TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 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

1.

Huijauspuheluiden suodatustoiminta voitti rikoksentorjuntakilpailun. [1] Kahden ensimmäisen toimintavuoden aikana on estetty 16 miljoonaa väärennettyä puhelua.

62%

M365-tietojenkalastelun liittyvien ilmoitusten trendi säilyi noususuhdanteisena. KTK:n vastaanottamien ilmoitusten määrä kasvoi noin 62 % elokuun lukemiin verrattuna.

Kybersää syyskuu 2025

Tietomurrot ja -vuodot

- Murretuilta Microsoft 365 -tileiltä lähetetään usein nopeasti suuri määrä uusia kalasteluviestejä eteenpäin.
- Joissain tapauksissa M365-tietomurrot ovat pitkäkestoisia: hyökkääjä pysyttelee ympäristössä tarkkaillen tilannetta jopa kuukausien ajan ennen kuin hyödyntää uhrin tunnuksia laskutuspetoksen tekemiseen.
- Lisäksi tietomurtoja on tehty hyödyntämällä reunalaitteiden, kuten palomuurien ja VPN-ratkaisujen haavoittuvuuksia.

Huijaukset ja kalastelut

- Huijauspuheluiden estotoiminta voitti rikoksentorjuntakilpailun 2025. Väärennösten estolla on torjuttu miljoonia huijauspuheluita.
- Microsoftin M365 -sähköpostitilien tietomurrot lisääntyivät edelleen. Syyskuussa julkaistiin vakava varoitus M365-tietojenkalastelusta. Tietojenkalastelun avulla tehdyt tietomurrot ovat yleisin tapa tunkeutua yrityksen järjestelmiin.

Haittaohjelmat ja haavoittuvuudet

- Syyskuun lopussa Euroopassa eri lentoasemien toiminta lamaantui kiristyshaittaohjelmatartunnan seurauksena. Välillisinä vaikutuksina lentoyhteydet Suomesta myöhästyivät ja reitittyivät uudelleen.
- Kriittisiä Cisco ASA- ja FTD-haavoittuvuuksia käytetty maailmalla hyväksi hyökkäyksissä.

Automaatio ja IoT

- Yhdysvaltain tievirasto kehotti tutkimaan teiden digitaalista infrastruktuuria piilotettujen komponenttien, kuten radioiden varalta. Teiden käyttöä voitaisiin häiritä tai vakoilla piilotetuilla laitteilla. [2]
- Euroopassa kyberkestävyyssäädös (CRA) ja NIS2-direktiivi luo vahvat toimintamallit sille, kuinka puuttua tällaisiin toimitusketjuista kumpuaviin kyberuhkiin. [3]

Verkkojen toimivuus

- Suomalaisiin organisaatioihin kohdistui useita palvelunestohyökkäyksiä. Merkittäviltä vaikutuksilta palveluiden saatavuuteen säästyttiin. Vaikutuksia vähensi hyvä varautuminen ja aktiiviset vastatoimet.
- Palvelunestohyökkäysten vaikutukset saattavat näkyä myös palveluissa, jotka eivät ole kohteena. Jaetut resurssit voivat ylikuormittua ja aiheuttaa häiriöitä useille palveluille yhtä aikaa.[4]

Vakoilu

- Iraniin liitettyjen uhkatoimijoiden aktiivisuuden Euroopassa kerrotaan kasvaneen. Erään APT-ryhmän raportoitiin pyrkineen murtautumaan teleoperaattoreiden järjestelmiin rekrytointihuijauksen avulla ja toisen APT-ryhmän puolestaan kerrottiin pyrkineen hankkimaan tietoa mm. satelliittitoimialan organisaatioista sekä puolustussektorilta. Kohteita näissä oli muun muassa Britanniassa, Ranskassa, Ruotsissa ja Tanskassa.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Microsoft 365-tilien kalastelu on jatkunut aktiivisena. Tapausmäärien voimakkaasta kasvusta ja niiden aiheuttamasta vaarasta johtuen Kyberturvallisuuskeskus julkaisi ilmiöstä varoituksen. [5]

Palvelunestohyökkäys voi haitata liiketoimintaa ja muodostua säännölliseksi kiusaksi ilman riittävää ennakointia. Varautumiseen kuuluu hyökkäystä edeltävä valmistautuminen, kuten hallinnolliset ja tekniset toimet, hyökkäyksen aikana tapahtuva reagointi sekä jälkitoimet. Voit lukea aiheesta kattavammin Tietoturva Nyt!-artikkelista *”Ennakointi on paras puolustus palvelunestohyökkäyksiä vastaan”.* [6]

Kyberturvallisuuskeskuksen viikkokatsausten yhteydessä käsitellään nyt uutena aihepiirinä myös haittaohjelmia! Haittaohjelmakatsaus on suunnattu erityisesti lukijoille, joille haittaohjelmat eivät ole vielä kovin tuttuja.

Syyskuun kyberturvallisuuden yleiskuva

Alkanut syksy näkyi sateisena säänä myös kyberturvallisuuden saralla. Syyskuu oli tapausmäärien kannalta kohtalaisen vilkas, ja kuukauden aikana havaittiin medianäkyvyyttä keränneitä poikkeamia sekä Suomessa että ulkomailla.

- Suomessa palvelunestohyökkäykset näkyivät uhkakentässä syyskuun puolivälin jälkeen alkaen. Useat hyökkäyksistä kohdistuivat tarkoituksellisesti mediahuomiota herättäviin verkkosivuihin ja organisaatioihin. Tapauksista aiheutuneet häiriöt olivat kuitenkin pääosin lyhytkestoisia. Palvelunestohyökkäykset ovat useille organisaatioille melko arkipäiväisiä ja niistä palaudutaan usein nopeasti.
- Microsoft 365 -tileihin kohdistunut kalastelu ja tietomurrot olivat edelleen kasvutrendissä. Ilmiö antoi aihetta myös varoituksen laatimiselle. [5]

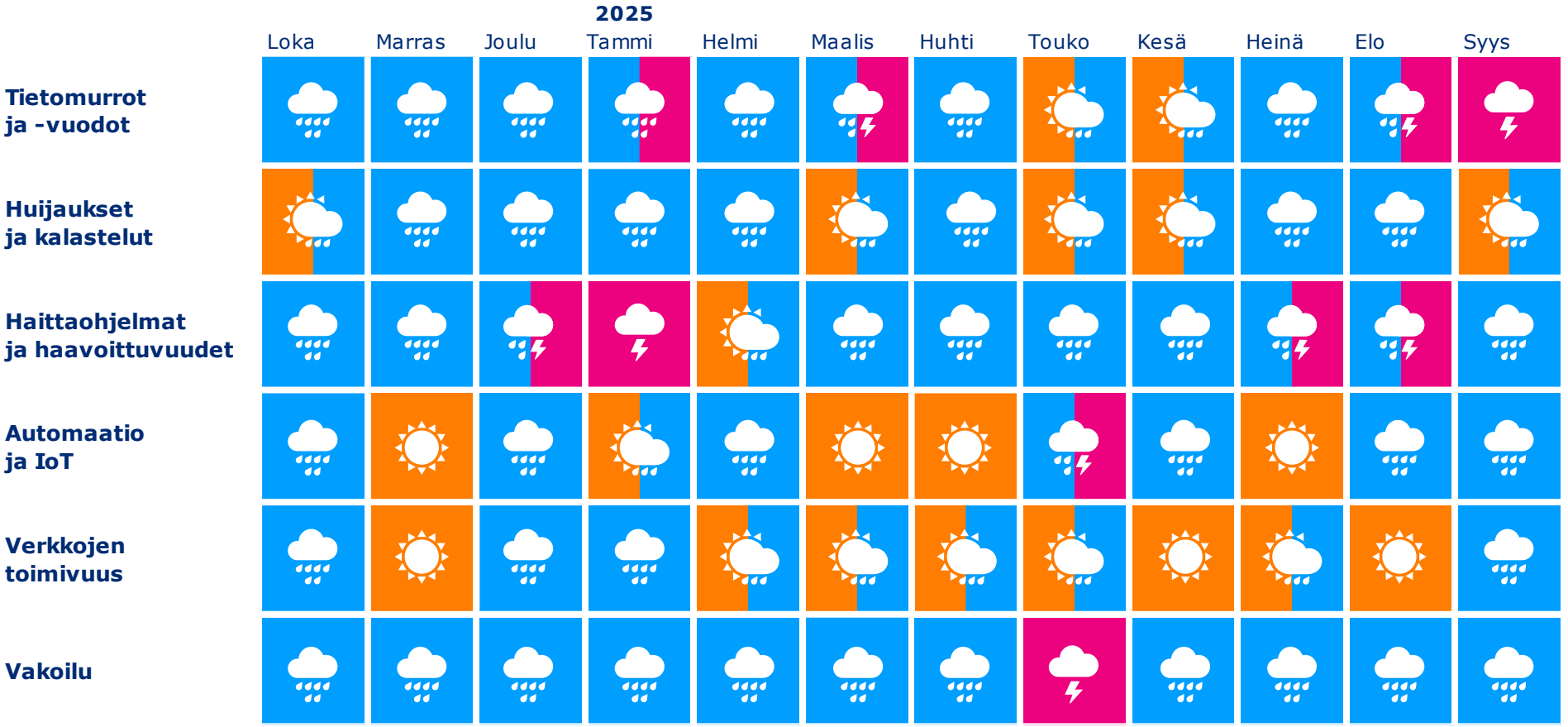
Laajavaikutteinen kyberhyökkäys häiritsi eurooppalaisten lentoasemien toimintaa 19.9 alkaen. [7 & 8]

- Check-in ja Boarding –palveluita tuottavaan Collins Aerospace-yhtiöön kohdistunut kiristyshaittaohjelmahyökkäys haittasi matkustajaliikennettä ainakin Brysselin, Berliinin, Heathrow'n kentillä.
- Hyökkäys aiheutti lentojen viivästymisiä ja perumisia. Osa lentoyhtiöistä otti onnistuneesti käyttöön vaihtoehtoisia menetelmiä asiakkaiden palvelemiseksi, ja esimerkiksi boarding-passeja laadittiin joissain tapauksissa käsin.
- Kokonaisuudessaan hyökkäys vaikutti lentoasemien toimintaan noin viikon ajan, vakavien häiriöiden ajoittuessa ensimmäisille päiville. Berliinin-Brandenburgin lentoaseman verkkosivuilla tiedotettiin vielä 9 lokakuuta kyberhyökkäyksen aiheuttamista häiriöistä.

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

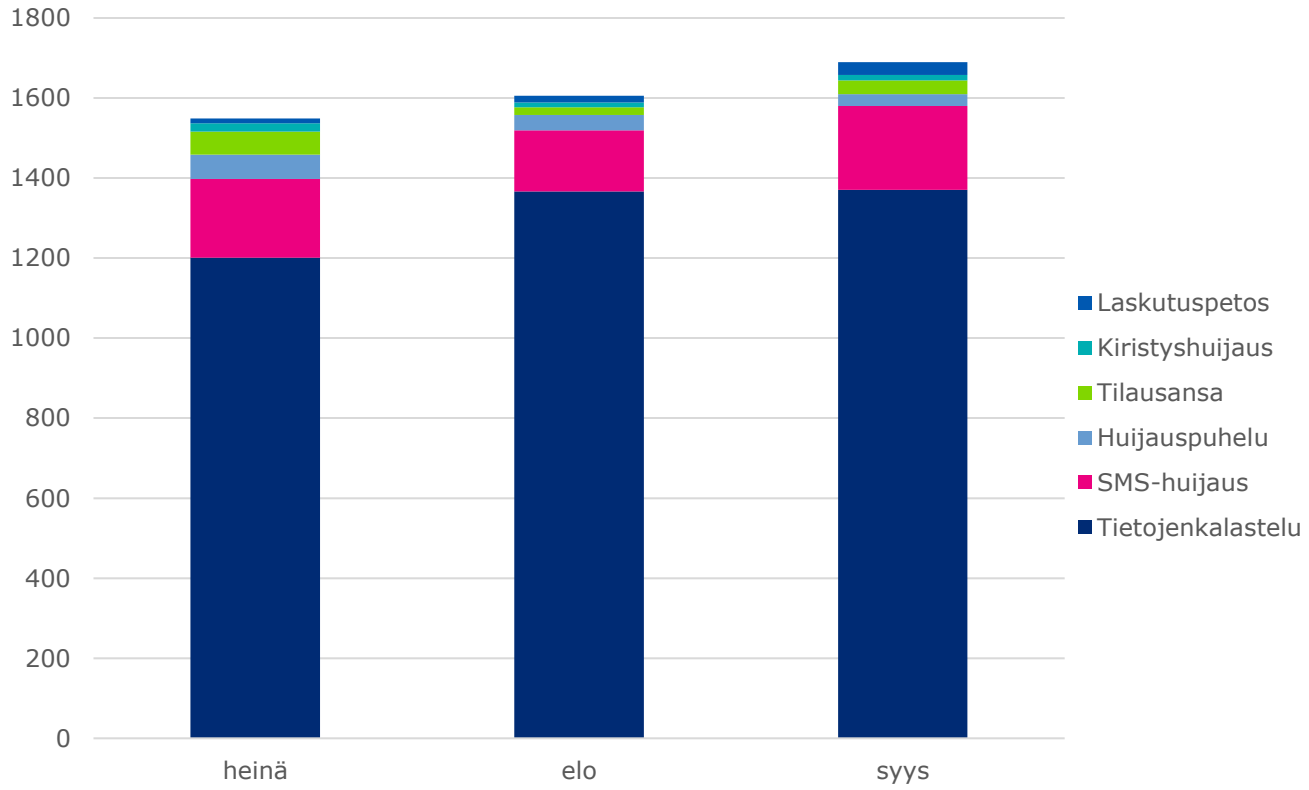


Käsiteltyjä huijaustapauksia
Q3/2025

3 kk

Vuoden 2025 toisen neljänneksen ilmiöitä ovat:

- Microsoft M365-tilien tunnuskalastelu kääntyi jyrkkään nousuun elo- ja syyskuussa.
- Lastensuojeluhuijauksen avulla murtauduttiin useiden yritysten tileihin, joilta varastettiin merkittäviä määriä rahaa.
- Pankkitunnusten kalastelu on edelleen määrällisesti hallitsevin petosmuoto. Pankkitunnuksia kalastelevia huijausviestejä tehtaillaan monin eri teemoin.

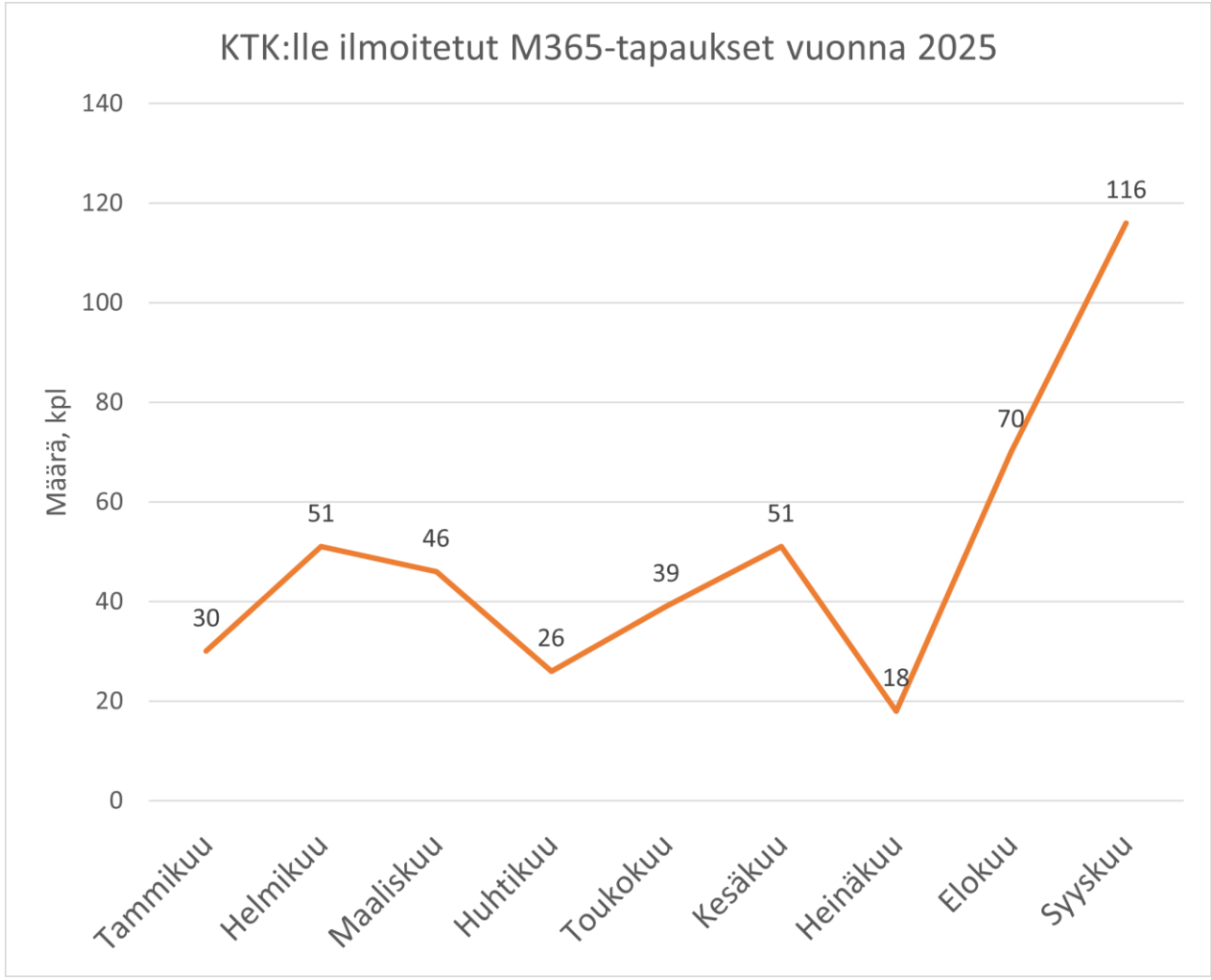


Kyberturvallisuuskeskukselle ilmoitetut tapaukset.

M365-tilimurtotapaukset

KTK:lle ilmoitetuissa M365-tapauksissa havaittiin merkittävää kasvua

- Vakava varoitus julkaistiin verkkosivuillemme 9.9.2025
- Elokuun jo ennätykselliset tapausmäärät ylittyivät syyskuussa
- Murrettuja tilejä käytetään muun muassa jatkokalasteluviestien lähettämiseen, laskutuspetoksiin ja tietojen varastamiseen
- Ota käyttöön suojaustoimia, pelkkä MFA ei yksin estä rikollisten toimintaa

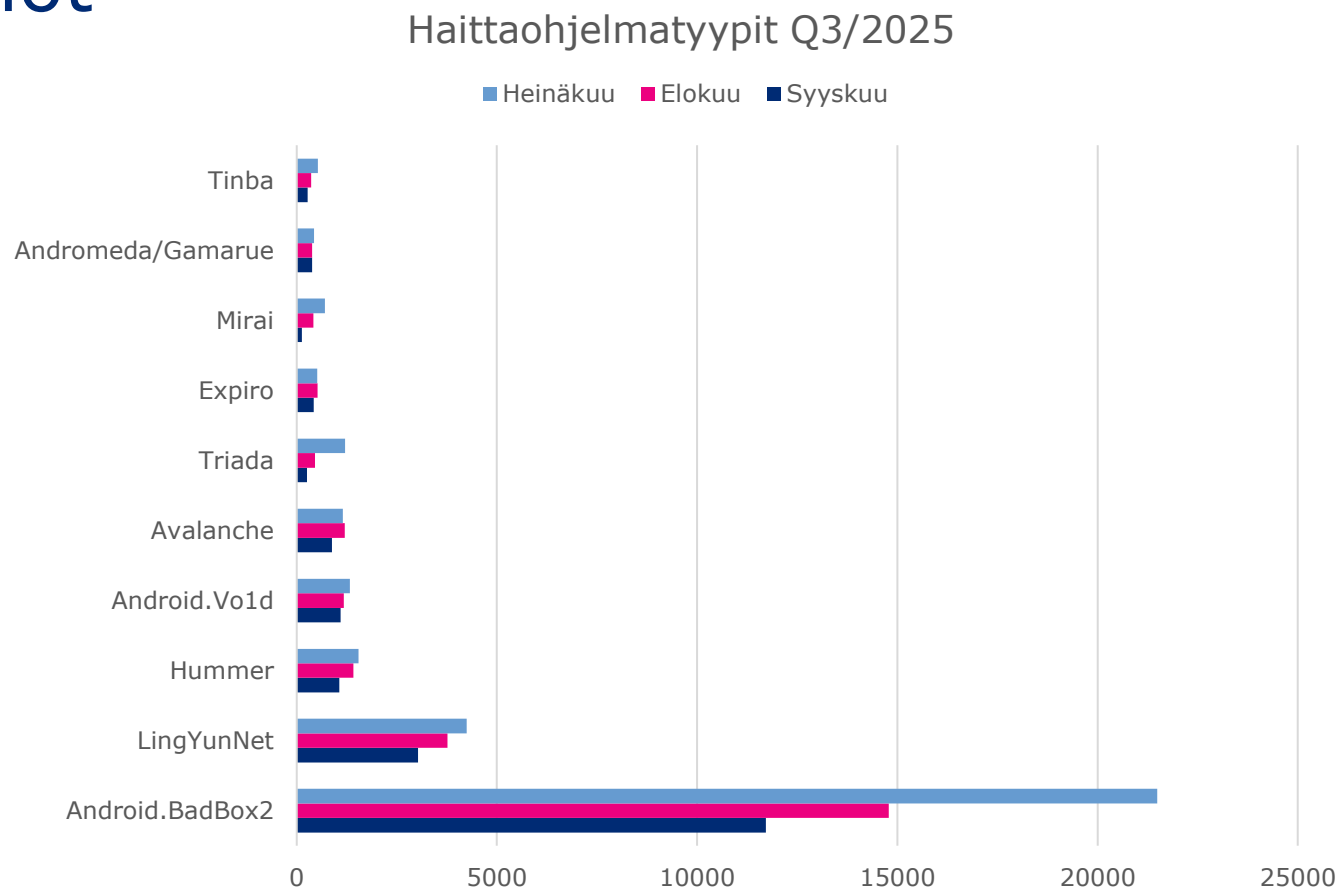


Autoreporterin haittaohjelmahavainnot

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.

Toimialakohtaiset havainnot

	Trendi 3 kk	Edeltävä 3 kk	
Elintarvike			Kyberturvallisuuskeskukselle ilmoitettiin 14 poikkeamasta, mikä oli kaksi kertaa edellisen tarkastelujakson määrä. Suhteellisesti eniten lisääntyivät ilmoitukset ICT-palveluiden saatavuuden häiriöistä, tietomurroista ja tietovuodoista.
Energia			Kyberturvallisuus nähdään entistä tärkeämpänä osana varautumista, harjoittelua sekä testaamista. Poikkeamailmoitusten määrässä ei tapahtunut suuria muutoksia. M365-murrot ja DDoS-hyökkäykset näkyivät myös energiasektorilta tulleissa ilmoituksissa. Sektorin toimijoita osallistui mm. Cyber Fortress ja Nordic Pine -harjoituksiin.
Finanssi			Microsoft 365 -tileihin kohdistuvaa kalastelua ja palveluhyökkäyksiä on raportoitu aikaisempaa enemmän. Pankkitunnusten kalastelu on jatkunut aktiivisena eri pankkien nimissä. EU:n pikamaksuasetus aiheuttaa muutoksia 9.10. alkaen maksutietojen tarkistuksiin ja maksujen nopeaan siirtymiseen pankista toiseen, mikä voi muuttaa myös huijareiden toimintatapoja.
Teollisuus			Tietojenkalastelu oli tarkastelujakson aikana aktiivista ja kalasteluviestien määrässä havaittiin selvää kasvua.
Logistiikka ja liikenne			Kesälomakauden jälkeen ilmoitusmäärät kääntyivät jälleen nousuun ja tarkastelujakso olikin ilmoitusmäärällä mitattuna vuoden aktiivisin. Valtaosa ilmoituksista liittyi kalasteluun tai erilaisiin huijausyrityksiin, mutta myös onnistuneita tietomurtoja ja tietomurron yrityksiä raportoitiin paljon. Yksittäiset organisaatiot olivat palvelunestohyökkäysten kohteena. Kansainvälisesti tarkastelujaksolla oli huomattavan paljon vakavia tapahtumia erityisesti ilmailusektorilla, johon kohdistui mm. kiristyshaittaohjelmahyökkäyksiä.
Valtion-hallinto			Valtionhallintoa koskevat tapaukset koostuivat pääasiassa toimitusjohtajahuijauksista, tietojenkalasteluyrityksistä ja M365-tilimurroista. Lisäksi etenkin jakson loppua kohden havaittiin palvelunestohyökkäyksiä, jotka kohdistuivat valtionhallinnon verkkosivuihin, mutta ne saatiin torjuttua ilman merkittäviä vaikutuksia. Jakson aikana esiintyi myös laskutuspetosyrityksiä ja teknisiä häiriöitä, jotka liittyivät päivityksiin tai järjestelmämuutoksiin. Yleistilanne valtionhallinnossa oli kyberturvallisuuden osalta kuitenkin rauhallinen.
Media			Kvartaali oli media-alan osalta rauhallinen, eikä merkittäviä poikkeamia raportoitu.
SOTE			Tapausten määrä kasvoi edellisestä tarkastelujaksosta yli puolella 72:een tapaukseen, ja samalla tapausten vakavuus kasvoi hieman. Yli puolet tapauksista oli petoksia tai kalasteluita ja niiden määrä kasvoi myös voimakkaimmin. Myös tietomurroista ja ohjelmistohaavoittuvuuksista ilmoitettiin aiempaa useammin.
Vesihuolto			Toimialalla havaittiin tarkastelujakson aikana kasvua kalasteluviestien ja toimitusjohtajahuijausten määrässä.
Kunnat			Kunnissa oli elo-syyskuussa lukuisia onnistuneita M365-tilimurtoja, jotka johtivat uusiin jatkokalasteluihin. Kuntia kohtaan tehtiin alkusyksystä myös palvelunestohyökkäyksiä, mutta niiden vaikutukset jäivät kuitenkin vähäisiksi.
Kiinteistö ja rakennus			Toimialalla tehtiin havaintoja mm. huijauslaskuista, M365-tilimurroista sekä julkiverkossa näkyvillä olevista sinne kuulumattomista verkkopalveluista. Alaan ei kuitenkaan kohdistunut merkittäviä kyberturvallisuuden poikkeamia tarkastelujakson aikana.

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: Avaruusteknologian kyberturvallisuus

- Kansallisvaltioiden ja kansalaisten päivittäiset toiminnot tulevat kaiken aikaa riippuvaisemmiksi avaruusteknologiasta.
  - Satelliittipaikannus (lisääntyvä häirintä ja harhauttaminen)
  - Tietoliikenneyhteydet (esim. Starlink/SpaceX Ukrainan sodassa)
  - Sääilmiöiden seuranta
  - Kaukokartoitus
- Avaruusteknologiaa käyttävät palvelut koostuvat useista segmenteistä (avaruuskomponentti, maatukiasemat, maatukiasemien väliset tietojärjestelmät...) ja kaikkiin näistä liittyy kyberturvallisuusriskejä.
  - Kyberturvallisuuden lainalaisuudet on tästä syystä pakko ottaa huomioon jo suunnitteluvaiheessa.
  - Pelkkä kybersuunnittelu ei riitä, vaan tarvitaan toteutuksen auditointeja ja mm. tunkeutumistestausta.
- Avainasemassa kyberturvallisuuden takaamiseksi on huolellinen suunnittelu, kestävät salausratkaisut (kvanttiteknologian mukaantulo) ja fyysisen turvallisuuden toimenpiteiden korostuminen erityisesti lähestyttäessä poikkeusoloja.
- Avaruusteknologian käyttö on kallista, mutta matalilla kiertoradoilla kiertävien mikro- ja piensatelliittien ansiosta ne tulevat entistä useampien ulottuville. Se lisää haavoittamismielessä palveluiden kiinnostavuutta.

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

- Hallitus esittää lainsäädäntöä EU:n data-asetuksen kansallisesta toimeenpanosta [9 & 10]
  - EU:n data-asetuksen soveltaminen on alkanut pääosin 12.9.2025. Data-asetus asettaa vaatimuksia erityisesti verkkoon liitettävien laitteiden valmistajille. Asetuksessa tarkoitettuja laitteita voivat olla esimerkiksi erilaiset sensorit ja älykellot.
  - Data-asetus luo tietoja keräävien laitteiden käyttäjille uusia oikeuksia. Yritykset ja kuluttajat voivat helpommin hallita ja hyödyntää omia tietojaan ja toimittaa dataa kolmannelle osapuolelle, esimerkiksi huoltoa tai lisäpalveluita tarjoavalle yritykselle. Pienempiä yrityksiä suojataan datan hyödyntämiseen ja jakamiseen liittyviltä epäreiluilta sopimusehdoilta. Etenkin yritysten kannalta asetus luo merkittävästi uusia edellytyksiä datan hyödyntämiselle.
  - Data-asetuksen myötä julkisilla toimijoilla on poikkeuksellisissa tilanteissa, esimerkiksi yleisissä hätätilanteissa, oikeus pyytää tietoja yksityiseltä sektorilta. Lisäksi asetus velvoittaa datankäsittelypalveluita, kuten pilvipalveluita, luomaan puitteet niiden helpommalle vaihtamiselle.
  - Hallitus antoi eduskunnalle data-asetusta täydentävää lainsäädäntöä koskevan lakiesityksen 25.9.2025. Hallituksen esityksessä ehdotetaan säädettäväksi uusi laki datan hallinnan ja jakamisen valvonnasta ja muutettavaksi eräitä muita lakeja. Uudessa laissa säädettäisiin toimivaltaisista viranomaisista ja niiden tehtävistä, Liikenne- ja viestintävirasto Traficomin valvontatoimivaltuuksista sekä seuraamuksista. Uuteen lakiin siirrettäisiin myös jo aiemmin säädetyt EU:n datanhallinta-asetuksen kansalliset toimeenpanosäännökset.
  - Uusia viranomaistehtäviä saisivat Traficom, Kilpailu- ja kuluttajavirasto ja kuluttaja-asiamies. Pääasiallisesti data-asetuksen noudattamista valvoisi Traficom. Traficom toimisi myös datakoordinaattorina, eli keskitettynä yhteyspisteenä asetuksen soveltamiseen liittyvissä asioissa Suomessa.
  - Lakien on tarkoitus tulla voimaan 1.1.2026.

Oikeudelliset asiat

- Lausuntokierros: Radiohäirintään tarkoitettujen laitteiden hallussapidosta tulossa rangaistavaa [11 & 12]
  - Liikenne- ja viestintäministeriö pyytää lausuntoja hallituksen esitysluonnoksesta koskien radiohäirintään tarkoitettuja radiolaitteita eli nk. jammereita koskevan lainsäädännön muuttamista. Muutokset tehtäisiin sähköisen viestinnän palveluista annettuun lakiin.
  - Esitysluonnoksessa ehdotetaan muutoksia sääntelyyn, joka koskee radiotaajuista viestintää häiritseviä tai väärentäviä laitteita. Radiotaajuista viestintää käyttävät esimerkiksi matkaviestinverkot ja satelliittipaikannusjärjestelmät, kuten GPS.
  - Jammereiden oikeudeton hallussapito kriminalisoitaisiin. Tällä hetkellä jammereita pidetään radiolähettiminä, joiden hallussapito on luvanvaraista. Esityksellä luotaisiin jammereille radiolähettimistä erillinen määritelmä, joka mahdollistaisi radiolähettimiä tiukemman sääntelyn. Jammereiden oikeudettoman hallussapidon kriminalisointi parantaisi muun muassa viranomaisten mahdollisuuksia puuttua laitteiden maahantuontiin.
  - Viranomaisten ja muiden oikeutettujen tahojen mahdollisuuksia käyttää laitteita tehtäviensä hoitamiseksi selvennettäisiin. Jatkossa jammereiden hallussapito ja käyttö tutkimusta ja tuotekehitystä varten olisi luvanvaraisesti sallittua, jos tietyt edellytykset täyttyvät. Lisäksi esitysluonnoksessa ehdotetaan muutoksia muun muassa Liikenne- ja viestintävirasto Traficomin tarkastusoikeuksiin.
  - Lausuntoja hallituksen esitysluonnoksesta voi antaa 29.10.2025 asti.
  - Laki on tarkoitus tulla voimaan 1.7.2026.

Oikeudelliset asiat

- Euroopan komissio on julkaissut uusia eIDAS-asetuksen täytäntöönpanoasetuksia [13-18]
  - Komissio on 30.9.2025 julkaissut EU:n virallisessa lehdessä kuusi uutta eIDAS-asetuksen täytäntöönpanoasetusta.
  - Täytäntöönpanoasetukset liittyvät hyväksyttyihin aikaleimoihin, sähköisten allekirjoitusten ja leimojen hyväksyttyihin varmenteisiin sekä niiden validointipalveluihin ja säilytyspalveluihin sekä hyväksyttyihin sähköisiin rekisteröityihin jakelupalveluihin.
  - Täytäntöönpanoasetukset tulevat voimaan 20.10.2025.

Oikeudelliset asiat

- S-Pankille 1,8 miljoonan euron seuraamusmaksu S-mobiilin tietoturvahaavoittuvuudesta [19 & 20]
  - Tietosuojavaltuutetun toimisto selvitti tietoturvaloukkausta S-Pankin elokuussa 2022 tekemän ilmoituksen perusteella. Pankki oli ottanut huhtikuussa 2022 käyttöön uuden kirjautumistoiminnallisuuden S-mobiilissa. Ohjelmistossa oli ilmennyt tietoturvahaavoittuvuus, joka oli ollut hyödynnettävissä yli kolmen kuukauden ajan huhtikuusta elokuuhun.
  - Haavoittuvuuden vuoksi osa pankin asiakkaista joutui tietoturvaloukkauksen kohteeksi. Pankkitunnusten väärinkäytökset aiheuttivat asiakkaille taloudellista vahinkoa. S-Pankki on ilmoittanut korvanneensa asiakkaille suorat menetykset.
  - Tietosuojavaltuutetun toimiston selvityksessä havaittiin, että S-Pankilla ei ollut käytössä riittäviä suojatoimia henkilötietojen turvallisuuden varmistamiseksi. Pankki ei ollut testannut uutta ohjelmistoa riittävästi ennen sen käyttöönottoa, eikä se ollut havainnut haavoittuvuutta ennen kuin toiminnallisuus otettiin käyttöön. Se ei myöskään reagoinut riittävällä tavalla asiakkaidensa yhteydenottoihin, joissa ilmoitettiin poikkeamista verkkopankin kirjautumisessa. S-pankin toiminta rikkoi EU:n tietosuoja-asetuksen vaatimuksia henkilötietojen turvallisesta käsittelystä.
  - Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi pankille 1,8 miljoonan euron seuraamusmaksun ja apulaistietosuojavaltuutettu antoi huomautuksen tietosuojalainsäädännön vastaisesta menettelystä. Seuraamuskollegio piti seuraamusmaksun määräämistä tietosuojarikkomuksesta välttämättömänä ihmisten oikeussuojan tarpeen, asian yleisen merkittävyyden sekä tietosuojavaltuutetun S-Pankille aiemmin antaman huomautuksen vuoksi. Seuraamuskollegio otti seuraamusmaksun määräämisessä huomioon myös Finanssivalvonnan 23.5.2025 antaman päätöksen ja kohtuullisti seuraamusmaksun määrää sen perusteella.
  - Päätös ei ole vielä lainvoimainen ja siitä voi valittaa hallinto-oikeuteen.

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) Huijauspuheluiden estotoiminta voitti rikoksentorjuntakilpailun 2025 https://valtioneuvosto.fi/-/1410853/huijauspuheluiden-estotoiminta-voitti-rikoksentorjuntakilpailun-2025
2) Exclusive: US warns hidden radios may be embedded in solar-powered highway infrastructure https://www.reuters.com/legal/government/us-warns-hidden-radios-may-be-embedded-solar-powered-highway-infrastructure-2025-09-10/
3) Kyberkestävyyssäädös (Cyber Resilience Act, CRA) https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra
4) The DDoS you knew is not the DDoS we're seeing now https://www.nokia.com/blog/the-ddos-you-knew-is-not-the-ddos-were-seeing-now/
5) Microsoft 365 -tilejä murretaan – varo tietojenkalastelua https://kyberturvallisuuskeskus.fi/fi/varoitus_1/2025
6) Ennakointi on paras puolustus palvelunestohyökkäyksiä vastaan https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ennakointi-paras-puolustus-palvelunestohyokkayksia-vastaan
7) Collins Aerospace working on restoring software for airlines hit by cyberattack https://www.reuters.com/business/aerospace-defense/collins-aerospace-working-restoring-software-airlines-hit-by-cyber-attack-2025-09-24/
8) Kyberhyökkäys viivästyttää lentoja Euroopan lentokentillä – Brysselin lentoasema peruu puolet sunnuntain lennoista https://yle.fi/a/74-20184054
9) Hallitus esittää lainsäädäntöä EU:n data-asetuksen kansallisesta toimeenpanosta https://lvm.fi/-/hallitus-esittaa-lainsaadantoa-eu-n-data-asetuksen-kansallisesta-toimeenpanosta
10) Tietoa data-asetuksesta https://traficom.fi/fi/viestinta/datatalous-ja-digipalvelut/tietoa-data-asetuksesta
11) Lausuntokierros: Jammereiden luvattomasta hallussapidosta tulisi rangaistavaa https://lvm.fi/-/lausuntokierros-jammereiden-luvattomasta-hallussapidosta-tulisi-rangaistavaa
12) Hallituksen esitys laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta (radiohäirintään tarkoitetut laitteet) https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=0be82d3e-d5cd-4fb1-a568-b02ee2a61b80
13) Commission Implementing Regulation (EU) 2025/1929 of 29 September 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501929
14) Commission Implementing Regulation (EU) 2025/1942 of 29 September 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501942
15) Commission Implementing Regulation (EU) 2025/1943 of 29 September 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501943
16) Commission Implementing Regulation (EU) 2025/1944 of 29 September 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501944
17) Commission Implementing Regulation (EU) 2025/1945 of 29 September 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501945
18) Commission Implementing Regulation (EU) 2025/1946 of 29 September 2025 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501946
19) S-Pankille seuraamusmaksu S-mobiilin tietoturvahaavoittuvuudesta https://tietosuoja.fi/-/s-pankille-seuraamusmaksu-s-mobiilin-tietoturvahaavoittuvuudesta
20) Tietoturvallisuuden laiminlyönti pankin tunnistuspalvelussa https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2025/2479