TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 2023

#kybersää

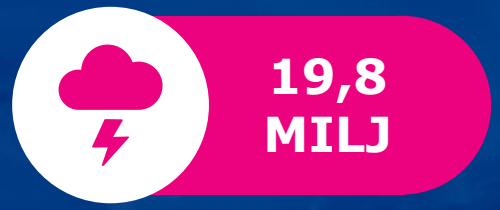
Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

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

Irlannin tietosuojaviranomainen on määrännyt TikTok Technology Limitedille 345 miljoonan euron seuraamusmaksun yleisen tietosuoja-asetuksen vastaisista käytännöistä lasten henkilötietojen käsittelyssä.[1]



Suomalaiset menettivät erilaisissa verkkohuijauksissa yhteensä 19,8 miljoonaa euroa vuoden 2023 ensimmäisten kuuden kuukauden aikana.[2]

Tietoturva 2023 –seminaariin on ilmoittautunut yli 2200 osallistujaa! Seminaari pidetään torstaina 12.10.2023.

Kybersää syyskuu 2023

Tietomurrot ja -vuodot

- Julkisuudessa olleen Essityn/Westlogin tietomurron seurauksena saimme ilmoituksia vuotaneista tiedoista.
- Sosiaalisen median tilimurroissa on nähty myös järjestelmiin tallennettujen luottokorttien väärinkäyttöjä esimerkiksi ostamalla mainoksia.

Huijaukset ja kalastelut

- Huijauspuheluita soitettiin väärennetyistä numeroista syyskuussa ennätysmäärä.
- Pankkitunnusten kalastelu siirtyi taas tekstiviesteistä sähköpostiin.
- Laskutuspetoksilla yritettiin huijata organisaatioita kalastusseuroista kotiseutuyhdistykseen.

Haittaohjelmat ja haavoittuvuudet

- Kriittinen ja etäkäytettävä haavoittuvuus libwebp-kirjastossa edellyttää välitöntä päivittämistä. Kirjasto on käytössä mm. useissa eri selaimissa.

Automaatio ja IoT

- NIST on päivittänyt teollisuusautomaatioympäristöjen suojaamiseen keskittyvän ohjeensa 800-82.[3]
- Uudessa versiossa huomioidaan mm. muuttuneet tuotanto-ympäristöjen kyberturvallisuus-uhkat, suojaustyökalut, suositellut käytännöt sekä arkkitehtuurit.

Verkkojen toimivuus

- Syyskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
- Haktivistit jatkavat palvelunestohyökkäyksiä ja kotimaiset organisaatiot ovat saaneet osansa hyökkäyksistä.
- Palvelunestohyökkäyksillä ei ole ollut vakavia vaikutuksia palveluiden saatavuuteen.

Vakoilu

- Puolivuosittain julkaistava Microsoftin raportti kuvaa Itä-Aasian kyberoperaatioiden trendiä.[4]
- Microsoftin raportti kertoo esimerkiksi Kiinaan liitettävästä kybervakoilusta ja vaikuttamisoperaatioista sekä Pohjois-Korean tietojenkeruusta ja kryptovaluuttojen hankinnasta.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Syyskuussa Kyberturvallisuuskeskuksen viestinnällinen teemakuukausi oli Tietoturvailmiöt tutuksi. Kuukauden aikana esittelimme somekanavissamme yleisimpiä tietoturvauhkia sekä kerroimme niitä vastaan suojautumisesta.[5]

Julkaisimme uuden ohjeen pilviympäristön poikkeamanhallinnasta.[6]

Syyskuussa julkaistiin kunnille suunnattu Hyöky-palvelu, jonka avulla voi kartoittaa kunnan hyökkäyspinnan julkisissa verkoissa.[7]

Syyskuun kyberturvallisuuden yleiskuva

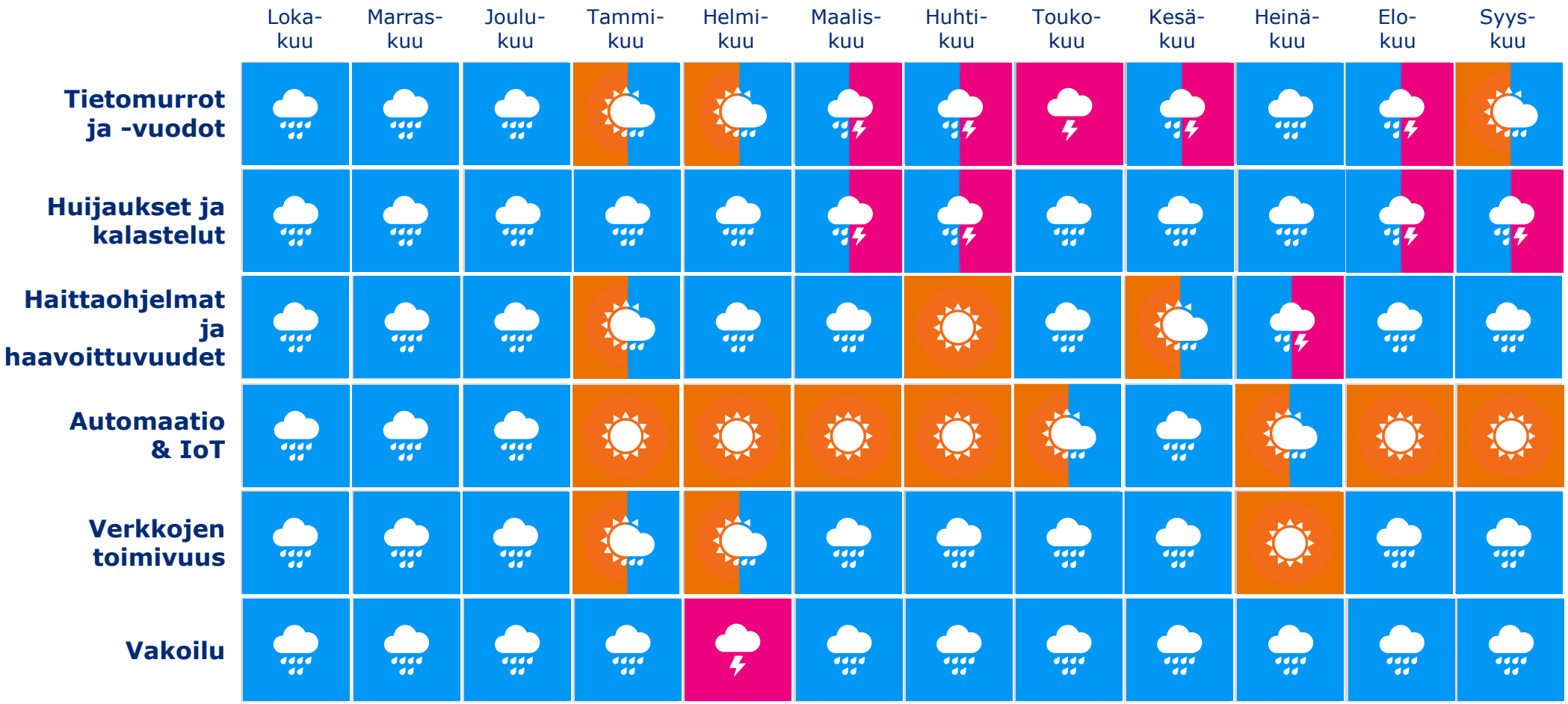
- Syyskuun alkupuolella haktivistiryhmä ilmoitti hyökänneensä useita eurooppalaisia kyberturvallisuusviranomaistahoja kohtaan.
  - Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus oli yksi ilmoitetuista kohteista.
  - Palvelunestohyökkäysten vaikutus palveluiden toimintaan on yleensä tilapäinen. Niitä on usein rinnastettu verkossa toteutettuun ruuhkaan tai mielenilmaukseen, joiden tavoitteena onkin saada aikaan uutisointia.
- Ilmoituksia väärennetyistä numeroista saapuvista huijauspuheluista tuli syyskuussa suuri määrä. Lokakuun alussa astui voimaan Traficomin määräys, joka velvoittaa teleoperaattorit torjumaan ulkomailta saapuvia suomalaisiksi numeroiksi väärennettyjä puheluita myös mobiilinumeroiden osalta.
- Kuluneen kuukauden aikana Kyberturvallisuuskeskukselle tulleet ilmoitusmäärät tietomurroista, tietomurron yrityksistä ja tietovuodoista ovat vähentyneet.

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

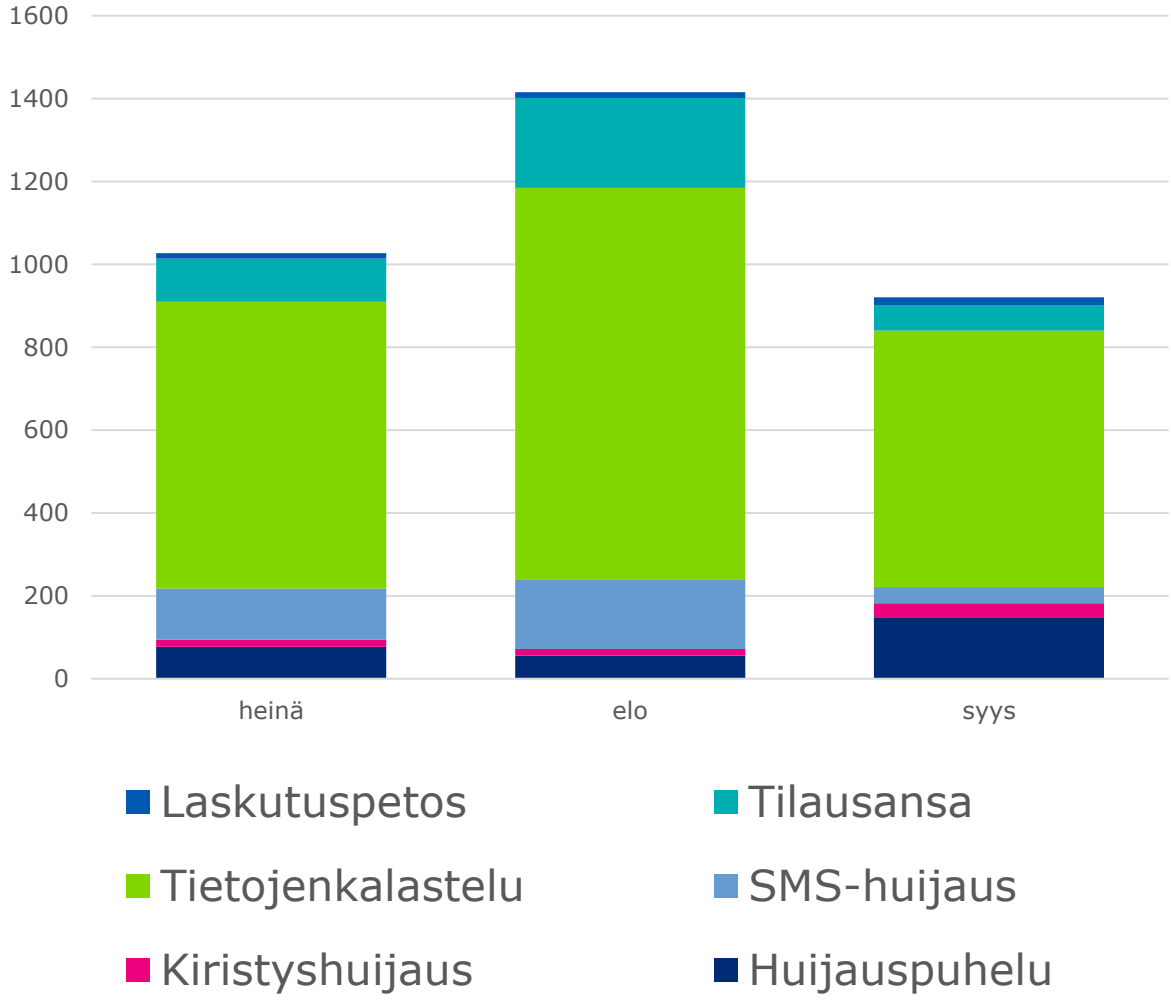


Käsiteltyjä huijaustapauksia
Q3/2023

3 kk

Vuoden 2023 kolmannen neljänneksen ilmiöitä ovat:

- Pankkitunnusten kalastelu on laajentunut tekstiviestistä sähköpostiin.
- Huijauspuhelut ottivat syyskuussa loppukirin ennen lokakuun viranomaismääräyksen astumista voimaan.
- Laskutuspetoksia on yritetty tasaiseen tahtiin kaikenlaisiin organisaatioihin.

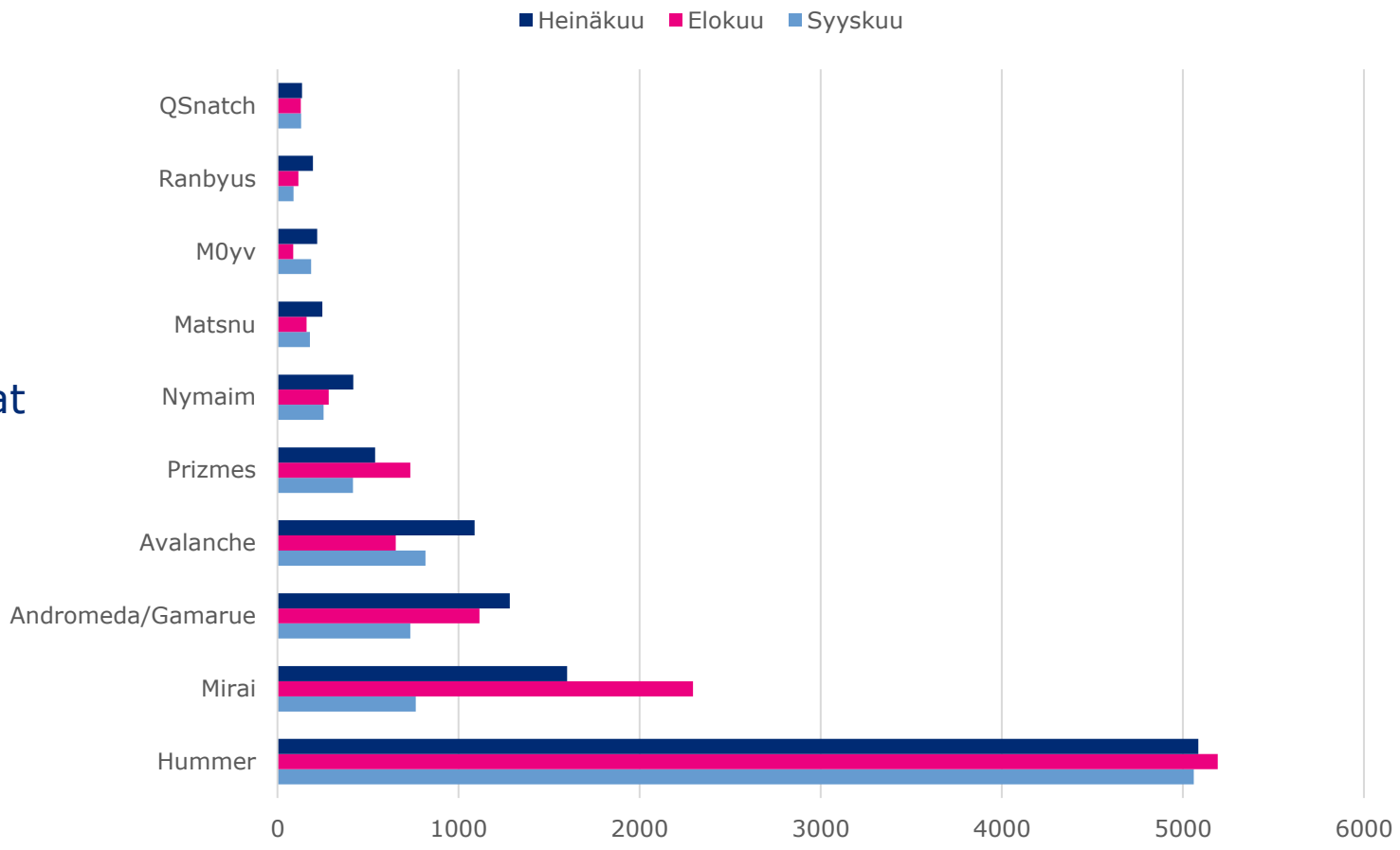


3 kk

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.

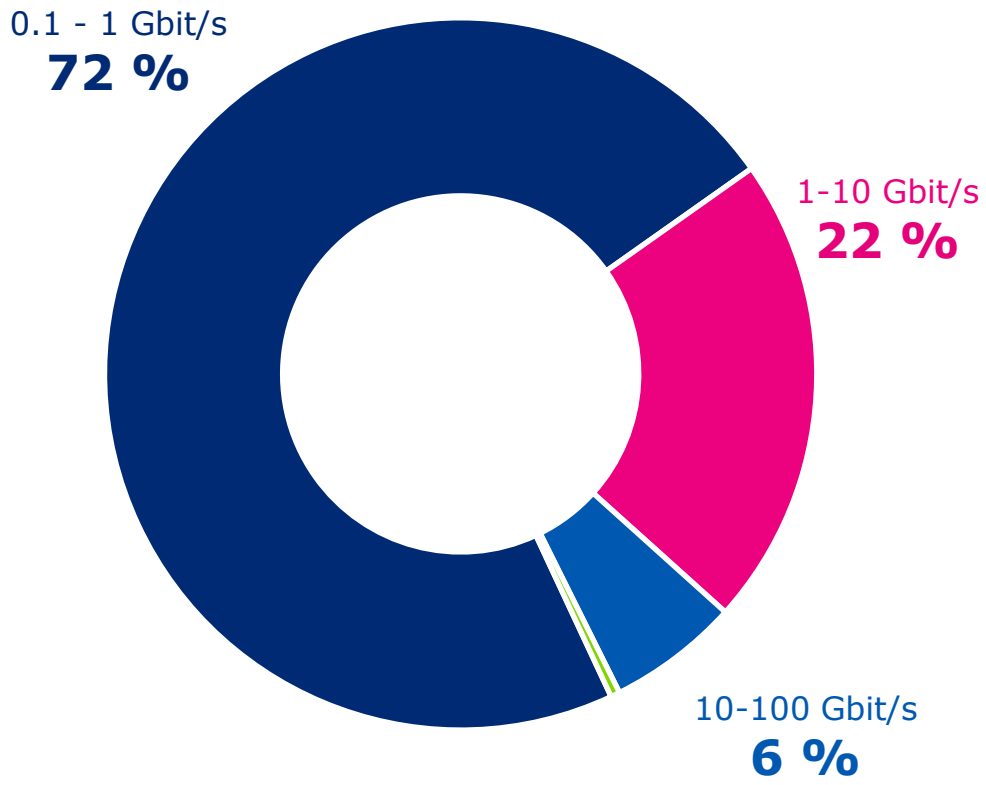
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla



3 kk

Palvelunestohyökkäysten tunnuslukuja
Q3/2023

- **163 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q3/2023.
- Noin 78% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Toimialakohtaiset havainnot

3 kk

	Trendi **3kk**	Edeltävä **3kk**	
Elintarvike			Ilmoitettujen poikkeamien määrä on laskenut. Moni yritys valmistautuu NIS2-direktiivin toimeenpanoon kehittämällä tietoturvallisuuden hallintajärjestelmäänsä.
Energia			Ilmoitettujen poikkeamien määrässä ei merkittäviä muutoksia. Onnistuneiden tietomurtojen tai niiden yritysten määrät lisääntyivät. Kyberturvallisuuden uhkataso on yhä koholla.
Finanssi			Pankkitunnusten kalastelu jatkuu eri muodoissaan. Pankkeihin kohdistuneet palvelunestohyökkäykset eivät aiheuttaneet häiriöitä palveluihin.
Teollisuus			Ilmoitettujen poikkeamien määrä on laskenut etenkin puolustus-, metsä-, ja kemianteollisuudessa. Erityisesti tietomurtojen määrät vähenivät ja ne kohdistuivat lähinnä sähköpostitileihin.
Logistiikka ja liikenne			Toimialaan kohdistunut palvelunestohyökkäyksiä.
Valtionhallinto			Jo vuoden ajan koholla ollut uhkataso näkyy edelleen valtionhallinnossa mm. erilaisina tietojenkalastelukampanjoina ja ajoittaisina palvelunestohyökkäyksinä eri organisaatioihin.
Media			Muutamaan media-alan yritykseen kohdistui palvelunestohyökkäyksiä, joilla ei ollut mainittavia vaikutuksia palveluihin.
SOTE			Ilmoitettujen poikkeamien määrä on laskenut; erityisesti tietomurrot ovat vähentyneet. Euroopassa esiintynyt entistä enemmän sote-palveluihin kohdennettuja kiristyshyökkäyksiä.
Vesihuolto			Ilmoitettujen poikkeamien määrässä ei juurikaan muutoksia; kalastelu- ja huijausyritykset jatkuvat välillä valitettavasti onnistuen.
Kunnat			Hyvin toteutettujen huijausviestien avulla onnistuneita tilimurtoja sekä teknisen tuen nimissä soitettuja huijauspuheluita, joiden yhteydessä saatu pääsy käyttäjän työasemalle. Palvelunestohyökkäyksiä.

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

Tarve kyber-turvallisuuden osaajille

Pula puolijohteista

Tekoälyn käyttö kyberrikolli-suudessa

Suurvalta-kilpailun vaikutukset sääntelyyn

Älylaitteiden elinkaari ja kierrätys

Kyber-vakoilun ja rikollisuuden rajojen hämärtymi-nen

IoT

6G

Kiristyshaitta-ohjelmien käyttö murroksessa

Teknologia osana suurvalta-kilpailua

Sääntelyn ulottuminen uusille toimialoille

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Kiristyshaittaohjelmien käyttö murroksessa

Teknologian ja tietoisuuden kehittyessä myös rikolliset pyrkivät kehittämään omaa toimintaansa ja olemaan askeleen edellä suojauksia.

- Kiristyshaittaohjelmat (eng. ransomware) ovat haittaohjelmia, jotka salaavat tai tuhoavat laitteella olevat tiedostot. Tiedostojen palauttamiseksi pyydetään usein maksamaan lunnaat.
- Lunnaiden maksamista ei suositella. Toisaalta rikolliset voivat myös kiristää uhria uhkaamalla julkaista kiristyshaittaohjelman salaamia tietoja.[8]
  - On mahdollista, että rikolliset julkaisevat tietoja myös siinä tapauksessa, että lunnaat maksetaan.
- Kiristyshaittaohjelmiin varaudutaan perinteisesti huolehtimalla varmuuskopioinnista, mutta on jo nähty viitteitä kiristyshaittaohjelmista, jotka pyrkivät salaamaan tai tuhoamaan myös varmuuskopiot.
  - Esimerkiksi vuoden 2023 aikana julkisuuteen noussut Akira-kiristyshaittaohjelma pyrkii salaamaan virtuaalikoneiden virtuaalisten kiintolevyjen tiedostoja.[8]
- Varmuuskopiot olisikin hyvä säilyttää siten, ettei mahdollinen kiristyshaittaohjelma pääse tuhoamaan niitä.
  - Varmuuskopioiden palauttamista olisi myös hyvä harjoitella tasaisin väliajoin.
- Tutustu Kyberturvallisuuskeskuksen ohjeisiin kiristyshaittaohjelmatapauksen varalle.[9, 10]

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

- Luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi on lähetetty lausuntokierrokselle. Lausuntoja voi antaa Lausuntopalvelu.fi-palvelussa 29.11.2023 asti.[11]
  - EU:n uusi kyberturvallisuusdirektiivi (EU) 2022/2555, eli niin sanottu NIS2-direktiivi annettiin 14.12.2022, ja sen säännökset on pantava täytäntöön kansallisesti 17.10.2024 mennessä.
  - Liikenne- ja viestintäministeriö on johtanut direktiivin täytäntöönpanoa, ja yhdessä sidosryhmien kanssa valmistellut luonnoksen hallituksen esitykseksi.
  - Luonnoksessa ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta, jossa säädettäisiin yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista. Julkishallinnon osalta velvoitteista säädettäisiin myös julkisen hallinnon tiedonhallinnasta annetussa laissa.

Oikeudelliset asiat

- Esityksellä kumottaisiin NIS2-direktiiviä edeltävän verkko- ja tietoturvadirektiivin (2016/1148/EU) täytäntöönpanosäädökset useista sektorikohtaisista laeista.
- Velvoitteiden valvonnassa jatkettaisiin sektorikohtaisesti hajautettua mallia.
- NIS2-direktiivi laajentaa niiden kriittisten toimijoiden joukkoa, joita sen mukaiset kyberturvallisuusvelvoitteet koskevat.
- Direktiivin alaan kuuluvia uusia toimijoita tulee esimerkiksi energian-, terveydenhuollon-, digitaalisen infrastruktuurin-, elintarvikkeiden valmistuksen sekä jätehuollon sektoreille.
- NIS2-direktiivi ja sen toimeenpanemiseksi säädettävä laki kyberturvallisuuden riskienhallinnasta tulevat täsmentämään ja tiukentamaan kriittisten toimialojen kyberturvallisuusvelvoitteita, sekä velvoitteiden noudattamiseen liittyvää viranomaisvalvontaa ja sanktiointia.

Oikeudelliset asiat

- Yango-taksipalvelun tiedonsiirtojen valvonta jatkuu Euroopan tietosuojaviranomaisten yhteistyössä – Yango saa jatkaa toimintaansa Suomessa toistaiseksi.[12, 13]
  - Tietosuojavaltuutetun toimisto sekä Alankomaiden ja Norjan tietosuojaviranomaiset ovat selvittäneet Yango-taksipalvelun toimintaa.
  - Venäjän uuden taksilainsäädännön vuoksi Tietosuojavaltuutettu antoi elokuussa Yandex LLC:lle ja Ridetech International B.V.:lle kiireellisesti väliaikaisen määräyksen keskeyttää Yango-taksipalvelussa kerättyjen henkilötietojen siirron Venäjälle.
  - Silloisen tiedon mukaan lainsäädäntö olisi laajentanut merkittävästi Venäjän turvallisuuspalvelu FSB:n oikeutta saada taksitoiminnassa käsiteltäviä tietoja.
  - Uuden selvityksen perusteella Venäjän uutta taksilainsäädäntöä ei kuitenkaan sovelleta taksien välitystoimintaan Suomessa, joten tietosuojavaltuutettu on poistanut antamansa määräyksen.
  - Päätös ei kuitenkaan tarkoita, että tiedonsiirrot Venäjälle olisivat tietosuoja-asetuksen mukaisia tai että Venäjän tietosuojan taso olisi riittävä, joten selvitystä jatketaan.

Oikeudelliset asiat

- Irlannin tietosuojaviranomainen on määrännyt TikTok Technology Limitedille 345 miljoonan euron seuraamusmaksun yleisen tietosuoja-asetuksen vastaisista käytännöistä lasten henkilötietojen käsittelyssä.[1]
  - Irlannin tietosuojaviranomainen selvitti TikTokin toimintatapoja 13–17-vuotiaiden lasten henkilötietojen käsittelyssä vuoden 2020 aikana. Selvitys kohdistui erityisesti lasten käyttäjätilien ja videoiden yksityisyysasetuksiin sovelluksessa
  - Irlannin tietosuojaviranomainen totesi, että TikTok on rikkonut alaikäisten lasten ja nuorten henkilötietojen käsittelyssä useita tietosuoja-asetuksen säännöksiä. Lapsikäyttäjien tilit oli esimerkiksi asetettu oletusarvoisesti julkisiksi, jolloin julkaisut olivat näkyneet kaikille. Tämä oli muun muassa minimointiperiaatteen ja sisäänrakennetun ja oletusarvoisen tietosuojan vastaista.

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)

Yhteiskunnan kannalta kriittisten organisaatioiden ilmoituslomake: https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx

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) TikTokille 345 miljoonan euron seuraamusmaksu lasten tietosuojaan liittyvistä rikkomuksista https://tietosuoja.fi/-/tiktokille-345-miljoonan-euron-seuraamusmaksu-lasten-tietosuojaan-liittyvista-rikkomuksista
2) Kalastelut ja muut huijaukset kasvoivat räjähdysmäisesti alkuvuonna – pankit saivat estettyä huijauksia lähes 16 miljoonan euron edestä https://www.finanssiala.fi/uutiset/kalastelut-ja-muut-huijaukset-kasvoivat-rajahdysmaisesti-alkuvuonna-pankit-saivat-estettya-huijauksia-lahes-16-miljoonan-euron-edesta/
3) Guide to Operational Technology (OT) Security https://csrc.nist.gov/pubs/sp/800/82/r3/final
4) China, North Korea pursue new targets while honing cyber capabilities https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/
5) Kyberturvallisuuskeskuksen viikkokatsaus - 36/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-362023
6) Kyberturvallisuuskeskuksen viikkokatsaus - 38/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-382023
7) Kyberturvallisuuskeskuksen viikkokatsaus - 37/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-372023

Lähdeluettelo

8) Kyberturvallisuuskeskuksen viikkokatsaus - 24/2023
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-242023
9) Toimintaohje – Kiristyshaittaohjelma
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf
10) Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toiminta%20kiristyshaittaohjelmatilanteessa%20-%20johdon%20ohje.pdf
11) Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi
https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd
12) Yango-taksipalvelun tiedonsiirtojen valvonta jatkuu Euroopan tietosuojaviranomaisten yhteistyössä – Yango saa jatkaa toimintaansa Suomessa toistaiseksi https://tietosuoja.fi/-/yango-taksipalvelun-tiedonsiirtojen-valvonta-jatkuu-euroopan-tietosuojaviranomaisten-yhteistyossa-yango-saa-jatkaa-toimintaansa-suomessa-toistaiseksi
13) Tietosuojavaltuutetun päätös ei ota kantaa tiedonsiirtojen lainmukaisuuteen Venäjälle – asian tutkinta ei pääty
https://tietosuoja.fi/-/tietosuojavaltuutetun-paatos-ei-ota-kantaa-tiedonsiirtojen-lainmukaisuuteen-venajalle-asian-tutkinta-ei-paaty