BRANDEFENSE COUNTRY REPORT · FINLAND 2026

Brandefense Suomen kyberuhkakatsaus 2026

Reunalaitteiden nollapäivät, toimittaja-altistus ja identiteettiväärinkäyttö Suomen verkottuneissa palveluissa

Odin by Brandefense
Tarkastelujakso: 1.1.–22.11.2026 (UTC; tuore jakso 8.–22.11.)
Versio 1.0 · Julkinen tutkimusjulkaisu · TLP:CLEAR · 24.11.2026

41 / 248
arvioidulla suomalaisella verkkotunnuksella oli tarkistushetkellä myynnissä oleva kirjautumistieto

7
dokumentoitua alamaailman väitetapausta vuodelta 2026

16
Suomeen merkittyä kiristyshaittaohjelmalistausta 8 nimikkeellä

7 / 25
valitulla suomalaisella rahoitusalan verkkotunnuksella oli aktiivinen tunnuslistaus

SISÄLLYS

Sisällys

Translated with AI

Käännetty tekoälyllä englanninkielisestä pääversiosta. Mahdollisissa tulkintaeroissa englanninkielinen versio on ensisijainen.

01	Johdon tiivistelmä ja puolustajan prioriteetit	05
	Raporttikartta	09
02	Suomen digitaalinen profiili ja vuoden 2026 tilannekuva	10
03	Kansallinen altistus ja 250 verkkotunnuksen havainnot	16
04	Alamaailman väitteet ja tapaukset	27
05	Julkiset tietoturvapoikkeamat, toimittajat ja tuore aktiviteetti	40
06	Häiriöt, haktivismi ja väitteet vastaan todellisuus	51
07	Kiristyshaittaohjelmat, vakoiluvaroitukset ja toimijaprofiilit	55
08	Petokset, identiteettiväärinkäyttö ja toissijainen vahinko	64
09	Pankkiala, vahva tunnistaminen ja maksamisen jatkuvuus	71
10	Sääntely, ilmoitusajat ja kansallinen reagointi	76
11	Näkymät ja ehdolliset varautumisskenaariot	81
12	Toimintasuunnitelma ja valmistumisnäyttö	85
A	Liite A. Menetelmä, rajaukset ja poissulkemiset	92
B	Liite B. Todisterekisteri	95
C	Liite C. Lähteet	96
D	Liite D. Sanasto	101
	Tietoja raportista	102

Hallitus ja ylin johto	01 05 10 11 12
Tietoturvajohtaja ja palveluomistajat	03 04 05 10 12
SOC ja uhkatiedustelu	02 04 06 07 12
Petostorjunta ja pankkitoiminnot	05 08 09 12
Tietosuoja, juridiikka ja viestintä	05 06 10 12

Tästä julkaisusta

Käännetty tekoälyllä. Tämä suomenkielinen laitos on käännetty englanninkielisestä pääversiosta (Brandefense Finland Cyber Threat Landscape Report 2026). Mahdollisissa tulkintaeroissa englanninkielinen versio on ensisijainen.

45/100

Kansallinen Atlas-yleisluku 248 arvioidulle verkkotunnukselle (tilannekuva 24. marraskuuta 2026)

749 602

Suomeen merkittyä julkaisua alamaailmassa (1. tammikuuta – 22. marraskuuta 2026; 96,9 % tammi–helmikuussa)

16

Suomeen merkittyä kiristyshaittaohjelmalistausta (1. tammikuuta – 22. marraskuuta 2026; 11 koko vuonna 2025)

60 milj. EUR

Pankkipetosyrityksiä alkuvuonna 2026 (20 000 yritystä; 28,3 milj. EUR menetetty)

Sisällys ja lukupolut

Luku	Kysymys
1 Johdon tiivistelmä	Mitkä löydökset ja päätökset vaativat johdon toimia ensin?
2 Kansallinen profiili	Miten digitalisaatio, viranomaistrendit ja massavolyymi muokkaavat kuvaa?
3 Kansallinen altistus	Mitkä tunnus-, laite- ja sähköpostipolitiikkahavainnot vaativat omistajan tarkistuksen?
4 Alamaailman väitteet	Mitä ilmoitukset, ostopyynnöt ja kierrätetyt aineistot osoittavat?
5 Julkiset tapaukset	Mitkä julkisesti raportoidut tapaukset ja toimittajatiedotteet koskivat Suomea?
6 Häiriöt ja haktivismi	Miten väitteet vertautuvat viralliseen tietoon ja palveluvaikutukseen?
7 Kiristyshaittaohjelmat ja toimijat	Mitä kiristyslistaukset ja vakoiluvaroitukset todentavat?
8 Petokset ja identiteetti	Miten vuodetut henkilötiedot ja alamaailman palvelut ruokkivat huijauksia?
9 Pankkiala ja vahva tunnistaminen	Miten hyökkääjät kohdistavat toimensa pankkitunnistamiseen ja maksamisen jatkuvuuteen?
10 Sääntely	Mikä viranomainen, portaali, peruste ja määräaika pätee Suomessa?
11 Näkymät	Mitkä ehdolliset merkit muuttavat puolustuksen valmiustasoa?
12 Toimintasuunnitelma	Kuka toimii, millä aikataululla ja millä valmistumisnäytöllä?
Liitteet A–D	Rajaukset, todisterekisteri, lähteet ja sanasto

LUKU 01

Johdon tiivistelmä ja puolustajan prioriteetit

01

TÄMÄ LUKU VASTAA

Mitkä vuoden 2026 havainnot vaativat suomalaisilta puolustajilta toimia tänään?

5

päälöydöstä erillisistä todisteaineistoista

1.1 Viisi päälöydöstä johdolle 06

1.2 Neljä välitöntä johdon päätöstä 07

1.3 Raportin rajaus ja vertailumaat 07

LUKU 01

Johdon tiivistelmä ja puolustajan prioriteetit

LYHYESTI

Suomen vuoden 2026 kyberuhkakuvaa määrittävät verkon reunalaitteiden nopea hyväksikäyttö, toimittajavuodot, kasvavat digipetosyritykset ja laaja tunnusaltistus. Marraskuun 24. päivän tilannekuvassa 248 arvioidulla suomalaisella verkkotunnuksella kansallinen Atlas-yleisluku on 45/100, ja 41 verkkotunnuksella oli myynnissä oleva kirjautumistieto. Raaka alamaailman julkaisumäärä vääristyy alkuvuoden massamainonnasta. Varmenna aktiiviset tunnuslistaukset, valtuuta reunalaitteiden eristys, vaadi kalastelunkestävää tunnistautumista ja sulje seurantatilan DMARC-aukot.

1.1 Viisi päälöydöstä johdolle

- **Reunalaitteiden nollapäivähaavoittuvuudet aiheuttivat merkittäviä operatiivisia häiriöitä.** Valtionhallinnon mobiililaitehallintaan murtauduttiin tammikuussa Ivanti EPMM -haavoittuvuuksien kautta, mikä koski jopa 50 000 käyttäjätietoa [S7][S32][S59][S60]. Syyskuun 27. päivänä julkaistut Citrix NetScaler -nollapäivät johtivat Suomessa murtoihin ja Kyberturvallisuuskeskuksen 1. lokakuuta antamaan vakavaan varoitukseen [S13][S14][S61][S62][S80]. Lokakuussa Valtori sulki julkisia verkkorajapintoja varotoimena ennen PHP-päivitysten julkaisua [S15][S34][S63][S64].
- **Toimittaja- ja arkistoaineistovuodot kasvattivat velvoitteita.** Useat merkittävät vuoden 2026 julkiset tapaukset johtuivat ulkoisista varaus- ja oppimistoimittajista [S35][S37][S44]. Pirkanmaalla kaksi sote-alan tapausta liittyi vuotta 2016 edeltäviin sekä vuosien 2020–2021 arkistoaineistoihin [S39][S40]. Tekninen palautuminen toimittajalla ei poista asiakkaisiin kohdistuvaa jatkokalastelun riskiä.
- **Digihuijausyritykset kasvoivat ja identiteettihyökkäykset muuttuivat.** Suomalaispankit tilastoivat vuonna 2025 huijausyrityksiä 148 miljoonan euron edestä ja alkuvuonna 2026 jo 60 miljoonaa euroa 20 000 yrityksessä (vuotta aiemmin 13 600) [S29][S30]. Turvatilihuijausyritykset laskivat alkuvuonna 2026 3,9 miljoonaan euroon (koko vuonna 2025 38,4 milj. euroa; eri jakson pituus) [S29][S30]. Samalla rikolliset siirtyivät käyttämään kalasteltuja pankkitunnuksia eSIM-korttien ja mobiilivarmenteiden hankintaan [S30]. Foorumeilla myytiin samanaikaisesti suomalaisia eSIM-profiileja, väärennettyjä SMS-lähettäjätunnuksia ja viidelle Suomessa toimivalle pankille räätälöityä SALTA3-kalastelupakettia [S1].
- **Kiristyshaittaohjelmalistaukset ylittivät vuoden 2025 tason, mutta vaativat varmennusta.** Ransompedia tallensi 22.11.2026 mennessä 16 Suomeen merkittyä listausta, kun koko vuonna 2025 niitä oli 11 (Norjassa myös 16) [S2]. Kaksi toistuvaa kohdetta rajaa yksilölliset väitteet enintään 14:ään, ja helmikuun kolme samana päivänä julkaistua 0apt-listausta jäävät todentamatta [S2]. Ulkoinen tutkimus esittää yleisen varoituksen 0apt:n alkuvuoden liioitelluista tai virheellisistä uhriväitteistä [S54]. Erikseen kaksi suomalaisorganisaatiota (nimet salattu) vahvisti tietomurron kesällä ja syksyllä 2026 virallisissa tiedotteissa [S49][S50].

- **Tunnusaltistus ja julkisen sektorin DMARC-aukot vaativat eri omistajat.** Marraskuun 24. päivän 2026 tilannekuvassa 248 arvioidulla suomalaisella verkkotunnuksella kansallinen Atlas-yleisluku on **45/100**, ja **41 verkkotunnuksella** oli myynnissä oleva kirjautumistieto (2 verkkotunnusta jää tuntemattomaksi) [S4]. Arvioidut verkkotunnukset kantavat myös vähintään **128 734 laitekytköstä** ja **2 245 122 historiallista tunnistetietuetta** [S4]. Erikseen 24.11.2026 otetussa kokoonpanotilannekuvassa **146 verkkotunnusta 250:stä (58,4 %)** julkaisee karanteenia tai hylkäystä pyytävän DMARC-politiikan (`quarantine` tai `reject`; politiikkaluokka, §3.5) [S3] [S67]. Toiset **94 (37,6 %)** ovat seurantatilassa, eniten kunnissa (18), koulutuksessa (15) ja valtionhallinnossa (13) [S3].

1.2 Neljä välitöntä johdon päätöstä

1. **Valtuuta internetiin näkyvien reunalaitteiden ja verkkopalvelujen nopea eristäminen etukäteen.** Tammikuun MDM-murto, syyskuun NetScaler-murrot ja lokakuun varotoimisulku PHP-haavoittuvuuksissa osoittavat, miksi nopea eristys on valtuutettava ennen päivitysten valmistumista [S14][S32][S34]. Johdon on sovittava ennakkoon, kuka saa katkaista haavoittuvan rajapinnan viiveettä.
2. **Varmenna aktiiviset tunnuslistaukset ja vaadi kalastelunkestävää tunnistautumista.** Valitusta joukosta 41 arvioidulla verkkotunnuksella 248:sta oli tarkistushetkellä myynnissä oleva kirjautumistieto [S4]. Kyberturvallisuuskeskus raportoi myös helmikuun Microsoft 365 -tilimurtojen 67 % kuukausikasvusta ja Device Code Flow -kalastelusta [S6][S7][S9][S11]. Ohjaa tunnushälytykset identiteettitiimille viipymättä, vaadi kalastelunkestävä MFA ja estä tarpeeton laitekoodikirjautuminen [S1].
3. **Siirrä julkiset SPF- ja DKIM-verkkotunnukset seurantatilasta täyden kattavuuden quarantine- tai reject-DMARC-politiikkaan.** Valitun joukon 94 seurantatilassa olevan verkkotunnuksen siirtäminen täyden kattavuuden `quarantine`- tai `reject`-tasolle vaikeuttaa nimissä lähetettävää huijausta aktiivisten Suomi.fi-, vero- ja toimituskalastelujen keskellä [S3][S20][S31][S67].
4. **Erota NIS2-, GDPR-, CER-, DORA- ja CRA-ilmoitusajat toisistaan ennen poikkeamaa.** Kyberturvallisuuslaki (124/2025), kriittisen infrastruktuurin laki (310/2025), tietosuojalaki, Finanssivalvonnan FISA-DORA-ilmoittaminen ja EU:n CRA-valmistajailmoitukset (11.9.2026 alkaen) asettavat eri aikarajat ja vastaanottajat [S21][S22][S23][S26][S74][S75]. Havaitsemis- ja luokitteluaikaleimat on kirjattava erikseen.

1.3 Raportin rajaus ja vertailumaat

Raportissa käytetään erillisiä tarkastelujaksoja ja tilannekuvapäiviä. Vuoden 2026 tapahtumajakso ulottuu **1.1.–22.11.2026** (UTC) alamaailmajulkaisuille, kiristyshaittaohjelmalistauksille, vuoden 2026 verkkotunnusmaininnoille ja julkisille tapahtumille. Tämän jakson sisällä **8.–22.11.2026** käsitellään erikseen luvussa §5.3. Liukuva 365 päivän verkkotunnusmainintajakso kattaa **23.11.2025–22.11.2026**, ja vuoden 2026 alajoukko (`1.1.–22.11.2026`) raportoidaan erikseen [S4]. Altistusarvioinnit (248 / 250 verkkotunnusta) ja passiiviset kokoonpanohavainnot (kaikki 250 verkkotunnusta) perustuvat **24. marraskuuta 2026** otettuun tilannekuvaan [S3][S4]. Kaikki ulkoiset julkiset lähteet varmennettiin **24. marraskuuta 2026**.

Neljä alueellista vertailumaata ovat **Ruotsi, Norja, Tanska ja Viro**. Ruotsi, Norja ja Tanska jakavat Suomen kanssa pohjoismaiset pankki-, tietoliikenne- ja teollisuusketjut. Viro on Suomen EU- ja Nato-naapuri Suomenlahdella, yhdistettynä merenalaisilla sähkö- ja tietoliikennekaapeleilla sekä rajat ylittävillä digipalveluilla.

Vertailumaat on valittu esimerkeiksi ainoastaan kontekstin antamiseksi; ne eivät merkitse paremmuusjärjestystä tai poliittista arviota.

Jokainen mittayksikkö pidetään erillään koko raportissa. Alamaailman viestejä, kiristyshaittaohjelmalistauksia, Brandefense Atlas -altistushavaintoja (248 / 250 verkkotunnusta), passiivisia kokoonpanohavaintoja (250 verkkotunnusta), pankkihuijaustilastoja ja viranomaisilmoituksia ei lasketa yhteen yhdeksi kansalliseksi hyökkäysluvuksi.

KESKEISET HAVAINNOT

01

Reunalaitteiden nollapäivät, toimittajavuodot, tunnusaltistus ja interaktiivinen pankkikalastelu määrittävät Suomen vuoden 2026 riskiä.

02

Erota raaka alamaailmavolyymi todennetusta suomalaisesta poikkeama- ja altistusnäytöstä.

03

Tarkista aktiiviset tunnuslistaukset, valtuuta reunaeristys, ota käyttöön quarantine- tai reject-DMARC-politiikka ja pidä lakisääteiset ilmoitusreitit erillään.

Raporttikartta

Kaksitoista lukua, viisi lukupolkua. Valitse omaa vastuutasi vastaava päätös ja pidä todisteaineiston rajat mukana jokaisessa havainnossa.

Hallitus ja ylin johto	Valtuuta reunaeristys ja vaadi valmistumisnäyttö	01 05 10 11 12
Tietoturvajohtaja ja palveluomistajat	Priorisoi oma altistus, sähköpostipolitiikka ja toimittajariskit	03 04 05 10 12
SOC ja uhkatiedustelu	Erota massavolyymi, alamaailman väitteet ja varoitukset	02 04 06 07 12
Petostorjunta ja pankkitoiminnot	Torju pankkikalastelu, vahvan tunnistamisen väärinkäyttö ja jatkohuijaukset	05 08 09 12
Tietosuoja, juridiikka ja viestintä	Erota lakisääteiset määräajat, portaalit ja tarkka sanamuoto	05 06 10 12

Todisteluokat ovat **havainto**, **toimijan väite**, **virallinen tiedote**, **lähteistetty raportointi** ja **analyytikon arvio**. Alamaailmajulkaisu voidaan havaita suoraan, vaikka sen väitetty sisältö jää todentamatta. Vahvistettukin poikkeama voi jättää tekijän ja kaikkien kohteiden määrän avoimeksi.

LUKU 02

Suomen digitaalinen profiili ja vuoden 2026 tilannekuva

TÄMÄ LUKU VASTAA

Miten Suomen korkea digitalisaatio muokkaa vuoden 2026 uhkapintaa?

98,2 %

internetin käyttöaste Suomen 5,52 miljoonan käyttäjän keskuudessa (loppuvuonna 2025)

2.1 Korkea digitaalinen integraatio luo yhteisiä riippuvuuksia 11

2.2 Virallinen tilannekuva vuodesta 2025 loppuvuoteen 2026 12

2.3 Alamaailman julkaisumäärien tulkinta Suomessa 13

LUKU 02

Suomen digitaalinen profiili ja vuoden 2026 tilannekuva

LYHYESTI

Suomessa yhdistyvät lähes täydellinen verkkoyhteys, pankkitunnuksiin nojaava vahva tunnistaminen, keskitetyt julkiset ICT-alustat sekä tiiviit pohjoismaiset ja baltialaiset infrastruktuurikytkökset. Vuosien 2025–2026 viranomaistiedot osoittavat kohonneen petostason, ClickFix-verkkosivumurtokampanjat ja tekoälypohjaisen haavoittuvuuksien etsinnän kiihdyttämän haavoittuvuustahdin. Alamaailman raakaluvut vääristyvät alkuvuoden volyymista. Suodata raakasyötteet alustan ja vahvistettujen tiedotteiden mukaan ennen puolustusprioriteettien valintaa.

2.1 Korkea digitaalinen integraatio luo yhteisiä riippuvuuksia

DataReportalin mukaan Suomessa oli loppuvuonna 2025 **5,52 miljoonaa internetin käyttäjää**, mikä vastaa **98,2 % käyttöastetta** [S58]. Julkiset palvelut tukeutuvat vahvasti Suomi.fi-viesteihin ja vahvaan sähköiseen tunnistamiseen, joka rakentuu ensisijaisesti pankkitunnusten ja teleoperaattorien mobiilivarmenteen varaan [S30] [S31].

Yhteiset alustat lisäävät tehokkuutta mutta keskittävät häiriöriskiä. Valtori tuottaa keskeisiä valtionhallinnon ICT- ja mobiililaitehallintapalveluja ministeriöille ja virastoille [S32][S34]. Kunnalliset kirjastokimpat jakavat avoimen lähdekoodin Koha-järjestelmiä [S41][S42], ja kauppa- sekä lentoliikenneala nojaavat erikoistuneisiin rajat ylittäviin ohjelmistotoimittajiin [S35][S48].

Vuoden 2026 strategiset arviot kuvaavat ympäristöä rauhallisen suoraviivaisesti. Maaliskuussa 2026 Suojelupoliisi (Supo) arvioi Venäjän muodostavan keskeisimmän tiedustelu-uhkan Suomelle ja nosti esiin tekoälyn tuomat haasteet [S55]. Supo myös korosti omien pilviratkaisujen tarvetta, jotta kriittiset järjestelmät eivät olisi riippuvaisia muista valtioista [S55]. Marraskuussa 2026 päivitetty Kansallinen riskiarvio (Kansallinen riskiarvio 2026) nosti esiin julkisiin palveluihin, infrastruktuuriin ja datakeskuksiin kohdistuvat riskit [S18][S56]. Sen julkistustilaisuudessa korostettiin myös tekoälyn nopeuttamaa kilpajuoksua hyökkääjien ja puolustajien välillä [S56].

Suomenlahden ja Itämeren merenalainen infrastruktuuri on osa laajempaa varautumiskuvaa. Elokuussa 2026 Helsingin hovioikeus kumosi käräjäoikeuden päätöksen Eagle S -tapauksessa ja linjasi, että Suomen tuomioistuimet voivat tutkia joulukuun 2024 merikaapelivaurioihin liittyvät rikossyytteet [S57]. Kyseessä on vuoden 2026 oikeudellinen käänne vuoden 2024 merenkulkutapauksessa, ei vuoden 2026 kybermurto, ja oikeusprosessi jatkuu [S57].

2.2 Virallinen tilannekuva vuodesta 2025 loppuvuoteen 2026

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus (NCSC-FI) tarjoaa tarkimman kansallisen vertailutason. Vuonna 2025 Kyberturvallisuuskeskukselle tehtiin **20 890 kyberturvallisuusilmoitusta** (225 031 automaattisen ilmoituksen lisäksi), joista **16 729 oli huijaus- ja kalastelutapauksia** (kasvua 20 % edellisvuodesta) [S5]. Kiristyshaittaohjelmailmoituksia kirjattiin vuonna 2025 yhteensä **14** (21 vuonna 2024 ja tyypillisesti noin 40 vuodessa) [S5]. Virasto muistutti ilmoittamisen olevan vapaaehtoista ja Akira-perheen pysyneen yleisimpänä [S5]. Ilmoitetut palvelunestotapaukset laskivat noin 9 % (ilmoittaminen on vapaaehtoista), kun taas muiden haittaohjelmien ilmoitukset kasvoivat noin 28 % [S5].

Vuoden 2026 kuukausittaiset Kybersää-katsaukset ja kesäkuun puolivuotiskatsaus osoittavat neljä teknistä muutosta [S6][S7][S9][S11][S17]:

Jakso 2026	Kyberturvallisuuskeskuksen viralliset havainnot	Puolustuksen painopiste
Tammi–helmikuu 2026	Valtionhallinnon nollapäivämurto (Ivanti EPMM); helmikuussa 1 332 tapausta; Microsoft 365 -tilimurrot +67 % kuukaudessa [S7]	Reunalaitteiden eristäminen, ehdollinen pääsynhallinta ja väliintulohyökkäysten (adversary-in-the-middle, AiTM) torjunta
Maalis–toukokuu 2026	WhatsApp-toimitusjohtajahuijaukset; yli 100 `.fi` -verkkotunnuksen poisto; pakollinen SMS-lähettäjätunnusten luvitus 4.5.; haavatiedotteet +50 % (15 vs 10); Device Code Flow -kalastelu [S8] [S9]	Suojatut SMS-tunnukset, laitekoodikirjautumisen esto ja nopea päivittäminen
Kesä–heinäkuu 2026	Globaali FortiBleed-kampanja vähäisin paikallisvaikutuksin; kesän johtajahuijausvaroitukset; heinäkuussa 1 012 tapausta (alle 1 458 keskiarvon) mutta kiristyshaittaohjelmien kasvu; WordPress `wp2shell` ; kaksi yhteistä vakoiluvaroitusta [S10][S11]	Kesän maksuhyväksynnät, WordPress-kovennus ja verkkolaitteiden tarkistus
Elo–lokakuu 2026	Laaja WordPress-murtoaalto ClickFix-haittaohjelman levittämiseen; vuoden ensimmäinen vakava varoitus Citrix NetScaler -nollapäivistä; kriittiset PHP-haavoittuvuudet ja Valtorin varotoimisulku [S12][S13][S14][S15] [S17]	Julkaisujärjestelmien päivitys, ClickFix-torjunta ja nopeat eristysmallit
Marraskuu 2026 (22.11. asti)	Euroopan kylmälaitehyökkäykset yltävät Suomeen (ennakoiva viranomaisyhteydenotto alkoi 13.10.); robottihuijauspuhelut; Black Friday -valekaupat; kotireitittimien välityspalvelinväärinkäyttö [S16][S18] [S19][S20]	OT-laitteiden poisto julkisesta verkosta, huijausviestintä ja kotiverkkojen suojaus

Kyberturvallisuuskeskuksen mukaan vakavien haavoittuvuuksien kasvun syy on erityisesti tekoälypohjainen haavoittuvuuksien metsästys [S11].

2.3 Alamaailman julkaisumäärien tulkinta Suomessa

Tammi- ja helmikuun massamainonta hallitsee Suomeen merkittyä julkaisumäärää



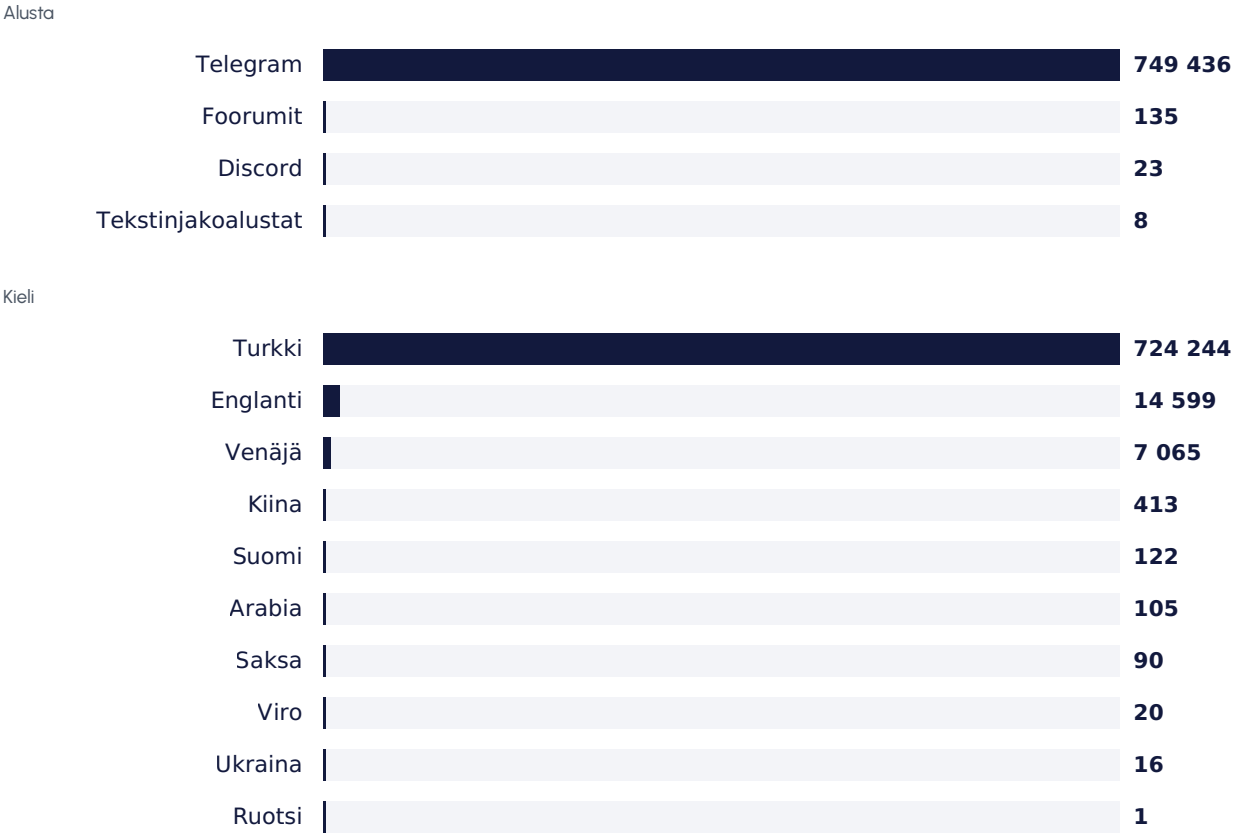
Lähde: Odin by Brandefense, Suomeen merkityt alamaailmajulkaisut 1.1.–22.11.2026; marraskuu on osittainen [S1]. Julkaisut eivät ole vahvistettuja poikkeamia; kielimerkinnät voivat olla päällekkäisiä.

Tarkastelujaksolla 1.1.–22.11.2026 Odin by Brandefense havaitsi **749 602 Suomeen merkittyä julkaisua** seuratuilla alamaailmakanavilla [S1]. Kuukausijakauma on äärimmäisen keskittynyt: **411 036 julkaisua tammikuussa** ja **315 239 helmikuussa**, yhteensä **726 275 julkaisua (96,9 %)** kahden ensimmäisen kuukauden aikana [S1]. Näistä 726

275 tammi–helmikuun julkaisusta **726 240** julkaistiin Telegramissa ja **723 961** kantoi turkin kielimerkintää [S1]. Maaliskuusta marraskuuhun kertyi yhteensä **23 327 julkaisua**, vaihdellen **1 469** (maaliskuu) ja **5 698** (lokakuu) välillä; osittaisessa marraskuussa (22.11. asti) kertyi **1 749** julkaisua [S1].

Yhdessä tarkastuksessa **622** kaikkiaan **627** tammi–helmikuun julkaisusta oli toistuvaa turkinkielistä kaupallista mainontaa Telegram-kanavilla, ei Suomeen kohdistettua kyberrikollisuutta [S1]. Myös lokakuun **5 698** viestin huippu selittyy suurelta osin monikansallisella pilvipalvelin- ja pelitilikaupalla [S1].

Telegram ja turkinkielinen massamainonta hallitsevat raakaa maamerkintää



Lähde: Odin by Brandefense, Suomeen merkityt alamaailmajulkaisut 1.1.-22.11.2026; marraskuu on osittainen [S1]. Julkaisut eivät ole vahvistettuja poikkeamia; kielimerkinnät voivat olla päällekkäisiä.

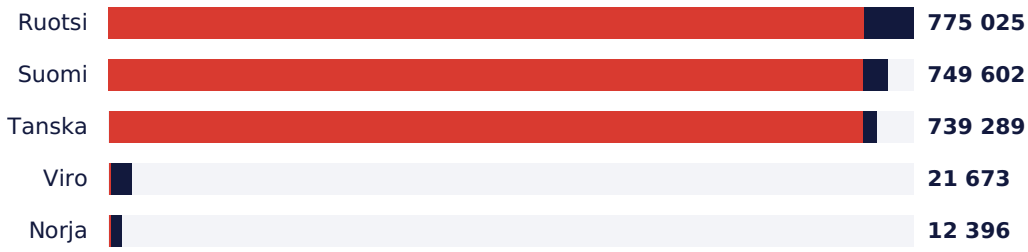
Alusta- ja kielijakauma vahvistaa ilmiön [S1]:

- **Alustat (tarkka summa 749 602):** Telegram kattaa **749 436 julkaisua (99,98 %)**, foorumit **135**, Discord **23**, tekstinjakoalustat **8** ja Tor-palvelut **0** [S1].
- **Kielet (merkinnät voivat olla päällekkäisiä):** turkki **724 244**, englanti **14 599**, venäjä **7 065**, kiina **413**, suomi **122**, arabia **105**, saksa **90**, viro **20**, ukraina **16** ja ruotsi **1** [S1].

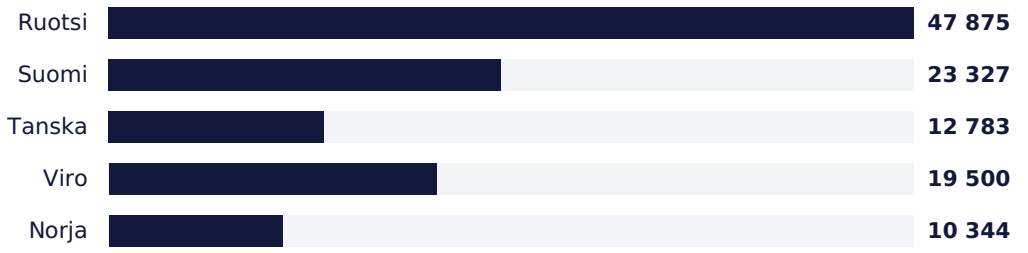
Ruotsi, Suomi ja Tanska saivat saman tammi- ja helmikuun massamainonta-aallon



Yhteensä 1.1.-22.11.2026 (tammi-helmi korallina, maalis-marras tummansinisenä)



Vain maalis-marraskuu 2026 (erillinen asteikko)



Maamerkityt raakajulkaisut seuratuilla kanavilla; lukuja ei ole suhteutettu väestöön tai lähdekattavuuteen. Lähde: Odin by Brandefense, Suomeen merkityt alamaailmajulkaisut 1.1.-22.11.2026; marraskuu on osittainen [S1]. Julkaisut eivät ole vahvistettuja poikkeamia; kielimerkinnät voivat olla päällekkäisiä.

Vertailumaat on valittu esimerkeiksi ainoastaan kontekstin antamiseksi; ne eivät merkitse paremmuusjärjestystä tai poliittista arviota.

Alueellinen vertailu selventää ilmiötä [S1]. **Ruotsi (775 025)**, **Suomi (749 602)** ja **Tanska (739 289)** saivat kaikki saman tammi–helmikuun Telegram-massamainonta-aallon, kun taas **Viro (21 673)** ja **Norja (12 396)** jäivät sen ulkopuolelle [S1]. Foorumeilla, joihin kohdennetut pääsy- ja tietokantaväitteet keskittyvät, Suomeen merkittiin **135** viestiä, mikä on vähemmän kuin **Virossa (506)**, **Ruotsissa (485)**, **Tanskassa (179)** ja **Norjassa (144)** [S1]. Ruotsin luvut tarkistettiin 24. marraskuuta 2026; Ruotsin raportissa ilmoitetaan 775 020 viestiä ja 484 foorumiviestiä (laskettu 23. marraskuuta) [S1].

KESKEISET HAVAINNOT

01

Korkea digitaalinen luottamus ja yhteiset alustat suurentavat toimittaja- ja reunalaitehäiriöiden vaikutusta Suomessa.

02

Tammi- ja helmikuu kattavat 96,9 % Suomeen merkityistä julkaisuista, ja niitä hallitsee Telegram-massamainonta.

03

Seuraa Kyberturvallisuuskeskuksen varoituksia, foorumiväitteitä ja vahvistettuja tiedotteita raakavolyymin sijaan.

LUKU 03

Kansallinen altistus ja 250 verkkotunnuksen havainnot

TÄMÄ LUKU VASTAA

Mitkä altistushavainnot ja kokoonpanoaukot vaativat omistajan tarkistusta 250 suomalaisessa verkkotunnuksessa?

41 / 248

arvioidulla suomalaisella verkkotunnuksella oli tarkistushetkellä myynnissä oleva kirjautumistieto

3.1 Joukon rajaus ja arvioinnin rajat 17

3.2 Kansallinen Atlas-yleisluku ja aktiiviset tunnuslistaukset 18

3.3 Saastuneiden laitteiden ja historiallisten tunnistetietueiden kytkökset 21

3.4 Asiakirjat, samankaltaiset verkkotunnukset ja 365 päivän maininnat 23

3.5 Sähköpostitodennus, DNSSEC, TLS ja HSTS 250 verkkotunnuksessa 24

3.6 Altistussignaalien muuttaminen erillisiksi tarkistusjonoiksi 26

LUKU 03

Kansallinen altistus ja 250 verkkotunnuksen havainnot

LYHYESTI

Marraskuun 24. päivän 2026 tilannekuvassa 248 arvioidulla suomalaisella verkkotunnuksella kansallinen Atlas-yleisluku on 45/100, ja 41 verkkotunnuksella oli myynnissä oleva kirjautumistieto. Joukkoon kytkeytyy vähintään 128 734 saastuneen laitteen kytköstä ja 2 245 122 historiallista tunnistetietuetta; 2 verkkotunnusta jää tuntemattomaksi. Erikseen 146 verkkotunnusta 250:stä (58,4 %) julkaisee karanteenia tai hylkäystä pyytävän DMARC-politiikan, kun 94 on seurantatilassa. Tarkista aktiiviset listaukset ensin, varmenna työntekijälaitteet ja siirrä seurantatilan verkkotunnukset quarantine- tai reject-DMARC-politiikkaan.

3.1 Joukon rajaus ja arvioinnin rajat

Kokosimme tarkoitushakuisen **250 DNS-varmennetun suomalaisen verkkotunnuksen** joukon, joka jakautuu kymmeneen 25 verkkotunnuksen toimialasoluun [S3][S4]. Yksittäiset verkkotunnukset pidetään salassa todentamattomien havaintojen suojaamiseksi.

Kohde	Rajaus
Ajankohdat	Vuoden 2026 tapahtumajakso on 1.1.–22.11.2026; liukuva 365 päivän mainintajakso on 23.11.2025–22.11.2026; altistus- ja kokoonpanotilannekuvat on otettu 24.11.2026; ulkoiset lähteet varmennettu 24.11.2026
Portfolio	250 valittua suomalaista verkkotunnusta 10 solussa, 25 kussakin (114 yksityistä, 88 kunta-/sote-/koulutustoimijaa, 48 valtionhallinnon tai valtio-omisteista)
Valintaperuste	Tarkoitushakuinen otos ministeriöistä, virastoista, hyvinvointialueista, kaupungeista, yliopistoista, pankeista, energiasta, televiestinnästä, liikenteestä ja teollisuudesta; ei kansallinen tilasto-otos
Yksikkö	Yksi ensisijainen verkkotunnus organisaatiota kohti; kaikki 250 ratkesivat DNS:ssä 24.11.2026 [S3]
Altistustilannekuva	248 / 250 valittua verkkotunnusta arvioitu 24.11.2026; 2 verkkotunnusta jää tuntemattomaksi (1 tietoliikenteessä, 1 terveys- ja hyvinvointipalveluissa) [S4]
Altistussignaalit	Kumulatiiviset saastuneiden laitteiden ja työntekijälaitteiden kytkökset, historialliset tunnistetietueet, aktiiviset myyntilistaukset, listaushistoria, asiakirjakytkökset ja 30 päivän samankaltaiset nimet [S4]

Kohde	Rajaus
Mainintakonteksti	Liukuva 365 päivän keskustelukanava- ja Tor-mainintajakso kaikille 250 verkkotunnukselle (23.11.2025–22.11.2026); vuoden 2026 alajoukko (1.1.–22.11.2026) raportoidaan erikseen [S4]
Passiivinen tilannekuva	Julkiset DNS-, DMARC-, SPF-, DKIM-, DNSSEC-, TLS- ja HSTS-havainnot kaikille 250 verkkotunnukselle 24.11.2026 [S3]
Julkaisurajaus	Vain kansallinen Atlas-yleisluku (45/100); toimiala-, ryhmä- tai organisaatiokohtaisia arvosanoja ei julkaista [S4]
Tulkintaraja	Signaalit voivat olla päällekkäisiä; puuttuva havainto ei ole nolla eikä yksikään luku vahvista tietomurtoa

Altistushavainnot ja passiiviset asetukset vastaavat eri kysymyksiin. Historiallinen tunnusvuoto voi esiintyä kunnossa olevan sähköpostisuojauksen rinnalla, eikä julkaistu `quarantine`- tai `reject`-DMARC-politiikka estä aktiivista tilikalastelua. Säilytä kummankin tarkastelun nimittäjä (`248` altistukselle, `250` asetuksille ja maininnoille).

3.2 Kansallinen Atlas-yleisluku ja aktiiviset tunnuslistaukset

41 arvioidulla suomalaisella verkkotunnuksella 248:sta (16,5 %) oli tarkistushetkellä myynnissä oleva kirjautumistieto [S4]. Kaikilla 41:llä oli myös aiempaa listaushistoriaa, yhteensä **299 historiallista merkintää** koko portfoliossa [S4].

Arvioidun portfolion kansallinen Atlas-yleisluku on 45/100 [S4]. Suurempi luku kuvaa suurempaa havaittua ulkoista altistusta asteikolla 0–100. Vain tämä yksi kansallinen yleisluku julkaistaan. Toimiala-, ryhmä- tai organisaatiokohtaisia arvosanoja ei esitetä tässä raportissa.

Yleisluku tukee priorisointia arvioidun portfolion sisällä. Se ei ole murrettujen organisaatioiden osuus, murron todennäköisyys eikä kansallinen esiintyvyysarvio. Kahden arvioimatta jääneen verkkotunnuksen altistus jää tuntemattomaksi eikä sitä merkitä nollaksi.

Aktiiviset tunnuslistaukset ja altistussignaalit 248 arvioidulla suomalaisella verkkotunnuksella

	Aktiivinen listaus	Laitekytkös	Työntekijälaitt	Tunnistetietueita	Asiakirjakytkös
Valtionhallinto	3/25	18/25	11/25	20/25	17/25
Alue- ja paikallishallinto	1/25	24/25	21/25	25/25	18/25
Pankki- ja rahoitusala	7/25	18/25	12/25	24/25	17/25
Energia ja yhdyskuntahuolto	2/25	20/25	6/25	24/25	10/25
Tietoliikenne ja digipalvelut	6/24	20/24	16/24	24/24	18/24
Teollisuus ja valmistus	0/25	21/25	21/25	24/25	21/25
Liikenne, merenkulku ja logistiikka	8/25	15/25	8/25	24/25	8/25
Terveys- ja hyvinvointipalvelut	0/24	15/24	13/24	20/24	6/24
Koulutus ja tutkimus	4/25	23/25	23/25	24/25	20/25
Kauppa, media ja kuluttajapalvelut	10/25	23/25	17/25	25/25	16/25

Aktiiviset tunnuslistaukset toimialoittain (koralli). Jokainen solu näyttää havaitut verkkotunnukset / arvioidut verkkotunnukset (24 tai 25); signaalit ovat päällekkäisiä. Lähde: Brandefensen altistushavainnot 248 arvioidulle verkkotunnukselle 250 valitusta suomalaisesta verkkotunnuksesta, 24.11.2026 tilannekuva (2 verkkotunnusta jää tuntematttomaksi) [S4]. Kumulatiiviset kytkökset voivat olla päällekkäisiä; ne eivät kuvaa yksittäisiä henkilöitä tai vahvistettuja murtoja.

Alla olevan taulukon jokainen sarake laskee arvioitujen **verkkotunnusten** lukumäärää kussakin signaalissa, ei yksittäisten laitteiden tai tietueiden määriä [S4].

Toimialasolu	Arvioituja verkkotunn. (25:stä)	Aktiivinen listaus (verkkotunn.)	Laitekytkös (verkkotunn.)	Työntekijälaite (verkkotunn.)	Tunnistetietueita (verkkotunn.)	Asiakirjakytkös (verkkotunn.)	Samankaltaisia nimiä 30 pv (verkkotunn.)
Valtionhallinto	25	3	18	11	20	17	14
Alue- ja paikallishallinto	25	1	24	21	25	18	19
Pankki- ja rahoitusala	25	7	18	12	24	17	14
Energia ja yhdyskuntahuolto	25	2	20	6	24	10	11
Tietoliikenne ja digipalvelut	24	6	20	16	24	18	21
Teollisuus ja valmistus	25	0	21	21	24	21	19

Toimialasolu	Arvioituja verkkotunn. (25:stä)	Aktiivinen listaus (verkkotunn.)	Laitekytkös (verkkotunn.)	Työntekijälaite (verkkotunn.)	Tunnistetietueita (verkkotunn.)	Asiakirjakytkös (verkkotunn.)	Samankaltaisia nimiä 30 pv (verkkotunn.)
Liikenne, merenkulku ja logistiikka	25	8	15	8	24	8	11
Terveys- ja hyvinvointipalvelut	24	0	15	13	20	6	9
Koulutus ja tutkimus	25	4	23	23	24	20	21
Kauppa, media ja kuluttajapalvelut	25	10	23	17	25	16	21
Yhteensä (248 / 250)	**248**	**41**	**197**	**148**	**234**	**151**	**160**

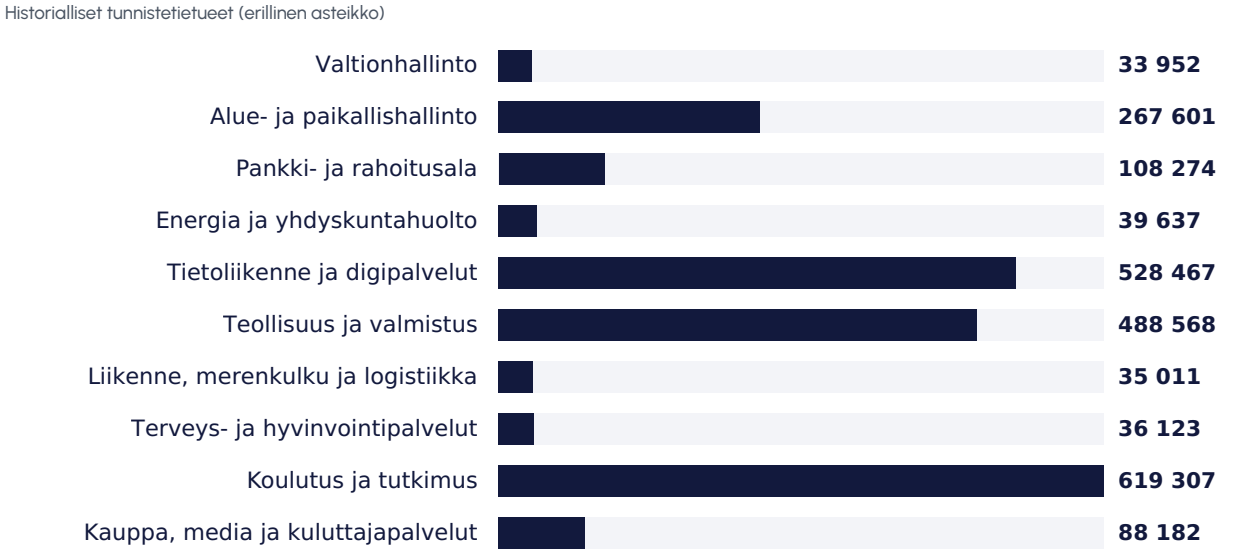
Aktiiviset tunnuslistaukset painottuvat **kauppaan, mediaan ja kuluttajapalveluihin (10 / 25)**, **liikenteeseen ja logistiikkaan (8 / 25)**, **pankki- ja rahoitusalalle (7 / 25)** sekä **tietoliikenteeseen ja digipalveluihin (6 / 24)** [S4]. Sitä vastoin **teollisuudessa (0 / 25)** ja **terveys- ja hyvinvointipalveluissa (0 / 24)** ei havaittu tarkistushetkellä yhtään aktiivista listausta [S4].

Toimialakohtaisissa altistustaulukoissa ja kaavioissa aktiiviset tunnuslistaukset laskevat arvioidut verkkotunnukset, joilla on tarkistushetkellä myynnissä oleva kirjautumistieto [S4]. Aktiivinen listaus on suorin kehote tarkistaa tili, mutta se ei todista toteutunutta kauppaa, toimivaa salasanaa tai palvelinmurtoa. Ohjaa jokainen valtuutettu hälytys identiteettitiimille tilin tilan, MFA-suojauksen ja viimeaikaisten istuntojen tarkistamiseksi.

3.3 Saastuneiden laitteiden ja historiallisten tunnistetietueiden kytkökset

Laite- ja tunnistekytkökset keskittyvät tietoliikenteeseen, kauppaan ja koulutukseen





Lähde: Brandefensen altistushavainnot 248 arvioidulle verkkotunnukselle 250 valitusta suomalaisesta verkkotunnuksesta, 24.11.2026 tilannekuva (2 verkkotunnusta jää tuntemattomaksi) [S4]. Kumulatiiviset kytkökset voivat olla päällekkäisiä; ne eivät kuvaa yksittäisiä henkilöitä tai vahvistettuja murtoja.

Toimialasolu	Arvioitu	Laitekytköksiä, vähintään	Työntekijälaitekytköksiä	Tunnistetietueita	Asiakirjakytköksiä	Samankaltaisia nimiä (30 pv)
Valtionhallinto	25	950	25	33 952	61	1 866
Alue- ja paikallishallinto	25	4 182	677	267 601	166	128

Toimialasolu	Arvioitu	Laitekytköksiä, vähintään	Työntekijälaitekytköksiä	Tunnistetietueita	Asiakirjakytköksiä	Samankaltaisia nimiä (30 pv)
Pankki- ja rahoitusala	25	7 317	59	108 274	120	7 362
Energia ja yhdyskuntahuolto	25	2 818	44	39 637	55	725
Tietoliikenne ja digipalvelut	24	67 715	2 060	528 467	530	544
Teollisuus ja valmistus	25	1 960	980	488 568	640	428
Liikenne, merenkulku ja logistiikka	25	12 591	45	35 011	29	750
Terveys- ja hyvinvointipalvelut	24	145	70	36 123	72	55
Koulutus ja tutkimus	25	8 611	1 656	619 307	718	8 965
Kauppa, media ja kuluttajapalvelut	25	22 445	74	88 182	93	5 855
Yhteensä (248 / 250)	**248**	**128 734**	**5 690**	**2 245 122**	**2 484**	**26 678**

Arvioiduista 248 verkkotunnuksesta **197** kantaa vähintään **128 734 laitekytköstä**, jotka jakautuvat **5 690 työntekijäluokiteltuun laitekytkökseen (4,4 %)** (**148** verkkotunnuksella) ja **123 044 ei-työntekijäluokiteltuun laitekytkökseen (95,6 %)** [S4]. Työntekijälaitekytkökset sisältyvät kokonaislaitekytköksiin eikä niitä saa laskea niiden päälle. Aineisto on kumulatiivista eikä pelkästään vuoden 2026 tapahtumia [S4].

Neljä käytännön ilmiötä ohjaa suomalaisia puolustajia [S4]:

- **Kuluttajapalvelut kantavat valtaosan laitekytköksistä.** Tietoliikenne ja digipalvelut vastaa vähintään **67 715** laitekytköksestä (52,6 % koko joukosta; 2 060 työntekijälaitekytköstä), ja seuraavina tulevat kauppa ja media (**22 445**; 74) sekä liikenne ja logistiikka (**12 591**; 45) [S4]. Suurin osa ei-työntekijäluokitelluista laitekytköksistä heijastaa uskottavasti kuluttajien omia laitteita, vaikka laitteen omistajuutta ei voida todentaa.
- **Työntekijälaitekytkökset keskittyvät neljään soluun.** Tietoliikenne (**2 060**), koulutus ja tutkimus (**1 656**, 23 / 25 verkkotunnuksella), teollisuus (**980**, 21 / 25) sekä alue- ja paikallishallinto (**677**, 21 / 25) kattavat **5 373 työntekijälaitekytköstä 5 690:stä (94,4 %)** [S4]. Yliopistoissa henkilökunta ja opiskelijat jakavat usein saman verkkotunnuksen, joten henkilöstöstatus on aina varmennettava ennen päätelaiterajausta.

- **Historiallisia tunnistetietueita on 2 245 122 yhteensä 234 verkkotunnuksella.** Ne jakautuvat **1 279 899 tietovuotokantatietueeseen (57,0 %)**, **783 695 yhdistelmälistatietueeseen (34,9 %)** ja **181 528 tietovarkauslokiriviin (8,1 %)** [S4]. Erikseen kytkeytyneet laitteet sisältävät vähintään **2 349 971** kaapattua tunnistetietoa eri palveluihin, ei pelkästään kyseiseen verkkotunnukseen [S4].
- **Muutama suuri verkkotunnus painottaa toimialasummia.** Koulutus (**619 307**), tietoliikenne (**528 467**), teollisuus (**488 568**) ja kunnat (**267 601**) kattavat **1 903 943 (84,8 %)** kaikista tunnistetietueista [S4]. Koko portfoliossa kaksi suurinta verkkotunnusta kantaa **28,1 %** tietueista, ja tietoliikenteessä kaksi verkkotunnusta kantaa **90,0 %** [S4]. Mediaaniverkkotunnuksella on **31** laitekytköstä ja **1 640** tunnistetietuetta, joten yksittäisen organisaation tulee aina tukeutua omaan tilannekuvaansa [S4].

3.4 Asiakirjat, samankaltaiset verkkotunnukset ja 365 päivän maininnat

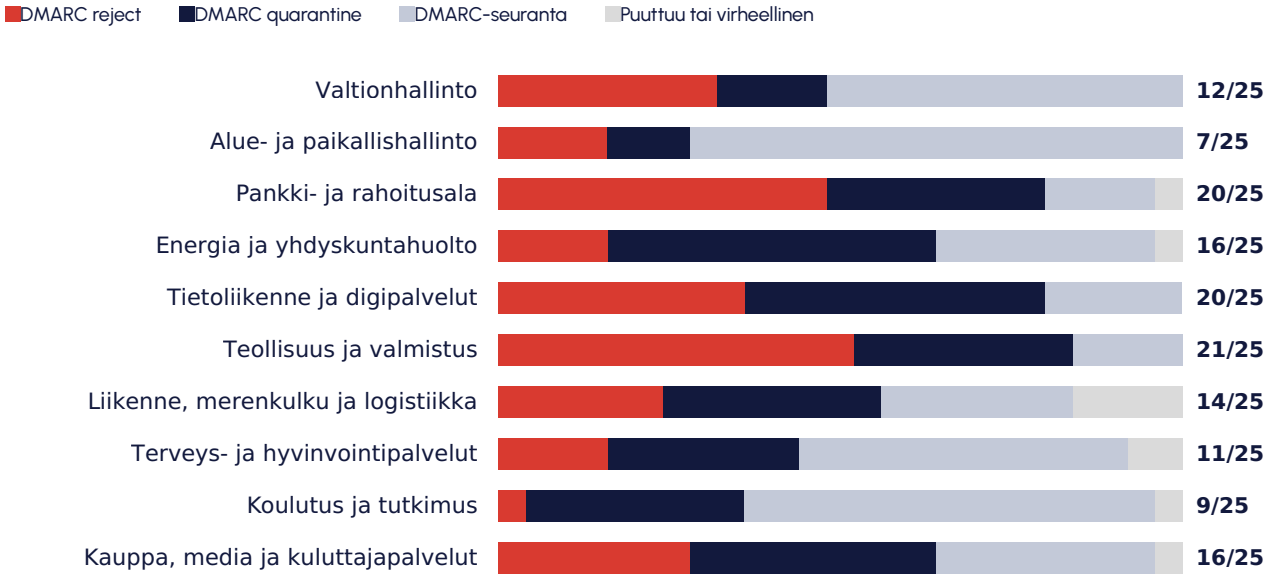
Kolme kontekstisignaalia täydentää tunnus- ja laitetarkistuksia [S4]:

- **Asiakirjakytkökset (248 arvioitua verkkotunnusta): 151 verkkotunnuksella** on **2 484 asiakirjakytköstä**, kärjessä koulutus (**718**, 20 verkkotunnuksella), teollisuus (**640**, 21) ja tietoliikenne (**530**, 18) [S4]. Asiakirjakytkös ei osoita luottamuksellisuutta, luvatonta hankintaa tai hyökkääjän latausta; julkiset esitteet ja kierrätetyt tiedostot ovat tavallisia selityksiä.
- **30 päivän samankaltaiset nimet (248 arvioitua verkkotunnusta): 160 verkkotunnuksella** havaittiin **26 678** uutta samankaltaista verkkotunnusrekisteröintiä edeltävän 30 päivän aikana, kärjessä koulutus (**8 965**), pankkiala (**7 362**) sekä kauppa ja media (**5 855**) [S4]. Lyhyet tai yleiset nimet osuvat myös ulkopuolisiin kansainvälisiin verkkotunnuksiin; määrät ovat tarkistusjono eivätkä vahvistettuja kalastelusivustoja.
- **Liukuvat 365 päivän keskustelukanava- ja Tor-maininnat (kaikki 250 verkkotunnusta, 23.11.2025–22.11.2026): 49 verkkotunnusta 250:stä (19,6 %)** keräsi **941 mainintaa** keskustelukanavilla, kärjessä kauppa ja media (**6 verkkotunnusta, 647**), tietoliikenne (**10, 167**) ja valtionhallinto (**13, 82**) [S4]. Erikseen **56 verkkotunnusta 250:stä (22,4 %)** keräsi **662 Tor-mainintaa**, kärjessä teollisuus (**6, 194**), valtionhallinto (**9, 130**), koulutus (**6, 130**) ja tietoliikenne (**6, 98**) [S4]. Kunnissa osumat levisivät laajimmalle (**14 / 25 verkkotunnusta, 24 mainintaa**) [S4].

Vuoden 2026 jaksolla (`1.1.–22.11.`) **29 verkkotunnusta** sai **207 mainintaa**, kärjessä kauppa ja media (**95**), tietoliikenne (**67**), valtionhallinto (**22**) ja koulutus (**13**) [S4]. Verkkotunnuksen maininta, asiakirjaosuma tai samankaltainen nimi ei ole näyttö tietomurrosta. Osumat voivat johtua uutisjaoista, käyttäjien omien laitteiden tietovarkauksista tai julkisista viittauksista ja vaativat omistajan tarkistuksen.

3.5 Sähköpostitodennus, DNSSEC, TLS ja HSTS 250 verkkotunnuksessa

Teollisuus ja pankit johtavat karanteeni- ja hylkäyspolitiikoissa julkisen sektorin jäädessä seurantatilaan



Lähde: passiiviset kokoonpanohavainnot 250 valitusta suomalaisesta verkkotunnuksesta, 24.11.2026 tilannekuva [S3]. Julkaistut politiikat eivät todista viestikohtaista estoa tai torjuttua väärennöstä.

Sähköpostin ja verkkoliikenteen perustekniikat ovat laajasti käytössä (tilannekuva 24.11.2026), mutta karanteenia tai hylkäystä pyytävä DMARC-politiikka jää jälkeen erityisesti julkisella sektorilla [S3]:

Toimialasolu (25 verkkotunnusta kussakin)	DMARC reject	DMARC quarantine	DMARC seuranta	DMARC puuttuu	SPF	DKIM	DNSSEC DS	Voimassa oleva TLS	HSTS (saatavilla olevista)
Teollisuus ja valmistus	13	8	4	0	23	24	3	25	17 / 22
Pankki- ja rahoitusala	12	8	4	1	24	22	6	24	22 / 24
Tietoliikenne ja digipalvelut	9	11	5	0	24	24	2	25	22 / 25
Energia ja yhdyskuntahuolto	4	12	8	1	25	25	2	24	17 / 23

Toimialasolu (25 verkkotunnusta kussakin)	DMARC reject	DMARC quarantine	DMARC seuranta	DMARC puuttuu	SPF	DKIM	DNSSEC DS	Voimassa oleva TLS	HSTS (saatavilla olevista)
Kauppa, media ja kuluttajapalvelut	7	9	8	1	24	23	4	25	18 / 22
Liikenne, merenkulku ja logistiikka	6	8	7	4	25	24	4	25	17 / 21
Valtionhallinto	8	4	13	0	24	18	6	25	12 / 13
Terveys- ja hyvinvointipalvelut	4	7	12	2	24	24	1	22	19 / 21
Koulutus ja tutkimus	1	8	15	1	24	23	0	25	19 / 23
Alue- ja paikallishallinto	4	3	18	0	24	25	3	24	17 / 24
Yhteensä (250 verkkotunnusta)	**68**	**78**	**94**	**10**	**241**	**232**	**31**	**244**	**180 / 218**

Kolme käytännön havaintoa nousee esiin [S3]:

- **Seurantatilan pullonkaula keskittyy julkisiin toimijoihin.** Kaikkiaan **146 verkkotunnusta 250:stä (58,4 %)** julkaisee karanteenia tai hylkäystä pyytävän DMARC-politiikan (`68 reject` , `78 quarantine`), **94 (37,6 %)** on seurantatilassa (`none`) ja **10 (4,0 %)** ilman voimassa olevaa tietuetta [S3][S67]. Neljä julkista solua vastaa **58:sta seurantatilan 94 verkkotunnuksesta**: alue- ja paikallishallinto (18), koulutus ja tutkimus (15, vain 1 `reject`), valtionhallinto (13) ja hyvinvointipalvelut (12) [S3].
- **Tekniset edellytykset ovat pääosin valmiina.** SPF-tietue löytyy **241 verkkotunnuksesta (96,4 %)** ja DKIM-tietue **232 verkkotunnuksesta (92,8 %)** [S3][S68][S69]. Kunnissa ja maakunnissa 24 julkaisee SPF:n ja kaikki 25 DKIM:n, mutta vain 7 julkaisee karanteenia tai hylkäystä pyytävän DMARC-politiikan [S3]. Siksi on selvitettävä välittömästi, mitkä tekniset tai toiminnalliset esteet pysäyttävät siirtymän pois seurantatilasta verkkotunnuksissa, joissa SPF ja DKIM jo julkaistaan.

- **Puuttuva DMARC keskittyy liikenteeseen ja DNSSEC on harvinainen.** Kymmenestä puuttuvasta DMARC-tietueesta neljä on liikenne- ja logistiikkasolussa [S3]. DNSSEC-delegaatio (`DS`) esiintyy **31 verkkotunnuksessa (12,4 %)**, eniten valtionhallinnossa (6) ja pankeissa (6) [S3]. Voimassa oleva TLS havaittiin **244 verkkotunnuksessa** (1 varmentamisvirhe, 5 ei saatavilla) [S3]. HSTS esiintyi **180:ssä 218 saatavilla olleesta HTTP-vastauksesta** (32 ei saatavilla, mukaan lukien 12 valtionhallinnon verkkotunnusta) [S3][S70].

Kokoonpanohavaintoihin liittyy selkeitä rajoja. Julkaistu `quarantine` - tai `reject` -DMARC-tietue kertoo pyydetyn politiikkaluokan eikä takaa täyttä suojaa, sillä DMARC sallii osittaisen soveltamisen ja vastaanottavien palvelimien käsittely vaihtelee [S67]. Vastaavasti julkaistu SPF- tai DKIM-tietue ei vahvista kohdistusta, DNSSEC-delegaatio ei osoita täyttä varmennusketjua, ja puuttuvat HTTP- tai TLS-tulokset eivät merkitse virheellistä kokoonpanoa [S68] [S69].

3.6 Altistussignaalien muuttaminen erillisiksi tarkistusjonoiksi

Eri ulkoiset havainnot kuuluvat eri vastuuomistajille ja vaativat päivätyn kuittauksen yleisten murtoilmoitusten sijaan:

Signaali	Vastuutaho	Ensimmäinen tarkistus	Valmistumisnäyttö
Aktiivinen tunnuslistaus	Identiteettioperaatiot	Tilin olemassaolo, aktiivisuus ja MFA-suojaus	Päivätty tilikuittaus ja istuntotarkistus
Työntekijälaitteen kytkös	Päätelaiteturva ja SOC	Hallittu työlaite ja istuntojen tuoreus	Eristys, istuntojen katkaisu ja laitetarkistus
Ei-työntekijälaitteen kytkös	Petostorjunta ja asiakasturva	Asiakastilin väärinkäyttömerkit ja poikkeavat maksut	Asiakassuojatoimi tai dokumentoitu sulku
Asiakirja, samankaltainen nimi tai maininta	Tieto- ja brändinomistajat	Luottamuksellisuus, omistajuus ja harhaanjohtava käyttö	Käsittelypäätös tai alasajopyyntö
Seurantatilan DMARC tai TLS-virhe	Sähköposti- ja verkkotiimit	Kohdistetut lähettäjät ja varmenneketju	Täyden kattavuuden quarantine- tai reject-politiikka tai korjattu varmenne

KESKEISET HAVAINNOT

01

Kansallinen Atlas-yleisluku on 45/100 arvioiduille 248 suomalaiselle verkkotunnukselle (tilannekuva 24. marraskuuta 2026), joista 41:llä oli aktiivinen tunnuslistaus.

02

Pidä aktiiviset listaukset, työntekijälaitteet, kuluttajalaitteet ja vanhat tietueet erillisissä tarkistusjonoissa.

03

94 seurantatilassa olevan suomalaisen verkkotunnuksen siirtäminen täyden kattavuuden quarantine- tai reject-DMARC-tasoon on välitön ja tehokas suojatoimi.

LUKU 04

Alamaailman väitteet ja tapaukset

TÄMÄ LUKU VASTAA

Mitä rikolliset tosiasiassa mainostavat, etsivät ja kierrättävät Suomen ympärillä?

7

dokumentoitua alamaailman väitetapausta vuodelta 2026

4.1 Kuinka alamaailman väitteitä luetaan 28

4.2 Kauppa-, kuluttaja- ja kierrätysväitteet 28

4.3 Yrityspääsyjen kysyntä, kalastelupaketit ja tunnuslistat 33

4.4 Televiestintä-, väärennös- ja muulisyötteet 37

LUKU 04

Alamaailman väitteet ja tapaukset

LYHYESTI

Suomeen liittyvät foorumi- ja keskusteluväitteet keskittyvät väitettyihin verkkokauppa- ja CRM-vienteihin, kierrätettyihin yhteystietolistoihin, yritysten Microsoft 365 -pääsyjen ostoon, reaaliaikaisiin pankkikalastelupaketteihin, tunnuslistoihin, suomalaisiin eSIM-profiileihin ja asiakirjaväärennöksiin. Useat julkaisut toistavat aiempia päivättyjä näytteitä ilman vuosilukua, kuten 17.11. julkaisu, jonka näyterivit vastaavat lokakuun 2023-merkittyä CSV:tä. Käsittele jokaista väitettä todentamattomana kunnes omat lokit vahvistavat asian.

4.1 Kuinka alamaailman väitteitä luetaan

Foorumijulkaisu todentaa varmuudella vain yhden asian: joku julkaisi tekstin kyseisenä päivänä kyseisellä alustalla. Se ei osoita tietojen aitoutta, tuoreutta, palvelinmurtoa, toimivaa pääsyä tai toteutunutta kauppaa. Kaikkien seitsemän alla olevan tapauksen (`Tapaus A` – `Tapaus G`) todentamattomat kohdenimet on salattu.

4.2 Kauppa-, kuluttaja- ja kierrätysväitteet

A

TAPAUS A

Toistuvat kolmitauluisten suomalaiskauppojen tietokantaväitteet

Väite todentamatta

Vähittäiskauppa ja verkkokauppa

VÄITE	Helmikuussa (`B01`), huhtikuussa (`B02`) ja katkaisupäivänä 22. marraskuuta (`B13`) foorumimyyjät mainostivat väitettyjä kolmitauluisten asiakas- ja tilausaineistojen vientejä suomalaisista vähittäis- ja verkkokaupoista [S1]. Helmi- ja huhtikuun ilmoitukset käyttivät identtistä tekstipohjaa tarjoten `Contact` -, `Order` - sekä `Address` - tai `Paymentinfo` -osioita [S1]. Marraskuun 22. päivän ilmoitus listasi CRM-tyyppisiä `Contact` - ja `Retail Order` -tauluja verkkokauppa-alustalta ja kauppiasyritykseltä [S1].
MIKÄ JÄÄ TODENTAMATTA	Yhdestäkään mainitusta kauppiaasta ei ollut virallista vahvistusta katkaisuhetkellä. Identtinen myyntiteksti lisää kierrätetyn tai kootun aineiston mahdollisuutta.
TOIMENPIDE	Hälytyksen saavan kauppiaan tulee verrata väitettyjä sarakkeita omaan CRM- ja verkkokaupparakenteeseensa ennen asiakastiedottamista.

Ydinviesti

Tarkista vastaako väitetty taulurakenne omaa CRM- tai verkkokauppavientiä ennen asiakasviestintää.

Todistekortti B01 18.2.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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.

KÄÄNNÖS

Tarjolla aineisto [suomalaiselta vähittäiskaupalta], sisältäen Contact-, Order- ja Address-taulut kolmessa osiossa.

Huomio. Kauppaketjun nimi on salattu, koska tapauksesta ei ole virallista vahvistusta.

Havaittu

Foorumimyyjä mainostaa väitettyä kolmitauluista asiakas-, tilaus- ja osoiteaineistoa liitettynä suomalaiseen vähittäiskauppaketjuun.

Ei todennettu

Aitoutta, tuoreutta, järjestelmäpääsyä, asiakasmäärää, alkuperää tai toteutunutta kauppaa.

Todistekortti B02 4.4.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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.

KÄÄNNÖS

Tarjolla aineisto [suomalaisesta verkkokaupasta], sisältäen Contact-, Order- ja Paymentinfo-taulut kolmessa osiossa.

Huomio. Identtinen myyntiteksti useissa kauppaväitteissä korostaa tarvetta varmentaa tiedot suoraan rekisterinpitäjältä.

Havaittu

Myyjä käyttää samaa kolmiosaista myyntipohjaa mainostaessaan suomalaiseen verkkokauppaan liitettyä väitettyä asiakas-, tilaus- ja maksutietoaineistoa.

Ei todennettu

Järjestelmämurtoa, maksukorttitietojen paljastumista, tietojen aitoutta, tuoreutta tai toteutunutta kauppaa.

Todistekortti B13 22.11.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Lähde: [verkkokauppa-alusta], vuokralainen: [kauppiasyritys], kolme CRM-taulua mukaan lukien Contact ja Retail Order.

Huomio. Molemmat mainitut yritykset on salattu, koska katkaisuhetkellä ei ollut virallista vahvistusta.

Havaittu
Katkaisupäivänä 22. marraskuuta foorumimyyjä mainostaa väitettyä kolmitauluista CRM-asiakas- ja tilausvientiä liitettynä verkkokauppa-alustaan ja kauppiasyritykseen.

Ei todennettu
Aitoutta, järjestelmämurtoa, tietueiden määrää, nykyistä asiakasaltistusta tai toteutunutta kauppaa.

B

TAPAUS B

Vastaavat suomalaiset yhteystieto-CSV-näytteet loka- ja marraskuussa 2026

Väite todentamatta

Kuluttajien yhteystiedot

VÄITE

Lokakuun 9. päivänä (`B03`) foorumilla mainostettiin 15 000 rivin CSV-tiedostoa suomalaisista nimistä, osoitteista ja `+358` -puhelinnumeroista merkinnällä `Year: 2023` [S1]. Marraskuun 17. päivänä (`B14`), tuoreen 8.–22.11. jakson aikana, toinen foorumi mainosti samaa 15 000 rivin määrää ja vastaavia näyterivejä puolipisteillä ilman `Year: 2023` -merkintää [S1].

MIKÄ JÄÄ TODENTAMATTA

Täysiä tiedostoja ei hankittu, joten `B03` - ja `B14` -tiedostojen täydellinen identtisyys jää todentamatta. Kumpikaan julkaisu ei osoita vuoden 2026 murtoa, alkuperäistä lähdettä tai näytetyn vuoden 2023 keräysajankohdan paikkansapitävyyttä.

TOIMENPIDE

Vertaa mainostettuja näyterivejä vanhoihin arkistoihin, jotta kierrätetty lista ei käynnistä tarpeetonta häiriöeskalaatiota.

Ydinviesti

Vertaa mainostettuja näyterivejä aiempiin arkistoihin ennen kuin marraskuun julkaisua käsitellään uutena murtona.

Todistekortti B03	9.10.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Yhteensä 15 000 riviä, CSV-tiedosto, merkintä Year: 2023, suomalaisia nimi-, osoite- ja puhelinnumerotietoja (esimerkkirivit salattu).

Huomio. Kaikki henkilönimet, katuosoitteet ja puhelinnumerot on poistettu; B14 julkaisee myöhemmin vastaavat näyterivit ja saman rivimäärän ilman vuoden 2023 merkintää.

Havaittu
Lokakuun foorumiviesti mainostaa 15 000 rivin CSV-tiedostoa suomalaisista yhteystiedoista merkinnällä Year: 2023.

Ei todennettu
Alkuperäistä lähdettä, todellista vuoden 2023 keräysajankohtaa, koko tiedoston sisältöä, ajantasaisuutta tai vuoden 2026 murtoa.

Todistekortti B14	17.11.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Yhteensä 15 000 riviä, CSV-tiedosto puolipiste-erottimilla; vastaavat suomalaiset esimerkkirivit kuin kortissa B03 ilman vuosilukumerkintää.

Huomio. Vertailu korttiin B03 osoittaa, kuinka vastaavat näyterivit ja rivimäärät julkaistaan uudelleen ilman aiempaa vuosilukua; täysiä tiedostoja ei hankittu tai verrattu.

Havaittu
Tuoreen 8.–22. marraskuuta jakson aikana toinen foorumi mainostaa 15 000 rivin suomalaista CSV-tiedostoa, jossa on vastaavat näyterivit kuin B03:ssa puolipisteillä ja ilman Year: 2023 -merkintää.

Ei todennettu
Koko tiedoston identtisyyttä B03:n kanssa, alkuperäistä keräysvuotta, uutta marraskuun 2026 murtoa tai tuoretta yhteystietokeräystä Suomesta.

4.3 Yrityspääsyjen kysyntä, kalastelupaketit ja tunnuslistat

TAPAUS C

C

Ostokysyntä suomalaisten yritysten Microsoft 365 -pääsyille BEC-petoksiin

Kysyntä todentamatta

Yritysten identiteetti ja sähköposti

VÄITE	Helmikuun 24. päivänä (B04) foorumin ostaja haki kumppaneita, joilla on pääsy yritysten Microsoft 365- tai sähköpostitileihin Suomessa ja Saksassa laskutuspetoksia varten [S1].
MIKÄ JÄÄ TODENTAMATTA	Ostohaku osoittaa rikollista kysyntää, ei vahvistettua murtoa suomalaisyritykseen. Se julkaistiin kuitenkin helmikuussa, jolta Kyberturvallisuuskeskus myöhemmin raportoi Microsoft 365 -tilimurtojen **67 % kuukausikasvun** [S7]. Finanssialan mukaan alkuvuoden 2026 toimitusjohtaja- ja laskutushuijauksissa rikollisille menetettiin **4,9 miljoonaa euroa**, ja pankit estivät tai palauttivat erikseen **0,4 miljoonaa euroa** [S30].
TOIMENPIDE	Pakota kalastelunkestävä MFA, estä vanha tunnistautuminen ja tarpeeton Device Code Flow [S9][S11], ja valvo edelleenlähetyssääntöjä sekä OAuth-oikeuksia.

Ydinviesti

Tarkista Microsoft 365 -edelleenlähetyssäännöt, OAuth-oikeudet ja poikkeavat kirjautumiset sekä ota käyttöön kalastelunkestävä MFA.

Todistekortti B04 24.2.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Etsitään kumppaneita, joilla on pääsy yritysten Microsoft 365 -tileihin tai sähköposteihin Saksassa ja Suomessa BEC-petoksia varten.

Huomio. Kysyntähavainto julkaistiin helmikuussa, jolta Kyberturvallisuuskeskus myöhemmin raportoi Microsoft 365 -tilimurtojen kasvaneen 67 % kuukaudessa.

Havaittu
Foorumin ostaja hakee aktiivisesti kumppaneita, jotka tarjoavat pääsyä suomalaisten ja saksalaisten yritysten Microsoft 365 -sähköposteihin laskutus- ja toimitusjohtajapetoksia varten.

Ei todennettu
Onnistunutta rekrytointia, vahvistettua pääsyä mihinkään suomalaisyritykseen, taloudellista vahinkoa tai yhteyttä julkistettuihin tapauksiin.

D

TAPAUS D

Suomalaispankeille räätälöity reaaliaikainen kalastelupaketti marraskuussa

Paketti myynnissä

Pankki- ja rahoitusala

VÄITE	Marraskuun 20. ja 22. päivänä (`B15`, esitelty luvussa §9) foorumimyyjä mainosti `SALTA3`-kalastelupakettia [S1]. Ilmoitus korosti reaaliaikaista ohjausta ja mallipohjia viidelle Suomessa toimivalle merkittävälle vähittäispankille [S1].
MIKÄ JÄÄ TODENTAMATTA	Myynti-ilmoitus ei osoita pankkien järjestelmämurtoa eikä kerro aktiivisen käytön laajuutta Suomessa.
TOIMENPIDE	Pankkien ja petostorjunnan tulee testata istuntokaappauksen esto ja varmistaa, että vahvistuspyynnöt näyttävät selvästi saajan, summan ja toimenpiteen (tarkemmin luvussa §9).

Ydinviesti

Testaa reaaliaikaisen istuntokaappauksen torjunta ja varmista selkeä maksutapahtuman konteksti vahvistuspyynnöissä.

E

TAPAUS E

Kohdennetut tunnuslistat ja massalistat

Digitaaliset kuluttajapalvelut

Väite todentamatta

VÄITE

Foorumeilla kiersi vuoden 2026 aikana 10 000–100 000 rivin Suomi-merkittyjä sähköposti-salasanalistoja (kuten `B05` 13.4.) [S1]. Pienemmät osoitekohtaiset poiminnat kohdistuivat suomalaisen mediatalon kirjautumiseen (`B06`, 100 riviä), verkkokauppapaikkaan (53 riviä), kuluttajapalveluun (45 riviä) ja pankkiportaaliin (100 riviä) [S1]. Syyskuun 25. päivän "Nordic Mix" (`B07`) sisälsi oman merkintänsä `JANUARY 2024` [S1].

MIKÄ JÄÄ TODENTAMATTA

Mikään ketju ei vahvista palvelinmurtoa mainituissa yhtiöissä. Osoitekohtaiset listat syntyvät usein päätelaitteiden tietovarkauksista, ja verkkotunnuksittain nimetyt foorumilistat sisältävät usein ulkopuolisia ulkomaisia osoitteita (§9.2).

TOIMENPIDE

Käsittele osoitelistoja todennäköisinä päätelaitemurtoina, rajoita kirjautumisyrityksiä ja tarkista omat hälytykset istuntolokeista.

Ydinviesti

Käsittele osoitekohtaisia tunnuslistoja todennäköisinä päätelaitemurtoina ja varmista kirjautumisyritysten suojaus.

Todistekortti B05 — 13.4.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Tietokanta: Suomi, sähköposti ja salasana, päiväys 13.4.2026, yli 12 000 riviä, merkitty tuoreeksi.

Huomio. Merkinnät FRESH ja HQ ovat myyntipuhetta, jota liitetään rutiininomaisesti kierrätettyihin salasanalistoihin.

Havaittu
Huhtikuun foorumi-ilmoitus mainostaa Suomelle merkittyä yli 12 000 rivin sähköposti- ja salasanalistaa.

Ei todennettu
Toimivia salasanoja, yksilöllisiä henkilöitä, alkuperäistä keräysaikaa, tuoretta murtoa tai toteutunutta kauppaa.

Todistekortti B06 — 26.5.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

100 rivin URL-, sähköposti- ja salasanalista suomalaisen mediayhtiön kirjautumispalveluun, ladattu 26.5.2026.

Huomio. Verkko-osoitekohtaiset tunnuslistat ovat tyypillisesti peräisin käyttäjien laitteiden tietovarkauksista eivätkä kohdesivuston murrosta.

Havaittu
Toukokuun foorumilataus sisältää 100 riviä suomalaisen mediatalon kertakirjautumispalveluun kohdistettuja tunnuksia.

Ei todennettu
Mediatalon palvelinmurtoa, salasanojen nykyistä toimivuutta tai toteutunutta tilikaappausta.

Todistekortti B07 — 25.9.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Pohjoismainen tunnuskooste (Tanska, Norja, Ruotsi ja Suomi), jonka omien metatietojen mukaan alkuperäinen päiväys on tammikuu 2024.

Huomio. Osoittaa, kuinka vuoden 2024 aineistoa kierrätetään uusina ketjuina loppuvuonna 2026.

Havaittu
Syyskuun 2026 foorumijulkaisu jakaa pohjoismaista tunnuslistaa, jonka omassa kuvauksessa keräysajankohdaksi ilmoitetaan tammikuu 2024.

Ei todennettu
Vuoden 2026 tietomurtoa, toimivia tunnuksia, Suomen tarkkaa osuutta tai yksittäistä lähdeorganisaatiota.

4.4 Televiestintä-, väärennös- ja muulisyötteet

TAPAUS F

F

Suomalaiset eSIM-profiilit, SIM-vuokraus ja SMS-lähettäjätunnuspalvelut

Väite todentamatta

Televiestintä ja vahva tunnistaminen

VÄITE	Helmikuun 11. (B08) ja maaliskuun 2. päivänä venäjänkielinen foorumimyyjä hinnoitteli **suomalaiset eSIM-profiilit 75 dollariin** muiden Euroopan maiden rinnalla [S1]. Tammi-, helmi-, huhti- (B09), heinä- ja marraskuussa muut toimijat markkinoivat väärennettyjä SMS-lähettäjätunnuksia ja fyysisten SIM-korttien vuokrausta kertakäyttökoodien vastaanottoon [S1].
MIKÄ JÄÄ TODENTAMATTA	Ilmoitukset eivät todista toimivaa liittymäaktivointia tai Traficomin 4.5.2026 suojausmääräajan kiertämistä [S8]. Ne sopivat kuitenkin suoraan yhteen Finanssialan syyskuisen eSIM- ja mobiilivarmennevaroituksen kanssa [S30].
TOIMENPIDE	Suojaa organisaation SMS-lähettäjätunnukset Traficomilla ja lisää tarkistuksia eSIM- sekä mobiilivarmennetilauksiin.

Ydinviesti

Suojaa organisaation tekstiviestitunnukset Traficomilla ja vahvista eSIM- sekä mobiilivarmennetilausten tarkistukset.

Todistekortti B08 11.2.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi venäjä

ALKUPERÄINEN

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

KÄÄNNÖS

Saatavilla olevat eSIM-profiilit: Liettua 70 USD, Suomi 75 USD, Ranska 100 USD, Iso-Britannia 70 USD.

Huomio. Yhteystiedot on poistettu; Finanssiala varoitti syyskuussa 2026 huijareiden yhdistävän pankkitunnuksia eSIM-kortteihin ja mobiilivarmenteeseen.

Havaittu
Venäjänkielinen foorumimyyjä mainostaa suomalaisia eSIM-profiileja 75 Yhdysvaltain dollarin pyyntihinnalla muiden Euroopan maiden ohella.

Ei todennettu
Toimivaa operaattoriaktivointia, teleoperaattorin osallisuutta, varastomäärää tai toteutunutta petosta.

Todistekortti B09 29.4.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Mukautettu lähettäjätunnus yli 70 maahan kryptovaluuttamaksulla.

Huomio. Julkaistu viisi päivää ennen Traficomin 4.5.2026 voimaan tullutta tekstiviestitunnusten suojausmääräaikaa.

Havaittu
Huhtikuun lopun foorumi-ilmoitus markkinoi väärennettäviä tekstiviestien lähettäjätunnuksia yli 70 maahan kryptovaluuttaa vastaan.

Ei todennettu
Viestien läpimenoa suojatuille suomalaisille SMS-tunnuksille Traficomin toukokuun 2026 määräajan jälkeen tai yhteyttä yksittäiseen kalasteluaaltoon.

TAPAUS G

G ■ Väärennetyt suomalaiset palkkalaskelmat, FI-IBAN-tilit ja muulivärväys

Väite todentamatta

Identiteetti, maksaminen ja toimitus

VÄITE	Foorumeilla myytiin suomalaisia palkkalaskelma- ja työsopimuspohjia (B10 , §8) sekä 25 dollarin EU-tason KYC-kuvapaketteja (Know Your Customer, asiakkaan tunteminen ja tunnistaminen) [S1]. Lisäksi tarjottiin väitettyjä FI-IBAN-yritystilejä (B16 , §9; ostohaku Telegramissa 8.11.), suomalaisia noutomuuleja älypuhelimille (B11 , §8) ja bulvaaniyritysten perustajia Suomi mukaan lukien (B12 , §8) [S1].
MIKÄ JÄÄ TODENTAMATTA	Yksikään viesti ei osoita toteutunutta pankkitilin avausta, myymälävarkautta tai aktiivista suomalaissolua.
TOIMENPIDE	Vahvista asiakirjojen tarkistusta, valvo arvokkaita noutotilauksia ja syvennä uusien yritystilien tunnistamista (luvut §8 ja §9).

Ydinviesti

Vahvista asiakirjojen tarkistusta ja seuraa arvokkaiden noutotilausten sekä uusien yritystilien avauksia.

KESKEISET HAVAINNOT

01

Alamaailman julkaisut osoittavat rikollista tarjontaa ja kysyntää, eivät vahvistettuja suomalaisvuotoja.

02

Näytevertailu havaitsi 17.11. julkaisun, jonka näyterivit ja rivimäärä vastaavat lokakuun 2023-merkittyä CSV:tä.

03

Kytke alamaailman petosvälineet suoraan Suomen pankki-, M365- ja televalvontaan.

LUKU 05

Julkiset tietoturvapoikkeamat, toimittajat ja tuore aktiviteetti

TÄMÄ LUKU VASTAA

Mitkä julkisesti raportoidut tapahtumat vaikuttivat suomalaisiin palveluihin vuonna 2026 (ml. 8.–22.11.)?

14

julkista tapauskuvausta tammikuusta 22. marraskuuta 2026 saakka

5.1 Tammi–heinäkuu 2026: nollapäivät, toimittajat ja vanhat arkistot 41

5.2 Elo–marraskuun alku 2026: rajapinnat, nollapäivät ja OT-laitteet 44

5.3 Tuore aktiviteetti: 8.–22. marraskuuta 2026 48

LUKU 05

Julkiset tietoturvapoikkeamat, toimittajat ja tuore aktiviteetti

LYHYESTI

Neljätoista tapauskuvausta kokoaa vahvistettuja vuoden 2026 suomalaisia ja pohjoismaisia tietomurtoja, valtionhallinnon varotoimisulun sekä yhden alueellisen uutisotsikon valtionhallinnosta, sote-alalta, korkeakouluista, kirjastoista, Ahvenanmaalta, päivittäistavarakaupasta ja lentoliikenteestä. Neljä teemaa toistuu: reunalaitteiden nollapäivät, toimittajamurrot, vanhojen arkistojen säilytys ja eristämättömät automaatio-ohjaimet. Tuore 8.–22.11. jakso toi Finnairin/Amadeuksen tiedotteen ja Lykon murron. Kartoita toimittajariippuvuudet, hävitä vanhat arkistot ja valtuuta nopea reunaeristys.

5.1 Tammi–heinäkuu 2026: nollapäivät, toimittajat ja vanhat arkistot

H

TAPAUS H

Valtorin mobiililaitehallinnan nollapäivämurto

Valtionhallinnon ICT

Vahvistettu nollapäivä

AIKAJANA	Valtion tieto- ja viestintätekniikkakeskus Valtori havaitsi 30.1.2026 mobiililaitehallintapalveluunsa kohdistuneen murron Ivanti Endpoint Manager Mobile -nollapäivähaavoittuvuuksien kautta (`CVE-2026-1281` ja `CVE-2026-1340`, julkaistu 29.1.2026) [S7][S32][S59][S60]. Alustava 3.2. arvio koski 20 000 laitetta; helmikuun 5. päivänä Valtori laajensi arvion jopa **50 000 valtionhallinnon käyttäjätietoon** ministeriöissä [S32]. Myöhempi Ylen ja STT:n uutisointi **7.5.2026** kertoi viranomaisasiakirjojen vahvistaneen murron osuneen myös useiden muiden valtionhallinnon organisaatioiden laitteisiin [S33].
ALTISTUNEET TIEDOT JA LAAJUUS	Selvityksessä ilmeni, että järjestelmä oli vain merkinnyt vanhat tiedot poistetuiksi hävittämisen sijaan [S32]. Vaarantuneet tiedot sisälsivät nimiä, työsähköposteja, puhelinnumeroita ja laitetietoja, mutteivät laitteille tallennettua sisältöä [S32]. Uutisoinnin mukaan Keskusrikospoliisi (KRP) tutkii tapausta [S33]. Haavoittuvat EPMM-versiot, korjaavat julkaisut ja valmistajan RPM-paketit on koottu lukuun §12.2 [S59][S60][S81][S82].
TOIMENPIDE	Päivitä korjattuun EPMM-versioon tai asenna valmistajan RPM-paketti luvun §12.2 mukaisesti, tarkista hallintajärjestelmien todellinen tietojen poisto ja eristä internetiin näkyvät konsolit heti kriittisen varoituksen tullessa.

Ydinviesti

Tarkista hallintajärjestelmien poistorutiinit ja eristä haavoittuvat reunalaitteet heti varoituksen tullessa.

TAPAUS I

I ■ Aalto EE ja Aalto-yliopisto: Instructure Canvas -toimittajamurto

Vahvistetut tiedotteet

Korkeakoulutus ja johtamiskoulutus

AIKAJANA	Ulkopuolinen toimija tunkeutui Instructuren Canvas-oppimisalustaan 25.–29.4.2026 osana laajasti uutisoitua globaalia tietomurtoa [S37][S84]. Instructure vahvisti 6.5. murron koskevan Aalto EE:n lisensoitua Canvas-ympäristöä, ja Aalto EE julkaisi virallisen tietoturvaloukkaustiedotteen sekä ilmoitti tietosuojavaltuutetulle **7.5.2026** [S37]. Erikseen **11.5.2026** Aalto-yliopisto julkaisi varotoimitiedotteensa todeten, ettei yliopistolla ole organisaatiolisenssiä Canvasiin, mutta yksittäiset opiskelijat tai työntekijät ovat voineet käyttää palvelua itsenäisesti [S38].
MAHDOLLISESTI ALTISTUNEET TIEDOT	Aalto EE:n tiedotteen mukaan sen Canvas-käyttäjiltä ovat saattaneet paljastua nimet, sähköpostiosoitteet, Canvas-rekisteritunnisteet ja alustan sisäisten viestien sisällöt [S37]. Aalto EE kertoi, ettei salasanojen, maksutietojen tai henkilötunnusten havaittu vaarantuneen [S37].
TOIMENPIDE	Kartoita yksikkökohtaiset SaaS-ympäristöt ja varoita käyttäjiä kurssiviestien kontekstia hyödyntävästä kalastelusta.

Ydinviesti

Kartoita yhteisen SaaS-alustan asiakasympäristöt ja varoita käyttäjiä viestisisältöä hyödyntävästä kalastelusta.

TAPAUS J

J ■ Kolmostien Terveyden arkistotiedosto ja Pirkanmaan muistitikkutapaus

Viralliset tiedotteet

Sosiaali- ja terveyspalvelut

AIKAJANA	Pirkanmaan hyvinvointialue ja Pihlajalinna tiedottivat 25.8.2026 Kolmostien Terveyden helmikuulta 2016 tai sitä vanhemmasta tiedostosta, johon murtauduttiin 24.7.2026 [S39][S83]. Aiemmin 13.1.2026 Pirkanmaan hyvinvointialue tiedotti erillisestä fyysisestä loukkauksesta kirpputorilta löytyneen muistitikun vuoksi [S40].

ALTISTUNEET TIEDOT	Kolmostien Terveyden tiedosto sisälsi **10 263 suomalaista henkilötunnusta** (ilman potilasnimiä) ja omaisten puhelinnumeroita noin 12 000 ihmiseltä, kun aktiiviset potilastiedot säilyivät koskemattomina [S39]. Muistitikulla oli vuosien 2020–2021 Akaan ja Urjalan eristys- ja karanteenipäätöksiä [S40].
TOIMENPIDE	Inventoi ja hävitä hyvinvointialueuudistuksessa siirtyneet vanhat kunta-arkistot sekä pakota kaikkien siirrettävien tallennusvälineiden salaus.

Ydinviesti

Inventoi ja poista vanhat kuntasiirtoaineistot sekä vaadi kaikkien siirrettävien tallennusvälineiden salaus.

TAPAUS K

K

Suomalaisen talous- ja yrityspalveluyhtiön heinäkuun tietomurto (nimi salattu)

Vahvistettu tiedote

Talous- ja yrityspalvelut

VAHVISTETTU KULKU	Heinäkuussa 2026 suomalainen talous- ja yrityspalveluyhtiö vahvisti virallisessa tiedotteessa sisäiseen IT-ympäristöönsä kohdistuneen tietomurron [S49]. Yhtiö ilmoitti tapauksesta havaitsemispäivänä Kyberturvallisuuskeskukselle, tietosuojavaltuutetulle ja poliisille, kertoi lyhyistä häiriöistä ja mahdollisesta pääsystä tiedostojärjestelmiin sekä totesi merkittävien asiakasvaikutusten jääneen tiedossa olevien tietojen mukaan pois [S49]. Yhtiön nimi ja tiedoteosoite salataan rajallisen valtakunnallisen tai alueellisen uutisoinnin vuoksi [S49].
TOIMENPIDE	Eriytä jaetut tiedostopalvelimet ydintuotannosta ja varmista palautus muuttumattomista varmuuskopioista.

Ydinviesti

Eriytä jaetut tiedostopalvelimet ydintuotannosta ja varmista varmuuskopioiden palautuvuus erikseen.

5.2 Elo–marraskuun alku 2026: rajapinnat, nollapäivät ja OT-laitteet

L

TAPAUS L

Ryden pohjoismainen asiakastietomurto Suomi mukaan lukien

Kuluttajien liikkumispalvelut

Vahvistettu murto

VAHVISTETTU KULKU	Pohjoismainen sähköpotkulautaoperaattori Ryde vahvisti 2.8.2026 (päivitetty 5.8.) asiakastietojen luvattoman kopioinnin [S46]. Murto koski kaikkia tiliä käyttäviä asiakkaita Norjassa, Ruotsissa, Suomessa ja Saksassa, ja yhtiö ilmoitti asiasta Norjan tietosuojaviranomaiselle [S46]. Tiedote ei eritellyt Suomen osuutta [S46].
TOIMENPIDE	Käsittele pohjoismaisia kuluttajavuotoja paikallisena kalasteluriskinä silloinkin, kun rekisterinpitäjä sijaitsee naapurimaassa.

Ydinviesti

Valmistele asiakasohjeistus rajat ylittäviin tilimurtoihin, joissa suomalaisilla on aktiivisia sovellustilejä.

M

TAPAUS M

Rahaliike Holmaston asiakashakurajapinnan tietoturvaloukkaus

Erikoiskauppa

Vahvistettu murto

VAHVISTETTU KULKU	Helsinkiläisen Rahaliike Holmaston asiakashakurajapinnan haavoittuvuuden kautta ulkopuolinen automaattinen järjestelmä haki asiakasrekisterin tietoja 30.8.2026 [S43]. Loukkaus koski noin **70 % asiakkaista**, ennen kuin hakupalvelun oma suojaus pysäytti haut [S43]. Holmasto julkaisi tiedotteen 2.9., ilmoitti tietosuojavaltuutetulle ja poliisille sekä tiedotti asiakkaita sähköpostitse ja tekstiviestein 14.–15.9. saakka [S43].
TOIMENPIDE	Varmista asiakashakurajapintojen todennus, pääsynhallinta ja nopeusrajoitukset sekä minimoi säilytettävät henkilötunnukset.

Ydinviesti

Varmista asiakashakurajapintojen todennus ja nopeusrajoitukset sekä arvioi henkilötunnusten säilytystarve.

N

TAPAUS N

Suomalaisen koulutus- ja valmennusorganisaation syyskuun kyberhyökkäys (nimi salattu)

Koulutus ja valmennus

Vahvistettu hyökkäys

VAHVISTETTU KULKU

Syyskuussa 2026 suomalainen koulutus- ja valmennusorganisaatio tiedotti ICT-ympäristöönsä kohdistuneesta hyökkäyksestä, joka korruptoi osan palvelinympäristöstä ja mahdollisti luvattoman pääsyn järjestelmiin ja mahdollisesti niihin tallennettuihin tietoihin [S50]. Koska tietoja ei voitu teknisesti yksilöidä, yksittäisiä henkilöitä ei voitu erikseen tiedottaa [S50]. Organisaatio ilmoitti tapauksesta tietosuojavaltuutetulle, Kyberturvallisuuskeskukselle ja poliisille; nimi ja tiedoteosoite jätetään mainitsematta [S50].

TOIMENPIDE

Kiirehdi vanhojen konesalien alasajoa ja pidä lokitus tasolla, jolla altistuneet tiedostot voidaan rajata.

Ydinviesti

Nopeuta vanhojen konesalien alasajoa ja pidä lokitus tasolla, jolla altistuneet tiedot voidaan rajata.

TAPAUS O

Kunnallisten Koha-kirjastojärjestelmien palvelunestohyökkäys

Kunnalliset kirjastojärjestelmät

Viralliset tiedotteet

VAHVISTETTU KULKU

Syyskuun 16.–17. päivänä (hallintaan noin klo 10) palvelunestohyökkäys häiritsi jaettuja Koha-kirjastojärjestelmiä useissa suomalaisissa kunnallisissa kirjastokimpoissa [S41][S42]. Kuntien virallisten tiedotteiden mukaan kirjastojen palvelimia käytettiin välikätenä kolmanteen maahan kohdistuneessa liikenteessä, eikä tietojen altistumisesta ollut merkkejä [S41] [S42]. Kunnallisten toimijoiden nimiä ja tiedoteosoitteita ei luetella tässä [S41] [S42].

TOIMENPIDE

Tarkista avoimet kunnalliset verkkopalvelut liikenteen vahvistusväärinkäytön varalta ja pidä operaattorisuojauksen yhteystiedot ajan tasalla.

Ydinviesti

Tarkista avoimet verkkopalvelut liikenteen vahvistusväärinkäytön varalta ja pidä suojausyhteystiedot ajan tasalla.

TAPAUS P

P Raportoitu syyskuun tietomurto ahvenanmaalaisessa organisaatiossa

Uutisraportti

Ahvenanmaalainen organisaatio

UUTISOTSIKKO JA VARMENNUSTILA	Syyskuussa 2026 ahvenanmaalainen paikallismedia uutisoi ahvenanmaalaisen organisaation tehneen tietomurrosta rikosilmoituksen [S45]. Organisaation nimi jätetään mainitsematta, eikä teknisiä yksityiskohtia raportoida [S45].
TOIMIVALTAHUOMIO	Toimivaltainen tietosuojaviranomainen määräytyy rekisterinpitäjän toiminnan sekä sovellettavan valtakunnan- tai maakuntalainsäädännön perusteella, ei pelkän Ahvenanmaalla sijainnin mukaan. Datainspektionen valvoo maakunta- ja kunnallishallintoa sekä määriteltyjä maakunnan toimivaltaan kuuluvia toimintoja, kun taas valtakunnallinen tietosuojavaltuutettu valvoo yksityisiä toimijoita [S23][S76][S79].
TOIMENPIDE	Määritä toimivaltainen tietosuojaviranomainen toiminnan ja sovellettavan lain perusteella etukäteen ennen poikkeamaa.

Ydinviesti

Määritä toimivaltainen tietosuojaviranomainen toiminnan ja sovellettavan valtakunnan- tai maakuntalain perusteella, ei pelkän sijainnin mukaan.

TAPAUS Q

Q Citrix NetScaler ADC- ja Gateway -nollapäivien hyväksikäyttö Suomessa

Virallinen varoitus

Verkon reunalaitteet eri toimialoilla

AIKAJANA	Citrix julkaisi **27.9.2026** kriittiset NetScaler ADC- ja Gateway-haavoittuvuudet (`CVE-2026-88771` ja `CVE-2026-88772`) sekä korjauspäivitykset [S61][S62]. Kyberturvallisuuskeskus antoi **1.10.2026** vuoden ensimmäisen vakavan varoituksensa (`1/2026`), joka kattaa kahdeksan haavoittuvuutta (`CVE-2026-88771` – `CVE-2026-88778`) [S13][S80]. Virasto vahvisti useita murtoja Suomessa ennen päivityksiä ja kehotti etsimään murron jälkiä [S14][S80].
HAAVOITTUVA LAAJUUS	Syyskuun vähimmäisversiot sekä Citrixin 12. marraskuuta julkaisemat uudemmat tietoturvapäivitykset (`CTX697305`, `CVE-2026-120868`) vakio-, FIPS- ja NDcPP-haaroille on esitetty luvussa §12.2 [S14][S61][S62][S80][S87]. Kyberturvallisuuskeskus painotti, ettei pelkkä päivitys poista ennen korjausta tunkeutunutta hyökkääjää [S14][S80].

TOIMENPIDE	Päivitä vakio-, FIPS- ja NDcPP-laitteet luvun §12.2 ajantasaisiin korjattuihin versioihin (tai siirry pois tukea vailla olevista haaroista), tutki laitteet pysyvyyden varalta ja mitätöi aktiiviset VPN-istunnot.

Ydinviesti

Päivitä NetScaler-laitteet välittömästi, etsi aiemman murron merkkejä ja uusi istuntoavaimet.

R

TAPAUS R

Valtorin varotoimisulku PHP-haavoittuvuuksissa ja Eckerö Linen alihankkijamurto

Sulku ja murto

Valtion verkkopalvelut ja laivaliikenne

VALTORIN PHP-VAROTOIMISULKU	Lokakuun 21. päivänä Kyberturvallisuuskeskus julkaisi tiedotteen 37/2026 kriittisistä PHP-haavoittuvuuksista (`CVE-2026-109618` ja `CVE-2026-109619`) ennen klo 17 korjauspäivitystä [S15][S63][S64][S72]. Valtori ajoi alas julkisia valtionhallinnon verkkopalveluja eri virastoissa ilmoitettuna varotoimena palvelujen suojaamiseksi ilman tiedossa ollutta aktiivista hyväksikäyttöä tiedotehetkellä [S34]. Haavoittuvat haarat, lokakuun vähimmäisversiot sekä erillisen 19. marraskuuta korjatun kriittisen istuntohaavoittuvuuden (`CVE-2026-115560`) korjaavat julkaisut on esitetty luvussa §12.2 [S15][S72][S85][S86].
ECKERÖ LINEN ALIHANKKIJAMURTO	Pian sen jälkeen Eckerö Line tiedotti varausjärjestelmätoimittajansa alihankkijan murrosta [S44]. Tapaus havaittiin ja rajattiin 26.10. (ilmoitettiin Eckerö Linelle 28.10.) ja paljasti noin **200 asiakkaan** varaustietoja ilman maksukorttitietoja [S44].
TOIMENPIDE	Asenna luvun §12.2 ajantasaiset korjaavat PHP-versiot tai siirry pois elinkaarensa päättyneistä haaroista, kohtele varotoimisulkua hyväksyttynä suojakeinona ja sido alihankkijat nopeaan ilmoitusvelvollisuuteen.

Ydinviesti

Sovi ennalta nopeista varotoimisuluista ja vaadi varausjärjestelmien alihankkijoilta nopeaa ilmoittamista.

TAPAUS S

S

Euroopan päivittäistavarakauppojen kylmälaitehyökkäykset Suomessa

Päivittäistavarakauppa ja OT-laitteet

Virallinen varoitus

AIKAJANA	Loka–marraskuun vaihteessa epäillyt kyberiskut Ranskassa, Belgiassa, Ruotsissa, Irlannissa ja Virossa kohdistuivat verkkoon kytkettyihin kylmäautomaatio-ohjaimiin nostaen lämpötiloja ja aiheuttaen hävikkiä [S48] [S73]. Kyberturvallisuuskeskus kertoi 6.11. olleensa yhteydessä haavoittuvien suomalaislaitteiden omistajiin jo **13.10.2026 alkaen** [S18].
VAIKUTUS SUOMESSA	Marraskuun alussa suomalaismedia uutisoi muutamien päivittäistavarakauppojen lyhyistä kylmälaitehäiriöistä, joiden syytä ei ollut vahvistettu [S48]. Erikseen Kyberturvallisuuskeskus raportoi epäillyistä tapauksista 3.11. ja vahvisti 6. ja 13.11. Suomessa havaitun muutamia ilkivaltaisia kylmälaitetapauksia [S16][S18][S19]. Virasto totesi aiemman varautumisen ja ennakoivien yhteydenottojen vähentäneen alttiita laitteita ja auttaneen välttämään suurimmat vahingot [S18][S19].
TOIMENPIDE	Poista kylmä- ja kiinteistöautomaation ohjaimet julkisesta internetistä välittömästi ja tarkista paikallinen varakäyttö.

Ydinviesti

Poista kylmä- ja kiinteistöautomaation ohjaimet julkisesta verkosta ja varmista turvallinen paikallinen ohjaus.

5.3 Tuore aktiviteetti: 8.–22. marraskuuta 2026

Katkaisua edeltäneet 15 päivää (`8.–22.11.2026`) sisälsivät **984 Suomeen merkittyä alamaailmajulkaisua**, mukaan lukien **19 foorumiviestiä** [S1]. Jakso toi myös yhden merkittävän toimittajatiedotteen, yhden pohjoismaisen kauppamurron ja kaksi Kyberturvallisuuskeskuksen viikkokatsausta [S19][S20][S35][S47]. Havainnot koskevat vain tätä 15 päivän jaksoa.

T

TAPAUS T

Finnair ja Aurinkomatkat: Amadeuksen maailmanlaajuinen varaustietovuoto

Virallinen tiedote

Lentoliikenne ja valmismatkat

AIKAJANA JA LAAJUUS	Marraskuun **9. päivänä 2026** Finnair julkaisi virallisen Cision-tiedotteen maailmanlaajuisen matkailutoimittaja Amadeuksen tietovuodosta, jossa useiden lentoyhtiöiden matkustajalistoilla oli mukana noin **116 000 Finnairin varausta** [S35][S36]. Amadeuksen mukaan näistä noin **750 varausta** avattiin tarkasteltavaksi, mukana noin **30 Aurinkomatkojen** valmismatkaa, ja luvaton toiminta pysäytettiin [S35].
ALTISTUNEET TIEDOT JA RAJAUS	Vain murto-osa tarkastelluista varauksista oli enää aktiivisia, ja Finnair vaihtoi niihin uudet varausnumerot [S35]. Luottokorttitietoja tai salasanoja ei vaarantunut, Finnairin omiin järjestelmiin ei tunkeuduttu, ja Amadeus teki GDPR-ilmoituksen rekisterinpitäjänä [S35].
TOIMENPIDE	Vaihda aktiiviset varauskoodit nopeasti toimittajavuodossa ja varoita matkustajia vanhoja lentotietoja käyttävistä huijauksista.

Ydinviesti

Vaihda aktiiviset varausnumerot nopeasti ja varoita matkustajia vanhoja lentotietoja käyttävistä huijauksista.

U

TAPAUS U

Lykon pohjoismainen verkkokauppamurto

Virallinen tiedote

Pohjoismainen verkkokauppa

VAHVISTETTU KULKU	Marraskuun puolivälissä (`12.–18.11.`) pohjoismainen verkkokauppa **Lyko** kertoi rajatun järjestelmän murrosta, josta suomalaismedia (Voice.fi) varoitti paikallisia asiakkaita [S47][S71].
TOIMENPIDE	Nojaa asiakasviestinnässä rekisterinpitäjän uusimpaan laajuustietoon rajat ylittävissä kauppamurroissa.

Ydinviesti

Nojaa asiakasviestinnässä rekisterinpitäjän uusimpaan laajuustietoon rajat ylittävissä kauppamurroissa.

Muut 8.–22. marraskuuta havainnot:

- **12. marraskuuta:** Lokakuun Kybersää nosti esiin kasvaneet WordPress-murrot ja ClickFix-haittaohjelmalevityksen [S17].

- **13. ja 20. marraskuuta:** Viikkokatsaukset 46 ja 47 varoittivat pankkien nimissä soitetuista robottipuheluista, Black Friday -valekaupoista ja kotireitittimien käytöstä rikollisten välityspalvelimina [S19][S20]. Viikkokatsaus 47 nosti esiin suomenkielisen EU:n kyberkestävyyssäädöksen soveltamisohjeen [S20].
- **17., 20. ja 22. marraskuuta:** Foorumeilla julkaistiin 15 000 rivin suomalainen CSV, jossa oli vastaavat näyterivit kuin lokakuun 2023-merkityssä `B03`:ssa ilman vuosilukua (`B14`), ja mainostettiin kahdesti viidelle suomalaispankille suunnattua `SALTA3`-pakettia (`B15`) [S1]. Lisäksi 22.11. julkaistiin väitetty kolmitauluisen kauppapaikan CRM-vienti (`B13`) [S1].

KESKEISET HAVAINNOT

01

Reunalaitteiden nollapäivät sekä SaaS- ja varaustoimittajien murrot aiheuttivat merkittäviä altistuksia vuoden 2026 dokumentoitujen tapausten joukossa.

02

Vanhat arkistot ja salaamattomat tallennusvälineet ovat yhä sote-alan tietosuojariski.

03

Tuore 8.–22.11. jakso yhdisti vahvistetut tiedotteet pankkikalastelupaketteihin ja kierrätettyyn dataan.

LUKU 06

Häiriöt, haktivismi ja väitteet vastaan todellisuus

TÄMÄ LUKU VASTAA

Miten suomalaiset puolustajat erottavat väitetyt hyökkäykset todennetusta palveluvaikutuksesta?

23

NoName057(16)-hyökkäyskierrosta 129 suomalaisorganisaatioon (Aalto-tutkimus)

6.1 Vuoden 2026 häiriöiden ja varautumisen aikajana 52

6.2 Pelillistetyt palvelunestohyökkäykset ja psykologinen paine 53

6.3 Väite vastaan virallinen tieto 53

LUKU 06

Häiriöt, haktivismi ja väitteet vastaan todellisuus

LYHYESTI

Palveluhäiriöt Suomessa jakautuvat vuonna 2026 kolmeen luokkaan: pelillistettyihin palvelunestohyökkäyksiin, avoimien järjestelmien välikäsiväärinkäyttöön sekä ennakoiviin varotoimisulkuihin kriittisten haavoittuvuuksien aikana. Aalto-yliopiston tutkijat kuvaavat NoName057(16)-ryhmän venäjämieliseksi ja arvioivat sen pyrkivän murentamaan kansalaisten luottamusta hallituksiin. Maaliskuun Telegram-väitteet suomalaisista asuntokameroista jäävät todentamatta ilman virallista vahvistusta. Nojaa omaan valvontaan ja selkeään häiriöviestintään.

6.1 Vuoden 2026 häiriöiden ja varautumisen aikajana

30.1.2026	Valtori havaitsee Ivanti EPMM -nollapäivämurron ja eristää palvelun [S7][S32]
5.3.2026	Telegram-kanavat jakavat todentamattomia Morningstar-väitteitä suomalaisista asuntokameroista [S1]
1.6.2026	Kansallinen kyberkestävyyslaki tulee voimaan Suomessa [S9]
27.8.2026	Helsingin hovioikeus kumoaa käräjäoikeuden päätöksen ja katsoo Suomella olevan toimivalta joulukuun 2024 Eagle S -kaapelitapauksessa [S57]
16.9.2026	Kunnallisia Koha-kirjastopalvelimia käytetään DDoS-välikätenä suomalaisissa kirjastokimpoissa [S41] [S42]
27.9.2026	Citrix julkaisee kriittiset NetScaler ADC- ja Gateway-nollapäivähaavoittuvuudet (CVE-2026-88771, CVE-2026-88772) [S61][S62]
1.10.2026	Kyberturvallisuuskeskus antaa vakavan varoituksen 1/2026 ja vahvistaa useita NetScaler-murtoja Suomessa [S13][S14][S80]
13.10.2026	Kyberturvallisuuskeskus aloittaa ennakoivat yhteydenotot haavoittuvien kylmälaitteiden omistajiin [S18]
21.10.2026	Valtori sulkee julkisia valtion verkkopalveluja varotoimena ennen PHP-päivityksiä [S15][S34]
3.11.2026	Kyberturvallisuuskeskus raportoi epäillyistä kylmälaitetapauksista Suomessa; muutama vahvistetaan 6. ja 13.11. [S16][S18][S19]
9.11.2026	Finnair tiedottaa Amadeuksen varaustietovuodosta (noin 116 000 varausta; noin 750 avattu) [S35]

6.2 Pelillistetyt palvelunestohyökkäykset ja psykologinen paine

Aalto-yliopiston kauppakorkeakoulun vuoden 2026 tutkimus selvitti tutkijoiden venäjämieliseksi kuvaaman **NoName057(16)**-ryhmän toimintaa [S53]. Tutkimus dokumentoi **23 palvelunestohyökkäyskierrosta** Suomeen 7.1.2025 alkaen, vaikuttaen **129 julkiseen ja yksityiseen organisaatioon**, mukaan lukien julkiset toimijat, kunnat ja rahoituslaitokset [S53]. Tutkijat totesivat hyökkäysten lisääntyneen merkittävästi vuoden 2023 Nato-jäsenyyden jälkeen [S53]. He arvioivat, että vaikka palvelunestohyökkäykset voivat häiritä julkisia palveluja, pelillistetyt kampanjat pyrkivät aktiivisesti murentamaan kansalaisten luottamusta hallituksiin [S53].

Ilmoitetut palvelunestotapaukset laskivat noin 9 % vuonna 2025 [S5]. Ilmoittaminen on vapaaehtoista, joten lasku ei osoita vastaavaa hyökkäysten vähenemistä eikä parantunutta suojausta [S5]. Syyskuun kunnallinen **Koha**-kirjastotapaus toi esiin toisenlaisen riskin: kunnallisten verkkopalvelujen valjastamisen ulospäin suuntautuvan hyökkäysliikenteen välikädeksi [S41][S42].

6.3 Väite vastaan virallinen tieto

Todentamattomat Telegram-kanavat liioittelevat rutiinikatkoja, varotoimia ja todentamattomia kuvakaappauksia onnistuneina iskuina. Alla oleva taulukko osoittaa oman teknisen varmennuksen tärkeyden.

Väite tai julkinen mielikuva	Vahvistettu tilanne	Puolustajan toimintatapa
Maaliskuun Telegram-viestit välittävät Morningstar-väitteitä pääsystä suomalaisiin ovipuhelinkameroihin [S1]	Suomea koskeva murtoväite jää todentamatta; virallista vahvistusta tai avoimesti todennettua selvitystä suomalaisesta murrosta ei ole [S1]	Varmenna kuvakaappaukset, laitteiden verkkonäkyvyys ja paikalliset lokit ennen murron olettamista
Lokakuun valtionhallinnon verkkokatko tulkitaan tietomurroksi [S34]	Valtori vahvisti ennakoivan varotoimisulun ennen PHP-päivityksiä ilman tiedossa ollutta aktiivista hyväksikäyttöä tiedotehetkellä [S15] [S34]	Tiedota selkeästi ennakoivasta suojauksesta ja palautusaikataulusta
Helmikuun 0apt-listaukset väittävät kolmen Suomeen merkityn kohteen murtoa samana päivänä [S2]	Kolme suomalaista merkintää jäävät todentamatta; Halcyon esittää yleisen varoituksen 0apt:n alkuvuoden liioitelluista tai virheellisistä uhriväitteistä toimivasta salaajasta huolimatta [S54]	Vaadi oma lokitodennus ennen tietovuodon julistamista

Väite tai julkinen mielikuva	Vahvistettu tilanne	Puolustajan toimintatapa
Euroopan pakastinhälytykset herättävät pelon laajasta ruokaketjukriisistä [S48] [S73]	Kyberturvallisuuskeskus vahvisti Suomessa muutamia tapauksia ja totesi 13.10. alkaneen ennakoinnin vähentäneen alttiita laitteita sekä aiemman varautumisen auttaneen välttämään suurimmat vahingot [S16][S18][S19]	Tarkista paikallinen laitealtistus kiinteistötekniikan kanssa
Haktivistikanavat väittävät pitkäkestoisia kaatoja ministeriöille ja pankeille [S53]	Aalto-tutkijat arvioivat tavoitteeksi kansalaisten luottamuksen murentamisen hallituksiin [S53]. Ilmoitetut palvelunestotapaukset laskivat noin 9 % vuonna 2025, mutta vapaaehtoinen ilmoittaminen ei osoita vastaavaa hyökkäysten vähenemistä tai parantunutta suojausta [S5]	Mittaa omaa käytettävyyttä ja viesti rauhallisesti toistamatta uhkaretoriikkaa

KESKEISET HAVAINNOT

01

Erota haktivistiväitteet, välikäsiväärinkäyttö ja varotoimisulut toisistaan häiriöviestinnässä.

02

Aalto-yliopiston tutkijat arvioivat näiden DDoS-kampanjoiden pyrkivän murentamaan kansalaisten luottamusta hallituksiin; arvioi tekninen vaikutus erikseen palveluvalvonnasta.

03

Julkaise rauhallisia aikaleimattuja tilannetiedotteita oman valvonnan perusteella.

LUKU 07

Kiristyshaittaohjelmat, vakoiluvaroitukset ja toimijaprofiilit

07

TÄMÄ LUKU VASTAA

Ketkä nimeävät suomalaisia kohteita, ja mikä erottaa kiristysnimikkeen valtiollisesta varoituksesta?

16

Suomeen merkittyä kiristyshaittaohjelmalistausta 8 nimikkeellä

7.1 Alueelliset kiristyshaittaohjelmalistaukset ja kausivaihtelu 56

7.2 Uhkaprosessien suhdekartta ja profiloidut ryhmät 58

7.3 Valtiolliset vakoiluvaroitukset ja haktivismi 61

LUKU 07

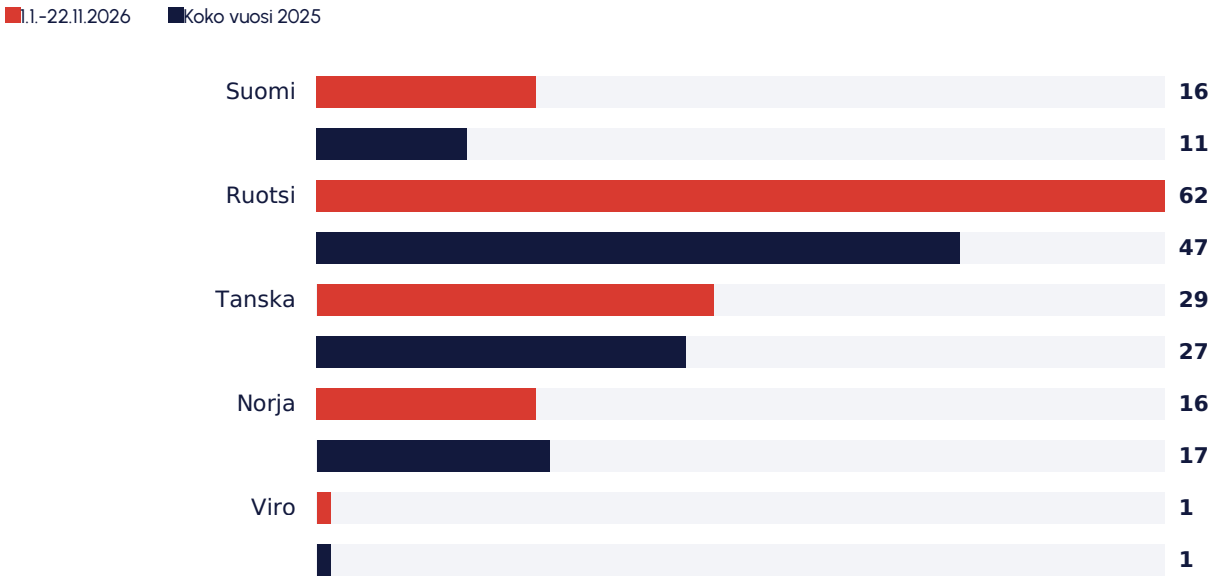
Kiristyshaittaohjelmat, vakoiluvaroitukset ja toimijaprofiilit

LYHYESTI

Ransompedia tallensi 16 Suomeen merkittyä kiristyshaittaohjelmalistausta 1.1.–22.11.2026, ylittäen koko vuoden 2025 luvun 11 ja vastaten Norjan 16 listausta. Kolmetoista 16 listauksesta julkaistiin kesä–marraskuussa, kaksi toistoa rajaa yksilölliset väitteet enintään 14:ään ja kaikki listaukset jäävät todentamatta. FBI:n ja Kyberturvallisuuskeskuksen varoitukset kuvaavat valtiollisesti attribuoitua toimintaa; GTIG arvioi korkealla varmuudella UNC7005:llä olevan Venäjä-kytköksen (ICE RELIC -yhteys kohtalaisella varmuudella). Varmenna jokainen kiristyslistaus omista lokeista, päivitä haavoittuvat reitittimet ja Zimbra-palvelimet sekä rajoita todentamattomia OAuth-oikeuksia.

7.1 Alueelliset kiristyshaittaohjelmalistaukset ja kausivaihtelu

Suomen 16 kiristyshaittaohjelmalistausta ylittävät vuoden 2025 tason ja vastaavat Norjaa



Lähde: Brandefense Ransompedia, 1.1.-22.11.2026 verrattuna koko vuoteen 2025 [S2]. Eripituiset jaksot; maamerkityt väitteet eivät kuvaa yksittäisiä uhreja, vahvistettuja murtoja tai kansallista paremmuusjärjestystä.

Vertailumaat on valittu esimerkeiksi ainoastaan kontekstin antamiseksi; ne eivät merkitse paremmuusjärjestystä tai poliittista arviota.

Jaksolla 1.1.–22.11.2026 Ransompedia kirjasi **16 Suomeen merkittyä listausta 8 eri nimikkeellä**, kun koko vuonna 2025 niitä oli **11** (kaikkina aikoina 40) [S2]. Vertailumaissa **Ruotsissa oli 62** (2025: 47), **Tanskassa 29** (2025: 27), **Norjassa 16** (2025: 17) ja **Virossa 1** (2025: 1) [S2].

Neljä havaintoa auttaa tulkitsemaan Suomen 16 listauksen lukua oikein [S2]:

- **Toistuvat listaukset pienentävät yksilöllisten kohteiden määrää.** INC Ransom listasi saman suomalaisorganisaation kahdesti loppuvuonna 2026 [S2]. Clop listasi vastaavasti saman Suomeen kytketyn organisaation kahdesti loppuvuonna 2026 [S2]. Näin 16 listauksen taustalla on enintään **14 erillistä väitettyä kohdetta** [S2].
- **Alkuvuoden luku sisältää kolme todentamatonta 0apt-merkintää.** Kolme Suomen 16 listauksesta julkaistiin samana päivänä **helmikuussa 2026** `0apt`-nimikkeellä, ja nämä kolme merkintää jäävät yksittäin todentamatta [S2]. Halcyonin riippumaton tutkimus esittää yleisen varoituksen: 0apt rakensi toimivan Rust-salaajan, mutta monet sen alkuvuoden uhriväitteistä jäivät todentamatta tai osoittautuivat liioitelluiksi [S54].
- **Listausten keskittyminen osuu yhteen Kyberturvallisuuskeskuksen erikseen raportoiman kesäkasvun kanssa.** Ilman helmikuun kolmea 0apt-merkintää **kaikki 13 jäljelle jäävää listausta** ajoittuivat kesä–marraskuulle (kesäkuu 1, heinäkuu 2, elokuu 4, syyskuu 4, lokakuu 1, marraskuu 1) [S2]. Ajoitus osuu yhteen heinäkuun Kybersään raportoiman kesän kasvun kanssa, mutta kausiyhtenevyys ei todenna yksittäisiä listauksia [S11].
- **Maamerkinnät vaativat tarkistuksen.** Toimialamerkinnöissä korostuivat teollisuus (6), energia (2) ja globaali (2) sekä yksittäiset merkinnät teknologia-, konsultointi-, koulutus-, kauppa-, julkishallinto- ja rahoitusaloilla [S2]. Lähdemaamerkinnät voivat kohdistaa ulkopuolisia organisaatioita tai ulkomaisia tytäryhtiöitä väärin Suomeen.

Toimijanimike	FI-listaukset 2026	Kuukaudet	Varmennushuomio
Qilin	3	Elo (2), loka	Jaettu kärki 0apt:n kanssa; yksittäiset väitteet todentamatta [S2]
0apt	3	Helmi	Saman päivän erä; yksittäiset väitteet todentamatta, Halcyonilta yleinen varoitus 0apt-väitteistä [S2][S54]
INC Ransom	2	Syys, marras	Toistuvat merkinnät; yksittäiset väitteet todentamatta [S2]
The Gentlemen	2	Heinä, syys	Kaksi Suomeen merkittyä listausta; yksittäiset väitteet todentamatta [S2]
Clop	2	Elo, syys	Toistuvat merkinnät; yksittäiset väitteet todentamatta [S2]
Lockbit5	2	Kesä, syys	Yksittäiset väitteet todentamatta [S2]
Krybit	1	Elo	Yksittäiset väitteet todentamatta [S2]
Deadlock	1	Heinä	Yksittäiset väitteet todentamatta [S2]

7.2 Uhkaprosessien suhdekartta ja profiloidut ryhmät

Alla oleva kartta pitää oman Ransompedia-aineiston (`own data`) erillään viranomaisvaroituksista (`official`) sekä tutkija- ja yliopistoraportoinnista (`public reporting`). Rikollisten kiristysnimikkeiden, haktivistien ja valtiollisten vakoiluvaroitusten välille ei oleteta todentamatonta yhteyttä.

Oma julkaisu · Edelleenjako · Virallinen varoitus · Julkinen tutkimus · Oma havainto

Qilin

Oma aineisto
3 listausta, S2 ↓

Suomeen merkityt listaukset

Oma aineisto
3 listausta, S2 ↑

0apt

INC Ransom

Oma aineisto
2 listausta, S2 ↓

Suomeen merkityt listaukset

Oma aineisto
2 listausta, S2 ↑

The Gentlemen

UNC7005

Julkinen tutkimus
GTIG-tutkijaraportti (korkea varmuus Venäjä-kytköksestä), S51 ↑

Tutkija- ja yliopistoraportointi

Julkinen tutkimus
Aalto-yliopiston tutkimus, S53 ↓

NoName057(16)

GRU / APT28 -varoitus

Virallinen varoitus
Yhteinen huhtikuun reititinvaroitus, S52 ↑

Viranomaisvaroitus (FBI / kumppanit)

EI TODENNETTUA YHTEYTTÄ MUIHIN TOIMIJOIHIN

Qilin

Nimike kiristyshaittaohjelma-aineistossa

Kiristyshaittaohjelman vuotosivustonimike | Valtiollista kytköstä ei todennettu tässä aineistossa

SUOMESSA, 2026

Vuoden 2026 jakso

3 Suomeen merkittyä listausta (elo- ja lokakuu 2026), S2

VÄITETYT KOHTEET

Suomeen merkittyjä kohteita; nimet ja toimialat salattu ja maamerkintä varauksellinen

JULKISISSA LÄHTEISSÄ

[S2] 3 listausta Ransompediassa (elo- ja lokakuu 2026)

ARVIOMME

Qilin jakaa kärkipaikan Suomen listauksissa 0apt:n kanssa. Listaus todentaa julkisen kiristysväitteen muttei vahvista salausta, tietojen aitoutta tai maamerkinnän oikeellisuutta; ulkopuolisia organisaatioita tai ulkomaisia tytäryhtiöitä voi kohdistua väärin Suomeen.

VARMUUS
Korkea listausmäärälle; yksittäiset väitteet todentamatta

0apt

0APT (nimike vuotosivustoaineistossa)

Kiristyshaittaohjelman vuotosivustonimike | Valtiollista kytköstä ei todennettu tässä aineistossa

SUOMESSA, 2026

Vuoden 2026 jakso

3 Suomeen merkittyä listausta samana päivänä helmikuussa 2026, S2

VÄITETYT KOHTEET

Kolme Suomeen merkittyä kohdetta samana päivänä; nimet ja toimialat salattu

JULKISISSA LÄHTEISSÄ

[S2] 3 saman päivän listausta Ransompediassa

[S54] Halcyonin tutkimus yleisenä varoituksena alkuvuoden liioitelluista tai todentamattomista 0apt-väitteistä

ARVIOMME

Halcyon vahvisti toimivan Rust-salaajan ja esitti yleisen varoituksen siitä, että monet alkuvuoden 2026 0apt-väitteistä olivat liioiteltuja tai todentamattomia. Kolme suomalaista merkintää jäävät yksittäin todentamatta ja vaativat oman teknisen tarkistuksen.

VARMUUS
Korkea listausmäärälle ja Halcyonin yleiselle varoitukselle; kolme suomalaista väitettä jäävät todentamatta

INC Ransom

Nimike vuotosivustoaineistossa

Kiristyshaittaohjelman vuotosivustonimike | Valtiollista kytköstä ei todennettu tässä aineistossa

SUOMESSA, 2026

Vuoden 2026 jakso

2 Suomeen merkittyä listausta (syys- ja marraskuu 2026), S2

VÄITETYT KOHTEET

Suomeen merkityt toistuvat kohteet; nimet ja toimialat salattu

JULKISISSA LÄHTEISSÄ

[S2] 2 toistuvaa listausta Ransompediassa

ARVIOMME

Toistuvat listaukset kasvattavat raakalukuja, kun sama organisaatio julkaistaan uudelleen uudella päivämäärällä tai toimialalla. Käsittele jokaista kiristyslistausta todentamattomana väitteenä, joka vaatii oman lokitarkistuksen.

VARMUUS

Korkea listausmäärälle ja toistorakenteelle; yksittäiset väitteet todentamatta

The Gentlemen

Nimike vuotosivustoaineistossa

Kiristyshaittaohjelman vuotosivustonimike | Valtiollista kytköstä ei todennettu tässä aineistossa

SUOMESSA, 2026

Vuoden 2026 jakso

2 Suomeen merkittyä listausta (heinä- ja syyskuu 2026), S2

VÄITETYT KOHTEET

Suomeen merkittyjä kohteita; nimet ja toimialat salattu

JULKISISSA LÄHTEISSÄ

[S2] 2 listausta Ransompediassa

ARVIOMME

Listaus todentaa kiristysväitteen muttei vahvista toimija-attribuutiota, salausta tai tietovuotoa. Sama nimike johti myös Ruotsin ja Tanskan vuoden 2026 listauksia.

VARMUUS

Korkea listausmäärälle; yksittäiset väitteet todentamatta

7.3 Valtiolliset vakoiluvaroitukset ja haktivismi

Vuonna 2026 julkaistut viranomais- ja tutkijaraportit korostavat jatkuvaa valtiollista tiedustelupainetta länsimaisiin kumppaneihin, Suomi mukaan lukien. Kaikki valtiolliset attribuutiot esitetään yksinomaan lähteiden omina arvioina.

Huhtikuun 7. päivänä 2026 FBI:n IC3 ja kansainväliset kumppanit, Suomi mukaan lukien, yhdistivät globaalin kotireititinkampanjan Venäjän sotilastiedusteluun (GRU / APT28) [S52]. Toimijat hyödynsivät haavoittuvia kotireitittimiä, muun muassa elinkaarensa päättyneitä TP-Link-malleja haavoittuvuuden `CVE-2023-50224` kautta, tunnusten keräämiseen ja DNS-kaappaukseen [S52][S66][S77]. TP-Link suosittelee korvaamaan päivittämättömät elinkaarensa päättyneet reitittimet tuetuilla malleilla ja poistamaan etähallinnan internetistä (§12.2) [S52][S77].

Erikseen **heinäkuussa 2026** Kyberturvallisuuskeskuksen Kybersää kertoi kahdesta suomalaisten ja kansainvälisten viranomaisten varoituksesta Venäjän valtiollisesta kybervakoilusta [S11]. Ensimmäinen varoitti FSB:hen yhdistetyn toimijan hyökkäyksistä heikosti suojattuihin yritysverkkolaitteisiin [S11]. Toinen varoitti valtiojohtoisen **Laundry Bear** -toimijan murroista sähköpostijärjestelmiin, mukaan lukien Zimbra-sähköposti (`CVE-2025-66376` ; haavoittuvat ja korjatut versiot luvussa §12.2) [S11][S65][S78]. Kumpaakaan heinäkuun varoitusta ei yhdistetä alla olevaan huhtikuun GRU/APT28-profiiliin.

Erikseen Google Threat Intelligence Group (GTIG) arvioi korkealla varmuudella **UNC7005 (STORM-2945)** -klusterilla olevan Venäjä-kytköksen (ICE RELIC -yhteys kohtalaisella varmuudella) [S51]. Klusteri rekisteröi 31.7.2026 alkaen **Finnish Operations Centeriä** jäljitteleviä verkkotunnuksia ja lähetti 6.–13.8. OAuth-kalasteluviestejä eurooppalaiselle puolustusteollisuudelle [S51]. Organisaation nimen käyttö syöttinä ei osoita sen omien järjestelmien murtoa [S51].

UNC7005 (STORM-2945)

GTIG:n seurantaklusteri

Venäjä-kytköksinen kalasteluklusteri (tutkijaraportti) | Venäjä-kytkös GTIG:n arvion mukaan (korkea varmuus); ICE RELIC -yhteys kohtalainen

SUOMESSA, 2026

31.7.–13.8.2026
Rekisteröi Finnish Operations Centeriä jäljitteleviä verkkotunnuksia eurooppalaisen puolustusteollisuuden OAuth-kalasteluun, S51

VÄITETYT KOHTEET

Tutkimus-, diplomatia-, järjestö- ja eurooppalaisen puolustusteollisuuden toimijat; suomalaisuhrien määrää ei tiedossa

JULKISISSA LÄHTEISSÄ

[S51] Google Threat Intelligence Groupin tekninen analyysi

ARVIOMME

GTIG havaitsi klusterin käyttävän suomalaisen puolustusalan toimijan nimeä syöttinä Google OAuth -kalastelussa aiempien erillisten laitekoodikalastelukampanjoiden ohella. Organisaation nimen käyttäminen syöttinä ei osoita sen omien järjestelmien murtoa.

VARMUUS
Korkea julkaistulle tutkijahavainnolle; ei riippumatonta attribuutiota tai suomalaista uhrimäärää

GRU / APT28 -reititinvaroitus

Fancy Bear, Forest Blizzard (viranomaisnimikkeet)

Virallinen kansainvälinen vakoiluvaroitus | Venäjän GRU-attribuutio esitetään yksinomaan varoituksen antaneiden viranomaisten arviona

SUOMESSA, 2026

7.4.2026
FBI IC3 sekä suomalaiset ja kansainväliset kumppanit varoittivat GRU/APT28:n reititinhyökkäyksistä (CVE-2023-50224), S52

VÄITETYT KOHTEET

Haavoittuvat kotireitittimet, mukaan lukien elinkaarensa päättyneet TP-Link-mallit (CVE-2023-50224)

JULKISISSA LÄHTEISSÄ

[S52] FBI IC3 PSA260407, jossa Suomi mainitaan kumppanimaana

[S66] NVD-merkintä CVE-2023-50224

[S77] TP-Linkin tietoturvatiedote (FAQ 5058)

ARVIOMME

FBI:n huhtikuun varoitus yhdistää reititinkampanjan GRU/APT28-toimijaan yhdessä Suomen ja kansainvälisten kumppanien kanssa [S52]. Se ohjaa puolustuksen koventamiseen eikä muodosta suomalaista uhrilaskentaa.

VARMUUS
Korkea viranomaisvaroitukselle; ei riippumatonta toimija-attribuutiota

NoName057(16)

Pelillistetty DDoS-ryhmä (Aalto-tutkimus)

Pelillistetty haktivistinen palvelunestoryhmä (yliopistotutkimus) | Venäjämielinen haktivistiryhmä Aalto-yliopiston tutkimuksen kuvauksen mukaan

SUOMESSA, 2026

Tammikuu 2025 – 2026 tutkimus

23 palvelunestohyökkäyskierrosta, vaikutuksia 129 julkiseen ja yksityiseen organisaatioon Suomessa, S53

VÄITETYT KOHTEET

Julkiset toimijat, kunnat, rahoituslaitokset ja julkiset verkkopalvelut

JULKISISSA LÄHTEISSÄ

[S53] Aalto-yliopiston kauppakorkeakoulun tutkimustiedote

ARVIOMME

Aalto-yliopiston tutkijat arvioivat, että pelillistetyt palvelunestokampanjat pyrkivät palveluhäiriöiden ohella murentamaan kansalaisten luottamusta hallituksiin. Arvioi tekninen vaikutus erikseen oman palveluvalvonnan perusteella, ei ryhmän väitteistä.

VARMUUS

Korkea julkaistulle Aalto-yliopiston tutkimukselle; yksittäiset väitteet vaativat omaa seurantaa

Tekniikkatunnisteita ei lisätä ilman lähdetekstin nimenomaista kartoitusta. Kohtele viranomaisvaroituksia välittöminä kovennuskehotuksina reitittimille, sähköpostipalvelimille ja OAuth-säännöille, ei todisteena yksittäisen organisaation saastumisesta.

KESKEISET HAVAINNOT

01

Kaikki 16 Ransompedia-listausta jäävät todentamatta, ja kesä–syksyn keskittyminen osuu yhteen Kyberturvallisuuskeskuksen raportoiman kesäkasvun kanssa.

02

Pidä kiristysnimikkeet, haktivistit ja valtiolliset vakoiluvaroitukset erillään.

03

Toimi reititin-, Zimbra- ja OAuth-varoitusten pohjalta heti ilman varmistamattomia uhriväitteitä.

LUKU 08

Petokset, identiteettiväärinkäyttö ja toissijainen vahinko

TÄMÄ LUKU VASTAA

Miten vuodetut henkilötiedot ja alamaailman palvelut ruokkivat Suomen petosrikollisuutta?

20 000

pankkien tilastoimaa huijausyritystä alkuvuonna 2026

8.1 Kansallisten digihuijausten laajuus ja taktiikoiden muutos 65

8.2 Väärennetyt suomalaiset asiakirjat, KYC-paketit ja muulivärväys 67

8.3 Maksukorttiaineisto: rajattu havainto 69

8.4 Toissijainen vahinko vahvistettujen tietovuotojen jälkeen 70

LUKU 08

Petokset, identiteettiväärinkäyttö ja toissijainen vahinko

LYHYESTI

Digihuijaukset ovat Suomen yleisin arjen kybervahinko. Pankit tilastoivat 148 miljoonan euron edestä huijausyrityksiä vuonna 2025 ja 60 miljoonaa euroa 20 000 yrityksessä alkuvuonna 2026; yritysmäärät kasvoivat jyrkästi samalla kun turvatilihuijausten summat pienenivät. Foorumeilla myydään suomalaisia palkkalaskelmaväärennöksiä, EU-tason KYC-kuvia, noutomuuleja ja bulvaaniyrityksiä. Yhdistä tietosuojapoikkeamien hallinta suoraan petostorjuntaan ja asiakaspalvelun ohjeistukseen.

8.1 Kansallisten digihuijausten laajuus ja taktiikoiden muutos

Finanssiala ry:n pankeilta keräämät luvut antavat selkeän kuvan ilmiön mittakaavasta [S29][S30]. Koko vuonna **2025** suomalaisilta yritettiin huijata **148 miljoonaa euroa**, kun vuonna 2024 summa oli 107,2 miljoonaa [S29]. Pankit estivät tai palauttivat **75,5 miljoonaa euroa** (yli 50 %), joten rikollisille meni **72,5 miljoonaa euroa** (vuonna 2024 yhteensä 62,9 miljoonaa) [S29].

Kalastelun osuus oli 53,1 miljoonaa euroa (lähes 17 000 kohdetta, joista 13 000 pelastettiin) [S29]. Turvatilihuijausten osuus oli 38,4 miljoonaa euroa yrityksinä (23,8 miljoonaa torjuttu, 14,6 miljoonaa menetetty) [S29][S30]. Finanssialan kuvaamissa huijaustapauksissa asiakas siirsi rahat itse rikollisille 60 prosentissa tapauksista [S29].

Alkuvuonna 2026 (tammi–kesäkuu) huijausyritysten yhteissumma oli **60 miljoonaa euroa** [S30]. Pankit estivät tai palauttivat **31,7 miljoonaa euroa (53 %)** ja rikollisille päätyi **28,3 miljoonaa euroa (47 %)** [S30]. Alkuvuonna 2025 pankit estivät 28 miljoonaa (48 %) ja rikollisille meni 30 miljoonaa [S30]. Samaan aikaan **yritysten lukumäärä nousi 20 000 tapaukseen** (6 000 toteutunutta ja 14 000 torjuttua), kun alkuvuonna 2025 yrityksiä oli **13 600** (3 700 toteutunutta ja 9 900 torjuttua) [S30].

Alkuvuoden 2026 huijauslaji (Finanssiala)	Rikollisille (milj. EUR)	Estetty tai palautettu (milj. EUR)	Havainto
Tietojen kalastelu	10,6	Sisältyy 31,7 yhteismäärään	Suuri määrä; tunnuksia käytetään yhä useammin tunnistusvälineenä [S30]
Sijoitushuijaukset	8,2	Sisältyy 31,7 yhteismäärään	Sosiaalisen median mainokset ja valekauppapaikat [S30]
Toimitusjohtaja- ja laskutushuijaukset	4,9	0,4	Heikoin torjuntaosuus; muutama suuri yrityssiirto [S30]
Dokumentti- ja rakkaushuijaukset	2,6	2,4	Pitkäkestoinen sosiaalinen manipulointi [S30]

Alkuvuoden 2026 huijauslaji (Finanssiala)	Rikollisille (milj. EUR)	Estetty tai palautettu (milj. EUR)	Havainto
Turvatilihuijaukset	2,0	1,9	3,9 milj. EUR yrityksiä H1 2026 (2,0 milj. menetetty) vs 38,4 milj. EUR yrityksiä koko vuonna 2025 (14,6 milj. menetetty; eri jakson pituus); Finanssialan mukaan neuvonta on voinut auttaa [S29][S30]
Yhteensä tammi–kesäkuu 2026	**28,3**	**31,7**	**60,0 milj. EUR 20 000 yrityksessä (53 % torjuttu/ palautettu)** [S30]

Kaksi Finanssialan syyskuun 2026 havaintoa on suoraan keskeisiä yritysjohtajille [S30]:

- **Laskutus- ja toimitusjohtajahuijaukset ovat pankeille vaikeimpia pysäyttää.** Vain 0,4 miljoonaa euroa torjuttiin 4,9 miljoonan menetyksiä vastaan [S30]. Sähköpostitodennus, M365-suojaus ja maksujen varmistus toisessa kanavassa ratkaisevat siis enemmän kuin jälkikäteinen palautus.
- **Viranomaisviestien jäljittely kehittyy jatkuvasti.** Digi- ja väestötietovirasto (DVV) varoitti 2.9.2026 **Suomi.fi**-nimissä leviävistä sähköposti-, SMS- ja WhatsApp-huijauksista [S31]. DVV muistutti, ettei Suomi.fi koskaan lähetä teksti- tai WhatsApp-viestejä eikä laita linkkejä sähköposti-ilmoituksiin [S31]. Kyberturvallisuuskeskus dokumentoi lisäksi suomenkielisiä WhatsApp-johtajahuijauksia maaliskuussa, pankkirobottipuheluita marraskuussa ja tekoälyllä viimeisteltyjä Black Friday -valekauppoja [S8][S19][S20].

8.2 Väärennetyt suomalaiset asiakirjat, KYC-paketit ja muulivärväys

Todistekortti B10 8.4.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi venäjä / englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Uutta: suomalaiset palkkalaskelma- ja työsopimuspohjat työsuhteen todistamiseen.

Huomio. Osoittaa Suomeen räätälöityjen väärennöspohjien tarjonnan yleisten passimallien lisäksi.

Havaittu

Asiakirjaväärennösten myyjä mainostaa räätälöityjä suomalaisia palkkalaskelma- ja työsopimuspohjia tunnistautumis- ja luottotarkistuksiin.

Ei todennettu

Suomalaisten pankkien, luotonantajien tai työnantajien tarkistusten ohittamista tai toteutuneita kauppoja.

Todistekortti B11 31.5.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi venäjä

ALKUPERÄINEN

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

KÄÄNNÖS

Haetaan ostajaa omilla noutajilla Suomessa valmiiksi maksettujen älypuhelimien hakemiseen; ilmoita kaupungit ja hinnasto.

Huomio. Kuvaa verkkomaksupetosten kytkeytymistä fyysiseen toimitukseen ja paikalliseen välikäsien värväykseen.

Havaittu

Venäjänkielinen ilmoitus hakee Suomessa toimivia fyysisiä noutajia ja välikäsiä petollisesti tilatun elektroniikan keräämiseen.

Ei todennettu

Toimivaa paikallista muuliverkostoa, vahingoittuneita suomalaiskauppoja tai toteutuneita noutoja.

Todistekortti B12 24.10.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi venäjä

ALKUPERÄINEN

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

KÄÄNNÖS

Haetaan bulvaaneja yrityksen ja kahden pankkitilin avaamiseen; ensisijaisia maita muun muassa Saksa, Iso-Britannia, Tanska, Alankomaat ja Suomi. Maksu avaamisen jälkeen.

Huomio. Yhteystunnus on poistettu; kuvaa yritysasiakkaiden tunnistamiseen ja tosiasiallisiin edunsaajiin kohdistuvaa kysyntää.

Havaittu
Lokakuun rekrytointiviesti mainitsee Suomen kahdentoista ensisijaisen Euroopan maan joukossa yritysten ja yrityspankkitilien avaamiseen haettaville välikäsille.

Ei todennettu
Yhtäkään Suomessa perustettua bulvaaniyritystä, pankkitunnistuksen pettämistä tai toimivaa paikallista solua.

Oma foorumiaineistomme näyttää Suomeen kohdistuvan petosrikollisuuden tukimarkkinan [S1]. Myyjät tarjosivat **suomalaisia palkkalaskelma- ja työsopimuspohjia** (B10 , 8.4.) sekä 25 dollarin EU-tason KYC-kuvapaketteja Suomi mukaan lukien (19.8.) [S1]. Muut ketjut värväsivät **paikallisia noutomuuleja** petollisesti tilatuille älypuhelimille (B11 , 31.5.) ja **bulvaaniyrittäjiä** kahdelletoista Euroopan markkinalle Suomi mukaan lukien (B12 , 24.10.) [S1].

Ilmoitukset osoittavat rikollista tarjontaa ja kysyntää, eivät onnistuneita tarkistusten ohituksia tai toimivia suomalaissoluja. Ne korostavat kuitenkin tarvetta vahvistaa asiakirjatarkistuksia, arvokkaiden noutotilausten valvontaa ja uusien yritysasiakkaiden tuntemista.

8.3 Maksukorttiaineisto: rajattu havainto

KORTTILUKUJEN RAJAUS

Nämä luvut kuvaavat rajattua julkaisuaineistoa. Ne eivät arvioi suomalaisten korttivarkauksien kokonaismäärää, petostappioita tai korttien toimivuutta.

Vuoden 2026 aineistossa havaittiin **73 erillistä Suomeen merkittyä maksukorttitietuetta**, jotka esiintyivät **109 kertaa 83 viestissä** ja **41 kuusinumeroisessa BIN-sarjassa** (bank identification number, pankkitunnistenumero) [S1]. Jakauma oli 36 Mastercard, 34 Visa, 1 American Express ja 2 muuta (16 debit, 12 credit, 45 merkitsemätöntä) [S1]. Esiintymät huipentuivat elokuussa (42 korttia 53 viestissä) [S1]. Lisäksi **1 711 myynti- ja korttikauppaviestiä** mainitsi Suomen ilman selväkielisiä korttinumeroita [S1]. Ryhmään kuului **1 520 monikansallista korttikauppapäivitystä** (mediaani 45 maata ja 1 538 korttia erässä; mediaanipyyntihinta 10–24 USD) [S1].

Selväkieliset julkaisut kattavat kapean osan korttimarkkinoista eivätkä osoita pankkimurtoa tai korttien käyttökelpoisuutta. Luvuista ei seuraa joukkosulkusuositusta; liikkeeseenlaskijoiden tulee toimia todennettujen BIN- ja maksutapahtumahälytysten perusteella.

8.4 Toissijainen vahinko vahvistettujen tietovuotojen jälkeen

Vahvistetut tapaukset kuten **Finnair / Amadeus** (`Tapaus T`), **Kolmostien Terveys** (`Tapaus J`), **Holmasto** (`Tapaus M`) ja **Eckerö Line** (`Tapaus R`) paljastivat aitoa henkilökontekstia [S35][S39][S43][S44]. **Aalto EE:n** (`Tapaus I`) virallisen tiedotteen mukaan nimet, sähköpostiosoitteet, Canvas-tunnisteet ja sisäiset viestit ovat saattaneet paljastua [S37]. Tiedotteissa paljastuneet tai mahdollisesti paljastuneet kentät vaihtelivat varausnumeroista ja viestisisällöistä suomalaisiin henkilötunnuksiin.

Henkilötunnus tai varausnumero on **kontekstia, ei koskaan tunnistautumista**. Asiakaspalvelun, laskutuksen ja potilasneuvonnan tulee varmistaa tärkeät muutokset erillisellä takaisinsoitolla ja kertoa selkeästi, mihin vuodetut tiedot eivät riitä.

KESKEISET HAVAINNOT

01

Huijausyritysten määrä nousi 20 000:een alkuvuonna 2026, ja yritysten laskutushuijauksissa pankkien torjuntaosuus oli heikoin.

02

Alamaailmassa markkinoidaan suomalaisia palkkalaskelmavääränöksiä, noutomuuleja ja bulvaaniyrityksiä.

03

Pidä rajatut korttihavainnot erillään pankkimurtoväitteistä ja valmenna asiakaspalvelu kontekstihuijauksia vastaan.

LUKU 09

Pankkiala, vahva tunnistaminen ja maksamisen jatkuvuus

09

TÄMÄ LUKU VASTAA

Miten hyökkääjät kohdistavat toimensa Suomen pankkipohjaiseen vahvaan tunnistamiseen?

7 / 25

valitulla suomalaisella rahoitusalan verkkotunnuksella oli aktiivinen tunnuslistaus

9.1 Valittujen 25 rahoitusverkkotunnuksen perustaso ja pankkialtistus 72

9.2 Vahvan tunnistamisen ketjutus, reaaliaikaiset paketit ja FI-IBAN-tilit 74

9.3 Toiminnan jatkuvuus ja uhkalähtöinen testaus 75

LUKU 09

Pankkiala, vahva tunnistaminen ja maksamisen jatkuvuus

LYHYESTI

Suomalaiset verkkopankkitunnukset toimivat pääasiallisena vahvana tunnistusvälineenä, joten kalastelu ulottuu eSIM-liittymiin, mobiilivarmenteeseen ja pikaluottoihin. Marraskuun 24. päivän 2026 tilannekuvassa 25 rahoitusverkkotunnuksesta 7:llä oli myynnissä oleva kirjautumistieto, vähintään 7 317 laitekytköstä (99,2 % ei-työntekijäluokiteltuja) ja 108 274 tunnistetietuetta. Erikseen 20 julkaisee karanteenia tai hylkäystä pyytävän DMARC-politiikan, ja marraskuun lopussa SALTA3-pakettia mainostettiin viidelle suomalaispankille. Varmenna aktiiviset tunnuslistaukset ensin, vahvista tunnistusvälineiden myöntöä ja harjoittele TIBER-FI- sekä DORA-jatkuvuutta.

9.1 Valittujen 25 rahoitusverkkotunnuksen perustaso ja pankkialtistus

Valittu **Pankki- ja rahoitusala** -solu käsittää **25 suomalaista verkkotunnusta** (ei kaikkia toimilupapankkeja tai maksulaitoksia), ja kaikilla 25:llä on sekä kokoonpano- että altistushavainnot [S3][S4]. Marraskuun 24. päivän passiiviset havainnot osoittavat vahvaa perustasoa ja rajattuja aukkoja [S3]:

- **DMARC: 20 verkkotunnusta 25:stä (80 %)** julkaisee karanteenia tai hylkäystä pyytävän DMARC-politiikan (`12 reject` , `8 quarantine`), **4** on seurantatilassa (`none`) ja **1** ilman kelvollista tietuetta [S3][S67]. Julkaistu politiikkaluokka ei yksin osoita täyttä kattavuutta tai vastaanottajien käsittelyä (§3.5) [S67].
- **Muut sähköposti- ja verkkosuojaukset: 24 / 25** julkaisee SPF:n [S68], **22** DKIM:n [S69] ja **6** DNSSEC-delegaation [S3]. **24** läpäisi TLS-tarkistuksen (1 ei saatavilla), ja **22 / 24** saatavilla olleesta HTTP-vastauksesta pakottaa HSTS:n [S3][S70].
- **Liukuvat 365 päivän alamaailmamaininnat (23.11.2025–22.11.2026): 6 / 25** verkkotunnusta keräsi **9 mainintaa** keskustelukanavilla ja **1** sai **1 maininnan** Tor-verkossa [S4]. Vuoden 2026 jaksolla (`1.1.–22.11.2026`) **3** verkkotunnusta sai **5 mainintaa** [S4].

Altistushavainnot kaikilla 25 rahoitusverkkotunnuksella erottavat aktiiviset markkinatarjoukset kumulatiivisista asiakaslaitekytköksistä [S4]. Toimiala- tai ryhmäkohtaisia arvosanoja ei julkaista.

Rahoitussolun mittari (25 arvioitua verkkotunnusta)	Havainto	Tulkintaraja
Aktiiviset tunnuslistaukset / listaushistoria	7 verkkotunnusta (kaikilla 7 historiaa; 15 merkintää) [S4]	Markkinailmoitus, ei testattu salasana tai pankkimurto
Saastuneiden laitteiden kytkökset, vähintään	7 317 yhteensä 18 verkkotunnuksella [S4]	Kumulatiivinen asiakas- ja työntekijälaitteiden summa
Työntekijäluokitellut laitekytkökset	59 yhteensä 12 verkkotunnuksella (0,8 % solun laitteista) [S4]	Sisältyy lukuun 7 317; varmenna hallitut työlaitteet
Ei-työntekijäluokitellut laitekytkökset	7 258 (99,2 % solun laitteista) [S4]	Uskottavasti asiakaslaitteita; petossignaali, ei pankkimurto
Historialliset tunnistetietueet	108 274 yhteensä 24 verkkotunnuksella (91 942 vuotokanta, 1 174 tietovarkausloki, 15 158 yhdistelmälista) [S4]	Kaksi suurinta kattaa 65,0 %; kumulatiivinen, ei vain 2026
Asiakirjakytkökset / 30 pv samankaltaiset nimet	120 (17 verkkotunnuksella) / 7 362 (14 verkkotunnuksella) [S4]	Konteksti ja tarkistuskandidaatteja, ei vahvistettuja kalastelusivustoja

Toimiluvallisten korttipankkien alajoukko (12 / 25 rahoitusverkkotunnusta). Kaksitoista verkkotunnusta 25 rahoitusverkkotunnuksen solussa edustaa Suomessa toimivia kortteja liikkeeseen laskevia pankkeja (pankkien nimet salattu) [S4]. Tämän rajatun 12 pankin alajoukon pitäminen erillään koko 25 verkkotunnuksen solusta selkeyttää kuluttaja-altistuksen painopistettä [S4]:

- **Kaikki 7 aktiivista tunnuslistausta** rahoitussolussa osuvat näihin **12 pankkiin** (`7 / 12`) [S4].
- **10 pankkia 12:sta** kantaa **7 095 ei-työntekijäluokiteltua laitekytköstä** (97,8 % koko solun luvusta 7 258) ja **7 / 12** kantaa **36 työntekijälaitekytköstä** (yhteensä **7 131** laitekytköstä ja **84 246** tunnistetietuetta 12 pankissa) [S4].
- **Keskittyminen:** Kolme suurinta pankkijoukkoa kattaa **78,6 %** (5 580 / 7 095) alajoukon ei-työntekijäluokitelluista laitekytköksistä [S4].
- **Maksukorttirajaus (§8.3):** Luvun §8.3 selväkielinen korttiaineisto ei osoita todennettua yhteyttä yksittäisiin pankkeihin eikä liikkeeseenlaskijoiden järjestystä [S1].

Rahoitusalan kysymys	Havainto	Vastuutaho
Julkaiseeko verkkotunnus karanteeni- tai hylkäyspolitiikan DMARC:ssa?	20 / 25 pyytää karanteenia tai hylkäystä (4 seurannassa, 1 puuttuu; §3.5) [S3]	Sähköposti- ja verkkotunnusturva
Onko rahoitusalan tunnuksia myynnissä nyt?	7 / 25 rahoitusverkkotunnusta (kaikki 7 kuuluvat 12 pankin alajoukkoon) [S4]	Identiteettioperaatiot ja SOC
Ovatko laitekytkökset henkilökuntaa vai asiakkaita?	Vähintään 7 317 yhteensä; 59 työntekijä (0,8 %) vs 7 258 muu (99,2 %) [S4]	Petostorjunta, asiakasturva ja päätelaitetiimit
Kohdistuuko Suomeen reaaliaikaisia kalastelupaketteja?	SALTA3 mainostettiin 20. ja 22.11. viidelle suomalaispankille [S1]	Petostorjunta ja digikanavat
Osoittaako foorumin tunnuslista pankkimurron?	Ei; verkkotunnuksittain nimetyt listat sekoittavat usein mukaan ulkopuolisia ulkomaisia osoitteita [S1]	Identiteetti- ja SOC-varmennus

9.2 Vahvan tunnistamisen ketjutus, reaaliaikaiset paketit ja FI-IBAN-tilit

Todistekortti B15 — 20.11.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

SALTA3-kalastelupaketti reaaliaikaisella hallintapaneelilla, mukautettu muun muassa viidelle Suomessa toimivalle vähittäispankille.

Huomio. Mainittujen pankkien nimet on salattu; reaaliaikaiset paneelit on suunniteltu vahvan tunnistautumisen interaktiiviseen kaappaamiseen.

Havaittu

Foorumimyyjä mainostaa 20. marraskuuta (ja uudelleen 22. marraskuuta) reaaliaikaista SALTA3-kalastelupakettia, jonka mallipohjat nimeävät viisi Suomessa toimivaa merkittävää vähittäispankkia.

Ei todennettu

Yhdenkään pankin järjestelmämurtoa, kampanjan aktiivista laajuutta Suomessa tai toteutuneita varojen menetyksiä.

Todistekortti B16 — 22.1.2026

Foorumikirjoittaja (nimimerkki salattu) Foorumiketju Foorumi englanti

ALKUPERÄINEN

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

KÄÄNNÖS

Väitetysti varmennettu yritysmaksutili suomalaisella FI-alkuisella IBAN-numerolla, rekisteröity yritys, asiakirjat ja verkkosivusto.

Huomio. Kysyntä saman tilintarjoajan tileille nousi uudelleen esiin Telegram-kanavalla 8.11.2026.

Havaittu

Tammikuun foorumiviesti mainostaa väitettyä suomalaisella FI-IBAN-tilinumerolla varustettua yritysmaksutiliä varmennettuna yhdessä rekisteröidyn yhtiön ja asiakirjojen kanssa.

Ei todennettu

Palveluntarjoajan järjestelmämurtoa, tilin aktiivista toimivuutta, SEPA-väärinkäyttöä tai toteutunutta kauppaa.

Finanssiala nosti syyskuussa 2026 esiin muutoksen: rikolliset kalastelevat pankkitunnuksia yhä useammin **tunnistusvälineeksi pelkän tilin tyhjentämisen sijaan** [S30]. Varastetuilla pankkitunnuksilla huijari avaa asiakkuuden toiseen pankkiin ja hankkii teleoperaattorilta sekä **eSIM-kortin** että **mobiilivarmenteen** [S30]. Kun rikollisella on hallussaan sekä pankin että operaattorin tunnisteet, pikavippien ja osamaksujen tekeminen useasta yhtiöstä samanaikaisesti vaikeuttaa tutkintaa ja torjuntaa [S30].

Talletetut alamaailmahavainnot sisältävät tämän mallin jokaista vaihetta vastaavia ilmoituksia [S1]:

- **Reaaliaikaiset kalastelupaketit (`B15`):** Marraskuun 20. ja 22. päivänä mainostettu `SALTA3` tarjoaa reaaliaikaista ohjausta (`Real-Time typing`) ja valmiita pohjia **viidelle Suomessa toimivalle merkittävälle vähittäispankille** (pankkien nimet salattu) [S1]. Reaaliaikaiset paneelit on rakennettu interaktiivisen vahvistuksen kaappaamiseen.
- **FI-IBAN-yritystilit (`B16`):** Myyjät mainostivat foorumilla tammikuussa väitettyjä suomalaisella `FI` -alkuisella IBAN-numerolla varustettuja yritysmaksutilejä varmennettuina, ja ostokysyntää esiintyi Telegramissa 8. marraskuuta [S1]. Rekisteröityihin yhtiöihin yhdistettyinä tällaiset ilmoitukset kohdistuvat yhtenäisen euromaksualueen (Single Euro Payments Area, SEPA) petostoimijoille [S1].
- **Televiestintävälineet (`Tapaus F`):** Suomalaiset eSIM-profiilit 75 dollarilla (`B08`), fyysisten SIM-korttien vuokraus ja SMS-lähettäjätunnuspalvelut (`B09`) täydentävät ketjua suoraan [S1].

Pankkinimillä jaettavat tunnuslistat vaativat silti tarkkaa teknistä tarkistusta. Yksi toukokuun 2026 sadan rivin foorumitiedosto yhdisti kourallisen suomalaisia kirjautumisrivejä täysin ulkopuolisiin ulkomaisiin verkkokauppaosoitteisiin [S1]. Tietoturvatiimien tulee aina tarkistaa näyterakenne ennen kuin pankkinimistä listaa pidetään pankin tietovuotona.

9.3 Toiminnan jatkuvuus ja uhkalähtöinen testaus

Maksamisen jatkuvuus Suomessa kytkee yhteen pankit, selvitysjärjestelmät, tietoliikenteen ja sähkönjakelun. EU:n DORA-asetuksen alla **Finanssivalvonta** valvoo ICT-riskienhallintaa, toimittajariippuvuuksia ja merkittävien häiriöiden ilmoittamista [S26][S27]. DORA:n rinnalla **Suomen Pankki** hallinnoi **TIBER-FI**-toimintamallia kriittisten rahoitusalan toimijoiden uhkalähtöiseen kybertestaukseen [S28].

Rahoitusalan tietoturvajohtajien kannattaa testata TIBER-FI- ja jatkuvuusharjoituksissa kahta vuoden 2026 skenaariota. Testaa ensin interaktiivisen pankkikalastelun ketjuttamista uuden pankkitilin ja eSIM-liittymän avaukseen. Harjoittele toiseksi kriittisen viestintä- tai ohjelmistotoimittajan katkosta vilkkaimpana maksuaikana.

KESKEISET HAVAINNOT

01

Kalastellut suomalaiset pankkitunnukset avaavat tien eSIM-kortteihin, mobiilivarmenteeseen ja pikaluottoihin.

02

Viidelle Suomessa toimivalle vähittäispankille räätälöity reaaliaikainen kalastelupaketti oli myynnissä marraskuun lopussa.

03

Yhdistä tunnistusvälineiden lisätarkistukset ja pankki-operaattori-hälytykset TIBER-FI- ja DORA-testaukseen.

LUKU 10

Sääntely, ilmoitusajat ja kansallinen reagointi

10

TÄMÄ LUKU VASTAA

Mikä viranomainen, portaali ja lakisääteinen määräaika koskee poikkeamaa Suomessa?

11. helmikuuta 2026

Finanssivalvonnan FISA-verkkolomake pakolliseksi DORA-ilmoituksissa

10.1 Suomen vuoden 2026 lakisääteinen perusta 77

10.2 Erilliset ilmoitusajat ja viranomaiset 78

10.3 Käytännön opit vuoden 2026 suomalaistapauksista 80

LUKU 10

Sääntely, ilmoitusajat ja kansallinen reagointi

LYHYESTI

Viisi säädöskokonaisuutta ohjaa Suomen kyber- ja tietosuojavelvoitteita vuonna 2026: kyberturvallisuuslaki (124/2025), kriittisen infrastruktuurin laki (310/2025), GDPR ja tietosuojalaki, DORA FISA-portaalin kautta sekä kyberkestävyyssäädös (kansallinen laki 1.6.2026; EU:n valmistajailmoitukset 11.9.2026 alkaen). Erota havaitsemis- ja luokitteluaikaleimat toisistaan, tarkista Ahvenanmaan toimivalta ja testaa varapääsy portaaleihin etukäteen.

10.1 Suomen vuoden 2026 lakisääteinen perusta

Viisi säädöskokonaisuutta määrittelee häiriönhallinnan, toimitusketjuvalvonnan ja johdon vastuun Suomessa vuonna 2026:

- **Kyberturvallisuuslaki (124/2025):** Huhtikuusta 2025 voimassa ollut kansallinen NIS2-laki säätää keskeisten ja tärkeiden toimijoiden riskienhallinnasta, johdon koulutuksesta ja vaiheittaisesta häiriöilmoittamisesta (11–13 §) [S21]. Lain 38 §:n mukaan hallinnollisen seuraamusmaksun enimmäismäärä on keskeiselle toimijalle 10 miljoonaa euroa tai 2 % edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi [S21]. Muulle kuin keskeiselle (tärkeälle) toimijalle enimmäismäärä on 7 miljoonaa euroa tai 1,4 % edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi [S21].
- **Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025):** Kansallinen CER-säädös määrittelee kriittisten toimijoiden häiriönsietokyvyn ja poikkeamailmoittamisen (16 §) kansallisen riskiarvion rinnalla [S22][S56]. Lain 2 § rajaa 14–16 §:n velvoitteiden ulkopuolelle pankkialan, rahoitusmarkkinoiden infrastruktuurin ja digitaalisen infrastruktuurin kriittiset toimijat (joihin sovelletaan sektorisääntelyä) sekä maanpuolustuksen, kansallisen turvallisuuden, lainvalvonnan ja nimetyt ylimmät valtioelimet [S22].
- **GDPR ja tietosuojalaki (1050/2018):** Toimivaltainen tietosuojaviranomainen määräytyy rekisterinpitäjän toiminnan sekä sovellettavan valtakunnan- tai maakuntalainsäädännön mukaan, ei pelkän Ahvenanmaalla sijainnin perusteella. Datainspektionen valvoo maakunta- ja kunnallishallintoa sekä määriteltyjä maakunnan toimivaltaan kuuluvia toimintoja, kun taas tietosuojavaltuutetun toimisto valvoo yksityisiä toimijoita [S23][S76] [S79]. Vuonna 2026 tietosuojavaltuutettu julkaisi Finlexissä päätöksen `2026/10` (31.3.2026) sivullisen pääsystä e-laskun tietoihin [S24]. Lisäksi hallitus esitti GDPR-seuraamusmaksujen ulottamista julkiselle sektorille, mistä Kunta- ja hyvinvointialuetyönantajat (KT) esitti kritiikkiä [S25].
- **DORA ja Finanssivalvonnan FISA-ilmoittaminen:** Valvottavatiedotteen `4/2026` (19.1.2026) mukaan DORA-häiriöilmoitukset on toimitettava **11.2.2026 alkaen** yksinomaan **FISA-asiointipalvelun verkkolomakkeella**, ja vanhat Excel-pohjat poistuivat käytöstä [S26][S27]. Ilmoitusajat ja poikkeukset määritellään komission delegoidun asetuksen (EU) 2025/301 5 artiklassa [S74].

- **Kyberkestävyyssäädös (EU 2024/2847) ja Traficomin viestintämääräykset:** EU:n säädöstä täydentävä kansallinen kyberkestävyyslaki tuli voimaan **1.6.2026** [S9]. CRA:n 71 artiklan 2 kohdan mukaan **14 artiklan valmistajien ilmoitusvelvoitteita sovelletaan 11.9.2026 alkaen** (tämän raportin tarkastelujaksolla), ennen laajempaa **11. joulukuuta 2027** alkavaa pääsoveltamista [S75]. Kyberturvallisuuskeskus nosti marraskuussa esiin komission suomenkielisen soveltamisohjeen [S20]. Lisäksi Traficom edellytti suojattujen **SMS-lähettäjätunnusten** luvitusta **4.5.2026** mennessä ja poisti yli 100 virheellisillä tiedoilla rekisteröityä `.fi`-verkkotunnusta [S8].

10.2 Erilliset ilmoitusajat ja viranomaiset

Yksi poikkeama voi käynnistää useita rinnakkaisia määräaikoja. Taulukko toimii operatiivisena lukuohjeena määräajoista ja niiden alkamishetkistä (ei yksittäistapauksen oikeudellisena neuvona):

Säädöskehikko	Käynnistävä kriteeri	Keskeiset määräajat	Toimivaltainen viranomainen Suomessa
Kyberturvallisuuslaki (124/2025, NIS2)	Merkittävä poikkeama soveltamisalaan kuuluvalla toimijalla	Ensi-ilmoitus **24 tunnissa** havaitsemisesta (11 §); jatkoilmoitus **72 tunnissa** havaitsemisesta (luottamuspalveluilla **24 tunnissa**, 11 §); väliraportti pyynnöstä tai **1 kuukaudessa** jatkoilmoituksesta pitkäkestoisessa poikkeamassa (12 §); loppuraportti **1 kuukaudessa** jatkoilmoituksesta tai pitkäkestoisen poikkeaman käsittelyn päättymisestä (13 §) [S21]	Toimialan valvova viranomainen ja Kyberturvallisuuskeskuksen reitti [S21]
GDPR / Tietosuojalaki	Henkilötietojen tietoturvaloukkaus, ellei riski ole epätodennäköinen	Ilmoitus **72 tunnissa** tiedoksisaannista; ilmoitus rekisteröidyille ilman aiheetonta viivytystä korkean riskin tilanteessa [S23]	Tietosuojavaltuutetun toimisto tai Ahvenanmaan Datainspektionen. Määritä toimivaltainen tietosuojaviranomainen rekisterinpitäjän toiminnan ja sovellettavan valtakunnan- tai maakuntalainsäädännön perusteella. Pelkkä sijainti Ahvenanmaalla ei ratkaise vastaanottajaa (valtakunnallinen valvonta koskee yksityisiä toimijoita) [S23][S76][S79]

Säädöskehikko	Käynnistävä kriteeri	Keskeiset määräajat	Toimivaltainen viranomainen Suomessa
DORA (EU 2022/2554; del. asetus 2025/301, 5 art.)	Merkittävä tieto- ja viestintätekniikkaan liittyvä poikkeama	Alustava ilmoitus **4 tunnissa** merkittäväksi luokittelusta ja enintään **24 tunnissa** havaitsemisesta; jos luokitellaan merkittäväksi 24 tunnin jälkeen, **4 tunnissa** luokittelusta (5 art. 2 kohta); väliraportti **72 tunnissa** alustavasta ilmoituksesta (päivitys toiminnan palauduttua); loppuraportti **1 kuukaudessa** väliraportista tai viimeisimmästä päivitetystä väliraportista (5 art. 1 kohta) [S26][S27][S74]	Finanssivalvonta FISA-verkkolomakkeella (pakollinen 11.2.2026 alkaen) [S26]
Kriittisen infrastruktuurin laki (310/2025, CER)	Keskeisen palvelun tarjontaa merkittävästi häiritsevä tai uhkaava poikkeama nimetyllä kriittisellä toimijalla (2 § rajaa pankki-, rahoitusmarkkina- ja digi-infrastruktuurin pois 14–16 §:stä sekä maanpuolustuksen, kansallisen turvallisuuden ja nimetyt valtioelimet)	Ensi-ilmoitus ilman aiheetonta viivytystä ja viimeistään **24 tunnissa** tiedoksisaannista (jollei operatiivinen este); yksityiskohtainen raportti tarvittaessa viimeistään **1 kuukaudessa** tiedoksisaannista (16 §) [S22]	Ensi-ilmoitus valvovalle viranomaiselle ja **Valtioneuvoston tilannekeskukselle**; yksityiskohtainen raportti yhteensovittavalle ministeriölle, toimialaministeriölle ja valvovalle viranomaiselle (16 §) [S22]
Kyberkestävyyssäädös (EU 2024/2847, CRA 14 ja 71 art.)	Valmistajan tietoon tullut **aktiivisesti hyödynnetty haavoittuvuus** tai digitaalisen tuotteen turvallisuuteen vaikuttava **vakava poikkeama** (sovelletaan **11.9.2026** alkaen; laajempi CRA **11.12.2027**)	Ensivaroitus **24 tunnissa** havaitsemisesta; haavoittuvuus- tai poikkeamailmoitus **72 tunnissa** havaitsemisesta; loppuraportti **14 päivässä** korjauksen tai lievennyskeinon valmistuttua (aktiivisesti hyödynnetyt haavoittuvuudet) tai **1 kuukaudessa** 72 tunnin ilmoituksesta (vakavat poikkeamat) (14 art.) [S75]	Koordinaattori-CSIRT (Suomessa Kyberturvallisuuskeskus) ja **ENISA** samanaikaisesti CRA:n keskitetyn raportointialustan kautta [S75]
Rikostutkinta	Epäilty törkeä tietomurto, vakoilu tai petos	Viipymätön rikosilmoitus ja lokinäytön säilytys [S33] [S43][S49]	Poliisi / Keskusrikospoliisi (KRP) tai Ahvenanmaan poliisi [S33][S76]

DORA-asetuksen delegoidun asetuksen 2025/301 5 artiklan 3–5 kohdan mukaan määräajan ylittyessä viranomaiselle on ilmoitettava syyt ennen määräajan päättymistä [S74]. Viikonloppu- ja arkipyhäsiirtymä seuraavan arkipäivän keskipäivään ei koske luottolaitosten, keskusvastapuolten, kauppapaikkojen ylläpitäjien eikä NIS2-keskeisten tai -tärkeiden finanssitoimijoiden alustavia tai väliraportteja [S74].

10.3 Käytännön opit vuoden 2026 suomalaistapauksista

Vuoden 2026 tapauksista erottuu kaksi käytännön oppia. Ensiksi **rekisterinpitäjän ja käsittelijän roolit ratkaisevat heti ensimmäisenä päivänä**. Finnairin Amadeus-tapauksessa (`Tapaus T`) Amadeus teki GDPR-ilmoituksen rekisterinpitäjänä, kun Finnair vaihtoi varaukset ja tiedotti matkustajia [S35]. Eckerö Linen (`Tapaus R`) ja Aalto EE:n (`Tapaus I`) tapauksissa toimittajan viive vaikutti juridisen tiedoksisaannin hetkeen [S37][S44]. Toiseksi **enimmäissakot ovat lakisääteisiä kattoja, eivät ennusteita**. Hallitusten kannattaa varmistaa dokumentoidut soveltamisala-arviot, valtuutetut Suomi.fi- ja FISA-käyttöoikeudet sekä päätöslokit. Todentamaton foorumiväite ei yksin käynnistä viranomaisilmoitusta.

KESKEISET HAVAINNOT

01

Suomen NIS2-, CER-, GDPR-, DORA- ja CRA-velvoitteet toimivat erillisillä määräajoilla ja portaaleilla.

02

Testaa valtuutetut FISA- ja Kyberturvallisuuskeskus-yhteydet ennen häiriötä.

03

Dokumentoi rekisterinpitäjäroolit sekä havaitsemis- ja luokitteluajat erikseen.

LUKU 11

Näkymät ja ehdolliset varautumisskenaariot

11

TÄMÄ LUKU VASTAA

Mitkä konkreettiset merkit muuttavat Suomen puolustuksen painopisteitä 22.11.2026 jälkeen?

4

ehdollista varautumisskenaariota omaan näyttöön kytkettynä

11.1 Keskeiset arviot ja näytön rajat 82

11.2 Neljä ehdollista varautumisskenaariota 83

11.3 Mikä muuttaisi tätä arviota 84

LUKU 11

Näkymät ja ehdolliset varautumisskenaariot

LYHYESTI

Vuoden 2026 näyttö perustelee jatkuvan valmiuden reunalaitteiden nollapäiville, toimittajavuodoille, interaktiiviselle pankkikalastelulle ja suojaamattomille OT-ohjaimille. Aineisto ei osoita yhtä koordinoitua tekijää kaikkien tapausten taustalla eikä laske hyökkäystodennäköisyyksiä. Käytä neljää alla olevaa ehdollista skenaariota kytkeäksesi varmennetut sisäiset hälytykset sovittuihin teknisiin, juridisiin ja viestinnällisiin toimiin.

11.1 Keskeiset arviot ja näytön rajat

Arvio	Peruste ja luottamus	Keskeinen rajaus	Omistettu päätös
Internetiin näkyvät reunalaitteet ja verkkopalvelut pysyvät nopeina murtoväylinä	Korkea Valtorin Ivanti-murron, Citrix NetScaler -murtojen ja PHP-vikojen perusteella [S14][S15][S32]	Päivitystahti vaihtelee; nollapäivien ajankohtaa ei voi ennustaa	Ylläpidä hätäeristysvalmiutta ja päivitystä edeltävää uhkametsästyslistaa
Toimittaja- ja arkistovuodot luovat pitkäkestoista jatkokalasteluriskiä	Korkea Amadeuksen/ Finnairin, Canvasin/Aalto EE:n, Eckerö Linen ja Kolmostien Terveyden nojalla [S35] [S37][S39][S44]	Eri rekisterinpitäjien joukkoja ei voi laskea yhteen	Tarkista alihankkijoiden ilmoitusehdot ja poista vanhat siirtoarkistot
Interaktiivinen kalastelu ja vahvan tunnistamisen ketjutus uhkaavat pankkeja ja yrityksiä	Korkea Finanssialan 20 000 yrityksen, M365-nousun ja SALTA3 / eSIM -mainosten nojalla [S1][S7][S30]	Alamaailman mainokset eivät mittaa toteutunutta onnistumisastetta	Pakota kalastelunkestävä MFA, estä Device Code Flow ja kovenna eSIM-myöntöä
Kiristys- ja murtotoipumisvalmius säilyy tarpeellisena teollisuudessa, palveluissa ja yhdyskuntahuollossa	Korkea 16 todentamattomalle Ransompedia-listaukselle [S2]; erikseen kaksi vahvistettua suomalaistiedotetta raportoidaan vain roolin mukaan [S49][S50]	Toistuvat merkinnät ja yleinen 0apt-varovaisuus rajaavat raakalukuja [S54]	Testaa muuttumattomat varmuuskopiot ja erota tekninen selvitys listamelusta

Arvio	Peruste ja luottamus	Keskeinen rajaus	Omistettu päätös
Eristämättömät OT-ohjaimet luovat paikallista fyysisen häiriön riskiä	Korkea Kyberturvallisuuskeskuksen kylmälaitevaroitusten ja ennakoinnin nojalla [S16] [S18][S19]	Kyberturvallisuuskeskuksen mukaan aiempi varautuminen ja ennakointi auttoivat välttämään suurimmat vahingot; tekijää ei ole julkisesti nimetty [S18] [S19]	Poista ohjaimet julkisesta verkosta ja varmista paikallinen käsiohjaus
Ulkoinen tunnusaltistus vaatii jatkuvaa tilien varmennusta	Korkea 248 verkkotunnuksen portfoliolle (kansallinen Atlas-yleisluku 45/100; 41 aktiivista listausta; 148 työntekijälaitteilla) [S4]	Kumulatiiviset havainnot eivät ole kansallinen esiintyvyys tai murtovarmistus; 2 jää tuntemattomaksi	Varmenna aktiiviset tunnuslistaukset viidessä arkipäivässä ja pidä henkilöstö- sekä asiakasjonot erillään

11.2 Neljä ehdollista varautumisskenaariota

Skenaario A: Kriittinen reunalaite- tai verkkorunkohaavoittuvuus julkaistaan

Jos Kyberturvallisuuskeskus antaa vakavan varoituksen internetiin näkyvästä yhdyskäytävästä, MDM-palvelimesta tai PHP-palvelusta ennen korjauspäivitystä, käynnistä ennalta sovittu eristys tai varotoimisulku (`Tapaus R`). Kerää haihtuvat lokit ennen uudelleenkäynnistystä ja etsi päivitystä edeltävän murron jälkiä heti korjauksen jälkeen (`Tapaus Q`). Jos tuote on todennetusti sisäverkossa, kirjaa rajaus ja päivitä kiireellisesti ilman tarpeetonta julkista katkoa.

Skenaario B: Keskeinen toimittaja tai alihankkija laajentaa murron laajuutta

Jos SaaS- tai varaustoimittaja laajentaa altistuneita tietoja suomalaisiin henkilötunnuksiin, viestisisältöihin tai aktiivisiin varauksiin (`Tapaukset I ja T`), uusi aktiiviset koodit ja istunnot heti. Organisaation oman laajuuden kasvusta ks. `Tapaus H` . Päivitä GDPR-, NIS2- ja DORA-arviot ja julkaise selkeä ohje siitä, mihin paljastuneet tiedot eivät riitä. Jos selvitys rajaa altistuksen vanhoihin ei-arkaluonteisiin tietoihin, säilytä molemmat tiedotteet ja pura korotettu valmius hallitusti.

Skenaario C: Alamaailman listaus tai tunnuslista nimeää suomalaisorganisaation

Jos valtuutettu uhkahälytys osoittaa foorumin tietokantaväitteeseen (`Tapaus A` , `Tapaus B`), tunnuslistaan (`Tapaus E`) tai kiristyslistaukseen (§7.1), vertaa näytesarakkeita ja käyttäjätilejä ensin omiin järjestelmiin ja vanhoihin arkistoihin. Tarkista selittääkö ulkopuolisten osoitteiden sekoittuminen tai foorumien välinen näytteiden kierrätys julkaisun ennen ilmoituksia tai laajoja salasananvaihtoja.

Skenaario D: Automaatio-ohjain tai julkinen palvelu kohtaa häiriön tai haktivistiväitteen

Jos paikallinen valvonta vahvistaa luvattomia asetusmuutoksia kylmä-, energia- tai kiinteistöohjaimessa (`Tapaus S`), katkaise etäyhteys, siirry paikalliseen varakäyttöön ja ilmoita Kyberturvallisuuskeskukselle sekä poliisille. Jos haktivistikanava väittää kaataneensa verkkopalvelun (§6.2), tarkista oma käytettävyys, aktivoi operaattorisuojaus ja viesti faktoin toistamatta tekijän retoriikkaa.

11.3 Mikä muuttaisi tätä arviota

Varmennettu tekninen näyttö yhteisestä infrastruktuurista useiden suomalaismurtojen taustalla nostaisi kampanjavaroitusten tasoa. Vahvistus aktiivisista suojaamattomista henkilöstötileistä 41 aktiivisen tunnuslistauksen verkkotunnuksessa, tai altistushavainnot kahdelle vielä arvioimattomalle verkkotunnukselle, muuttaisi toimialapriorisointia. Vastaavasti vahvistettu vanha alkuperä, korjatut maamerkinnät tai 94 seurantatilan verkkotunnuksen siirtyminen täyden kattavuuden `quarantine`- tai `reject`-DMARC-politiikkaan kaventaisivat arvioituja riskejä.

KESKEISET HAVAINNOT

01

Liitä jokaiseen arvioon sen näytön rajat, jotta johto panostaa todennettuihin suojauksiin.

02

Käynnistä eristys-, toimittaja-, väitetarkistus- ja OT-varakäyttömallit varmennetuista paikallisista merkeistä.

03

Päivitä altistustarkistusten tärkeysjärjestys aina, kun tilivarmennus paljastaa aktiivisen pääsyn tai sulkee historiallisen osuman.

LUKU 12

Toimintasuunnitelma ja valmistumisnäyttö

12

TÄMÄ LUKU VASTAA

Kuka toimii, millä ehdolla ja mikä osoittaa suojauksen toimivan?

30 / 60 / 90

varmennusvälietapit; kiireellinen reuna- ja identiteettisuojaus alkaa tänään

12.1 Ensisijaiset toimintakaistat ja valmistumisnäyttö 86

12.2 Haavoittuvuuksien korjausviite 88

12.3 Jatkuvan varmennuksen tuki 90

LUKU 12

Toimintasuunnitelma ja valmistumisnäyttö

LYHYESTI

Kiireellinen reunalaitteiden päivitys, avoimien OT-laitteiden poisto ja aktiivisten tilimurtojen rajaaminen alkavat heti eivätkä odota neljännesvuosikatsauksia. Käytä alla olevia 30, 60 ja 90 päivän kaistoja nimetäksesi kullekin suomalaiselle prioriteetille teknisen ja liiketoiminnan omistajan sekä selkeän todennettavan valmistumisnäytön.

12.1 Ensisijaiset toimintakaistat ja valmistumisnäyttö

1**Välittömästi (0–7 pv)**

Inventoi internetiin näkyvät reunalaitteet, MDM-palvelimet, PHP-rajapinnat ja OT-/kylmäohjaimet; asenna luvun §12.2 korjatut versiot (tai korvaa tukea vailla olevat laitteet), poista OT julkisesta verkosta ja valtuuta hätäeristys

OMISTAJA

Infrastruktuuri, OT-tekniikka ja CISO

VALMISTUMISNÄYTTÖ

Allekirjoitettu ulkoisten laitteiden rekisteri, päivityslokit ja hyväksytty hätäeristysohje

Tarkista Microsoft 365- ja identiteettiympäristöt poikkeavien kirjautumisten, edelleenlähetyssääntöjen ja OAuth-oikeuksien varalta; estä tarpeeton Device Code Flow ja varmenna aktiiviset tunnuslistaukset viidessä arkipäivässä

OMISTAJA

Identiteetti- ja SOC-vastaavat

VALMISTUMISNÄYTTÖ

Ehdollisen pääsynhallinnan vienti, päivätyt listauskuittaukset ja puhdas kirjautumis-/OAuth-tarkastusloki

2**30 päivää**

Täsmäytä työntekijäluokitellut laitekytkökset hallittuun laiteinventaarioon, katkaise altistuneet istunnot ja ohjaa ei-työntekijälaitteiden signaalit petostorjuntaan

OMISTAJA

Päätelaite-, identiteetti- ja petosvastaavat

VALMISTUMISNÄYTTÖ

Täsmäytetty laitetarkistusrekisteri päivättyine katkaisuineen tai sulkupäätöksineen

Siirrä seurantatilan verkkotunnukset (`p=none`) täyden kattavuuden `quarantine` - tai `reject` -DMARC-politiikkaan, tarkista SPF/DKIM-kohdistus ja vahvista Traficomin suojattu SMS-lähettäjätunnus

OMISTAJA

Sähköpostiturva ja brändinomistaja

VALMISTUMISNÄYTTÖ

Live-DNS-tarkistus omille verkkotunnuksille ja Traficomin SMS-tunnusvahvistus

Varmista valtuutetut ilmoitusoikeudet ja varapääsy Finanssivalvonnan FISA-lomakkeelle (DORA), Kyberturvallisuuskeskukselle (NIS2) ja tietosuojavaltuutetulle (sekä Ahvenanmaan viranomaisille toiminnan ja lain edellyttäessä)

OMISTAJA

Lakiasiat, vaatimustenmukaisuus ja CISO

VALMISTUMISNÄYTTÖ

Testattu portaalipääsykuvakaappaus, varavastuulista ja päivitetty aikarajaohje

3**60 päivää**

Tarkista vanhat siirtoarkistot (ml. ennen vuotta 2023 syntyneet kunta-/sote-aineistot) ja muistitikkukäytännöt; testaa asiakashakurajapintojen todennus ja nopeusrajat sekä asiakaspalvelun huijausohjeet

OMISTAJA

Tietosuoja, rajapintakehitys ja asiakaspalvelu

VALMISTUMISNÄYTTÖ

Arkistojen poistotodistus, rajapintatestin raportti ja asiakaspalveluharjoituksen muistio

Testaa pankeissa ja telekytköksisissä palveluissa reaaliaikaisen kalastelun torjunta sekä eSIM-/mobiilivarmenne-lisätarkistukset; harjoittele varauskoodien nopea vaihto matkailu- ja kauppatoimittajissa

OMISTAJA

Petostorjunta, digikanavat ja toimittajariski

VALMISTUMISNÄYTTÖ

Allekirjoitettu testiraportti ja päivitetty toimittajien ilmoitus-SLA-rekisteri

4**90 päivää**

Järjestä yhteinen palautus- ja jatkuvuusharjoitus (TIBER-FI-, NIS2- tai CER-velvoitteiden mukaisesti) kattaen toimittajakatkon, kiristyshaittaohjelmapalautuksen ja rauhallisen tilanneviestinnän

OMISTAJA

Johtoryhmän sponsori, jatkuvuusvastaava ja CISO

VALMISTUMISNÄYTTÖ

Päivätty harjoitusraportti, mitatut palautusajat ja hyväksytty jäännösriskirekisteri

12.2 Haavoittuvuuksien korjausviite

Alla oleva taulukko kokoaa haavoittuvat ja korjatut versiot ajantasaisista NVD-, CVE CNA- ja valmistajatiedotteista raportissa korostetuille CVE-tunnisteille, mukaan lukien korvausohjeet kun tuettua korjausta ei ole saatavilla. Aiemmien haavoittuvuuksien vähimmäiskorjaukset eivät korvaa tuettujen haarojen myöhempiä tietoturvajulkaisuja:

Tuote ja CVE-tunnisteet	Haavoittuvat versiot	Korjatut versiot ja korvausohje	Lähteet
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` ja aiemmat `12.x` -versiot	Päivitä Ivanti EPMM -versioon `12.8.0.0` tai uusimpaan tuettuun `12.8.x` -tietoturvajulkaisuun tai asenna haarakohtainen RPM-päivitys Ivantin tiedotteen mukaan [S81] [S82]. Ivantin päivitetyt RPM-paketit ovat `ivanti-security-update-1761642-1.1.0S-5.noarch.rpm` (`12.5.0.0` , `12.6.0.0` ja `12.7.0.0`) ja `ivanti-security-update-1761642-1.1.0L-5.noarch.rpm` (`12.5.1.0` ja `12.6.1.0`) [S81][S82]. Korvaa tukea vailla olevat haarat ja tarkista konsolit aiemman murron varalta.	[S59][S60][S81][S82]
Citrix NetScaler ADC ja Gateway (`CVE-2026-88771` , `CVE-2026-88772` ; varoitus 1/2026 kattaa kahdeksan haavoittuvuutta `CVE-2026-88771` – `CVE-2026-88778` ; myöhempi 12.11. `CTX697305` ml. `CVE-2026-120868`)	Syyskuun nollapäivät: `14.1` ennen `14.1-73.37` , `13.1` ennen `13.1-64.23` , `14.1` FIPS ennen `14.1-73.37` FIPS, `13.1` FIPS/NDcPP ennen `13.1-37.279` . Marraskuun `CTX697305` (`CVE-2026-120868`): `14.1` ennen `14.1-73.57` , `13.1` ennen `13.1-64.39` , `14.1` FIPS ennen `14.1-73.58` FIPS, `13.1` FIPS/NDcPP ennen `13.1-37.293` (sekä EOL-haarat).	Syyskuun vähimmäisversiot haavoittuvuuksille `CVE-2026-88771` – `CVE-2026-88778` olivat `14.1-73.37` , `13.1-64.23` , `14.1-73.37` FIPS ja `13.1-37.279` FIPS/NDcPP [S80]. Ajantasaiseen korjaukseen Citrixin 12.11. päivityksen (`CTX697305` , `CVE-2026-120868`) kanssa päivitä versioihin `14.1-73.57` , `13.1-64.39` , `14.1-73.58` FIPS tai `13.1-37.293` FIPS/NDcPP (tai uudempaan tuettuun versioon) [S87]. Siirrä elinkaarensa päättyneet haarat tuettuun versioon, etsi pysyvyyttä ja uusi istuntoavaimet.	[S14][S61][S62][S80][S87]

Tuote ja CVE-tunnisteet	Haavoittuvat versiot	Korjatut versiot ja korvausohje	Lähteet
PHP (`CVE-2026-109618` , `CVE-2026-109619` ; sekä erillinen 19.11. tiedote `CVE-2026-115560` / `GHSA-658j-r8rw-q6mx`)	`CVE-2026-109618` / `109619` : PHP `8.5` ennen `8.5.12` , `8.4` ennen `8.4.27` , `8.3` ennen `8.3.36` , `8.2` ennen `8.2.35` sekä tukea vailla olevat `8.1` ja vanhemmat (`7.3.0+` / `5.4.0+`). Erillinen `CVE-2026-115560` : PHP `8.5` ennen `8.5.13` , `8.4` ennen `8.4.28` , `8.3` ennen `8.3.37` , `8.2` ennen `8.2.36` (ml. lokakuun versiot) sekä tukea vailla olevat `5.4.0+` -haarat.	Lokakuun vähimmäisversiot haavoittuvuuksille `CVE-2026-109618` / `109619` olivat `8.5.12` , `8.4.27` , `8.3.36` ja `8.2.35` . Ajantasaiseen korjaukseen 19.11. `CVE-2026-115560` -paikan kanssa päivitä versioihin `8.5.13` , `8.4.28` , `8.3.37` tai `8.2.36` (tai `8.6.0` / uudempaan tuettuun versioon tai jakelun/LTS-korjaukseen) [S72][S85]. Siirry pois `8.1` - ja vanhemmista haaroista (PHP `8.2` elinkaari päättyy 31.12.2026); päivittäminen on välttämätöntä, koska mikään väliaikainen asetus ei tee asennuksesta turvallista [S72]. `CVE-2026-115560` edellyttää käytössä olevaa upload progress -toimintoa, keskenään eriäviä `session.serialize_handler` -asetuksia ajon aikana tai jaetussa istuntovarastossa sekä sopivaa luokkaketjua [S85]. Marraskuun korjaus poistaa `session.upload_progress.enabled` -asetuksen oletuksena, mutta nimenomainen asetus ohittaa oletuksen, eikä korjaus pakota samaa serialisoijaa jaetuissa varastoissa [S85]. Pidä `session.upload_progress.enabled=0` ennen pyynnön jäsentämistä (`php.ini` , FPM-pooli tai palvelinasetus, ei `ini_set()` eikä `.user.ini`) työprosessit uudelleenkäynnistäen tai yhdenmukaista serialisoijat [S85]. Haavoittuvuudessa `CVE-2026-109619` asetus estää vain varmistetut istuntopolut eikä muita muunnelmia.	[S15][S63][S64][S72][S85][S86]

Tuote ja CVE-tunnisteet	Haavoittuvat versiot	Korjatut versiot ja korvausohje	Lähteet
Zimbra Collaboration (`CVE-2025-66376`)	Zimbra Collaboration (ZCS) `10.0` ennen `10.0.18` ja `10.1` ennen `10.1.13` (Classic UI XSS)	Haavoittuvuuden `CVE-2025-66376` vähimmäiskorjaus on `10.1.13` ; päivitä uusimpaan tuettuun `10.1.x` -tietoturvajulkaisuun [S78]. Vaikka myös `10.0.18` korjasi vian, `10.0` -haaran elinkaari päättyi 31.12.2025, joten siirrä `10.0` - ja vanhemmat ympäristöt tuettuihin `10.1.x` -julkaisuihin.	[S65][S78]
TP-Link SOHO -reitittimet (`CVE-2023-50224`)	Elinkaarensa päättyneet mallit mukaan lukien `TL-WR841N` (`v11` ennen `11_211209` , `v12` ennen `12_230317`) ja lukuisat päivittämättömät EOL-reitittimet ja tukiasemat	Korvaa päivittämättömät elinkaarensa päättyneet laitteet valmistajan tukemilla malleilla, jotka saavat säännölliset tietoturvapäivitykset; jos päivitys on saatavilla, asenna uusin laiteohjelmisto, estä etähallinta internetistä ja vaihda oletustunnukset	[S52][S66][S77]

12.3 Jatkuvan varmennuksen tuki

Organisaatiot, jotka kaipaavat kohdennettua näkyvyyttä verkkotunnusaltistukseen, tietovarkaus-tunnushälytyksiin, samankaltaisiin verkkotunnuksiin ja suomalaisbrändeihin kohdistuviin alamaailmaväitteisiin, voivat pyytää Brandefensen esittelyn osoitteesta Brandefense demo request.

KESKEISET HAVAINNOT

01

Aloita reunaeristys, avoimien OT-laitteiden poisto ja Device Code Flow -esto välittömästi.

02

Sulje 94 verkkotunnuksen DMARC-seuranta-aukko ja testaa FISA- sekä NIS2-ilmoitusreitit 30 päivässä.

03

Vaadi päivätty palautus-, rajapinta- ja jatkuvuustestinäyttö välietappien kuittaamiseen.

LIITTEET

Liitteet

A–D

TÄMÄ LUKU VASTAA

Liite A. Menetelmä, rajaukset ja poissulkemiset · Liite B. Todisterekisteri · Liite C. Lähteet · Liite D. Sanasto

87
lähdettä

Liite A. Menetelmä, rajaukset ja poissulkemiset 92
Liite B. Todisterekisteri 95
Liite C. Lähteet 96
Liite D. Sanasto 101

Liite A. Menetelmä, rajaukset ja poissulkemiset

Vertailumaat on valittu esimerkeiksi ainoastaan kontekstin antamiseksi; ne eivät merkitse paremmuusjärjestystä tai poliittista arviota.

A.1 Tarkastelujakso ja todisteiden erottaminen

Raportissa sovelletaan erillisiä tarkastelujaksoja ja tilannekuvapäiviä. Vuoden 2026 tapahtumajakso kattaa **1.1.–22.11.2026** (UTC, julkaisuaikaleiman mukaan) alamaailmajulkaisuille, Ransompedia-listauksille, vuoden 2026 verkkotunnusmaininnoille ja julkisille tapahtumille, ja **8.–22.11.2026** eritellään luvussa §5.3 [S1][S2][S4]. Liukuva 365 päivän verkkotunnusmainintajakso kattaa **23.11.2025–22.11.2026**, erillään vuoden 2026 alajoukosta [S4].

Brandefense Atlas -altistusarvioinnit (248 / 250 verkkotunnusta) sekä passiivinen kokoonpanotilannekuva (kaikki 250 verkkotunnusta) on päivätty **24.11.2026** [S3][S4]. Kaikki viranomaisvaroitukset, säädökset, pankkihuijaustilastot ja uutislähteet varmennettiin **24.11.2026**. Kukin lähde tukee vain omaa väitettään.

A.2 Alamaailman julkaisumäärät ja aineistorajaus

Suomeen merkittyjen viestien kokonaismäärä on **749 602** [S1]. Tammikuu (411 036) ja helmikuu (315 239) kattavat yhdessä **726 275 viestiä (96,9 %)**, joista 726 240 julkaistiin Telegramissa ja 723 961 kantoi turkin kielimerkintää [S1]. Yhdessä tarkastuksessa 622 kaikkiaan 627 tammi–helmikuun julkaisusta oli toistuvaa kaupallista Telegram-mainontaa [S1]. Esitetyt tapaukset ja otteet perustuvat suppeampaan talletettuun aineistoon, joka ei ole kattava luettelo kaikesta julkaistusta. Marraskuu on osittainen 22.11. saakka.

A.3 250 verkkotunnuksen portfolio ja passiiviset tarkistukset

Passiivinen portfolio käsittää **250 DNS-varmennettua suomalaista verkkotunnusta** kymmenessä 25 verkkotunnuksen solussa **24.11.2026** tilannekuvan mukaan [S3]. Valinta on tarkoitushakuinen eikä edusta koko maan tilastollista otosta. DMARC-luvut kuvaavat julkaistuja politiikkaluokkia eivätkä todennettua täyttä kattavuutta tai vastaanottajien käsittelyä (§3.5) [S67]. DNSSEC-, TLS- ja HSTS-luvut säilyttävät arvioidut nimittäjänsä; puuttuvat HTTP- tai TLS-tulokset (mukaan lukien 12 valtionhallinnon verkkotunnusta) kirjataan erikseen eikä virheiksi [S3].

A.4 Valittujen verkkotunnusten altistusarviointi ja maininnat

Brandefense Atlas -altistushavainnot kattavat **248 valituista 250 verkkotunnuksesta 24.11.2026** tilannekuvassa (kaksi päivää 22.11. päättyneen tapahtumajakson jälkeen) [S4]. Altistus jää tuntemattomaksi kahdelle verkkotunnukselle (1 tietoliikenteessä, 1 terveys- ja hyvinvointipalveluissa), eikä puuttuvia havaintoja merkitä nollaksi [S4]. Vain kansallinen Atlas-yleisluku (**45/100**) julkaistaan; toimiala-, ryhmä- tai organisaatiokohtaisia arvosanoja ei esitetä.

Portfolion altistussignaalit kattavat kumulatiiviset laitekytkökset (vähintään 128 734; 5 690 työntekijälaitekytköstä), historialliset tunnistetietueet (2 245 122), asiakirjakytkökset (2 484), 30 päivän samankaltaiset nimet (26 678) ja aktiiviset tunnuslistaukset (41 verkkotunnusta) [S4]. Signaalit voivat olla päällekkäisiä eivätkä kuvaa yksilöllisiä henkilöitä, pelkästään vuoden 2026 toimintaa tai vahvistettuja poikkeamia [S4]. Erikseen liukuvat 365 päivän keskustelukanava- (49 verkkotunnusta, 941 mainintaa) ja Tor-maininnat (56 verkkotunnusta, 662 mainintaa) kattavat kaikki 250 verkkotunnusta ajalta **23.11.2025–22.11.2026**, ja vuoden 2026 alajoukko eritellään erikseen [S4]. Luvun §9.1 12 toimiluvallisen korttipankin luvut ovat tarkka alajoukko 25 rahoitusverkkotunnuksen solusta [S4].

A.5 Kiristyshaittaohjelmalistaukset

Ransompedian **16 Suomeen merkittyä listausta** 22.11.2026 mennessä (koko vuonna 2025 yhteensä 11) mittaavat julkisia kiristysväitteitä eivätkä vahvistettuja murtoja [S2]. Kaksi toistuvaa kohdetta (INC Ransom ja Clop) rajaa yksilölliset merkinnät enintään 14:ään, ja helmikuun kolme 0apt-merkintää jäävät todentamatta Halcyonin yleisen 0apt-varoituksen rinnalla [S2][S54]. Vertailuvuosi 2025 kattaa koko kalenterivuoden.

A.6 Maksukorttirajaus

> KORTTILUKUJEN RAJAUS
>
> Nämä luvut kuvaavat rajattua julkaisuaineistoa. Ne eivät arvioi suomalaisten korttivarkauksien kokonaismäärää, petostappioita tai korttien toimivuutta.

Havaitut **73 Suomeen merkittyä korttitietuetta** (109 esiintymää 83 viestissä, 41 BIN-sarjaa) sekä **1 711 tarjousviestiä** ilman selväkielisiä korttinumeroita (1 520 korttikauppapäivitystä) eivät osoita korttien aitoutta, saldoa tai pankkimurtoa [S1].

A.7 Julkiset tapaukset, poissulkemiset ja nimeämissääntö

Neljätoista julkista tapausta (`Tapaukset H–U`) ja seitsemän alamaailman väitetapausta (`Tapaukset A–G`) muodostavat tuetut löydökset.

Kolme aineistoryhmää on rajattu selkeästi pois vuoden 2026 suomalaisista kyberpoikkeamista. Ensiksi Helsingin hovioikeuden elokuun 2026 toimivaltaratkaisu joulukuun 2024 Eagle S -kaapelitapauksessa on oikeudellinen vaihe vuoden 2024 merenkulkutapahtumassa eikä vuoden 2026 kyberhyökkäys [S57]. Toiseksi tietosuojavaltuutetun Finlex-päätös `2026/10` on hallinnollinen tietosuojapäätös [S23][S24]. Kolmanneksi Morningstarin maaliskuun Telegram-väitteet suomalaisista asuntokameroista jätettiin pois, koska Suomea koskeva murtoväite jää todentamatta [S1].

Kohdeorganisaatio nimetään vain, kun tapaus on **sekä** virallisesti vahvistettu että laajasti uutisoitu valtakunnallisessa tai alueellisessa mediassa. Vahvistetut suomalaiset tiedotteet ilman avoimesti saatavilla olevaa laajaa uutisointia (`Tapaus K`) kuvataan yleisen roolin kautta jättäen verkkotunnukset ja osoitteet julkaisematta [S49]. Tapaukset N ja O ovat vahvistettuja ja alueellisesti uutisoituja tapauksia, jotka esitetään roolin mukaan ilman organisaatioiden verkkotunnuksia ja osoitteita [S41][S42][S50].

Kun uutislähde nimeää vahvistamattoman tai rekisteröimättömän organisaation (`Tapaukset H, P ja S`), viitataan vain uutisjulkaisijan juuriosoitteeseen artikkeliosoite salattuna [S33][S45][S48]. Muut ulkoiset lähteet sisältävät varmennetut linkit.

Liite B. Todisterekisteri

Todelliset otteet esitetään vastaavissa luvuissa. Päivämäärä kuvaa julkaisuhetkeä; yksikään kortti ei yksin osoita toteutunutta kauppaa tai vahvistettua murtoa.

Kortti	Päivämäärä	Alusta	Nimimerkki	Kieli	Luku
B01	2026-02-18	Foorumiketju	Nimimerkki salattu	englanti	§4
B02	2026-04-04	Foorumiketju	Nimimerkki salattu	englanti	§4
B03	2026-10-09	Foorumiketju	Nimimerkki salattu	englanti	§4
B04	2026-02-24	Foorumiketju	Nimimerkki salattu	englanti	§4
B05	2026-04-13	Foorumiketju	Nimimerkki salattu	englanti	§4
B06	2026-05-26	Foorumiketju	Nimimerkki salattu	englanti	§4
B07	2026-09-25	Foorumiketju	Nimimerkki salattu	englanti	§4
B08	2026-02-11	Foorumiketju	Nimimerkki salattu	venäjä	§4
B09	2026-04-29	Foorumiketju	Nimimerkki salattu	englanti	§4
B10	2026-04-08	Foorumiketju	Nimimerkki salattu	venäjä / englanti	§8
B11	2026-05-31	Foorumiketju	Nimimerkki salattu	venäjä	§8
B12	2026-10-24	Foorumiketju	Nimimerkki salattu	venäjä	§8
B13	2026-11-22	Foorumiketju	Nimimerkki salattu	englanti	§4
B14	2026-11-17	Foorumiketju	Nimimerkki salattu	englanti	§4
B15	2026-11-20	Foorumiketju	Nimimerkki salattu	englanti	§9
B16	2026-01-22	Foorumiketju	Nimimerkki salattu	englanti	§9

Liite C. Lähteet

S1: Odin by Brandefense. Talletetut alamaailmahavainnot ja julkaisumäärät (1.1.–22.11.2026; tuore jakso 8.–22.11.2026). URL salattu; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S2: Ransompedia. Maamerkityt kiristyshaittaohjelmalistaukset (1.1.–22.11.2026 ja koko vuosi 2025). URL salattu; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S3: Odin by Brandefense. 250 valitun suomalaisen verkkotunnuksen kokoonpanohavainnot (24.11.2026). URL salattu; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S4: Brandefense Atlas ja Odin by Brandefense. Altistushavainnot 248 arvioidulle suomalaiselle verkkotunnukselle (24.11.2026). Liukuvat 365 päivän keskustelukanava- ja Tor-maininnat kaikille 250 valitulle verkkotunnukselle (23.11.2025–22.11.2026; vuoden 2026 alajoukko 1.1.–22.11.2026). URL salattu; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S5: Traficom / Kyberturvallisuuskeskus. Kybertilannekuva 2025. https://vuosiraportit.traficom.fi/fi/kyberturvallisuuden-vuosi-2025/kybertilannekuva-2025 Varmennettu 2026-11-24.

S6: Traficom / Kyberturvallisuuskeskus. Kyberturvallisuuden ensimmäinen vuosipuolisko 2026, 15.6.2026. https://www.traficom.fi/fi/uutiset/kyberturvallisuuden-ensimmainen-vuosipuolisko-2026-kyberuhkien-torjuminen-vaatii-vahvempaa-varautumista-ja-resursointia Varmennettu 2026-11-24.

S7: Kyberturvallisuuskeskus (Traficom). Kybersää helmikuu 2026 (PDF), 15.4.2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20helmikuu%202026.pdf Varmennettu 2026-11-24.

S8: Kyberturvallisuuskeskus (Traficom). Viikkokatsaus 13/2026 (WhatsApp-huijaus, ClickFix, `.fi`-poistot, SMS-tunnusten määräaika 4.5.2026), 27.3.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-132026 Varmennettu 2026-11-24.

S9: Kyberturvallisuuskeskus (Traficom). Kybersää, toukokuu 2026 (PDF), 11.6.2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4,%20toukokuu%202026.pdf Varmennettu 2026-11-24.

S10: Kyberturvallisuuskeskus (Traficom). Kybersää kesäkuu 2026 (PDF), 2.7.2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20kes%C3%A4kuu%202026.pdf Varmennettu 2026-11-24.

S11: Kyberturvallisuuskeskus (Traficom). Kybersää heinäkuu 2026 (PDF), 13.8.2026. https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20hein%C3%A4kuu%202026.pdf Varmennettu 2026-11-24.

S12: Kyberturvallisuuskeskus (Traficom). Elokuun Kybersää 2026, 10.9.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/elokuun-kybersaa-2026 Varmennettu 2026-11-24.

S13: Kyberturvallisuuskeskus (Traficom). Syyskuun kybersää 2026, 15.10.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/syyskuun-kybersaa-2026 Varmennettu 2026-11-24.

S14: Kyberturvallisuuskeskus (Traficom). Citrix NetScaler -haavoittuvuuksia hyväksikäytetty Suomessa, 1.10.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/citrix-netscaler-haavoittuvuuksia-hyvaksikaytetty-suomessa Varmennettu 2026-11-24.

S15: Kyberturvallisuuskeskus (Traficom). Kriittisiä haavoittuvuuksia PHP:ssa (tiedote 37/2026; julkaistu 21.10.2026, päivitetty 30.10.2026; luettelee CVE-2026-109618, CVE-2026-109619 ja CVE-2026-115560). https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-37 Varmennettu 2026-11-24.

S16: Kyberturvallisuuskeskus (Traficom). IoT- ja OT-ympäristöjen tietoturva alkaa laitteiden suojaamisesta, 3.11.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/iot-ja-ot-ymparistojen-tietoturva-alkaa-laitteiden-suojaamisesta Varmennettu 2026-11-24.

S17: Kyberturvallisuuskeskus (Traficom). Lokakuun Kybersää 2026, 12.11.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/lokakuun-kybersaa-2026 Varmennettu 2026-11-24.

S18: Kyberturvallisuuskeskus (Traficom). Viikkokatsaus 45/2026 (ennakoivat kylmälaiteyhteydenotot 13.10. alkaen, Kansallinen riskiarvio, Taisto), 6.11.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-452026 Varmennettu 2026-11-24.

S19: Kyberturvallisuuskeskus (Traficom). Viikkokatsaus 46/2026 (robottihuijauspuhelut, koti-IoT ja kylmälaitteet), 13.11.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-462026 Varmennettu 2026-11-24.

S20: Kyberturvallisuuskeskus (Traficom). Viikkokatsaus 47/2026 (Black Friday -huijaukset, kotiyhteyksien välitysväärinkäyttö, CRA-ohje), 20.11.2026. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-472026 Varmennettu 2026-11-24.

S21: Finlex. Kyberturvallisuuslaki (124/2025). https://www.finlex.fi/fi/lainsaadanto/2025/124 Varmennettu 2026-11-24.

S22: Finlex. Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025). https://www.finlex.fi/fi/lainsaadanto/2025/310 Varmennettu 2026-11-24.

S23: Finlex. Tietosuojalaki (1050/2018). https://www.finlex.fi/fi/lainsaadanto/2018/1050 Varmennettu 2026-11-24.

S24: Finlex. Tietosuojavaltuutetun päätös 2026/10: sivullisen pääsy e-laskun tietoihin, 31.3.2026. https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2026/10 Varmennettu 2026-11-24.

S25: Kunta- ja hyvinvointialuetyönantajat KT. Hallitus esittää seuraamusmaksua tietosuojarikkomuksesta myös julkiselle sektorille, 2026. https://www.kt.fi/uutiset-ja-tiedotteet/2026/hallitus-esittaa-seuraamusmaksua-tietosuojarikkomuksesta-myos-julkiselle Varmennettu 2026-11-24.

S26: Finanssivalvonta. Valvottavatiedote 4/2026: DORA-häiriöilmoitusten toimitus FISA-verkkolomakkeelle 11.2.2026 alkaen, 19.1.2026. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2026/hairioilmoitusten-toimitustapa-muuttuu/ Varmennettu 2026-11-24.

S27: Finanssivalvonta. DORA-sääntelykokonaisuus, 2026. https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/dora/ Varmennettu 2026-11-24.

S28: Suomen Pankki. TIBER-FI-toimintamalli, 2026. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/tiber-fi-toimintamalli/ Varmennettu 2026-11-24.

S29: Finanssiala ry. Vuoden 2025 pankkihuijausluvut (148 milj. EUR), 3.2.2026. https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-huijata-148-miljoonaa-euroa-vuonna-2025/ Varmennettu 2026-11-24.

S30: Finanssiala ry. Alkuvuoden 2026 huijausluvut (60 milj. EUR, 20 000 yritystä), 16.9.2026. https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-alkuvuonna-huijata-60-miljoonaa-euroa-huijausyritysten-lukumaarat-hurjassa-kasvussa/ Varmennettu 2026-11-24.

S31: Digi- ja väestötietovirasto (DVV / Suomi.fi). Varoitus Suomi.fin nimissä liikkuvista huijausviesteistä, 2.9.2026. https://www.suomi.fi/uutiset/varo-liikkeella-olevia-suomi-fin-nimissa-liikkuvia-huijausviesteja Varmennettu 2026-11-24.

S32: AfterDawn (dawn.fi). Valtorin tietomurron laajuus jopa 50 000 käyttäjään, 6.2.2026. https://dawn.fi/uutiset/2026/02/06/valtori-tietomurto Varmennettu 2026-11-24.

S33: Demokraatti (STT / Yle). Valtorin tietomurto osui myös muiden valtionhallinnon organisaatioiden laitteisiin, 7.5.2026. https://demokraatti.fi (artikkelilinkki salattu nimeämättömän organisaation suojaamiseksi). Varmennettu 2026-11-24.

S34: Demokraatti (STT). Valtori ajaa julkisia verkkopalveluja alas varotoimena PHP-haavoittuvuuksien vuoksi, 21.10.2026. https://demokraatti.fi/valtori-valtionhallinnon-verkkopalveluja-ajetaan-alas-varotoimena Varmennettu 2026-11-24.

S35: Finnair (Cision). Virallinen tiedote: Amadeuksen globaali tietovuoto Finnairin ja Aurinkomatkojen varauksista, 9.11.2026. https://news.cision.com/fi/finnair/r/amadeuksen-globaalissa-tietovuodossa-on-ollut-mukana-myos-finnairin-asiakkaiden-tietoja,c4422110 Varmennettu 2026-11-24.

S36: Lentoposti.fi. Amadeuksen varausjärjestelmämurto ja Finnair-tiedot, marraskuu 2026. https://www.lentoposti.fi/uutiset/tietomurto_amadeuksen_j_rjestelmiin_kohteena_lentoyhti_iden_matkustajalistat_mukana_finnair_tietoja Varmennettu 2026-11-24.

S37: Aalto EE. Data Breach Notification: Canvas Learning Platform, 7.5.2026. https://www.aaltoee.fi/en/newsroom/2026/data-breach-notification-canvas-learning-platform Varmennettu 2026-11-24.

S38: Aalto-yliopisto. Tiedote Canvas-oppimisalustan tietomurrosta ja yliopistolisenssin puuttumisesta, 11.5.2026. https://www.aalto.fi/en/news/canvas-learning-platform-data-breach-there-may-be-users-at-aalto Varmennettu 2026-11-24.

S39: Pirkanmaan hyvinvointialue (STT Info). Kolmostien Terveyden tiedostomurto (10 263 henkilötunnusta), 25.8.2026. https://www.sttinfo.fi/tiedote/72261363/tietomurto-kolmostien-terveyden-tietoja-sisaltaneeseen-tiedostoon-on-aiheuttanut-tietoturvaloukkauksen?publisherId=69818823&lang=fi Varmennettu 2026-11-24.

S40: Pirkanmaan hyvinvointialue (STT Info). Kirpputorilta löytynyt muistitikku Akaassa ja Urjalassa, 13.1.2026. https://www.sttinfo.fi/tiedote/71732462/kirpputorilta-loytynyt-muistitikku-aiheutti-tietoturvaloukkauksen-akaassa-ja-urjalassa?publisherId=69818823&lang=fi Varmennettu 2026-11-24.

S41: Kunnallinen kirjastotiedote; nimi salattu. Jaettuihin Koha-kirjastojärjestelmiin kohdistunut palvelunestohyökkäys, syyskuu 2026. Verkkolinkki salattu kunnallisen toimijan suojaamiseksi; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S42: Alueellinen kirjastotiedote; nimi salattu. Jaettujen Koha-kirjastojärjestelmien palvelunestohäiriö, syyskuu 2026. Verkkolinkki salattu kunnallisen toimijan suojaamiseksi; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S43: Rahaliike Holmasto. Tietoturvaloukkaus asiakasrekisterissä, päivitetty 15.9.2026. https://www.holmasto.fi/tietoturvaloukkaus/ Varmennettu 2026-11-24.

S44: Eckerö Line. Tiedote varausjärjestelmätoimittajan alihankkijan hyökkäyksestä, lokakuu 2026. https://www.eckeroline.fi/blog/tarkeaa-tietoa-henkilotietojesi-turvallisuudesta Varmennettu 2026-11-24.

S45: Nya Åland. Alueellinen uutisraportti ahvenanmaalaisen organisaation ilmoittamasta tietomurrosta, syyskuu 2026. https://www.nyan.ax (artikkelilinkki salattu). Varmennettu 2026-11-24.

S46: Ryde Technology. Security Incident August 2026, päivitetty 5.8.2026. https://www.ryde-technology.com/security-incident-2026-08-02 Varmennettu 2026-11-24.

S47: Lyko. Lehdistötiedote rajatun järjestelmän tietomurrosta, marraskuu 2026. https://lyko.com/no/om-lyko/media/pressemeldinger/lyko-har-atgardat-dataintrang-i-en-avgransad-del-av-sitt-system Varmennettu 2026-11-24.

S48: AfterDawn (dawn.fi). Euroopan kauppojen kylmälaiteiskut ja suomalaisten päivittäistavarakauppojen lyhyet kylmälaitehäiriöt, marraskuu 2026. https://dawn.fi (artikkelilinkki salattu vahvistamattoman kauppiaan suojaamiseksi). Varmennettu 2026-11-24.

S49: Organisaatiotiedote; nimi salattu. Tietomurto suomalaisen talous- ja yrityspalveluyhtiön IT-ympäristöön, heinäkuu 2026. Verkkolinkki salattu uhrin suojaamiseksi; lähdekartoitus talletettu. Varmennettu 2026-11-24.

S50: Organisaatiotiedote; nimi salattu. Kyberhyökkäys suomalaisen koulutus- ja valmennusorganisaation palvelinympäristöön, syyskuu 2026. Verkkolinkki salattu uhrin suojaamiseksi; lähdekartoitus talletettu. Varmennettu 2026-11-24.

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

S52: FBI IC3. PSA260407: Venäjän GRU (APT28) hyödyntää haavoittuvia reitittimiä, 7.4.2026. https://www.ic3.gov/PSA/2026/PSA260407 Varmennettu 2026-11-24.

S53: Aalto-yliopisto. Tutkimus pelillistetyistä NoName057(16)-palvelunestohyökkäyksistä Nato-maita ja Suomea vastaan, 2026. https://www.aalto.fi/fi/uutiset/tutkimus-pelillistetyt-palvelunestohyokkaykset-pyrkivat-psykologiseen-sodankayntiin-nato-maita Varmennettu 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 Varmennettu 2026-11-24.

S55: Suomenmaa (STT). Supon kansallisen turvallisuuden katsaus 2026, 10.3.2026. https://www.suomenmaa.fi/uutiset/supo-julkisti-kansallisen-turvallisuuden-katsauksen-terrorismin-uhka-arvio-ennallaan-tekoalysta-uudenlaisia-ongelmia/ Varmennettu 2026-11-24.

S56: Suomenmaa (STT). Kansallinen riskiarvio 2026 nostaa esiin kyberoperaatiot, tekoälyn ja datakeskukset, 2.11.2026. https://www.suomenmaa.fi/uutiset/kansallinen-riskiarvio-tuo-esiin-datakeskuksiin-liittyvan-terroriuhan/ Varmennettu 2026-11-24.

S57: Suomenmaa (STT). Helsingin hovioikeuden toimivaltaratkaisu Eagle S -merikaapelitapauksessa, elokuu 2026. https://www.suomenmaa.fi/uutiset/hovioikeus-kumosi-karajaoikeuden-paatoksen-eagle-s-aluksen-miehiston-syytteet-merikaapelirikoista-voi-tutkia-suomessa/ Varmennettu 2026-11-24.

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

S59: NVD. CVE-2026-1281 (Ivanti Endpoint Manager Mobile), julkaistu 29.1.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-1281 Varmennettu 2026-11-24.

S60: NVD. CVE-2026-1340 (Ivanti Endpoint Manager Mobile), julkaistu 29.1.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-1340 Varmennettu 2026-11-24.

S61: NVD. CVE-2026-88771 (Citrix NetScaler ADC ja Gateway), julkaistu 27.9.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-88771 Varmennettu 2026-11-24.

S62: NVD. CVE-2026-88772 (Citrix NetScaler ADC ja Gateway), julkaistu 27.9.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-88772 Varmennettu 2026-11-24.

S63: NVD. CVE-2026-109618 (PHP-muistinhallintahaavoittuvuus), julkaistu 21.10.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Varmennettu 2026-11-24.

S64: NVD. CVE-2026-109619 (PHP-tilanhallintahaavoittuvuus), julkaistu 21.10.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Varmennettu 2026-11-24.

S65: NVD. CVE-2025-66376 (Zimbra Collaboration Classic UI XSS), julkaistu 5.1.2026. https://nvd.nist.gov/vuln/detail/CVE-2025-66376 Varmennettu 2026-11-24.

S66: NVD. CVE-2023-50224 (TP-Link TL-WR841N todennushaavoittuvuus), julkaistu 3.5.2024. https://nvd.nist.gov/vuln/detail/CVE-2023-50224 Varmennettu 2026-11-24.

S67: RFC Editor. DMARC-standardi (RFC 7489), maaliskuu 2015. https://www.rfc-editor.org/rfc/rfc7489.html Varmennettu 2026-11-24.

S68: RFC Editor. SPF-standardi (RFC 7208), huhtikuu 2014. https://www.rfc-editor.org/rfc/rfc7208.html Varmennettu 2026-11-24.

S69: RFC Editor. DKIM-allekirjoitukset (RFC 6376), syyskuu 2011. https://www.rfc-editor.org/rfc/rfc6376.html Varmennettu 2026-11-24.

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

S71: Voice.fi. Suomalaisten uutisointi Lykon tietomurrosta, marraskuu 2026. https://www.voice.fi/ilmiot/teitko-ostoksia-lykossa-tietosi-saattavat-olla-vaarassa-uhka-koskee-pelkastaan-ruotsissa-jopa-50-000-asiakasta Varmennettu 2026-11-24.

S72: PHP Project. Tietoturvajulkaisut ja vuoden 2026 uutisarkisto (loka- ja marraskuun 2026 tietoturvajulkaisut). https://www.php.net/archive/2026.php Varmennettu 2026-11-24.

S73: The Guardian. Euroopan kauppojen kylmälaitteisiin kohdistuneet epäillyt kyberhyökkäykset, 2.11.2026. https://www.theguardian.com/world/2026/nov/02/supermarket-freezers-across-europe-hit-by-second-suspected-cyber-attack Varmennettu 2026-11-24.

S74: Euroopan komissio (EUR-Lex). Komission delegoitu asetus (EU) 2025/301, 5 artikla (DORA-häiriöilmoitusten määräajat), 20.2.2025. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng Varmennettu 2026-11-24.

S75: Euroopan parlamentti ja neuvosto (EUR-Lex). Asetus (EU) 2024/2847 (kyberkestävyyssäädös, CRA), 14 ja 71 artikla, 20.11.2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng Varmennettu 2026-11-24.

S76: Datainspektionen (Ahvenanmaa). Ahvenanmaan tietosuojaviranomaisen virallinen verkkopalvelu, 2026. https://www.di.ax/ Varmennettu 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/ Varmennettu 2026-11-24.

S78: Zimbra. Zimbra Daffodil 10.1.13 Patch Release (CVE-2025-66376 korjaus), marraskuu 2025. https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.13 Varmennettu 2026-11-24.

S79: Ahvenanmaan maakuntapäivät (Ålands lagting). Lagförslag 13/2023-2024: Lakiesityksen perustelut Ahvenanmaan Datainspektionenin ja valtakunnallisen tietosuojavaltuutetun toimivallanjaosta (43 §), 2024. https://www.lagtinget.ax/dokument/lagforslag-132023-2024-57832 Varmennettu 2026-11-24.

S80: Kyberturvallisuuskeskus (Traficom). Varoitus 1/2026: Citrix NetScaler ADC- ja Gateway-tuotteissa kriittisiä haavoittuvuuksia, useita tietomurtoja Suomessa, julkaistu 1.10.2026 (päivitetty 20.10.2026). https://www.kyberturvallisuuskeskus.fi/fi/varoitukset/citrix-netscaler-adc-ja-gateway-tuotteissa-kriittisia-haavoittuvuuksia-useita-tietomurtoja-suomessa Varmennettu 2026-11-24.

S81: Ivanti. Security Advisory: Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281 ja 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 Varmennettu 2026-11-24.

S82: CISA. Known Exploited Vulnerabilities (KEV) Catalog -merkintä haavoittuvuudelle CVE-2026-1340 (Ivantin EPMM RPM-paketit), 2026. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-1340 Varmennettu 2026-11-24.

S83: Ylä-Satakunta. Alueellinen uutisointi Kolmostien Terveyden tiedostomurrosta, 25.8.2026. https://www.ylasatakunta.fi/kolmostien-terveyteen-kohdistui-tietomurto-heinakuussa--yli-10-000-henkilotunnusta-paatyi-vaariin-kasiin-6.184.131488.a15349cb2e Varmennettu 2026-11-24.

S84: The Guardian. Kansainvälinen uutisointi Instructuren Canvas-oppimisalustan tietomurrosta, 12.5.2026. https://www.theguardian.com/technology/2026/may/12/canvas-hacker-deal-student-stolen-data Varmennettu 2026-11-24.

S85: PHP Project (GitHub Security Advisory). GHSA-658j-r8rw-q6mx: istuntoserialisoinnin epäsuhta voi mahdollistaa etäkoodin suorituksen (CVE-2026-115560), 19.11.2026. https://github.com/php/php-src/security/advisories/GHSA-658j-r8rw-q6mx Varmennettu 2026-11-24.

S86: NVD. CVE-2026-115560 (PHP:n session upload progress -istuntoserialisoinnin epäsuhta), julkaistu 19.11.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-115560 Varmennettu 2026-11-24.

S87: NVD. CVE-2026-120868 (Citrix NetScaler ADC ja Gateway pakettikäsittelyn muistin ylivuoto, tiedote CTX697305), julkaistu 12.–13.11.2026. https://nvd.nist.gov/vuln/detail/CVE-2026-120868 Varmennettu 2026-11-24.

Liite D. Sanasto

- **Kansallinen Atlas-yleisluku.** Yksi 0–100-asteikon Brandefense Atlas -altistusluku koko arvioidulle portfoliolle; suurempi luku kuvaa suurempaa havaittua ulkoista altistusta eikä koskaan murtotodennäköisyyttä tai toimialarankingia [S4].
- **ClickFix.** Manipulointitekniikka, joka houkuttelee käyttäjän kopioimaan ja ajamaan haitallisen komennon väärennetyltä verkkosivulta [S12].
- **DMARC.** Verkkotunnuksen politiikka, joka ohjaa vastaanottajia käsittelemään ja raportoimaan todennuksessa epäonnistuneet sähköpostit [S67].
- **SPF.** DNS-mekanismi, jolla verkkotunnus ilmoittaa sallitut lähettävät sähköpostipalvelimet [S68].
- **DKIM.** Digitaalinen sähköpostiallekirjoitus, joka sitoo lähettäjäverkkotunnuksen viestiin [S69].
- **HSTS.** HTTP-otsikkopolitiikka, joka ohjaa selaimen käyttämään aina salattua HTTPS-yhteyttä [S70].
- **DORA / FISA.** EU:n rahoitusalan digitaalisen häiriönsietokyvyn asetus ja Finanssivalvonnan sähköinen ilmoituslomake 11.2.2026 alkaen [S26][S27].
- **Kyberturvallisuuslaki (124/2025).** EU:n NIS2-direktiivin kansallinen täytäntöönpanolaki Suomessa [S21].
- **Henkilötunnus.** Suomalainen yksilöintitunnus; sen tietäminen on kontekstia eikä koskaan riittävä tunnistautuminen [S39].
- **Mobiilivarmenne / Pankkitunnukset.** Teleoperaattorien ja pankkien vahvan sähköisen tunnistamisen välineet Suomessa [S30].
- **NCSC-FI / Kyberturvallisuuskeskus.** Traficomin alaisuudessa toimiva Suomen kansallinen kyberturvallisuuskeskus [S5].
- **TIBER-FI.** Suomen Pankin viitekehys kriittisten rahoitusalan toimijoiden uhkalähtöiseen testaukseen [S28].
- **SMS-lähettäjätunnus.** Tekstiviestin kirjaintunniste, jonka suojaus Traficomilla tuli luvitettavaksi 4.5.2026 mennessä [S8].
- **AiTM (adversary-in-the-middle, väliintulohyökkäys).** Kalastelutekniikka, jossa hyökkääjä asettuu käyttäjän ja aidon kirjautumissivun väliin varastaakseen kirjautumistiedot ja aktiivisen istuntotunnisteen.
- **BIN (bank identification number, pankkitunnistenumero).** Maksukorttinumeron alkunumerot (perinteisesti kuusi ensimmäistä numeroa), jotka yksilöivät korttiverkoston ja liikkeeseenlaskijan.
- **KYC (Know Your Customer, asiakkaan tunteminen).** Asiakkaan henkilöllisyyden varmistaminen ja tuntemisvelvoite, jota rahoituslaitokset ja säännellyt toimijat soveltavat ennen tilien tai palvelujen avaamista.
- **SEPA (Single Euro Payments Area, yhtenäinen euromaksualue).** Eurooppalainen maksujärjestelmäkehys, joka yhdenmukaistaa euromääräiset tilisiirrot ja suoraveloitukset osallistuvissa maissa yhteisten standardien alle.
- **TLP:CLEAR.** Jaettavissa ilman TLP-rajoitusta tietosuoja- ja lakivelvoitteet huomioiden.

Tietoja raportista

Laatinut Odin by Brandefense. Versio 1.0 noudattaa erillisiä tarkastelujaksoja ja tilannekuvapäiviä. Vuoden 2026 tapahtumajakso kattaa 1.1.–22.11.2026 (8.–22.11. eriteltynä), ja liukuva 365 päivän verkkotunnusmainintajakso kattaa 23.11.2025–22.11.2026. Altistusarvioinnit (248 / 250 valittua verkkotunnusta) ja passiiviset kokoonpanohavainnot (kaikki 250 verkkotunnusta) perustuvat 24.11.2026 tilannekuvaan. Kaikki julkiset lähteet varmennettiin 24.11.2026, ja 2 valittua verkkotunnusta jää altistushavainnoissa tuntemattomaksi.

Tämä suomenkielinen laitos on käännetty tekoälyllä englanninkielisestä pääversiosta; tulkintaeroissa englanninkielinen laitos on ensisijainen. Suositukset on arvioitava kunkin organisaation omien järjestelmien ja lakivelvoitteiden mukaisesti.

© 2026 Brandefense. Kaikki oikeudet pidätetään.

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