TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 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

INTERPOLin koordinoimassa viranomaisoperaatiossa puututtiin kyberrikollisuuteen eri puolilla Afrikkaa. Kansainvälisessä yhteisoperaatiossa pidätettiin yhteensä 1209 kyberrikoksista epäiltyä henkilöä ja takavarikoitiin huomattava määrä rikollisten käyttämää infrastruktuuria. [1]

Kyberturvallisuuskeskukselle ilmoitettujen Microsoft 365 -tietomurtoilmoitusten määrä kolminkertaistui heinäkuuhun verrattuna. Kasvaneiden ilmoitusmäärien taustalla vaikuttaa pääasiassa kesälomakauden päättyminen, mutta kasvu on ollut aiempiin vuosiin nähden poikkeuksellisen voimakasta etenkin M365:n osalta.

Kybersää elokuu 2025

Tietomurrot ja -vuodot

- Tietomurtojen tapausmäärät nousivat yli kolminkertaisiksi hiljaisen heinäkuun jälkeen. Tapausmäärät ovat tyypillisesti nousseet alkusyksystä, työntekijöiden palatessa työpaikoille.
- Useissa tapauksissa murtojen tausalla oli edelleen onnistunut M365-jatkokalastelu, jolloin linkki haitalliseen sisältöön saapui tutulta lähettäjältä.
- Myös Teams-puhelut ovat yleistyneet tietomurtojen juurisyynä elokuussa. [2]

Huijaukset ja kalastelut

- Lastensuojelun nimissä tehdyillä tekstiviestihuijauksilla on saatu huomattavaa rikoshyötyä. Menetykset kansalaisilta ja organisaatioilta ylsivät elokuussa satoihin tuhansiin euroihin.
- Rikolliset käyttävät huijauksiin sähköpostin, tekstiviestien ja puheluiden lisäksi nyt myös Microsoft Teams -puheluita. IT-tukena esiintyvät huijarit yrittävät saada uhrin asentamaan etähallintaohjelmiston laitteelleen.

Haittaohjelmat ja haavoittuvuudet

- Citrix Netscaler ADC ja NetScaler Gateway -tuotteiden kriittistä haavoittuvuutta käytetään aktiivisesti hyväksi.
- Suomessa ja maailmalla on havaittu PDF-editoriksi naamioitua haittaohjelmaa. Ohjelmia ladatessa on hyvä huomioida sekä ladattavan ohjelman että verkkosivun luotettavuus.
- Maailmalla on raportoitu ensimmäisestä tekoälypohjaisesta kiristyshaittaohjelmasta. Haittaohjelma voi kirjoittaa tekoälyllä haitallista koodia saastuneessa laitteessa, mikä hankaloittaa sen tunnistamista ja havaitsemista.

Automaatio ja IoT

- Puolassa pienen sähköä tuottavan padon huonosti suojattu etähallintajärjestelmä joutui väärinkäytösten kohteeksi. Ukrainassa puolestaan Internetiin avoimesti näkyvät verkkokamerat ja päivittämättömät IoT-laitteet altistuivat väärinkäytöksille. [3 & 4]
- Tapaukset muistuttavat perusasioiden tärkeydestä IoT- ja automaatiojärjestelmien suojaamisessa.

Verkkojen toimivuus

- Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä vaikutuksia suomalaisiin verkkopalveluihin.
- Maailmalla raportoidaan kuitenkin jatkuvasti ennätyksellisen suurista palvelunestohyökkäyksistä. [5]

Vakoilu

- Viranomaiset useista maista varoittivat Kiinaan liitetyn APT-ryhmä toteuttamasta kybervakoilusta, jonka kohteina ovat mm. teleoperaattorit ja internetpalveluntarjoajat.
- Ryhmästä on julkisuudessa käytetty esimerkiksi nimiä Salt Typhoon, Operator Panda ja Ghost Emperor.
- Myös Suojelupoliisi Suomesta osallistui julkaisuun.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Rahoitustukihaku kyberturvallisuuslain toimeenpanemisen tukemiseksi avattiin elokuussa. Liikenne- ja viestintävirasto Traficom voi myöntää soveltamisalaan kuuluville mikrokokoisille, pienille ja keskisuurille organisaatioille kyberturvallisuuslaissa asetettujen vaatimusten toteuttamiseksi ja toimijoiden kyberturvallisuustason nostamiseksi organisaatiossa. Haku on auki 16.10.2025 klo 16:15 asti. [6]

Traficom julkaisi yhdessä Suojelupoliisin kanssa tiedotteen Suomen kyberturvallisuuden uhkatasosta. Uhkataso nousi Ukrainan sodan myötä vuona 2022 ja on säilynyt kohonneella tasolla. Kyberturvallisuuskeskuksen selvittämien vakavien tapausten määrä onkin yli kaksinkertaistunut viime vuoteen verrattuna. [7]

EU:n radiolaitteita koskevia tietoturvavaatimuksia alettiin soveltamaan elokuun alussa. Sääntelyn piiriin kuuluvat radiotaajuuksia hyödyntävät laitteet, kuten esimerkiksi puhelimet, älykellot ja itkuhälyttimet. Uudet pelisäännöt parantavat kuluttajien tietoturvaa, koska jatkossa EU:n markkinoille saa tuoda vain tietoturvavaatimukset täyttäviä radiolaitteita. [8]

Elokuun kyberturvallisuuden yleiskuva

Elokuu toi mukanaan päätöksen rauhalliselle kesäkaudelle. Kesälomien loppuminen ja paluu työpaikoille näkyivät selvänä tapausmäärien kasvuna sekä paluuna arkeen KTK:n vastaanottamien ilmoitusten lukumäärissä.

- Elokuun merkittäviä ilmiöitä olivat muun muassa haavoittuvuudet ja tietomurrot, jotka korostuivat myös kyberturvallisuuteen liittyvässä kansainvälisessä uutisoinnissa. Heinä-elokuussa vaivannut globaali SharePoint-haavoittuvuus aiheutti huolta myös Suomessa, mutta onnistuneet hyväksikäyttötapaukset ovat jääneet määrältään melko vähäisiksi. Patoihin kohdistuneet kyberhyökkäykset Norjassa ja Puolassa korostavat turvallisuusnäkökulmien huomioimista ja haavoittuvien järjestelmien suojaamista – alaan sekä kohteeseen katsomatta. [3 & 9]

Elokuussa vastaanotettujen tietomurtoilmoitusten kokonaismäärä saavutti kuluvan vuoden huipun. Useiden onnistuneiden tietomurtotapausten johdosta myös syyskuussa voidaan odottaa runsaasti havaintoja tietojenkalastelusta ja tietomurtojen yrityksistä.

- Osassa Suomessa havaituista tietomurtotapauksista on käytetty monivaiheisen tunnistautumisen kiertävää Adversary-in-the-Middle (AiTM) -tekniikkaa. Hyökkäyksessä kaappauksen yhteydessä saatetaan esimerkiksi luoda sähköpostitilille sääntö, joka siirtää postilaatikkoon tulevat viestit suoraan poistetut tai arkistot-kansioon ja merkitsee ne luetuksi. Uudelleenohjaussääntöjen avulla rikollinen pyrkii pitämään käyttäjältä piilossa ilmoitukset ja kyselyt tililtä lähetetyistä jatkoviesteistä. [10]

Tietojenkalastelu on ollut koko kesäkauden ajan merkittävä uhka. Elokuu ei tehnyt poikkeusta trendiin, ja kasvua havaittiin etenkin Microsoft 365 -tunnuksiin kohdistuvassa kalastelussa. Tietojenkalasteluun liittyvien ilmoitusten kokonaismäärä vaikuttaa kuitenkin tasaantuneen kesän voimakkaasta nousutrendistä.

- KTK vastaanotti useita ilmoituksia kalastelutapauksista, joissa viesti on tullut ilmoittajalle tutulta taholta. Kalasteluviestin otsikossa voidaan viitata esimerkiksi jaettuun tiedostoon. Viestin linkki johtaa usein organisaation Online SharePoint- tai OneDrive-palvelusta jaettuun dokumenttiin. Varsinainen kalastelulinkki on kuitenkin jaettuun dokumenttiin upotettu uusi linkki, joka vie Microsoft 365 -tunnusten kalastelusivulle. [11]

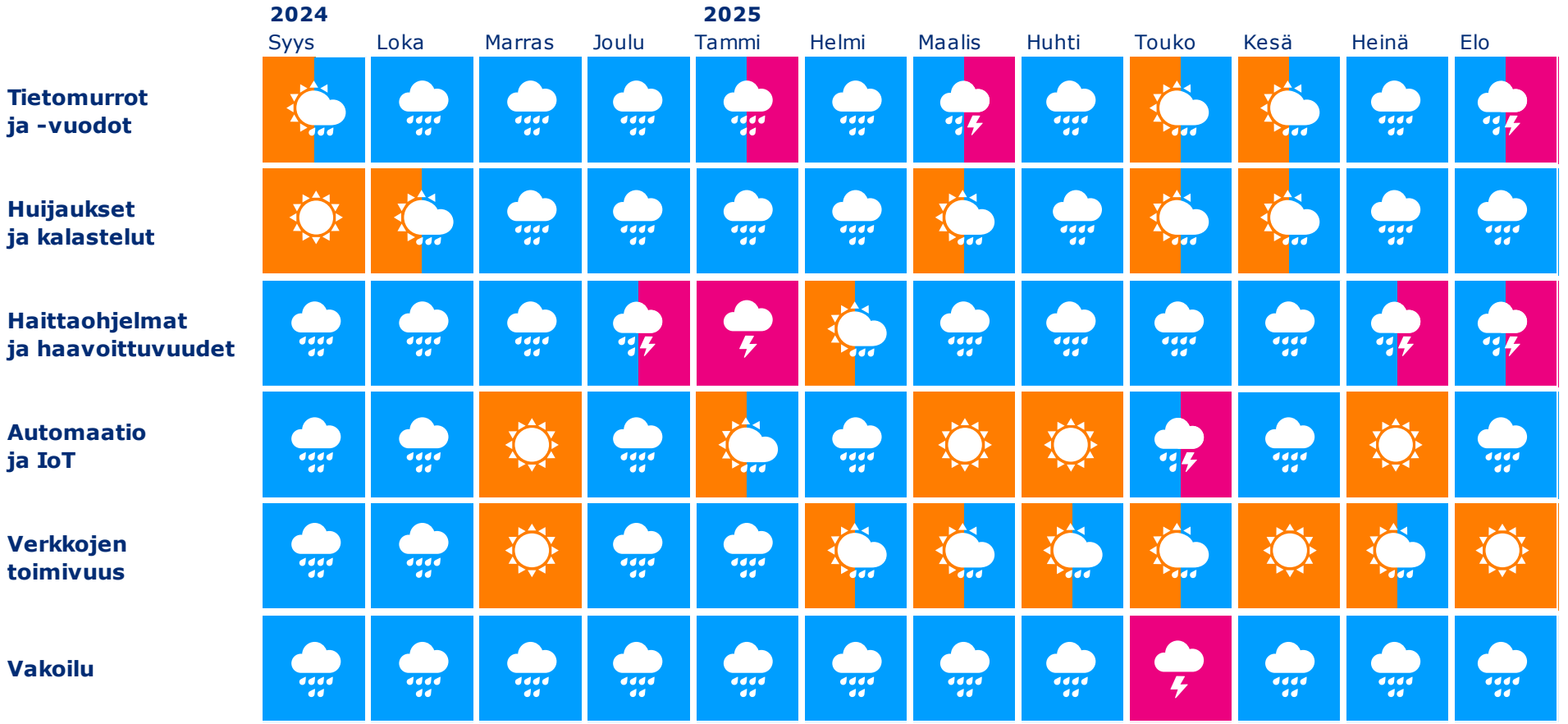
- Lomakauden päätyttyä on syytä muistuttaa henkilöstöä tietojenkalastelun vaarasta. Syksyn kynnyksellä on hyvä käydä läpi muun muassa yhteiset pelisäännöt, sekä erilaisia tapoja tunnistaa mahdollisia tietojenkalasteluviestejä ja huijausyrityksiä. Esimerkiksi linkkien ja verkko-osoitteiden tarkastaminen on yksinkertainen, mutta tärkeä taito monelta uhkalta välttymiselle. [11] KTK on julkaissut ohjeita mm. AiTM-kalastelu tunnistamiseen [10]

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

1 kk



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: Verkkojen turvallisuus

Verkkojen turvallisuuteen liittyvät merkittävät poikkeamat ovat harvinaisia, mutta muun muassa palvelunestohyökkäykset ovat jatkuva uhka. Internetin toimintaperiaatteiden vuoksi palvelunestohyökkäyksiä ei voida tulevaisuudessakaan kokonaan estää.

- Palvelunestohyökkäysten suojausmekanismeja tarjoavat yritykset raportoivat tasaisesti havaitsemistaan ennätyksellisen suurista palvelunestohyökkäyksistä. [12]
  - Vaikka merkittäviä häiriötilanteita syntyy harvoin, on jatkuvilla palvelunestohyökkäyksillä taloudellisia ja yhteiskunnallisia vaikutuksia. Hyökkäyksillä pyritään kuluttamaan yhteiskunnan voimavaroja ja heikentämään luottamusta digitaalisiin palveluihin. [13]
- Kyberrikollisuuden teollistuminen on synnyttänyt erikoistuneen DDoS-as-a-Service -ekosysteemin, jossa hyökkäykset ovat muuttuneet helposti saataviksi kuluttajapalveluiksi.
  - Vaikka kansainväliset poliisioperaatiot onnistuvat lamauttamaan näitä palveluja, kokonaisuutena rikolliset markkinat mukautuvat ja palautuvat nopeasti. [14] Rikollisille tarjottuja palveluita myös kehitetään yhä ammattimaisemmiksi ja helpommiksi käyttää.
- Palvelunestohyökkäyksissä käytetään laajoja bottiverkkoja, jotka koostuvat haittaohjelmilla saastutetuista tavallisten ihmisten laitteista ympäri maailmaa.
  - Toistaiseksi koko maailman väestöstä vain 68 % käyttää internetiä, mutta käyttäjien määrä kasvaa koko ajan. [15] Tulevaisuudessa se todennäköisesti tarkoittaa entistä enemmän huonosti suojattuja internetiin kytkettyjä laitteita, joita rikolliset pyrkivät kaappaamaan osaksi bottiverkkojaan.
  - Heikosti suojatuista kuluttajaverkkolaitteista koostuvia bottiverkkoja hyödynnetään aktiivisesti myös kybervakoiluun. [16]

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

EU:n tekoälyasetuksen osittainen soveltaminen alkoi elokuun alussa [17 & 18]

- EU:n tekoälyasetuksen tarkoituksena on varmistaa, että EU:n alueella markkinoille tuotavat ja käyttöönotettavat tekoälyjärjestelmät eivät vaaranna ihmisten terveyttä, turvallisuutta tai perusoikeuksia.
- Asetuksessa säädellään tekoälyjärjestelmiä niiden aiheuttamien riskien perusteella. Erittäin haitalliset tekoälyn käyttötavat kielletään ja tietyille korkeariskisiksi luokiteltaville tekoälyjärjestelmille asetetaan tiukennettuja vaatimuksia.
- Tekoälyasetus tuli voimaan 2.8.2024, ja sen soveltaminen alkaa vaiheittain. Asetuksen säännöksiä muun ohella yleiskäyttöisistä tekoälymalleista on alettu soveltaa EU-maissa 2.8.2025 alkaen. Yleiskäyttöisiä tekoälymalleja ovat esimerkiksi laajat generatiiviset tekoälymallit.
- Tekoälyasetus on lähtökohtaisesti suoraan sovellettavaa oikeutta, mutta edellyttää täydentävää kansallista lainsäädäntöä.
- Hallituksen esitys täydentäväksi kansalliseksi lainsäädännöksi EU:n tekoälyasetuksen täytäntöönpanemiseksi (HE 46/2025 vp) on annettu eduskunnalle 8.5.2025, mutta esityksen käsittely on edelleen kesken eduskunnassa, minkä vuoksi kansallisten viranomaisten tehtäviin, ilmoitettujen laitosten nimeämiseen ja seuraamuksiin liittyvä kansallinen lainsäädäntö ei tule voimaan vielä 2.8.2025 alkaen.

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) African authorities dismantle massive cybercrime and fraud networks, recover millions https://www.interpol.int/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions
2) IT-tukena esiintyvät hyökkääjät lähestyvät organisaatioita Teams-puheluilla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/it-tukena-esiintyvat-hyokkaajat-lahestyvat-organisaatioita-teams-puheluilla
3) Russian Hackers Breach Polish Hydropower Plant in Major Cyberattack https://united24media.com/latest-news/russian-hackers-breach-polish-hydropower-plant-in-major-cyberattack-10882
4) The Resurgence of IoT Malware: Inside the Mirai-Based Botnet Campaign https://www.fortinet.com/blog/threat-research/iot-malware-gayfemboy-mirai-based-botnet-campaign
5) Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/
6) Rahoitustukihaku kyberturvallisuuslain toimeenpanemisen tukemiseksi avattu https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/rahoitustukihaku-kyberturvallisuuslain-toimeenpanemisen-tukemiseksi-avattu
7) Traficom ja Supo: Kyberturvallisuuden uhkataso pysynyt koholla - vakavien tapausten määrät kasvussa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-ja-supo-kyberturvallisuuden-uhkataso-pysynyt-koholla-vakavien-tapausten
8) Älykellot, itkuhälyttimet ja puhelimet yhä turvallisempia – EU kiristää tietoturvavaatimuksia https://traficom.fi/fi/ajankohtaista/alykellot-itkuhalyttimet-ja-puhelimet-yha-turvallisempia-eu-kiristaa
9) Norway spy chief blames Russian hackers for dam sabotage in April https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
10) AiTM (adversary-in-the-middle) -hyökkäykset ja niiden torjunta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-tietoturva-ammattilaisille/aitm-adversary-middle
11) Kyberturvallisuuskeskuksen viikkokatsaus - 33/2025 https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-332025
12) https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/
13) Estimating the Societal Cost of DDoS Attacks: A Dual-Lens Model for National Impact Assessment https://thegfce.org/wp-content/uploads/2025/08/Societal-Cost-DDoS-Attacks-Carlos-Alvarez.pdf
14) Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services https://www.usenix.org/conference/usenixsecurity25/presentation/vu
15) International Telecommunication Union – Statistics https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx
16) Kyberturvallisuuden uhkataso pysynyt koholla – vakavien tapausten määrät kasvussa https://supo.fi/-/kyberturvallisuuden-uhkataso-pysynyt-koholla-vakavien-tapausten-maarat-kasvussa
17) EU:n tekoälyasetuksen kansallinen toimeenpano https://tem.fi/tekoalyasetus
18) EU:n tekoälyasetuksen kansallisen toimeenpanon työryhmä https://tem.fi/hanke?tunnus=TEM044:00/2024