TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 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

70

Suomalaiset menettivät vuonna 2024 verkkohuijauksissa yli 84 miljoonaa euroa, mikä on **70 %** suurempi summa kuin edellisenä vuonna.[1]

2024

Kyberturvallisuuskeskuksen vuosikatsaus Kyberturvallisuuden vuosi 2024 on julkaistu. Aiemmin pdf-muotoisena julkaistu tuote on nyt verkkosivuilla.[2]

3350

Traficomin ja Huoltovarmuuskeskuksen järjestämä Tietoturva 2025 – seminaari keräsi kaikkien aikojen ennätysyleisön, 3350 osallistujaa Suomesta ja ulkomailta.[3]

Kybersää maaliskuu 2025

Tietomurrot ja -vuodot

- Akira-tapauksissa on alkuvuoden aikana ollut kasvua. Hyökkäyksissä hyödynnetään edelleen sisäänmenovektorina verkon reunalaitteita ja puuttuvaa MFA:ta.
- Murretuilta M365-tileiltä lähetettiin laskutushuijauksia, joiden uskottavuutta lisättiin rekisteröimällä uhrin verkkotunnusta muistuttava domain (typosquatting).

Huijaukset ja kalastelut

- Kyberturvallisuuskeskuksen uusi ohje auttaa varomaan huijareita verkossa ja puhelimessa.
- Verotusteemaa on käytetty pankkitunnuskalasteluihin maaliskuussa varsin paljon.
- Sosiaalisen median tilejä kaapataan taas kysymällä pikaviestillä puhelinnumeroa ja sen jälkeen muka ”arvontakoodia”.

Haittaohjelmat ja haavoittuvuudet

- Havaintoja kiristyshaittaohjelmatartunnoista maaliskuun aikana, erityisesti Akira-haittaohjelma korostui ilmoituksissa. Hyökkäyksissä on hyödynnetty haavoittuvia verkon reunalaitteita.
- Verkon reunalaitteiden päivitykset on suositeltavaa asentaa aina viipymättä.

Automaatio ja IoT

- Japani on julkaissut oman tietoturvamerkkinsä IoT-laitteille.[4]
- Eurooppalaiset standardointijärjestöt ovat hyväksyneet komission kyberkestävyyssäädöksen (CRA) standardointipyynnön ja työ on käynnistynyt.

Verkkojen toimivuus

- Maaliskuussa yleisissä viestintäverkoissa ei havaittu toimivuushäiriöitä.
- Ostettavat DDOS-palvelut yleistyvät palvelunestohyökkäysten toteutuksissa. Esimerkiksi Mirai-pohjaista GorillaBot bottiverkkoa [5] on käytetty hyökkäyksissä suomalaisiin kohteisiin.

Vakoilu

- Kiinalaiset APT-ryhmät hyödyntävät IT-toimitusketjuja sekä etäkäyttö- ja hallintatyökaluja ja näiden haavoittuvuuksia organisaatioihin murtautumisessa.[6]
- Ukrainaan ja sen toimitusketjuihin kohdistuvat kyberhyökkäykset jatkuivat aktiivisina. Kohteina ovat mm. logistiikka- ja puolustussektori sekä valtionhallinto.[7]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberturvallisuuskeskus on julkaissut 27.3. organisaatioille suunnatun kriisiviestintäohjeen, jossa kerrotaan erilaisista kyberhyökkäyksistä sekä rikollisten käyttämistä menetelmistä ja keinoista. Ohjeessa annetaan vinkkejä viestinnälliseen varautumiseen sekä viestintään kyberhyökkäysten aikana ja jälkeen.[8]

Microsoft tuo jatkuvasti pilvipalveluihinsa uusia päivityksiä. Tilausten asetukset tarkistetaan mielellään puolen vuoden välein Microsoft 365 -tilauksen Entra ID:n (aiemmin Azure Active Directory) asetuksista, ellei organisaation Microsoft 365 -tilauksen päivityksiä muuten seurata jatkuvasti. Kyberturvallisuuskeskus on luonut ohjeen, jossa käsitellään Entra ID:n hakemiston ja käyttäjän hallintaan liittyviä asetuksia.[9]

Kyberturvallisuuskeskus on päivittänyt neuvoja salasanan hallintasovelluksen käyttöönottoon.[10]

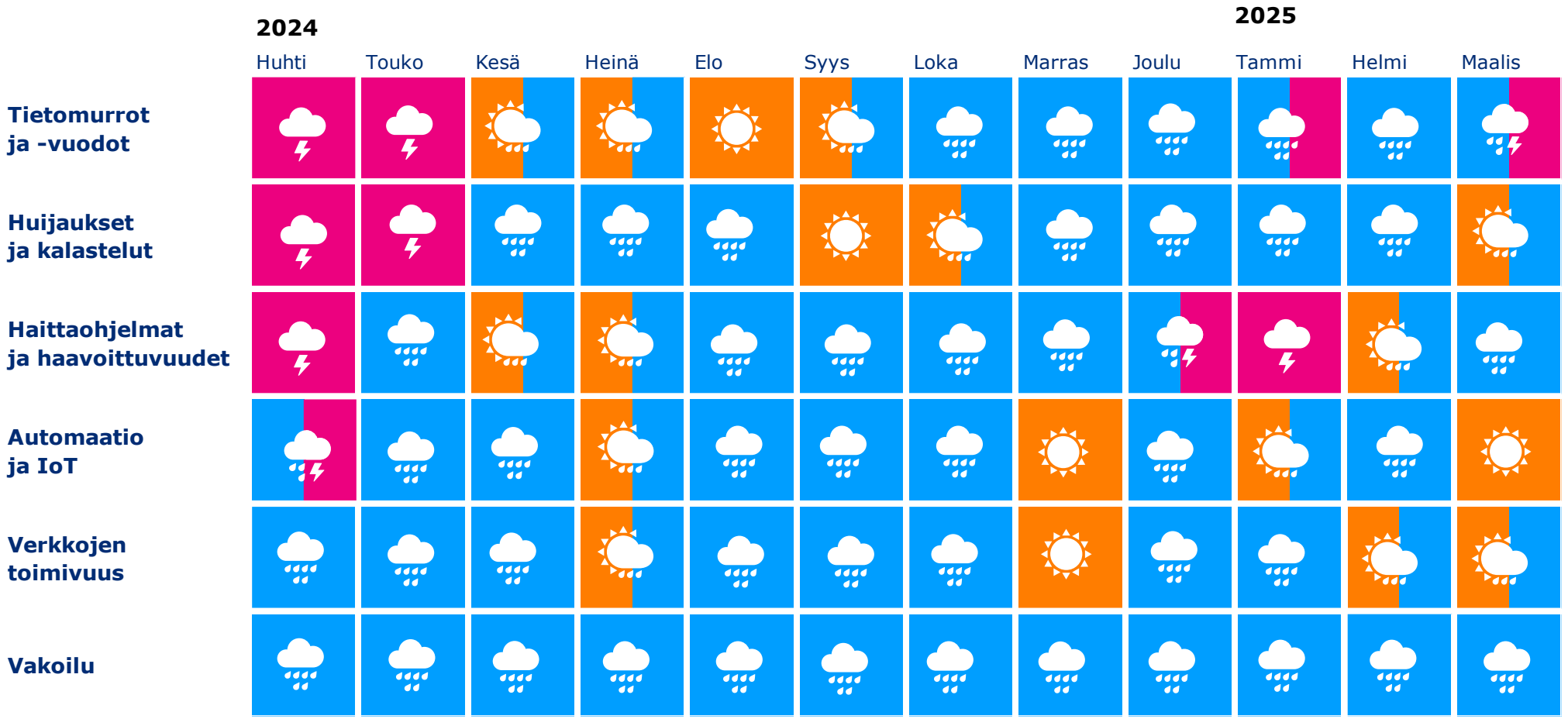
Maaliskuun kyberturvallisuuden yleiskuva

- Maaliskuussa on tullut ilmoituksia verkon reunalaitteiden haavoittuvuuksien hyväksikäytöstä. Verkon reunalaitteiden haavoittuvuudet ovat merkittävä sisäänpääsyvektori ja siksi kyseiset laitteet tulisi pitää päivitettyinä.
  - Useat kansainväliset tietoturvaviranomaiset ovat varoittaneet mm. Fortinetin laajasti käytössä olevien palomuurituotteiden haavoittuvuuksista. Esimerkiksi Yhdysvaltain kyberturvallisuusvirasto CISA lisäsi Fortinetin alkuvuonna julkistetun haavoittuvuuden CVE-2025-24472 hyväksikäytettyjen haavoittuvuuksien luetteloon.[11] Haavoittuvuuksia on hyväksikäytetty esimerkiksi kiristyshaittaohjelmien levittämisessä. Hyökkäykset kohdistuvat erityisesti palomuurilaitteiden hallintaliittymiin.
  - Myös Kyberturvallisuuskeskuksen vastaanottamissa ilmoituksissa ovat korostuneet Fortinetin verkkolaitteet. Fortinetin verkkolaitteiden käyttäjiä suositellaan tarkistamaan ja estämään laitteidensa hallintakäyttöliittymän näkymisen julkisiin verkkoihin heti, sekä varmistamaan että laitteiden päivitykset ovat ajantasalla.[12]
- Erilaiset huijaukset ovat jatkuneet.
  - Kyberturvallisuuskeskukselle on ilmoitettu esimerkiksi huijauspuheluista Kyberturvallisuuskeskuksen nimissä, pankkikalastelusta verottajan nimissä, huijausviesteistä S-pankin nimissä, Neste-teemaisesta huijauksesta, sekä tietojenkalastelusta Postin nimissä.
  - Myös Facebook-tunnuksia kaapataan edelleen siten, että Messengerissä lähetetään huijausviestejä, joissa pyritään kaappaamaan tili puhelinnumeron ja vahvistuskoodin avulla.
  - Näin tunnistat aidot verkkosivut ja viranomaiset – vältä huijaukset verkossa . https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille/nain-tunnistat-aidot
- Useita AiTM-tekniikalla toteutettuja M365-tietomurtoja on raportoitu monilla toimialoilla. Tileiltä on useissa tapauksissa pyritty lähettämään jatkoviestejä.
  - Kyberturvallisuuskeskuksen AiTM-ohjeeseen pääset tutustumaan täällä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-tietoturva-ammattilaisille/aitm-adversary-middle

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

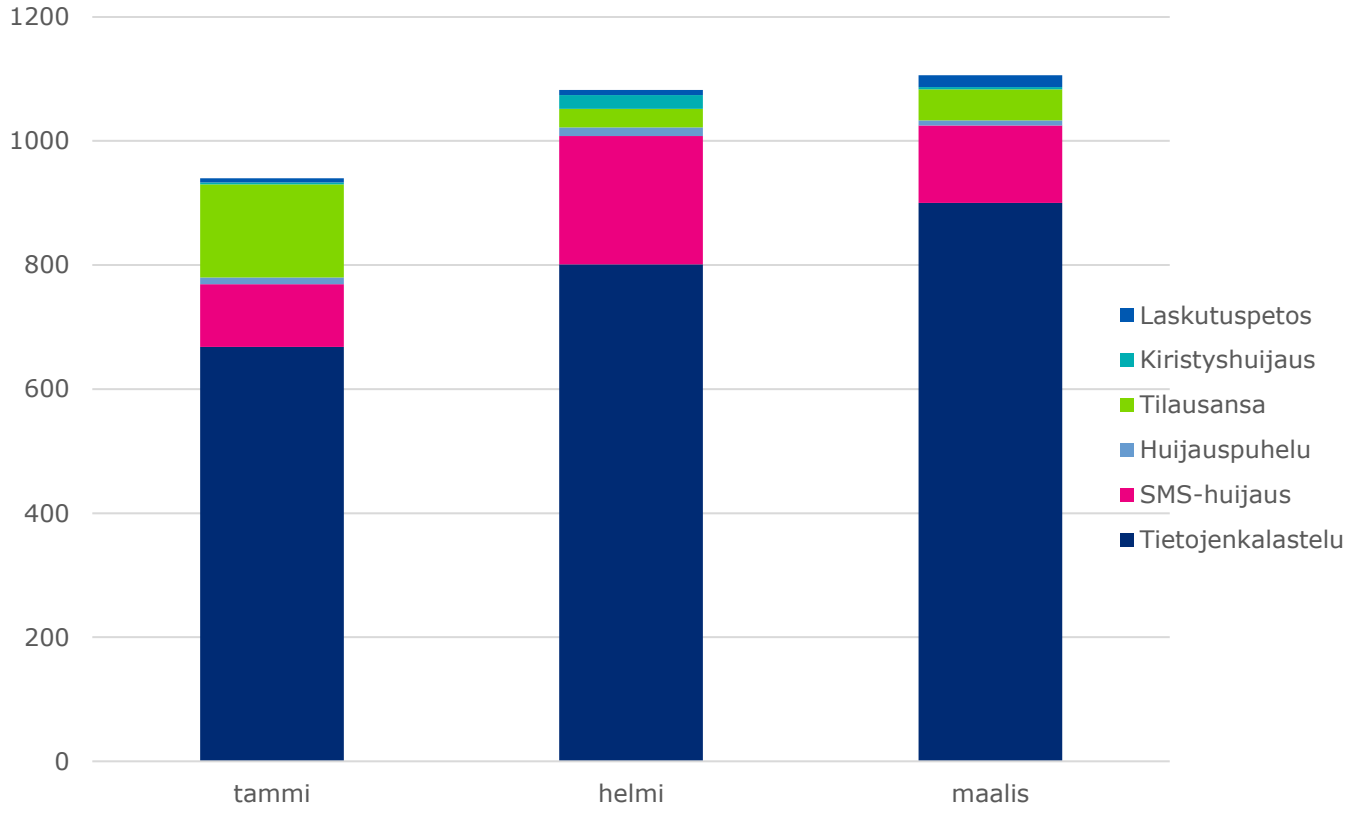


3 kk

Käsiteltyjä huijaustapauksia
Q1/2025

Vuoden 2025 ensimmäisen neljänneksen ilmiöitä ovat:

- Pankkitunnusten kalasteluun käytetään kalastelusivujen lisäksi entistä enemmän tekstiviestejä ja puheluita.
- Nettihuijausten kokonaismäärä on ollut vuoden alusta jälleen kasvussa.
- Huijauksiin käytetään kaikkia viestivälineitä sähköposteista ja tekstiviesteistä pikaviestimiin ja puheluihin.

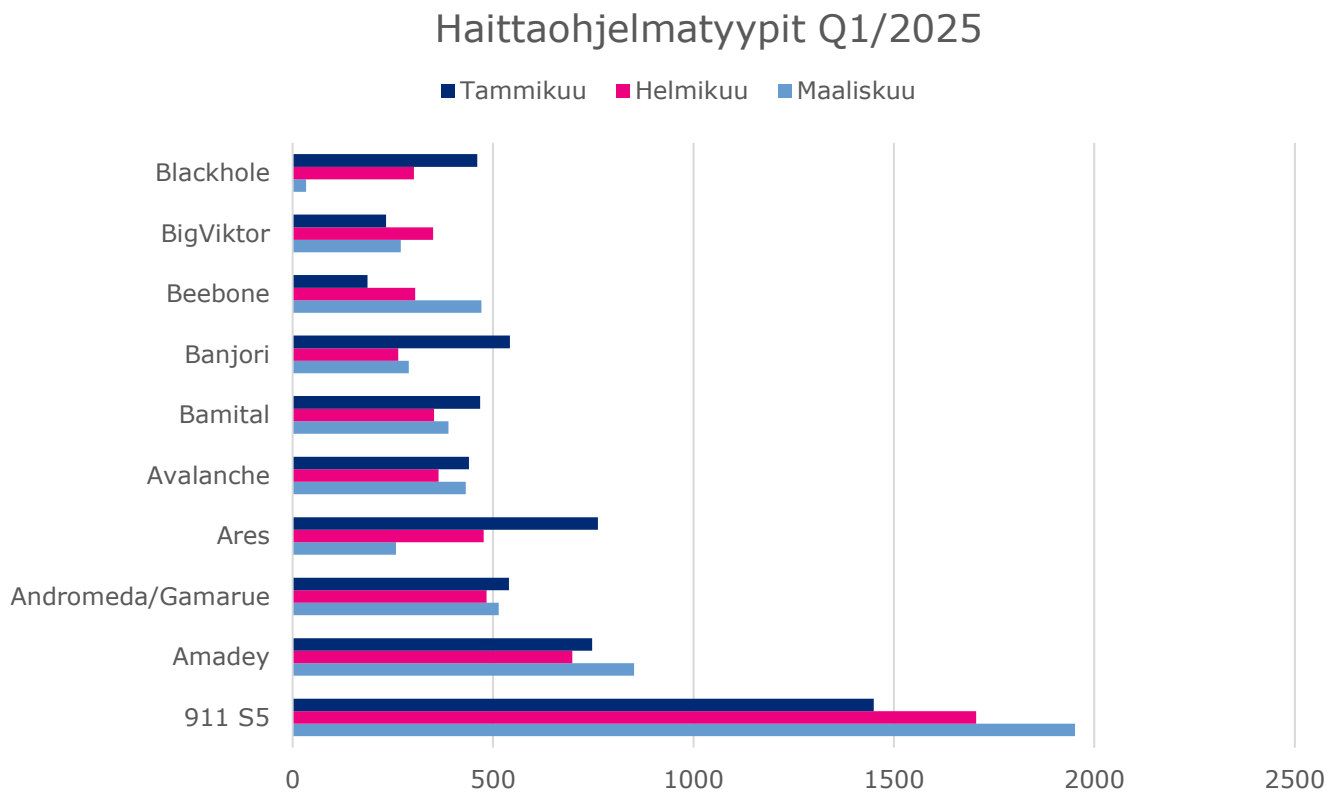


3 kk

Autoreporterin haittaohjelmahavainnot

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



3 kk

Toimialakohtaiset havainnot

Energia		Varautumiseen panostetaan aiempaa enemmän. Yhteistyökumppaneiden sähköpostitileihin kohdistuneet tietomurrot johtivat sektorilla havaittuihin kalasteluviesteihin ja joissakin tapauksissa onnistuneisiin laskutushuijauksiin. Energiavirasto on maaliskuussa ilmoittanut kyberturvallisuusverkkosäännön (NCCS) piiriin kuuluville ehdokkaille näiden yksilöinnistä.
Finanssi		Palvelunestohyökkäykset hieman lisääntyneet. Aktiivisimpana toimijoina Gorillabot ja Noname. Hyökkäyksillä ei kuitenkaan merkittäviä vaikutuksia palveluiden toimintaan. Uutena havaintona mobillivarmenteen hyväksikäyttöön liittyvien huijausten lisääntyminen.
Teollisuus		Tarkastelujaksolla etenkin raportoitujen tietomurtojen määrä on kasvanut merkittävästi, yli puolella edelliseen jaksoon verrattuna. Myös kiristyshaittaohjelmatapaukset lisääntyivät.
Logistiikka ja liikenne		Tarkastujaksolla poikkeamia raportoitiin enemmän kuin edellisellä jaksolla. Raportoitiin palvelunestohyökkäyksistä, joilla ei ollut vaikutuksia tai joiden vaikutukset saatiin rajattua. Lisäksi havaintoja M365-sähköpostitilimurtoihin johtaneista tietojenkalastelusta, huijauskampanjoista, kirjautumisyrityksistä VPN-palveluihin sekä brute force -hyökkäysyrityksistä. Lisäksi organisaatioiden nimissä huijauksia ja tietojenkalastelua.
Valtion-hallinto		Tarkastelujaksolla oli runsaasti tapahtumia, mutta tietoon ei tullut erityisen vakavia poikkeamia. Nähtiin erityyppisiä ja eri toimijoiden toteuttamia palvelunestohyökkäyksiä, joilla ei kuitenkaan ollut merkittäviä vaikutuksia. Lisäksi organisaatioihin kohdistui tietojen kalastelua, tiedonkeruuta ja laskutushuijausyrityksiä. Myös työntekijöiden nimissä olevista sosiaalisen median valetileistä raportoitiin.
Media		Kiristyshaittaohjelmahyökkäys alan organisaatioon.
SOTE		Kyberturvallisuuden poikkeamien määrä väheni noin neljänneksellä, mutta vakavien poikkeamien määrä kasvoi. Vakavin tapaus oli uutisiinkin päätynyt tietomurto Pharmadatan järjestelmiin. Yleisimpiä poikkeamien tyyppejä olivat pankkitunnusten kalastelu, muiden käyttäjätunnusten kalastelu ja tietomurto (yleensä kalastellulla käyttäjätunnuksella).
Vesihuolto		Ilmoitettujen poikkeaminen määrässä oli laskua edelliseen tarkastelujaksoon verrattuna.
Kunnat		Kuntaorganisaatioihin kohdistui mm. laskutushuijausteemaista kalastelua. Kuntayhtymän tietoverkkoon kohdistui ulkoisesta haittaohjelmasta johtunut tietoturvaloukkaus, jolla oli vaikutuksia organisaation tietojärjestelmien toimintaan. Suomalaisia kuntia kohtaan tehtiin myös palvelunestohyökkäyksiä venäjämielisten haktivistien toimesta.
Kiinteistö ja rakennus		Edellisen vuosineljänneksen tapaan tarkasteltavalla jaksolla ollut Dropbox-teemaisia M365-tilimurtoja. Alan organisaatioihin myös kohdistunut onnistuneita pankkitunnusten kalasteluja, jotka ovat johtaneet rahallisiin menetyksiin. Määrällisesti ajanjaksolla on ollut kuitenkin keskimääräistä vähemmän tapahtumia.

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: Kyberrikollisuuden kehittyminen: Kyberrikollisuuden näkymiä Euroopasta

- Kiristyshaittaohjelmat, tietojenkalastelu ja tietomurrot muodostivat vuonna 2024 valtaosan Euroopan Unionin (EU) alueella havaituista rikollisiin motiiveihin yhdistetyistä kyberhyökkäyksistä. Palvelunestohyökkäyksiä on perinteisen tietoliikenteen häiritsemisen ohella hyödynnetty myös kiristystarkoituksessa.[13]
- Järjestäytyneeseen kyberrikollisuuteen liittyvät kiristyshaittaohjelmahyökkäykset ovat säilyneet Euroopassa edelleen merkittävänä uhkana. Suurten yritysten kyberturvallisuuden kehittymisen myötä hyökkäyksiä on viime vuosina suunnattu myös toimitusketjuihin, sekä pieniin ja keskisuuriin yrityksiin.[13]
  - Kiristyshaittaohjelmat säilyvät todennäköisesti keskeisenä uhkana yrityksille myös jatkossa.
  - Viranomaisten suorituskyvyt ja kansainvälinen yhteistyö ovat vaikeuttaneet rikollisten toimintaa.[14]
- Tekoäly kasvattaa jatkuvasti rooliaan osana rikollisten työkalupakkia.
  - Kehitys näkyy esimerkiksi aiempaa laadukkaampina tietojenkalasteluviesteinä sekä haittaohjelmavarianttien määrän kasvuna.[14 ja 15]
- Kyberrikollisuus mukautuu nopeasti hyödyntämään uusia työkaluja ja haavoittuvuuksia. Ilmiö säilyttää merkityksensä kybermaailman uhkakuvastossa myös tulevina vuosina.
- Kybermaailmaan kytkeytyvän sääntelyn kehittyminen edistää kyberturvallisuuden toteutumista EU:n alueella.[16] Turvallisuutta parantava lainsäädäntö edistää kyberrikollisuuden vaikutusten hillitsemistä.
- Kyberrikollisuuden trendit painottuvat EU-jäsenmaissa eri tavoin. Kyberturvallisuuskeskus seuraa Suomessa tapahtuvaa kehitystä.

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

Kyberturvallisuuslaki astuu voimaan 8.4.2025.

- Soveltamisala kattaa toimijoita esimerkiksi liikenne-, energia- ja terveydenhuoltoaloilla sekä digitaalisen infrastruktuurin palveluntarjoajia.
- Soveltamisen alkaessa:
  - Soveltamisalaan kuuluvia toimijoita edellytetään ilmoittamaan yhteystietonsa valvovalle viranomaiselle.
  - Soveltamisalaan kuuluvia toimijoita edellytetään ilmoittamaan merkittävistä poikkeamista valvovalle viranomaiselle.
  - Toimijalla on oltava käytössä ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.
- Valvovia viranomaisia ovat toimialakohtaisesti Liikenne- ja viestintävirasto Traficom, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira ja Lääkealan turvallisuus- ja kehittämiskeskus Fimea.
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tukee NIS-direktiivin kohteena olevia organisaatioita ylläpitämään ja kehittämään tietoturvaansa erilaisin palveluin.
  - Katso lisää: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa

Oikeudelliset asiat

Gigabittiasetuksen toimeenpano lähtee lausuntokierrokselle.

- Gigabittiasetuksen tavoitteena on vauhdittaa erittäin suuren kapasiteetin verkkojen rakentamista.
  - Gigabittiasetus sisältää yhteiskäyttöä ja -rakentamista helpottavia keinoja, kuten keskitetyn tietopisteen kehittämistä ja muutoksia lupaprosessiin. Asetuksessa edellytetään, että verkkoinfrastruktuurin rakentamista varten tarvittavia lupia ja asennusoikeuksia voisi jatkossa hakea sähköisessä muodossa keskitetysti.
  - Liikenne- ja viestintävirasto Traficom valvoisi gigabittiasetuksen velvoitteiden noudattamista ja toimisi riitojenratkaisuelimenä.
  - Esitysluonnoksen lausuntoaika päättyy 29.4.2025. Uuden lain on tarkoitus tulla voimaan syksyllä 2025. Katso lisää: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=ba26422e-30b4-4b78-9339-d81273ccc822

Hallitus on antanut eduskunnalle esityksen sähköisen tiedoksiannon ensisijaisuutta viranomaistoiminnassa koskevaksi lainsäädännöksi.

- Esityksen tavoitteena on, että viranomaisen tiedoksiannot lähetettäisiin ensisijaisesti sähköisesti ja julkisen hallinnon digitaaliset palvelut olisivat hallinnon asiakkaille ensisijainen tapa asiointiin. Esityksellä tavoitellaan kansalaisten sujuvampaa ja paikkariippumatonta asiointia ja lisäksi tehokkaampia viranomaismenettelyitä ja parempaa tuottavuutta.
  - Sääntelyn myötä Suomi.fi-tunnistusta käyttävälle täysi-ikäiselle henkilölle luotaisiin automaattisesti Suomi.fi-viestit-tili, mikäli henkilöllä ei sitä olisi vielä käytössä.
  - Lausuntoaika **16.4.2025 saakka.** Muutosten on tarkoitus tulla voimaan 1.1.2026. Katso lisää: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=c839a803-4cdf-4d29-b911-249178fed2c6

Oikeudelliset asiat

Kyberkestävyyssäädösprosessi edistyy.

- Kyberkestävyyssäädöksen (CRA) täytäntöönpanosäännöksen luonnos koskien luokkien III ja IV tärkeiden ja kriittisten tuotteiden teknisiä kuvauksia on tullut lausuntokierrokselle.
- Luokkiin kuuluvilta tuotteilta saatetaan vaatia muita perusteellisempia vaatimuksenmukaisuuden arviointiprosesseja.
- Lausuntokierros päättyy 15.4.2024.

Katso lisää säädöksestä: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_en.

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) Näin tunnistat aidot verkkosivut ja viranomaiset – vältä huijaukset verkossa - https://www.epressi.com/tiedotteet/tietoturva/nain-tunnistat-aidot-verkkosivut-ja-viranomaiset-valta-huijaukset-verkossa.html
2) Kyberturvallisuuden vuosi 2024 - https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2024
3) Traficomin ja Huoltovarmuuskeskuksen järjestämä Tietoturva 2025 -tapahtuma kokosi ennätysyleisön - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-122025#83695-0
4) Launch of IoT Product Security Labeling Scheme (JC-STAR) - https://www.meti.go.jp/english/press/2025/0325_006.html
5) Comprehensive Threat Intelligence Assessment on GorillaBot Botnet Campaign and its Massive DDoS Attack Operations - https://voodootomato.medium.com/comprehensive-threat-intelligence-assessment-on-gorillabot-botnet-campaign-and-its-massive-ddos-82393b61a5cb
6) Silk Typhoon targeting IT supply chain - https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain
JA Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability/
7) Цільова активність UAC-0212 у відношенні розробників та постачальників рішень АСУТП з метою здійснення кібератак на об'єкти критичної інфраструктури України (CERT-UA#13702) - https://cert.gov.ua/article/6282517 JA UAC-0200: Шпигунство за оборонно-промисловим комплексом за допомогою DarkCrystal RAT (CERT-UA#14045)- https://cert.gov.ua/article/6282737 JA Russian Intelligence Service-backed Campaigns Impersonate the CIA to Target Ukraine Sympathizers, Russian Citizens and Informants - https://www.silentpush.com/blog/russian-intelligence-phishing/
8) Miten viestimme kyberhyökkäyksistä? - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/miten-viestimme
9) Milloin viimeksi tarkistit oman organisaatiosi Microsoft 365 Entra ID:si asetukset? - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-112025#83578-1
10) Hallitse salasanojasi turvallisesti- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-102025#83074-0
11) CISA Adds Two Known Exploited Vulnerabilities to Catalog - https://www.cisa.gov/news-events/alerts/2025/03/18/cisa-adds-two-known-exploited-vulnerabilities-catalog
12) Fortinetin FortiOS ja FortiProxy -tuotteissa kriittinen haavoittuvuus - https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_3/2025
13) ENISA, Threat Landscape 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
14) Europol, Internet Organized Crime Threat Assesment 2024 - https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
15) Fortinet, Cyber Threat Predictions For 2025 - https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-prediction-2025.pdf
16) ENISA, 2024 report on the State of the Cybersecurity in the Union - https://enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union