TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Kybersää

## Huhtikuu 2021

#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

# Kybersää huhtikuu 2021

## Tietomurrot ja -vuodot

- Office 365 –tietomurroista tulee edelleen ilmoituksia, mutta ilmoitusmäärät ovat olleet laskussa vuonna 2021.

## Huijaukset ja kalastelut

- Tekstiviestihuijaukset yleistyvät. Pankkitietoja kalastellaan, tilausansoihin houkutellaan ja haittaohjelmia levitetään tekstiviestien avulla.
- Pornokiristyskampanjat hiljenivät huhtikuussa, mutta jatkuvat taas.

## Haittaohjelmat ja haavoittuvuudet

- Pulse Connect Secure -etäkäyttöhaavoittuvuus, päivitys on nyt julkaistu ja se tulisi asentaa viipymättä.
- FluBot- ja FakeCop/FakeSpy–haittaohjelmaa levitetään tekstiviesteitse.

## Automaatio

- Nimet BadAlloc ja NAME:WRECK saaneet haavoittuvuudet vaikuttavat satoihin miljooniin sulautettuihin järjestelmiin.
- Sähköautot ja niiden latauspisteet yleistyvät nopeasti. Latauspisteiden kyberturvallisuudesta ei kuitenkaan juuri puhuta.

## Verkkojen toimivuus

- Huhtikuussa Suomessa vain kaksi merkittävää toimivuushäiriötä.
- Microsoftilla kaksi suurta pilvipalveluiden häiriötä.
- Huhtikuussa noin puolet meille tulleista ilmoituksista palvelunestohyökkäyksiin liittyen koski kouluja tai opetusalustoja.

## Vakoilu

- Pulse Connect Securen vakavaa haavoittuvuutta on käytetty mahdollisesti valtiollisessa vakoilussa.
- Yhdysvallat ja Britannia syyttävät Venäjän ulkomaantiedustelua SolarWinds Orion -hallintatyökalun päivitysketjuun ujuttautumisesta.

# Kuukauden tunnuslukuja

**25.4.**

YHDYSVALTAIN VIRANOMAISET AJOIVAT SAASTUNEIDEN KONEIDEN VERKKOON POISTOKÄSKYJÄ 25.4., MIKÄ KÄYTÄNNÖSSÄ LAKKAUTTI EMOTET-HAITTAOHJELMAVERKON TOIMINNAN.

**~50%**

HUHTIKUUSSA NOIN PUOLET MEILLE TULLEISTA ILMOITUKSISTA PALVELUNESTOHYÖKKÄYKSIIN LIITTYEN KOSKI KOULUJA TAI OPETUSALUSTOJA.

**48**

VUODEN 2021 AIKANA OLEMME VASTAANOTTANEET VAIN 48 OFFICE 365 –TIETOMURTOILMOITUSTA. VUONNA 2020 NIITÄ OLI YLI 450.

# **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 →

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

## 3 ↓

**Tietojenkalastelu** on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdennetuissa hyökkäyksissä ja vakoilussa.

## 4 →

**Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako.** Kyberuhkien vaikutuksia ei osata ennakoida ja epäselvyydet palveluiden hallinnan vastuunjaossa heikentävät tietoturvaa.

## 5 →

**Lokitietojen puutteellisuus** on riski monessa organisaatiossa. Puutteellisen lokitietojen keruun, seuraamisen ja säilyttämisen takia poikkeamatilanteita ei kyetä havainnoimaan tai selvittämään.

↑ *kohonnut*

↓ *laskenut*

→ *ennallaan*

*Keltainen* = uutta/ päivitettyä*

# **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.

- 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 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**

UUSI

Microsoft tiedotti 2.3. Exchange-sähköpostipalvelimien kriittisistä haavoittuvuuksista ja niiden aktiivisesta hyväksikäytöstä. Kyberturvallisuuskeskus havaitsi suomessa aluksi lähes 300 haavoittuvaa Exchange-palvelinta. Mukana oli myös palvelimia, joihin oli jo murtauduttu haavoittuvuutta hyväksi käyttäen. Suomalaisten organisaatioiden haavoittuvat Exchange-palvelimet oli päivitetty huhtikuun alkuun mennessä. Organisaatioiden kyky reagoida kriittisiin haavoittuvuuksiin, päivityksiin sekä tietomurtojen tutkintaan nousi tärkeäksi osaksi Exchange-haavoittuvuuksien hoidossa.

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

## 2

**Eri kyberhyökkäysmenetelmien käyttö kiristämisessä yleistyy, mikä uhkaa myös 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 ilmiöstä ilmoituksia myös vuonna 2021.

Yleensä organisaatio saa kiristysviestin sähköpostitse, joka on allekirjoitettu näennäisesti tunnettujen haitallisten toimijoiden nimissä. Joissakin tapauksissa kiristysviestiä on ryyditetty palvelunestohyökkäyksellä viestin tehostamiseksi. Viestissä kerrotaan organisaation kohtaavan suuren palvelunestohyökkäyksen, jos lunnaita ei makseta. Ohjeemme on ja pysyy: älä maksa kiristäjille.

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

## 3

**Tietojenkalastelu** ja muu käyttäjien manipulointi (social engineering) on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdistetuissa hyökkäyksissä ja vakoilussa.

- Tietojenkalastelusta on tullut hyvin yleistä. Tyypillisesti rikolliset kalastelevat suomalaisilta Office 365 -tuotteiden ja sähköpostin käyttäjätunnuksia ja salasanoja.
- Linkki kalastelusivulle voi olla piilotettu kokouskutsuun, naamioitu turvapostiksi tai väärennetty postin tai pankin tekstiviestiksi.
- Hakukoneiden hakutuloksiin on ujutettu myös huijaussivuja, joilla kalastellaan tietoja. Varsinkin väärin kirjoitettu hakusana johtaa helposti rikollisten rakentamaan ansaan (typosquatting).
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua ja käyttäjän manipulaatiota opitaan tunnistamaan koulutuksen avulla, jolloin tietojenkalastelu jää vain yritykseksi.

**CASE**

Verkkopankin asiakkaiden pankkitilejä tyhjennettiin ja rahaa varastettiin lyhyessä ajassa suuria summia.

Epäiltiin uutta tehokasta haittaohjelmaa, mutta syyllinen olikin hakukoneiden tietokannan manipulointi tai verkkomainonta.

Rikollinen onnistui nostamaan omia sivujaan tuloksissa oikeiden verkkopankkien edelle ja kymmenet käyttäjät erehtyivät tietojenkalastelusivulle.

Pankkitietojen avulla rikollinen pääsi verkkopankkiin ja tyhjensi uhrien tilit.

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

## 4

**Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako.** Kyberuhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Epäselvyydet palveluntoimittajan, alihankkijoiden ja tilaajan vastuiden välillä heikentävät organisaation tietoturvan hallintaa.

- Tietoturvaloukkauksiin vastaamista tai niistä toipumista ei usein suunnitella riittävästi ennakkoon. Häiriön iskiessä palautumisen monimutkaisuus ja työläys yllättävät.
- Tehdyt suunnitelmat tulee testata ja niitä pitää harjoitella.
- Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä, jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä. Vastuut tulisi tehdä selväksi viimeistään hankinnan sopimusvaiheessa.

**CASE**

Organisaatio käyttää pilvipohjaista sovellusta (Software as a Service, SaaS) raporttien tekoon kumppaneidensa kanssa. Yhden raportin julkaisussa tapahtuneiden epäselvyyksien vuoksi pilvipalveluntarjoajaa pyydetään toimittamaan lokitiedot raportin käsittelystä. Palveluntarjoaja vastaa, etteivät he voi luovuttaa lokitietoja, sillä heidän jaettuja resursseja käyttävät palvelut eivät erottele eri asiakkaiden lokitietoja. Tältä tilanteelta oltaisiin voitu välttyä, jos tämä vastuunjakoon liittyvä asia olisi sovittu jo sopimuksentekovaiheessa.

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

## 5

**Lokitietojen puutteellisuus on riski monessa organisaatiossa**. Poikkeamatilanteita ei kyetä havainnoimaan ja selvittämään, jos oikeiden järjestelmien tai sovellusten lokitietoja ei kerätä, seurata ja säilytetä riittävän kauan.

- Kattavan lokienhallinnan avulla tietomurto on mahdollista havaita jo alkuvaiheessa. Pahimmillaan joissain tapauksissa ei lokitietojen riittämättömyydestä johtuen koskaan saada selville, milloin, miten ja kuinka laajalti ympäristöön on tunkeuduttu.
- Organisaatioiden on tunnistettava, mitkä ovat heille keskeiset järjestelmät ja sovellukset tietoturvaloukkausten havainnoinnissa ja selvittämisessä. Sen on myös huolehdittava riittävästä lokitietojen keräämisestä ja niiden riittävän pitkästä varastoinnista.
- Tietoturvaloukkauksen selvitykseen tarvittavia lokitietoja olisi hyvä säilyttää vähintään vuoden ajan.

**CASE**

Yrityksen etäkäyttöpalvelussa on havaittu kirjautumiseen viittaavaa liikennettä epäilyttävästä lähteestä. Palvelusta ei kuitenkaan kerätä kirjautumislokeja, joten tapausta ei voida selvittää tämän pidemmälle.

Organisaation Windows-ympäristössä vain epäonnistuneista kirjautumisyrityksistä tehdään lokimerkintä. Tunkeutujan anastamilla tai itse luomilla tunnuksilla tehdyt kirjautumiset jäävät piiloon, eikä tunkeutumisen laajuutta pystytä selvittämään.

# Tietomurrot ja -vuodot

Tietomurroissa ja -vuodoissa käsitellään suojauskeinoja sekä tietoomme tulleita ilmiöön liittyviä trendejä. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita ja kolhuja maineeseen.

# Tietomurrot ja -vuodot

- Office 365 –tietomurtoja ilmoitetaan edelleen, mutta ilmoitusmäärät ovat laskussa
  - Suomalaisten organisaatioiden Office 365 –tilejä on murrettu, ja niitä on hyödynnetty kalasteluviestien välitykseen.
    - Tietomurtojen kohteina on ollut mm. julkishallinnon organisaatioita.
  - Office 365 –tietomurtojen ilmoitusmäärät laskussa vuonna 2021.
    - Vuonna 2019 saimme 347 ja vuonna 2020 vastaanotimme 453 Office 365 –tietomurtoilmoitusta.
    - Vuonna 2021 (4.5.2021 mennessä) olemme vastaanottaneet 48 Office 365 –tietomurtoilmoitusta.

**ANALYYSI**

- Monivaiheisen tunnistautumisen käyttöönotto ja vanhojen tunnistautumismenetelmien (legacy authentication) poistaminen käytöstä ovat tehokkain keino tietomurtojen ehkäisemisessä

# Huijaukset ja kalastelut

Huijauksiin ja tietojenkalasteluun sisältyy esimerkiksi käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia ja kiristyksiä. Lisäksi organisaatioihin voi kohdistua pankkitunnusten ja maksukorttitietojen kalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.

# Huijaukset ja kalastelut

- Tietojenkalastelua laidasta laitaan
  - Huhtikuuta täplittivät hyvin monenlaiset eri tietojenkalastelut. Joukossa oli kömpelöitä ja yksinkertaisia sähköpostiyrityksiä, joissa kysyttiin kaikkia mahdollisia tietoja laidasta laitaan sekä huolellisesti valmisteltuja monimutkaisia kalastelukampanjoita.
  - Monimutkaisissa kalastelukampanjoissa oli etukäteen rekisteröity ja valmisteltu uskottavan oloinen kalastelusivu, jonne uhrit houkuteltiin tiukoilla tekstiviesteillä.
  - Myös OmaPosti-teemaisia tekstiviestihuijauksia lähetetään edelleen hyvin paljon.

**ANALYYSI**

- Tietoja kalastellaan myös kirpputori- ja myyntipalveluissa.
- Verkon palvelusivujen asunto- ja autokauppojen sekaan piilotetaan kalastelu- ja huijausyrityksiä.
- Oikotie-palvelu ilmoittaa säännöllisesti erilaisista huijausyrityksistä.

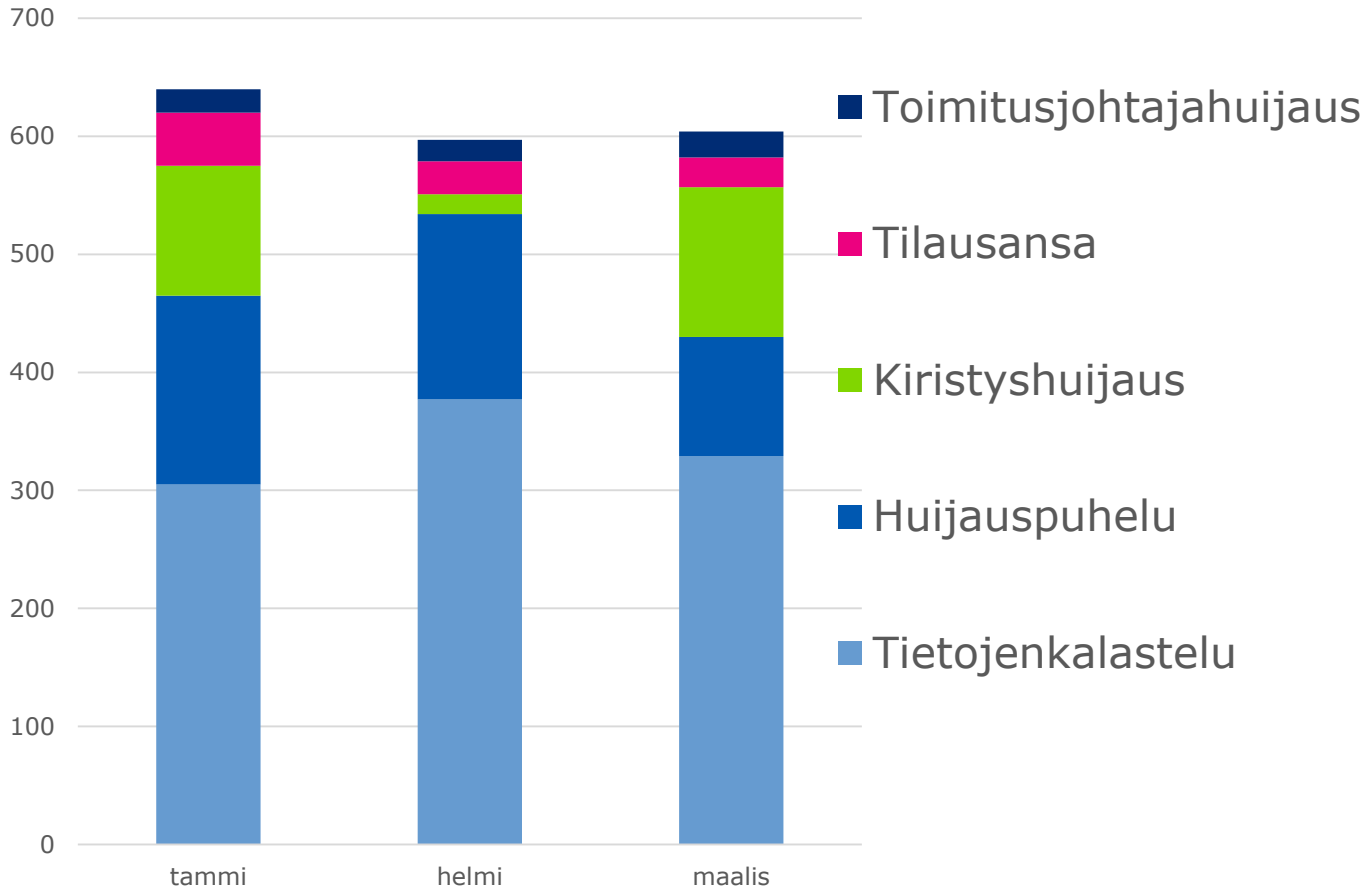
# Huijaukset ja kalastelut

- Kiristysviesteissä kiristetään kaikella mahdollisella.
  - Pitkään suomalaisiakin piinanneet pornokiristysviestit hiljenivät huhtikuussa hetkeksi.
  - Huijausviestit, joissa väitetään kiristäjän murtautuneen uhrin tietokoneelle ja kuvanneen arkaluontoista materiaalia, jatkuvat kuitenkin taas.
  - Kiristysviestin uutena uhkauskeinona on väittää, että kiristäjä on murtautunut uhrin verkkosivuille ja uhkaa laittaa sinne näkyville pornoa, ellei uhri maksa lunnaita.
  - Nämäkin uhkaukset ovat kaikki huijausta.

**ANALYYSI**

- Teknisen tuen huijauspuheluita tulee Suomeen edelleen, mutta määrä vaikuttaa vähentyvän.
- Aiemmin on nähty viitteitä, että teknisen tuen huijauspuheluita soitetaan intialaisista puhelukeskuksista. Intiassa parhaillaan meneillään olevat COVID-19-liikkumisrajoitukset saattavat vaikeuttaa puhelukeskusten toimintaa.

# Käsiteltyjä huijaustapauksia Q1/2021




- Vuoden ensimmäisen neljänneksen 2021 ilmiöitä ovat:
  - Kiristyshuijaukset esiintyivät kausittain aalloissa. Välillä pornokiristyksiä raportoitiin jatkuvasti, kunnes ne parin viikon kuluttua taas laantuivat kokonaan.
  - Jatkuvat Postin nimissä tehdyt huijaukset, jotka johtavat tilausansoihin, pikavippeihin, tai puhelimen haittaohjelmaan.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.

# Haittaohjelmat ja haavoittuvuudet

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

# Haittaohjelmat

- Tekstiviestein levitetään haittaohjelmia UPS:n, DHL:n ja OmaPostin teemoilla
  - Tekstiviesteillä levitetään OmaPosti-aiheista huijausviestiä, jossa on linkki haitalliselle sivulle.
  - FakeCop-haittaohjelma houkutellaan lataamaan hyödyntäen tunnettujen toimijoiden nimiä kuten OmaPosti ja Chrome.
  - Uutta Android-haittaohjelmaa nimeltään FluBot levitetään myös Suomessa tekstiviesteitse, joissa käytetään UPS- ja DHL–teemaa.

- Lisätietoja: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

**ANALYYSI**

- Jos olet asentanut haittaohjelman, suosittelemme laitteen palauttamista tehdasasetuksiin. Ota myös yhteyttä omaan operaattoriisi, koska liittymästäsi on voinut lähteä myös tekstiviestejä.

# Haavoittuvuudet

- Pulse Connect Secure -etäkäyttöhaavoittuvuus 20.4.2021
  - Haavoittuvuus on havaittu muun muassa valtion etäyhteyksissä käytetyssä Pulse-VPN-ympäristössä, ja tutkinta mahdollisesta hyväksikäytöstä on aloitettu.
  - Haavoittuvuuteen on tarjolla lievennyskeinoja, joilla haavoittuvuuden vaikutusta on mahdollista alentaa.
  - Laitteita on kartoitettu ja tunnistettu Suomesta hieman yli 700.
  - Kyberturvallisuuskeskus on yrittänyt tavoittaa laitteiden haltijoita yhteistyössä teleoperaattoreiden kanssa.
  - Valmistaja on julkaissut maanantaina 3.5. tuotteeseen päivityksen, joka tulisi asentaa viipymättä.

**ANALYYSI**

- Etäkäyttöratkaisut ovat hyökkääjille kiinnostavia kohteita.
- Hyökkäyksien selvittäminen ja haavoittuvuuksien korjaaminen voivat vaikuttaa liiketoimintaan tai organisaatioon merkittävästi esimerkiksi, jos haavoittuvuus estää etätyöyhteysratkaisun käytön.
- Etätyöjärjestelyt eivät saisi vaarantaa yhdenkään organisaation tietoturvaa. Poikkeusratkaisut, jos sellaisia on, pitäisi purkaa normaalioloihin palattaessa. Ilman ratkaisujen dokumentointia niiden purkaminen huolellisesti ei ole mahdollista.

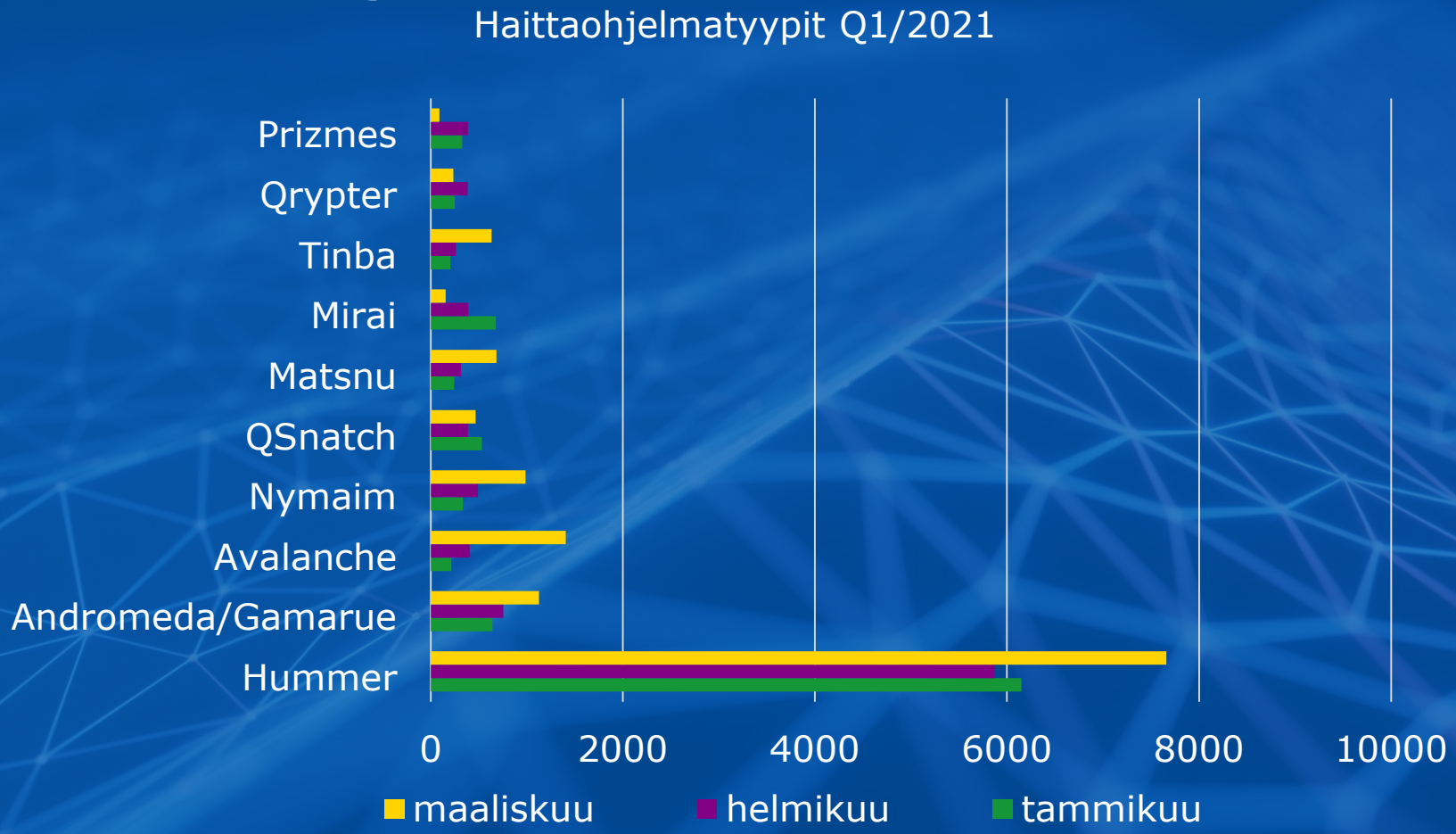
# Kuukauden haavoittuvuusjulkaisut

- Kuukausittainen päivitystiistai korjasi monia kriittisiä ja vakavia haavoittuvuuksia (11/21)
- Pulse Connect Secure -etäkäyttöhaavoittuvuus (12/21)
  - Pulse Secure julkaisi 3.5.2021 korjaavan päivityksen koskien kriittistä etäkäyttöhaavaa.
  - Korjaus tulee suorittaa välittömästi, sillä haavoittuvuutta käytetään aktiivisesti hyväksi.
  - Valmistajalla on myös eheystyökalu, jolla voi yrittää todentaa mahdollisen haavoittuvuuden hyväksikäytön.
- Lue lisää: www.kyberturvallisuuskeskus.fi/haavottuvuudet

**ANALYYSI**

- Päivitykset tulee asentaa viipymättä, haavoittuvuuksien hyväksikäyttö on todella nopeaa.
- Kriittisten palveluiden hallintarajapintojen näkyvyys internetiin on asia, jota tulisi jatkuvasti seurata.
- Kehotamme kartoittamaan, mitä palveluita omasta organisaatiosta on avoinna internetiin.
- On lieviä merkkejä siitä, että muutkin kuin kehittyneet toimijat yrittävät hyödyntää toimitusketjuhyökkäyksiä.

# Autoreporterin haittaohjelmahavainnot




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

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla.

Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa Autoreporter-järjestelmän avulla. Autoreporter-järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

# Automaatio ja IoT

Automaatio-osiossa kerrotaan alan uutisista ja ilmiöistä maailmalla ja kotimaassa. Automaatiojärjestelmiä käytetään ohjaamaan ja monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.

# IoT

- Sähköautojen latausinfran kyberturvallisuuden merkitys kasvaa
  - Tilastokeskuksen mukaan maaliskuussa ensirekisteröidyistä henkilöautoista 7,6 prosenttia oli täyssähköautoja ja 21,1 prosenttia ladattavia hybridejä.
  - Muun muassa kauppaketjujen, alan isojen toimijoiden ja energiayhtiöiden uutisoitiin lisäävän pikalatauspaikkoja lähitulevaisuudessa. Pikalataustolppien määrän ennustetaan tuplaantuvan tämän vuoden aikana.

**ANALYYSI**

- Sähköajoneuvojen latausinfran puutteellisen tietoturvan aiheuttamia riskejä ovat esimerkiksi asiakastietojen joutuminen vääriin käsiin ja siitä seuraava virheellinen laskutus.
- Latausinfran suojaaminen torjuu myös muita sähköverkkoon kohdistuvia uhkia, esimerkiksi tahallaan aiheutettuja sähköpiikkejä tai sähkömarkkinoiden manipulointiyrityksiä.
- Koska tietoturvallisuuden hankkiminen jälkeenpäin on kallista ja vaikeaa, se on hyvä ottaa huomioon jo latausinfraa hankittaessa.
- Lataustolppien tietoturvallisuutta on myös hyvä myös testata tai testauttaa.

# IoT ja automaatio

- BadAlloc-haavoittuvuudet
  - Useiden reaaliaikakäyttöjärjestelmien (RTOS), ohjelmistokehitykseen käytettävien työkalupakettien (SDK) sekä C-ohjelmointikielen kirjastojen (libc) muistinkäyttöön liittyvistä funktioista on löytynyt kriittisiä haavoittuvuuksia.
  - Haavoittuvuudet voivat vaikuttaa kuluttajakäyttöön ja lääketieteelliseen käyttöön suunnatuista IoT-laitteista aina teollisuusautomaatiojärjestelmiin saakka.
- NAME:WRECK-haavoittuvuudet
  - Haavoittuvuuksia sulautetuissa järjestelmissä yleisten TCP/IP-pinojen tavassa käsitellä nimipalvelukyselyitä.
  - Haavoittuvia toteutuksia on Nucleus NET:ssä (mm. Siemens Nucleus RTOS:ssa), FreeBSD-käyttöjärjestelmässä ja NetX:ssä (mm. ThreadX RTOS:ssa). Haavoittuvuuksien löytäjät arvioivat, että haavoittuvuuksia on helppo käyttää hyväksi noin 100 miljoonassa laitteessa. Haavoittuvia laitteita käytetään erityisen paljon julkishallinnossa ja terveydenhuollossa.

**ANALYYSI**

- Pidä lukua järjestelmistäsi ja laitteistasi ja seuraa niiden haavoittuvuuksia. Käytä tarvittaessa SBOM:a.
- Asenna päivitykset heti, kun ne ovat saatavilla. Jos päivityksiä ei tarjota, seuraa valmistajan ohjeistuksia ja pyri lieventämään riskiä muilla keinoilla.
- Haavoittuvuuksia hyväksikäyttämällä hyökkääjä voi pahimmillaan saada suoritettua omaa koodia järjestelmässä tai aiheuttaa järjestelmän kaatumisen. Tästä voi aiheutua suoraa haittaa laitteen toiminnalle.
- Tyypillisesti tällaisia haavoittuvuuksia käytetään hyväksi bottiverkkojen luomiseen. Bottiverkoilla voidaan muun muassa tehdä palvelunestohyökkäyksiä kolmansia osapuolia vastaan.

# Verkkojen toimivuus

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

# Verkkojen toimivuus

- Huhtikuussa vain kaksi merkittävää toimivuushäiriötä
  - Toinen koski useita viestintäpalveluita Vaasassa 4.4. ja toinen kaapeli-TV- ja internetyhteyspalveluita Espoossa 9.4.
  - Häiriöiden vaikutukset olivat suhteellisen pieniä.
- Yksi teleyritys ilmoitti huhtikuussa myös häiriöstä, joka oli tapahtunut jo maaliskuussa, mutta todettu merkittäväksi vasta myöhemmin.

**ANALYYSI**

- Yleisten viestintäpalveluiden toimivuus Suomessa on ollut alkuvuoden 2021 aikana hyvä. Merkittäviä toimivuushäiriöitä on ollut 20, mikä ennustaisi koko vuoden summaksi 60. Se olisi selvästi vähemmän kuin viime vuonna.
- Historiallisesti alkuvuodesta on kuitenkin ollut keskimäärin vähemmän merkittäviä häiriöitä kuin loppuvuodesta. Määrään vaikuttavat voimakkaasti kesän ja syksyn myrskyt.

# ICT-palveluiden toimivuus

- Microsoftin pilvipalveluissa oli huhtikuussa kaksi maailmanlaajuisesti vaikuttanutta häiriötä
  - 1.4. Azure-pilvipalvelun DNS-palvelimista paljastui välimuistin ohjelmointivirhe, jonka vuoksi DNS-palvelimet ylikuormittuivat, eikä Azuressa sijainneisiin palveluihin saanut välttämättä yhteyttä.
  - 27.4. Teams-palvelussa oli satunnaisia häiriöitä palvelun ylläpidossa tehdyn konfiguraatiovirheen vuoksi.

**ANALYYSI**

- Suurissa pilvipalveluissa on viime aikoina ollut kuukausittain maailmanlaajuisesti vaikuttaneita häiriöitä. Niiden toistumiseen kannattaa varautua esimerkiksi häiriötilanteiden toimintatapoja suunnittelemalla ja harjoittelemalla.
- Ihmiset ja organisaatiot vaikuttavat onneksi edelleen kykenevän sopeutumaan ajoittaisiin pilvipalveluiden häiriöihin.

# Palvelunestohyökkäykset

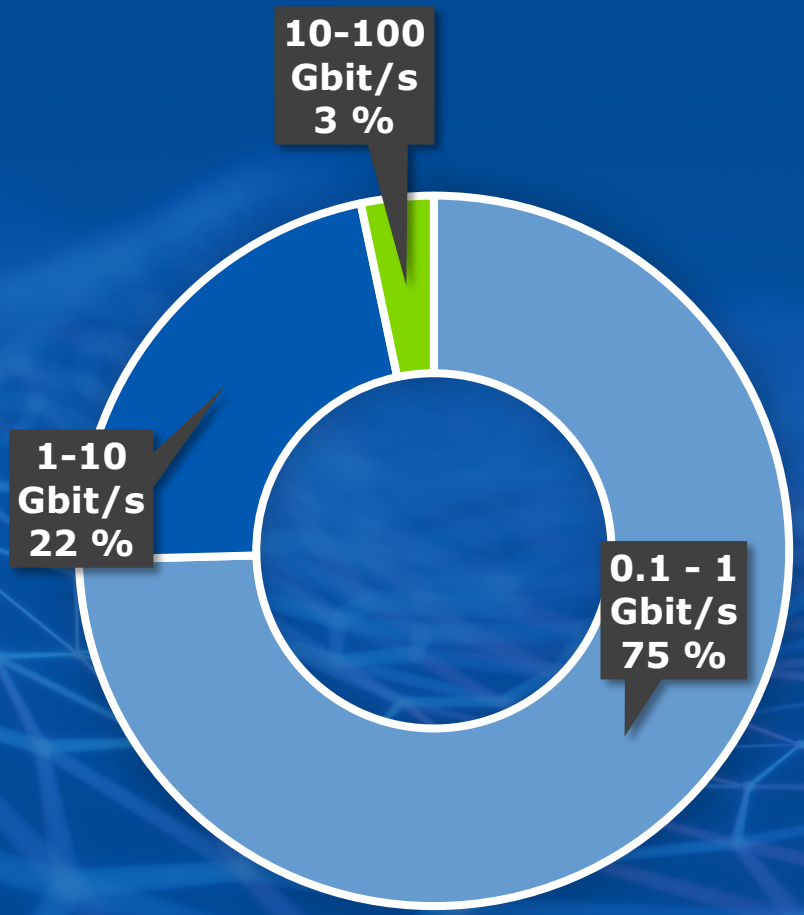
- Huhtikuussa noin puolet saamistamme palvelunestohyökkäyksiin liittyvistä tietoturvailmoituksista koski kouluja tai opetusalustoja
  - Hyökkäyksillä on ollut myös välillisiä vaikutuksia muihin palveluihin.
  - Ilkivaltaiset palvelunestohyökkäykset voivat olla helppoja tilata ja halpoja toteuttaa. Vaikka organisaatio olisi varautunut hyökkäyksiin esimerkiksi mitigaatiopalveluilla, voi välillinen vaikutus hyökkäyksen alussa näkyä myös muissa palveluissa.
  - Meille on ilmoitettu erilaisista ilkivaltaisista palvelunestohyökkäyksistä aiemminkin. Esimerkiksi verkkosivuilla olevia lomakkeita on täytetty tuhatmäärin, linkkejä verkkokoulutustilaisuuksiin on lähetetty ulkopuolisille häiriköille tai esimerkiksi peliyhteisön palvelimia on koputeltu isommallakin moukarilla.

**ANALYYSI**

- Koska palvelunestohyökkäyksen voi tilata verkosta muutamilla kympeillä tai sen voi toteuttaa kekseliäästi muilla tavoin, on tärkeää muistaa, että palvelunestohyökkäys ja sen yritys ovat rikoksia, joista myös alle 15-vuotias voi joutua vastuuseen.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/etaopiskeluymparistoihin-kohdistuneet-palvelunestohyokkaysten-yritykset-taas-kasvussa

# Palvelunestohyökkäysten tunnuslukuja

- 86 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q1/2021.
- Noin 65% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.




**SUOMEEN KOHDISTUNEIDEN PALVELUNESTOHYÖKKÄYSTEN VOLYYMIT (Q1/2021 - TILASTO PÄIVITETÄÄN KVARTAALEITTAIN.)**

# Vakoilu

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

# Vakoilu

- Pulse Connect Secure -tuotteesta löydettyä nollapäivähaavoittuvuutta hyödynnettiin valtiolliseen toimintaan yhdistetyssä tietomurto-operaatiossa
  - Kyseessä on VPN-ratkaisu, jollaisella mahdollistetaan suojatun yhteyden muodostaminen esimerkiksi yrityksen verkon ja työntekijän päätelaitteen välillä.
  - Tietoturvayhtiö FireEyen mukaan kampanja on kohdistunut ainakin valtionhallintoon ja puolustusteollisuuden alan yrityksiin.
  - Esimerkiksi Yhdysvaltojen tietoturvaviranomainen CISA on kertonut avustaneensa viittä virastoa Pulse Connect Secureen liitettyjen epäiltyjen tietomurtojen tutkinnassa.
  - Suomessa valtiohallinnon tietotekniikkapalveluita tuottava Valtori tiedotti aluksi myös tutkivansa Pulse Securen etäkäyttösovellukseen liittyvää mahdollista tietomurtoa, mutta on sittemmin kertonut, että ensivaiheen havainto tietomurrosta näyttää johtuneen järjestelmävirheestä, eikä tietomurrosta ole löydetty merkkejä.

**ANALYYSI**

- Keskeiset verkkolaitteet ja organisaation verkon tietoturvaratkaisut ovat houkuttelevia tunkeutumiskohteita hyökkääjälle, jota kiinnostaa organisaation kriittinen tieto tai jalansijan saaminen verkkoon.
- Tilanteissa, joissa haavoittuvuutta on voitu ehtiä hyödyntämään, ei pelkkä järjestelmän päivittäminen riitä, vaan organisaation tulisi muilla keinoin varmistua siitä, että järjestelmään ei ole ehditty murtautua.

# Vakoilu

- Yhdysvallat ja Britannia syyttävät Venäjän ulkomaantiedustelupalvelua (SVR) aiemmin julki tulleesta SolarWinds Orion -hallintatyökalun päivitysten haitallisesta muuntelusta
  - Toimijoiden mukaan operaation taustalla olevat tahot tunnetaan julkisuudessa myös nimillä APT29, Cozy Bear ja The Dukes.
  - Maiden viranomaisten mukaan SVR on ollut taustalla myös COVID-19-rokotetutkimukseen kohdistuneessa kybervakoilussa, jossa hyödynnettiin WellMess-nimellä tunnettua haittaohjelmaa.
  - Julkilausuman mukaan toiminnalle on ominaista erilaisten julki tulleiden haavoittuvuuksien hyödyntäminen.

**ANALYYSI**

- Myös valtiolliset toimijat hyödyntävät jo tiedossa olevia haavoittuvuuksia.
- Julkisesta internetistä saavutettavissa olevat järjestelmät pitäisi pystyä päivittämään tai muutoin suojaamaan mieluiten vuorokauden kuluessa haavoittuvuuden julkaisusta johtuen siitä, että aikaikkuna haavoittuvuuksien julkistamisesta niiden hyödyntämiseen on lyhentynyt.

# Vakoilu

- Ghostwriters-nimellä tunnettu informaatio-operaatio on jatkunut keväällä aktiivisena Euroopassa
  - Esimerkiksi maaliskuussa sen tavoitteena on vaikuttanut olevan poliittisen hajaannuksen lisääminen Puolassa informaatiovaikuttamisen keinoin. Myös Liettua ja Latvia ovat olleet aktiivisen vaikuttamisen kohteena.
  - Operaatioon on kuulunut poliitikkojen ja toimittajien sosiaalisen median tilien kaappauksia, oikeita sivustoja kopioivia valesivustoja ja todellisten sivustojen murtoja sekä valheellisten sisältöjen julkaisua kaikissa näistä.
  - Tyypillisesti vaikuttamisessa on pyritty herättämään pahennusta esimerkiksi poliitikkoja tai armeijaa kohtaan, kyseenalaistamaan sotilasliitto NATO:a, lisäämään maiden sisäisiä jännitteitä tai vaikuttamaan maiden välisiin suhteisiin.
  - Tietoturvayhtiö FireEyen mukaan Ghostwriters-operaatiota ei tällä hetkellä pystytä yhdistämään mihinkään tunnettuun toimijaan, mutta sen mukaan ainakin jotkin Ghostwritersin toiminnan osat voidaan linkittää tunnusten keräykseen ja haittaohjelmiin keskittyneeseen ryhmään, jota FireEye seuraa nimellä UNC1151.

**ANALYYSI**

- Esimerkiksi sosiaalisen median tilien käyttö osana informaatio-operaatiota korostaa tilien vahvan suojaamisen merkitystä, koska se vähentää niiden pahantahtoisen käytön riskiä myös sellaisessa tilanteessa, jossa tunnukset syystä tai toisesta – esimerkiksi tietojenkalastelun seurauksena – joutuvat vääriin käsiin.

# 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.

# Oikeudelliset asiat

- Hallinto-oikeuden ratkaisut selkeyttivät evästesääntelyn tulkintaa
  - Helsingin hallinto-oikeus antoi 8.4.2021 kaksi ratkaisua, jotka koskivat Traficomin tekemiä päätöksiä evästeiden käytöstä ja suostumuksen antamisesta muille kuin välttämättömille evästeille.
  - https://www.traficom.fi/fi/ajankohtaista/hallinto-oikeuden-ratkaisut-selkeyttivat-evastesaantelyn-tulkintaa

**ANALYYSI**

- Palveluntarjoajan tulee pyytää käyttäjän suostumus evästeiden käyttöön evästebannerilla. Internetselaimen asetusten kautta tehty hyväksyntä ei ole riittävä.
- Hallinto-oikeus totesi Traficomin olevan toimivaltainen viranomainen evästeasioissa, myös suostumuksen tulkintakysymyksissä.
- Traficom tulee uudistamaan evästeiden ja muiden verkkopalveluista käyttäjien päätelaitteille tallentuvien tietojen käyttöä koskevaa ohjeistustaan.

# Oikeudelliset asiat

- Ilmailulain uudistus lausuntokierroksella 20.5.2021 asti
  - Muutoksia esitetään ilmailulakiin, liikenteen palveluista annettuun lakiin, sähköisen viestinnän palveluista annettuun lakiin ja rikoslakiin.
  - Ilmailulakiin esitetään uutta 169 a §:ää, joka mahdollistaisi miehittämättömän ilma-aluksen kulun ja lennätyksen havainnoinnin ilmailun turvallisuuden varmistamiseksi.
  - https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=7c7db681-a721-4ce3-8f49-e130bf0b2221

**ANALYYSI**

- Miehittämättömien ilma-alusten kulun ja lennätyksen havainnointi olisi mahdollista yhtiömuotoisille ilmailutoimijoille, kuten lentoaseman pitäjille ja ilmaliikennepalvelun tarjoajalle.
- Muutos mahdollistaisi lennätykseen liittyvän radioviestinnän, sähköisten välitystietojen ja sijaintitietojen käsittelyn miehittämättömän ilma-aluksen yksilöimiseksi sekä aluksen ja sen lennättäjän paikantamiseksi.
- Muutos ei kuitenkaan oikeuttaisi ilmailutoimijoita puuttumaan miehittämättömän ilma-aluksen kulkuun.

# Arjen kyberturvallisuus - huhtikuu

## Nasevia neuvoja tiliesi turvaamiseksi

- Verkkopalveluissa käytettäviä tilejä yritetään murtaa ja ottaa haltuun usein eri keinoin.
- Olemme koonneet lyhyet ohjeet sekä ennalta suojautumisen kannalta että murron tapahduttua.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

## Tietoturvataidot – äh mikä mörkö!

- Kyberturvallisuus, tietoturva, palomuuri, virusturvaohjelma, salattu yhteys. Joko tuli hiki? Ei hätää, yksinkertaisuudessaan näissä on kyse sinun turvallisuudestasi ja maalaisjärjestä.
- Lue lisää ja tutustu myös SeniorSurfin toimintaan: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvataidot-ah-mika-morko

## Pidä kiinni rahoistasi - ikääntyneet ovat houkutteleva kohde verkkorikollisille

- Erilaiset huijaukset ovat tulleet jäädäkseen ja ikääntyneet ovat erityisessä vaarassa joutua verkkorikollisten uhreiksi. Ikävään trendiin kuitenkin voi ja pitää vaikuttaa.
- Lue lisää aiheesta ja katso asiantuntijan kommentit: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pida-kiinni-rahoistasi-ikaantyneet-ovat-houkutteleva-kohde-verkkorikollisille

## Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä

- Huijarit ovat jälleen aktivoituneet aikuisviihdeteemaisten eli "pornokiristys” -huijausviestien lähettelyssä.
- Viestejä on nyt liikkeellä monikielisinä, saman sisältöinen viesti voidaan lähettää englanniksi tai suomeksi.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pornokiristyksia-runsaasti-liikkeella-ala-usko-huijarien-vaitteita

# Uutisia Kyberturvallisuuskeskuksesta

## Uusi kokeilu on käynnistynyt - Lauttatonttu

- Kokeilussa keskitytään organisaation sisäverkon tietoturvaratkaisuihin. Tavoitteena on kevyiden, ketterien ja helppojen ratkaisuiden löytäminen organisaation käyttöön.
- Kokeilun perusteella yritykset saavat käytännön kokemuksia erilaisten tietoturvan valvontaan liittyvien kyvykkyyksien tarpeesta ja käytöstä tietoverkkojensa valvonnassa.
- Tutustu lisää ja ilmoittaudu mukaan: https://www.kyberturvallisuuskeskus.fi/fi/tonttu

## 5G Cyber Security Hack 2021

- Liikenne- ja viestintävirasto Traficom, Traficomin Kyberturvallisuuskeskus sekä Huoltovarmuuskeskus järjestävät yhteistyössä kansainvälisen hackathonin 5G-kyberturvallisuuden kehittämiseksi ja digiyhteiskunnan turvaamiseksi.
- Tapahtuma järjestetään virtuaalisena 18.-20.6.2021, ja se on suunnattu kokeneille tietoturva-ammattilaisille.
- Haastekumppaneina ovat Cisco, Ericsson, Nokia, PwC Finland ja Aalto yliopisto.
- https://app.hackjunction.com/events/5g-cyberhack/

## Tieto tarvitsee tulevaisuuden turvaajia

- Keskusrikospoliisi ja tietoturva-alan vaikuttajina eri organisaatioissa toimivat asiantuntijat toteuttivat nuorille suunnatun Kyberkaappauksen KRP:n Instagramissa. Yksi asiantuntijoista oli tietoturva-asiantuntijamme Juho Jauhiainen.
- Tutustu blogitekstiin, jossa kerrotaan kaappauksesta ja siitä, miten uusia osaajia alalle tarvitaan https://poliisi.fi/blogi/-/blogs/tieto-tarvitsee-tulevaisuuden-turvaajia

# 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