BRANDEFENSE COUNTRY REPORT · FINLAND 2026

Brandefense Finland Cyber Threat Landscape Report 2026

Edge zero-days, supplier exposure and identity abuse across Finland's connected services

Odin by Brandefense
Research window: 1 January to 22 November 2026 (UTC; recent highlight 8 to 22 November)
Version 1.0 · Public Research Edition · TLP:CLEAR · 24 November 2026

41 of 248
assessed Finnish domains had a credential listed for sale when checked

7
documented underground claim cases across 2026

16
Finland-labelled ransomware listings across 8 claimant labels

7 of 25
selected Finnish finance domains had a current credential listing

CONTENTS

Contents

01	Executive brief and defender priorities	05
	Report map	09
02	National digital profile and 2026 landscape	10
03	National exposure and selected-domain observations	16
04	Underground claims and cases	27
05	Public incidents, suppliers and recent activity	37
06	Disruption, hacktivism and claim versus reality	48
07	Ransomware, espionage advisories and threat profiles	52
08	Fraud, identity abuse and secondary harm	61
09	Banking, strong authentication and payment continuity	68
10	Regulation, reporting clocks and national response	73
11	Outlook and conditional planning scenarios	78
12	Action plan and completion evidence	82
A	Appendix A. Method, scope and exclusions	89
B	Appendix B. Evidence register	92
C	Appendix C. Sources	93
D	Appendix D. Glossary	98
	About this report	99

Board and executives	01 05 10 11 12
CISO and service owners	03 04 05 10 12
SOC and threat intelligence	02 04 06 07 12
Fraud and banking operations	05 08 09 12
Privacy, legal and communications	05 06 10 12

About this edition

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

45/100

National Atlas headline across 248 assessed Finnish domains (24 November 2026 snapshot)

749,602

Finland-tagged underground posts (1 January to 22 November 2026; 96.9% in Jan-Feb)

16

Finland-labelled ransomware listings (1 January to 22 November 2026; 11 in full-year 2025)

EUR 60M

Attempted bank fraud in H1 2026 (20,000 attempts; EUR 28.3M lost)

Contents and reading routes

Chapter	Question
1 Executive brief	Which findings and decisions require leadership action first?
2 National profile	How do digital reliance, official trends and bulk volume shape the picture?
3 National exposure	Which credential, device and mail-policy observations require owner validation?
4 Underground claims	What do advertisements, buyer requests and recycled datasets establish?
5 Public incidents	Which publicly reported events and supplier disclosures affected Finland?
6 Disruption and hacktivism	How do claims compare against official records and service impact?
7 Ransomware and actors	What do ransomware listings and espionage advisories establish?
8 Fraud and identity	How do leaked personal details and underground services fuel fraud?
9 Banking and strong ID	How do attackers target bank-linked identity and payment continuity?
10 Regulation	Which authority, portal, trigger and legal deadline apply in Finland?
11 Outlook	Which conditional triggers should shift defensive posture?
12 Action plan	Who acts, on what timeline and with what completion evidence?
Appendices A–D	Scope, evidence register, sources and definitions

CHAPTER 01

Executive brief and defender priorities

01

THIS CHAPTER ANSWERS

Which 2026 signals require action from Finnish defenders today?

5

core findings grounded in distinct evidence populations

1.1 Five findings for leadership 06

1.2 Four immediate executive decisions 07

1.3 Scope and boundaries of this report 07

CHAPTER 01

Executive brief and defender priorities

IN SHORT

Finland's 2026 cyber landscape is defined by rapid edge-device exploitation, third-party supplier data exposure, surging digital-fraud attempts and widespread identity exposure across leading domains. On the 24 November snapshot across 248 assessed Finnish domains, the national Atlas headline is 45/100, and 41 domains had a credential listed for sale when checked. Raw underground post volume is heavily skewed by early-year bulk promotion. Validate current credential listings, pre-authorise edge isolation, require phishing-resistant authentication and close monitoring-only DMARC gaps.

1.1 Five findings for leadership

- **Edge software zero-days drove major 2026 operational disruptions.** Central-government mobile device management was breached in January via Ivanti EPMM flaws affecting up to 50,000 user records [S7][S32] [S59][S60]. Citrix NetScaler zero-days disclosed on 27 September caused pre-patch intrusions in Finland, prompting NCSC-FI's 1 October severe warning [S13][S14][S61][S62][S80]. In October, Valtori shut down public web interfaces as a precaution before PHP fixes shipped [S15][S34][S63][S64].
- **Supplier and legacy-data exposures multiplied downstream obligations.** Several major 2026 Finnish disclosures stemmed from external booking and learning suppliers [S35][S37][S44]. Two healthcare disclosures in Pirkanmaa involved pre-2016 and 2020-2021 archived records [S39][S40]. Technical recovery at a vendor does not end secondary phishing risk for affected residents.
- **Digital fraud attempts jumped while identity abuse shifted.** Finnish banks logged EUR 148 million in attempted fraud during 2025 and EUR 60 million across 20,000 attempts in the first half of 2026, up from 13,600 attempts a year earlier [S29][S30]. Safe-account scam attempts fell to EUR 3.9 million in H1 2026 (EUR 38.4 million across full-year 2025; different period lengths) [S29][S30]. Meanwhile, criminals shifted toward abusing phished bank credentials to obtain eSIMs and Mobile Certificates [S30]. Underground forums simultaneously advertised Finnish eSIMs, spoofed SMS Sender ID gateways and the SALTA3 live-panel kit targeting five major retail banks operating in Finland [S1].
- **Ransomware listings surpassed 2025 totals but require verification.** Ransompedia recorded 16 Finland-labelled listings through 22 November 2026, exceeding the 11 recorded across all of 2025 and matching Norway's 16 [S2]. Two repeat entries reduce unique claims to at most 14, and three same-day February 0apt listings remain unverified [S2]. External research supplies a general caution about inflated or false early 0apt claims [S54]. Separately, two Finnish organisations (identities withheld) confirmed IT intrusions during summer and autumn 2026 in official notices [S49][S50].

- **Identity exposure and public-sector DMARC gaps require separate owners.** On the 24 November 2026 snapshot across 248 assessed Finnish domains, the national Atlas headline is **45/100**, with **41 domains** showing a credential listed for sale (2 domains remain unknown) [S4]. Those assessed domains also carry at least **128,734 device associations** and **2,245,122 historical credential records** [S4]. Separately, on the 24 November 2026 configuration snapshot, **146 of 250 domains (58.4%)** publish DMARC policies requesting `quarantine` or `reject` (policy category only; §3.5) [S3][S67]. Another **94 (37.6%)** stay in monitoring mode, led by regional administration (18), education (15) and central public administration (13) [S3].

1.2 Four immediate executive decisions

1. **Pre-authorise rapid isolation for internet-facing edge appliances and web services.** The January MDM breach, September NetScaler intrusions and October precautionary PHP shutdown show why defenders need pre-authorised isolation before patches ship [S14][S32][S34]. Management teams should define in advance who can suspend an exposed interface without waiting for board approval.
2. **Validate current credential listings and require phishing-resistant authentication.** Across the portfolio, 41 of 248 assessed domains had a credential listed for sale when checked [S4]. NCSC-FI also reported a 67% monthly rise in Microsoft 365 account takeovers in February alongside Device Code Flow warnings [S6][S7][S9][S11]. Route credential alerts to identity teams immediately, require phishing-resistant MFA and block unnecessary device-code flows [S1].
3. **Move monitoring-only public-facing domains already publishing SPF and DKIM to quarantine or reject DMARC policies.** Migrating the 94 monitoring-only domains in the selected portfolio to full-coverage `quarantine` or `reject` policies reduces direct domain spoofing during active Suomi.fi, tax and delivery phishing waves [S3][S20][S31][S67].
4. **Separate reporting clocks across NIS2, GDPR, CER, DORA and CRA before an event occurs.** Finland's Cybersecurity Act (124/2025), CER Act (310/2025), Data Protection Act, FIN-FSA's FISA DORA regime and EU CRA manufacturer reporting (from 11 September 2026) impose distinct triggers, recipients and deadlines [S21][S22][S23][S26][S74][S75]. Awareness timestamps and major-incident classification timestamps must be logged independently.

1.3 Scope and boundaries of this report

Distinct observation windows and snapshot dates govern this report. The 2026 activity window runs from **1 January to 22 November 2026** (UTC) for underground posts, ransomware listings, 2026 domain mentions and public events. Within that span, **8 to 22 November 2026** is examined separately in §5.3. Rolling 365-day domain mentions span **23 November 2025 to 22 November 2026**, with the 2026 subset (`1 January to 22 November 2026`) reported separately [S4]. Exposure assessments (248 of 250 domains) and passive domain configurations (all 250 domains) reflect a snapshot taken on **24 November 2026** [S3][S4]. All external public sources were verified on **24 November 2026**.

Four regional peers provide comparative context: **Sweden, Norway, Denmark and Estonia**. Sweden, Norway and Denmark share Nordic banking, telecom and industrial supply chains with Finland. Estonia is Finland's Gulf of Finland EU and NATO neighbour, linked by submarine power cables, communications cables and cross-border digital services.

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

Every counting unit stays separate throughout this report. Underground posts, ransomware listings, Brandefense Atlas exposure assessments (248 of 250 domains) and passive observations (250 domains) measure different populations. Bank fraud statistics and official notices remain separate too and are never summed into one attack total.

KEY TAKEAWAYS

01

Edge zero-days, supplier breaches, identity exposure and interactive banking phishing define Finland's 2026 operational risk.

02

Separate raw underground volume from validated Finnish incident and exposure evidence.

03

Triage current credential listings, pre-authorise edge isolation, adopt quarantine or reject DMARC policies and separate statutory reporting paths.

Report map

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

Board and executives	Pre-authorise edge isolation and require completion evidence	01 05 10 11 12
CISO and service owners	Prioritise owned exposures, mail policy and supplier risks	03 04 05 10 12
SOC and threat intelligence	Separate bulk volume, underground claims and advisories	02 04 06 07 12
Fraud and banking operations	Counter bank phishing, strong-ID abuse and secondary harm	05 08 09 12
Privacy, legal and communications	Separate statutory clocks, portals and careful wording	05 06 10 12

The evidence categories are **observation**, **actor claim**, **official notice**, **attributed reporting** and **analyst assessment**. An underground post can be directly observed while its claimed contents remain unverified. A confirmed incident can leave attribution and the full affected population unresolved.

CHAPTER 02

National digital profile and 2026 landscape

02

THIS CHAPTER ANSWERS

How does Finland's digital reliance shape its 2026 threat surface?

98.2%

internet penetration across 5.52 million users in Finland (late 2025)

2.1 High digital integration creates shared dependencies 11

2.2 Official Finnish threat tempo from 2025 into late 2026 11

2.3 Interpreting Finland's underground publication volume 13

CHAPTER 02

National digital profile and 2026 landscape

IN SHORT

Finland combines near-universal internet use, bank-linked strong electronic identification and concentrated public ICT platforms with deep Nordic and Baltic infrastructure ties. Official 2025-2026 reports show elevated fraud, website intrusions using ClickFix and rising vulnerability counts that NCSC-FI links to AI-based discovery. Underground totals are heavily skewed by early-year volume. Filter raw underground feeds by platform and verified disclosures before setting defensive priorities.

2.1 High digital integration creates shared dependencies

DataReportal recorded **5.52 million internet users** in Finland in late 2025, representing **98.2% online penetration** [S58]. Public services rely heavily on Suomi.fi messaging and strong electronic identification mediated primarily through Finnish retail bank credentials and telecom Mobile Certificates [S30][S31].

Shared infrastructure concentrates both efficiency and operational risk. Valtori provides core ICT and mobile-device management services across central-government ministries and agencies [S32][S34]. Municipal library consortia share open-source Koha installations [S41][S42], while retailers and airlines depend on specialised cross-border software suppliers [S35][S48].

Strategic assessments published in 2026 underline this exposure in measured terms. In March 2026, the Finnish Security and Intelligence Service (Supo) identified Russia as the most significant intelligence threat to Finland and noted growing artificial-intelligence challenges [S55]. Supo also called for national cloud solutions so that critical systems do not depend on other states [S55]. In November 2026, the updated National Risk Assessment (Kansallinen riskiarvio 2026) highlighted cyber risks to public services, infrastructure and data centres [S18][S56]. Its official briefing also noted faster AI-assisted attack and defence cycles [S56].

Physical subsea infrastructure in the Gulf of Finland and Baltic Sea remains part of the broader resilience backdrop. In August 2026, the Helsinki Court of Appeal overturned a District Court dismissal in the Eagle S case. The court ruled that Finnish courts hold jurisdiction to hear criminal charges regarding December 2024 subsea cable damage [S57]. That ruling is a 2026 judicial milestone concerning a 2024 maritime event rather than a 2026 cyber intrusion, and criminal proceedings remain ongoing [S57].

2.2 Official Finnish threat tempo from 2025 into late 2026

Traficom's National Cyber Security Centre Finland (NCSC-FI) provides the clearest national baseline. In its full-year 2025 review, NCSC-FI recorded **20,890 cyber incident notifications** (excluding 225,031 automated system notifications), led by **16,729 fraud and phishing reports** (up 20% year on year) [S5]. NCSC-FI logged **14 ransomware reports** in 2025, down from 21 in 2024 and below the typical annual average of roughly 40 [S5]. NCSC-FI noted that voluntary reporting omits some private cases and that Akira remained the most common family [S5]. Reported denial-of-service notifications fell roughly 9% in 2025 (reporting is voluntary), whereas other malware notifications rose about 28% [S5].

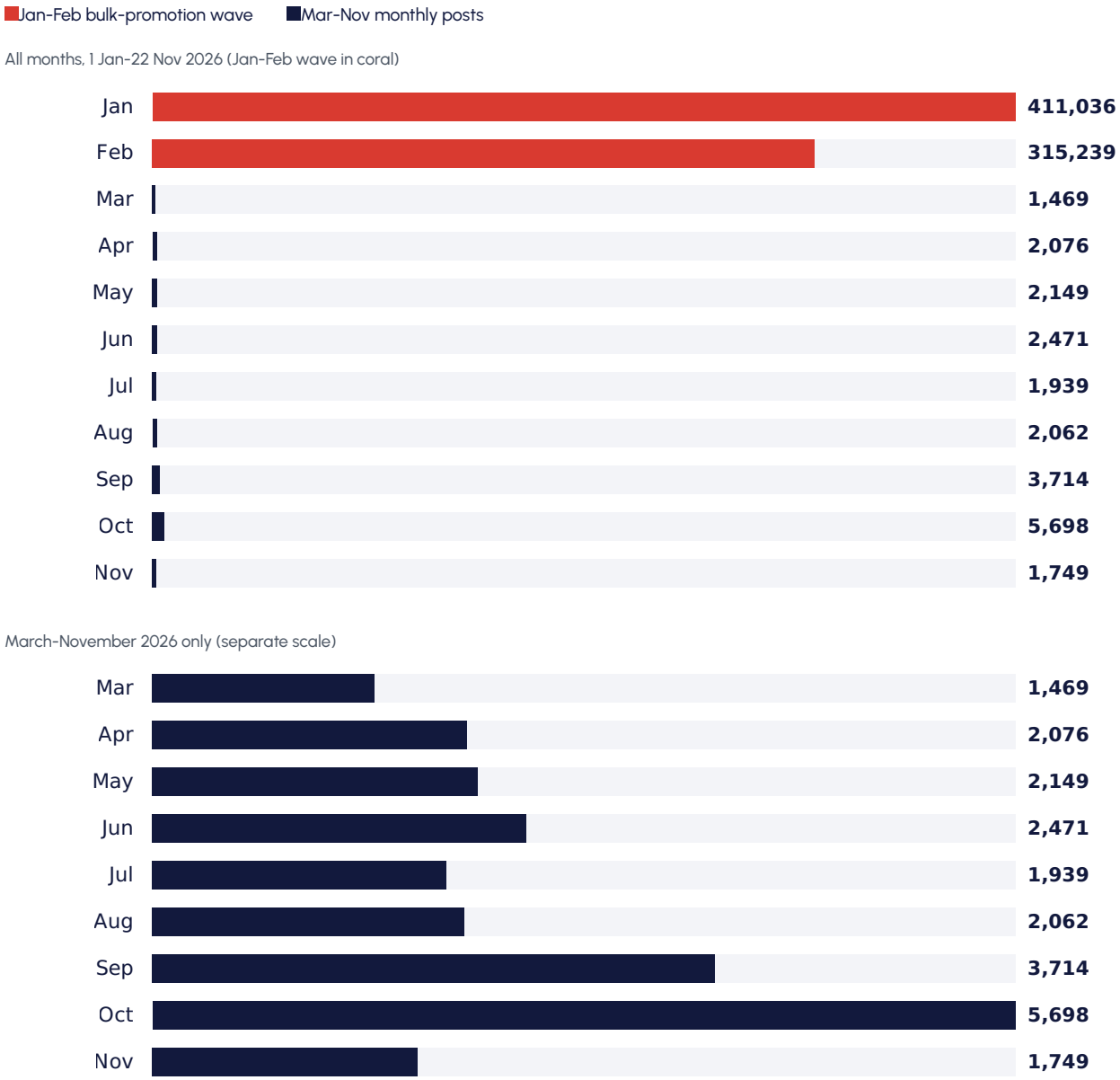
Monthly 2026 NCSC-FI Cyber Weather (Kybersää) bulletins and the June half-year review show a steady, elevated baseline marked by four distinct technical shifts [S6][S7][S9][S11][S17]:

2026 period	Official NCSC-FI observations	Defensive focus
Jan-Feb 2026	Major public-sector zero-day MDM breach (Ivanti EPMM); 1,332 cases handled in February; M365 account takeovers jumped 67% month on month [S7]	Edge-appliance isolation, conditional access and adversary-in-the-middle (AiTM) defence
Mar-May 2026	Whats-App corporate BEC lures; over 100 `.fi` domains removed for false registrant data; mandatory SMS Sender ID licensing deadline 4 May; vulnerability advisories up 50% YoY (15 vs 10 by early June); Device Code Flow phishing [S8] [S9]	Protected SMS Sender IDs, Device Code Flow blocking and rapid patching
Jun-Jul 2026	Global FortiBleed campaign with limited local effect; summer CEO-fraud warnings; 1,012 cases in July (below 1,458 12-month average) but renewed ransomware uptick; WordPress `wp2shell` exploitation begins; two joint intelligence warnings on Russian espionage [S10] [S11]	Summer payment controls, WordPress hardening and edge-device review
Aug-Oct 2026	Major wave of Finnish WordPress intrusions delivering ClickFix malware; first severe warning of 2026 on Citrix NetScaler zero-days exploited in Finland; critical PHP flaws triggering Valtori precautionary DMZ closure [S12][S13][S14] [S15][S17]	CMS patching, ClickFix script blocking and emergency edge playbooks
Nov 2026 (to 22nd)	European grocery refrigeration OT attacks reach Finland (proactive NCSC-FI owner outreach started 13 Oct); bank-spoofing robocalls; Black Friday phishing; residential-proxy abuse of home routers [S16][S18][S19][S20]	OT internet removal, consumer scam alerts and home-router hygiene

NCSC-FI attributed this year's rise in serious vulnerabilities especially to AI-based vulnerability hunting [S11].

2.3 Interpreting Finland's underground publication volume

January and February bulk promotion dominates raw Finland-tagged post volume

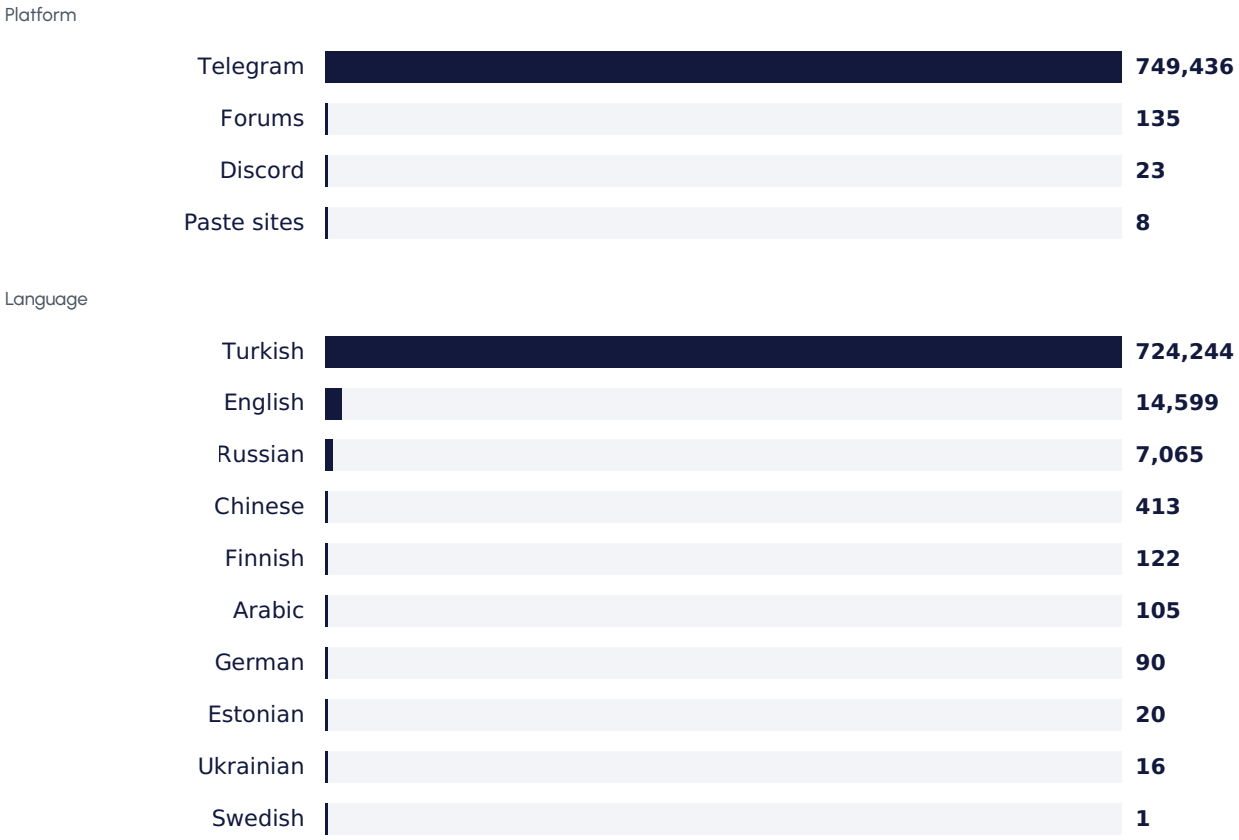


Source: Odin by Brandefense, Finland-tagged underground posts, 1 January-22 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

Between 1 January and 22 November 2026, Odin by Brandefense observed **749,602 Finland-tagged posts** across monitored underground venues [S1]. Monthly counts show extreme concentration: **411,036 posts in January** and **315,239 in February**, totalling **726,275 posts (96.9%)** in the first two months alone [S1]. Within those 726,275 January-February posts, **726,240** appeared on Telegram and **723,961** carried Turkish language tags [S1]. March through November together account for **23,327 posts**, ranging between **1,469 in March** and **5,698 in October**, with **1,749 in partial November** (through 22 November) [S1].

622 of 627 January-February posts in one review were repetitive Turkish-language commercial promotions on Telegram rather than targeted Finnish cybercrime [S1]. Likewise, the October peak of 5,698 posts is heavily inflated by multi-country cloud-VPS resellers and mobile-gaming account trading chats [S1].

Telegram and Turkish-language bulk templates dominate raw Finland-tagged posts



Source: Odin by Brandefense, Finland-tagged underground posts, 1 January-22 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

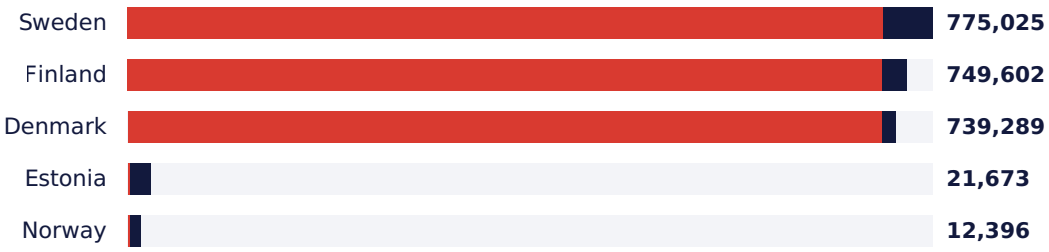
Platform and language splits confirm this distortion [S1]:

- **Platforms (exact sum 749,602):** Telegram accounts for **749,436 posts (99.98%)**, forums **135**, Discord **23**, paste sites **8** and Tor hidden services **0** [S1].
- **Languages (tags may overlap):** Turkish leads with **724,244** tagged posts, followed by English (**14,599**), Russian (**7,065**), Chinese (**413**), Finnish (**122**), Arabic (**105**), German (**90**), Estonian (**20**), Ukrainian (**16**) and Swedish (**1**) [S1].

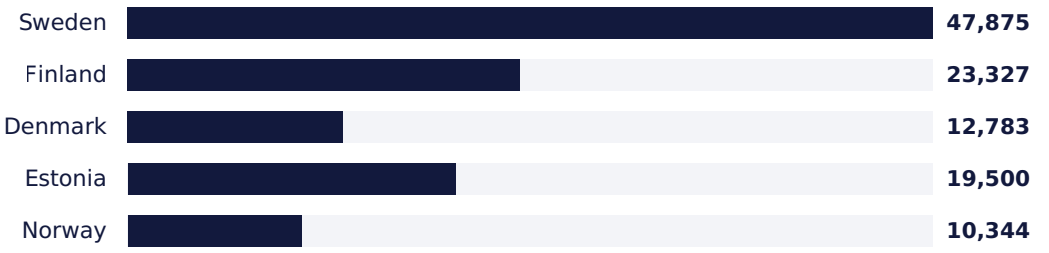
Sweden, Finland and Denmark absorbed the same January-February bulk wave



1 Jan-22 Nov 2026 total (Jan-Feb in coral, Mar-Nov in navy)



March-November 2026 only (separate scale)



Country-tagged raw posts across monitored channels; not adjusted for population or source coverage. Source: Odin by Brandefense, Finland-tagged underground posts, 1 January-22 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

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

Regional comparison clarifies the pattern immediately [S1]. **Sweden (775,025)**, **Finland (749,602)** and **Denmark (739,289)** all absorbed the same January-February bulk Telegram promotion wave, whereas **Estonia (21,673)** and **Norway (12,396)** did not [S1]. On forums, where targeted access offers and database claims actually concentrate, Finland logged **135** country-tagged forum posts across the window, below **Estonia (506)**, **Sweden (485)**, **Denmark (179)** and **Norway (144)** [S1]. Sweden figures were recounted on 24 November 2026; the Sweden report gives 775,020 total posts and 484 forum posts (counted 23 November) [S1].

KEY TAKEAWAYS

01

High digital trust and shared platforms magnify supplier and edge-software failures in Finland.

02

January and February account for 96.9% of Finland-tagged posts, dominated by Telegram bulk promotion.

03

Track NCSC-FI advisories, forum claims and confirmed disclosures rather than raw chat volume.

CHAPTER 03

National exposure and selected-domain observations

03

THIS CHAPTER ANSWERS

Which exposure signals and configuration gaps require validation across 250 Finnish domains?

41 of 248

assessed Finnish domains had a credential listed for sale when checked

3.1 Universe card and assessment boundary 17
3.2 National Atlas headline and current credential listings 18
3.3 Infected-device and historical credential-record associations 21
3.4 Documents, similar domain names and 365-day underground mentions 23
3.5 Mail authentication, DNSSEC, TLS and HSTS across 250 Finnish domains 24
3.6 Turning exposure signals into separate validation queues 26

CHAPTER 03

National exposure and selected-domain observations

IN SHORT

On the 24 November 2026 snapshot across 248 assessed Finnish domains, the national Atlas headline is 45/100, and 41 domains had a credential listed for sale. The portfolio carries at least 128,734 infected-device associations and 2,245,122 historical credential records, while 2 domains remain unknown. Separately, 146 of 250 domains (58.4%) publish DMARC policies requesting quarantine or rejection, while 94 stay in monitoring mode. Triage current credential listings first, validate employee devices and move monitoring-only domains to quarantine or reject DMARC policies.

3.1 Universe card and assessment boundary

We assembled a purposive portfolio of **250 DNS-verified Finnish domains** spanning ten equal sector cells of 25 domains each [S3][S4]. Individual domain names remain private to avoid exposing unverified security observations.

Item	Scope
Reference dates	2026 activity window runs 1 January to 22 November 2026; rolling 365-day domain mentions run 23 November 2025 to 22 November 2026; exposure and passive snapshots are dated 24 November 2026; external sources verified 24 November 2026
Portfolio	250 selected Finnish domains across 10 cells of 25 domains each (114 private, 88 municipal/health/education public bodies, 48 state-owned or central government)
Selection	Purposive selection of central ministries, agencies, wellbeing counties, cities, universities, supervised banks, energy, telecom, transport and industrial leaders; not a national census
Unit	One primary domain per organisation; all 250 resolved in DNS on 24 November 2026 [S3]
Exposure snapshot	248 of 250 selected domains assessed on 24 November 2026; 2 domains remain unknown (1 in telecom and digital services, 1 in health and wellbeing services) [S4]
Exposure signals	Cumulative infected-device and employee-device associations, historical credential records, current credential listings, listing history, document associations and 30-day similar-name observations [S4]
Mention context	Rolling 365-day dark-chat and dark-web (Tor) domain mentions across all 250 domains (23 November 2025 to 22 November 2026), with the 1 January to 22 November 2026 subset reported separately [S4]

Item	Scope
Passive snapshot	Public DNS, DMARC, SPF, DKIM, DNSSEC, TLS and HSTS observations across all 250 domains on 24 November 2026 [S3]
Publication boundary	National Atlas headline only (45/100); no per-sector ratings, per-group ratings or organisation scores are published [S4]
Inference limit	Signals can overlap across domains and people; missing observations are not zeros and no count establishes a confirmed breach

Exposure observations and passive configurations answer different questions. A historical credential record can coexist with sound current email controls, while a published `quarantine` or `reject` DMARC policy does not prevent active-account phishing. Keep both views within their stated denominators (`248` assessed domains for exposure; `250` selected domains for configuration and mentions).

3.2 National Atlas headline and current credential listings

41 of 248 assessed Finnish domains (16.5%) had a credential tied to their domain listed for sale when checked [S4]. All 41 also carry a prior listing history, representing **299 historical listing entries** across the portfolio [S4].

The assessed portfolio's national Atlas headline is 45/100 [S4]. Higher values indicate greater observed external exposure on the 0 to 100 scale. Only this single national headline is published. No per-sector ratings, per-group ratings or individual organisation scores appear anywhere in this report.

The headline supports prioritisation across the assessed portfolio. It is not a breach percentage, a probability of future intrusion or a national prevalence estimate. Missing exposure observations for 2 selected domains remain unknown rather than zero.

Current credential listings and exposure signals across 248 assessed Finnish domains

	Current listings	With devices	Employee devices	With credentials	With documents
Public administration	3/25	18/25	11/25	20/25	17/25
Regional and local administration	1/25	24/25	21/25	25/25	18/25
Banking and finance	7/25	18/25	12/25	24/25	17/25
Energy and utilities	2/25	20/25	6/25	24/25	10/25
Telecom and digital services	6/24	20/24	16/24	24/24	18/24
Industry and manufacturing	0/25	21/25	21/25	24/25	21/25
Transport, maritime and logistics	8/25	15/25	8/25	24/25	8/25
Health and wellbeing services	0/24	15/24	13/24	20/24	6/24
Education and research	4/25	23/25	23/25	24/25	20/25
Retail, media and consumer services	10/25	23/25	17/25	25/25	16/25

Current credential listings by sector (coral). Each cell shows observed domains / assessed domains (24 or 25); signals overlap. Source: Brandefense exposure observations for 248 assessed domains out of 250 selected Finnish domains, 24 November 2026 snapshot (2 domains remain unknown) [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector cell	Assessed (of 25)	Current listings	With devices	With employee devices	With credentials	With documents	With 30-day similar names
Public administration	25	3	18	11	20	17	14
Regional and local administration	25	1	24	21	25	18	19
Banking and finance	25	7	18	12	24	17	14
Energy and utilities	25	2	20	6	24	10	11
Telecom and digital services	24	6	20	16	24	18	21
Industry and manufacturing	25	0	21	21	24	21	19
Transport, maritime and logistics	25	8	15	8	24	8	11

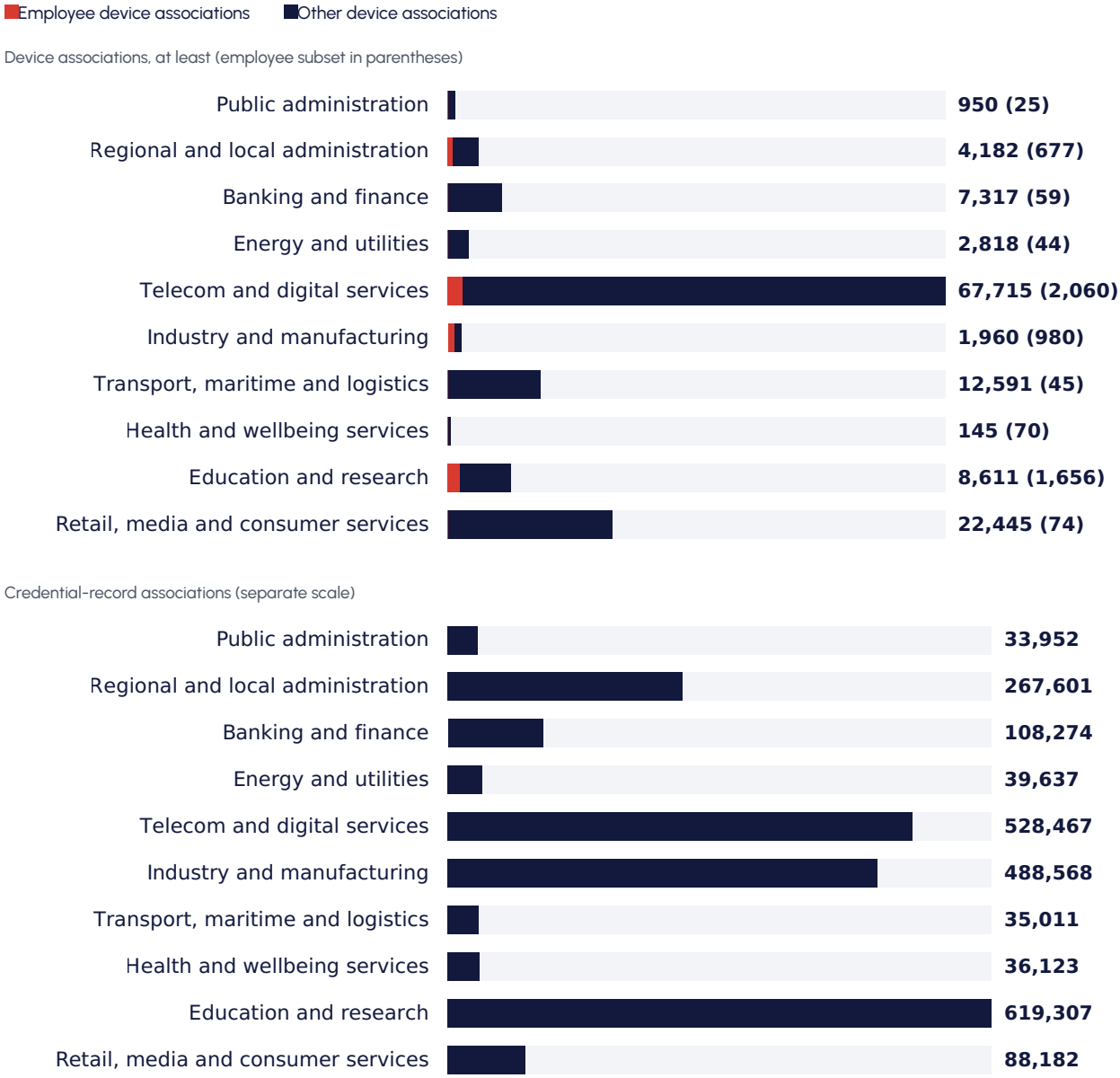
Sector cell	Assessed (of 25)	Current listings	With devices	With employee devices	With credentials	With documents	With 30-day similar names
Health and wellbeing services	24	0	15	13	20	6	9
Education and research	25	4	23	23	24	20	21
Retail, media and consumer services	25	10	23	17	25	16	21
Total (248 of 250)	**248**	**41**	**197**	**148**	**234**	**151**	**160**

Current credential listings concentrate in **retail, media and consumer services (10 of 25)**, **transport, maritime and logistics (8 of 25)**, **banking and finance (7 of 25)** and **telecom and digital services (6 of 24)** [S4]. By contrast, **industry and manufacturing (0 of 25)** and **health and wellbeing services (0 of 24)** showed zero current listings at the snapshot date [S4].

In the sector exposure tables and charts, current credential listings count assessed domains with a credential listed for sale at the snapshot date [S4]. A current listing is the most direct market prompt to check an account. It does not prove a completed sale, a working password or a server-side intrusion. Route every authorised listing alert to identity teams to verify account status, MFA protection and recent sessions.

3.3 Infected-device and historical credential-record associations

Device and credential-record associations concentrate in telecom, retail and education



Source: Brandefense exposure observations for 248 assessed domains out of 250 selected Finnish domains, 24 November 2026 snapshot (2 domains remain unknown) [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector cell	Assessed	Devices, at least	Employee devices	Credential records	Documents	Similar names (30d)
Public administration	25	950	25	33,952	61	1,866
Regional and local administration	25	4,182	677	267,601	166	128

Sector cell	Assessed	Devices, at least	Employee devices	Credential records	Documents	Similar names (30d)
Banking and finance	25	7,317	59	108,274	120	7,362
Energy and utilities	25	2,818	44	39,637	55	725
Telecom and digital services	24	67,715	2,060	528,467	530	544
Industry and manufacturing	25	1,960	980	488,568	640	428
Transport, maritime and logistics	25	12,591	45	35,011	29	750
Health and wellbeing services	24	145	70	36,123	72	55
Education and research	25	8,611	1,656	619,307	718	8,965
Retail, media and consumer services	25	22,445	74	88,182	93	5,855
Total (248 of 250)	**248**	**128,734**	**5,690**	**2,245,122**	**2,484**	**26,678**

Across the 248 assessed domains, **197 domains** carry at least **128,734 infected-device associations**, splitting into **5,690 employee-classified devices (4.4%)** across **148 domains** and **123,044 non-employee device associations (95.6%)** [S4]. Employee-classified devices are a subset of the device total and must never be added to it. Records are cumulative rather than 2026-only [S4].

Four practical patterns guide Finnish defenders [S4]:

- **Consumer-facing services carry most device associations.** Telecom and digital services accounts for at least **67,715** (52.6% of total; 2,060 employee), followed by retail, media and consumer services (**22,445**; 74 employee) and transport, maritime and logistics (**12,591**; 45 employee) [S4]. Most non-employee device records plausibly reflect customer or public devices logging into consumer portals, though device ownership is not established.
- **Employee-classified devices cluster in four sectors.** Telecom (**2,060**), education and research (**1,656** across 23 of 25 domains), industry and manufacturing (**980** across 21 of 25) and regional administration (**677** across 21 of 25) hold **5,373 of 5,690 (94.4%)** [S4]. Because university domains frequently serve both staff and students, asset owners should confirm workforce status before initiating corporate endpoint containment.

- **Historical credential records reach 2,245,122 across 234 domains.** They comprise **1,279,899 breach-database records (57.0%)**, **783,695 combolist entries (34.9%)** and **181,528 stealer-log lines (8.1%)** [S4]. Separately, the associated infected devices hold at least **2,349,971** captured credential lines across all services, not solely the assessed domain [S4].
- **Heavy domains skew sector sums.** Education (**619,307**), telecom (**528,467**), industry (**488,568**) and regional administration (**267,601**) hold **1,903,943 (84.8%)** of all credential records [S4]. Across the portfolio, two domains hold **28.1%** of credential records, and inside telecom two domains hold **90.0%** [S4]. The median assessed domain holds **31** device associations and **1,640** credential records, confirming that individual organisations must rely on their own asset telemetry rather than sector sums [S4].

3.4 Documents, similar domain names and 365-day underground mentions

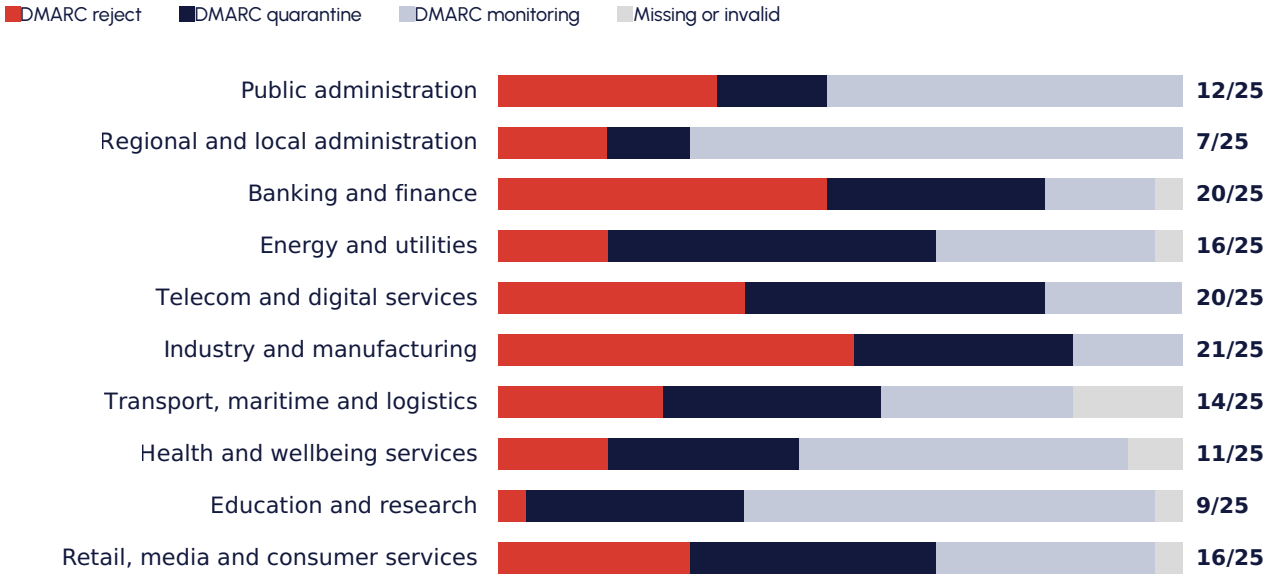
Three contextual signal families complement credential and device triage [S4]:

- **Exposed document associations (248 assessed domains): 151 domains** carry **2,484 document associations**, led by education (**718** across 20 domains), industry (**640** across 21) and telecom (**530** across 18) [S4]. A document association does not establish confidentiality, unlawful acquisition or adversary download; public brochures and recycled files are common explanations.
- **30-day similar-name observations (248 assessed domains): 160 domains** had **26,678** newly observed similar-name registrations in the preceding 30 days, led by education (**8,965**), banking (**7,362**) and retail, media and consumer services (**5,855**) [S4]. Short or common brand strings can match unrelated global domains; treat similar names as triage inputs rather than confirmed phishing infrastructure.
- **Rolling 365-day dark-chat and dark-web mentions (all 250 selected domains, 23 November 2025 to 22 November 2026).** In total, **49 of 250 domains (19.6%)** recorded **941 dark-chat mentions**, led by retail, media and consumer services (**6 domains, 647**), telecom (**10, 167**) and public administration (**13, 82**) [S4]. Separately, **56 of 250 domains (22.4%)** recorded **662 dark-web (Tor) mentions**, led by industry (**6, 194**), public administration (**9, 130**), education (**6, 130**) and telecom (**6, 98**) [S4]. Regional administration showed the widest spread (**14 of 25 domains**, 24 mentions) [S4].

During the 2026 window (`1 Jan-22 Nov`), **29 of 250 domains** generated **207 mentions**, led by retail (**95**), telecom (**67**), public administration (**22**) and education (**13**) [S4]. A domain mention, document match or similar domain name is **not** evidence of a breach. Mentions frequently reflect news mirrors, consumer stealer logs or public references and require asset-owner triage.

3.5 Mail authentication, DNSSEC, TLS and HSTS across 250 Finnish domains

Private industry and banking lead quarantine or reject DMARC policies while public sectors stay in monitoring mode



Source: passive configuration observations for 250 selected Finnish domains, 24 November 2026 snapshot [S3]. Published policies do not establish message-level enforcement or prevented spoofing.

Across the 250 selected Finnish domains (24 November 2026 snapshot), foundational email and web standards are widely deployed, yet policies requesting quarantine or rejection lag sharply in several public-facing sectors [S3]:

Sector cell (25 domains each)	DMARC reject	DMARC quarantine	DMARC monitoring	DMARC missing	SPF	DKIM	DNSSEC DS	Valid TLS	HSTS (of available)
Industry and manufacturing	13	8	4	0	23	24	3	25	17 of 22
Banking and finance	12	8	4	1	24	22	6	24	22 of 24
Telecom and digital services	9	11	5	0	24	24	2	25	22 of 25
Energy and utilities	4	12	8	1	25	25	2	24	17 of 23

Sector cell (25 domains each)	DMARC reject	DMARC quarantine	DMARC monitoring	DMARC missing	SPF	DKIM	DNSSEC DS	Valid TLS	HSTS (of available)
Retail, media and consumer services	7	9	8	1	24	23	4	25	18 of 22
Transport, maritime and logistics	6	8	7	4	25	24	4	25	17 of 21
Public administration	8	4	13	0	24	18	6	25	12 of 13
Health and wellbeing services	4	7	12	2	24	24	1	22	19 of 21
Education and research	1	8	15	1	24	23	0	25	19 of 23
Regional and local administration	4	3	18	0	24	25	3	24	17 of 24
Total (250 domains)	**68**	**78**	**94**	**10**	**241**	**232**	**31**	**244**	**180 of 218**

Three operational conclusions stand out from this snapshot [S3]:

- **The monitoring bottleneck is concentrated in public-facing Finnish institutions.** Overall, **146 of 250 domains (58.4%)** publish DMARC policies requesting quarantine or rejection (`68 reject`, `78 quarantine`), **94 (37.6%)** sit in monitoring mode (`none`), and **10 (4.0%)** have no valid DMARC record [S3][S67]. Four public-facing cells account for **58 of the 94 monitoring-only domains** [S3]. They are regional administration (18), education and research (15, with only 1 on `reject`), central public administration (13) and health and wellbeing services (12) [S3].
- **Technical prerequisites are mostly already in place.** SPF records appear on **241 of 250 domains (96.4%)** and DKIM records on **232 of 250 (92.8%)** [S3][S68][S69]. In regional administration, 24 publish SPF and all 25 publish DKIM while only 7 publish a `quarantine` or `reject` DMARC policy [S3]. Investigating what blocks transition out of monitoring mode on domains already publishing SPF and DKIM is an immediate operational priority.

- **Transport leads missing DMARC while DNSSEC remains niche.** Four of the 10 domains missing DMARC sit in transport, maritime and logistics [S3]. DNSSEC delegation records (`DS`) appear on **31 of 250 domains (12.4%)**, led by public administration (6) and banking (6), with none in education [S3]. Valid TLS appeared on **244 of 250 domains**, with 1 validation failure and 5 unavailable [S3]. HSTS appeared on **180 of 218 domains** with available HTTP responses, while 32 were unavailable (including 12 government portals) [S3][S70].

Configuration observations carry strict boundaries. A published `quarantine` or `reject` DMARC record shows the requested policy category, not guaranteed protection, because DMARC permits partial message sampling and receiver handling varies [S67]. Similarly, a published SPF or DKIM record does not verify alignment, DNSSEC delegation does not confirm chain validation, and unavailable HTTP or TLS results are not misconfigurations [S68][S69].

3.6 Turning exposure signals into separate validation queues

Different external signals belong to different owners and require dated closure evidence rather than blanket incident declarations:

Signal	Accountable owner	First validation check	Completion evidence
Current credential listing	Identity operations	Account existence, active status and MFA protection	Dated account disposition and session review
Employee-device association	Endpoint response and SOC	Managed workforce endpoint and session freshness	Containment, token revocation and endpoint audit
Non-employee device association	Fraud and customer protection	Customer-account abuse indicators and anomalous transfers	Customer protection action or documented closure
Document, similar name or mention	Information and brand owners	Sensitivity, ownership and active deceptive use	Handling decision or takedown request
Monitoring-only DMARC or TLS failure	Messaging and infrastructure	Aligned legitimate senders and certificate chain	Published full-coverage quarantine or reject policy, or fixed certificate

KEY TAKEAWAYS

01

The national Atlas headline is 45/100 across 248 assessed Finnish domains (24 November 2026 snapshot), with 41 showing a current credential listing.

02

Keep current listings, employee devices, non-employee devices and historical credentials in separate validation queues.

03

Moving 94 monitoring-only Finnish domains to full-coverage quarantine or reject DMARC policies remains an immediate, high-impact defensive win.

CHAPTER 04

Underground claims and cases

04

THIS CHAPTER ANSWERS

What are threat actors actually advertising, seeking and recycling around Finland?

7

documented underground claim cases across 2026

4.1 How to read underground claims 28

4.2 Retail, consumer-data and recycling claims 28

4.3 Corporate access demand, banking kits and credential extracts 31

4.4 Telecom, identity-forgery and local mule inputs 34

CHAPTER 04

Underground claims and cases

IN SHORT

Underground forum and chat claims targeting Finland cluster around purported retail CRM exports, recycled residential contact lists, corporate Microsoft 365 access demand, live banking phishing kits, credential extracts, Finnish eSIMs and document forgery. Several posts reuse older date-labelled material without dates, including a 17 November listing sharing matching sample rows with an October 2023-labelled CSV. Treat every underground claim as unverified until validated against internal logs and custodian records.

4.1 How to read underground claims

An underground post establishes one thing with high confidence: someone published those words on that date in that venue. It does **not** verify record authenticity, fresh collection, server-side intrusion, active access or a completed sale. In the seven cases below (`Case A` through `Case G`), all unconfirmed victim and target organisation names are withheld to prevent unverified harm.

4.2 Retail, consumer-data and recycling claims

A

CASE A

Repeated three-table Finnish retail and e-commerce export claims

Retail and e-commerce

Claim unverified

CLAIM	Across February (`B01`), April (`B02`) and the cut-off date 22 November (`B13`), forum posts advertised purported three-table customer and order datasets attributed to Finnish retail and e-commerce brands [S1]. The February and April posts used identical text offering `Contact` , `Order` and `Addre ss` or `Paymentinfo` sections [S1]. The 22 November post listed Salesforce-style `Contact` and `Retail Order` schemas naming an e-commerce platform and a retail tenant [S1].
WHAT IS NOT ESTABLISHED	No official breach confirmation existed at cut-off for any of the named retailers. Shared listing wording across `B01` and `B02` raises the risk of scraped, synthetic or recycled material.

RESPONSE

A retail data custodian receiving an authorised alert should compare advertised column names against live storefront and CRM schemas before issuing customer notices.

Bottom line

Check whether the claimed table schema matches a live CRM or storefront export before issuing customer notices.

Evidence card B01 — 18 Feb 2026

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

ORIGINAL

Offering a dataset originating from [Finnish retailer]. It provides a detailed look at the organization's operations, including Contact, Order, Address. The data is fresh and organized across 3 main sections.

Note. The named retailer is withheld because no official breach confirmation was identified.

Held
A forum seller advertises a purported three-table customer, order and address dataset linked to a Finnish retail chain.

Not established
Authenticity, fresh capture, system access, affected customer count, original provenance or completed transfer.

Evidence card B02 — 4 Apr 2026

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

ORIGINAL

Offering a dataset originating from [Finnish online retailer]. It provides a detailed look at the organization's operations, including Contact, Order, Paymentinfo. The data is fresh and organized across 3 main sections.

Note. Identical listing phrasing across multiple retail claims warrants heightened scepticism until validated by the named custodian.

Held
A seller uses the same three-section listing template to advertise purported customer, order and payment-information tables attributed to a Finnish online retailer.

Not established
Source-system access, payment-card exposure, record authenticity, fresh capture or any completed sale.

Evidence card B13 — 22 Nov 2026

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

ORIGINAL

Source: [e-commerce platform] Tenant: [retail tenant] Tables: 3 Table list: 1. Contact: Customer_External_Id__c, Customer_Full_Name__c, Email, Phone [...] 2. Retail Order

Note. Both named companies are withheld because no official breach confirmation existed at cut-off.

Held
On the 22 November cut-off date, a forum seller advertises a purported three-table CRM customer and retail-order export naming an e-commerce platform and a retail tenant.

Not established
Authenticity, source-system intrusion, record count, current customer exposure or completed sale.

CASE B

B Matching Finnish residential CSV samples across October and November 2026

Claim unverified

Cross-sector consumer data

CLAIM

On 9 October 2026 (`B03`), a forum thread advertised a 15,000-row CSV of purported Finnish names, street addresses, postal codes and `+358` mobile numbers displaying `Year: 2023` [S1]. On 17 November 2026 (`B14`), during the 8 to 22 November window, a second forum advertised the same 15,000-row count and matching sample rows with semicolons while omitting the `Year: 2023` label [S1].

WHAT IS NOT ESTABLISHED

Full files were not obtained, so complete-file identity between `B03` and `B14` is unverified. Neither post establishes a 2026 intrusion, original data provenance or whether the displayed 2023 year label is accurate.

RESPONSE

Security teams should check advertised sample rows against prior historical archives so recycled consumer lists do not trigger unnecessary incident escalation or skewed board metrics.

Bottom line

Compare advertised sample rows against historical archives before treating a November post as a fresh breach.

Evidence card B03 — 9 Oct 2026

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

ORIGINAL

Total count: 15k File type: .csv Year: 2023 Sample FIRST NAME,LAST NAME,ADDRESS,CITY,ZIP,COUNTRY,PHONE [Finnish residential sample rows withheld]

Note. All personal names, street addresses and phone numbers are removed; B14 later posts matching sample rows and the same advertised row count without the Year: 2023 label.

Held

An October forum post advertises a 15,000-row CSV of purported Finnish residential names, postal addresses and mobile numbers displaying the label Year: 2023.

Not established

Original source, actual 2023 collection date, complete-file contents, current accuracy or a 2026 intrusion.

Evidence card B14 — 17 Nov 2026

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

ORIGINAL

Total count: 15k File type: .csv Sample FIRST NAME;LAST NAME;ADDRESS;CITY;ZIP;COUNTRY;PHONE [matching Finnish residential sample rows withheld]

Note. Comparing B14 with B03 shows how matching sample rows and counts reappear without earlier date labels; full files were not obtained or compared.

Held

During the 8 to 22 November window, a second forum advertises a 15,000-row Finnish CSV sharing matching sample rows with B03, using semicolon delimiters and omitting the Year: 2023 label.

Not established

Complete-file identity with B03, original collection year, a new November 2026 breach or fresh collection of Finnish residential records.

4.3 Corporate access demand, banking kits and credential extracts

CASE C

C

Active buyer demand for Finnish corporate Microsoft 365 access for BEC

Demand unverified

Corporate identity and email

CLAIM	On 24 February 2026 (B04), a forum buyer explicitly solicited partners with corporate Office 365 or email access in Finland and Germany for business email fraud [S1].
WHAT IS NOT ESTABLISHED	A recruitment post shows criminal interest rather than confirmed access to any Finnish firm or a link to a specific loss. However, it appeared in February, the month for which NCSC-FI later reported a **67% month-on-month rise** in Microsoft 365 account takeovers [S7]. Finance Finland later reported **EUR 4.9 million** lost to criminals in H1 2026 CEO and invoice fraud, while banks separately prevented or recovered **EUR 0.4 million** [S30].
RESPONSE	Enforce phishing-resistant MFA, block legacy authentication and unnecessary Device Code Flow logins [S9][S11], and monitor mailbox forwarding rules and OAuth app grants.

Bottom line

Audit Microsoft 365 forwarding rules, OAuth consents and anomalous sign-ins and enforce phishing-resistant MFA.

Evidence card B04 — 24 Feb 2026

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

ORIGINAL

Looking for Partners with Traffic / Access office 365 / Email access to Corps / Companies for BEC jobs [...] For Germany / Finland

Note. This is demand evidence published in February, the month for which NCSC-FI later reported a 67% month-on-month rise in Microsoft 365 account takeovers.

Held

A forum buyer actively solicits partners supplying corporate Microsoft 365 or email access in Finland and Germany for business email fraud.

Not established

Successful recruitment, confirmed access to any Finnish organisation, financial loss or a link to any disclosed breach.

CASE D

D ■ Live-panel banking phishing kit customised for Finland in November 2026

Banking and finance

Kit advertised

CLAIM	On 20 and 22 November 2026 (`B15` , shown in §9), a forum vendor advertised the `SALTA3` live-panel phishing kit [S1]. The listing highlighted real-time operator interaction and templates naming five major retail banks operating in Finland [S1].
WHAT IS NOT ESTABLISHED	The advertisement does not establish system intrusion at any named bank or measure active deployment volume in Finland.
RESPONSE	Financial institutions and enterprise fraud teams should evaluate interactive session-interception defences and ensure out-of-band approval prompts clearly state payee, amount and enrolment action (analysed further in §9).

Bottom line

Test real-time session-interception controls and verify that out-of-band approval prompts show clear transaction context.

CASE E

E ■ Targeted Finnish login extracts and bulk combos

Consumer digital services

Claim unverified

CLAIM	Forum posts across 2026 advertised bulk Finland-labelled email-password lists of 10K to 100K lines, such as `B05` on 13 April [S1]. Smaller URL-filtered extracts targeted a Finnish media login portal (`B06` , 100 lines), an online marketplace (53 lines), a consumer service (45 lines) and a banking portal (100 lines) [S1]. A 25 September "Nordic Mix" (`B07`) openly carried a `JANUARY 2024` dump date [S1].
WHAT IS NOT ESTABLISHED	None of these postings confirms server-side intrusion at the referenced organisations. URL-bound extracts typically arise from end-user infostealer logs, and unrelated foreign records frequently appear in domain-labelled forum lists (see §9.2).
RESPONSE	Treat URL-filtered credential lists as probable end-user device theft, apply credential-stuffing rate limits and validate any owned-account alert against current session logs.

Bottom line

Treat URL-filtered login extracts as probable end-user device theft and review credential-stuffing defences.

Evidence card B05 — 13 Apr 2026

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

ORIGINAL

Database: Finland Type: Email : Password Date: [13/ APR/2026] Combo: [12 K++] Line Status: FRESH | HQ

Note. Fresh and HQ are marketing labels routinely attached to recycled credential compilations.

Held
An April forum advertisement promotes a Finland-labelled email-and-password credential list claiming more than 12,000 lines.

Not established
Working passwords, unique individuals, original capture date, fresh breach provenance or completed transfer.

Evidence card B06 — 26 May 2026

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

ORIGINAL

[Finnish media login domain]-100-785 [...] Total Lines: 100 Content Type: URL / Email / Password Combo Date Uploaded: 2026-05-26

Note. URL-bound login extracts typically reflect end-user credential theft on infected devices rather than a breach of the named site.

Held
A May forum upload packages 100 URL, email and password lines filtered for a Finnish media publisher's single-sign-on portal.

Not established
Server-side intrusion at the publisher, current password validity or active account takeover.

Evidence card B07 — 25 Sep 2026

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

ORIGINAL

Download HQ Nordic Mix and Enjoy Using them This Mix Includes: Denmark, Norway, Sweden & Finland [...] Dump Date: JANUARY 2024

Note. Included to show how 2024 material circulates as new forum threads in late 2026.

Held
A September 2026 forum listing distributes a multi-country Nordic credential collection whose own metadata gives a January 2024 dump date.

Not established
Any 2026 breach, working logins, Finnish record share or single-organisation source.

4.4 Telecom, identity-forgery and local mule inputs

CASE F

F

Finnish eSIM profiles, non-VoIP SIM rental and spoofed SMS Sender ID gateways

Claim unverified

Telecommunications and strong ID

CLAIM	On 11 February (B08) and 2 March 2026, a Russian-language forum vendor listed **Finnish eSIM profiles at USD 75** alongside Baltic and European jurisdictions [S1]. Across January, February, April (B09), July and November, additional forum vendors marketed spoofed alphanumeric SMS Sender ID gateways and non-VoIP physical SIM rentals for OTP interception [S1].
WHAT IS NOT ESTABLISHED	Listings do not establish live carrier activation, telecom insider involvement or bypass of Traficom's protected Sender ID regime after 4 May 2026 [S8]. They do, however, align closely with Finance Finland's September 2026 warning on eSIM and Mobile Certificate abuse [S30].
RESPONSE	Register protected Finnish SMS Sender IDs through Traficom and enforce step-up verification on eSIM provisioning and Mobile Certificate issuance.

Bottom line

Register protected Finnish SMS Sender IDs with Traficom and add step-up checks for eSIM and Mobile Certificate issuance.

Evidence card B08 11 Feb 2026

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

ORIGINAL

Актуальные eSim: Lithuania - 70$ Finland - 75$ France - 100$ [...] UK - 70$

TRANSLATION

Current eSIMs: Lithuania USD 70, Finland USD 75, France USD 100, UK USD 70.

Note. Contact handles are removed; Finance Finland warned in September 2026 that fraudsters pair stolen bank logins with eSIMs and Mobile Certificates.

Held

A Russian-language forum vendor advertises Finnish eSIM profiles at an asking price of USD 75 alongside other European jurisdictions.

Not established

Live carrier activation, telecom-operator involvement, stock volume or completed fraud.

Evidence card B09 29 Apr 2026

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

ORIGINAL

Custom Sender ID - Send as ANY company name, brand, or person [...] 70+ Countries supported - Europe, Asia, Americas, Middle East [...] Anonymous Crypto Top-Up

Note. Posted five days before Traficom's 4 May 2026 Finnish SMS Sender ID protection deadline.

Held

A late-April forum advertisement markets spoofed alphanumeric SMS Sender ID delivery across more than 70 countries for cryptocurrency.

Not established

Successful delivery to protected Finnish Sender IDs after Traficom's May 2026 enforcement date or attribution to any specific smishing wave.

CASE G

G ■ Forged Finnish employment paperwork, FI-IBAN accounts and drop recruitment

Claim unverified

Identity, payments and fulfilment

CLAIM	Forum sellers offered custom Finnish payslip and employment-contract templates (`B10` , §8) and USD 25 EU digital Know Your Customer (KYC) selfie packs `[S1]`. Posts also advertised purported FI-prefix IBAN business accounts (`B16` , §9, with buyer demand on 8 November), Finnish pickup drops (`B11` , §8) and nominee company-formation drops including Finland (`B12` , §8) `[S1]`.
WHAT IS NOT ESTABLISHED	None of these posts establishes successful bank onboarding, retailer theft or an active Finnish mule cell.
RESPONSE	Strengthen manual verification of Finnish employment documents, monitor high-value click-and-collect smartphone orders and apply enhanced due diligence on newly incorporated nominee businesses (expanded in §8 and §9).

Bottom line

Strengthen manual document-verification checks and monitor high-value pickup orders and new corporate-account onboarding.

KEY TAKEAWAYS

01

Underground posts establish criminal supply and demand, not confirmed Finnish breaches.

02

Sample comparison flagged a 17 November post sharing matching rows and counts with an earlier 2023-labelled CSV.

03

Match underground fraud inputs directly to Finnish telecom, M365 and banking controls.

CHAPTER 05

Public incidents, suppliers and recent activity

THIS CHAPTER ANSWERS

Which publicly reported events affected Finnish services in 2026, including 8-22 November?

14

public-event dossiers from January through 22 November 2026

5.1 January to July 2026: zero-days, suppliers and legacy archives 38

5.2 August to early November 2026: APIs, edge zero-days and operational technology 41

5.3 Recent activity: 8 to 22 November 2026 45

CHAPTER 05

Public incidents, suppliers and recent activity

IN SHORT

Fourteen public-event dossiers cover confirmed 2026 Finnish and Nordic breaches, a precautionary government web shutdown and one regional press report across government, healthcare, education, libraries, Åland, retail OT and aviation. Four patterns dominate: zero-day edge exploitation, supplier breaches, legacy-file retention failures and unsegmented operational controllers. The 8 to 22 November window brought the Finnair/Amadeus disclosure and Lyko's intrusion. Map third-party dependencies, purge legacy archives and pre-authorise rapid edge isolation.

5.1 January to July 2026: zero-days, suppliers and legacy archives

CASE H

H

Valtori mobile-device-management zero-day breach

Central government ICT

Confirmed zero-day

CHRONOLOGY	On 30 January 2026, Finland's Government ICT Centre Valtori detected an intrusion into its mobile-device-management service exploiting Ivanti Endpoint Manager Mobile zero-day flaws (`CVE-2026-1281` and `CVE-2026-1340`, published 29 January 2026) [S7][S32][S59][S60]. Initial estimates on 3 February cited 20,000 devices; on 5 February, Valtori expanded scope to up to **50,000 central-government ICT user records** across ministries [S32]. Later Yle/STT reporting on **7 May 2026** stated that document disclosures also confirmed affected devices across additional central-government organisations [S33].
EXPOSED INFORMATION AND SCOPE	Investigators found the software marked old records as deleted instead of purging them [S32]. Affected data included names, work emails, phone numbers and device details, while data stored on handsets was not reported affected [S32]. Press reporting stated that the National Bureau of Investigation (KRP) is investigating the incident [S33]. Affected EPMM versions, resolved releases and vendor RPM packages are listed in §12.2 [S59][S60][S81][S82].
RESPONSE	Upgrade to a resolved EPMM release or apply the applicable vendor RPM package per §12.2, review true-deletion behaviour inside MDM tools and isolate internet-facing management consoles immediately upon critical advisory release.

Bottom line

Audit soft-deleted lifecycle retention in management tools and isolate vulnerable edge consoles immediately upon advisory.

CASE I

I Aalto EE and Aalto University: Instructure Canvas supplier breach

Confirmed notices

Executive and higher education

CHRONOLOGY

Between 25 and 29 April 2026, an external actor gained unauthorised access to Instructure's Canvas learning platform during a widely reported global breach [S37][S84]. Instructure confirmed on 6 May that Aalto EE's licensed Canvas environment was affected, and Aalto EE published its formal breach notice and notified the Data Protection Ombudsman on **7 May 2026** [S37]. Separately, on **11 May 2026**, Aalto University published a precautionary notice stating it had no institutional Canvas licence, while noting that individual staff or students might have used Canvas independently [S38].

POTENTIALLY EXPOSED INFORMATION

Aalto EE reported that for its Canvas users, names, email addresses, Canvas register IDs and private Canvas inbox messages may have been exposed [S37]. Aalto EE reported no indication that passwords, financial data or government ID numbers were involved [S37].

RESPONSE

Map which organisational units use shared SaaS platforms independently of central IT and warn affected learners about targeted phishing referencing genuine course messages.

Bottom line

Map which institutional tenants share a SaaS platform and warn affected users against message-context phishing.

CASE J

J Kolmostien Terveys legacy-file breach and Pirkanmaa USB incident

Official releases

Health and wellbeing services

CHRONOLOGY

On 25 August 2026, the Wellbeing Services County of Pirkanmaa (Pirkanmaan hyvinvointialue) and Pihlajalinna disclosed a 24 July intrusion into a legacy file from February 2016 or earlier belonging to joint venture Kolmostien Terveys [S39][S83]. Earlier, on 13 January 2026, Pirkanmaa disclosed a separate physical breach after a healthcare worker found a USB drive inside a flea-market laptop bag [S40].

EXPOSED INFORMATION	The Kolmostien Terveys file contained **10,263 Finnish personal identity codes** (without patient names attached) and next-of-kin phone numbers affecting roughly 12,000 people, while active patient records remained unaffected [S39]. The USB drive contained 2020-2021 Akaa and Urjala infectious-disease isolation decisions [S40].
RESPONSE	Audit and purge decommissioned municipal handover archives created during Finland's 2023 wellbeing-county transition and enforce hardware encryption on all removable storage.

Bottom line

Inventory and purge decommissioned municipal transfer files and enforce encryption on all removable media.

CASE K

K

Confirmed July intrusion at a Finnish financial and business-services firm (identity withheld)

Confirmed notice

Financial and business services

ESTABLISHED ACCOUNT	In July 2026, a Finnish financial and business-services firm published an official notice confirming an intrusion into its internal IT environment [S49]. The company notified NCSC-FI, the Data Protection Ombudsman and police on the day of detection, reported short-term disruptions and potential file-system access, and noted no major customer impact known at the time [S49]. Its identity and notice URL are withheld because wide national or regional press coverage remained limited [S49].
RESPONSE	Keep shared corporate file servers strictly segmented from core client-production platforms and test clean restoration from immutable backups.

Bottom line

Separate shared file servers from core client-production platforms and verify backup restoration independently.

5.2 August to early November 2026: APIs, edge zero-days and operational technology

L

CASE L

Ryde Nordic consumer-data breach affecting Finland

Consumer mobility services

Confirmed breach

ESTABLISHED ACCOUNT	On 2 August 2026 (updated 5 August), Nordic micromobility operator Ryde confirmed unauthorised copying of customer data [S46]. The breach affected all account holders across Norway, Sweden, Finland and Germany, and Ryde notified Norway's data authority [S46]. The controller's notice did not publish a Finland-only user count [S46].
RESPONSE	Treat regional consumer breaches as local phishing triggers even when the controller is headquartered in a neighbouring Nordic country.

Bottom line

Prepare customer guidance for cross-border account breaches where Finnish residents hold active app profiles.

M

CASE M

Rahaliike Holmasto customer-register API breach

Specialist retail

Confirmed breach

ESTABLISHED ACCOUNT	On 30 August 2026, Helsinki numismatics dealer Rahaliike Holmasto suffered an automated extraction via a customer-search API flaw [S43]. Roughly **70% of its customer register** was affected before the lookup service's own safeguard halted queries [S43]. Holmasto disclosed the breach on 2 September, notified the Data Protection Ombudsman and police, and sent personal email and SMS notices through 14-15 September [S43].
RESPONSE	Enforce strict authentication, object-level access controls and query rate limits on customer-lookup APIs, and minimise stored personal identity data.

Bottom line

Enforce strict authentication and rate limits on customer-lookup APIs and review personal-ID retention.

CASE N

N ■ Confirmed September cyberattack at a Finnish educational and training institution (identity withheld)

Education and training

Confirmed attack

ESTABLISHED ACCOUNT

In September 2026, a Finnish educational and training institution disclosed a cyberattack against part of its ICT environment that corrupted servers and allowed unauthorised access to systems and potentially stored data [S50]. Because the exposed files could not be technically enumerated, individual notifications could not be sent [S50]. The institution reported the attack to the Data Protection Ombudsman, NCSC-FI and police; its identity and notice URL are withheld [S50].

RESPONSE

Accelerate migration off legacy on-premise server rooms and maintain access logging sufficient to determine which data repositories were touched.

Bottom line

Accelerate decommissioning of legacy server rooms and maintain logging capable of bounding affected datasets.

CASE O

O ■ Municipal Koha library-system DDoS intermediary attack

Municipal library infrastructure

Official notices

ESTABLISHED ACCOUNT

From 16 September into the morning of 17 September 2026 (mitigated around 10:00), a distributed denial-of-service attack disrupted shared Koha library systems across multiple Finnish municipal library consortia [S41][S42]. Official municipal notices stated that Finnish library servers were abused as a traffic intermediary against a third country rather than being the ultimate target, and found no evidence of data exposure [S41][S42]. Affected municipal identities and notice URLs are not listed here [S41][S42].

RESPONSE

Audit internet-facing open-source municipal applications for reflection or proxy abuse vectors and maintain current network-provider DDoS escalation contacts.

Bottom line

Check open-source public portals for traffic-amplification abuse and keep upstream DDoS mitigation contacts current.

CASE P

P ■ Reported September data intrusion at an Åland-based organisation

Press report

Åland organisation

REPORTED HEADLINE AND STATUS	In September 2026, regional press on Åland reported that an Åland-based organisation filed a police report regarding a data intrusion [S45]. The organisation's identity is withheld and technical scope details are not reported here [S45].
JURISDICTION NOTE	Determine the competent data-protection authority from the controller's activity and applicable national or Åland legislation. Location on Åland alone does not determine the recipient: Datainspektionen supervises regional and municipal administration and specified Åland-competence activities, while the national Ombudsman remains competent for private operators [S23] [S76][S79].
RESPONSE	Confirm the competent supervisory authority by controller activity and applicable national or Åland legislation before an incident occurs.

Bottom line

Determine the competent data-protection authority from controller activity and applicable national or Åland law, not location on Åland alone.

CASE Q

Q ■ Citrix NetScaler ADC and Gateway zero-day exploitation in Finland

Official warning

Network perimeter across sectors

CHRONOLOGY	On **27 September 2026**, Citrix disclosed critical NetScaler ADC and Gateway zero-day flaws (`CVE-2026-88771` and `CVE-2026-88772`) and published patches [S61][S62]. On **1 October 2026**, NCSC-FI issued its first severe warning of 2026 (`1/2026`), covering eight related CVEs (`CVE-2026-88771` to `CVE-2026-88778`) [S13][S80]. NCSC-FI confirmed multiple pre-patch intrusions in Finland and urged immediate patching alongside forensic hunting for prior exploitation [S14][S80].
AFFECTED SCOPE	Historical September minima and current recommended standard, FIPS and NDcPP builds incorporating Citrix's 12 November security update (`CTX697305` , `CVE-2026-120868`) appear in §12.2 [S14][S61][S62][S80][S87]. NCSC-FI emphasised that patching alone does not evict attackers who gained access before patch deployment [S14][S80].

RESPONSE	Patch standard, FIPS and NDcPP appliances to the current supported builds in §12.2 (or migrate unsupported branches), inspect gateways for pre-patch persistence and rotate active VPN session secrets.

Bottom line

Patch NetScaler appliances immediately, hunt for pre-patch persistence and rotate gateway session secrets.

CASE R

R

Valtori precautionary PHP DMZ shutdown and Eckerö Line subcontractor breach

Government web services and ferry travel

Shutdown and breach

VALTORI PHP SHUTDOWN	On 21 October 2026, NCSC-FI issued advisory 37/2026 on critical unpatched PHP flaws (`CVE-2026-109618` and `CVE-2026-109619`) ahead of the 17:00 vendor patch [S15][S63][S64][S72]. Valtori closed central-government public web interfaces across affected agencies as a stated preventive measure to protect services, with no active exploitation known at the time of the notice [S34]. Affected branches, the October historical minima and current November releases addressing a separate critical session flaw (`CVE-2026-115560`) appear in §12.2 [S15][S72][S85][S86].
ECKERÖ LINE SUBCONTRACTOR BREACH	Days later, ferry operator Eckerö Line disclosed a cyberattack at a subcontractor of its booking-system vendor [S44]. Detected and contained on 26 October (reported to Eckerö Line on 28 October), it exposed booking details for roughly **200 customers** without payment-card data [S44].
RESPONSE	Apply the current fixed PHP releases or migrate off End-of-Life PHP branches per §12.2, treat precautionary isolation as a valid executive control and bind sub-processors to rapid contractual incident notification.

Bottom line

Pre-authorise rapid precautionary DMZ cut-offs and require booking subcontractors to disclose incidents rapidly.

CASE S

S

European grocery refrigeration-controller attacks reaching Finland

Official advisory

Retail and operational technology

CHRONOLOGY	In late October and early November 2026, suspected cyberattacks across France, Belgium, Sweden, Ireland and Estonia targeted internet-exposed industrial refrigeration controllers, raising cold-storage temperatures and causing spoilage [S48][S73]. NCSC-FI revealed on 6 November that it had proactively contacted owners of vulnerable exposed Finnish controllers starting **13 October 2026** [S18].
FINNISH IMPACT	In early November, Finnish press reported brief cold-storage disruptions at a few grocery stores whose cause had not been confirmed [S48]. Separately, NCSC-FI reported suspected local cases on 3 November and confirmed a few malicious refrigeration incidents on 6 and 13 November [S16][S18][S19]. NCSC-FI noted that earlier Finnish OT preparedness and proactive outreach reduced exposed devices and helped avoid major national damage [S18][S19].
RESPONSE	Remove building-management and refrigeration controllers from the public internet immediately and verify safe local manual temperature controls with facilities teams.

Bottom line

Remove refrigeration and building controllers from the public internet and verify safe local manual overrides.

5.3 Recent activity: 8 to 22 November 2026

The final 15 days before cut-off (`8 to 22 November 2026`) recorded **984 Finland-tagged underground posts**, including **19 Finland-tagged forum posts** [S1]. The window also brought one major supplier-linked disclosure, one cross-border retail breach and two NCSC-FI weekly alerts [S19][S20][S35][S47]. These observations apply strictly to this 15-day window and do not imply a longer surveillance baseline.

CASE T

T

Finnair and Aurinkomatkat: Amadeus global reservation-system breach

Air transport and package travel

Official release

CHRONOLOGY AND SCOPE	On **9 November 2026**, Finnair issued an official Cision release confirming that a data breach at global travel-software supplier Amadeus involved multi-airline passenger lists containing approximately **116,000 Finnair reservations** [S35][S36]. Amadeus reported that roughly **750 Finnair reservations** were opened for viewing, including approximately **30 Aurinkomatkat package trips**, and that unauthorised activity was stopped [S35].
EXPOSED INFORMATION AND CONTAINMENT	Only a small fraction of viewed bookings remained active, and Finnair rotated them to new reservation codes [S35]. No credit cards or passwords were affected, Finnair's own systems stayed untouched, and Amadeus filed EU GDPR notification as controller [S35].
RESPONSE	Rotate active booking references rapidly when a reservation supplier is breached and warn travellers against targeted impersonation citing real past flight details.

Bottom line

Rotate active booking references promptly and warn travellers about impersonation using historical flight details.

CASE U

U

Lyko Nordic retail breach

Nordic retail

Official notice

ESTABLISHED ACCOUNT	In mid-November (`12 to 18 November`), Nordic beauty retailer **Lyko** disclosed a contained system intrusion that prompted Finnish consumer warnings (Voice.fi) regarding potential contact-data exposure for Nordic shoppers including Finland [S47][S71].
RESPONSE	Rely on controllers' latest scope notices when advising consumers about cross-border retail breaches.

Bottom line

Rely on controllers' latest scope notices when advising consumers about cross-border retail breaches.

Other 8 to 22 November underground and official signals:

- **12 November:** NCSC-FI published October Cyber Weather highlighting surging WordPress intrusions delivering ClickFix malware [S17].
- **13 and 20 November:** NCSC-FI Weekly Reviews 46 and 47 warned on bank-spoofing robocalls, Black Friday fake webshops and residential-proxy abuse of home routers [S19][S20]. Week 47 also highlighted Finnish-language EU Cyber Resilience Act guidance [S20].
- **17, 20 and 22 November:** One forum posted a 15,000-row Finnish CSV sharing matching sample rows with October's 2023-labelled `B03` without the year label (`B14`) [S1]. Forum posts also twice advertised the `SALTA3` kit naming five Finnish retail banks (`B15`) and claimed a 3-table retail CRM export (`B13`) [S1].

KEY TAKEAWAYS

01

Zero-day edge appliances and third-party SaaS or booking suppliers accounted for major exposures among the documented 2026 cases.

02

Legacy pre-2016 archives and unencrypted removable media remain active healthcare privacy liabilities.

03

The 8 to 22 November window combined confirmed disclosures with live banking-kit advertising and recycled data.

CHAPTER 06

Disruption, hacktivism and claim versus reality

THIS CHAPTER ANSWERS

How should Finnish defenders distinguish claimed attacks from verified service impact?

23

NoName057(16) DDoS rounds affecting 129 Finnish organisations (Aalto study)

6.1 Chronology of 2026 disruption and resilience milestones 49

6.2 Gamified DDoS and psychological pressure 50

6.3 Claim versus official record 50

CHAPTER 06

Disruption, hacktivism and claim versus reality

IN SHORT

The 2026 disruptions documented here fall into three groups: gamified DDoS waves, abuse of open-source systems as intermediaries and precautionary shutdowns during critical vulnerability windows. Aalto University researchers describe NoName057(16) as pro-Russian and assess that its campaigns seek to erode citizens' trust in governments. March Telegram claims alleging access to Finnish residential cameras remain unverified without official confirmation. Rely on owned service telemetry and transparent status notices rather than actor claims.

6.1 Chronology of 2026 disruption and resilience milestones

30 Jan 2026	Valtori detects Ivanti EPMM zero-day MDM intrusion and isolates service [S7][S32]
5 Mar 2026	Telegram channels relay unverified Morningstar claims alleging access to Finnish residential cameras [S1]
1 Jun 2026	National Cyber Resilience Act enters into force in Finland [S9]
27 Aug 2026	Helsinki Court of Appeal overturns dismissal and finds Finnish jurisdiction in Dec 2024 Eagle S cable case [S57]
16 Sep 2026	Shared municipal Koha library servers abused as DDoS intermediary across Finnish library consortia [S41][S42]
27 Sep 2026	Citrix discloses critical NetScaler ADC and Gateway zero-days (CVE-2026-88771, CVE-2026-88772) [S61][S62]
1 Oct 2026	NCSC-FI issues severe warning 1/2026 and confirms multiple pre-patch NetScaler intrusions in Finland [S13][S14][S80]
13 Oct 2026	NCSC-FI begins proactive outreach to owners of vulnerable exposed Finnish refrigeration controllers [S18]
21 Oct 2026	Valtori performs precautionary public web shutdown ahead of critical PHP security patches [S15][S34]
3 Nov 2026	NCSC-FI reports suspected refrigeration-controller cases in Finland; a few are confirmed on 6 and 13 November [S16][S18][S19]
9 Nov 2026	Finnair discloses Amadeus global reservation breach (~116,000 reservations; ~750 viewed) [S35]

6.2 Gamified DDoS and psychological pressure

A 2026 Aalto University School of Business study examined the group **NoName057(16)**, which the researchers describe as pro-Russian [S53]. It documented **23 DDoS rounds** against Finland since 7 January 2025, affecting **129 public and private organisations**, including public bodies, municipalities and financial institutions [S53]. The researchers noted that targeting rose markedly after Finland's 2023 NATO accession [S53]. They assessed that while DDoS attacks can disrupt public services, these gamified campaigns actively seek to erode citizens' trust in governments [S53].

Reported DoS notifications fell roughly 9% in 2025 [S5]. Reporting is voluntary, so this does not establish a comparable decrease in attacks or demonstrate improved mitigation [S5]. At the same time, the September municipal **Koha** library incident demonstrated a different operational hazard: public-sector web applications being co-opted as an outbound traffic intermediary against external targets [S41][S42].

6.3 Claim versus official record

Unverified Telegram channels routinely exaggerate routine outages, precautionary maintenance or unverified screenshots as successful cyberattacks. The comparison below illustrates why Finnish organisations must validate every public claim against internal service telemetry.

Claim or public perception	Established record	Defensive discipline
March Telegram posts relay Morningstar claims alleging access to private Finnish apartment cameras [S1]	The Finnish intrusion claim remains unverified; no official confirmation or accessible independent verification confirms a private Finnish residential-intercom breach [S1]	Verify claimed screenshots, camera exposure and local device logs before assuming an intrusion
October public web outage at central-government sites perceived as a breach [S34]	Valtori confirmed a deliberate precautionary DMZ closure ahead of PHP patches, with no active exploitation known at the time of the notice [S15] [S34]	Publish plain status notices explaining preventive isolation clearly
February 0apt leak-site listings claim three Finland-labelled entries on one day [S2]	The three Finnish entries remain unverified; Halcyon provides a general caution about inflated or false early 0apt claims despite a functional encryptor [S54]	Require forensic log confirmation before declaring data theft

Claim or public perception	Established record	Defensive discipline
European retail freezer alerts raise fears of nationwide Finnish food-chain collapse [S48][S73]	NCSC-FI confirmed a few local incidents, noting that proactive outreach from 13 October reduced exposed devices and earlier Finnish OT preparedness helped avoid major damage [S16][S18][S19]	Confirm local controller exposure with facilities teams rather than reacting to headlines
Hacktivist DDoS channels claim prolonged takedowns of Finnish ministries or banks [S53]	Aalto researchers assess aims to erode citizens' trust in governments [S53]. Reported DoS notifications fell roughly 9% in 2025, but reporting is voluntary, so this does not establish a comparable decrease in attacks or demonstrate improved mitigation [S5]	Measure real uptime telemetry and communicate next update times without quoting slurs

KEY TAKEAWAYS

01

Separate hacktivist availability claims, intermediary abuse and precautionary shutdowns in incident communications.

02

Aalto University researchers assess that these DDoS campaigns seek to erode citizens' trust in governments; determine technical impact separately from service telemetry.

03

Publish calm, timestamped service-status notices grounded in owned telemetry.

CHAPTER 07

Ransomware, espionage advisories and threat profiles

THIS CHAPTER ANSWERS

Who is claiming Finnish targets, and what separates an extortion label from a state advisory?

16

Finland-labelled ransomware listings across 8 claimant labels

7.1 Regional ransomware listings and seasonal shift 53

7.2 Threat network and profiled groups 55

7.3 State-linked espionage advisories and hacktivism 58

CHAPTER 07

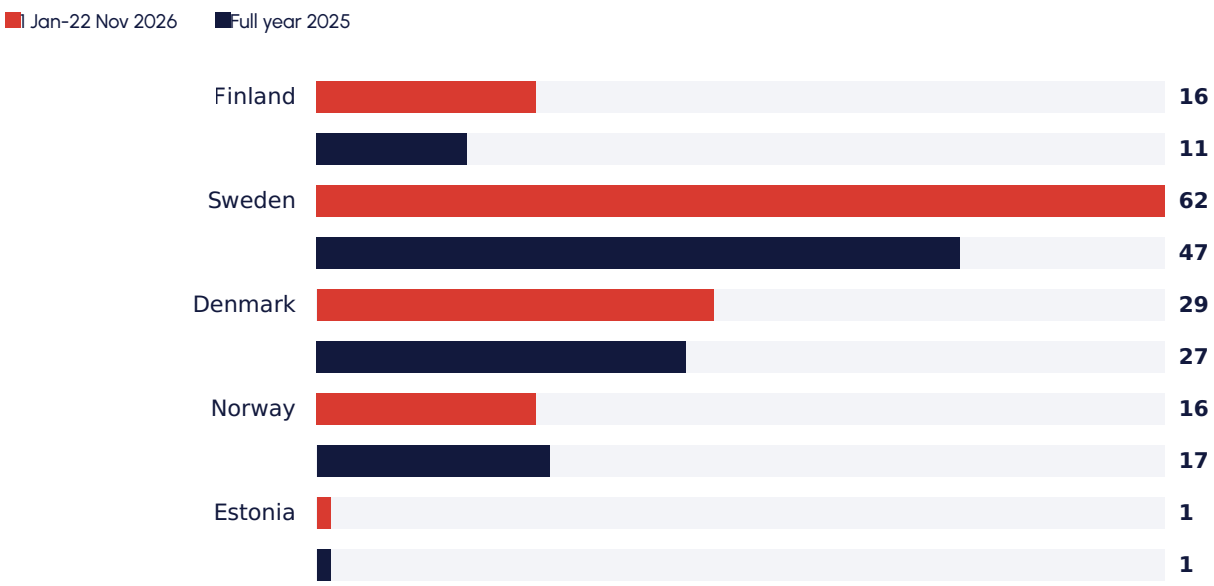
Ransomware, espionage advisories and threat profiles

IN SHORT

Ransompedia recorded 16 Finland-labelled ransomware listings from 1 January to 22 November 2026, surpassing 11 in 2025 and matching Norway's 16. Thirteen arrived between June and November, two repeats bound unique claims to at most 14, and all listings remain unverified. FBI and NCSC-FI advisories report state-attributed activity; GTIG assesses with high confidence that UNC7005 has a Russian nexus (moderate confidence for its ICE RELIC link). Verify extortion listings against owned logs, patch exposed edge routers and Zimbra servers, and restrict unverified OAuth consents.

7.1 Regional ransomware listings and seasonal shift

Finland's 16 ransomware listings surpass 2025 totals and match Norway's count



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

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

Between 1 January and 22 November 2026, Ransompedia logged **16 Finland-labelled listings** across **8 claimant labels**, up from **11 across all of 2025** (and 40 all-time) [S2]. Among Finland's four regional comparators, **Sweden logged 62** (vs 47 in 2025), **Denmark 29** (vs 27), **Norway 16** (vs 17) and **Estonia 1** (vs 1) [S2].

Four analytical nuances prevent misreading Finland's raw count of 16 [S2]:

- **Repeat listings reduce unique entries.** INC Ransom listed one Finnish organisation twice in the second half of 2026 [S2]. Clop likewise listed one Finland-linked organisation twice in the second half of 2026 [S2]. At most **14 distinct claimed entries** underlie the 16 listings [S2].

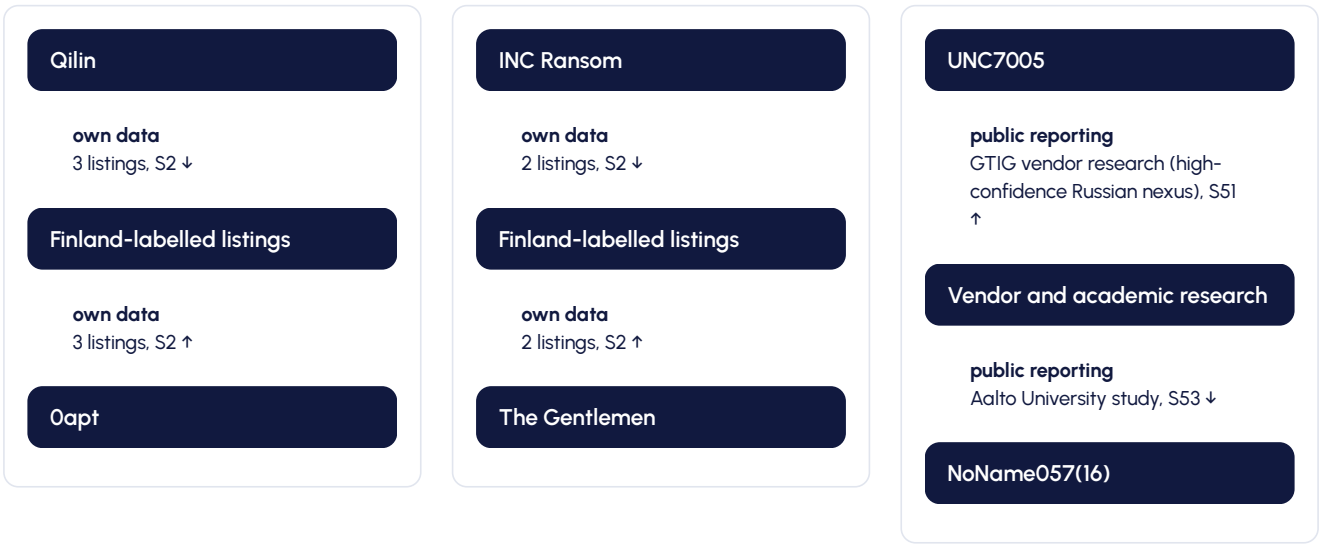
- **Early-year counts include three unverified 0apt entries.** Three of Finland's 16 listings appeared on one day in **February 2026** under the `0apt` label and remain individually unverified [S2]. Independent analysis by Halcyon supplies a general caution that while 0apt built a functional Rust encryptor, many of its early-2026 victim claims were inflated or unverifiable [S54].
- **The concentration of listings coincides with NCSC-FI's separately reported summer increase.** Excluding the three February 0apt entries, **all 13 remaining listings** appeared between June and November (June 1, July 2, August 4, September 4, October 1, November 1) [S2]. That timing coincides with NCSC-FI's July Cyber Weather report of a summer increase in ransomware notifications, though seasonal alignment does not verify individual listings [S11].
- **Country enrichment requires verification.** Source-assigned industry labels led with manufacturing (6), energy (2) and global (2), plus single entries across high-tech, IT consulting, education, retail, public administration and finance [S2]. Source country tags can misassign unrelated organisations or overseas subsidiaries to Finland, so listings never establish confirmed victimhood on their own.

Claimant label	2026 FI listings	Window months	Verification note
Qilin	3	Aug (2), Oct	Leading active label alongside 0apt; individual claims unverified [S2]
0apt	3	Feb	Same-day batch; individual claims unverified, with Halcyon supplying a general caution on early 0apt claims [S2][S54]
INC Ransom	2	Sep, Nov	Repeat entries; individual claims unverified [S2]
The Gentlemen	2	Jul, Sep	Two Finland-labelled entries; individual claims unverified [S2]
Clop	2	Aug, Sep	Repeat entries; individual claims unverified [S2]
Lockbit5	2	Jun, Sep	Individual claims unverified [S2]
Krybit	1	Aug	Individual claims unverified [S2]
Deadlock	1	Jul	Individual claims unverified [S2]

7.2 Threat network and profiled groups

The relationship view below keeps own-source Ransompedia listing edges (`own data`) strictly separate from official government advisories (`official`) and vendor or academic research (`public reporting`). No unverified operational linkage is inferred between criminal ransomware labels, hacktivist collectives and state-linked espionage clusters.

Own post · Relay · Official statement · Public reporting · Our observation



Qilin

Label in the retained listing population

Ransomware/extortion listing label · No state attribution established here

IN FINLAND, 2026

2026 window

3 Finland-labelled listings (August and October 2026), S2

CLAIMED TARGETS

Finland-labelled entries; identities and sectors withheld and country association qualified

SEEN IN PUBLIC REPORTING

[S2] 3 listings recorded in Ransompedia (August and October 2026)

OUR ASSESSMENT

Qilin is the joint most frequent claimant label on Finnish entries alongside 0apt. A listing verifies an extortion assertion rather than confirmed encryption, data authenticity or accurate country tagging; unrelated organisations or overseas subsidiaries can be misassigned to Finland.

CONFIDENCE
High for the recorded count; individual claims unverified

0apt

0APT (label in the retained listing population)

Ransomware/extortion listing label | No state attribution established here

IN FINLAND, 2026

2026 window

3 Finland-labelled listings on one day in February 2026, S2

CLAIMED TARGETS

Three Finland-labelled entries on one day; identities and sectors withheld

SEEN IN PUBLIC REPORTING

[S2] 3 same-day listings recorded in Ransompedia

[S54] Halcyon research supplying a general caution about inflated or unverifiable early 0apt victim claims

OUR ASSESSMENT

Halcyon confirmed a functional Rust encryptor while providing a general caution that many early-2026 0apt claims were inflated or unverifiable. The three Finnish entries remain individually unverified and require internal forensic validation rather than assumed data loss.

CONFIDENCE
High for the recorded count and Halcyon's general caution; the three Finnish claims remain unverified

INC Ransom

Label in the retained listing population

Ransomware/extortion listing label | No state attribution established here

IN FINLAND, 2026

2026 window

2 Finland-labelled listings (September and November 2026), S2

CLAIMED TARGETS

Finland-labelled repeat entries; identities and sectors withheld

SEEN IN PUBLIC REPORTING

[S2] 2 repeat listings recorded in Ransompedia

OUR ASSESSMENT

Repeat listings inflate raw victim counts when the same organisation is re-posted under a fresh date or industry tag. Treat any extortion listing as an unverified claim requiring independent forensic validation.

CONFIDENCE

High for the recorded count and repeat-entry structure; individual claims unverified

The Gentlemen

Label in the retained listing population

Ransomware/extortion listing label | No state attribution established here

IN FINLAND, 2026

2026 window

2 Finland-labelled listings (July and September 2026), S2

CLAIMED TARGETS

Finland-labelled entries; identities and sectors withheld

SEEN IN PUBLIC REPORTING

[S2] 2 listings recorded in Ransompedia

OUR ASSESSMENT

A listing verifies an extortion assertion rather than confirmed operator attribution, encryption or data loss. The label also led Swedish and Danish 2026 Ransompedia counts.

CONFIDENCE

High for the recorded count; individual claims unverified

7.3 State-linked espionage advisories and hacktivism

Official and vendor advisories published in 2026 highlight sustained state-linked intelligence pressure affecting Western and Nordic partners including Finland, alongside gamified DDoS campaigns. All state attributions below remain strictly the cited issuing agencies' or researchers' assessments.

On **7 April 2026**, the FBI Internet Crime Complaint Center (IC3) and international partners including Finland attributed a global SOHO router campaign to Russian GRU (APT28) [S52]. Actors exploited vulnerable SOHO routers worldwide, including legacy End-of-Life TP-Link models via `CVE-2023-50224`, to harvest credentials and hijack DNS [S52][S66][S77]. TP-Link advises replacing unpatched End-of-Life routers with supported products and disabling internet-facing remote management (see §12.2) [S52][S77].

Separately, in **July 2026**, NCSC-FI's Cyber Weather described two joint Finnish-international warnings on Russian state-linked espionage [S11]. One warned of an FSB-linked actor targeting poorly secured enterprise network devices [S11]. The other warned of the state-linked actor **Laundry Bear** targeting email systems, including Zimbra webmail (`CVE-2025-66376`; see affected and fixed versions in §12.2) [S11][S65][S78]. Neither July warning is merged into the April GRU/APT28 profile below.

Separately, Google Threat Intelligence Group (GTIG) assesses with high confidence that **UNC7005 (STORM-2945)** has a Russian nexus (moderate confidence for its ICE RELIC link) [S51]. Starting 31 July 2026, it registered domains spoofing the **Finnish Operations Center** and sent OAuth spearphishing emails (6-13 August) to European defence targets [S51]. Spoofing an organisation's name as a phishing lure does not indicate that the spoofed organisation's own infrastructure was breached [S51].

UNC7005 (STORM-2945)

GTIG tracking cluster

Phishing cluster with Russian nexus (vendor research) | Russian nexus per GTIG (high confidence); ICE RELIC link moderate confidence

IN FINLAND, 2026

31 Jul - 13 Aug 2026

Registered domains spoofing Finnish Operations Center and sent OAuth phishing to European defence targets, S51

CLAIMED TARGETS

Academia, diplomatic, nonprofit and European defence-industrial personnel; no Finnish victim count established

SEEN IN PUBLIC REPORTING

[S51] Google Threat Intelligence Group technical analysis

OUR ASSESSMENT

GTIG observed UNC7005 using Finnish defence-market branding as a lure in Google OAuth phishing, alongside device-code phishing in separate earlier campaigns. The use of a Finnish organisation's name as a lure does not mean that organisation's own systems were breached.

CONFIDENCE

High for the published vendor findings; no independent attribution or Finnish victim total

GRU / APT28 router advisory

Fancy Bear, Forest Blizzard (agency labels)

Official international espionage advisory | Russian GRU attribution retained strictly as the issuing agencies' assessment

IN FINLAND, 2026

7 Apr 2026

FBI IC3 and Finnish/international partners warn on GRU/APT28 SOHO router exploitation (CVE-2023-50224), S52

CLAIMED TARGETS

Vulnerable SOHO routers, including legacy End-of-Life TP-Link models (CVE-2023-50224)

SEEN IN PUBLIC REPORTING

[S52] FBI IC3 PSA260407 naming Finland among international partners

[S66] NVD entry for CVE-2023-50224

[S77] TP-Link Security Advisory (FAQ 5058)

OUR ASSESSMENT

The FBI's April advisory attributes the router campaign to GRU/APT28, alongside international partners including Finland [S52]. It supplies defensive hardening priorities rather than a Finnish victim census.

CONFIDENCE

High for the official agency advisory; no independent operator attribution

NoName057(16)

Gamified DDoS collective (Aalto study)

Gamified hacktivist DDoS collective (academic study) | Pro-Russian hacktivist alignment as described by Aalto University research

IN FINLAND, 2026

Jan 2025 - 2026 study

23 DDoS attack rounds affecting 129 Finnish public and private organisations, S53

CLAIMED TARGETS

Public bodies, municipalities, financial institutions and public web services

SEEN IN PUBLIC REPORTING

[S53] Aalto University School of Business study release

OUR ASSESSMENT

Aalto University researchers assess that these gamified DDoS campaigns seek to erode citizens' trust in governments alongside service disruption. Determine technical impact separately from owned service telemetry rather than actor claims.

CONFIDENCE

High for the published Aalto University study; individual claim verification requires service telemetry

Technique identifiers are omitted where the cited public source passages do not publish an explicit mapping. Defenders should treat every state advisory as a concrete hardening prompt for edge routers, webmail servers and OAuth application policies rather than evidence of a specific local infection.

KEY TAKEAWAYS

01

All 16 Ransompedia listings remain unverified, and the summer-autumn concentration coincides with NCSC-FI's separately reported summer increase.

02

Keep criminal extortion labels, hacktivist DDoS and state-attributed espionage advisories strictly separate.

03

Act on router, Zimbra and OAuth advisories immediately without inferring unproven local breaches.

CHAPTER 08

Fraud, identity abuse and secondary harm

THIS CHAPTER ANSWERS

How do leaked personal details and underground services fuel Finland's fraud economy?

20,000

bank-logged fraud attempts in Finland in H1 2026

8.1 National digital-fraud scale and shifting attacker tactics 62

8.2 Forged Finnish documents, KYC kits and local mule recruitment 64

8.3 Payment-card material: a narrow observation 66

8.4 Secondary harm after legitimate data breaches 67

CHAPTER 08

Fraud, identity abuse and secondary harm

IN SHORT

Digital fraud is Finland's highest-volume everyday cyber harm. Finnish banks logged EUR 148 million in attempted fraud in 2025 and EUR 60 million across 20,000 attempts in H1 2026. Attempt counts surged even as average transfer sizes fell and safe-account totals declined. Underground forums supply forged Finnish payslips, EU KYC selfies, physical-pickup drops and nominee company formation. Defenders must connect privacy breach handling directly to fraud prevention and safe customer support.

8.1 National digital-fraud scale and shifting attacker tactics

Data collected from Finnish banks by Finance Finland (Finanssiala ry) provides an authoritative financial benchmark [S29][S30]. Across full-year **2025**, criminals attempted to defraud Finnish customers of **EUR 148 million**, up from EUR 107.2 million in 2024 [S29]. Banks stopped or recovered **EUR 75.5 million** (over 50%), leaving **EUR 72.5 million** lost (vs EUR 62.9 million in 2024) [S29].

Phishing accounted for EUR 53.1 million attempted (targeting nearly 17,000 people, with 13,000 saved) [S29]. Safe-account scams (turvatilihuijaukset) totalled EUR 38.4 million attempted (EUR 23.8 million stopped, EUR 14.6 million lost) [S29][S30]. Across the fraud cases described by Finance Finland, customers themselves transferred money to criminals in 60% of cases [S29].

In **H1 2026** (January to June), attempted fraud totalled **EUR 60 million** [S30]. Banks stopped or recovered **EUR 31.7 million (53%)** while criminals took **EUR 28.3 million (47%)** [S30]. In H1 2025, banks stopped EUR 28 million (48%) and criminals took EUR 30 million [S30]. Beneath the steady euro total, however, **attempt volume jumped sharply to 20,000 cases** (6,000 completed and 14,000 blocked), up from **13,600** in H1 2025 (3,700 completed and 9,900 blocked) [S30].

H1 2026 fraud category (Finance Finland)	Lost to criminals (EUR M)	Prevented or recovered (EUR M)	Operational pattern
Phishing (tietojen kalastelu)	10.6	Included in 31.7 total	High volume; credentials increasingly reused as strong ID [S30]
Investment fraud (sijoitushuijaukset)	8.2	Included in 31.7 total	Social-media lures and fake trading platforms [S30]
CEO and invoice fraud (toimitusjohtaja- ja laskutushuijaukset)	4.9	0.4	Worst stop rate; driven by a small number of large corporate transfers [S30]
Document and romance fraud	2.6	2.4	Multi-week social engineering [S30]

H1 2026 fraud category (Finance Finland)	Lost to criminals (EUR M)	Prevented or recovered (EUR M)	Operational pattern
Safe-account scams (turvatili)	2.0	1.9	EUR 3.9M attempted in H1 2026 (EUR 2.0M lost) vs EUR 38.4M attempted across full-year 2025 (EUR 14.6M lost; different period lengths); Finance Finland notes warnings may have helped [S29][S30]
Total H1 2026	**28.3**	**31.7**	**EUR 60.0M attempted across 20,000 cases (53% prevented/recovered)** [S30]

Two structural warnings in Finance Finland's September 2026 report directly guide Finnish CISOs [S30]:

- **Corporate BEC remains the hardest category for banks to intercept.** Only EUR 0.4 million was stopped against EUR 4.9 million lost in CEO and invoice fraud [S30]. Corporate email authentication, M365 hardening and out-of-band payment verification therefore matter far more than post-transfer recovery.
- **Public-service impersonation keeps evolving.** On 2 September 2026, the Digital and Population Data Services Agency (DVV) warned of email, SMS and WhatsApp lures spoofing **Suomi.fi** [S31]. DVV reminded residents that genuine Suomi.fi notices never arrive by SMS or WhatsApp and never contain login links [S31]. NCSC-FI additionally documented Finnish-language WhatsApp executive-group scams in March, bank-spoofing robocalls in November and AI-polished Black Friday fake webshops in late November [S8][S19][S20].

8.2 Forged Finnish documents, KYC kits and local mule recruitment

Evidence card B10 — 8 Apr 2026

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

ORIGINAL

NEW - для подтверждения занятости - зарплатная / платежная ведомость Финляндия + трудовой договор For proof of employment - payslip / payroll / paystub + employment contract / agreement Finland

TRANSLATION

New: for proof of employment, Finnish payslip and employment contract templates.

Note. Demonstrates tailored Finnish document supply beyond generic passport templates.

Held

A document-forgery seller advertises custom Finnish payslip and employment-contract templates for onboarding or verification checks.

Not established

Successful bypass of any Finnish bank, lender or employer verification check, or completed sales.

Evidence card B11 — 31 May 2026

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

ORIGINAL

Ищу скупку со своими дропами Финляндия - нужно ходить забирать уже оплаченные айфоны [...] просьба сразу присылать ваш скупп лист и в каких городах у вас есть дропы

TRANSLATION

Looking for a buyer with local drops in Finland to pick up already paid smartphones; send your payout list and which cities you cover.

Note. Shows how online payment fraud connects to physical fulfilment and local mule recruitment.

Held

A Russian-language post recruits local physical-pickup mule operators in Finnish cities to collect fraudulently ordered electronics.

Not established

Active local drop networks, named Finnish retailers affected, actual thefts or completed payouts.

Evidence card B12 — 24 Oct 2026

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

ORIGINAL

нужны дропы под открытие фирмы + 2 счёта [...] приоритет стран германия, Британия [...] Дания [...] Нидерланды, Финляндия Оплата после открытия.

TRANSLATION

Seeking nominees to open a company plus two bank accounts; priority countries include Germany, UK, Denmark, Netherlands and Finland. Payment after opening.

Note. Contact handle removed; highlights corporate-onboarding and beneficial-ownership abuse demand.

Held
An October recruitment post lists Finland among twelve European priority jurisdictions for recruiting nominee company directors and opening corporate bank accounts.

Not established
Any successfully registered Finnish company, bank-onboarding failure or active mule cell in Finland.

Our retained underground forum corpus illustrates the specialised support economy behind digital fraud targeting Finland [S1]. Sellers advertised custom **Finnish payslip and employment-contract templates** (`B10` , 8 April) and USD 25 EU KYC selfie packs including Finland (19 August) [S1]. Other threads recruited **local pickup drops** for carded smartphones (`B11` , 31 May) and **nominee company directors** across twelve European countries including Finland (`B12` , 24 October) [S1].

These advertisements show criminal supply and recruitment demand, not successful onboarding bypasses or active Finnish cells. Still, they show why document-upload checks alone cannot guard consumer credit, click-and-collect electronics retail or corporate bank onboarding.

8.3 Payment-card material: a narrow observation

SCOPE OF THE CARD FIGURES

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

Across the retained 2026 corpus, we observed **73 distinct Finland-labelled payment card records** across **109 appearances in 83 posts** and **41 six-digit bank identification numbers (BINs)** [S1]. The split comprised 36 Mastercard, 34 Visa, 1 American Express and 2 other (16 debit, 12 credit, 45 unlabelled) [S1]. Clear-text card appearances

peaked in August (42 distinct cards across 53 posts) [S1]. Separately, **1,711 card-shop or offer posts** referenced Finland without clear-text card numbers [S1]. That group included **1,520 multi-country shop updates** (median 45 countries and 1,538 cards per batch; median asking range USD 10 to 24) [S1].

Clear-text postings represent a narrow slice of underground card markets and establish neither confirmed theft from a Finnish bank nor active card balances. No mass card-cancellation conclusion follows from these counts; issuers and merchants should act strictly on verified BIN alerts and transaction telemetry.

8.4 Secondary harm after legitimate data breaches

Confirmed disclosures such as **Finnair / Amadeus** (`Case T`), **Kolmostien Terveys** (`Case J`), **Holmasto** (`Case M`) and **Eckerö Line** (`Case R`) exposed personal context [S35][S39][S43][S44]. In **Aalto EE** (`Case I`), the official notice stated that names, email addresses, Canvas register IDs and private inbox messages may have been exposed [S37]. Across these notices, exposed or potentially exposed fields ranged from booking references and inbox text to Finnish personal identity codes (`henkilötunnus`). Even when payment cards and passwords are untouched, genuine context allows a caller or message to sound completely legitimate.

Remember that an individual's personal identity code or booking number is **context, never authentication**. Customer support, billing desks and patient-service lines should verify high-risk requests through independent callbacks and clearly tell affected people what exposed data cannot be used to authorise.

KEY TAKEAWAYS

01

Finnish fraud attempt volume surged to 20,000 in H1 2026 while corporate BEC suffered the lowest bank stop rate.

02

Underground markets actively advertise Finnish payslip forgeries, local pickup drops and nominee company formation.

03

Keep narrow clear-text card observations separate from bank intrusion claims and harden support lines against real-context lures.

CHAPTER 09

Banking, strong authentication and payment continuity

09

THIS CHAPTER ANSWERS

How are attackers targeting Finland's bank-linked strong electronic identity?

7 of 25

selected Finnish finance domains had a current credential listing

9.1 Selected finance-sector posture and bank exposure 69

9.2 Strong-ID chaining, live phishing kits and FI-IBAN accounts 71

9.3 Operational resilience and threat-led testing 72

CHAPTER 09

Banking, strong authentication and payment continuity

IN SHORT

Finnish online bank credentials serve as Finland's primary strong electronic identity, extending phishing harm into eSIMs, Mobile Certificates and instant loans. On the 24 November 2026 snapshot across 25 finance domains, 7 had a current credential listing, with at least 7,317 device associations (99.2% non-employee) and 108,274 credential records. Separately, 20 publish quarantine or reject DMARC policies, while late-November forums twice advertised SALTA3 targeting five Finnish banks. Validate current listings first, harden strong-ID enrolment and exercise TIBER-FI and DORA continuity plans.

9.1 Selected finance-sector posture and bank exposure

The selected **Banking and finance** cell contains **25 Finnish domains** (not a complete census of every licensed bank, insurer or payment institution), and all 25 have both configuration and exposure observations [S3][S4]. Passive configuration observations on 24 November 2026 show strong baseline hygiene with narrow remaining gaps [S3]:

- **DMARC: 20 of 25 domains (80%)** publish DMARC policies requesting quarantine or rejection (`12 reject`, `8 quarantine`), **4** remain in monitoring mode (`none`), and **1** lacks a valid DMARC record [S3][S67]. Published policy categories do not establish full coverage or receiver behaviour (§3.5) [S67].
- **Supporting mail and web controls: 24 of 25** publish SPF [S68], **22** publish DKIM [S69] and **6** publish DNSSEC delegation records [S3]. In total, **24** passed TLS validation (1 unavailable), and **22 of 24** with available HTTP responses enforce HSTS [S3][S70].
- **Rolling 365-day underground domain mentions (23 November 2025 to 22 November 2026): 6 of 25 finance domains** recorded **9 dark-chat mentions** and **1 domain** recorded **1 dark-web mention** [S4]. During the 2026 window (`1 January to 22 November 2026`), **3 domains** recorded **5 mentions** [S4].

Exposure observations across all 25 finance domains separate active market offers from cumulative customer-device noise [S4]. No sector or group exposure rating is published.

Finance-cell measure (25 assessed domains)	Observation	Decision boundary
Current credential listings / prior history	7 domains (all 7 with history; 15 entries) [S4]	Market offer, not a tested password or bank breach
Infected-device associations, at least	7,317 across 18 domains [S4]	Cumulative across customer and staff devices
Employee-classified device associations	59 across 12 domains (0.8% of cell devices) [S4]	Subset of 7,317; validate managed staff endpoints
Non-employee device associations	7,258 (99.2% of cell devices) [S4]	Plausibly customer devices; fraud signal, not bank breach
Historical credential records	108,274 across 24 domains (91,942 breach DB, 1,174 stealer, 15,158 combolist) [S4]	Top two domains hold 65.0%; cumulative, not 2026-only
Document associations / 30-day similar names	120 across 17 domains / 7,362 across 14 domains [S4]	Context and triage candidates, not confirmed phishing

Licensed card-issuing bank subset (12 of 25 finance domains). Twelve domains within the 25-domain cell represent licensed card-issuing banks in Finland (bank names withheld) [S4]. Keeping this strict 12-bank subset separate from the wider 25-domain finance cell clarifies where consumer-facing exposure sits [S4]:

- **All 7 current credential listings** in the finance cell sit within the **12 licensed banks** (`7 of 12`) [S4].
- **10 of 12 licensed banks** carry **7,095 non-employee device associations** (97.8% of the cell's 7,258) and **7 of 12** carry **36 employee-classified device associations** [S4]. Across those 12 banks, total device associations reach **7,131** alongside **84,246** historical credential records [S4].
- **Concentration:** The three largest bank populations account for **78.6%** (5,580 of 7,095) of subset non-employee device associations [S4].
- **Payment-card boundary (§8.3).** The clear-text card material in §8.3 establishes no validated card-to-bank relationship and no issuer ranking [S1].

Finance-domain question	Observed signal	Responsible owner
Does the domain publish a quarantine or reject DMARC policy?	20 of 25 requesting quarantine or rejection (4 monitoring, 1 missing; §3.5) [S3]	Messaging and domain security
Are finance credentials currently listed for sale?	7 of 25 finance domains (all 7 within the 12-bank subset) [S4]	Identity operations and SOC
Are finance device associations mostly staff or customers?	At least 7,317 total; 59 employee (0.8%) vs 7,258 other (99.2%) [S4]	Fraud, customer protection and endpoint teams
Are live banking phishing kits targeting Finland?	SALTA3 kit advertised 20 and 22 Nov naming five Finnish retail banks [S1]	Fraud operations and digital channels
Does an underground credential file establish a bank breach?	No; domain-labelled compilations frequently mix unrelated global URLs [S1]	Identity and SOC validation

9.2 Strong-ID chaining, live phishing kits and FI-IBAN accounts

Evidence card B15 — 20 Nov 2026

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

ORIGINAL

SALTA3 is a live panel phishing kits customized to target specific banks, including top financial institutions in the EU: [...] Finland [five major retail banks withheld] [...] Key Features: Real-Time typing

Note. Targeted bank names are withheld; real-time operator panels are built to intercept interactive strong-authentication flows.

Held
On 20 November (and repeated 22 November), a forum seller advertises the SALTA3 real-time interactive phishing kit with templates naming five major retail banks operating in Finland.

Not established
Intrusion at any named bank's systems, active deployment volume in Finland or successful customer fund theft.

Evidence card B16 — 22 Jan 2026

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

ORIGINAL

Premium quality [account provider withheld] & UK REAL COMPANY NOT FAKE (with the entered business database registry) FI IBAN (finland) [...] DOCUMENTS + WEBSITE

Note. Demand for the same account provider reappeared in a Telegram verification-trading channel on 8 November 2026.

Held
A January forum post advertises a purported business payment account with a Finnish FI-prefix IBAN, claiming verified status and bundling a registered company, documents and website.

Not established
Provider system intrusion, valid active banking status, successful SEPA abuse or completed transfer.

Finance Finland highlighted a shift in September 2026: criminals increasingly phish Finnish bank credentials (`pankkitunnukset`) **as an identification instrument rather than solely to drain an account** [S30]. Using stolen bank logins, fraudsters open an account at a second bank and obtain an **eSIM** and **Mobile Certificate (mobiilivarmenne)** from a mobile operator [S30]. Holding both bank and telecom credentials enables rapid instant loans and instalment purchases across multiple firms [S30].

Retained underground observations include advertisements matching each step of that pattern [S1]:

- **Interactive phishing kits (`B15`):** Advertised on 20 November and 22 November 2026, `SALTA3` markets real-time operator interaction (`Real-Time typing`) with dedicated templates for **five major retail banks operating in Finland** (bank names withheld) [S1]. Real-time panels are engineered to relay victims through live bank-app or code prompts.
- **FI-IBAN business accounts (`B16`):** Sellers advertised purported business payment accounts with Finnish `FI` -prefix IBANs, claiming verified status, on forums in January, while Telegram buyer demand appeared on 8 November [S1]. Bundled with registered companies, such listings target Single Euro Payments Area (SEPA) fraud operators [S1].
- **Telecom inputs (`Case F`):** Finnish eSIMs priced at USD 75 (`B08`), non-VoIP SIM rentals and spoofed SMS Sender ID services (`B09`) directly complement cross-bank strong-ID abuse [S1].

Equally important is verifying banking-labelled credential dumps critically. One May 2026 forum file claiming 100 lines for a Finnish banking domain mixed a handful of Finnish login strings with unrelated international e-commerce URLs [S1]. Security teams should always inspect sample structure before treating a banking-named combo list as an institutional leak.

9.3 Operational resilience and threat-led testing

Payment continuity in Finland connects banks, clearing infrastructure, telecommunications and electricity. Under the EU Digital Operational Resilience Act (DORA), the Financial Supervisory Authority (FIN-FSA / Finanssivalvonta) supervises ICT risk management, third-party dependencies and major-incident reporting [S26][S27]. Alongside DORA, the **Bank of Finland (Suomen Pankki)** administers **TIBER-FI**, Finland's national framework for intelligence-led red-team testing of critical financial entities [S28].

Financial-sector CISOs should test two 2026 scenarios inside TIBER-FI and continuity exercises. First, test interactive strong-ID phishing chained into second-bank and eSIM enrolment. Second, exercise loss of a critical communications or software supplier during peak payment windows.

KEY TAKEAWAYS

01

Phished Finnish bank logins now unlock eSIMs, Mobile Certificates and cross-bank consumer loans.

02

Real-time phishing kits explicitly customised for five retail banks operating in Finland were advertised in late November.

03

Pair strong-ID enrolment friction and cross-sector bank-telecom alerts with TIBER-FI and DORA continuity testing.

CHAPTER 10

Regulation, reporting clocks and national response

THIS CHAPTER ANSWERS

Which Finnish authority, portal and legal deadline applies when an incident hits?

11 February 2026

FIN-FSA FISA web form became mandatory for DORA incident reports

10.1 Finland's 2026 statutory baseline 74

10.2 Distinct reporting clocks and recipients 75

10.3 Practical compliance lessons from 2026 Finnish cases 77

CHAPTER 10

Regulation, reporting clocks and national response

IN SHORT

Five statutory regimes govern Finnish cyber and privacy duties in 2026: NIS2 (124/2025), CER (310/2025), GDPR and the Data Protection Act, DORA via FISA, and the Cyber Resilience Act. Finland's national CRA law took effect on 1 June 2026, and EU manufacturer reporting applies from 11 September 2026. Separate awareness from classification timestamps, confirm Åland jurisdiction where applicable, and pre-verify backup portal access.

10.1 Finland's 2026 statutory baseline

Five statutory frameworks shape incident response, supply-chain governance and board accountability in Finland during 2026:

- **Cybersecurity Act (Kyberturvallisuuslaki 124/2025):** Finland's national NIS2 implementation, in force since April 2025, sets risk-management, executive-training and phased incident-reporting duties (Sections 11 to 13) for essential and important entities across designated sectors [S21]. Under Section 38, maximum administrative fines for essential entities reach EUR 10 million or 2% of preceding-financial-year global annual turnover, whichever is higher [S21]. For important (non-essential) entities, the ceiling is EUR 7 million or 1.4% of preceding-financial-year global annual turnover, whichever is higher [S21].
- **Critical Infrastructure Protection and Resilience Act (310/2025):** Finland's national CER Directive statute governs resilience and incident reporting (Section 16) for designated critical entities alongside national risk assessments [S22][S56]. Under Section 2, CER Sections 14 to 16 duties exclude banking, financial-market infrastructure and digital infrastructure, which follow sector regimes [S22]. Section 2 also excludes defence, national security, law-enforcement and specified constitutional bodies [S22].
- **GDPR and Data Protection Act (Tietosuojalaki 1050/2018):** Determine the competent data-protection authority from the controller's activity and applicable national or Åland legislation. Location on Åland alone does not determine the recipient. Datainspektionen supervises Åland regional and municipal administration and specified regional-competence activities, while the national Ombudsman (Tietosuojavaltuutetun toimisto) remains competent for private operators [S23][S76][S79]. In 2026, the Ombudsman published Finlex ruling `2026/10` (31 March 2026) on e-invoice access [S24], while a government proposal extending GDPR fines to public bodies drew debate from KT [S25].
- **DORA and FIN-FSA FISA reporting:** Under FIN-FSA release `4/2026` (19 January 2026), supervised financial entities must submit DORA incident reports via the **FISA electronic web form** from **11 February 2026**, retiring legacy Excel templates [S26][S27]. Reporting time limits and exceptions are set by Commission Delegated Regulation (EU) 2025/301, Article 5 [S74].

- **Cyber Resilience Act (EU 2024/2847) and telecom orders:** Finland's complementary national law (Kyberkestävyyslaki) entered into force on **1 June 2026** [S9]. Under CRA Article 71(2), **Article 14 manufacturer reporting obligations apply from 11 September 2026** (within this report's window), ahead of the broader **11 December 2027** general application date [S75]. NCSC-FI highlighted Finnish-language European Commission guidance in November [S20]. Additionally, Traficom required organisations to license protected **SMS Sender IDs** ahead of the **4 May 2026** cutoff and removed over 100 `.fi` domains with inaccurate registrant details [S8].

10.2 Distinct reporting clocks and recipients

One cyber incident can trigger several legal clocks simultaneously. The operational guide below summarises principal timelines and starting events (not legal advice for a specific case):

Regime	Core trigger	Principal reporting sequence	Competent Finnish recipient
Cybersecurity Act (124/2025, NIS2)	Significant incident affecting an in-scope essential or important entity	Early warning within **24 hours** of awareness (Section 11); follow-up notification within **72 hours** of awareness (**24 hours** for trust-service providers, Section 11); intermediate report on request or within **1 month** of follow-up if ongoing (Section 12); final report within **1 month** of the follow-up notification, or within **1 month** of concluding incident handling for ongoing incidents (Section 13) [S21]	Sector supervisory authority and NCSC-FI reporting route [S21]
GDPR / Data Protection Act	Personal-data breach unless risk to rights and freedoms is unlikely	Notify within **72 hours** of becoming aware where feasible; communicate to individuals without undue delay when high risk is likely [S23]	Office of the Data Protection Ombudsman or Åland Datainspektionen. Determine the competent data-protection authority from the controller's activity and applicable national or Åland legislation. Location on Åland alone does not determine the recipient (national supervision remains relevant to private operators) [S23][S76][S79]

Regime	Core trigger	Principal reporting sequence	Competent Finnish recipient
DORA (EU 2022/2554; Delegated Reg. 2025/301, Art. 5)	Major ICT-related incident at an in-scope financial entity	Initial notification within **4 hours** of major classification and no later than **24 hours** from awareness; if classified major after 24 hours, within **4 hours** of that later classification (Art. 5(2)); intermediate report within **72 hours** of initial notification (updated on recovery); final report within **1 month** of the intermediate or latest updated intermediate report (Art. 5(1)) [S26][S27][S74]	Financial Supervisory Authority (FIN-FSA) via FISA web form (mandatory from 11 Feb 2026) [S26]
Critical Infrastructure Act (310/2025, CER)	Significant incident disrupting or capable of disrupting essential services at a designated critical entity (Section 2 excludes banking, financial-market and digital infrastructure from Sections 14 to 16 duties, plus defence, national security and specified state bodies)	Initial notification without undue delay and within **24 hours** of awareness (barring operational impossibility); detailed report where required within **1 month** of awareness (Section 16) [S22]	Initial notice to sector supervisory authority and **Government Situation Centre (Valtioneuvoston tilannekeskus)**; detailed report to coordinating ministry, sector ministry and supervisory authority (Section 16) [S22]
Cyber Resilience Act (EU 2024/2847, Arts. 14 and 71)	Manufacturer awareness of an **actively exploited vulnerability** or a **severe incident** affecting the security of a product with digital elements (applies from **11 Sep 2026**; broader CRA applies **11 Dec 2027**)	Early warning within **24 hours** of awareness; vulnerability or incident notification within **72 hours** of awareness; final report within **14 days** after a corrective or mitigating measure is available (actively exploited vulnerabilities) or within **1 month** after the 72-hour notification (severe incidents) (Art. 14) [S75]	Coordinator CSIRT (NCSC-FI in Finland) and **ENISA** simultaneously via the CRA Single Reporting Platform [S75]
Criminal investigation	Suspected aggravated data breach, espionage or fraud	Prompt police report preserving forensic logs and evidence [S33][S43][S49]	Finnish Police / National Bureau of Investigation (KRP) or Åland Police [S33][S76]

Under DORA Delegated Regulation 2025/301 Article 5(3)-(5), entities unable to meet a deadline must notify the authority before expiry with reasons [S74]. Weekend or bank-holiday deferral to noon the next working day does not apply to initial or intermediate reports from credit institutions, central counterparties, trading-venue operators or NIS2 essential and important financial entities [S74].

10.3 Practical compliance lessons from 2026 Finnish cases

Two operational lessons stand out from 2026 disclosures. First, **controller versus processor boundaries matter on day one**. In Finnair's Amadeus disclosure (`Case T`), Amadeus filed GDPR notification as controller while Finnair rotated bookings and informed passengers [S35]. In Eckerö Line (`Case R`) and Aalto EE (`Case I`), supplier delays shaped legal awareness [S37][S44]. Second, **statutory maximums are exposure ceilings, not forecasts**. Boards should maintain documented scope assessments, delegated Suomi.fi / FISA filing rights and preserved decision logs. Unverified underground claims are not automatic filing triggers.

KEY TAKEAWAYS

01

Finland's NIS2, CER, GDPR, DORA and CRA rules run on separate legal clocks and portals.

02

Verify delegated FISA and NCSC-FI reporting access before normal identity systems are disrupted.

03

Document controller-processor roles and log awareness and classification times independently.

CHAPTER 11

Outlook and conditional planning scenarios

11

THIS CHAPTER ANSWERS

Which concrete triggers should shift Finnish defensive posture after 22 November 2026?

4

conditional planning scenarios tied to owned evidence

11.1 Key judgements and evidential limits 79

11.2 Four conditional planning scenarios 80

11.3 What would change this assessment 80

CHAPTER 11

Outlook and conditional planning scenarios

IN SHORT

The 2026 evidence justifies sustained readiness for edge-software zero-days, supplier data exposure, interactive strong-ID phishing and unsegmented operational controllers. It does not establish a single coordinated actor behind Finland's diverse incidents or predict attack probabilities. Use the four conditional scenarios below to link validated internal signals to pre-agreed technical, legal and communications actions.

11.1 Key judgements and evidential limits

Judgement	Basis and confidence	Key limit	Owned decision
Internet-facing edge appliances and web runtimes will remain rapid initial-access vectors	High based on Valtori Ivanti EPMM, Citrix NetScaler Finland intrusions and PHP flaws [S14][S15][S32]	Patching velocity varies across sectors; zero-day timing is unpredictable	Maintain an emergency edge-isolation roster and pre-patch hunting checklist
Supplier and legacy-archive breaches will continue generating downstream customer phishing risk	High based on Amadeus/Finnair, Canvas/Aalto EE, Eckerö Line and Kolmostien Terveys disclosures [S35][S37][S39][S44]	Each incident involves separate controllers and unmerged populations	Audit SaaS/subcontractor notice clauses and purge obsolete handover archives
Interactive phishing and strong-ID chaining threaten both banks and non-bank enterprises	High based on Finance Finland 20,000 attempts, NCSC-FI M365 surges and SALTA3 / eSIM underground ads [S1][S7][S30]	Underground ads do not measure campaign conversion or exact bank losses	Enforce phishing-resistant MFA, block Device Code Flow and harden eSIM/ID enrolment
Extortion and intrusion-recovery readiness remains necessary across manufacturing, services and utilities	High for 16 unverified Ransompedia listings [S2]; separately, two confirmed Finnish intrusion disclosures are reported by role only [S49][S50]	Repeat entries and general 0apt claim caution limit raw listing counts [S54]	Verify immutable backup recovery and separate forensic verification from leak-site noise
Unsegmented OT controllers pose localised physical-disruption risk	High for NCSC-FI refrigeration advisories and proactive outreach [S16][S18][S19]	NCSC-FI noted prior OT preparedness and outreach helped avoid major damage; no actor attribution was published [S18][S19]	Remove controllers from public internet and verify safe local manual overrides
External identity exposure requires sustained account triage	High for the 248-domain assessed portfolio (national Atlas headline 45/100; 41 current listings; 148 with employee devices) [S4]	Cumulative portfolio signals are not national prevalence or confirmed intrusions; 2 domains remain unknown	Validate current credential listings within five working days and separate staff from customer queues

11.2 Four conditional planning scenarios

Scenario A: Critical edge-appliance or web-runtime zero-day advisory arrives

If NCSC-FI issues a severe warning on an internet-facing gateway, MDM server or web runtime before patches ship, invoke pre-authorised isolation or DMZ closure (`Case R`). Collect volatile logs before rebooting and hunt for pre-patch persistence after patching (`Case Q`). If the product is internal-only with verified network isolation, document the boundary and patch on the expedited window without unnecessary public outage.

Scenario B: A key supplier or subcontractor revises breach scope after initial notice

If a supplier expands breach scope to Finnish personal identity codes, inbox messages or active bookings (`Cases I and T`), rotate active tokens and reservation codes immediately. For an in-house scope expansion, see `Case H` . Update GDPR, NIS2 and DORA assessments and publish plain guidance on what exposed fields cannot authorise. If subsequent forensics narrow exposure to historical non-sensitive data, retain both notices and close heightened alerts cleanly.

Scenario C: An underground listing or credential file names your Finnish organisation

An authorised threat alert may flag a forum database post (`Case A` , `Case B`), credential extract (`Case E`) or extortion listing (§7.1). Validate sample schemas and user accounts against live systems and historical breach archives first. Confirm whether unrelated URL collisions or cross-forum sample reuse explains the posting before triggering breach notifications or customer password resets.

Scenario D: An operational controller or public service faces disruption or hacktivist claims

If local engineering telemetry confirms unexpected parameter changes on refrigeration, energy or building controllers (`Case S`), trigger physical isolation and manual fallback immediately and notify NCSC-FI and police. If a hacktivist channel claims a DDoS takedown (`§6.2`), validate real uptime metrics, engage network-provider mitigation and publish factual status updates without repeating actor rhetoric.

11.3 What would change this assessment

Validated technical evidence linking multiple Finnish intrusions to shared infrastructure or credentials would justify elevating cross-sector campaign warnings. Confirmation of active, unmitigated staff accounts among the 41 domains with current credential listings, or exposure observations for the 2 currently unassessed domains, would also alter sector triage priorities. Conversely, confirmed historical provenance, corrected feed country tags or migration of the 94 monitoring-only Finnish domains to full-coverage `quarantine` or `reject` DMARC policies would materially narrow specific exposure judgements.

KEY TAKEAWAYS

01

Pair every key judgement with its evidential boundary so leadership invests in verified controls.

02

Activate isolation, supplier-update, claim-triage and OT-fallback playbooks on validated local triggers.

03

Reassess exposure triage whenever validated account checks confirm active credentials or close historical signals.

CHAPTER 12

Action plan and completion evidence

12

THIS CHAPTER ANSWERS

Who acts, on which trigger, and what shows the control actually works?

30 / 60 / 90

assurance milestones; urgent edge and identity containment starts today

12.1 Priority action lanes and completion evidence 83

12.2 Vulnerability remediation reference 85

12.3 Supporting continuous validation 87

CHAPTER 12

Action plan and completion evidence

IN SHORT

Urgent edge-appliance patching, exposed OT removal and active account containment begin immediately rather than waiting for quarterly reviews. Use the 30, 60 and 90-day lanes below to assign a named technical owner and business owner to each Finnish priority, requiring verifiable test evidence rather than paper policies to mark work complete.

12.1 Priority action lanes and completion evidence

1**Immediate (0-7 days)**

Inventory all internet-facing edge gateways, MDM servers, PHP web interfaces and OT/refrigeration controllers; apply the fixed releases in §12.2 (or replace unsupported End-of-Life devices), remove exposed OT from public internet and pre-authorise emergency DMZ cut-offs

OWNER

Infrastructure, OT engineering and CISO

COMPLETION EVIDENCE

Signed external-asset register, patch verification logs and approved emergency isolation runbook

Audit Microsoft 365 and identity tenants for anomalous sign-ins, inbox forwarding rules and OAuth app grants; block unnecessary Device Code Flow via Conditional Access and validate any current credential listing within five working days

OWNER

Identity and SOC leads

COMPLETION EVIDENCE

Conditional Access policy export, dated listing dispositions and clean sign-in / OAuth audit record

2**30 days**

Reconcile employee-classified device associations against managed endpoint inventories, revoke exposed sessions and keep non-employee device signals routed to fraud protection

OWNER

Endpoint, identity and fraud leads

COMPLETION EVIDENCE

Reconciled device-triage register with dated revocations or documented closure

Move monitoring-only domains (`p=none`) to full-coverage `quarantine` or `reject` DMARC policies, verify SPF/DKIM alignment and confirm protected Finnish SMS Sender ID registration with Traficom

OWNER

Messaging security and brand owner

COMPLETION EVIDENCE

Live DNS DMARC verification across owned domains and Traficom Sender ID confirmation

Verify delegated reporting credentials and backup access for FIN-FSA FISA (DORA), NCSC-FI / NIS2, Data Protection Ombudsman (and Åland authorities where applicable by activity and statute); log separate awareness and classification workflows

OWNER

Legal, compliance and CISO

COMPLETION EVIDENCE

Tested portal access screenshot, delegated backup roster and updated incident-clock playbook

3**60 days**

Audit legacy handover archives (including pre-2023 municipal/health transfers) and removable media policies; review customer-lookup API authentication and rate limits; test customer-support scripts against real-context impersonation

OWNER

Data protection, API engineering and customer operations

COMPLETION EVIDENCE

Archive-purge certificate, API penetration-test report and completed support tabletop notes

For banks and telecom-linked services, test interactive phishing defences and cross-channel eSIM / Mobile Certificate step-up controls; rehearse booking/token rotation for travel and retail suppliers

OWNER

Fraud operations, digital channels and vendor risk

COMPLETION EVIDENCE

Signed control-test report and updated supplier notification SLA register

4**90 days**

Conduct a joint restoration and continuity exercise (aligned with TIBER-FI, NIS2 or CER obligations) covering supplier outage, immutable backup restore from ransomware and public status communication without actor rhetoric

OWNER

Executive sponsor, continuity lead and CISO

COMPLETION EVIDENCE

Dated exercise after-action report, measured recovery times and accepted residual-risk register

12.2 Vulnerability remediation reference

The table below lists affected and fixed versions from current NVD, CVE CNA and vendor records for the CVEs highlighted in this report, including replacement guidance where no supported upstream fix exists. Historical minimum builds for earlier CVEs do not substitute for later cumulative security releases on supported branches:

Product and CVEs	Affected versions	Fixed versions and replacement guidance	Sources
Ivanti Endpoint Manager Mobile (`CVE-2026-1281` , `CVE-2026-1340`)	EPMM `12.5.0.0` , `12.5.1.0` , `12.6.0.0` , `12.6.1.0` , `12.7.0.0` and earlier `12.x` builds	Upgrade to Ivanti EPMM `12.8.0.0` or the latest supported `12.8.x` security release, or apply the branch-matched RPM package from Ivanti's advisory [S81][S82]. Ivanti's updated RPM packages are `ivanti-security-update-1761642-1.1.0S-5.noarch.rpm` (`12.5.0.0` , `12.6.0.0` and `12.7.0.0`) and `ivanti-security-update-1761642-1.1.0L-5.noarch.rpm` (`12.5.1.0` and `12.6.1.0`) [S81] [S82]. Replace unsupported branches and inspect exposed consoles for pre-patch persistence.	[S59][S60][S81][S82]
Citrix NetScaler ADC and Gateway (`CVE-2026-88771` , `CVE-2026-88772` ; NCSC-FI warning 1/2026 lists eight CVEs `CVE-2026-88771` to `CVE-2026-88778` ; superseded by 12 Nov `CTX697305` incl. `CVE-2026-120868`)	For Sep zero-days: `14.1` before `14.1-73.37` , `13.1` before `13.1-64.23` , `14.1` FIPS before `14.1-73.37` FIPS, `13.1` FIPS/NDcPP before `13.1-37.279` . For 12 Nov `CTX697305` (`CVE-2026-120868`): `14.1` before `14.1-73.57` , `13.1` before `13.1-64.39` , `14.1` FIPS before `14.1-73.58` FIPS, `13.1` FIPS/NDcPP before `13.1-37.293` (plus EOL branches).	Historical September minima for `CVE-2026-88771` to `CVE-2026-88778` were `14.1-73.37` , `13.1-64.23` , `14.1-73.37` FIPS and `13.1-37.279` FIPS/NDcPP [S80]. For current remediation covering Citrix's 12 November update (`CTX697305` , `CVE-2026-120868`), upgrade to `14.1-73.57` , `13.1-64.39` , `14.1-73.58` FIPS or `13.1-37.293` FIPS/NDcPP (or later supported builds) [S87]. Migrate End-of-Life branches to a supported build, hunt for pre-patch persistence and rotate session secrets.	[S14][S61][S62][S80][S87]

Product and CVEs	Affected versions	Fixed versions and replacement guidance	Sources
PHP (`CVE-2026-109618` , `CVE-2026-109619` ; plus separate 19 Nov advisory `CVE-2026-115560` / `GHSA-658j-r8rw-q6mx`)	For `CVE-2026-109618` / `109619` : PHP `8.5` before `8.5.12` , `8.4` before `8.4.27` , `8.3` before `8.3.36` , `8.2` before `8.2.35` , and unsupported `8.1` and older (`7.3.0+` / `5.4.0+`). For separate `CVE-2026-115560` : PHP `8.5` before `8.5.13` , `8.4` before `8.4.28` , `8.3` before `8.3.37` , `8.2` before `8.2.36` (including the October releases) and unsupported `5.4.0+` branches.	Historical October minima for `CVE-2026-109618` / `109619` were `8.5.12` , `8.4.27` , `8.3.36` and `8.2.35` . For current remediation incorporating the 19 November `CVE-2026-115560` fix, upgrade to `8.5.13` , `8.4.28` , `8.3.37` or `8.2.36` (or `8.6.0` / later supported releases or OS/LTS backports) [S72][S85]. Migrate End-of-Life `8.1` and older (PHP `8.2` reaches EOL 31 December 2026); updating remains necessary because no interim setting makes an installation safe [S72]. `CVE-2026-115560` requires session upload progress enabled, mismatched `session.serialize_handler` settings across runtime or shared session stores, and a gadget chain for RCE [S85]. The 19 November fix disables `session.upload_progress.enabled` by default, but explicit configs override it, and the fix does not enforce matching serializers across shared stores [S85]. Keep `session.upload_progress.enabled=0` before request parsing (`php.ini` , FPM pool or server config, not `ini_set()` or `.user.ini`) with workers restarted, or align serializers across shared stores [S85]. For `CVE-2026-109619` , that setting blocks confirmed session paths only, not other variants.	[S15][S63][S64][S72][S85][S86]

Product and CVEs	Affected versions	Fixed versions and replacement guidance	Sources
Zimbra Collaboration (`CVE-2025-66376`)	Zimbra Collaboration (ZCS) `10.0` before `10.0.18` and `10.1` before `10.1.13` (Classic UI stored XSS)	Historical minimum for `CVE-2025-66376` is `10.1.13` ; upgrade to the latest supported `10.1.x` security release [S78]. Although `10.0.18` also patched the flaw, the `10.0` branch reached End of Life on 31 December 2025, so migrate `10.0` and older deployments to supported `10.1.x` releases.	[S65][S78]
TP-Link SOHO routers (`CVE-2023-50224`)	Legacy End-of-Life models including `TL-WR841N` (`v11` before `11_211209` , `v12` before `12_230317`) and numerous unpatched EOL routers and access points	Replace unpatched End-of-Life hardware with vendor-supported models receiving regular security updates; where interim firmware exists, apply the latest firmware, disable internet remote management and change default credentials	[S52][S66][S77]

12.3 Supporting continuous validation

Organisations seeking tailored visibility into domain exposure, stealer-credential alerts, lookalike domains and underground claims targeting Finnish brands can request a Brandefense briefing at Brandefense demo request.

KEY TAKEAWAYS

01

Start edge isolation, exposed OT removal and M365 Device Code Flow blocking immediately.

02

Close the 94-domain monitoring DMARC gap and test FISA and NIS2 reporting access within 30 days.

03

Require dated restoration, API and continuity test evidence to mark milestones complete.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Method, scope and exclusions · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

87
sources

Appendix A. Method, scope and exclusions 89
Appendix B. Evidence register 92
Appendix C. Sources 93
Appendix D. Glossary 98

Appendix A. Method, scope and exclusions

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

A.1 Observation window and evidence separation

Distinct observation windows and snapshot dates apply throughout this report. The 2026 activity window covers **1 January to 22 November 2026** (UTC, by publication timestamp) for underground posts, Ransompedia listings, 2026 domain mentions and public events [S1][S2][S4]. Within that window, **8 to 22 November 2026** is examined separately in §5.3 [S1]. Rolling 365-day domain mentions span **23 November 2025 to 22 November 2026**, reported separately from the 2026 subset [S4].

Brandefense Atlas exposure assessments (248 of 250 selected domains) and the passive domain configuration snapshot (all 250 domains) are dated **24 November 2026** [S3][S4]. All external advisories, legislative records, industry fraud statistics and press sources were verified on **24 November 2026**. Every source supports only its own proposition.

A.2 Underground post volume and corpus boundary

The observed Finland-tagged post population totals **749,602** [S1]. January (411,036) and February (315,239) together comprise **726,275 posts (96.9%)**, including 726,240 on Telegram and 723,961 tagged Turkish [S1]. In one review, 622 of 627 January-February posts were repetitive commercial Telegram promotions [S1]. The cited cases and excerpts come from a narrower retained corpus. That corpus is not a complete census of everything published. November is partial through 22 November.

A.3 Selected 250-domain portfolio and configuration snapshot

The passive portfolio comprises **250 DNS-verified Finnish domains** across ten equal sector cells of 25 domains each, snapshotted on **24 November 2026** [S3]. Selection is purposive and does not represent a statistical census of all Finnish entities. Mail-policy counts reflect published policy categories rather than demonstrated enforcement coverage or receiver behaviour (§3.5) [S67]. DNSSEC, TLS and HSTS counts preserve their assessed denominators; unavailable HTTP or TLS results (including 12 government portals) are counted separately rather than treated as failures [S3].

A.4 Selected-domain exposure assessments and mentions

Brandefense Atlas exposure observations cover **248 of the 250 selected domains** on the **24 November 2026** snapshot (two days after the 22 November activity-window close) [S4]. Exposure remains unknown for 2 selected domains (1 in telecom and digital services, 1 in health and wellbeing services), and missing observations are never treated as zero [S4]. Only the single national Atlas headline (**45/100**) is published; no per-sector, per-group or organisation exposure ratings appear anywhere in this report.

Portfolio exposure signals comprise cumulative device associations (at least 128,734; 5,690 employee), historical credential records (2,245,122), document associations (2,484), 30-day similar-name observations (26,678) and current credential listings (41 domains) [S4]. These signals may overlap and do not represent unique people, 2026-only activity or confirmed incidents [S4]. Separately, rolling 365-day dark-chat (49 domains, 941 mentions) and dark-web (56 domains, 662 mentions) observations cover all 250 domains from **23 November 2025 to 22 November 2026**, with the 2026 subset labelled separately [S4]. Licensed card-issuing bank figures in §9.1 cover a strict 12-domain subset of the 25-domain banking and finance cell and retain their smaller denominator [S4].

A.5 Ransomware listings

The **16 Finland-labelled listings** recorded in Ransompedia through 22 November 2026 (and 11 across full-year 2025) count public criminal assertions rather than confirmed intrusions or unique victims [S2]. Two repeat listings (INC Ransom and Clop) reduce distinct entries to at most 14, and the three February 0apt entries remain unverified alongside Halcyon's general caution about inflated early 0apt claims [S2][S54]. Prior-year comparator numbers cover full-year 2025 while 2026 covers through 22 November.

A.6 Payment-card scope

SCOPE OF THE CARD FIGURES

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

The retained corpus contains **73 distinct Finland-labelled card records** (109 occurrences across 83 posts, 41 BINs) and **1,711 offer posts** without clear-text card numbers (1,520 shop updates) [S1]. Neither count verifies issuance, stolen status, live balance or bank intrusion [S1].

A.7 Public incidents, exclusions and naming discipline

Fourteen public-event dossiers (`Cases H-U`) and seven underground claim cases (`Cases A-G`) document supported findings.

Three categories of material are excluded from the 2026 Finnish cyber-incident count. First, the August 2026 Helsinki Court of Appeal jurisdictional ruling in the December 2024 Eagle S subsea-cable case is a judicial milestone on a 2024 maritime event rather than a 2026 cyber intrusion [S57]. Second, Data Protection Ombudsman decision `2026/10` addresses an administrative privacy ruling rather than a new 2026 attack [S23][S24]. Third, March Telegram claims by Morningstar alleging access to Finnish apartment cameras were excluded because the Finnish intrusion claim remains unverified [S1].

An affected organisation is named only when **both** officially confirmed and widely reported in national or regional press. Confirmed Finnish notices without accessible wide press reporting (`Case K`) are presented by broad role with domains and URLs omitted [S49]. Cases N and O are confirmed and regionally reported events presented by role, with organisation domains and URLs omitted [S41][S42][S50].

Where press reporting names an unconfirmed or unregistered affected body (`Cases H, P and S`), only the press publisher's site root is cited with the article URL withheld [S33][S45][S48]. External public sources carry verified links except where a URL is withheld under this rule.

Appendix B. Evidence register

Authentic excerpts are shown inline in the chapters listed below. Post dates reflect publication time; no card establishes a completed transaction or confirmed intrusion on its own.

Card	Date	Venue	Alias	Language	Section
B01	2026-02-18	Forum thread	Alias withheld	English	§4
B02	2026-04-04	Forum thread	Alias withheld	English	§4
B03	2026-10-09	Forum thread	Alias withheld	English	§4
B04	2026-02-24	Forum thread	Alias withheld	English	§4
B05	2026-04-13	Forum thread	Alias withheld	English	§4
B06	2026-05-26	Forum thread	Alias withheld	English	§4
B07	2026-09-25	Forum thread	Alias withheld	English	§4
B08	2026-02-11	Forum thread	Alias withheld	Russian	§4
B09	2026-04-29	Forum thread	Alias withheld	English	§4
B10	2026-04-08	Forum thread	Alias withheld	Russian / English	§8
B11	2026-05-31	Forum thread	Alias withheld	Russian	§8
B12	2026-10-24	Forum thread	Alias withheld	Russian	§8
B13	2026-11-22	Forum thread	Alias withheld	English	§4
B14	2026-11-17	Forum thread	Alias withheld	English	§4
B15	2026-11-20	Forum thread	Alias withheld	English	§9
B16	2026-01-22	Forum thread	Alias withheld	English	§9

Appendix C. Sources

S1: Odin by Brandefense. Retained underground observations and publication counts (1 January to 22 November 2026; recent window 8 to 22 November 2026). URL withheld; source mapping retained. Verified on 2026-11-24.

S2: Ransompedia. Country-labelled ransomware listings (1 January to 22 November 2026 and full-year 2025). URL withheld; source mapping retained. Verified on 2026-11-24.

S3: Odin by Brandefense. Configuration snapshot of 250 selected Finnish domains (24 November 2026). URL withheld; source mapping retained. Verified on 2026-11-24.

S4: Brandefense Atlas and Odin by Brandefense. Exposure observations for 248 assessed Finnish domains (24 November 2026). Rolling 365-day dark-chat and dark-web mention counts across all 250 selected domains (23 November 2025 to 22 November 2026; 2026 subset 1 January to 22 November 2026). URL withheld; source mapping retained. Verified on 2026-11-24.

S5: Traficom / NCSC-FI. Cyber Threat Landscape 2025 (Kybertilannekuva 2025). https://vuosiraportit.traficom.fi/fi/kyberturvallisuuden-vuosi-2025/kybertilannekuva-2025 Verified on 2026-11-24.

S6: Traficom / NCSC-FI. First half of 2026 cybersecurity review, 15 June 2026. https://www.traficom.fi/fi/uutiset/kyberturvallisuuden-ensimmainen-vuosipuolisko-2026-kyberuhkien-torjuminen-vaatii-vahvempaa-varautumista-ja-resursointia Verified on 2026-11-24.

S7: NCSC-FI (Traficom). February 2026 Cyber Weather PDF (Kybersää helmikuu 2026), 15 April 2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20helmikuu%202026.pdf Verified on 2026-11-24.

S8: NCSC-FI (Traficom). Weekly Review 13/2026 (WhatsApp BEC, ClickFix, `.fi` removals, SMS Sender ID deadline 4 May 2026), 27 March 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-132026 Verified on 2026-11-24.

S9: NCSC-FI (Traficom). May 2026 Cyber Weather PDF (Kybersää, toukokuu 2026), 11 June 2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4,%20toukokuu%202026.pdf Verified on 2026-11-24.

S10: NCSC-FI (Traficom). June 2026 Cyber Weather PDF (Kybersää kesäkuu 2026), 2 July 2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20kes%C3%A4kuu%202026.pdf Verified on 2026-11-24.

S11: NCSC-FI (Traficom). July 2026 Cyber Weather PDF (Kybersää heinäkuu 2026), 13 August 2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20hein%C3%A4kuu%202026.pdf Verified on 2026-11-24.

S12: NCSC-FI (Traficom). August 2026 Cyber Weather (Elokuun Kybersää 2026), 10 September 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/elokuun-kybersaa-2026 Verified on 2026-11-24.

S13: NCSC-FI (Traficom). September 2026 Cyber Weather (Syyskuun kybersää 2026), 15 October 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/syyskuun-kybersaa-2026 Verified on 2026-11-24.

S14: NCSC-FI (Traficom). Citrix NetScaler vulnerabilities exploited in Finland, 1 October 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/citrix-netscaler-haavoittuvuuksia-hyvaksikaytetty-suomessa Verified on 2026-11-24.

S15: NCSC-FI (Traficom). Critical vulnerabilities in PHP (advisory 37/2026; published 21 October 2026, updated 30 October 2026; lists CVE-2026-109618, CVE-2026-109619 and CVE-2026-115560). https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-37 Verified on 2026-11-24.

S16: NCSC-FI (Traficom). IoT and OT security starts with protecting devices, 3 November 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/iot-ja-ot-ymparistojen-tietoturva-alkaa-laitteiden-suojaamisesta Verified on 2026-11-24.

S17: NCSC-FI (Traficom). October 2026 Cyber Weather (Lokakuun Kybersää 2026), 12 November 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/lokakuun-kybersaa-2026 Verified on 2026-11-24.

S18: NCSC-FI (Traficom). Weekly Review 45/2026 (proactive refrigeration-controller outreach from 13 October, National Risk Assessment, Taisto exercise), 6 November 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-452026 Verified on 2026-11-24.

S19: NCSC-FI (Traficom). Weekly Review 46/2026 (bank-spoofing robocalls, home IoT and refrigeration incidents), 13 November 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-462026 Verified on 2026-11-24.

S20: NCSC-FI (Traficom). Weekly Review 47/2026 (Black Friday phishing, residential-proxy abuse and EU CRA Finnish guidance), 20 November 2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-472026 Verified on 2026-11-24.

S21: Finlex. Cybersecurity Act (Kyberturvallisuuslaki 124/2025). https://www.finlex.fi/fi/lainsaadanto/2025/124 Verified on 2026-11-24.

S22: Finlex. Act on Protection and Resilience of Critical Infrastructure (310/2025). https://www.finlex.fi/fi/lainsaadanto/2025/310 Verified on 2026-11-24.

S23: Finlex. Data Protection Act (Tietosuojalaki 1050/2018). https://www.finlex.fi/fi/lainsaadanto/2018/1050 Verified on 2026-11-24.

S24: Finlex. Office of the Data Protection Ombudsman decision 2026/10 on unauthorised e-invoice access, 31 March 2026. https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2026/10 Verified on 2026-11-24.

S25: KT (Local and County Government Employers). Government proposal to extend data-protection administrative fines to public-sector bodies, 2026. https://www.kt.fi/uutiset-ja-tiedotteet/2026/hallitus-esittaa-seuraamusmaksua-tietosuojarikkomuksesta-myos-julkiselle Verified on 2026-11-24.

S26: FIN-FSA (Finanssivalvonta). Supervisory release 4/2026: DORA incident-reporting delivery shifts to FISA web form from 11 February 2026, 19 January 2026. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2026/hairioilmoitusten-toimitustapa-muuttuu/ Verified on 2026-11-24.

S27: FIN-FSA (Finanssivalvonta). DORA regulatory overview, 2026. https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/dora/ Verified on 2026-11-24.

S28: Bank of Finland (Suomen Pankki). TIBER-FI threat-led penetration testing framework, 2026. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/tiber-fi-toimintamalli/ Verified on 2026-11-24.

S29: Finance Finland (Finanssiala ry). 2025 bank-reported digital fraud figures, 3 February 2026. https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-huijata-148-miljoonaa-euroa-vuonna-2025/ Verified on 2026-11-24.

S30: Finance Finland (Finanssiala ry). First half of 2026 bank-reported digital fraud figures, 16 September 2026. https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-alkuvuonna-huijata-60-miljoonaa-euroa-huijausyritysten-lukumaarat-hurjassa-kasvussa/ Verified on 2026-11-24.

S31: Digital and Population Data Services Agency (DVV / Suomi.fi). Warning on phishing messages impersonating Suomi.fi, 2 September 2026. https://www.suomi.fi/uutiset/varo-liikkeella-olevia-suomi-fin-nimissa-liikkuvia-huijausviesteja Verified on 2026-11-24.

S32: AfterDawn (dawn.fi). Scope of Valtori mobile-device-management breach expands up to 50,000 users, 6 February 2026. https://dawn.fi/uutiset/2026/02/06/valtori-tietomurto Verified on 2026-11-24.

S33: Demokraatti (STT / Yle). Valtori breach affected devices at additional central-government organisations, 7 May 2026. https://demokraatti.fi (article URL withheld to protect unnamed organisation). Verified on 2026-11-24.

S34: Demokraatti (STT). Valtori precautionary shutdown of central-government public web services over PHP vulnerabilities, 21 October 2026. https://demokraatti.fi/valtori-valtionhallinnon-verkkopalveluja-ajetaan-alas-varotoimena Verified on 2026-11-24.

S35: Finnair (Cision). Official release: Amadeus global reservation breach involving Finnair and Aurinkomatkat, 9 November 2026. https://news.cision.com/fi/finnair/r/amadeuksen-globaalissa-tietovuodossa-on-ollut-mukana-myos-finnairin-asiakkaiden-tietoja,c4422110 Verified on 2026-11-24.

S36: Lentoposti.fi. Amadeus reservation-system breach reporting including Finnair passenger records, November 2026. https://www.lentoposti.fi/uutiset/tietomurto_amadeuksen_j_rjestelmiin_kohteena_lentoyhti_iden_matkustajalistat_mukana_finnair_tietoja Verified on 2026-11-24.

S37: Aalto EE. Data Breach Notification: Canvas Learning Platform, 7 May 2026. https://www.aaltoee.fi/en/newsroom/2026/data-breach-notification-canvas-learning-platform Verified on 2026-11-24.

S38: Aalto University. Canvas learning platform data breach notice clarifying no institutional licence, 11 May 2026. https://www.aalto.fi/en/news/canvas-learning-platform-data-breach-there-may-be-users-at-aalto Verified on 2026-11-24.

S39: Wellbeing Services County of Pirkanmaa (Pirkanmaan hyvinvointialue, STT Info). Breach of legacy Kolmostien Terveys file exposing 10,263 personal identity codes, 25 August 2026. https://www.sttinfo.fi/tiedote/72261363/tietomurto-kolmostien-terveyden-tietoja-sisaltaneeseen-tiedostoon-on-aiheuttanut-tietoturvaloukkauksen?publisherId=69818823&lang=fi Verified on 2026-11-24.

S40: Wellbeing Services County of Pirkanmaa (Pirkanmaan hyvinvointialue, STT Info). Flea-market USB drive breach in Akaa and Urjala, 13 January 2026. https://www.sttinfo.fi/tiedote/71732462/kirpputorilta-loytynyt-muistitikku-aiheutti-tietoturvaloukkauksen-akaassa-ja-urjalassa?publisherId=69818823&lang=fi Verified on 2026-11-24.

S41: Municipal library notice; identity withheld. Denial-of-service attack targeting shared Koha library systems, September 2026. URL withheld to protect the affected municipality; source mapping retained. Verified on 2026-11-24.

S42: Regional library notice; identity withheld. Shared Koha library-system DDoS notice, September 2026. URL withheld to protect the affected municipality; source mapping retained. Verified on 2026-11-24.

S43: Rahaliike Holmasto. Customer-register API breach notification, updated 15 September 2026. https://www.holmasto.fi/tietoturvaloukkaus/ Verified on 2026-11-24.

S44: Eckerö Line. Booking-system subcontractor cyberattack notification, October 2026. https://www.eckeroline.fi/blog/tarkeaa-tietoa-henkilotietojesi-turvallisuudesta Verified on 2026-11-24.

S45: Nya Åland. Regional press report on a police filing over a data intrusion at an Åland-based organisation, September 2026. https://www.nyan.ax (article URL withheld). Verified on 2026-11-24.

S46: Ryde Technology. Security incident notice for 2 August 2026 breach, updated 5 August 2026. https://www.ryde-technology.com/security-incident-2026-08-02 Verified on 2026-11-24.

S47: Lyko. Official press notice on contained system intrusion, November 2026. https://lyko.com/no/om-lyko/media/pressemeldinger/lyko-har-atgardat-dataintrang-i-en-avgransad-del-av-sitt-system Verified on 2026-11-24.

S48: AfterDawn (dawn.fi). European retail refrigeration cyberattacks and brief Finnish grocery cold-storage disruptions, November 2026. https://dawn.fi (article URL withheld to protect unconfirmed retailer). Verified on 2026-11-24.

S49: Organisation statement; identity withheld. IT environment intrusion at a Finnish financial and business-services firm, July 2026. URL withheld to protect the victim; source mapping retained. Verified on 2026-11-24.

S50: Organisation statement; identity withheld. Server-environment cyberattack at a Finnish educational and training institution, September 2026. URL withheld to protect the victim; source mapping retained. Verified on 2026-11-24.

S51: Google Threat Intelligence Group. Distinct clusters target individuals of interest to Russia (UNC7005 spoofing Finnish Operations Center), 2026. https://cloud.google.com/blog/topics/threat-intelligence/distinct-clusters-target-individuals-of-interest-to-russia Verified on 2026-11-24.

S52: FBI IC3. PSA260407: Russian GRU exploiting vulnerable routers to steal sensitive information, 7 April 2026. https://www.ic3.gov/PSA/2026/PSA260407 Verified on 2026-11-24.

S53: Aalto University. Research on gamified NoName057(16) DDoS campaigns targeting NATO countries and Finland, 2026. https://www.aalto.fi/fi/uutiset/tutkimus-pelillistetyt-palvelunestohyokkaykset-pyrkivat-psykologiseen-sodankayntiin-nato-maita Verified on 2026-11-24.

S54: Halcyon. 0APT: Credible Technical Depth Despite Inflated Victim Claims, 2026. https://www.halcyon.ai/ransomware-research-reports/0apt-credible-technical-depth-despite-inflated-victim-claims Verified on 2026-11-24.

S55: Suomenmaa (STT). Supo National Security Overview 2026, 10 March 2026. https://www.suomenmaa.fi/uutiset/supo-julkisti-kansallisen-turvallisuuden-katsauksen-terrorismin-uhka-arvio-ennallaan-tekoalysta-uudenlaisia-ongelmia/ Verified on 2026-11-24.

S56: Suomenmaa (STT). National Risk Assessment 2026 highlights cyber operations, AI and data centres, 2 November 2026. https://www.suomenmaa.fi/uutiset/kansallinen-riskiarvio-tuo-esiin-datakeskuksiin-liittyvan-terroriuhan/ Verified on 2026-11-24.

S57: Suomenmaa (STT). Helsinki Court of Appeal jurisdictional ruling in the Eagle S subsea-cable case, August 2026. https://www.suomenmaa.fi/uutiset/hovioikeus-kumosi-karajaoikeuden-paatoksen-eagle-s-aluksen-miehiston-syytteet-merikaapelirikoista-voi-tutkia-suomessa/ Verified on 2026-11-24.

S58: DataReportal. Digital 2026: Finland, 2026. https://datareportal.com/reports/digital-2026-finland Verified on 2026-11-24.

S59: NVD. CVE-2026-1281 (Ivanti Endpoint Manager Mobile), published 29 January 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-1281 Verified on 2026-11-24.

S60: NVD. CVE-2026-1340 (Ivanti Endpoint Manager Mobile), published 29 January 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-1340 Verified on 2026-11-24.

S61: NVD. CVE-2026-88771 (Citrix NetScaler ADC and Gateway), published 27 September 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-88771 Verified on 2026-11-24.

S62: NVD. CVE-2026-88772 (Citrix NetScaler ADC and Gateway), published 27 September 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-88772 Verified on 2026-11-24.

S63: NVD. CVE-2026-109618 (PHP out-of-memory request cleanup), published 21 October 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Verified on 2026-11-24.

S64: NVD. CVE-2026-109619 (PHP global-state use-after-free), published 21 October 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Verified on 2026-11-24.

S65: NVD. CVE-2025-66376 (Zimbra Collaboration Classic UI stored XSS), published 5 January 2026. https://nvd.nist.gov/vuln/detail/CVE-2025-66376 Verified on 2026-11-24.

S66: NVD. CVE-2023-50224 (TP-Link TL-WR841N improper authentication), published 3 May 2024. https://nvd.nist.gov/vuln/detail/CVE-2023-50224 Verified on 2026-11-24.

S67: RFC Editor. DMARC protocol reference (RFC 7489), March 2015. https://www.rfc-editor.org/rfc/rfc7489.html Verified on 2026-11-24.

S68: RFC Editor. SPF protocol reference (RFC 7208), April 2014. https://www.rfc-editor.org/rfc/rfc7208.html Verified on 2026-11-24.

S69: RFC Editor. DKIM signatures reference (RFC 6376), September 2011. https://www.rfc-editor.org/rfc/rfc6376.html Verified on 2026-11-24.

S70: RFC Editor. HTTP Strict Transport Security reference (RFC 6797), November 2012. https://www.rfc-editor.org/rfc/rfc6797.html Verified on 2026-11-24.

S71: Voice.fi. Finnish consumer reporting on the Lyko data breach, November 2026. https://www.voice.fi/ilmiot/teitko-ostoksia-lykossa-tietosi-saattavat-olla-vaarassa-uhka-koskee-pelkastaan-ruotsissa-jopa-50-000-asiakasta Verified on 2026-11-24.

S72: PHP Project. Security releases and 2026 news archive (October and November 2026 security releases). https://www.php.net/archive/2026.php Verified on 2026-11-24.

S73: The Guardian. Shop fridges and freezers across Europe hit by fresh suspected cyber-attack, 2 November 2026. https://www.theguardian.com/world/2026/nov/02/supermarket-freezers-across-europe-hit-by-second-suspected-cyber-attack Verified on 2026-11-24.

S74: European Commission (EUR-Lex). Commission Delegated Regulation (EU) 2025/301, Article 5 (DORA major ICT incident reporting time limits), 20 February 2025. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng Verified on 2026-11-24.

S75: European Parliament and Council (EUR-Lex). Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 14 and 71, 20 November 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng Verified on 2026-11-24.

S76: Datainspektionen (Åland). Åland Data Protection Authority official portal, 2026. https://www.di.ax/ Verified on 2026-11-24.

S77: TP-Link. Security Advisory for CVE-2023-50224: Impact on Legacy TP-Link Router and Access Point Products (FAQ 5058), 2026. https://www.tp-link.com/us/support/faq/5058/ Verified on 2026-11-24.

S78: Zimbra. Zimbra Daffodil 10.1.13 Patch Release resolving CVE-2025-66376, November 2025. https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.13 Verified on 2026-11-24.

S79: Åland Parliament (Ålands lagting). Lagförslag 13/2023-2024: Explanatory commentary on Åland Datainspektionen and national Data Protection Ombudsman supervisory competence (Section 43), 2024. https://www.lagtinget.ax/dokument/lagforslag-132023-2024-57832 Verified on 2026-11-24.

S80: NCSC-FI (Traficom). Warning 1/2026: Critical vulnerabilities in Citrix NetScaler ADC and Gateway, multiple intrusions in Finland, published 1 October 2026 (updated 20 October 2026). https://www.kyberturvallisuuskeskus.fi/fi/varoitukset/citrix-netscaler-adc-ja-gateway-tuotteissa-kriittisia-haavoittuvuuksia-useita-tietomurtoja-suomessa Verified on 2026-11-24.

S81: Ivanti. Security Advisory: Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281 and CVE-2026-1340), 2026. https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US Verified on 2026-11-24.

S82: CISA. Known Exploited Vulnerabilities (KEV) Catalog entry for CVE-2026-1340 identifying Ivanti EPMM RPM packages, 2026. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-1340 Verified on 2026-11-24.

S83: Ylä-Satakunta. Regional press report on Kolmostien Terveys legacy-file breach, 25 August 2026. https://www.ylasatakunta.fi/kolmostien-terveyteen-kohdistui-tietomurto-heinakuussa--yli-10-000-henkilotunnusta-paatyi-vaariin-kasiin-6.184.131488.a15349cb2e Verified on 2026-11-24.

S84: The Guardian. Canvas platform strikes deal with hackers to delete students' stolen data, 12 May 2026. https://www.theguardian.com/technology/2026/may/12/canvas-hacker-deal-student-stolen-data Verified on 2026-11-24.

S85: PHP Project (GitHub Security Advisory). GHSA-658j-r8rw-q6mx: Session serializer mismatch can lead to remote code execution (CVE-2026-115560), 19 November 2026. https://github.com/php/php-src/security/advisories/GHSA-658j-r8rw-q6mx Verified on 2026-11-24.

S86: NVD. CVE-2026-115560 (PHP session upload progress serializer mismatch), published 19 November 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-115560 Verified on 2026-11-24.

S87: NVD. CVE-2026-120868 (Citrix NetScaler ADC and Gateway packet-processing memory overflow, Security Bulletin CTX697305), published 12-13 November 2026. https://nvd.nist.gov/vuln/detail/CVE-2026-120868 Verified on 2026-11-24.

Appendix D. Glossary

- **National Atlas headline.** The single 0 to 100 Brandefense Atlas exposure figure published for the assessed portfolio as a whole; higher values indicate greater observed external exposure and never represent a breach percentage or sector ranking [S4].
- **ClickFix.** Social-engineering technique prompting users to copy and run malicious commands from spoofed web pages or verification prompts [S12].
- **DMARC.** Domain policy specifying how receivers handle and report mail failing aligned authentication checks [S67].
- **SPF.** DNS mechanism declaring authorised sending hosts for a domain [S68].
- **DKIM.** Cryptographic mail signature binding a signing domain to message headers and content [S69].
- **HSTS.** HTTP policy instructing browsers to connect strictly over encrypted HTTPS [S70].
- **DORA / FISA.** EU Digital Operational Resilience Act and FIN-FSA's electronic reporting portal mandatory for Finnish financial-sector incident notices from 11 February 2026 [S26][S27].
- **Kyberturvallisuuslaki (124/2025).** Finland's Cybersecurity Act implementing the EU NIS2 Directive [S21].
- **Henkilötunnus.** Finnish personal identity code; knowledge of this code is context, never sufficient authentication [S39].
- **Mobiilivarmenne / Pankkitunnukset.** Telecom Mobile Certificate and retail-bank credentials used for strong electronic identification across Finland [S30].
- **NCSC-FI.** Finland's National Cyber Security Centre (Kyberturvallisuuskeskus) operating within Traficom [S5].
- **TIBER-FI.** Bank of Finland framework for threat-led red-team testing of critical financial entities [S28].
- **SMS Sender ID.** Alphanumeric sender label protected in Finland through mandatory Traficom registration from 4 May 2026 [S8].
- **AiTM (adversary-in-the-middle).** Phishing technique placing a proxy between a user and a legitimate login page to capture credentials and active session tokens.
- **BIN (bank identification number).** Leading digits of a payment card number (traditionally the first six digits) identifying the card network and issuing institution.
- **KYC (Know Your Customer).** Identity-verification and customer due-diligence checks run by financial institutions and regulated providers before onboarding accounts or services.
- **SEPA (Single Euro Payments Area).** European payment-integration framework harmonising euro-denominated credit transfers and direct debits across participating countries under common standards.
- **TLP:CLEAR.** Shareable without Traffic Light Protocol restriction while observing privacy and statutory duties.

About this report

Prepared by Odin by Brandefense. Version 1.0 applies distinct reference dates. The 2026 activity window runs from 1 January to 22 November 2026 (with 8 to 22 November examined separately), while rolling 365-day domain mentions span 23 November 2025 to 22 November 2026. Exposure assessments (248 of 250 selected domains) and passive configurations (all 250 domains) reflect a 24 November 2026 snapshot. All public sources were verified on 24 November 2026, and 2 selected domains remain unknown in exposure observations.

The Finnish edition translates the English master; the English edition prevails where wording differs. Recommendations require validation against each organisation's own assets, service dependencies and legal obligations.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS

4.7 / 5

COVERAGE

3 pillars

CTI, DRPS, EASM

MONITORING

24 / 7

Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO