TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kesäkuu 2025

#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

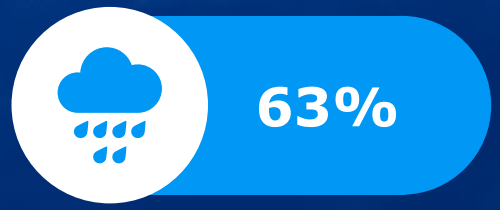
Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville. Lukija saa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja

BadBox 2.0 -haittaohjelma yleistyi nopeasti kesäkuussa. Haittaohjelmaa on tavattu myös esiasennettuna erityisesti edullisissa ja vähemmän tunnettujen valmistajien Android-laitteissa.

Kyberturvallisuuskeskus julkaisi kesäkuussa neljä tiedotetta kriittisistä haavoittuvuuksista. Edellisen kerran haavatiedotteita on julkaistu huhtikuun lopulla.



Kesäkausi on ollut vilkasta aikaa tietoverkoissa tapahtuvien petosten osalta. Kyberturvallisuuskeskus sai kesäkuussa kvartaalin alkuun verrattuna noin 63 % enemmän huijauksiin ja tietojenkalasteluun lukeutuvia ilmoituksia. Näistä valtaosa oli pankkiteemaista tietojenkalastelua.

Kybersää kesäkuu 2025

Tietomurrot ja -vuodot

- Kesäkuu oli melko rauhallinen tietomurtojen ja -vuotojen osalta.
- Haavoittuvuusskannaus on aktiivista. Hyökkääjät etsivät jatkuvasti haavoittuvia laitteita tai ohjelmistoja, joita voidaan käyttää tietomurtoihin.
- Microsoft 365 -sähköpostitilien kalastelu oli aktiivisia. Varastetut tunnukset mahdollistivat tuhansien kalasteluviestien lähettämisen.

Huijaukset ja kalastelut

- Verkkohuijaukset ovat kasvaneet hälyttävästi. Kyberturvallisuuskeskus julkaisi ohjeita huijausten uhreille. Älä jää yksin murehtimaan, jos tulit huijatuksi!
- Huijauspuheluita soitetaan pankin, poliisin tai muiden viranomaisten nimissä. Kesäkuussa huijarit ovat väittäneet soittavansa Kyberturvallisuuskeskuksesta.

Haittaohjelmat ja haavoittuvuudet

- Kesäkuun aikana havaittiin korostuneesti BadBox 2.0 -haittaohjelmaa, joka vaikuttaa Android -käyttöjärjestelmällä toimiviin laitteisiin.
- Kesäkuussa havaittiin kriittisiä haavoittuvuuksia NetScaler ADC & NetScaler GateWay -tuotteissa, sekä Cisco ISE & Passive Identity Connector tuotteissa.

Automaatio ja IoT

- Android-pohjaisia televisioita, TV-bokseja, tabletteja ja muita päätelaitteita on jouduttu poistamaan käytöstä valmistusvaiheessa asennetun BadBox 2.0 -haittaohjelman vuoksi.
- BadBox 2.0 on hyvä esimerkki IoT-laitteiden toimitusketjujen kyberturvallisuuden merkityksestä, tässä tapauksessa erityisesti kuluttajalaitteiden osalta.

Verkkojen toimivuus

- Kesäkuussa yleisissä viestintäverkoissa havaittiin yksi toimivuushäiriö.
- Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä vaikutuksia suomalaisiin verkkopalveluihin.

Vakoilu

- Lähi-idän tilanne heijastuu kyberturvallisuustilanteeseen sekä haktivismina että kybervakoiluna.
- Pohjois-Koreaan julkisuudessa yhdistetty uhkatoimija jatkaa mm. ohjelmistokehittäjiin kohdistuvaa kampanjaansa, jossa ihminen pyritään samaan asentamaan laitteelleen haittaohjelma esimerkiksi työnhakuun liittyvän kokeen tai avunpyynnön varjolla.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberala murroksessa -webinaari järjestettiin 9.6. Tilaisuudessa perehdyttiin muun muassa avaruus- ja kvanttiteknologian kehitykseen, mahdollisuuksiin sekä turvallisuushaasteisiin. Webinaarin tallenne on katsottavissa Traficomin YouTube -kanavalla.[1]

Verkkoon sijoittuvan huijauksen tai petoksen uhriksi voi joutua käytännössä kuka tahansa, ja tapauksella saattaa olla merkittäviä vaikutuksia talouteen tai mielenrauhaan. Apua ja tukea on kuitenkin saatavilla monesta paikasta. Julkaisimme aiheesta Tietoturva Nyt! -artikkelin *”Mistä apua, jos tulee huijatuksi netissä?”.*[2]

Julkaisimme myös kaksi ohjetta Microsoft 365 -ympäristön tietoturvan parantamiseksi, jotka koskevat Admin Consent Workflow sekä Unified Audit Log -toimintoja. Admin Consent Workflown avulla voidaan hallita sovellusten käyttöoikeuksien myöntämistä ja vähentää väärinkäytön riskiä, kun taas Unified Audit Log toiminnolla parannat näkyvyyttä käyttäjien ja ylläpitäjien toimiin. Toimintojen avulla voidaan ehkäistä tilimurtoja, seurata tiedostojen käyttöä sekä täyttää tietosuoja- ja valvontavelvoitteet.[3 & 4]

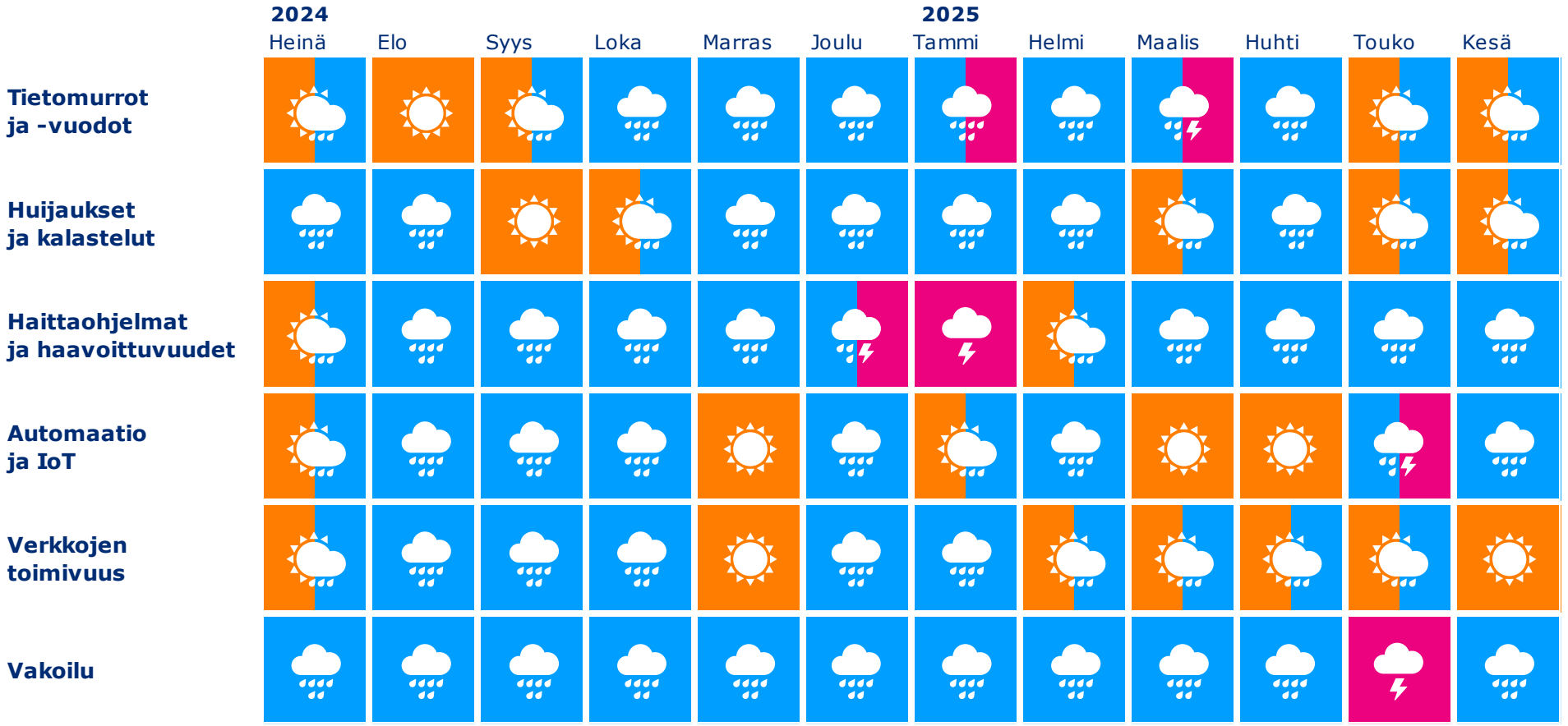
Kesäkuun kyberturvallisuuden yleiskuva

- Alkukesä on tarjonnut pääosin leutoa kybersäätä, eikä kesäkuu tehnyt poikkeusta trendiin. Kesäkaudelle tyypilliset teemat säilyivät edelleen merkittävinä kyberturvallisuuden kannalta:
  - Kesäkuun havainnoissa korostuivat erityisesti pankki-, vero-, Suomi.fi, Omakanta- ja toimitusjohtajateemaiset huijaukset. Mobiilivarmenteeseen kohdistuvaa kalastelua havaitaan edelleen.
  - Kyberturvallisuuskeskuksen viikkokatsauksessa käsiteltiin joillekin ulkomaanmatkoille tarvittaviin ETA- ja ESTA-matkustusilmoituksiin liittyviä huijauksia, jotka aiheuttavat ylimääräisiä kuluja ja saattavat vaarantaa tietoja. Matkustusluvan tai viisumin osalta tulee aina käyttää luvan käsittelystä vastaavan viranomaisen omia verkkosivuja ja ohjeita.[5]
- Haittaohjelmat muodostivat uhkia etenkin kuluttajille, kun BadBox 2.0 havainnot yleistyivät Suomessa nopeasti kesäkuun puolivälissä. Julkaisimme aiheesta Tietoturva Nyt! –artikkelin, jossa haittaohjelmaa käsitellään laajemmin.[6] Muiden haittaohjelmien osalta kuukauden sää oli huomattavasti tyynempi.
- Englannissa sairaalaan kohdistuneen kiristyshaittaohjelmahyökkäyksen uutisoitiin vaikuttaneen potilaan menehtymiseen, hoidon kannalta tärkeiden lääketieteellisten kokeiden viivästyttyä.[7] Tapaus on ensimmäisiä, jossa kyberhyökkäys on mahdollisesti myötävaikuttanut ihmishengen menetykseen.
- Hajautettujen palvelunestohyökkäysten saralla rikottiin jälleen ennätyksiä, kun Cloudflare julkaisi tiedotteen 7,3 Tbit/s palvelunestohyökkäyksestä, joka tuotti 45 sekunnissa tietoliikennettä noin 37.4 teratavun edestä.[8]

Ilmiöiden ja toimialojen trendit

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä eri aikaväleillä. Toimialakohtaisissa nostoissa on esitelty eri toimialojen tilannetta yleistasolla.

Kyberturvallisuuden trendit
kulunut 12 kk

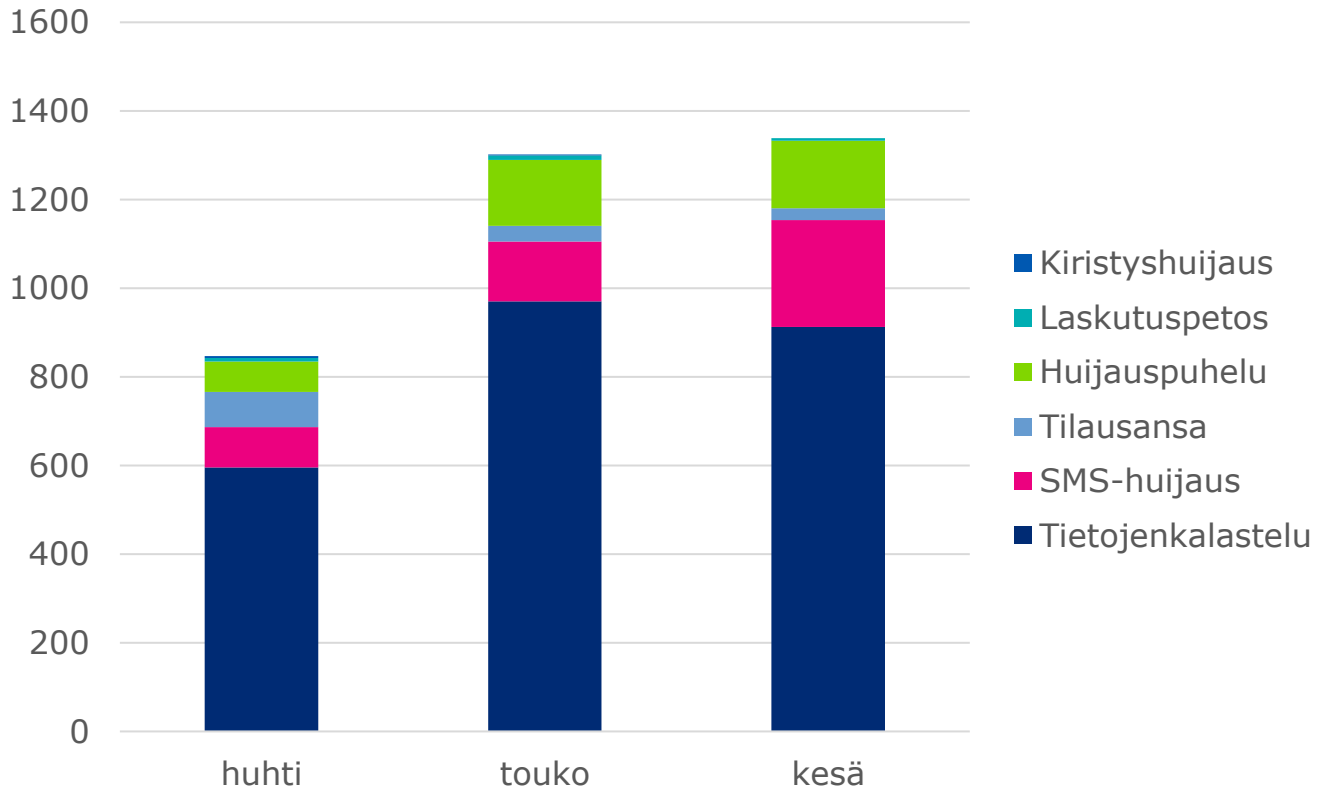


Käsiteltyjä huijaustapauksia
Q2/2025

3 kk

Vuoden 2025 toisen neljänneksen ilmiöitä ovat:

- Nettihuijausten kokonaismäärä on ollut kasvussa vuoden alusta alkaen.
- Verkkopankkitunnusten lisäksi rikolliset ovat alkaneet enenevissä määrin kalastella mobiilivarmennetunnistautumisia.[9]
- Huijauksiin käytetään kaikkia viestivälineitä sähköposteista ja tekstiviesteistä pikaviestimiin ja puheluihin.



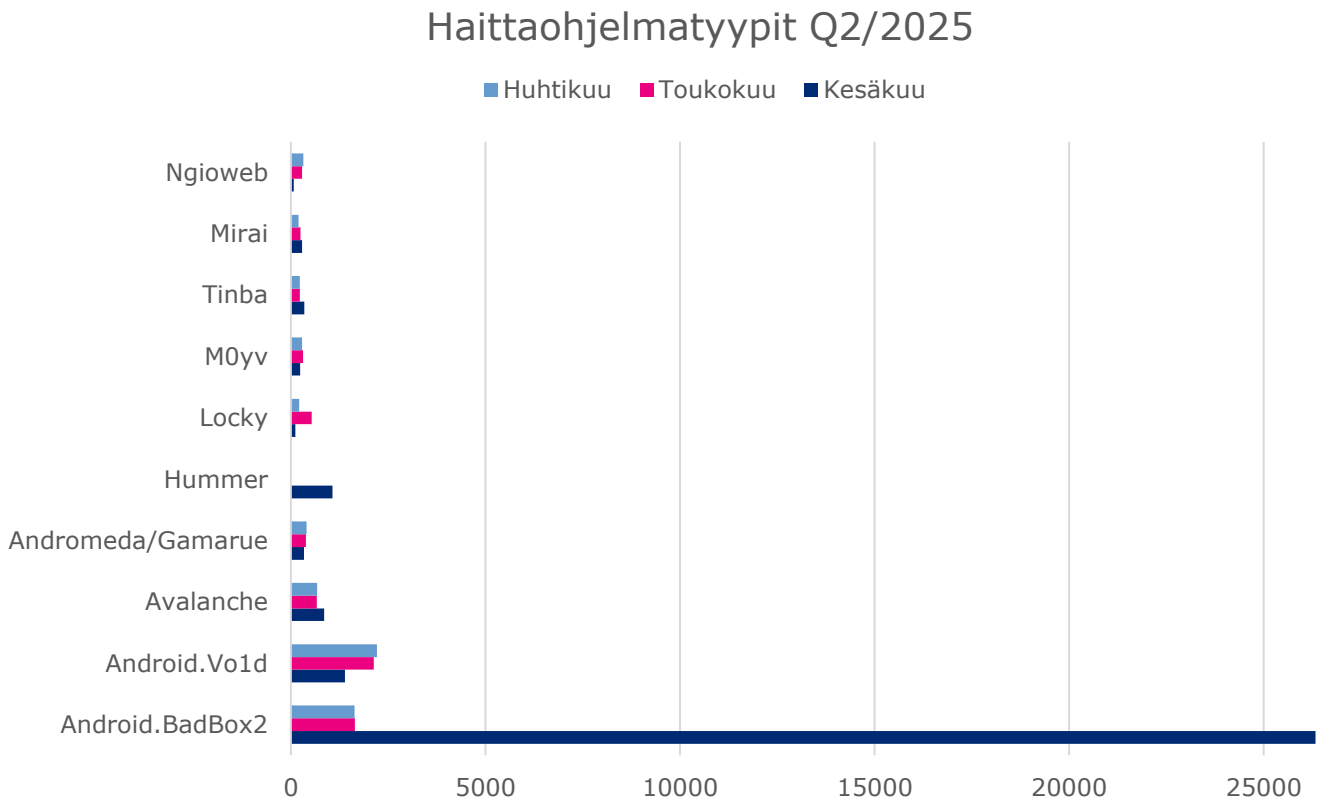
Kyberturvallisuuskeskukselle ilmoitetut tapaukset.

Autoreporterin haittaohjelmahavainnot

3 kk

Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa **Autoreporter-järjestelmän** avulla. Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla



Tilastot kuvaavat haittaohjelmiin kytkeytyviä tapahtumia / liikennettä, eivät yksittäisiä saastuneita laitteita.

3 kk

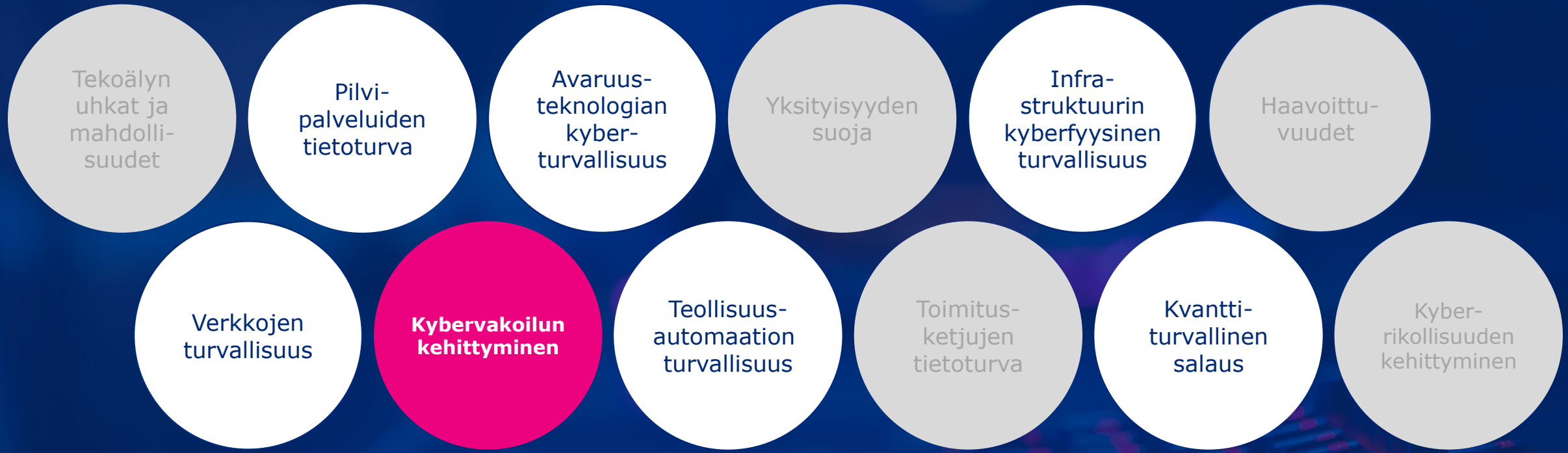
Toimialakohtaiset havainnot

	Trendi 3 kk	Edeltävä 3 kk	
Elintarvike			Kansainvälinen maksuliikennehäiriö vaikutti elintarvikealan vähittäismyynnin toimintaan. Alalla oli kuitenkin pääosin rauhallista.
Energia			Ilmoitettujen tietoturvapoikkeamien määrä väheni. Verkkosivuihin kohdistui palvelunestohyökkäyksiä ja Internetiin näkyviin reunalaitteisiin murtoyrityksiä. Edelleen jatkuva energiamurros muuttaa toimintakenttää, ja mm. suojattavien kohteiden määrä lisääntyy. Sähkökatko Espanjassa, Portugalissa ja Etelä-Ranskassa havainnollisti sähkön saatavuuden tärkeyden myös välillisten vaikutusten kautta.
Finanssi			Kesäkausi on ollut finanssialan kannalta pääosin rauhallinen. Palvelunestohyökkäyksiä havaitaan lähes viikoittain, mutta niillä ei ole merkittäviä vaikutuksia palveluiden toimintaan. Mobillivarmenteen hyväksikäyttöön liittyvät huijaukset ovat jatkuneet.
Teollisuus			Tarkastelujaksolla nähtävissä nousua merkittävien poikkeamien määrässä. Myös vapaaehtoisten ilmoitusten määrä on merkittävästi noussut NIS 2 -direktivin kansallisen lainsäädännön voimaantulon myötä. Tarkastelujaksolla nähty lievää nousua toimitusketjuja koskettavien poikkeamien laajuudessa.
Logistiikka ja liikenne			Ilmoitettujen poikkeamien määrä jatkoi tarkastelujaksolla kasvuaan, mutta tietoon ei tullut erityisen vakavia poikkeamia. Ylivoimaisesti suurin osa ilmoituksista liittyi kalasteluun tai erilaisiin huijausyrityksiin ja monessa ilmoituksessa mainittiin haitallisen viestin lähettäjäksi tutun organisaation murrettu sähköpostitili. Tarkastelujaksolla raportoitiin myös yksittäisiä palvelunestohyökkäyksiä sekä teknisiä häiriöitä organisaation palveluissa.
Valtion-hallinto			NIS 2 -direktiivin mukaiset velvoitteet astuivat voimaan tarkastelujakson aikana, ja ne koskevat myös merkittävää osaa valtionhallinnon organisaatioista. Merkittäviä tietoturvapoikkeamia ei kuitenkaan tullut Kyberturvallisuuskeskuksen tietoon. Ilmoituksia tuli totutusti mm. palvelunestohyökkäyksistä, tietojenkalastelusta ja erilaisista petosyrityksistä.
Media			Kvartaali oli media-alan osalta rauhallinen, eikä merkittäviä poikkeamia raportoitu.
SOTE			Hyvinvointialueilla oli seurantajaksolla tietoliikennehäiriöitä, joilla oli vaikutuksia useisiin terveyskeskuksiin. Myös potilastietojärjestelmissä ilmeni teknisiä vikatilanteita. Palvelunestohyökkäyksiltä ja kalasteluilta ja huijauksiltakaan ei vältytty, mutta merkittäviä kyberturvallisuuden poikkeamia ei siitä huolimatta ilmennyt.
Vesihuolto			Tapahtumien määrä tarkastelujaksolla oli lievästi nousujohteinen. Kohdistettuja kalastelukampanjoita näkyvillä kasvavissa määrin.
Kunnat			Suomalaisia kuntia kohtaan tehtiin kunta- ja aluevaalien yhteydessä palvelunestohyökkäyksiä venäjämielisten haktivistien toimesta. Vakavammilta vaikutuksilta kuitenkin vältyttiin.
Kiinteistö ja rakennus			Tarkasteltavalla ajanjaksolla havaintoja onnistuneista mobiilivarmenneteemaisista kalasteluista, M365-tilimurroista, sekä palomuurituotteen haavoittuvuuden hyväksikäytöstä. Palomuurituotteen haavoittuvuuden hyväksikäyttö ei ole kuitenkaan johtanut merkittäviin seurauksiin. Yleisesti ottaen alalla ollut edellisen kvartaalin tapaan melko rauhallista.

Pitkä aikaväli ja lähitulevaisuus

Osiossa on esitelty pitkän aikavälin ja lähitulevaisuuden kyberturvallisuuden ilmiöitä. Seuraamiemme pitkän aikavälin ilmiöiden joukosta analysoidaan kuukausittain yksi ilmiö. Top 5 –kyberuhkat kertovat puolestaan lähitulevaisuuden uhkista.

Pitkän aikavälin (5v+) kybersää: ilmiöt joita seuraamme



Pitkän aikavälin kybersää: Kybervakoilun kehittyminen

- Kybervakoilu säilyy valtiollisten toimijoiden työkalupakissa yhtenä keinona hankkia tietoa ja pyrkiä strategisiin tavoitteisiin.
  - Kybervakoilun keinoin toteutettavan tiedonhankinnan keskiössä on jatkossakin etenkin poliittinen päätöksenteko mutta myös teollisuusvakoilu, joka liittyy valtioiden tavoittelemaan osaamiseen ja kiinnostaviin teknologioihin ja yrityssalaisuuksiin.
  - Myös Suomi tulee jatkossakin olemaan kiinnostava kohde kybervakoilulle sekä poliittiseen päätöksentekoon liittyen että Nato- ja EU-jäsenyyden ja teknologisen ja muun osaamisen vuoksi.
- Konfliktien kehittyminen ja sodat heijastuvat kybervakoilutilanteeseen monin tavoin. Esimerkiksi Ukrainan ja Venäjän välisen sodan päättyminen voisi vapauttaa resursseja muuhun toimintaan niiltä Venäjään yhdistetyiltä valtiollisilta toimijoilta, jotka nyt ovat toteuttaneet runsaasti kyberhyökkäyksiä Ukrainassa esimerkiksi valtionhallintoa tai kriittistä infrastruktuuria kohtaan.
- Mm. murretuista verkkolaitteista muodostettujen peite- eli anonymisointiverkkojen käyttö tulee todennäköisesti yleistymään entisestään, ja todennäköisesti niitä alkavat hyödyntää myös sellaiset toimijat, joihin ei vielä tällä hetkellä yhdistetä peiteverkkojen käyttöä.
- Tekoälyratkaisujen hyödyntäminen ja kehittyminen tulevat todennäköisesti vaikuttamaan myös kybervakoiluun liittyviin kyberhyökkäyksiin sekä informaatiovaikuttamiseen.
  - Tekoälyä voidaan jo nyt hyödyntää esimerkiksi käännöksissä ja laajojen aineistojen läpikäynnissä.
  - Esimerkkejä käyttökohteista kyberhyökkäyksissä voivat olla esimerkiksi kohdistettujen haitallisten viestien räätälöinti ja luominen, uusien haavoittuvuuksien löytäminen, hyökkäysten toteuttamiseen liittyvä automaatio sekä kiinnijäämisriskin pienentäminen, operaatioturvallisuuden parantaminen tai havainnoinnin vaikeuttaminen.

Tietoturva-alan kehitys, sääntely ja standardit

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat

Kyberturvallisuuslain täydennykset voimaan heinäkuun alussa[10]

- Tasavallan presidentti vahvisti 27.6.2025 muutokset kyberturvallisuuslakiin.
- Muutokset tulivat voimaan 1.7.2025.
- Lakimuutosten myötä kyberturvallisuuslakia sovelletaan myös yhteisöihin, jotka määritetään tulevaisuudessa kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla (ns. CER-direktiivin täytäntöönpanolaki).
- Julkishallinnon osalta vastaavat muutokset tehdään tiedonhallinnasta annettuun lakiin.
- Lakimuutokset tulevat voimaan samaan aikaan uuden yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain kanssa.

Oikeudelliset asiat

Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta voimaan 1.7.2025[11]

- Niin sanottuun CER-direktiiviin (Critical Entities Resilience Directive) perustuva laki asettaa velvoitteita elintärkeitä palveluja tuottaville yrityksille ja muille toimijoille, jotka määritetään kriittisiksi toimijoiksi direktiivin asettamassa aikataulussa.[12]
- Kriittisen toimijan keskeiset velvoitteet liittyvät riskiarviointiin, häiriönsietokykyä koskevaan suunnitelmaan ja toimenpiteisiin häiriönsietokyvyn varmistamiseksi. Lisäksi on ilmoitettava poikkeamista, jotka voivat häiritä keskeisten palvelujen tarjoamista.
- Lainsäädäntö koskee yhtätoista toimialaa: energia, liikenne, pankkiala, rahoitusmarkkinoiden infrastruktuuri, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkishallinto, avaruus sekä elintarvikkeiden tuotanto, jalostus ja jakelu.
- Toimialan vastuuministeriöt tunnistavat ja määrittävät sektorinsa kriittiset toimijat 17.7.2026 mennessä.

Oikeudelliset asiat

Hallituksen esitysluonnos EU:n kyberkestävyyssäädöksen toimeenpanosta lausunnoille[13]

- Liikenne- ja viestintäministeriö pyytää lausuntoja hallituksen esitysluonnoksesta koskien EU:n kyberkestävyyssäädöksen (Cyber Resilience Act, CRA) toimeenpanoa Suomessa.
- Esitysluonnoksessa ehdotetaan säädettäväksi uusi laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista. Lisäksi tehtäisiin muutoksia sähköisen viestinnän palveluista annettuun lakiin ja kyberturvallisuuslakiin.
- EU:n kyberkestävyyssäädös asettaa kyberturvallisuutta koskevat vähimmäisvaatimukset tuotteille ja ohjelmistoille, jotka ovat yhdistettävissä internetiin tai toiseen laitteeseen.
  - Esim. valvontakamerat, jääkaapit, älykellot, televisiot, tietokoneet, puhelimet, lelut, sovellukset ja muut ohjelmistot.
- Asetuksella velvoitetaan laitteiden ja ohjelmistojen valmistajat noudattamaan olennaisia kyberturvallisuusvaatimuksia sekä ilmoittamaan haavoittuvuuksista ja hallitsemaan niitä.

Oikeudelliset asiat

Hallituksen esitysluonnos EU:n kyberkestävyyssäädöksen toimeenpanosta lausunnoille

- Hallituksen esitysluonnoksessa ehdotetaan viranomaisvalvonnan osalta muun muassa, että kyberkestävyyssäädöksen markkinavalvontaa sekä ilmoitettujen laitosten nimeämistä ja valvontaa koskevat tehtävät keskitettäisiin Liikenne- ja viestintävirasto Traficomiin.
- Lisäksi Traficom valvoisi kyberkestävyyssäädöksen vaatimustenmukaisuutta.
- Lausunnon hallituksen esitysluonnoksesta voi antaa osoitteessa Lausuntopalvelu.fi.[14]
- Lausuntoaika suomeksi päättyy 12.8.2025.
- Hallituksen esityksen ruotsinnos lisätään lausuntopalveluun käännöksen valmistuttua ja lausuntoaika ruotsiksi ilmoitetaan erikseen lausuntopalvelussa.
- Asetuksen soveltaminen alkaa siirtymäajan jälkeen 11.12.2027. Aktiivisesti hyödynnettyjen haavoittuvuuksien ilmoittamista sovelletaan kuitenkin jo 11.9.2026 alkaen ja ilmoitettuja laitoksia koskevaa sääntelyä 11.6.2026 alkaen.

Oikeudelliset asiat

Liikenne- ja viestintäministeriö julkaisi kansallisen 6G-tiekartan[15]

- Liikenne- ja viestintäministeriö julkaisi 17.6.2025 6G-viestintäteknologioiden edistämisen työryhmän valmisteleman kansallisen 6G-tiekartan.[16]
- Tiekartassa esitetään askelmerkit 2030-luvulle seuraavan sukupolven matkaviestinteknologioiden kehittämiseen ja käyttöönottoon.
- Suomen tavoitteena on pysyä matkaviestinverkkojen ja verkkoteknologioiden edelläkävijänä 2030-luvulla. Lisäksi tiekartassa asetetaan kuusi muuta tavoitetta:
  - turvallisuus on sisäänrakennettu 6G-teknologiaan ja -sääntelyyn
  - sääntely ja taajuuksien saatavuus tukevat 6G-palveluiden kehittämistä ja aikaista käyttöönottoa
  - suomalaiset yritykset ovat merkittäviä toimijoita 6G:n eri sektoreilla
  - Suomi vaikuttaa entistä aktiivisemmin kansainvälisessä 6G-standardointityössä
  - Suomi pysyy kärkimaana 6G-teknologian tutkimuksessa, kehittämisessä ja innovaatioissa
  - 6G edistää kestävää kehitystä ja energiatehokkuutta.

Oikeudelliset asiat

Liikenne- ja viestintäministeriö julkaisi kansallisen 6G-tiekartan

- Lisäksi 6G-tiekartassa on nimetty neljä painopistettä tavoitteiden saavuttamiseksi. Jokaiselle painopisteelle on tunnistettu keskeisimmät askelmerkit vuosille 2025–2030:
  1. Sääntely- ja taajuustyö
  2. Verkkoturvallisuus
  3. Standardointi
  4. Tutkimus, koulutus ja innovaatio (TKI) -toiminta ja yritysten kilpailukyky.
- Tiekartan toimeenpanoa seurataan osana turvallisuutta ja uutta talouskasvua tietoverkoista (TUUTTI) -hanketta ja verkkoturvallisuuden neuvottelukunnan työtä.
- TUUTTI-hankkeessa muodostetaan Suomen viestintäverkkopolitiikan linjauksia vuoteen 2037 asti. Hankkeessa huomioidaan myös teknologinen kehitys ja maailmanlaajuisen toimintaympäristön muutokset.

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)

Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Lähdeluettelo

1) Kyberala murroksessa –webinaari 09.06.2025 https://www.youtube.com/watch?v=Q5tiFnpQwvw
2) Mistä apua, jos tulee huijatuksi netissä? - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mista-apua-jos-tulee-huijatuksi-netissa
3) Onko teillä jo Microsoft 365 tilauksen Unified Audit Login käytössä? Tarkista että on.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/onko-teilla-jo
4) Paranna tietoturvaa Admin Consent Workflowilla Microsoft Entra ID:ssä ja Microsoft 365:ssa
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/paranna-tietoturvaa
5) Huijaussivustot hyödyntävät ETA- ja ESTA -matkustuslomakkeita – varmista virallinen asiointikanava
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-232025#86408-0
6) Haittaohjelma voi lymyillä laitteessa jo ostovaiheessa – laitteet on poistettava käytöstä, jos valmistaja ei tarjoa korjausta
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haittaohjelma-voi-lymyilla-laitteessa-jo-ostovaiheessa-laitteet-poistettava-kaytosta
7) Ransomware attack contributed to patient’s death, says Britain’s NHS https://therecord.media/ransomware-attack-contributed-patient-death-uk-nhs
8) Defending the Internet: how Cloudflare blocked a monumental 7.3 Tbps DDoS attack https://blog.cloudflare.com/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos/
9) Mobiilivarmenteita käytetään nyt huijauksiin – varmenteella pystyy tarkastelemaan henkilötietoja ja hakemaan lainoja https://poliisi.fi/-/mobiilivarmenteita-kaytetaan-nyt-huijauksiin-varmenteella-pystyy-tarkastelemaan-henkilotietoja-ja-hakemaan-lainoja
10) Kyberturvallisuuslain täydennykset voimaan heinäkuun alusta https://lvm.fi/-/kyberturvallisuuslain-taydennykset-voimaan-heinakuun-alusta
11) Kriittisen infrastruktuurin suojaamista ja kriisinkestävyyttä koskeva laki https://intermin.fi/kansallinen-turvallisuus/mita-on-kansallinen-turvallisuus/kriittinen-infrastruktuuri
12) Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta
https://www.finlex.fi/eli?uri=http://data.finlex.fi/eli/sd/2025/310/ajantasa/2025-06-13/fin
13) Esitysluonnos kyberkestävyyssäädöksen toimeenpanosta lausunnoille
https://lvm.fi/-/esitysluonnos-kyberkestavyyssaadoksen-toimeenpanosta-lausunnoille
14) Lausuntopyyntö: luonnos hallituksen esitykseksi kyberkestävyyssäädöksen toimeenpanoa koskevaksi lainsäädännöksi
https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=a4dd7483-6129-4fd4-bf89-415bd61daf20
15) Kansallinen 6G-tiekartta viitoittaa matkaviestinteknologioiden kehittämistä ja käyttöönottoa
https://lvm.fi/-/kansallinen-6g-tiekartta-viitoittaa-matkaviestinteknologioiden-kehittamista-ja-kayttoonottoa
16) Kansallinen 6G-tiekartta : Suomen askelmerkit 2030-luvulle seuraavan sukupolven matkaviestinteknologioiden kehittämiseen ja käyttöönottoon
https://urn.fi/URN:ISBN:978-952-243-886-7