TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Kybersää

Lokakuu 2021

# #kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tämä tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

vakava

TRAFICOM

# Kybersää lokakuu 2021

## Tietomurrot ja -vuodot

- Twitch-palvelussa tietomurto, jonka seurauksena palvelun kriittisiä tietoja pääsi vuotamaan.
- Argentiinan valtiolliseen tietojärjestelmään tehtiin tietomurto ja kymmenien miljoonien kansalaisten tiedot päätyivät rikollisten käsiin.

## Huijaukset ja kalastelut

- Pankkitunnuksia on lokakuussa kaapattu erittäin aktiivisesti.
- Sähköpostihuijauksien lisäksi tunnuskalasteluun houkutellaan myös tekaistuilla tekstiviesteillä.

## Haittaohjelmat ja haavoittuvuudet

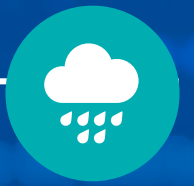
- QakBot-haittaohjelmaa levitetään aktiivisesti.
- Tietoturva Nyt!-artikkeli: Riippuvuusristiriidat (dependency confusion) altistavat yrityksiä hyökkäyksille.

## IoT ja automaatio

- IoT:n ja automaation kyberturvallisuusteen liittyvät strategiat ja ohjeistukset lisääntyvät ja kertovat kasvavasta tietoisuudesta aihepiirin tärkeydestä

## Verkkojen toimivuus

- 10 merkittävää toimivuushäiriötä
- Osa toimivuushäiriöistä johtui erilaisista muutostöistä tai konfiguraatiovirheistä.
- Kuntasektori raportoi koulujen osoitteisiin tehdyistä palvelunestohyökkäyksistä, joilla on ollut myös välillistä vaikutusta muihin palveluihin.



## Vakoilu

- Teleoperaattorit kiinnostavat kybervakoojia: LightBasin ryhmä on tunkeutunut lukuisten teleoperaattoreiden järjestelmiin maailmalla.
- NOBELIUM hyödynsi IT-palvelutoimittajien ylläpitotunnuksia niiden asiakasorganisaatioihin tunkeutumisessa.

TRAFICOM

# Kuukauden tunnuslukuja

**~270%**

Lokakuun säätä synkensi pankkikalastelut. Olemme saaneet huomattavasti paljon enemmän pankkikalasteluilmoituksia ajalla 1-10/2021 kuin 1-10/2020. Suomessa on 2021 vuoden aikana ollut useampia aktiivisia kampanjoita.

**27.10.**

Julkaisimme varoituksen Omakannan ja Suomi.fi-palvelun nimissä tehtävistä pankkitunnusten kaappausyrityksistä

**1**

Euroopan kyberturvallisuuskuukausi pyrki lokakuun ajan lisäämään tietoisuutta kyberturvallisuudesta. Viranomaiset ja organisaatiot jakoivat paljon tietoa aiheesta. Muistetaan jatkaa tärkeää työtä myös kaikkina muina kuukausina!

TRAFICOM

# Julkaisimme varoituksen 3/2021 Huijarit kaappaavat pankkitunnuksia Omakannan ja Suomi.fi-palvelun nimissä

- Julkaisimme keltaisen varoituksen 27.10.2021.
- Omakannan ja Suomi.fi-palvelun nimissä pyritään varastamaan käyttäjien pankkitunnuksia sähköpostiviesteissä olevia väärennettyjä linkkejä käyttäen.
- Mikäli käytät palvelua selaimella, kirjaudu palveluun aina kirjoittamalla osoitekenttään palvelun koko osoite. Myös mobiilisovellusta käyttämällä vältyt pankkitunnusten kalastelulta.
- Tässä tietojenkalastelukampanjassa on samoja piirteitä kuin aiemmin ilmoittamassamme pankkikalastelussa. Käytetyt viestityyppit ja toimintamallit vaikuttavat samalta. Vaikuttaa siltä, että tekijät ovat vaihtaneet pankkien nimet Omakannan ja Suomi.fi-palveluiksi.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/huijarit-kaappaavat-pankkitunnuksia-omakannan-ja-suomifi-palvelun-nimissa

# Tietoturva 2021 - virtuaaliseminaari

- Mitä? Kyberturvallisuuskeskuksen vuosittainen tietoturva seminaari. Tänä vuonna juhlistamme 20 vuoden taivalta ja tarkastelemme seminaarissa kyberturvallisuutta yhteiskunnan toimivuuden ja huoltovarmuuden perustana sekä kerromme esimerkein, miten kyberturvallisuus rakennetaan tiiviissä yhteistyössä viranomaisten, yritysten ja kolmannen sektorin kanssa.
- Milloin? 24.11.2021 klo 11-15
- Missä? Siellä missä sinä olet! Hyppää siis mukaan virtuaaliseminaariin.
- Tutustu ohjelmaan ja ilmoittaudu: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2021-virtuaaliseminaari


TRAFICOM

# **Top 5 kyberuhat** - merkittävät pidemmän aikavälin ilmiöt

## 1

**Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon.** Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

## 2

**Käyttäjätunnukset ovat organisaation arvokasta tietoa** Käyttäjätunnusten kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle.

## 3

**Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta.** Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

*Symbolit*

*Uusi*

*Päivitetty*

## 4

**Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät.** Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

## 5

**Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää.** Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

TRAFICOM

# 1. Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon

Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- Haavoittuvuus tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, prosesseissa, kotiautomaatiossa tai niitä voi aiheutua ihmisten toiminnan seurauksena.
- Vuonna 2020 siirryttiin kiireen vilkkaa etätyö-moodiin. Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.
- Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja tunnistavat kohteet, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- Valtiolliset toimijat ovat tyypillisesti ensimmäisten joukossa hyödyntämässä uusia haavoittuvuuksia kybervakoiluun ja vaikuttamiseen. Valtiollisilla toimijoilla on myös riittävät resurssit päivitysten takaisinmallintamista varten uusien hyökkäysten mahdollistamiseksi kriittisissä ohjelmistoissa.

**CASE**

Atlassian Confluence Server ja Data Center -tuotteista löydettyä haavoittuvuutta (CVE-2021-26084) hyväksikäyttämällä hyökkääjä pystyi suorittamaan etänä omaa ohjelmakoodiaan palvelimella ilman tunnuksia. Poikkeavan tapauksesta tekee se, että valmistaja julkaisi päivitykset ja ilmoitti alustavasti, ettei haavoittuvuus ollut kriittinen. Aluksi arvoitiin, että järjestelmään pääsemiseksi tarvitaan käyttäjätunnus. Kaksi päivää myöhemmin havaittiin, että tunnuksia ei tarvita lainkaan, vaan haavoittuvuuden hyväksikäyttö on helpompaa. Tästä syystä valmistaja muutti haavoittuvuuden arvion kriittiseksi.

TRAFICOM

# 2. Käyttäjätunnukset ovat organisaation arvokasta tietoa

Käyttäjätunnusten kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

- Tunnuskalastelua tehdään monella eri tavalla ja eri laitteiden kautta. Sitä kohdistetaan organisaatioihin kuin yksityishenkilöihin. Se on helppoa ja yksinkertaista, jolla saadaan merkittävää hyötyä.
- Tunnuksia pyritään myös arvaamaan koneellisesti (password spray tai brute force) tai hyödyntämään erilaisia salansanatietovuotoja.
- Organisaation tietoturva tulee olla ratkaistuna niin, että teknisten kontrolleiden tulee estää ja havaita tunnusten väärinkäytökset. Siksi on tärkeää, että esimerkiksi kaksi- tai monivaiheinen tunnistautuminen on käytössä.
- Tunnusten ja oikeuksien käytöstä tulee kertyä riittävän tarkkaa lokia, jota analysoidaan poikkeamien varalta. Lokien tulee olla myös riittävän pitkään (esim. 6kk) käytössä jälkikäteen tehtävän selvittelyn vuoksi.

**CASE**

Microsoftin mukaan valtion tukemat hakkeriryhmät tavoittelevat käyttäjien salasanoja ja tunnuksia hyödyntäen nk. password spray menetelmää. Se on hyökkääjälle tehokas ja vähän resurssia vaativa keino. Microsoft arvioi, että yli kolmasosa tilien vaarantumisesta on password spray-hyökkäyksiä, vaikka tällaisten hyökkäysten onnistumisprosentti tilien kohdalla on 1 %, elleivät organisaatiot käytä teknisiä kontrolleja, joiden avulla voidaan estää ja havaita tunnusten käyttö. Havaintomme mukaan myös suomalaisiin organisaatioihin kohdistuu password spray-hyökkäyksiä

TRAFICOM

# 3. Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta

Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

- Erityisen merkittävä uhka on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen high tech -jättiin.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Toiminta on aktiivista ja kehittyy jatkuvasti.

**CASE**

Palvelunestohyökkäyksillä kiristäminen nousi maailmalla ilmiönä loppu-vuodesta 2020 ja ilmiö rantautui myös Suomeen. Kyberturvallisuuskeskus on saanut ilmoituksia myös vuonna 2021 aiheeseen liittyen.

Yleisesti organisaatio vastaanottaa kiristysviestin sähköpostitse, joka on allekirjoitettu näennäisesti tunnettujen haitallisten toimijoiden nimissä. Kiristysviestin lähettämisen aikoihin on joissain tapauksissa tehty myös palvelunestohyökkäys viestin tehostamiseksi. Viestissä kerrotaan organisaation kohtaavan suuren palvelunestohyökkäyksen, mikäli lunnaita ei makseta. Ohjeemme on ja pysyy: älä maksa kiristäjille.

TRAFICOM

# 4. Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät

Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

- Pilvipalveluratkaisuiden hahmottaminen on vaikeaa, koska ympäristö on laaja. Siirtyminen pilveen on jäänyt puolitiehen ja tietojärjestelmien migraatio on jäänyt viimeistelemättä. Vanhoja palveluita voidaan edelleen hyväksikäyttää.
- Aivan kuten perinteisessä tietoverkossa, mikäli hyökkääjä onnistuu pääsemään pilven reunalle, voi sen kautta levittäytyä myös organisaation muihin verkon segmentteihin pilven ulkopuolellakin.
- Tarve kehittää yleisesti hyväksytyt tietoturvavaatimukset pilvipalveluille.
- Suomessa pilven tietoturvavaatimuksia on lähestytty esim. PITUKRI https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkosivuiltamme-neuvoja-pilvipalveluiden-turvalliseen-kayttoon

**CASE**

Alkuvuonna 2021 laajamittainen Microsoft Exchange -sähköpostipalvelimien tietomurtoaalto pyyhkäisi myös Suomen yli. Tietomurtoaaltoa tutkittaessa paljastui, että kaikilla pilvipalveluiden käyttöön siirtyneillä organisaatioilla oli edelleen käytössään myös murrettavissa oleva perinteinen Exchange-sähköpostipalvelin. Osalla palvelin oli edelleen jossain marginaalisessa käytössä ja osalla se oli yksinkertaisesti unohdettu sulkea pilvimigraation lopuksi. Kaikkiin palvelimiin kuitenkin murtauduttiin. Tapaus on surullinen esimerkki siitä, kuinka loppumetreillä kesken jäänyt teknologiamuutos jättää ovet auki hyökkääjille.

TRAFICOM

# 5. Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

- Organisaatiot ostavat yhä enemmän palveluita ulkoisilta palveluntarjoajilta.
- Organisaatioiden olisi keskeistä ymmärtää omat alihankkijaketjunsa. On tärkeä ymmärtää kolmannen osapuolen tietoturvan taso. Esimerkiksi:
  - Konsultit ja heidän oman organisaation sisäiset järjestelmät.
  - Laitteistot ja palvelut joita voidaan käyttää joko osana omaa tuotetta tai palvelukokonaisuutena, tai ostettuna palveluna.
  - Organisaation tulee ymmärtää alihankinnanketju, myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- Organisaation tulisi kartoittaa, mistä osista sen eri palvelut muodostuvat, jotta ison kokonaisuuden voi hahmottaa. Erityisesti hankintavaiheessa tällaisen tekeminen on oleellista.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos (kyber)turvallisuutta ei ole huomioitu.

**CASE**

Viime joulukuussa paljastunut Yhdysvaltojen hallintoon ja lukuisiin yrityksiin iskenyt SolarWinds-hyökkäys on merkittävä tietoturvatapaus. Tietomurron ja vakoilun mahdollistanut takaovi onnistuttiin levittämään tuhansiin organisaatioihin, joita oli myös Suomessa. Erilaiset toimitus- ja alihankintaketjut voivat mahdollistaa hyökkääjille keinon päästä huomaamattomammin varsinaiseen kohteeseensa tai saamaan samalla kertaa pääsyn laajaan kohdejoukkoon.

TRAFICOM

# Tietomurrot ja -vuodot

Tietomurroissa ja -vuodoissa käsitellään suojauskeinoja sekä tietoomme tulleita trendejä tietomurroista ja –vuodoista. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita sekä mainetappioita.

TRAFICOM

# Tietomurrot ja -vuodot

- Twitch-palvelussa tietovuoto
  - Reaaliaikaiseen suoratoistoon eli streamaukseen laajalti käytetty Twitch-palvelu oli tietomurron kohde.
  - Tietovuoto sisältää eri lähteiden mukaan esimerkiksi Twitchin lähdekoodin, tietoa streamaajille maksetuista palkkioista sekä käyttäjien nimiä.
  - Twitch kirjoittaa omassa julkaisussaan, että tiedot vuosivat internetiin palvelimen konfiguraatiomuutoksessa sattuneen virheen takia.
  - Tekijät ovat julkaisseet osan halussaan olevista tiedoista. He ilmoittivat, että julkaistu osa oli ensimmäinen erä ja toinen osa tiedoista olisi tuloillaan. Tämä uhka ei ole kuitenkaan vielä realisoitunut.
  - Useista lähteistä saatujen tietojen mukaan kyseinen vuoto ei sisällä loppukäyttäjien tietoja, kuten salasanatietoja tai maksukorttitietoja.

**Analyysi**

- Kyberhyökkäykseen reagointia kannattaa harjoitella, jotta oikeassa tilanteessa toimintatavat ovat tuttuja.
- Kyberhyökkäys voi pahimmillaan lamauttaa liiketoiminnan kokonaan.
- Vaikka tässä tietovuodossa ei raporttien mukaan vuotanutkaan käyttäjätunnuksia tai salasanoja on silti aina suositeltavaa vaihtaa tietovuodon kohteena olleen palvelun salasana ja asettaa monivaiheinen tunnistautuminen.

TRAFICOM

# Tietomurrot ja -vuodot

- Maailmalla uutisoitiin isoista tietomurroista
  - Argentiinan valtion viraston tietojärjestelmään murtauduttiin ja murtautujat saivat haltuunsa kaikkien Argentiinan kansalaisten henkilötunnistetiedot.
    - Tietojen joukossa olivat ainakin kansalaisten etu- ja sukunimi, kotiosoite, henkilökortin voimassaolopäivämäärät sekä kansalaisten kuvat.
    - Argentiinan populaation koko on yli 45 miljoonaa ja suurimmalla osalla on ollut tietonsa tässä kansallisessa rekisterissä.
  - Syniverse kertoi, että sen järjestelmissä on käyty useita kertoja ulkopuolisen tahon toimesta vuodesta 2016 alkaen.
    - Syniverse tarjoaa viestintäpalveluita useille muille organisaatioille kuten Verizon ja AT&T.

**Analyysi**

- Tietomurtojen ja –vuotojen osalta ilmoitusmäärät Kyberturvallisuuskeskukselle olivat lokakuussa maltillisia.
- Saimme lokakuun aikana 48 ilmoitusta, joissa tapaustunniste oli joko tietomurto tai –vuoto.
- Heinäkuussa vastaavia ilmoituksia tuli 72, elokuussa 62 ja syyskuussa 75.

TRAFICOM

# Huijaukset ja kalastelut

Huijauksiin ja tietojenkalasteluun sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyksiä ja muita vastaavia huijauksia. Lisäksi organisaatioihin voi kohdistua pankkitunnuskalastelua, maksukorttikalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.

# Huijaukset ja pankkikalastelut

- Pankkikalastelurintamalla synkkä lokakuu
  - Lokakuun tietojenkalastelutilannetta on synkistänyt laajana ja aktiivisena jatkunut pankkitunnusten kalastelu.
  - Melkein kaikkien kotimaisten pankkien nimissä on lähetetty sähköposteja, joissa käytetty huijausteema vaihtui tiheästi.
  - Tyypillisesti huijauksissa peloteltiin uhria umpeutuvilla pankkipalveluilla tai viranomaisviesteillä.
  - Viestin linkki johtaa pankin kirjautumissivuston näköiselle kalastelusivulle, jonne syötetyt pankkitunnukset päätyvät rikollisten haltuun.
  - Kalastelu on ollut tehokasta ja rikolliset ovat saaneet paljon rikoshyötyä.
  - Pankkien lisäksi huijausviestejä on tekaistu myös Kelan ja Kanta-palvelun ja Otavan nimissä. Niissäkin olleet linkit johtavat pankkitunnistautumisen näköisille sivuille eli taas pankkitunnusten kalasteluun.

**Analyysi**

- Verkkopankkien lisäksi Omakannan hakutuloksia on väärennetty joihinkin hakukoneisiin. Selaimen osoitesivulle syötetty pelkkä pankin nimi tai vaillinainen verkko-osoite ei johdakaan oikealle verkkosivulle, vaan rikollisen väärentämään hakutulokseen.
- Väärennetty sivu voi näyttää pankin tai Omakannan oikealta kirjautumissivulta, mutta sinne syötetyt kirjautumistiedot menevät rikolliselle.
- Rikollinen syöttää hakukoneisiin linkkejä joko optimointimekanismeilla tai ostamalla hakukoneesta mainostilaa.

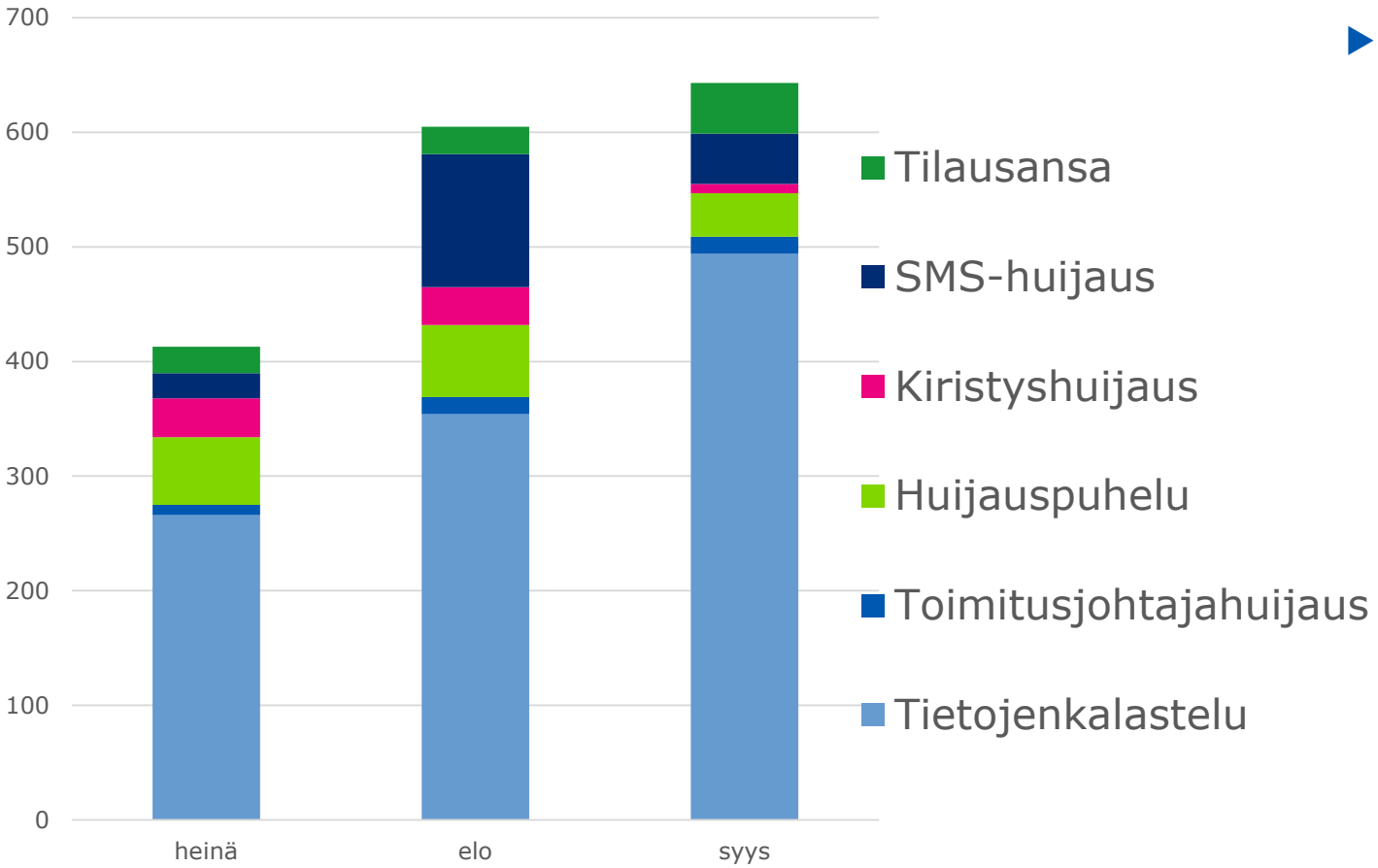
# Huijaukset ja tietojenkalastelut

- Tietojenkalastelulla pyritään rahalliseen hyötyyn
  - Tori.fi-myyntipalstan käyttäjiä huijarit ovat lähestyneet WhatsApp-viesteillä eri verukkeilla, kuten PostNordin nimissä.
  - Näillä huijausviesteillä on pyritty kalastelemaan mm. luottokorttitietoja.
  - Myös DHL:n nimissä kalastellaan luottokortteja.
- Amerikkalaisen huijauksen harhalaukauksia
  - Yhdysvalloissa on liikkunut huijaustapaa, jossa uhrille lähetetään väärennetty tilausvahvistus Norton antivirus -tuotteesta.
  - Tilausvahvistuksessa houkutellaan soittamaan väärennettyyn asiakaspalveluun, jossa uhria yritetään laskuttaa perusteettomasti.
  - Huijaustapa tuskin Suomessa tuottaa tulosta, mutta huijausviestejä on silti tullut Suomeenkin.

**Analyysi**

- Verkon kirpputoreilla ja myyntipaikoilla on raportoitu automatisoituja huijauksia.
- Osto-, myynti-, tai vuokraus-ilmoituksen laatineita käyttäjiä on lähestytty WhatsApp-viesteillä, jossa huijari väittää kiinnostuneensa ilmoituksen kohteesta ja olevansa valmis kauppoihin.
- Huijarin lähettämässä WhatsApp-viestissä on linkki, joka johtaa väärennetyille Postin sivuille.
- Väärennetyllä sivulla uhrilta kalastellaan maksukorttitietoja ja pankkitunnuksia.

# Käsiteltyjä huijaustapauksia Q3/2021




- Vuoden 2021 kolmannen neljänneksen ilmiöitä ovat:
  - Tietojenkalastelutapauksia on ilmoiteltu Kyberturvallisuus-keskukselle syksyn alettua merkittävästi kesää enemmän.
  - Tietojenkalasteluun pankkitunnusten kalastelu on aiheuttanut tasaista kasvua. Syyskuussa pankkikalasteluita ilmoitettiin 30 % enemmän kuin kesäkuukausina.
  - Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.

# Haittaohjelmat ja haavoittuvuudet

Haittaohjelmissa ja haavoittuvuuksissa käsitellään aihealueen merkittävimmät julkaisut ja havainnot sekä annetaan toimenpidesuosituksia ja linkkejä lisätietoihin.

TRAFICOM

16.9.2021

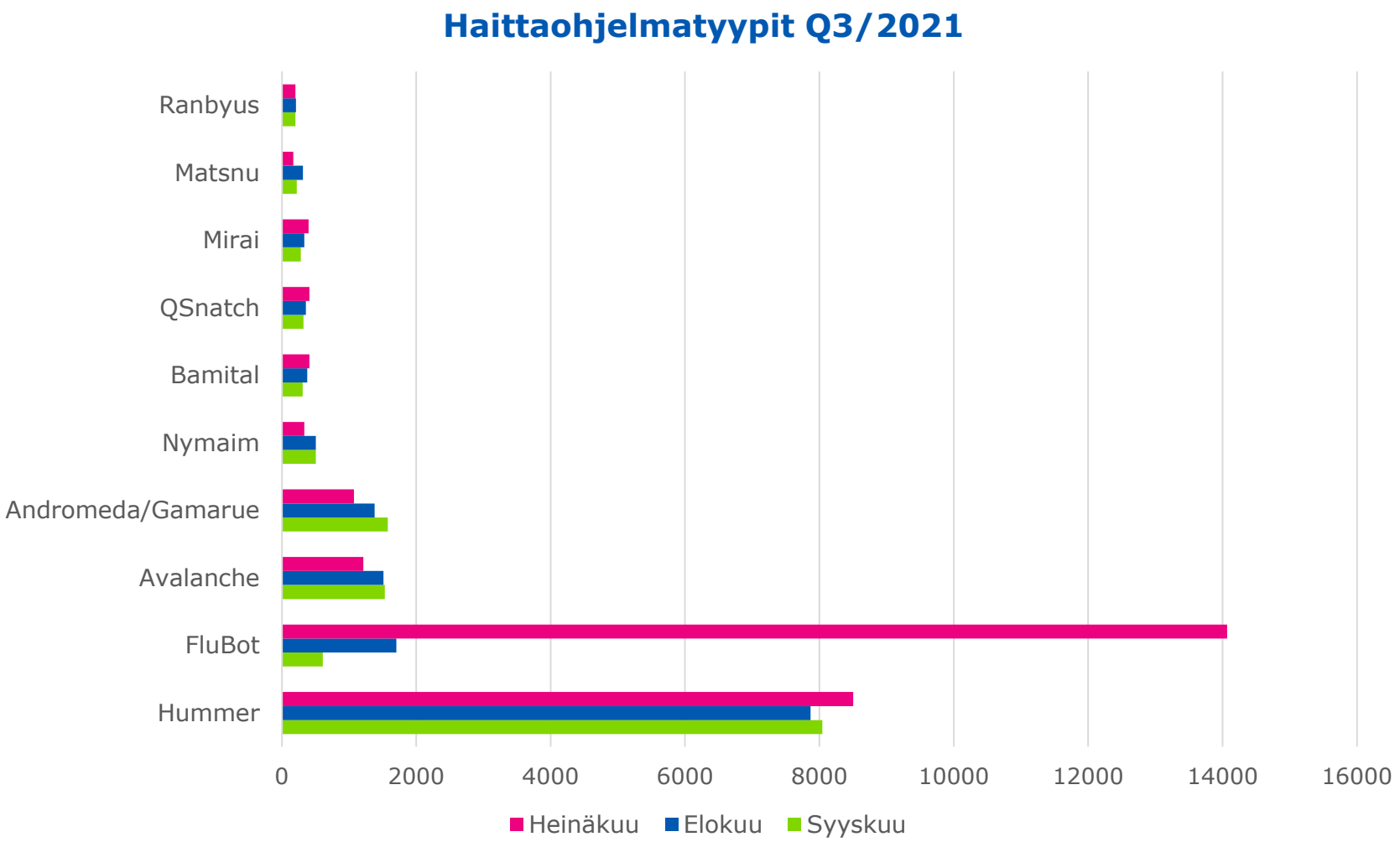
# Haittaohjelmat

- Olemme saaneet ilmoituksia QakBot-haittaohjelman levityksestä
  - QakBot on tietoja varastava troijalainen, joka kykenee myös levittämään muita haittaohjelmia saastuneisiin laitteisiin.
  - Haittaohjelmaa levitetään samalla mallilla kuin 2020 Suomeen iskenyttä Emotet-haittaohjelmaa.
    - Jollakin tavalla varastettuun postikeskusteluun tulee väärennetystä lähteestä uusi viesti, jossa pyydetään lataamaan tiedosto.
    - Tiedostosta uhrin Windows-laitteeseen tarttuu QakBot-haittaohjelma.
  - Osana ilmiötä on nähty myös jalansijaa muille haittaohjelmille tarjoava Squirrelwaffle-haittaohjelma, joka levittää uhrien koneelle mm. QakBot- ja/tai Cobalt Strike–haittaohjelmaa.
    - Squirrelwaffle leviää sähköpostitse linkkien tai liitteiden kautta.

**Analyysi**

- Squirrelwafflea pidetään Emotet-haittaohjelman seuraajana.
- Squirrelwafflen levitysyritykset ovat lisääntyneet merkittävästi syyskuun 2021 aikana.
- Sähköpostin liitteiden avaamisen, lataamisen ja makrojen suorittamisen kanssa tulee olla valppaana.

# 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. Niistä voi lukea tarkempia tietoja kotisivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

Katso lisää tilastoja:
https://www.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot

# Haavoittuvuus

- Riippuvuusristiriidat altistavat hyökkäyksille
  - Aiemmin tänä vuonna julkaistun raportin mukaan tutkija onnistui tunkeutumaan esimerkiksi Applen ja Microsoftin järjestelmiin ujuttamalla niihin omia ohjelmistopakettejaan.
  - Organisaatioissa käytössä olevat tiedostot, ohjelmistot ja järjestelmät muodostavat monimutkaisia ja pitkiä ketjuja.
  - Mikäli näiden toimitusketjujen riskejä halutaan aidosti hallita on syytä myös tietää millaisista osista nämä erilaiset ketjut koostuvat.
  - Riippuvuusristiriitoja voi syntyä, kun saman nimisiä paketteja löytyy sekä yrityksen sisäisistä jakeluista että heidän käyttämistään ulkoisista jakelukanavista.
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riippuvuusristiriidat-altistavat-hyokkayksille

**Analyysi**

- Yrityksien sisäisissä ohjelmistoissa käytetään kirjastoja, joista osa on tarkoitettu vain yrityksen sisäiseen käyttöön.
- Näitä kirjastoja jaellaan sisäisesti, eikä julkaista avoimena lähdekoodina julkisiin palveluihin.
- Samanniminen paketti yrityksen sisäisessä kirjastossa ja julkisessa palvelussa voi johtaa niiden sekoittumiseen siten, että julkisen palvelun paketti korvaa sisäisessä käytössä olevan kirjaston osan.

# Kuukauden haavoittuvuusjulkaisut

- Win32k-komponentissa aktiivisesti hyväksikäytetty haavoittuvuus (32/2021)
  - Tämä ei ole etänä hyväksikäytettävä haava, jolla rikolliset tulevat sisään, vaan kyseessä on ns. II-vaiheen haava.
  - Haava ei auta tunkeutumaan järjestelmään, vaan sitä käytetään hyökkäyksen myöhemmässä vaiheessa järjestelmässä etenemiseen.
- Oraclen lokakuun 2021 kriittiset korjaukset (33/2021)
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

**Analyysi**

- Päivitykset tulee asentaa viipymättä, haavoittuvuuksien hyväksikäyttö on todella nopeaa.
- Päivityssyklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksikin aikaa.
- Organisaation sisällä viestiminen on tärkeää, jotta työntekijät eivät lykkää omien päivitystensä asentamista tarpeettomasti.

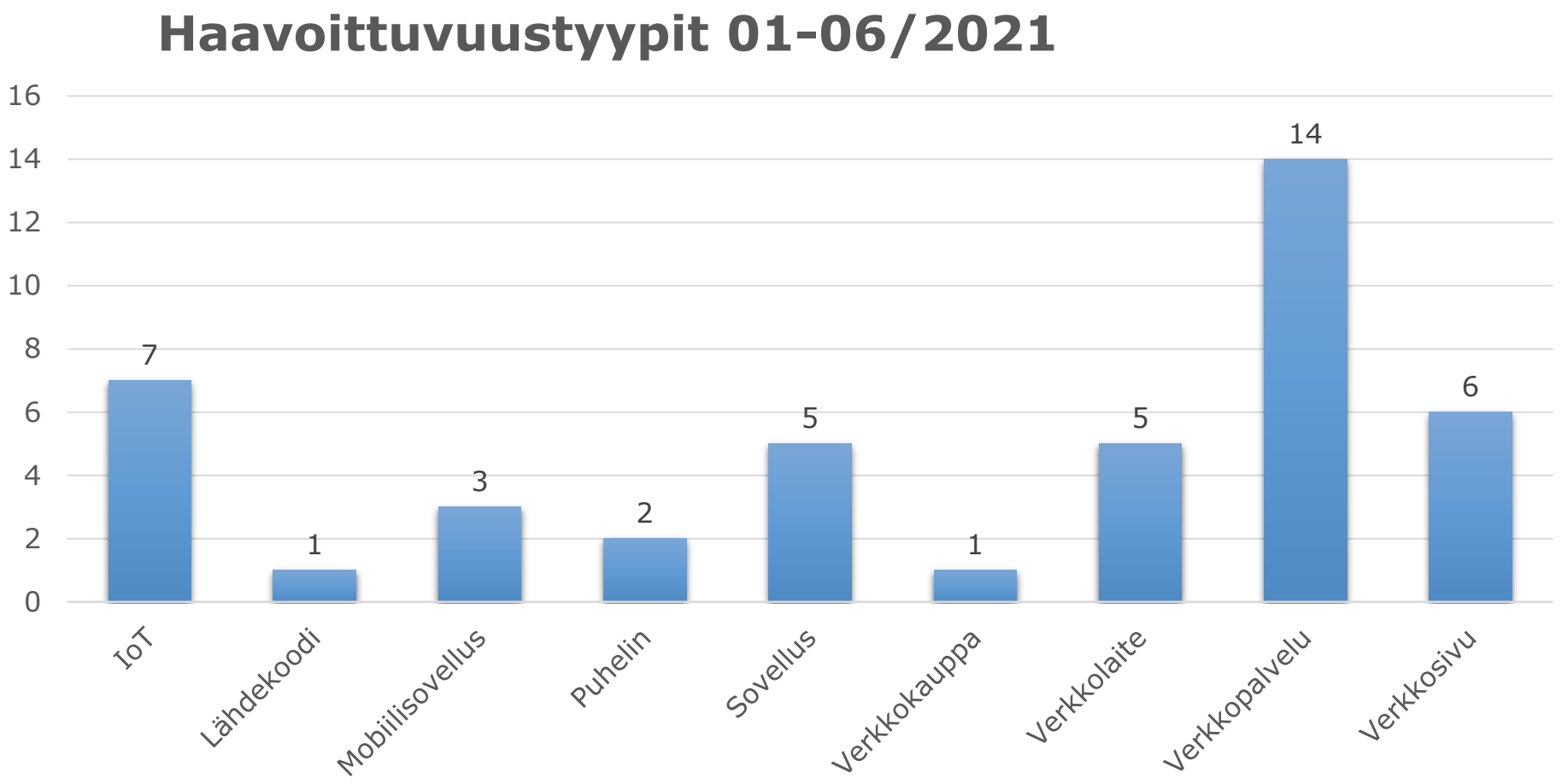
# Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta
- **Haavoittuvuustiedotteita tänä vuonna 33 kpl (tilanne 9.11.2021)**
  - Mukana mm. Microsoft Exchange Server ja etäkäyttötoteutusten haavoittuvuudet
- **Tilaamalla haavoittuvuuskoosteen saat tietoa erilaisista haavoittuvuuksista**
  - Kaikista haavoittuvuuksista ei julkaista suomenkielistä haavoittuvuustiedotetta
  - Kooste julkaistaan lähes päivittäin ja sen voi tilata kotisivuiltamme https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

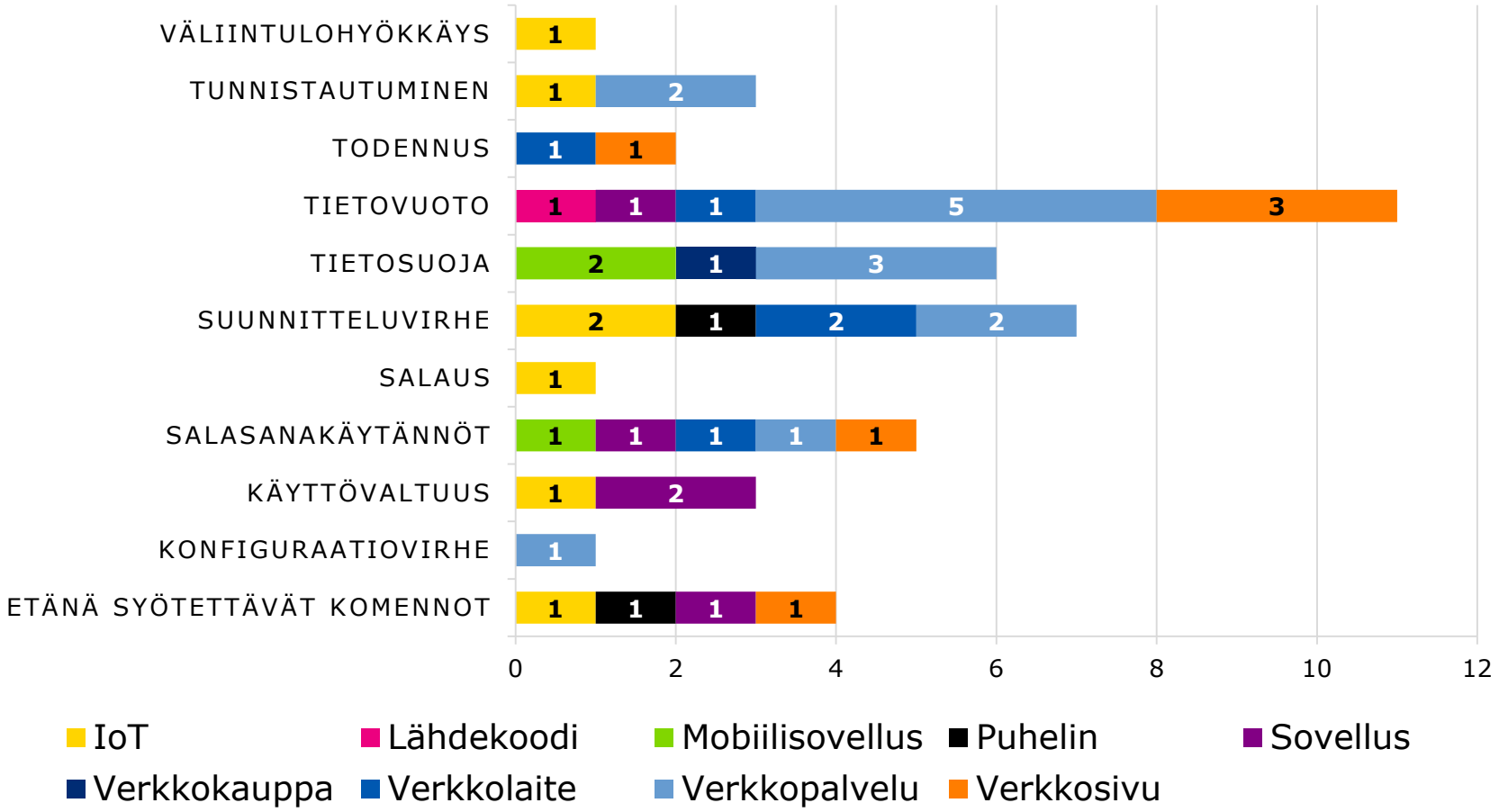
# Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat usein toistuva ongelma. Voi olla, että muutoin tietoturvallisesta tuotteesta löytyy kovakoodattu oletussalasana. Erilaisissa verkkopalveluissa voi myös olla parannettavaa salasanakäytännöissä esim. salasanan vaatimusten vai vaihto-ominaisuuksien osalta.
- IoT- ja verkkolaitteiden testaus on yleistä tietoturvatutkijoiden keskuudessa. Laitteiden turvallisuuden parantaminen on tärkeää verkossa ja kotona käytössä olevien laitteiden määrien jatkuvan kasvun vuoksi.
- Kyberturvallisuuskeskus saa haavoittuvuuksista ilmoituksia laidasta laitaan. Mikäli sinä tai organisaatiosi tarvitsette apua haavoittuvuuden löytyessä, haavoittuvuuden koordinoinnissa tai esimerkiksi CVE-tunnisteen haussa – olettehan yhteydessä Kyberturvallisuuskeskukseen.
- https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

# Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

# Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio




Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuodelta 2021.

Tutustu aiheeseen tarkemmin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

# Automaatio ja IoT

Automaatio-osiossa ilmiöseurantaryhmä seuraa alan uutisia ja ilmiöitä maailmalla ja kotimaassa. Automaatiojärjestelmiä käytetään ohjaamaan sekä monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.

TRAFICOM

# Kansallisten kyberturvallisuus-strategioiden kehitys

- Suomen kanssa lokakuun alussa IoT-tietoturvamerkkien vastavuoroisesta tunnustamisesta sopimuksen tehnyt Singapore on julkaissut uuden Kyberturvallisuusstrategiansa
  - Strategia on rakennettu kolmen kantavan kokonaisuuden varaan. Nämä tähtäävät kriittisen infrastruktuurin resilienssin lisäämiseen, kyberavaruuden turvaamiseen ja kansainvälisen yhteistyön lisäämiseen
  - https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021
- Myös muilla mailla on strategioita, jotka ottavat kantaa kriittisen infrastruktuurin automaatioon: esimerkiksi Tanska on luonut toimialakohtaiset kyberturvallisuusstrategiat

**Analyysi**

- Eri toimialojen digitalisointi ja sen vaikutukset huoltovarmuuskriittisen infrastruktuurin toimintaan ja siihen liittyviin riskeihin ovat luoneet kansallisia varautumistarpeita
- Erilaiset kansallisen tason strategiat kuvaavat sitä, että valtiojohto on havahtunut kyberturvallisuuden merkittävyyteen yhteiskunnan kriittisten toimintojen järjestämisessä

TRAFICOM

# Automaatio - Rakentaminen

- Motiva on julkaissut artikkelin taloautomaatiosta ja siihen liittyvistä kyber- ja tietoturvallisuusnäkökulmista
  - https://www.motiva.fi/ajankohtaista/artikkelit/artikkelit_2021/energiansaastoa_ja_helpotusta_arkeen_taloautomaatiolla.17964.news

**Analyysi**

Kiinteistöautomaatio tarjoaa lukuisia keinoja parantaa mm. rakennusten asumismukavuutta. Kiinteistöautomaatiojärjestelmät pitää suojata samalla kuten muukin Internetiin kytketty elektroniikka.

Suojaamattomat kiinteistöautomaatiolaitteet luovat riskejä, jotka pahimmillaan aiheuttavat mittavia rahallisia kustannuksia.

# Automaatio - Rakentaminen

- Kyberturvallisuuskeskus kartoittaa vuosittain suojaamattomia automaatiolaitteita Suomen tietoverkoista. Työn tavoitteena on parantaa tilannekuvaa ja kyberturvallisuutta Suomessa. Tänä vuonna kartoitus toteutettiin viikkojen 43-44 aikana. Aikaisempien vuosien kartoituksissa havaituista suojaamaattomista automaatiolaitteista suurin osa on ollut rakennusautomaatiolaitteita.
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kartoitus2021
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

**Analyysi**

Puutteellinen rakennusautomaatio-laitteiden suojaus altistaa kyberuhille. Kyberturvallisuus-keskus pyytää ottamaan rakennusautomaation suojauksiin liittyvät asiat esille esimerkiksi asunto-osakeyhtiöiden vuosikokouksissa.

Isännöitsijät ja muut kiinteistöjen ylläpidon ammattilaiset ovat avainasemassa tiedottamaan myös tietoturva-uhista asiakkaitaan. Laitteistojen suojaamiseen saa apua esimerkiksi laitevalmistajien tai laitteen jälleenmyyjien kautta.

TRAFICOM

# IoT

Lokakuu oli EU:n kyberturvallisuuskuukausi, jossa yhtenä teemana oli kuluttajien ja kotien IoT

- Kampanjan yhteydessä julkaistiin ohjeistuksia älykotien turvalliseen käyttöön. Kyberturvallisuuskeskus työskentelee aktiivisesti kuluttajien tietoturvatietoisuuden parantamiseksi mm. luomansa Tietoturvamerkin avulla.
  - https://cybersecuritymonth.eu/resources/top-tips-to-make-your-home-cyber-safe
  - https://cybersecuritymonth.eu/resources/be-cyber-secure-at-home-episode-1
  - https://cybersecuritymonth.eu/resources/be-cyber-secure-at-home-episode-2
  - https://cybersecuritymonth.eu/resources/be-cyber-secure-at-home-episode-3

TRAFICOM

# Verkkojen toimivuus

Verkkojen toimivuus -osassa käsitellään yleisten viestintäpalveluiden merkittäviä toimivuushäiriöitä Suomessa, muiden ICT-palveluiden huomattavia häiriöitä Suomessa ja maailmalla, sekä palvelunestohyökkäyksiä Suomessa ja maailmalla.

TRAFICOM

# Verkkojen toimivuus

- Lokakuussa yleisissä viestintäpalveluissa oli 10 merkittävää toimivuushäiriötä. Häiriöiden kohteet ja syyt vaihtelivat.
  - Vakavuusluokat: A: 0, B: 4, C: 6
- Osa toimivuushäiriöistä johtui erilaisista muutostöistä, laitevioista tai konfiguraatiovirheistä.
  - Varmistukset eivät toimineet suunnitellusti ja vikatilanteen sattuessa yhteydet eivät siirtyneetkään varareitille onnistuneesti.
  - Vikatilanteiden jälkeen tarkistetaan voidaanko vastaavalta tilanteelta välttyä esimerkiksi laitteen ohjelmistopäivityksellä tai muiden vastaavien laitteiden huolloilla ja tarkastuksilla.
- Yleisradion radiolähetyksissä oli katkoksia 26.10. aamulla kello kuuden jälkeen eri puolilla Suomea

**Analyysi**

- Yleisten viestintäpalveluiden toimivuus Suomessa on vuonna 2021 ollut keskimäärin hyvä.
- Kuukaudessa on keskimäärin vajaat kuusi merkittävää toimivuushäiriötä.
- Toimivuushäiriöt kotimaan verkossa ja globaaleissa palveluissa osoittavat meille, että 2020-luvulla merkittävän palvelukatkoksen aiheuttajana voi olla edelleen hajonnut laite, kaivinkoneen kauha tai työntekijä näppäimistöineen.

TRAFICOM

# ICT-palveluiden toimivuus

- Korttimaksamisessa häiriöitä hetkellisesti koko maassa
  - Aamupäivällä 1.11. korttimaksaminen estyi S-ryhmän ja joidenkin muiden liikkeiden palveluissa. Häiriö vaikutti maksamiseen ainakin Visa- ja Mastercard-korteilla Pohjoismaissa ja Baltiassa.
  - Uutistietojen mukaan häiriö johtui korttimaksujen reititys- ja tilityspalveluja kaupoille tuottavan palveluntarjoajan verkkoyhteysongelmista.
  - https://yle.fi/uutiset/3-121688666
- Telia ilmoitti ongelmista palveluissa 7.10. kansainvälisistä verkkohäiriöistä johtuen
  - Verkkohäiriöt heijastuivat Suomessa mm. mobiilidatapalveluihin, yritysten kansainvälisiin datayhteyksiin, ulkomailla tuotettaviin puhepalveluihin ja tekstiviestiratkaisuihin.
  - https://www.telia.fi/asiakastuki/hairiotiedote?id=sabre_349823542&lang=fi

**Analyysi**

- Erilaiset häiriöt ovat näkyneet tavallisille käyttäjille viime aikoina ja osoittaneet kuinka riippuvaisia olemme toimivista yhteyksistä ja ICT-palveluista.
- Korttimaksamisen häiriöt 1.11. vaikeuttivat esimerkiksi kansalaisten kauppaostoksia hetkellisesti aamupäivällä.
- Viimeaikaiset katkokset kuitenkin osoittavat, että jokaisen tulee varautua töissä ja vapaa-ajalla erilaisiin häiriötilanteisiin ja pohtia mistä digimaailman asioista olemme riippuvaisia 2020-luvulla.

TRAFICOM

# Palvelunestohyökkäykset

- Palvelunestohyökkäyksiä kuntasektorilla kouluja kohtaan
  - Hyökkäyksillä on ollut myös välillisiä vaikutuksia muihin palveluihin. Julkisen IP-osoitteen takana voi olla muitakin palveluja ja infrastruktuuria kuin koulu.
  - Ilkivaltaiset palvelunestohyökkäykset voivat olla helppoja tilata ja halpoja toteuttaa.
  - Vaikka organisaatio olisi varautunut hyökkäyksiin esimerkiksi mitigaatiopalveluilla, voi välillinen vaikutus hyökkäyksen alussa näkyä myös muissa palveluissa.
- Noin 40% meille ilmoitetuista hyökkäyksistä (Q3/2021) Suomessa oli kooltaan yli 1 Gbit/s. Ilmoitettujen hyökkäysten perusteella skaala ulottuu tänä vuonna jopa 260 Gbit/s tasolle asti.

**Analyysi**

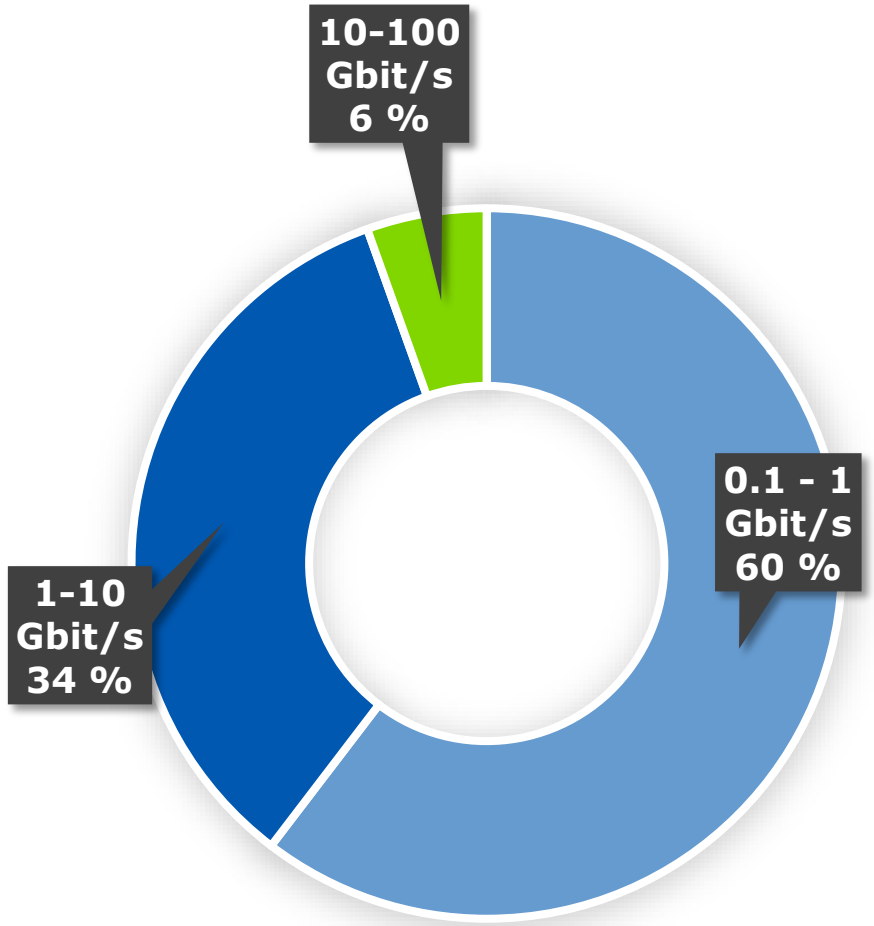
- Lukukauden aikana myös hyökkäykset aktivoituvat oppimispalveluita ja opintohallintojärjestelmiä kohtaan.
- Koululaisille ja muille hakkeroinnin alkeisiin tutustuville kannattaa muistuttaa, että tietoverkkojen häirintä on laitonta ja siitä koituvista rikosoikeudellisista seuraamuksista aiheutuu paljon harmia myöhemmässä elämässä.
- Palvelunestohyökkäys voi myös välillisesti aiheuttaa muutakin haittaa kohteelle, jolloin vahinkoa ei aiheuteta pelkästään oppimispalveluihin.

TRAFICOM

# Palvelunestohyökkäysten tunnuslukuja

3kk

- 99 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q3/2021.
- Noin 76% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.




Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q3/2021 - tilasto päivitetään kvartaaleittain.)

TRAFICOM

# Vakoilu

Vakoiluosiossa käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista. Tavoitteena voi olla poliittinen tiedonhankinta, yritysvakoilu tai esimerkiksi tietojärjestelmien tuhoaminen.

# Vakoilu

- Teleoperaattoreihin kohdistuneet ja kybervakoiluun liittyvät tietomurrot tai niiden yritykset ovat olleet viime aikoina esillä runsaasti.
- Esimerkiksi LightBasin-nimellä kutsuttu ryhmä on tunkeutunut lukuisten matkapuhelinoperaattoreiden järjestelmiin useiden vuosien aikana.
  - Ryhmä on myös pyrkinyt säilyttämään jalansijansa organisaatioissa erilaisin keinoin.
  - Hyökkääjän kohteena olivat olleet erityisesti roaming-järjestelmät, ja tunkeutumiset ovat kohdistuneet erityisesti Linux- ja Solaris-palvelimiin.
- Lokakuussa paljastui myös, että matkaviestintäpalveluita toteuttavaan Syniverseen on kohdistunut useita vuosia kestänyt tietomurto.
  - Syniverse tukee useiden kansainväisesti merkittävien operaattoreiden verkkojen välillä lähetettävien tekstiviestien välitystä.

**Analyysi**

- Teleoperaattorit ovat kybervakoilun ja tiedonhankinnan näkökulmasta kiinnostava kohde hyökkääjälle, sillä niiden hallussa olevaa tietoa voidaan käyttää monin tavoin hyödyksi.
- Teleoperaattoreihin kohdistuneita hyökkäyksiä paljastuu maailmalla säännöllisesti, ja niiden onkin syytä varautua tämänkaltaisen toiminnan estämiseen ja sen havaitsemiseen.

TRAFICOM

# Vakoilu

- Venäläiseksi epäilty NOBELIUM-ryhmä on Microsoftin tutkijoiden mukaan murtautunut toukokuusta lähtien ainakin neljäntoista IT- ja pilvipalveluntarjoajan järjestelmään.
  - Tunkeutumista oli lisäksi yritetty yli 140 vastaavaan organisaatioon siinä onnistumatta.
- Tietomurtojen tavoitteena vaikuttaa olleen murtautuminen palveluntarjoajien asiakkaiden järjestelmiin.
- Kohteet ovat sijainneet Microsoftin tietojen mukaan Yhdysvalloissa ja Euroopassa.
- Kampanjassa on pyritty hankkimaan pääsy korotettujen käyttöoikeuksien tileille mm. haitta-ohjelmien, kohdistetun kalastelun tai salasanojen massakokeilun (*password spray*) avulla.
  - Ylläpitotunnuksia ja luottamussuhdetta hyödyntäen on pyritty tunkeutumaan asiakasorganisaatioihin eri tavoin.

**Analyysi**

- IT-toimitusketjujen kautta toteutetuista hyökkäyksistä erityisen vaarallisia tekee se, että hyökkääjä voi saada tällöin yhden toimijan kautta pääsyn useisiin muihin organisaatioihin eli palveluntarjoajan asiakkaisiin.
- Asiakkaan ja palveluntarjoajan välisiä luotettuja yhteyksiä hyödyntävät tunkeutumiset voivat olla vaikeampia havaita.
- NOBELIUMin uskotaan olleen myös SolarWinds-tietomurtojen taustalla.

# Tietoturva-alan kehitys

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

TRAFICOM

# Oikeudelliset asiat

- EU:n tekoälyasetuksen valmistelu etenee
  - Ehdotus Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi (Artificial Intelligence Act)
  - Komissio antoi asetusehdotuksen 21.4.2021 ja ehdotuksen käsittely alkanut neuvoston televiestintä- ja yhteistyöryhmässä.
  - Komissio ehdottaa asetuksella oikeudellista kehystä eurooppalaisen lähestymistavan luomiseksi sekä yleisten etujen, erityisesti terveyden, turvallisuuden, perusoikeuksien ja -vapauksien korkean tason suojelun toteuttavan tekoälyn kehittämisen ja käyttöönoton edistämiseksi. Lähtökohtana on riskiperustainen ja käyttötapauskohtainen lähestymistapa tekoälyn soveltamiseen.
- Suomessa perustuslakivaliokunta on antanut lausuntonsa asetusehdotuksesta 21.10.2021 (PeVL 37/2021 vp — U 28/2021 vp)
  - https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PeVL_37+2021.pdf
  - Perustuslakivaliokunnan mielestä ehdotettu tekoälyasetus vaikuttaa tulevaisuuden yhteiskuntaan perustavanlaatuisella tavalla, eikä sitä voi pitää yksin tuoteturvallisuutta koskevana lainsäädäntönä. Tekoälyasetuksen oikeusvaikutukset ovat perusoikeusjärjestelmän kannalta erittäin merkittäviä.
  - Valiokunta on alustavasti tarkastellut asetusehdotusta kaupallisten intressien, perus- ja ihmisoikeuksien turvaamisen, kansallisen liikkumavaran, tietosuojasääntelyn ja asetusehdotuksen sisältämän seuraamusmaksusääntelyn kannalta.

TRAFICOM

# Arjen kyberturvallisuus

## Euroopan kyberturvallisuuskuukausi - European Cyber Security Month

- Lokakuussa vietettiin kyberturvallisuuskuukautta. Organisaatiot ja viranomaiset jakoivat omia vinkkejään tietoturvan parantamiseen. Muistetaan hyvät vinkit myös kaikkina muina kuukausina!
- https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month

## Laajoista kansalaisia koskevista tietoturvahäiriöistä ja -tilanteista tiedotetaan 112 Suomi -sovelluksen avulla

- 112 Suomi -sovellus toimii uutena viestintäkanavanamme yksityishenkilöille. Laajoista kansalaisia koskevista tietoturvahäiriöistä on tärkeää saada tieto jaettua mahdollisimman nopeasti ja laajasti. Kännykkä on tähän erinomainen väline
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/laajoista-kansalaisia-koskevista-tietoturvahairioista-ja-tilanteista-tiedotetaan-112

## Verkkopankkitunnuksien kalastelu jyrkässä nousussa - tällä viikolla kasvua yli 70%

- Kyberturvallisuuskeskus, poliisi sekä useat eri pankit ovat aktiivisesti tiedottaneet sekä varoittaneet pankkitunnuskalastelusta tämän vuoden aikana. Syksyn aikana olemme nähneet ilmoitusmäärissä huomattavaa kasvua.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkopankkitunnuksien-kalastelu-jyrkassa-nousussa-talla-viikolla-kasvua-yli-70

## Vieraskynä: Päivittäminen hallussa? SeniorSurf tukee senioreita digitaidoissa

- SeniorSurf rohkaisee ikääntyneitä ihmisiä tarttumaan tietokoneisiin ja nettiin. Yhdistys toimii valtakunnallisesti ja on mukana senioreiden digiopastustoiminnassa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vieraskyna-paivittaminen-hallussa-seniorsurf-tukee-senioreita-digitaidoissa

# Uutisia Kyberturvallisuuskeskuksesta

## Kyberturvallisuuskeskus kartoittaa jälleen suojaamattomia automaatiojärjestelmiä

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus etsii tietoverkoista suojaamattomia automaatiolaitteita. Työn tavoitteena on parantaa tilannekuvaa ja kyberturvallisuutta Suomessa. Saatuja tuloksia verrataan aikaisempien vuosien tuloksiin.
- Selvitys toteutetaan lähettämällä yhteydenavauspyyntöjä suomalaisissa verkoissa olevien tietokoneiden ja verkkolaitteiden tiettyihin tietoliikenneportteihin ja analysoimalla niistä tulevia vastausviestejä viikoilla 43-44.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kartoitus2021

## HAVARO-palvelulle Vuoden tietoturvatuote –tunnustus

- Tietoturva ry on valinnut Vuoden tietoturvatuote -tunnustuksen saajaksi HAVARO-palvelun, joka havainnoi ja varoittaa tietoturvaloukkauksista. Palvelun ovat yhteistyössä kehittäneet Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ja Huoltovarmuuskeskus.
- Tutustu Havaro-palveluun: https://www.kyberturvallisuuskeskus.fi/fi/havaro-palvelu
- Lue lisää tunnustuksesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/havaro-palvelulle-vuoden-tietoturvatuote-tunnustus

## Traficomin Kyberturvallisuuskeskus julkaisi Suomen ensimmäisen tekoälyselvityksen

- Selvitys tarkastelee tekoälyä kyberturvallisuuden ja riskienhallinnan näkökulmasta. Se kannustaa tekoälypohjaisten palvelujen tai tuotteiden kehittäjiä tekemään nämä kolme asiaa jo nyt: menemään kehitystyön kyberturvallisuus ja riskienhallinta edellä, hahmottamaan koneoppimismallin koko elinkaari ja panostamaan datan laatuun.
- Kyberturvallisuuskeskus esitteli myös uuden työkalun tekoälyn kyberturvallisuuden riskienhallintaan.
- https://www.traficom.fi/fi/ajankohtaista/miten-rakennetaan-kyberturvallinen-tekoalyratkaisu-traficomin-kyberturvallisuuskeskus

TRAFICOM

# 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

TRAFICOM