TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Joulukuu 2024

#kybersää

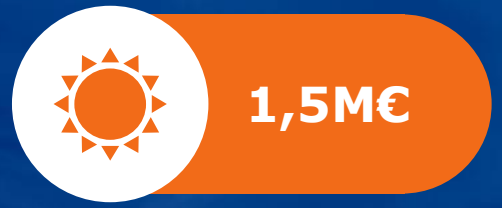
Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

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

Puolustusvoimat ja Kyberturvallisuuskeskus perustivat uuden yhteistoimintaryhmän (MIL-ISAC). Suomessa toimii tällä hetkellä 24 ISAC-ryhmää ja niihin kuuluu satoja yrityksiä, yhteisöjä sekä organisaatiota. [1]



Vuoden aikana kansallisen koordinointikeskuksen myöntämä rahoitus mikro- ja pk-yrityksille oli yhteensä 1,5 miljoonaa euroa, ja tukea sai 37 yritystä tietoturvaratkaisujen käyttöönottoon. Rahoituksen avulla pyritään vahvistamaan pk-yritysten kykyä suojautua kyberhyökkäyksiltä sekä parantamaan Suomen kansallista kyberkapasiteettia ja infrastruktuuria. [2]

Traficomin Kyberturvallisuuskeskus sai 25. joulukuuta tiedon useista sähkönsiirto- ja tietoliikennekaapelien vaurioista Suomenlahdella. Vauriot kohdistuivat neljän eri yrityksen kaapeleihin. Kyberturvallisuuskeskus käynnisti erityisseurannan tapauksiin liittyen. [3]

Kybersää joulukuu 2024

Tietomurrot ja -vuodot

- Saimme joulukuussa ilmoituksia verkon reunalaitteisiin kohdistuvista tietomurron yrityksistä, jotka onnistuessaan voivat johtaa esimerkiksi kiristyshaittaohjelma-tartuntaan.
- Kryptovaluuttatilejä murrettiin eri kryptopalveluiden nimissä lähetetyillä kalasteluviesteillä.

Huijaukset ja kalastelut

- Huijarit kalastelevat pankkitunnuksia myös viranomaisten nimissä. Hakukoneisiin on ostettu mainostilaa väärennetyille sivuille.
- QR-koodeilla tehdyt huijaukset johtuvat useimmiten haitallisista lukijasovelluksista. Kannattaa silti varmistaa, ettei koodia ole peukaloitu tai liimattu päälle tarraa.

Haittaohjelmat ja haavoittuvuudet

- Joulukuun aikana useita ilmoituksia kiristyshaittaohjelmista.
- Yksittäisiä ilmoituksia tietokoneiden saamista Lumma Stealer -tartunnoista.
- Ivanti Connect Secure -tuotteessa olevan haavoittuvuuden (CVE-2025-0282) hyväksikäyttöä on jo havaittu. Päivitä välittömästi.

Automaatio ja IoT

- IOCONTROL-haittaohjelmaa on havaittu useissa israelilaisissa ja yhdysvaltalaisissa automaatiojärjestelmissä. Haittaohjelman tekijöiden uskotaan toimivan Iranin valtion lukuun. [4]
- Sähköautojen sijaintihistoriat ja omistajien tiedot julkisella palvelimella suojaamattomina paljastivat yksityisten henkilöiden lisäksi esim. poliitikkojen tai poliisiautojen tarkat ajoreitit ja pysähtymispaikat. [5]

Verkkojen toimivuus

- Merenalaisten tietoliikennekaapeleiden vaurioilla ei ollut merkittäviä vaikutuksia Suomen tietoliikenneyhteyksiin.
- Muutamia palvelunestohyökkäyksiä, joissa verkossa olevaa lomaketta ruuhkauttamalla aiheutettiin lyhyitä käyttökatkoja palveluun.

Vakoilu

- Ukrainaan kohdistuvat kyberhyökkäykset jatkuvat edelleen. Joulukuussa kerrottiin muun muassa väestötietoja sisältävän rekisterin toiminnan häiritsemisestä.
- Esimerkiksi Venäjään yhdistetyt APT-ryhmät Turla ja Sandworm ovat olleet aktiivisiä Ukrainassa.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Yhdysvaltojen kyberturvallisuudesta vastaava virasto CISA ylläpitää #StopRansomware sivustoa. Sivustolle on koottu hyvää ja ajantasaista tietoa kiristyshaittaohjelmista.[6]

Euroopan Unionin kyberturvallisuusvirasto Enisa julkaisi Euroopan laajuisen kyberharjoituksen loppuraportin. Harjoitukseen osallistui noin 5000 henkilöä ympäri Eurooppaa. Suomesta mukana oli noin 50 henkilöä. Kyberturvallisuuskeskus vastasi harjoituksen kansallisesta suunnittelusta ja toimeenpanosta. [7]

Kyberturvallisuuskeskus järjesti webinaarin Kyberkestävyyssäädöksen (Cyber Resilience Act, CRA) asettamista vaatimuksista, jossa kerrottiin mitkä tuotteet kuuluvat sen piiriin ja samalla käytiin läpi vinkkejä, joiden avulla organisaatio voi valmistautua säädöksen tuloon ennakoivasti. Webinaarista on tallenne tulossa, jotta voit saada vinkit talteen mikäli webinaari meni sivu suun. [8], [9]

Joulukuun kyberturvallisuuden yleiskuva

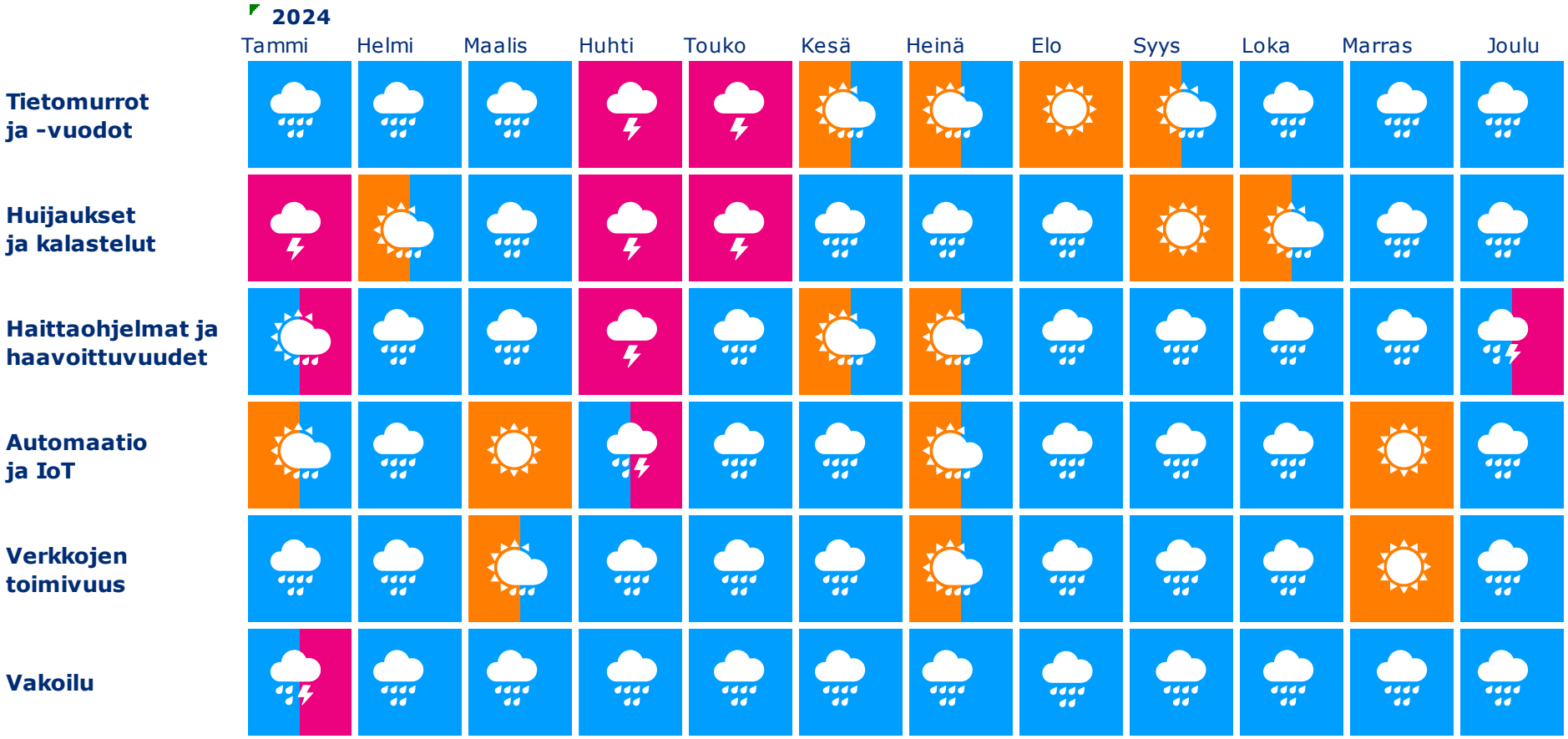
- Kiristyshaittaohjelmien määrä kääntyi loppuvuodesta 2024 ilmoitusten perusteella lievään kasvuun
  - Kaikissa ilmoitetuissa tapauksissa oli kyseessä eri kiristyshaittaohjelmavariantti.
  - Sisäänpääsyssä hyödynnetään edelleen verkon reunalaitteita. Haavoittuvuudet, puutteet prosesseissa ja konfiguraatiovirheet altistavat organisaatiot hyökkääjille. Säännöllinen harjoittelu auttaa organisaatioita varautumaan erilaisiin kyberpoikkeamiin. Kirjoitimme tästä myös maaliskuussa 2024. [10]
  - Moni organisaatio palautui viime vuonna kiristyshaittaohjelmahyökkäyksestä varmuuskopioiden avulla.
  - Organisaatioiden tulee myös tarkastella sisäverkosta ulos lähtevää liikennettä, sillä osassa tapauksista kiristyshaittaohjelman aktivoituminen tai latautuminen voidaan tunnistaa ja estää juuri sisältä ulos tapahtuvassa liikenteessä.
- Marraskuun lisäksi myös joulukuussa havaittiin tietoliikennekaapelivaurioita
  - Kyberturvallisuuskeskus sai joulupäivänä 25.12. tiedon useista sähkö- ja tietoliikennekaapelien vaurioista Suomenlahdella. Kyberturvallisuuskeskus käynnisti erityisseurannan tapauksiin liittyen.
  - Tapahtuneella ei ole ollut vaikutusta Suomen huoltovarmuuteen ja valtaosa vaurioituneista kaapeleista on jo saatu korjattua. Suomi on varautunut hyvin erilaisiin sähkönsiirron ja tietoliikenteen häiriöihin. Yhteiskunnan eri sektorit tekevät tiivistä yhteistyötä erilaisiin häiriöihin varautumisessa ja viranomaiset sekä yritykset harjoittelevat säännöllisesti yhdessä.

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

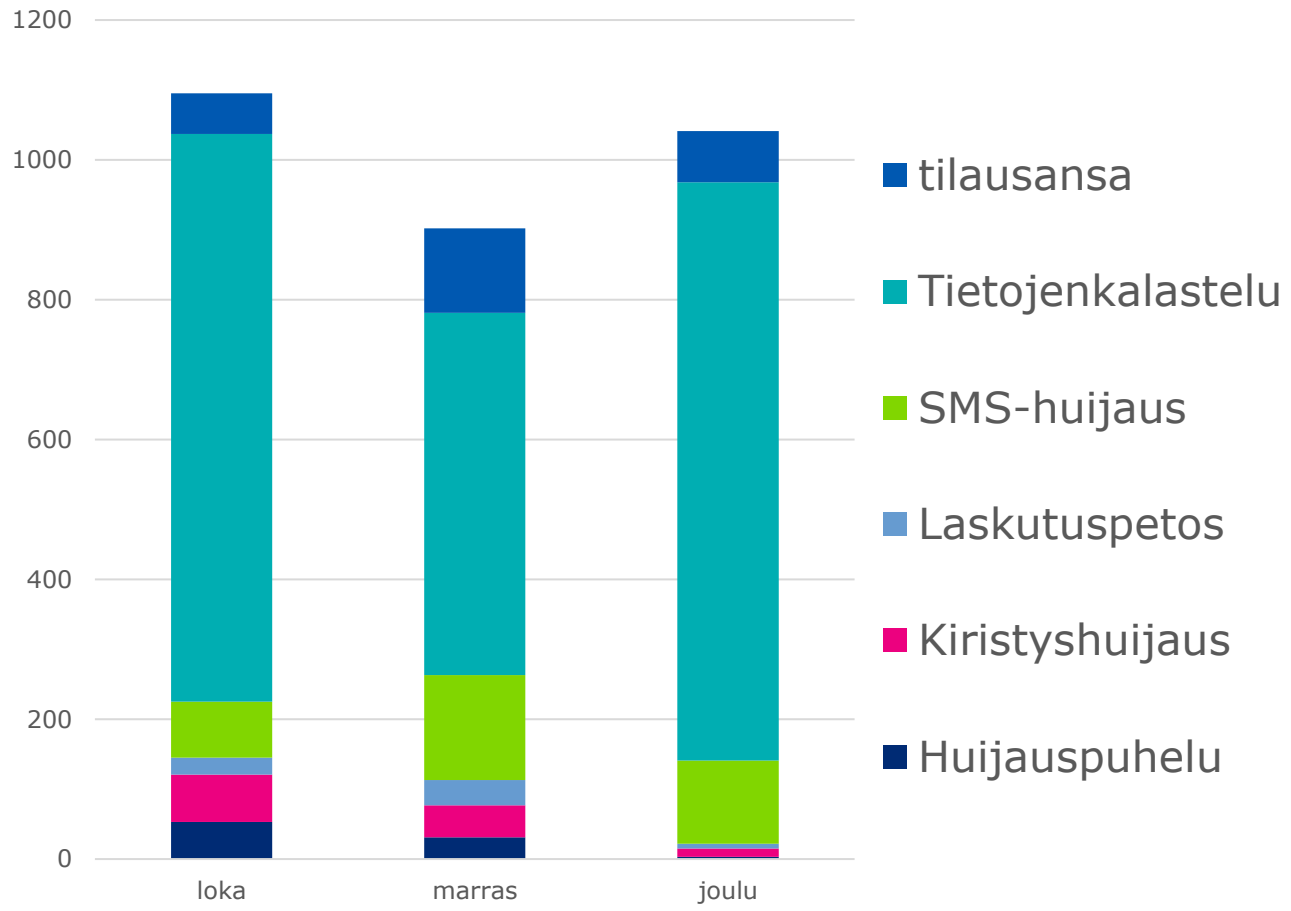


Käsiteltyjä huijaustapauksia
Q4/2024

3 kk

Vuoden 2024 viimeisen neljänneksen ilmiöitä ovat:

- Suomalaisista puhelinnumeroista soitettujen huijauspuheluiden määrä on romahtanut.
- Tekstiviestien käyttö huijauksiin on tullut jäädäkseen ja on aktiivista.
- Tietojenkalastelu ja erilaiset verkkokauppahuijaukset lisääntyivät vuodenvaihteen sesonkien lähestyessä.
- Nettihuijarit pyrkivät aktiivisesti kiertämään torjuntatoimia uusilla huijaustavoilla.

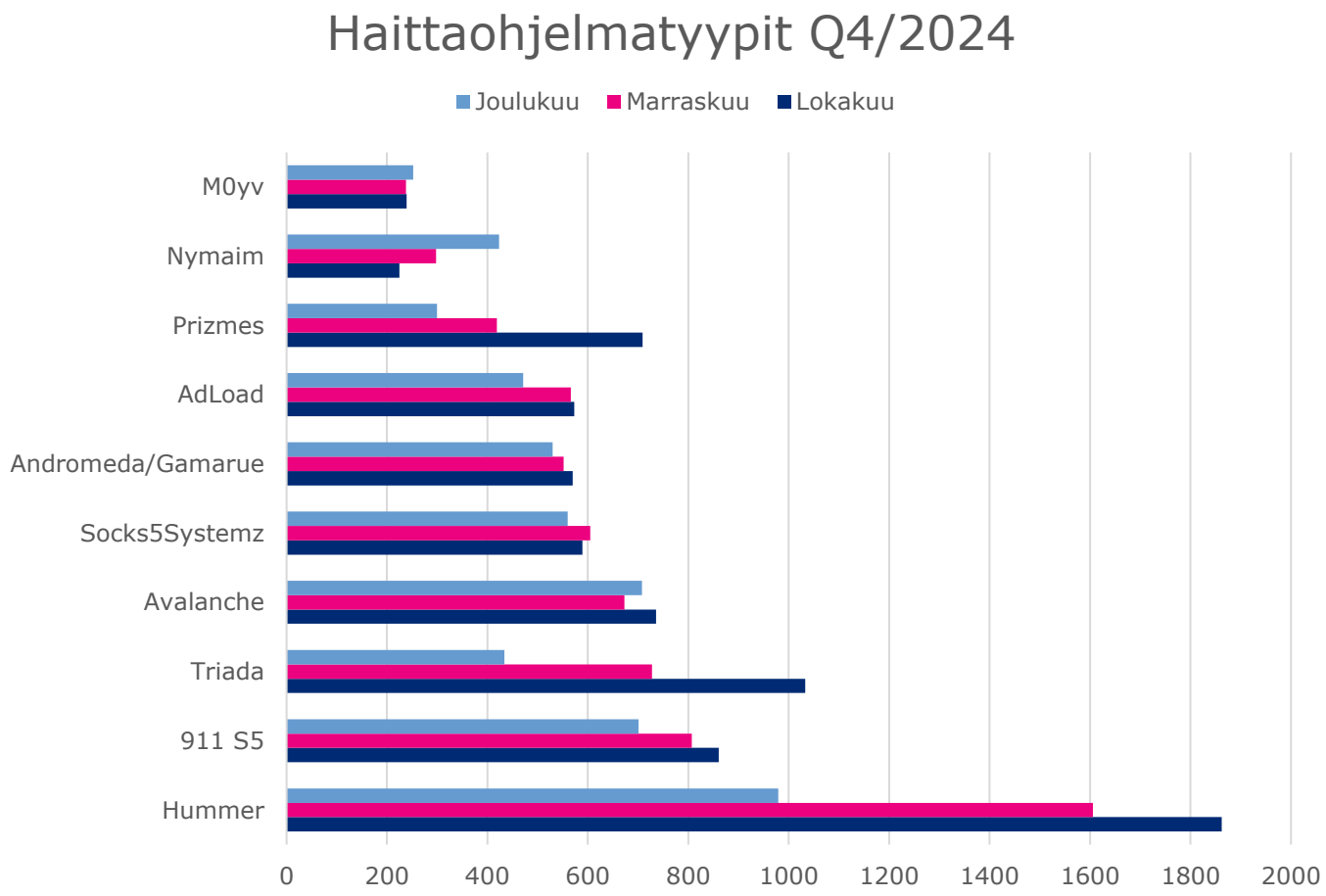


Autoreporterin haittaohjelmahavainnot

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.

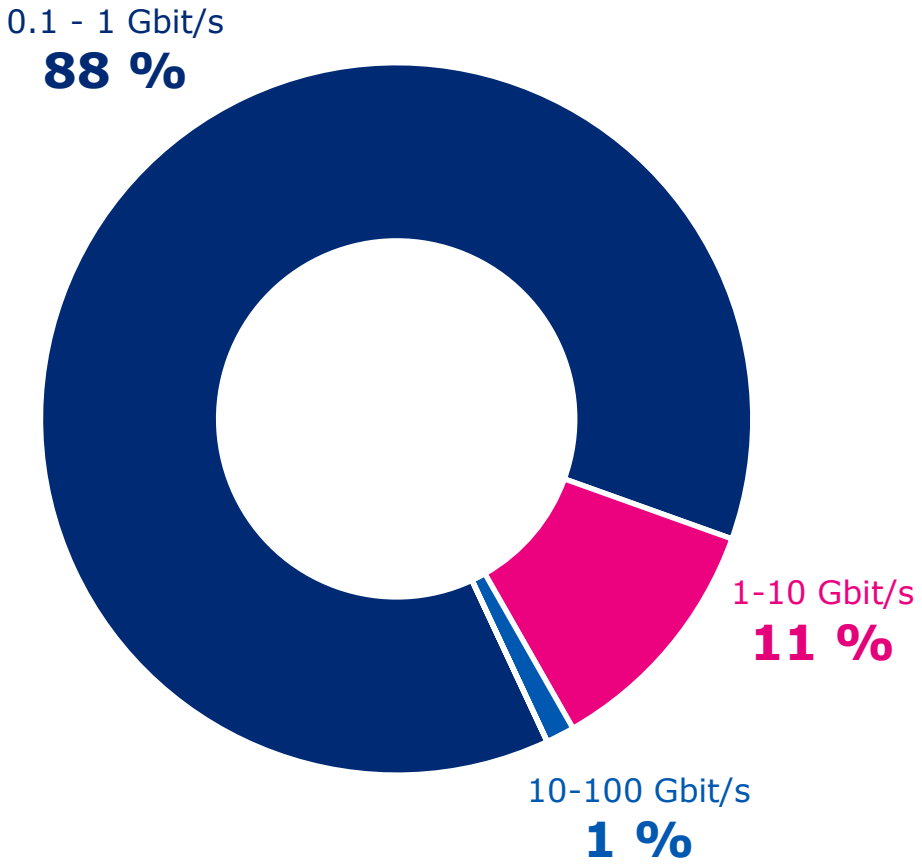
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla



3 kk

Palvelunestohyökkäysten tunnuslukuja
Q4/2024

- **140 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q4/2024.
- Noin **70%** hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.
- Lyhyitä palvelunestohyökkäyksiä voidaan käyttää hyökkäyskohteiden kartoitukseen ja testaamiseen.



Toimialakohtaiset havainnot

3 kk

	Trendi 3kk	Edeltävä 3kk	
Elintarvike			Alaa koskevien poikkeamatapausten määrä pysyi huomattavan pienenä ja väheni muutamalla tapauksella kolmanteen vuosineljännekseen verrattuna. Yleisin poikkeaman tyyppi oli tietomurto. Merkille pantavaa on myös, että elintarvikealaan kohdistuneesta tietojenkalastelusta ei ilmoitettu kertaakaan. Todennäköisesti elintarvikealaa uhkaavia poikkeamia tapahtuu siinä missä muitakin toimialoja uhkaavia, mutta elintarvikealaa uhkaavista ilmoitetaan harvemmin.
Energia			Suomen ja Viron välinen Estlink2-merikaapeli katkesi joulukuussa. Kyberturvallisuuskeskuksen tietoon tulleiden poikkeamien perusteella suosittelemme kartoittamaan ja rajoittamaan omaa hyökkäyspinta-alaa, testaamaan asiakasrajapintojen tietoturvaa, tutustumaan password spraying -hyökkäyksien torjumiseen, varmistamaan laskujenkäsittelyprosessit ja rekisteröimään käyttämänne SMS sender ID-tunnukset. Sektorin toimijoita osallistui mm. TIETO24-harjoitukseen.
Finanssi			Pankkiteemainen kalastelu on jatkunut aktiivisena. Palvelunestohyökkäykset ovat hieman rauhoittuneet syys-lokakuun pitkäkestoisen hyökkäyksen jälkeen.
Kemian-teollisuus			Ilmoitettujen poikkeamien määrässä ei muutoksia, mutta etenkin tietomurrot lisääntyivät. Mukana oli myös joitakin kiristyshaittaohjelmatapauksia.
Logistiikka ja liikenne			Alaa on koskettanut tarkasteltavalla ajanjaksolla M365-tilimurrot sekä erilaiset alan organisaatioiden nimissä tehdyt huijausyritykset.
Valtionhallinto			Vaikka palvelunestohyökkäysten määrä yleisesti väheni loppuvuotta kohden, niitä raportoitiin valtionhallinnon organisaatioista useana viikkona. Valtionhallintoon kohdistuu jatkuvasti kalasteluyrityksiä ja tietomurtojen yrityksiä, ja raportointiaikana ilmoitettiin myös yrityksistä levittää haittaohjelma organisaation verkkoon. Kyberturvallisuuskeskuksen tietoon ei ole kuitenkaan tullut vakavia tietoturvapoikkeamia.
Media			Ilmoitetuissa poikkeamissa ei merkittäviä muutoksia.
SOTEPE			Alaa välittömästi koskevien poikkeamailmoitusten määrä kasvoi merkittävästi vuoden kolmannesta neljänneksestä. Sähköisesti tehtyjä petoksia, tietojenkalastelua ja identiteetin väärinkäytöksiä koskevat ilmoitukset olivat yleisimpiä SOTEPE-alalla samoin kuin toimialoilla keskimäärin. Neljänneksi eniten SOTEPE-alaa koskivat tietomurrot, mikä poikkesi merkittävästi toimialojen keskiarvosta. Näin oli myös vuoden kolmannella neljänneksellä.
Vesihuolto			Ilmoitettujen poikkeamien määrä on kasvanut. Mukana oli esimerkiksi websivujen lomakkeiden väärinkäyttötapauksia. Internetiin näkyvien automaatioprosessien ohjauksessa käytettyihin laitteisiin kohdistuneista tietomurroista uutisoitiin laajasti maailmalla.
Kunnat			Kuntaorganisaatioihin kohdistui kalastelua, johtaen onnistuneisiin tilimurtoihin. Kuntien keskeiseen tietojärjestelmään saatiin tehtyä onnistuneita tietomurtoja. Suomalaisia kuntia kohtaan tehtiin myös palvelunestohyökkäyksiä venäjämielisten haktivistien toimesta.
Kiinteistö ja rakennus			Julkiverkkoon sinne kuulumattomia avoimena näkyviä kiinteistöautomaation laitteita havaittiin tarkastelujaksolla. Edellisen vuosineljänneksen tapaan havaittiin myös Dropbox teemaisia M365-tilimurtoja, jotka johtivat jatkokalasteluihin.

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: Kuudennen sukupolven langaton teknologia, 6G

- 6G, eli kuudennen sukupolven langaton teknologia, on seuraava askel mobiiliviestinnässä 5G:n jälkeen. 6G:ltä odotetaan merkittäviä edistysaskeleita nopeudessa, viiveessä, yhteyksien laadussa ja yleisessä suorituskyvyssä.
- Vaikka 5G on yhä laajentumassa maailmalla, monet maat ja organisaatiot ovat jo investoineet 6G-tutkimukseen ja –kehitykseen. 6G:n täysimittainen käyttöönotto on odotettavissa noin vuonna 2030.
- Uudet taajuusalueet, tekoälyn ja koneoppimisen integrointi sekä mahdollinen kvanttilaskennan hyödyntäminen tulevat olemaan 6G:n keskeisiä elementtejä. Samalla uudet elementit haastavat tietoturvaa, sillä mahdollisten haavoittuvuuksien kenttä laajenee.
- Myös Euroopan komissio valmistautuu 6G:tä varten. Euroopan komissio perusti vuonna 2021 älykkäiden verkkojen ja palvelujen yhteisyrityksen (SNS-yhteisyritys) tukemaan siirtymistä 6G:hen. SNS-yhteisyrityksellä on kunnianhimoinen 900 miljoonan euron EU-budjetti vuosiksi 2021–2027. [11]
- 6G-standardoinnin odotetaan alkavan noin vuonna 2025 varhaisten tutkimusvaiheiden kautta, joissa noudatetaan maailmanlaajuista 6G-visiota [12]

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

- Hallituksen esitysluonnos EU:n datasäädöksen täytäntöönpanoa koskevaksi lainsäädännöksi lausuntokierrokselle
  - Liikenne- ja viestintäministeriö pyytää lausuntoja hallituksen esitysluonnoksesta EU:n datasäädöksen täytäntöönpanoa koskevaksi lainsäädännöksi. [13]
  - EU:n datasäädös tuli voimaan 11.1.2024 ja sen soveltaminen alkaa pääosin 12.9.2025. Datasäädös on sellaisenaan sovellettavaa EU-sääntelyä, mutta sen toimeenpano edellyttää täydentävien kansallisten säännösten antamista mm. viranomaistehtävistä ja seuraamuksista.
  - Datasäädös asettaa vaatimuksia erityisesti verkkoon liitettävien laitteiden (esim. sensorit ja älykellot) valmistajille laitteilla kerätyn datan jakamisen ja käytön osalta. Asetus luo myös uusia oikeuksia datan käyttäjille mm. omien tietojen hallinnan ja epäreilujen sopimusehtojen osalta.
  - Uusia viranomaistehtäviä saisivat esityksen mukaan Liikenne- ja viestintävirasto Traficom, Kilpailu- ja kuluttajavirasto sekä kuluttaja-asiamies.
  - Lausuntoja hallituksen esitysluonnoksesta voi antaa 31.1.2025 saakka. Lausuntoja voivat antaa kaikki organisaatiot ja kansalaiset lausuntopalvelussa. [14]

Oikeudelliset asiat

- Kyberturvallisuusstrategian toimeenpanosuunnitelma on julkaistu 3.12.2024
  - Suomen kyberturvallisuusstrategia uudistettiin pääministeri Orpon hallitusohjelman mukaisesti vastaamaan muuttunutta toimintaympäristöä. 10.10.2024 julkaistun strategian tavoitetila ulottuu vuoteen 2035. [15]
  - 3.12.2024 julkaistussa strategian **toimeenpanosuunnitelmassa** määritellään toimet strategian tavoitteiden saavuttamiseksi. [16]
  - Suunnitelmassa priorisoitavia toimenpiteitä ovat esimerkiksi kansalaisten kybervalmiuksien ja varautumisen kehittäminen, kvanttiturvallisten salausratkaisujen käyttöönotto sekä yhteisten tieto- ja viestintäteknisten palveluiden ja tietovarantojen turvallisuuden ja toimintavarmuuden edistäminen.
  - Merkittäviä toimia ovat myös kyberturvallisuusharjoitusten kehittäminen, kyberpuolustuksen yhteensovittaminen kokonaismaanpuolustukseen sekä yksityisen ja julkisen sektorin kyberosaamisen vahvistaminen.
  - Valtion kyberturvallisuusjohtajan toimisto koordinoi toimenpiteiden seurantaa yhdessä ministeriöiden muodostaman seurantaryhmän ja sen sihteeristön kanssa. [17]

Oikeudelliset asiat

- Valtiovarainministeriö julkaisi 12.12.2024 raportin *Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset* [18]
  - Raportin keskeiset kehittämisehdotukset lainsäädäntöön ovat:
    - Parannetaan arviointien saatavuutta ja viranomaisyhteistyötä tarkistamalla viranomaisten arviointitehtäviä.
    - Parannetaan salaustuotteiden valmistajien, TEMPEST-tuotteiden valmistajien ja arviointilaitosten elinkeinotoiminnan edellytyksiä.
    - Sujuvoitetaan arviointimenettelyjä riskiperusteisesti sekä selkeytetään ja täydennetään arviointiperusteita.
  - Sääntelyn ja arviointitoiminnan kehittäminen on myös kyberturvallisuusstrategian toimeenpano-ohjelmassa.
  - Raportti on valmisteltu tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmässä, jonka työ jatkuu 2025 aiheeseen liittyvän hallituksen esityksen valmisteluna.

Oikeudelliset asiat

- Tietosuojavaltuutettu määräsi lainanvertailupalveluja tarjoavalle Sambla Groupille seuraamusmaksun tietoturvallisuuden laiminlyönnistä
  - Tietosuojavaltuutetun toimiston seuraamuskollegio on määrännyt 950 000 euron seuraamusmaksun lainojen vertailupalveluja tarjoavalle Sambla Groupille, sillä heikon tietoturvan vuoksi asiakkaiden lainahakemusten tiedot olivat olleet ulkopuolisten saatavilla asiakkaille tarkoitettujen henkilökohtaisten linkkien kautta.
  - Linkit eivät yrityksen mukaan enää ole käytössä. Yritys määrättiin ilmoittamaan tapahtuneesta asiakkailleen.
  - Tietosuojavaltuutetun toimiston teknisessä selvityksessä havaittiin, että Sambla Groupin lainaparkki.fi- ja rahoitu.fi -lainanvertailupalveluissa oli vakavia tietoturvapuutteita. Yritys määrättiin lopettamaan lainanhakijoiden henkilötietojen käsittely sähköisissä palveluissaan heti, kun tietoturvapuutteiden vakavuus tuli ilmi maaliskuussa 2024.
  - Tekninen selvitys osoitti, että verkko-osoitteisiin oli kohdistunut kalastelua ja henkilötietoja oli myös päätynyt ulkopuolisille. Linkkien kautta oli ollut saatavilla lainanhakijan yhteystietoja sekä muun muassa tietoja tuloista, asumismenoista, siviilisäädystä ja mahdollisista lapsista.
  - Päätös ei ole vielä lainvoimainen ja siitä voi valittaa hallinto-oikeuteen. [19]

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) Puolustusvoimat ja Traficom käynnistivät kyberturvallisuuden yhteistyöryhmän https://puolustusvoimat.fi/-/puolustusvoimat-ja-traficom-kaynnistivat-kyberturvallisuuden-yhteistyoryhman
2) Kansallisen koordinointikeskuksen vuosi 2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kansallisen-koordinointikeskuksen-vuosi-2024
3) Traficom mukana selvittämässä Suomenlahden kaapelivaurioita https://traficom.fi/fi/ajankohtaista/traficom-mukana-selvittamassa-suomenlahden-kaapelivaurioita
4) Inside a New OT/IoT Cyberweapon: IOCONTROL https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol
5) Wir wissen, wo dein Auto steht https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027
6) Stop Ransomware https://www.cisa.gov/stopransomware
7) Cyber Europe 2024 - After Action Report https://www.enisa.europa.eu/publications/cyber-europe-2024-after-action-report
8) Kyberkestävyyssäädös (Cyber Resilience Act, CRA) https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra
9) Uusi kyberkestävyyssäädös tulossa https://traficom.fi/fi/ajankohtaista/tilaisuudet/uusi-kyberkestavyyssaados-tulossa-nyt-aika-valmistautua-webinaari
10) Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskialttiit-verkon-reunalaitteet-aktiivisten-murtoyritysten-kohteena
11) Euroopan komissio valmistelee Eurooppaa 6G:tä varten https://digital-strategy.ec.europa.eu/fi/policies/6g

Lähdeluettelo

12) IMT towards 2030 and beyond (IMT-2030) https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

13) Hallituksen esitys EU:n datasäädöksen täytäntöönpanoa koskevaksi lainsäädännöksi lausunnoille https://lvm.fi/-/hallituksen-esitys-eu-n-datasaadoksen-taytantoonpanoa-koskevaksi-lainsaadannoksi-lausunnoille

14) Lausuntopyyntö: Hallituksen esitysluonnos EU:n datasäädöksen täytäntöönpanoa koskevaksi lainsäädännöksi https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1110d2de-26b3-4c1b-8a63-f31111654667

15) Suomen kyberturvallisuusstrategia 2024–2035 http://urn.fi/URN:ISBN:978-952-383-376-0

16) Kyberturvallisuusstrategian toimeenpanosuunnitelma https://api.hankeikkuna.fi/asiakirjat/b9b35c4c-2719-4cfb-89fa-4388c855e2f0/c4785613-4037-43b5-b1cc-22d9b82c0d69/SUUNNITELMA_20241204070347.PDF

17) Kyberturvallisuusstrategian toimeenpanosuunnitelma on julkaistu https://lvm.fi/-/kyberturvallisuusstrategian-toimeenpanosuunnitelma-on-julkaistu-kyberturvallisuus-erottamattomaksi-osaksi-kokonaisturvallisuutta

18) Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset https://api.hankeikkuna.fi/asiakirjat/cc687f08-8228-4cdc-9d52-86e9bd57a29c/25ce2e2b-9b3f-42dd-858a-fd8b1b8be9fe/RAPORTTI_20241217074537.PDF

19) Lainanvertailupalveluja tarjoavalle Sambla Groupille seuraamusmaksu tietoturvallisuuden laiminlyönnistä https://tietosuoja.fi/-/lainanvertailupalveluja-tarjoavalle-sambla-groupille-seuraamusmaksu-tietoturvallisuuden-laiminlyonnista-yrityksen-on-ilmoitettava-asiakkailleen