity checks, incidents can support convincing follow-up approaches	Medium, conditional	Cases G, O and P show why data and customer response belong together. No rate of follow-up misuse is measured. Signal: verified customer reports using incident-specific information
Shared-service incidents will remain an important continuity planning scenario	High as a planning priority	Cases K, L, M and O involve distinct service dependencies, not one common route. Signal: provider notices and the time required to establish each customer's scope
Current public technical gaps warrant owned validation, rather than a national risk score	High for this selected list	Chapter 3 has bounded observations and group overlap. Signal: confirmed corrections, approved exceptions and unresolved ownership in the organisation's own issue register
Extortion readiness should include publication of data as well as restoration	High as a preparedness judgement	Ransomware listings are claims, and the cases do not establish a route for every listing. Signal: accepted listing activity plus evidence specific to the organisation's data [S3]
Connected assets and personal accounts need explicit owners in sensitive work	Medium as a planning judgement	The official campaign evidence concerns particular messaging, camera and malware activity. It is not a forecast against every asset. Signal: official campaign updates and validated exposure of owned assets

11.2 Evidence that would change the assessment

Current interpretation	Evidence that would change it	Decision affected
A database offer is an unverified lead	Authorised validation connects the material to a specific current system or an official confirmation establishes scope	Activate the relevant incident and customer-protection process
A supplier incident has uncertain customer scope	The provider identifies the customer's affected tenant, records or interface with supporting evidence	Adjust notice, containment and reconnection decisions
A domain observation needs owner validation	The owner confirms a production gap or an approved architecture explains the result	Correct the gap or record the exception; do not retain an unexplained alert
A connected-system claim has unknown physical effect	Local records and operations staff establish an unauthorised setting change or material service impact	Escalate operational containment and continuity response
A state attribution belongs to the quoted source	The responsible source issues a materially different assessment with evidence	Update the attribution while retaining evidence-led controls
A service outage has no established malicious cause	The provider or authority establishes an attack affecting the relevant service	Add incident-response and reporting assessments to continuity work

11.3 Conditional scenarios for an exercise

A supplier sends an incomplete notice. If the notice identifies a service but not the customer's data, ask for the scope needed for the customer's own assessment. The signal is missing tenant, data or interface information. The decision is who escalates, what is provisionally isolated and when the next update is required.

A caller knows genuine details and requests a recovery change. If the caller cannot use the established trusted route, apply the approved exception process rather than accepting familiarity as authority. The signal is the requested trust change. The decision is who can authorise it and what evidence must remain in the record.

A remote-control claim coincides with a service problem. If local readings or logs show a relevant change, involve operations immediately and assess safe isolation. The signal is verified equipment or service evidence, not the advertisement alone. The decision is how to protect the process while preserving an authorised recovery path.

The normal communications provider is unavailable. If responders cannot receive messages or reach the duty owner, use the tested independent route. The signal is loss of the required function. The decision is who publishes status and how the team obtains supplier and legal input without that service.

These scenarios are planning assumptions, not measured intervals or claims that any named organisation omitted a control. Their value is the decision record from a realistic exercise: what the team knew, what it did and what prevented the next action.

KEY TAKEAWAYS

01

Forecasts should name a condition, evidence limit and signal that an owner can watch.

02

Change the response when verified scope or operational effects change.

03

Review the plan monthly while escalating actual material threats immediately.

CHAPTER 12

A 90-day plan with evidence of completion

12

THIS CHAPTER ANSWERS

What should each team do, and how will leadership know that the work changed a real control?

23

actions with accountable owners and completion evidence

12.1 Actions and completion evidence 81
12.2 A scorecard that measures finished work 84
12.3 Technical reference: patch state and earlier access 85
12.4 First decisions by role 85
12.5 How Brandefense can help 86

CHAPTER 12

A 90-day plan with evidence of completion

IN SHORT

Start with a trusted route for incident signals, account recovery, supplier notices and operational escalation. Then close confirmed technical and process gaps, including browser dependencies and remote administration. Exercise restoration, fraud handling and the reporting clocks together. The dates below organise improvement work; they do not delay response to an active threat. Report the completed evidence, remaining exceptions and accountable owners to leadership by day 90.

12.1 Actions and completion evidence

This is a sequence, not a waiting period. A credible material signal enters the incident process immediately. If required alerts or supplier information are unavailable, record the dependent task as blocked, name the owner and state what will unblock it. Monitoring can come from an internal team or an appropriate provider.

Start patching or applying authoritative mitigations immediately for applicable critical or actively exploited vulnerabilities on internet-facing services. Do not wait for the milestones below or signs of exploitation. [S22]

1Days 1-30	
Confirm the route for relevant account, data-offer and service alerts; test one handoff into incident response	
OWNER CISO and threat intelligence	COMPLETION EVIDENCE Source and duty owner named; test received and acknowledged
Require independent verification for password, MFA and high-impact recovery changes; test an impersonated colleague	
OWNER Identity and service desk	COMPLETION EVIDENCE Approved procedure; authorised test caught; genuine-user exception tested
For credible account-access signals, validate ownership and current access; revoke relevant sessions or tokens where justified	
OWNER Identity and incident response	COMPLETION EVIDENCE Dated disposition per signal; active access decisions recorded

List critical suppliers holding customer, patient, student, member or case data, with an incident contact and alternate

OWNER
Procurement and service owners

COMPLETION EVIDENCE
Dated service/data list; contacts successfully tested

Map applicable Cbw, GDPR and DORA duties, including awareness, classification, recipient and reporter

OWNER
Legal, privacy and CISO

COMPLETION EVIDENCE
Entity-specific reporting map approved; alternates named

Identify cooling and other operational controls with remote administration; validate the access owner and safe isolation decision

OWNER
Operations, facilities and OT

COMPLETION EVIDENCE
Owned-asset review; unsafe paths addressed or urgent exceptions escalated

Test incident communications without normal cloud mail or collaboration access

OWNER
Incident commander and communications

COMPLETION EVIDENCE
Duty contacts reached; status update approved through independent route

Prepare customer-support escalation for credible safety concerns following data theft

OWNER
Fraud, customer operations and security

COMPLETION EVIDENCE
Confidential route tested; staff know the duty contact

2Days 31-60

Validate authorised mail senders and stage DMARC enforcement where appropriate

OWNER
Messaging and business senders

COMPLETION EVIDENCE
Aligned sender inventory; controlled test and rollback route

Complete the planned patch backlog for internet-facing products named in relevant authoritative warnings; verify remediation and decide separately whether earlier access warrants investigation

OWNER
Infrastructure and incident response

COMPLETION EVIDENCE
Asset/version and verification evidence; separate access-investigation decision recorded

Inventory third-party browser scripts and accounts allowed to change them; test emergency disablement

OWNER
Web, security and digital marketing

COMPLETION EVIDENCE
Dependency owner and change access known; disable/rollback test passed

Agree evidence required before reconnecting a supplier interface, including business approval and rollback

OWNER
Service owners and supplier management

COMPLETION EVIDENCE
Reconnection checklist exercised on one critical dependency

Test changed payment or booking instructions against an attacker who knows genuine customer details

OWNER
Finance, fraud and customer operations

COMPLETION EVIDENCE
Independent verification catches an authorised simulation

Establish reporting and recovery guidance for work-related personal messaging accounts

OWNER
Security and relevant business owners

COMPLETION EVIDENCE
Linked-device/recovery review available; confidential escalation tested

Review camera administration and access to recordings relevant to sensitive activities

OWNER
Facilities and security

COMPLETION EVIDENCE
Authorised access list; removed default or unnecessary remote access

Review exports and temporary data copies created during service workarounds

OWNER
Privacy and data owners

COMPLETION EVIDENCE
Copy locations and access reconciled; retention/deletion decisions recorded

Update customer notices to distinguish affected information, service status, safe verification and the next update

OWNER
Privacy, communications and support

COMPLETION EVIDENCE
Approved templates tested against two materially different cases

3Days 61-90

Restore one critical business process from the documented fallback and reconcile temporary work

OWNER
Infrastructure and process owner

COMPLETION EVIDENCE
Timed result against recovery objective; reconciliation evidence

Exercise an incomplete supplier notice alongside an unavailable interface

OWNER
Incident response, supplier and business owner

COMPLETION EVIDENCE
Scope questions, decisions, update times and blockers recorded

Exercise Cbw, privacy and financial reporting where applicable using one chronology

OWNER

Legal, privacy and regulatory reporters

COMPLETION EVIDENCE

Timed awareness/classification decisions and draft notices preserved

Run an authorised fraud/recovery simulation with a genuine-user exception and customer escalation

OWNER

Fraud and identity

COMPLETION EVIDENCE

Fraud attempt stopped; legitimate recovery completed through approved route

Recheck confirmed domain, certificate and header gaps after correction

OWNER

Network, web and messaging

COMPLETION EVIDENCE

Before/after evidence; approved exceptions carry owners and dates

Present the scorecard, exceptions and row-level completion evidence to leadership

OWNER

CISO and accountable service owners

COMPLETION EVIDENCE

Board paper with residual risks, decisions and completion dates

12.2 A scorecard that measures finished work

The targets below are suggested defaults for the organisation's own control programme. They are not measurements of how Dutch organisations already operate. Adjust them to the business context and record who approves an exception.

Measure	Suggested target
Critical services with an incident owner, alternate and tested contact	100% by day 30
Credible access signals with a dated owner disposition	Within five working days, or immediate incident escalation where material
Critical data-holding suppliers with a tested notice route	100%, or a dated exception, by day 60
High-impact recovery changes using the approved verification process	100%; exceptions independently authorised and recorded
Remote administration of operational controls with an accountable owner	100% by day 30; urgent unsafe access handled immediately
Third-party browser dependencies with an owner and disablement plan	100% of critical customer journeys, or a dated plan, by day 60

Measure	Suggested target
Applicable reporting routes tested with named alternates	Completed by day 90
Critical-process restoration and workaround reconciliation	Passed against the organisation's objective, or a dated fix, by day 90

12.3 Technical reference: patch state and earlier access

NCSC's October PHP advice illustrates the distinction between prevention and a confirmed attack. Its notice treated precautionary shutdown separately from established intrusion. The PHP advisories identify corrected branches for CVE-2026-109618 and CVE-2026-109619. A site's temporary withdrawal does not establish that either flaw was exploited there. [S22][S25][S26][S27][S28]

PHP branch	Affected versions for both CVEs	Fixed release
8.2	8.2.x before 8.2.35	8.2.35
8.3	8.3.x before 8.3.36	8.3.36
8.4	8.4.x before 8.4.27	8.4.27
8.5	8.5.x before 8.5.12	8.5.12

The advisories list no fixed releases for older unsupported branches. Migrate those deployments to a supported branch. [S25][S26][S27][S28]

The owner should match the deployed branch to the relevant authoritative advice, record the change and verify the exposed service. A patch completion entry should not silently close an earlier-access investigation. The Ivanti campaign in Case H provides the separate reason to ask what happened before remediation.

12.4 First decisions by role

Role	First decision
Board and executives	Ask which critical service, supplier and recovery decisions have tested owners and which exceptions require resources
CISO	Connect relevant evidence to incident ownership, supplier scope and the reporting chronology
SOC and incident response	Define the proposition under investigation, preserve the evidence and avoid promoting an alert into unsupported attribution
Identity and service desk	Establish authority for recovery changes independently of what the caller knows

Role	First decision
Infrastructure, web and operations	Confirm the relevant asset, remote administration path and safe correction or isolation route
Fraud and customer operations	Verify consequential instructions through known channels and route credible safety concerns promptly
Privacy, legal and communications	Keep scope, legal tests, public statements and updates consistent without waiting for complete certainty

KEY TAKEAWAYS

01

Confirm signal routes, recovery authority and operational ownership in the first 30 days.

02

By day 60, close validated supplier, browser, remote-access and communication gaps.

03

By day 90, demonstrate restoration, reporting and fraud response with evidence and owned exceptions.

12.5 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The report illustrates how external posts, public technical observations and ransomware claims can support bounded investigative questions. A signal is most useful when connected to the assets, data and decisions the organisation can validate.

A demonstration can use the organisation's domains, brands and security priorities to show that relationship. The discussion should establish what a service observes, which owner receives a relevant alert and how the organisation records a disposition. Historical information and criminal claims still require validation.

Request a demo

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Scope, evidence and interpretation · Appendix B. Post evidence register · Appendix C. Sources · Appendix D. Glossary

109

sources

Appendix A. Scope, evidence and interpretation 88

Appendix B. Post evidence register 91

Appendix C. Sources 93

Appendix D. Glossary 98

Appendix A. Scope, evidence and interpretation

A.1 Window and source populations

The research window runs from 1 January to the retained snapshot on 22 November 2026. The recent-activity window begins on 8 November. The cutoff day describes the snapshot used; it is not assurance of coverage through midnight. Posting, incident, disclosure and update dates remain separate.

Brandefense Blackhole posts, Atlas exposure associations, selected-domain public observations, Ransompedia listings and clear-text card observations are separate populations. Company statements, public authorities and technical research supply external evidence and context. The report does not combine them into a national attack count. [S1][S2][S3][S4]

A.2 Underground posts

The held population is 5,160 posts, including 329 recent-window posts. Country-tag totals are 127,762, with 3,286 held tag posts. Theme and language tables concern that held tag subset, while the platform table concerns the held union. Country mentions can be incidental and languages can overlap. [S1]

Posts establish advertisements, requests, assertions or replies. They do not establish unique incidents, working access, authentic data, operator nationality or completed sales. A repost is evidence of circulation, and an old event does not become current because its advertisement is new.

A.3 Selected candidate domains

The universe contains 250 candidate domains across twelve sector cells, with exposure observations for all entries and passive observations for 249. Entries can represent institutions, groups or operating brands. Group overlap and domain/entity uncertainty prevent interpreting the list as independent national organisations or a representative population. The unavailable candidate is not counted as a failed control. [S2]

A.4 Atlas exposure boundary

The national Atlas headline is 50 out of 100 for 250 selected entries. Only that national rating is published. Device, credential, listing and document associations describe the retained snapshot, can overlap and can include historical material. They do not establish unique people, current working accounts or confirmed intrusions. [S2]

A.5 Passive settings

Public results concern the observed domain and snapshot. DMARC enforcement means a published quarantine or reject policy. DKIM not observed does not establish no signing. DS presence does not establish a valid DNSSEC chain. Certificate, homepage and HSTS results use their actual observation bases. [S2][S85][S86][S88]

A.6 Card scope

Only cards visible in clear text in the retained posts are counted: 36 distinct cards, 66 appearances and 43 posts, with no issuer attribution. Brandefense detects stolen cards through other methods outside this report. These figures do not measure active cards, national theft, issuer prevalence or losses. [S4]

A.7 Ransomware comparison

Ransompedia holds 77 accepted Dutch research-window listings. Comparators use the retained corresponding window; the previous-year column covers full-year 2025. Counts describe criminal claims and can include repeated victim references. They are not unique confirmed breaches or population-adjusted national risk. [S3]

A.8 Incident dating and exclusions

Campaigns, individual examples, supplier notices, subsequent updates, enforcement and prevention are distinguished throughout the report. A collective notice does not establish the complete customer or person population. A worldwide figure does not become Dutch merely because Dutch authorities participated in the response.

The following boundaries prevent older or unrelated reporting from entering current Dutch incident conclusions:

Material	Treatment
A botnet notice dated September 2024 [S80]	Historical context, excluded from 2026 incident conclusions
April and June 2025 DDoS notices [S81][S82]	Historical context, distinct from verified 2026 DigiD reporting
A ransomware notice dated April 2024 [S83]	Historical context, not a new 2026 campaign
Reissued maritime reporting matching a June 2023 event [S100]	Does not establish a new 2026 port incident
A 2026 rail-pass disclosure with December 2025 file transfer	Included as disclosure context in Case R, with the event date explicit
Uncorroborated accounting-service or port-ransom allegations	No public case or accepted incident finding without supporting evidence
GPS disruption and cloud-service outage	Continuity evidence, without an established malicious cause in the cited official accounts
B22 and B23	Visible exclusion examples; no established Dutch incident

Absence from this report does not establish absence of an incident. Private dealings, undisclosed incidents and incomplete public information limit the picture. The report does not claim an exhaustive census of Dutch cybercrime.

A.9 Confidence, naming and public protection

Confidence applies to a specific proposition. An accurately reproduced criminal assertion can have high confidence as a post observation while the asserted intrusion remains unverified. Alternatives and limits remain visible where they affect the decision.

Victim names require official confirmation and broad reporting; generic roles remain appropriate elsewhere. Actor attribution is kept with the company, authority or researcher making it. Public excerpts omit personal records, contact routes and working indicators. Full sensitive provenance is outside this public report.

Appendix B. Post evidence register

Each displayed card identifies the post date, generic venue, role label and proposition limits. Posting dates are not intrusion dates. Short excerpts retain bracketed redactions; B22 and B23 are displayed as exclusions, not Dutch incident evidence. Full sensitive provenance is outside this public report.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-02-19	Forum thread	Data seller (alias withheld)	English	§4.4
B02	2026-11-08	Forum thread	Healthcare-data seller (alias withheld)	English	§4.4
B03	2026-10-18	Forum thread	Retail-data seller (alias withheld)	English	§4.4
B04	2026-04-03	Forum thread	Access seller (alias withheld)	English	§4.4
B05	2026-07-30	Forum thread	Lead-data seller (alias withheld)	English	§4.4
B06	2026-08-23	Forum thread	Forum uploader (alias withheld)	English	§4.4
B07	2026-06-01	Forum thread	Forum reposter (alias withheld)	English	§4.5
B08	2026-01-31	Forum thread	Forum uploader (alias withheld)	English	§4.5
B09	2026-02-01	Forum thread	Education-data seller (alias withheld)	English	§4.5
B10	2026-05-10	Forum thread	Forum poster (alias withheld)	English	§4.5
B11	2026-05-03	Forum thread	Retail-data seller (alias withheld)	English	§4.5
B12	2026-08-11	Forum thread	Automated uploader (alias withheld)	English	§4.6
B13	2026-06-26	Forum thread	Automated uploader (alias withheld)	English	§4.6
B14	2026-09-02	Forum thread	Log buyer (alias withheld)	English	§4.6

Card	Posted	Venue	Alias as shown	Language	Shown in
B15	2026-11-20	Forum thread	Phishing-kit seller (alias withheld)	English	§8.1
B16	2026-11-08	Forum thread	Lead-data seller (alias withheld)	English	§8.1
B17	2026-07-18	Forum thread	Lead-data seller (alias withheld)	English	§8.1
B18	2026-09-13	Forum thread	Forum promoter (alias withheld)	English	§8.1
B19	2026-04-15	Forum thread	Account seller (alias withheld)	English	§8.1
B20	2026-11-15	Forum thread	Forum member (alias withheld)	English	§8.1
B21	2026-11-10	Forum thread	Database buyer (alias withheld)	English	§8.1
B22	2026-05-02	Forum thread	Forum poster (alias withheld)	Indonesian original; English retained translation quoted	§4.7; excluded
B23	2026-11-09	Forum thread	Access seller (alias withheld)	English	§4.7; excluded
B24	2026-08-21	Forum thread	Forum reposter (alias withheld)	English	§4.5

Appendix C. Sources

References retain their source IDs across editions. Own-data entries have no public dataset URL. External entries identify the source and verification date; where an article path identifies a withheld target, the public citation retains only the publisher root.

S1: Odin by Brandefense, Retained Netherlands-associated underground posts. Retained research snapshot, 22 November 2026.

S2: Odin by Brandefense, Atlas and Blackhole exposure associations for 250 selected candidate domains, read on 21–22 November 2026, plus passive observations. Retained research snapshot, 22 November 2026.

S3: Ransompedia, Netherlands and regional ransomware-listing snapshot. Retained research snapshot, 22 November 2026.

S4: Brandefense Blackhole, Payment-card aggregates in retained posts. Retained research snapshot, 22 November 2026.

S5: NCSC, DTC and NCSC combined from 1 January 2026 (2026-01-06). https://www.ncsc.nl/nieuws/versterkt-ncsc-alle-nederlandse-organisaties-krijgen-een-aanspreekpunt-voor-digitale-weerbaarheid. Verified on 2026-11-22.

S6: CBS, ICT use by companies, Digitalisering en kenniseconomie 2025 (2026-02-10). https://www.cbs.nl/nl-nl/longread/rapportages/2026/digitalisering-en-kenniseconomie-2025/3-ict-gebruik-bij-bedrijven. Verified on 2026-11-22.

S7: De Nederlandsche Bank, Register of banks. https://www.dnb.nl/openbaar-register/register-van-banken/. Verified on 2026-11-22.

S8: NCTV, Cyberbeveiligingswet. https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet. Verified on 2026-11-22.

S9: Official Gazette, Cyberbeveiligingswet, Staatsblad 2026,187 (2026-07-10). https://zoek.officielebekendmakingen.nl/stb-2026-187.html. Verified on 2026-11-22.

S10: Official Gazette, Cyberbeveiligingsbesluit, Staatsblad 2026,189 (2026-07-10). https://zoek.officielebekendmakingen.nl/stb-2026-189.html. Verified on 2026-11-22.

S11: EUR-Lex, General Data Protection Regulation, Articles33–34 (2016-04-27). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. Verified on 2026-11-22.

S12: EUR-Lex, DORA incident-reporting technical standard, Regulation2025/301 (2025-02-20). https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng. Verified on 2026-11-22.

S13: Odido, Initial cyberattack disclosure (2026-02-12). https://newsroom.odido.nl/en-us/odido-informs-customers-of-cyber-attack/. Verified on 2026-11-22.

S14: Odido, Updated cyberattack FAQ. https://www.odido.nl/veiligheid-eng. Verified on 2026-11-22.

S15: Politie, Voice of suspected caller in customer-system data theft (2026-09-07). https://www.politie.nl/nieuws/2026/september/7/11-stem-van-verdachte-odido-hack-te-horen-in-opsporing-verzocht.html. Verified on 2026-11-22.

S16: RDI, Joint investigation and Julyupdate on customer-system incident (2026-03-26). https://www.rdi.nl/actueel/nieuws/2026/03/26/rdi-en-ap-starten-onderzoek-naar-aanleiding-van-het-incident-bij-odido. Verified on 2026-11-22.

S17: ACM, ACM joins telecom data-breach investigation (2026-07-13). https://www.acm.nl/en/publications/acm-joins-investigations-data-breach-dutch-telecom-operator-odido. Verified on 2026-11-22.

S18: ChipSoft, Supplier ransomware incident timeline (2026-04-28). https://informatie.chipsoft.com/chip-soft-informatiepagina-ransomware-incident/. Verified on 2026-11-22.

S19: Ahold Delhaize, Update on cybersecurity incident (2026-10-19). https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident. Verified on 2026-11-22.

S20: Ahold Delhaize, Third-quarter2026 interim report (2026-11-04). https://media.aholddelhaize.com/media/voehurnq/ahold-delhaize-q3-2026-interim-report.pdf. Verified on 2026-11-22.

S21: NCSC, Ivanti EPMM exploitation timeline (2026-02-27). https://www.ncsc.nl/alerts/casus-kwetsbaarheden-ivanti-epmm-systemen. Verified on 2026-11-22.

S22: NCSC, Updated PHP vulnerability advice (2026-10-23). https://www.ncsc.nl/alerts/update-php-kwetsbaarheden-nog-steeds-reden-om-direct-te-patchen. Verified on 2026-11-22.

S25: NVD, CVE-2026-109618 record (2026-10-21). https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2026-109618. Verified on 2026-11-22.

S26: NVD, CVE-2026-109619 record (2026-10-21). https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2026-109619. Verified on 2026-11-22.

S27: PHP Security Team, PHP out-of-memory advisory (2026-10-21). https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w. Verified on 2026-11-22.

S28: PHP Security Team, PHP stale-state advisory (2026-10-21). https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp. Verified on 2026-11-22.

S29: Report URI, Malicious scripts delivered through experimentation supplier (2026-11-16). https://blog.report-uri.com/worlds-largest-brands-infected-with-malware-via-optimizely/. Verified on 2026-11-22.

S30: Tweakers, Webshop customer-data incident (organisation withheld) (2026-09-18). https://tweakers.net/ (article URL withheld). Verified on 2026-11-22.

S31: ncsc.nl, Active exploitation campaign (Cross-sector). https://www.ncsc.nl/alerts/casus-kwetsbaarheden-ivanti-epmm-systemen. Verified on 2026-11-22.

S32: open.overheid.nl, Mobile-management system exploitation (Public administration / justice). https://open.overheid.nl/documenten/3ea80b7e-deca-41cc-82f6-3a1b9ab84120/file. Verified on 2026-11-22.

S33: nos.nl, Mobile-management system exploitation (Public administration / justice) (2026-02-06). https://nos.nl/artikel/2601216-datalek-bij-autoriteit-persoonsgegevens-en-raad-voor-de-rechtspraak. Verified on 2026-11-22.

S34: autoriteitpersoonsgegevens.nl, Customer-contact data theft / extortion (Telecommunications) (2026-03-26). https://www.autoriteitpersoonsgegevens.nl/actueel/ap-en-rdi-starten-onderzoek-naar-odido. Verified on 2026-11-22.

S35: nos.nl, Customer-contact data theft / extortion (Telecommunications) (2026-02-12). https://nos.nl/artikel/2602080-hack-bij-odido-gegevens-miljoenen-klanten-in-handen-van-criminelen. Verified on 2026-11-22.

S36: aivd.nl, Messaging-account phishing campaign (Government / defence / media targeting) (2026-03-09). https://www.aivd.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts. Verified on 2026-11-22.

S37: rijksoverheid.nl, Unauthorised system access / containment disruption (Central government) (2026-03-23). https://www.rijksoverheid.nl/actueel/nieuws/2026/03/23/ministerie-van-financien-onderzoekt-ongeautoriseerde-toegang-tot-systemen. Verified on 2026-11-22.

S38: nos.nl, Unauthorised system access / containment disruption (Central government) (2026-03-23). https://nos.nl/artikel/2607547-ministerie-van-financien-gehackt-systemen-geblokkeerd-door-ministerie. Verified on 2026-11-22.

S39: politie.nl, Phishing / short unauthorised access (Law enforcement). https://www.politie.nl/nieuws/2026/maart/25/00-politie-doelwit-van-phishing.html. Verified on 2026-11-22.

S40: ad.nl, Phishing / short unauthorised access (Law enforcement) (2026-03-25). https://www.ad.nl/binnenland/hacker-had-uur-lang-toegang-tot-politiedata-na-phishingactie-maar-schade-lijkt-beperkt~a39827e6/. Verified on 2026-11-22.

S41: epe.nl, ClickFix-related network intrusion and file theft (Local government). https://www.epe.nl/datalek-gemeente-epe. Verified on 2026-11-22.

S42: nos.nl, ClickFix-related network intrusion and file theft (Local government) (2026-04-23). https://nos.nl/artikel/2611660-persoonsgegevens-van-vrijwel-alle-inwoners-epe-gestolen-bij-cyberaanval. Verified on 2026-11-22.

S43: ncsc.nl, Software supply-chain campaign (Software development). https://www.ncsc.nl/alerts/ontwikkelaars-opgelet-gecompromitteerde-npm-en-python-packages. Verified on 2026-11-22.

S44: z-cert.nl, Ransomware and patient-data theft (Healthcare software / healthcare) (2026-04-17). https://z-cert.nl/actueel/nieuws/ransomware-incident-chipsoft-nieuwe-informatie-17-april. Verified on 2026-11-22.

S45: theregister.com, Ransomware and patient-data theft (Healthcare software / healthcare) (2026-04-08). https://www.theregister.com/security/2026/04/08/ransomware-knocks-dutch-healthcare-software-vendor-offline/5220887. Verified on 2026-11-22.

S46: s25.q4cdn.com, Guest-booking information unauthorised access (Travel technology). https://s25.q4cdn.com/383369491/files/content_files/BKNG-3Q26-10Q.pdf. Verified on 2026-11-22.

S47: abc.net.au, Guest-booking information unauthorised access (Travel technology) (2026-04-13). https://www.abc.net.au/news/2026-04-13/booking-com-data-security-breach-personal-details/106557630. Verified on 2026-11-22.

S48: UK NCSC, AIVD and MIVD, China-nexus covert-network advisory (Cross-sector / national security) (2026-04-23). https://www.ncsc.gov.uk/news/international-cyber-agencies-fresh-advice-defend-against-china-linked-covert-networks. Verified on 2026-11-22.

S49: uva.nl, Supplier data theft and precautionary shutdown (Higher education / education technology) (2026-05-07). https://www.uva.nl/content/nieuws/nieuwsberichten/2026/05/stand-van-zaken-datalek-bij-leverancier-canvas.html. Verified on 2026-11-22.

S50: nos.nl, Supplier data theft and precautionary shutdown (Higher education / education technology) (2026-05-08). https://nos.nl/artikel/2613564-universiteiten-en-hogescholen-blokkeren-studie-app-canvas-na-hack. Verified on 2026-11-22.

S51: politie.nl, VPN service disruption (Criminal infrastructure). https://www.politie.nl/nieuws/2026/mei/21/criminele-vpn-dienst-first-vpn-offline-gehaald.html. Verified on 2026-11-22.

S52: politie.nl, Botnet disruption (Hosting / connected devices). https://www.politie.nl/nieuws/2026/mei/28/06-politie-en-ncsc-halen-groot-botnetwerk-offline.html. Verified on 2026-11-22.

S53: hospecs.com, Guest-data exposure / targeted payment phishing investigation (Hospitality). https://www.hospecs.com/ (article URL withheld). Verified on 2026-11-22.

S54: nos.nl, Guest-data exposure / targeted payment phishing investigation (Hospitality) (2026-06-02). https://nos.nl/ (article URL withheld). Verified on 2026-11-22.

S55: politie.nl, Malware distribution campaign / international disruption (Cross-sector web ecosystem). https://www.politie.nl/nieuws/2026/juni/18/11-politie-en-om-openen-de-jacht-op-beruchte-malwaregroep-socgholish.html. Verified on 2026-11-22.

S56: politie.nl, Infostealer disruption / credential recovery (Cross-sector). https://www.politie.nl/nieuws/2026/juni/24/11-operatie-endgame-opnieuw-twee-infostealers-offline.html. Verified on 2026-11-22.

S57: aivd.nl, Messaging backup recovery-key phishing (Government / defence / media) (2026-06-30). https://www.aivd.nl/actueel/nieuws/2026/06/30/russische-hackers-richten-zich-op-signal-backups-via-nieuwe-phishing-methode. Verified on 2026-11-22.

S58: aivd.nl, IP-camera espionage campaign (Logistics / private connected infrastructure) (2026-07-10). https://www.aivd.nl/actueel/nieuws/2026/07/10/nederland-doelwit-van-russische-spionageoperatie-via-ip-cameras. Verified on 2026-11-22.

S59: aivd.nl, Zimbra espionage advisory (Foreign defence / ICT) (2026-07-23). https://www.aivd.nl/actueel/nieuws/2026/07/23/russische-hackersgroep-laundry-bear-hackt-zimbra-mailservers. Verified on 2026-11-22.

S60: autoriteitpersoonsgegevens.nl, Active exploitation and personal-data breach wave (Cross-sector websites). https://autoriteitpersoonsgegevens.nl/actueel/advies-van-de-ap-aan-wordpress-gebruikers-die-getroffen-zijn-door-datalek. Verified on 2026-11-22.

S61: aivd.nl, CHOSEN BRICK targeted malware campaign (Civil society / media / individuals) (2026-09-15). https://www.aivd.nl/actueel/nieuws/2026/09/15/cyberactoren-uit-iran-zetten-malware-in-tegen-dissidenten-activisten-en-journalisten. Verified on 2026-11-22.

S62: aivd.nl, China-nexus edge-device espionage advisory (Cross-sector) (2026-10-07). https://www.aivd.nl/actueel/nieuws/2026/10/07/mivd-en-aivd-verwachten-toename-chinese-cyberaanvallen-via-edge-devices. Verified on 2026-11-22.

S63: ncsc.nl, Multiple cyberincidents / relationship assessment (Food supply). https://www.ncsc.nl/nieuws/in-het-nieuws-cyberaanvallen-op-levensmiddelensector. Verified on 2026-11-22.

S64: cityam.com, Reported internal-folder unauthorised access / actor claim (Air transport) (2026-10-12). https://www.cityam.com/ (article URL withheld). Verified on 2026-11-22.

S65: politie.nl, International enforcement action (Hosting / criminal infrastructure). https://www.politie.nl/nieuws/2026/oktober/28/03-internationale-actie-tegen-bulletproof-hoster.html. Verified on 2026-11-22.

S66: ncsc.nl, Cooling-system cyberattacks (Retail / food / operational technology). https://www.ncsc.nl/nieuws/in-het-nieuws-cyberaanvallen-op-koelinstallaties-in-europa. Verified on 2026-11-22.

S67: aa.com.tr, Cooling-system cyberattacks (Retail / food / operational technology) (2026-11-02). https://www.aa.com.tr/ (article URL withheld). Verified on 2026-11-22.

S68: allunited.nl, Database data theft / interface disruption (Sports membership SaaS / associations). https://www.allunited.nl/artikelen/datalek/. Verified on 2026-11-22.

S69: nu.nl, Database data theft / interface disruption (Sports membership SaaS / associations) (2026-11-11). https://www.nu.nl/tech/6416219/meer-dan-350-sportclubs-melden-datalek-na-cyberaanval-op-allunited.html. Verified on 2026-11-22.

S70: politie.nl, Warning against criminal online markets (Public prevention). https://www.politie.nl/nieuws/2026/november/9/08-ben-jij-zichtbaar-op-een-verdacht-online-platform-november-2026.html. Verified on 2026-11-22.

S71: politie.nl, Operation Endgame disruption (Cross-sector / hosting). https://www.politie.nl/nieuws/2026/november/12/11-internationale-actie-maakt-netwerken-van-cybercriminelen-onschadelijk.html. Verified on 2026-11-22.

S72: politie.nl, Operation Endgame disruption (Cross-sector / hosting). https://www.politie.nl/en/news/2026/november/international-action-disables-cybercriminal-network.html. Verified on 2026-11-22.

S73: ncsc.nl, Service outage (Cloud productivity / digital supply chain). https://www.ncsc.nl/nieuws/in-het-nieuws-storing-microsoft-exchange-online. Verified on 2026-11-22.

S74: support.optimizely.com, Third-party JavaScript injection (Web experimentation SaaS / cross-sector). https://support.optimizely.com/hc/en-us/articles/50521849710605. Verified on 2026-11-22.

S75: politie.nl, Customer-data theft and subsequent attempted violence (Banking / personal safety). https://www.politie.nl/nieuws/2026/november/19/06-onderzoek-naar-datadiefstal-bij-bank-revolut.html. Verified on 2026-11-22.

S76: nos.nl, Customer-data theft and subsequent attempted violence (Banking / personal safety) (2026-11-19). https://nos.nl/artikel/2640151-verdachten-opgepakt-die-geweld-wilden-plegen-bij-klanten-van-revolut-na-datadiefstal. Verified on 2026-11-22.

S77: politie.nl, Fake-shop awareness campaign (Consumer e-commerce / prevention). https://www.politie.nl/nieuws/2026/november/21/00-oeps%E2%80%A6-je-trapte-er-bijna-in-nieuwe-nepwebsite-van-de-politie.html. Verified on 2026-11-22.

S78: politie.nl, Ticket-fraud awareness campaign (Consumer fraud prevention). https://www.politie.nl/nieuws/2026/januari/15/politie-waarschuwt-met-nepwebsite-voor-ticketfraude.html. Verified on 2026-11-22.

S79: politie.nl, Phishing/extortion email warning (Consumer / public-sector impersonation). https://www.politie.nl/nieuws/2026/januari/23/pas-op-voor-phishingmail-over-kinderporno.html. Verified on 2026-11-22.

S80: ncsc.nl, Chinese botnet historical advisory (Connected devices). https://www.ncsc.nl/nieuws/nederlandse-apparaten-onderdeel-van-chinees-botnet. Verified on 2026-11-22.

S81: ncsc.nl, DDoS campaign historical advisory (Cross-sector). https://www.ncsc.nl/nieuws/lopende-ddos-aanvallen-op-nederlandse-organisaties. Verified on 2026-11-22.

S82: ncsc.nl, DDoS historical advisory (Public administration / transport context). https://www.ncsc.nl/nieuws/opnieuw-ddos-aanvallen-rondom-navo-top-vervoerssector-ook-doelwit. Verified on 2026-11-22.

S83: ncsc.nl, Ransomware historical advisory (Cross-sector). https://www.ncsc.nl/nieuws/ook-nederlandse-bedrijven-slachtoffer-van-ransomwaregroepering-cactus. Verified on 2026-11-22.

S84: NCTV, Cyberbeveiligingswet significant-incident reporting. https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/meldplicht. Verified on 2026-11-22.

S85: RFC Editor, DMARC protocol reference. https://www.rfc-editor.org/rfc/rfc7489.html. Verified on 2026-11-22.

S86: RFC Editor, DKIM signatures. https://www.rfc-editor.org/rfc/rfc6376.html. Verified on 2026-11-22.

S87: RFC Editor, Sender Policy Framework. https://www.rfc-editor.org/rfc/rfc7208.html. Verified on 2026-11-22.

S88: RFC Editor, HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html. Verified on 2026-11-22.

S89: politie.nl, International forum takedown (Criminal market infrastructure). https://www.politie.nl/nieuws/2026/maart/4/politie-ontmantelt-groot-cybercrimineel-forum-in-wereldwijde-actie.html. Verified on 2026-11-22.

S90: Rijksoverheid, Annual-report retrospective (Cross-sector / national security). https://www.rijksoverheid.nl/documenten/2026/04/22/openbaarjaarverslagmivd2025. Verified on 2026-11-22.

S91: aivd.nl, Annual-report retrospective (Cross-sector / national security) (2026-04-23). https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025. Verified on 2026-11-22.

S94: nos.nl, Reported supplier-related personal-data exposure (Entertainment / hospitality marketing / research hosting) (2026-11-12). https://nos.nl/ (article URL withheld). Verified on 2026-11-22.

S95: AIVD, UK NCSC and FBI, CHOSEN BRICK joint campaign advisory (2026-09-15). https://www.ncsc.gov.uk/sites/default/files/2026-09/Advisory-Iranian-Cyber-Targeting-of-Dissidents-Activists-and-journalists.pdf. Verified on 2026-11-22.

S96: tweedekamer.nl, Recurring DDoS availability disruption (Digital government / authentication) (2026-10-07). https://www.tweedekamer.nl/downloads/document?id=2026D49475. Verified on 2026-11-22.

S97: ad.nl, Recurring DDoS availability disruption (Digital government / authentication) (2026-10-30). https://www.ad.nl/binnenland/storing-na-ddos-aanval-bij-online-diensten-digid-weer-opgelost~a1a03520/. Verified on 2026-11-22.

S98: rdi.nl, GPS signal disruption under investigation (Aviation / radio navigation) (2026-11-16). https://www.rdi.nl/actueel/nieuws/2026/11/16/rdi-start-onderzoek-naar-storing-gps-vliegtuigen. Verified on 2026-11-22.

S100: gcaptain.com, Historical DDoS story republished in 2026 (Ports / maritime) (2023-06-14). https://gcaptain.com/ (article URL withheld). Verified on 2026-11-22.

S101: dustingroup.com, Supplier internal-system breach; unverified customer-specific claims (IT reseller / managed services / supplier chain). https://www.dustingroup.com/en/information. Verified on 2026-11-22.

S102: dutchitleaders.nl, Supplier internal-system breach; unverified customer-specific claims (IT reseller / managed services / supplier chain). https://www.dutchitleaders.nl/ (article URL withheld). Verified on 2026-11-22.

S103: interrail.com, Customer-data breach disclosed in 2026; 2025 exfiltration (Travel / rail-pass services) (2026-02-13). https://www.interrail.com/en-int/ni/data-security-incident. Verified on 2026-11-22.

S104: bleepingcomputer.com, Customer-data breach disclosed in 2026; 2025 exfiltration (Travel / rail-pass services). https://www.bleepingcomputer.com/news/security/eurail-says-december-data-breach-impacts-300-000-individuals/. Verified on 2026-11-22.

S105: interrail.com, Interrail News: Data security incident announcement (2026-01-10). https://www.interrail.com/en/about-us/press-room/interrail-news. Verified on 2026-11-22.

Appendix D. Glossary

- **AIVD / MIVD:** the Dutch General Intelligence and Security Service and Military Intelligence and Security Service. Attributions in this report remain theirs.
- **AP:** Autoriteit Persoonsgegevens, the Dutch data-protection authority.
- **Rvdr:** Raad voor de rechtspraak, the Council for the Judiciary.
- **NCSC:** the Dutch National Cyber Security Centre; distinct from the UK body with the same abbreviation.
- **NCTV:** the Dutch National Coordinator for Counterterrorism and Security.
- **RDI / ACM:** the Dutch digital-infrastructure inspectorate and competition/consumer authority; their investigation remits are kept distinct.
- **DNB:** De Nederlandsche Bank. Its bank register differs from this report's selected finance-domain cell.
- **Cbw:** Cyberbeveiligingswet, the Dutch cyber-security law discussed in Chapter 10.
- **CSIRT:** computer security incident response team; identify the designated team for the applicable reporting regime.
- **GDPR / controller / processor:** European personal-data rules; the controller determines processing purposes and means, while the processor acts for the controller.
- **DORA:** the EU Digital Operational Resilience Act for in-scope financial entities; its reporting stages differ from privacy reporting.
- **National Atlas headline:** a single exposure summary for the selected portfolio, not national prevalence or an intrusion probability.
- **Blackhole / Ransompedia / Atlas:** Brandefense data and product names. Posts, ransomware listings and exposure ratings are distinct concepts; Only the national Atlas headline is published in this edition.
- **Credential combination / stealer log:** respectively a file advertised as login pairs and information associated with information-stealing malware. File labels alone do not establish provenance or validity.
- **MFA / session / linked device:** respectively an additional sign-in factor, continuing authenticated access and another device connected to an account. Recovery and revocation decisions must address the relevant access.
- **KYC:** know-your-customer identity checks. A claimed bypass is not evidence of successful account opening.
- **RDWEB / EPMM:** remote-desktop web access and Endpoint Manager Mobile; product descriptions do not establish a target's actual configuration.
- **SaaS / tenant:** software delivered as a service and a customer's distinct service environment.
- **DDoS:** distributed denial of service. An availability attack does not itself establish data theft.
- **OT:** operational technology controlling a physical process. Camera viewing and a credential advertisement are not automatically industrial-control access.
- **DMARC / SPF / DKIM:** mail-domain policy, sending-host authorisation and message signing. Published settings are not measured delivery or fraud outcomes.

- **TLS / HSTS:** encrypted-connection technology and a browser HTTPS policy; each observation is bounded to its relevant endpoint or homepage.
- **DNSSEC / DS:** signed DNS and a delegation record. DS presence alone does not establish full validation.
- **CVE:** a vulnerability identifier, distinct from evidence that the vulnerability was exploited at a particular organisation.
- **Post card / claim / confirmed incident:** a redacted evidence excerpt, an assertion and an event established by the relevant organisation or authority. Their evidential roles differ.
- **TLP:CLEAR:** shareable without a TLP restriction; privacy, contractual and other applicable obligations still matter.

About this report

Prepared by Odin by Brandefense. Version 1.0 uses a research cutoff snapshot on 22 November 2026 and a recent-activity window beginning 8 November. Public notices can describe earlier incidents; those dates remain explicit. The report prioritises bounded evidence and distinguishes criminal claims from events established by organisations or authorities.

This is not a national census, a legal determination or assurance about any organisation's complete security state. Recommendations describe actions a reader can consider; they do not establish that a named organisation omitted those controls. A Dutch-language edition accompanies the English master; the English edition prevails where they differ.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS

4.7 / 5

COVERAGE

3 pillars

CTI, DRPS, EASM

MONITORING

24 / 7

Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO