TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Kybersää

## Helmikuu 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 helmikuu 2021

## Tietomurrot ja -vuodot

- Ranskan tietoturvaviranomainen ANSSI julkaisi raportin Centreon-ohjelmistoihin kohdistuneista tietomurroista
- Julkaisimme kaksi artikkelia liittyen tunkeutumisen laajentamisen estämiseen ja toiminnan tunnistamiseen

## Huijaukset ja kalastelut

- OmaPosti-teemaiset huijaustekstiviestit piinasivat suomalaisia päivittäin.
- Veronpalautuksen verukkeella kalasteltiin viattomien veronmaksajien luottokorttitietoja.

## Haittaohjelmat ja haavoittuvuudet

- Punainen varoitus 1/21: Exchange-palvelimen haavoittuvuuksista
- BazarStrike-kampanjassa haittaohjelman levitysyritystä roskapostin kautta

## Automaatio ja IoT

- Dragos julkaisi vuosiraportin teollisuusautomaation tietoturvasta
- Etähallittavissa automaatio- ja IoT-palveluissa havaittavissa helppokäyttöisyyden priorisointia tietoturvan kustannuksella

## Verkkojen toimivuus

- Viisi merkittävää häiriötä yleisissä viestintäpalveluissa. Vaikutukset melko pieniä.
- Kotimainen teleoperaattori massiivisen palvelunestohyökkäyksen kohteena. Hyökkäys aiheutti merkittävää internet-liikenteen hidastelua asiakkaille noin tunnin ajan.

## Vakoilu

- Microsoftin mukaan Kiinaan linkitetty APT-ryhmä Hafnium hyödynsi sen Exchange-sähköpostipalvelimien nollapäivähaavoittuvuuksia tietojen varastamiseen.
- Suomalaisten yritysten ja yksityishenkilöiden verkkoreitittimiä on käytetty ulkomaisten tiedustelupalvelujen toimesta kybervakoiluun.

# Kuukauden tunnuslukuja

~2300

VUOSI SITTEN HELMIKUUSSA SAIMME ENSIMMÄISET ILMOITUKSET TEKNISEN TUEN HUIJAUSPUHELUISTA. VUODEN AIKANA ILMOITUKSIA ON TULLUT TUHANSIA EIKÄ LOPPUA NÄY! LÄHES 700 ILMOITUSTA TULI PELKÄSTÄÄN 2/2020 AIKANA. KAIKISTA TAPAUKSISTA EMME EDES SAA ILMOITUSTA.

1

HELMI-MAALISKUUN TAITTEESSA JULKAISTU HAAVOITTUVUUS MICROSOFTIN EXCHANGE-PALVELIMISSA ON VAKAVA JA TEIMME TÄSTÄ PUNAISEN VAROITUKSEN!

1

PÄÄSIMME KERTOMAAN KANSANEDUSTAJILLE KYBERTURVALLISUUDEN MERKITYKSESTÄ, KUN HEILLE JÄRJESTETTIIN HELMIKUUSSA TIETOTURVAKOULUTUSTA

# Varoitus 1/2021 Exchange-palvelimen haavoittuvuuksia käytetään aktiivisesti hyväksi (1/2)

- Julkaisimme punaisen varoituksen 3.3.2021
- Kyberturvallisuuskeskus päivitti 8.3. punaista varoitustaan - useiden suomalaisten organisaatioiden sähköpostipalvelimet tietomurron kohteena
- Haavoittuvuuksien avulla hyökkääjät pääsivät sähköpostipalvelimen avulla uhrien sähköpostitileille. Tämän jälkeen hyökkääjät ovat asentaneet haittaohjelman, jonka avulla he ovat vahvistaneet jalansijaa uhrin ympäristössä.
- Tilanne ei edellytä toimenpiteitä yksittäiseltä käyttäjältä tai kuluttajalta.
- Lue koko varoitus: https://www.kyberturvallisuuskeskus.fi/fi/varoitus-exchangen-hyvaksikaytetty-haavoittuvuus

# Varoitus 1/2021 Exchange-palvelimen haavoittuvuuksia käytetään aktiivisesti hyväksi (2/2)

- Tietoturvavastaava, tutustu ohjeisiimme: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeita-webshell-takaporttien-etsimiseen
- Mikäli organisaatiolla on tai on ollut käytössään haavoittuva Exchange-palvelin, tulee organisaatiossa toteutettavien toimenpiteiden lähtökohtana olla, se että organisaatio on joutunut onnistuneen tietomurron kohteeksi. On huomioitava, että pelkkä ohjelmistopäivityksen asentaminen ei riitä pitämään hyökkääjää loitolla.
- Kyberturvallisuuskeskus kehottaa kaikkia suomalaisia organisaatioita, joilla on haavoittuva Exchange-sähköpostipalvelin, ryhtymään välittömiin toimenpiteisiin haavoittuvuuksien korjaamiseksi sekä hyökkääjien asentamien ns. takaporttien löytämiseksi ja korjaamiseksi.

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

**1**

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

**2**

**Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy** ja uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

**3**

**Haavoittuvuuksien hyväksikäyttö on nopeaa**, mikä edellyttää nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

*kohonnut*

*laskenut*

*ennallaan*

*Keltainen* = uutta/ päivitettyä*

**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.

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

## 1

**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.

- Tietojenkalastelu on ollut hyvin yleistä pidemmän aikavälin tarkastelulla. 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 vääriä 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

## 2

**Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy** ja uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse.
- Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia rikollistoimijoita tulee jatkuvasti.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Myös palvelunestohyökkäyksiä käytetään hyödyksi ja niillä uhkaillaan sekä kiristetään organisaatioita.

**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.

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

## 3

**Haavoittuvuuksien hyväksikäyttö on nopeaa**, mikä edellyttää nopeita päivityksiä tai muita toimenpiteitä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- 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.
- Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

**CASE**

Marraskuussa hakkeriryhmä julkaisi 50 000:n haavoittuvan VPN-laitteen tiedot verkossa. Haavoittuvuus oli tullut julki jo vuonna 2018 ja siihen oli ollut olemassa korjaava päivitys siitä asti.

Organisaatiot, jotka eivät olleet päivittäneet laitteitaan ajan tasalle joutuivat listalle. VPN-tunnukset mahdollistavat hyökkääjälle organisaation verkon haltuunoton ja esimerkiksi haittaohjelman asentamisen. On ensisijaisen tärkeää päivittää laitteet ajallaan, kuten tämäkin esimerkki opettaa.

# **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 siitä 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. Erään raportin julkaisussa tapahtuneiden epäselvyyksien johdosta pilvipalveluntarjoajaa pyydetään toimittamaan lokitiedot kyseisen 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 mikäli 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 sekä 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 trendejä tietomurroista ja –vuodoista. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita sekä mainetappioita.

# Tietomurrot ja -vuodot

- Julkaisimme kaksi osaa Tietoturva Nyt!-juttusarjasta ”Tunnetko tunkeutumisen laajentamisen”
  - Suomeen ja suomalaisiin kohdistetaan tietomurtoja, joissa pyritään tunkeutumisen laajentamisen keinoin luomaan hyökkääjälle mahdollisimman edullinen asema ja työrauha
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-1
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-2

**ANALYYSI**

- Mitä kauemmin hyökkääjä toimii organisaation verkossa, sitä todennäköisemmin hän onnistuu tavoitteessaan. On erittäin tärkeää, että hyökkäykset havaitaan ajoissa.
- Hyökkääjä pyrkii tyypillisesti sulkemaan ja estämään tietoturvamekanismien ja -järjestelyiden toiminnan, jotta saisi toimia kohteessa häiriöttä.

# Tietomurrot ja -vuodot

- Centreon-järjestelmähallintaohjelmisto, jota käytetään palvelinympäristöjen valvontaan
  - Ranskan tietoturvaviranomainen ANSSI julkaisi raportin Centreon-ohjelmistoihin kohdistuneista tietomurroista
  - Kampanja kohdistui IT-alan palveluntarjoajiin
  - Ensimmäiset uhrit ovat tulleet ilmi jo vuonna 2017 ja kampanja on ollut aktiivinen vuoteen 2020 asti
  - Hyökkääjät pyrkivät murtamaan internettiin avoinna olevia Centreon-järjestelmiä ja pääsemään sieltä kohteen verkkoon
  - Centreon-järjestelmiä on käytössä myös suomalaisissa organisaatioissa, mutta Kyberturvallisuuskeskukselle ei ole tullut ilmoituksia niihin kohdistuneista tietomurroista

**ANALYYSI**

- Ympäristöjen monitorointi- ja hallintajärjestelmät tulisi eriyttää erilliseen verkkosegmenttiin, eikä niiden tulisi olla saavutettavissa suoraan avoimesta internetistä.

# Huijaukset ja kalastelut

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

# Huijaukset ja kalastelut

- Kuukauden aikana kalasteltiin taas pankkitunnuksia ja luottokorttitietoja eri palveluiden nojalla lähetetyillä huijausviesteillä. Huijauksia tehtailtiin mm. Netflixin, DHL:n, Amazonin ja eri pankkien nimissä.
- Teams- ja Zoom-kokouskutsuiksi naamioidaan huijausviestejä. Kutsuissa olevat linkit johtavat kuitenkin vain tietojenkalastelusivuille.
- OmaPosti-teemaisia tekstiviestihuijauksia lähetettiin jälleen tuhansittain. Määrä tuntuu aina vain lisääntyvän ja uusia huijaussivustoja syntyy kun entisiä saadaan poistettua.

**ANALYYSI**

- Omaposti-teemaiset tekstiviestihuijaukset
  - Omaposti-viesteiksi naamioiduissa tekstiviesteissä houkuteltiin taas huijaussivustolle, jolla tarjottiin Android-puhelimille FakeCop/FakeSpy-haittaohjelmaa.
  - Haittaohjelma lähettää puhelimesta tuhansittain tekstiviestejä liittymän laskuun.
  - Apple-puhelimilta kalasteltiin käyttäjätunnuksia tai yritettiin saada lupaa maksaa maksuja.
  - Huijaussivu piileskeli .top- ja .xyz-päätteisten verkkotunnusten suojissa ja vaihtoi paikkaa aina kun edellinen saatiin poistettua.

# Huijauksia ja petoksia

- Veronpalautusteemaa käytetään jälleen huijausviesteihin. Sähköpostiviesteissä luvataan veronpalautusta, mutta linkki johtaakin tietojenkalastelusivulle.
- Koronavirusteemaa käytettiin luottokorttitietojen kalasteluun. Sähköpostitse lupailtiin pääsyä rokotusjonojen ohitse, mutta sitä varten piti antaa luottokortin numero ja huijaustahan sekin kaikki valitettavasti on.

**VANHAN ILMIÖN UUDET METKUT**

- Veronpalautusteemaiset huijausviestit toistuvat säännöllisesti ja sitkeästi vuosittain.
- Tänä keväänä on nähty huijausviestejä, joissa vastaanottajalle luvataan 136,99 euron veronpalautus. Tarvitsee vain klikata linkkiä ja täyttää lomake.
- Huijauslomakkeella kalastellaan veronmaksajilta luottokorttitietoja rikollisille.
- Suomenkielisten huijausten kieliasu on melko hyvää, muttei kuitenkaan virheetöntä. Se on silti riittävän hyvää ollakseen uskottava. Myös palautuslomakkeen verkkosivun osoite on onnistuttu hämäämään melko uskottavaksi.

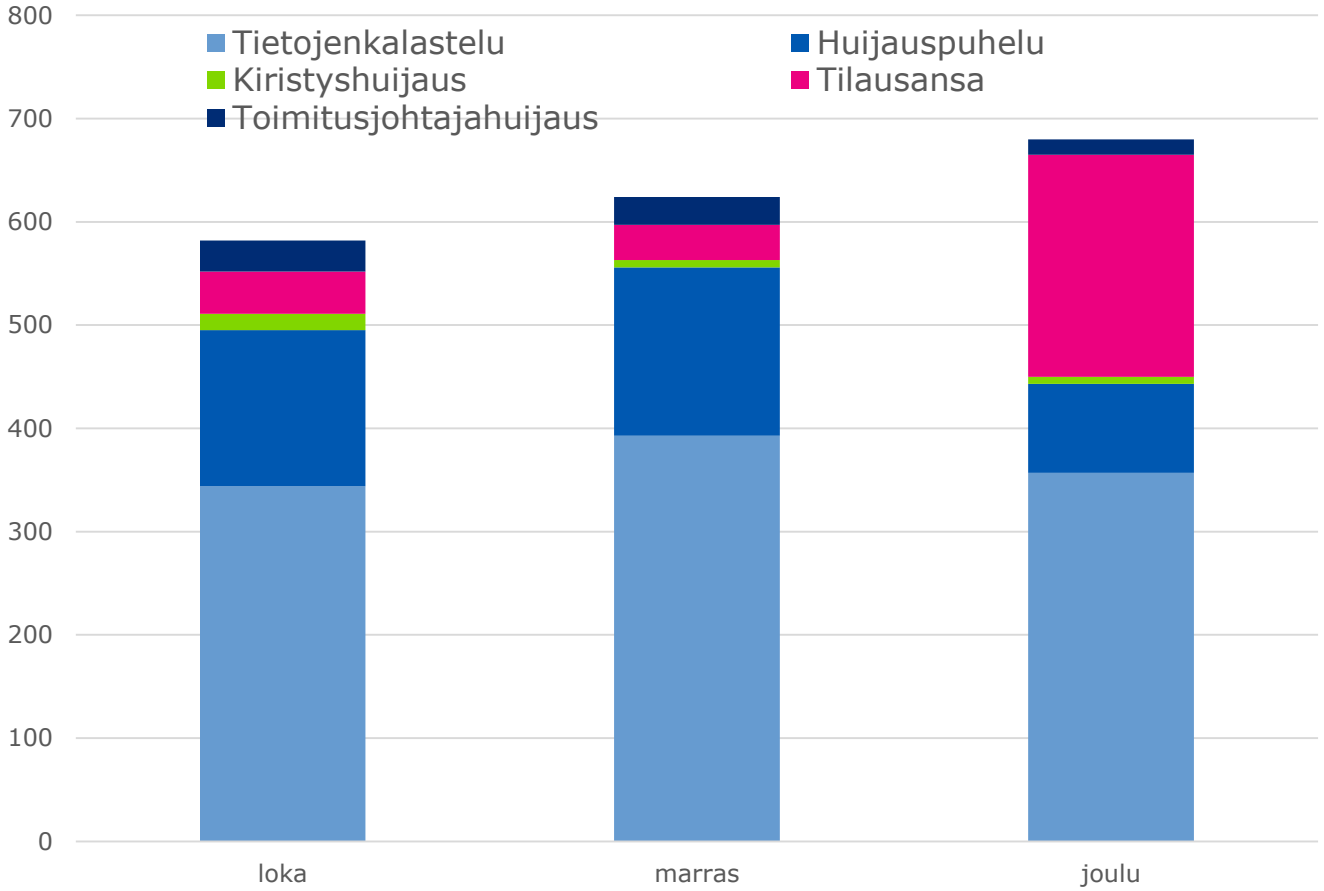
# Teknisen tuen nimissä soittelu jatkuu

- Microsoftin nimissä soittelevat puhelinhuijarit jatkavat edelleen suomalaisten kuluttajien kiusaamista. Helmikuussa Kyberturvallisuuskeskukselle ilmoitettiin jälleen kymmeniä huijauspuheluita.
- Tuntemattomaan numeroon vastaaminen ei ole vaarallista eikä siitä koidu kuluja. Soittajalle ei kuitenkaan pidä kertoa pankkitunnuksia, salasanoja eikä henkilötietoja.
  - Yhteistä tapauksille on soittajan halu saada ”asiakkaan” koneelle etähallintayhteys, jolla uhrin tietoihin pääsee käsiksi. Etäyhteyteen käytetään TeamVieweria tai muuta vastaavaa etähallintasovellusta.

**ANALYYSI**

- Valvomaton pääsy organisaation työasemalle määrittämättömäksi ajaksi on merkittävä tietoturvariski.
- Yrityksen tulee varmistaa keinot selvittää tapaus jälkikäteen. Uhri harvoin pystyy kertomaan tarkasti, mitä etäyhteyden kautta tehtiin teknisen selvittämisen mahdollistamiseksi.
- On tärkeä varmistaa lokituksen toimivuus, jotta mahdollinen onnistunut huijaus ja koneelle pääsy voidaan jälkikäteen selvittää niiden avulla.
- Turvallisuuskulttuurin merkitys korostuu: jos oviakaan ei avata tuntemattomalle, miksi tietokoneelle pitäisi päästä tuntematon taho?
- Yksityishenkilön ei ole tarpeen säilyttää käyttämätöntä etähallintaohjelmaa asennettuna laitteella.

# Käsiteltyjä huijaustapauksia Q4/2020




- Viimeisen neljänneksen 2020 näkyvimmät trendit ovat olleet:
  - Jatkuvat Postin nimissä tehdyt huijaukset, jotka johtavat tilausansoihin, pikavippeihin, tai puhelimen haittaohjelmaan.
  - Teknisen tuen huijauspuhelut jatkuivat, mutta laantuivat loppuvuonna.
- 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.

# Haittaohjelmat

- Kyberturvallisuuskeskus on saanut ilmoituksia haittaohjelman levitysyrityksistä roskapostin (malspam) kautta
  - Kyseessä on BazarLoader-troijalaisen kautta levitettävä Cobalt Strike-haittaohjelma, kampanjasta käytetään myös nimitystä ”BazarStrike”
  - Viestejä on lähetetty usealle eri sektorille ja kampanja oli hyvin aktiivinen
  - Haittaohjelman aktivoituminen organisaatiossa voi edetä nopeasti ja päätyä lopulta esim. Ryuk-kiristyshaittaohjelman aktivoitumiseen
  - Kampanja on aktiivinen myös maailmalla, ja haittaohjelmaa levittävät sähköpostit on kirjoitettu englanniksi

**ANALYYSI**

- Sähköpostien linkkien avaamisessa ja .exe-tiedostojen suorittamisessa tulee käyttää harkintaa, sillä sähköposti on yhä yleisin keino levittää haittaohjelmia
- Käyttäjien kouluttaminen haitallisten sähköpostien havaitsemiseen voisi ehkäistä vahinkojen syntymistä

# Haittaohjelmat

- TietoEVRY kiristyshaittaohjelmahyökkäyksen kohteena Norjassa
  - Maanantaina 22.2. TietoEVRY havaitsi teknisiä häiriöitä useissa palveluissa
  - Selvitystöiden jälkeen häiriöiden aiheuttajaksi paljastui kiristyshaittaohjelmahyökkäys
  - Tapahtuma ei vaikuta TietoEVRYn suomalaisiin asiakkaisiin

**ANALYYSI**

- Kiristyshaittaohjelmatartuntaan on hyvä varautua ja toimintaa tartuntatilanteessa on hyvä harjoitella etukäteen
- Tapaus osoittaa, että keinot haittaohjelman leviämisen estämiseksi ovat hyödyllisiä vahinkojen rajaamisessa, julkaisimme kaksi artikkelia aiheeseen liittyen

  https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-1

  https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-2

# Helmikuun haavoittuvuusjulkaisut

- Haavoittuvuuksia VMwaren tuotteissa - päivitä heti (6/2021)
- Microsoft korjasi kriittisiä haavoittuvuuksia Exchange Serverissä (7/2021)
  - Julkaisimme Exchange-haavoittuvuuksista myös punaisen varoituksen ja aiheesta kertovan TTN-artikkelin
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

**ANALYYSI**

- Vmwaren selainpohjaisen hallinta-alustan tulisi olla verkkoteknisesti rajattu niin, että se on näkyvissä ainoastaan sisä-/hallintaverkossa eikä näkyvissä avoimeen internettiin
- Päivitykset tulee asentaa viipymättä, haavoittuvuuksien hyväksikäyttö on todella nopeaa
- Kriittisten palveluiden hallintarajapintojen näkyvyys internetiin on asia, jota tulisi jatkuvasti seurata
- Kehoitamme kartoittamaan mitä palveluita omasta organisaatiosta on avoinna internetiin

# Automaatio ja IoT

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

# Automaatio

- Tietoturvayritys Dragos on julkaissut vuosiraporttinsa teollisuusautomaation tietoturvasta
  - Dragosin konsultoimissa asiakasongelmissa 90 prosentissa paljastui, että asiakas ei kyennyt havainnoimaan automaatiojärjestelmäänsä riittävän tarkasti
  - Dragosin mukaan 22 prosentissa haavoittuvuustiedotteista ei sisältänyt korjaavaa ohjelmistopäivitystä. Näistä 64 prosentissa ei ollut myöskään ohjeita riskin pienentämiseksi.
  - Niissä 78 prosentista haavoittuvuustiedotteita, joissa oli mukana korjaava ohjelmistopäivitys, 61 prosentissa ei annettu muita keinoja riskin pienentämiseksi kuin päivityksen asentaminen.
  - https://hub.dragos.com/2020-year-in-review-download?submissionGuid=5d105f06-a484-4587-9a48-b8345c98ee92

**ANALYYSI**

- Havainnointikyky on ikuisuusongelma, joka näkyy voimakkaasti myös automaatiojärjestelmissä.
- Automaatiolaitteiden haavoittuvuuksien hallinta on vaikeaa muun muassa siksi, että valmistajien haavoittuvuustiedotteissa usein on vain vähän tietoa hallinnan tueksi.
- Ohjelmistopäivitysten asentaminen automaatiojärjestelmiin viivästyy usein siksi, että käyttäjät haluavat varmistaa päivitysten toimivuuden ennen niiden asentamista tuotantoympäristöön. Lisäksi päivityksiä tehdään yleensä vain ennalta suunniteltujen huoltokatkojen aikana, joita saattaa olla vain kerran vuodessa.
- Automaatiojärjestelmien valmistajat voisivat parantaa huomattavasti alan turvallisuutta lisäämällä haavoittuvuustiedotteisiinsa suosituksia riskin pienentämiseksi myös ilman ohjelmistopäivityksen asentamista.

# Automaatio

- Käytettävyys ja saatavuus määritellään toisinaan automaatio- ja IoT-järjestelmissä tärkeämmiksi kuin tiedon luottamuksellisuus tai yksityisyys.
  - Erilaisten automaatiojärjestelmien siirtyessä etähallittaviksi on niiden tietoturvasta ja niissä olevan tiedon suojaamisesta huolehdittava entistä paremmin.
  - Erään etenkin Euroopassa käytetyn pellettilämmitysjärjestelmän pilvipohjaisessa etähallintapaneelissa vierailevat voivat nähdä mm. palvelun käyttäjien, rakennusten ja lämmittimien tietoja.

**ANALYYSI**

- Kyberturvallisuuskeskus kehottaa palveluntarjoajia ja käyttäjiä arvioimaan huolellisesti eri hallintaratkaisuihin liittyvät tietoturvallisuusriskit
- Mikäli tarjoat tällaisia palveluja, selitä asiakkaillesi selvästi mitä tietoa julkaistaan vakioasetuksilla ja miten asetuksia voi muokata paremmin yksityisyyttä suojaavaksi.
- Mikäli käytät palveluita, testaa ja koita selvittää paljastaako palvelu sinusta tai omaisuudestasi tietoja, joita et haluaisi jakaa ulkopuolisille.

# Automaatio ja IoT

- Forescout raportoi Number: Jack -haavoittuvuudesta TCP/IP-pinon toteutuksessa (Initial sequence number -luonnissa ennakoitavuus).
  - Kyseessä jo pitkään tiedossa ollut haavoittuvuus, joka on pääosin korjattu. Forescoutin mukaan se aiheuttaa IoT-maailmassa edelleen ongelmia
  - https://www.forescout.com/company/blog/numberjack-forescout-research-labs-finds-nine-isn-generation-vulnerabilities-affecting-tcpip-stacks/
- Cujo AI on julkaissut artikkelin: Genetics of modern IoT attacks
  - Hyvä yleiskatsaus kuluttajamarkkinoiden IoT-laitteiden haavoittuvuuksiin ja siihen, miten kyberrikolliset käyttävät niitä hyväkseen.
  - https://cujo.com/genetics-of-a-modern-iot-attack/

# 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

- Helmikuussa tapahtui 5 merkittävää toimivuushäiriötä yleisissä viestintäpalveluissa.
  - Yksi niistä tapahtui Helsingissä 18.2., jossa harvinainen sähkökatko haittasi useiden yleisten viestintäpalveluiden toimintaa. Kuitenkin vain yhden teleyrityksen palveluiden häiriöt muodostuivat merkittäviksi.
- Nordean verkko- ja mobiilipankkipalveluissa oli 23.2. häiriöitä Suomessa ja muutamissa muissa maissa.

**ANALYYSI**

- Yleisten viestintäpalveluiden merkittävien häiriöiden määrä oli lähellä kuukausittaista keskiarvoa ja vaikutukset suhteellisen pieniä.
- Helsingin tapaus osoitti, että myös taajamissa, joissa sähköverkon toimivuus on hyvin varmistettu, tarvitaan viestintäverkkojen akkuvarmennuksia.
- Laajat pankkien ICT-palveluiden häiriöt ovat melko harvinaisia.

# Palvelunestohyökkäykset

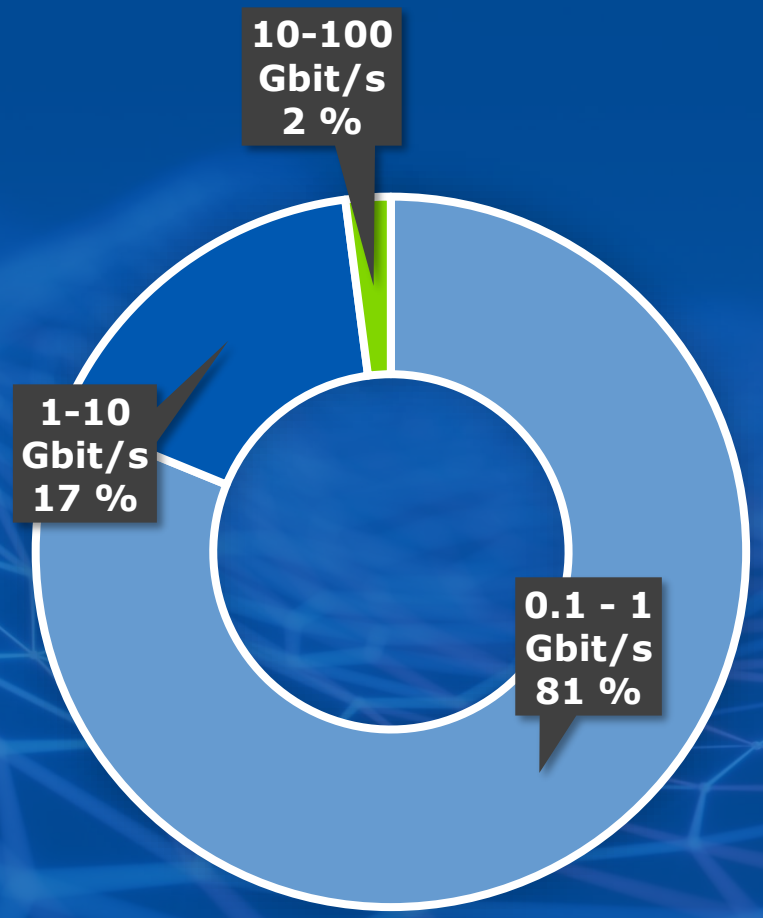
- Helmikuussa saimme ilmoituksia palvelunestohyökkäyksistä, joilla oli vaikutuksia organisaatioiden toimintaan.
  - Olemme saaneet viime aikoina aktiivisesti ilmoituksia palvelunestohyökkäyksistä ja toivomme edelleen, että ilmoitatte meille organisaatioihinne kohdistuneista tietoturvaloukkauksista. Yhteystiedot ilmoittamiseen löytyvät kybersään viimeiseltä sivulta.
- Palveluntarjoajat palvelunestohyökkäysten kohteena
  - Kotimainen teleoperaattori massiivisen palvelunestohyökkäyksen kohteena. Hyökkäys aiheutti merkittävää internet-liikenteen hidastelua asiakkaille noin tunnin ajan.
  - Palvelunestohyökkäyksillä on häiritty esimerkiksi yrityksen ajanvarausjärjestelmää.
  - Emoyhtiöön maailmalla kohdistunut palvelunestohyökkäys vaikutti Suomessa asti.
- Nimipalveluiden toiminnan suojaamiseksi suosittelemme ottamaan käyttöön maksuttoman toissijaisen hajautetun nimipalvelumme FI-verkkotunnuksille: https://www.traficom.fi/fi/hajautettu-nimipalvelu-valittajien-kayttoon

**ANALYYSI**

- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen. Kiristysviestien yhteydessä on havaittu yli 100 Gbps-hyökkäyksiä, joilla voi olla vaikutuksia pk-yrityksen toimintaan.
- Hyökkäyksiin varautumisessa tulisi huomioida sekä volumetriset että sovellustason hyökkäykset.

# Palvelunestohyökkäysten tunnuslukuja

- 61 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q4/2020.
- Noin 73% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.




**SUOMEEN KOHDISTUNEIDEN PALVELUNESTOHYÖKKÄYSTEN VOLYYMIT (Q4/2020 - 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

- Microsoftin Exchange-sähköpostipalvelimiin liittyvät nollapäivähaavoittuvuudet ovat johtaneet Suomessa ja maailmalla merkittävään joukkoon tietomurtoja organisaatioissa, joilla on ollut internetistä käsin saavutettavissa oleva Exchange-palvelin.
  - Nollapäivähaavoittuvuudesta kertonut Microsoft kutsuu alkuperäisen kampanjan taustalla olevaa toimijaa nimellä Hafnium. Microsoft arvioi ryhmän toimivan Kiinasta käsin, mutta huomauttaa sen toimintamalleihin kuuluvan muun muassa Yhdysvalloissa sijaitsevien virtuaalipalvelinten käyttämisen toiminnassaan.
  - Microsoftin mukaan Hafniumin kohteina on ollut muun muassa tartuntatauteja tutkivia tahoja, lakifirmoja, korkeakouluja, puolustusteollisuuden yrityksiä ja ajatushautomoita. Tietomurtojen tavoitteena vaikuttaa olleen tiedon varastaminen sähköpostitileiltä.
- Kyberturvallisuuskeskus on julkaissut haavoittuvuuksista ja niihin liittyvistä tietomurroista kriittisen varoituksen: https://www.kyberturvallisuuskeskus.fi/fi/varoitus-exchangen-hyvaksikaytetty-haavoittuvuus

**ANALYYSI**

- Haavoittuvuuden hyväksikäyttö kybervakoilussa ja verkkorikollisuudessa yleistyy todennäköisesti nopeasti.
- Haavoittuvat palvelimet on syytä päivittää välittömästi. Lisäksi järjestelmät tulee tarkistaa mahdollisen tunkeutumisen varalta, sillä haavoittuvuuksia hyödynnetään aktiivisesti.

# Vakoilu

- Suojelupoliisi varoitti suomalaista infrastruktuuria hyödyntävän kybervakoilun lisääntyneen. Kymmeniä suomalaisten yksityishenkilöiden ja yritysten verkkolaitteita ja palvelimia on käytetty hyväksi autoritääristen valtioiden tiedustelupalveluiden kybervakoiluoperaatioissa.
- Murretut laitteet ovat liitetty osaksi tiedustelupalvelun operaatiossa käytettävää infrastruktuuria, jolloin operaatioon liittyvä liikenne on ohjattu suomalaisen verkkolaitteen kautta. Tällöin kohdeorganisaatiolle hyökkäysliikenne näyttää tulevan suomalaisesta organisaatiosta tai yksityishenkilöltä.
- Laitteisiin on murtauduttu kirjautumalla julkisessa internetissä avoinna olevien hallintapaneelien kautta oletussalasanoja käyttäen.

**ANALYYSI**

- Esineiden internetiin lukeutuvien laitteiden, kuten reitittimien ja muiden verkkolaitteiden käyttö kyberhyökkäyksissä on tavanomaista niiden heikon tietoturvan tason vuoksi.
- Kyberturvallisuuskeskus suosittelee laitteiden omistajia pitämään huolta laitteidensa ajantasaisesta ohjelmistosta, rajoittamaan hyökkäyspinta-alaa ja vaihtamaan laitteiden oletussalasanat vahvoiksi.

# Vakoilu

- Muun muassa 2015 Ukrainan sähkökatkojen aiheuttajaksi arvioidun Sandworm-ryhmän epäillään olevan sekä ranskalaisiin IT-alan yrityksiin että yhdysvaltalaisiin energia-alan organisaatioihin kohdistuneiden tietomurtojen takana. Sandworm on linkitetty julkisissa lähteissä Venäjän sotilastiedusteluun.
  - Ranskan tietoturvaviranomainen ANSSI varoitti Centreon-nimiseen IT-ympäristön valvontatyökaluun kohdistuneesta murrosta, jonka seurauksena useita IT- tai hosting-palveluita tarjoavia yrityksiä oli Ranskassa joutunut tietomurron uhriksi. ANSSI on linkittänyt tietomurrot Sandwormiin, ja sen mukaan ryhmän läsnäolo kohdejärjestelmissä jatkui useiden vuosien ajan. (ks. myös osio Tietomurrot ja -vuodot)
  - Tietoturvayhtiö Dragos puolestaan kertoi vuosikatsauksessaan Sandwormiin linkittämänsä hakkeriryhmän pyrkineen murtautumaan useiden vuosien ajan yhdysvaltalaisiin energia- ja teollisuusalan organisaatioihin. Dragosin mukaan kouralliseen organisaatioita oli myös tuona aikana onnistuttu tunkeutumaan, mutta murrot eivät tiettävästi edenneet siihen pisteeseen, että tunkeutuja olisi aiheuttanut tuhoa järjestelmille tai haitannut niiden toimintaa.

**ANALYYSI**

- Teollisuusautomaatioon erikoistunut tietoturvayhtiö Dragos on arvioinut, että Sandworm-ryhmään linkittyy kaksi toisistaan tavoitteiltaan poikkeavaa ryhmittymää: Dragosin Kamacite-nimellä kutsuma ryhmä, joka vastaa jalansijan saamisesta järjestelmiin ja jonka toimia Dragos kuvaa nähneensä, ja toinen, joka pystyy toteuttamaan tuhovoimaisia, järjestelmien toimintaa vakavasti haittaavia tai estäviä kyberhyökkäyksiä.

# 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

**Lausuntopyyntö määräykseksi viestintäverkon kriittisistä osista sekä sen perustelumuistioksi**

- Määräyksen tarkoituksena on määritellä tarkemmin sähköisen viestinnän palveluista annetun lain (917/2014) 244 a §:ssä tarkoitetut viestintäverkon kriittiset osat.
- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=0c026e2d-3285-4b85-946d-d7d45cdb632a

**EU:n neuvosto vahvisti kantansa sähköisen viestinnän tietosuojasääntöihin**

- Jäsenmaat pääsivät 10.2.2021 sopimukseen neuvotteluvaltuutuksesta, joka koskee yksityisyyden ja luottamuksellisuuden suojaa sähköisten viestintäpalvelujen käytössä koskevien sääntöjen tarkistamista. Näin ollen ns. trilogineuvottelut lopullisesta tekstistä voidaan aloittaa Euroopan parlamentin kanssa.
- https://www.consilium.europa.eu/fi/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

**Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (COM (2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta (verkko- ja tietoturvadirektiivi)**

- Valtioneuvosto katsoo, että direktiiviehdotus sisältää kansallisen ennakkovaikuttamisen pääkohdat. Lisäksi ehdotus sisältää kansallisen tietoturvan ja tietosuojan parantamista koskevan työryhmän väliraportin johtopäätösten kanssa samansuuntaisia tavoitteita.
- https://www.eduskunta.fi/FI/vaski/Kirjelma/Sivut/U_9+2021.aspx

# Oikeudelliset asiat

HE (237/2020) laeiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta sekä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta annetun lain voimaantulosäännöksen muuttamisesta

**ANALYYSI**

- Hallituksen esitystä koskeva liikenne- ja viestintävaliokunnan mietintö valmistui. Valiokunta ehdotti ensimmäisen lakiehdotuksen henkilötietojen käsittelyä koskeviin säännöksiin lakiteknisiä muutoksia.
- Esityksellä jatkettaisiin ensitunnistamisen ketjuttamisen enimmäishintasääntelyä kahdella vuodella. Hinta olisi jatkossakin korkeintaan 0,03 euroa.
- Liikenne- ja viestintävirastolle esitetään uutta tehtävää kerätä ja muodostaa tilastotietoa vahvan sähköisen tunnistamisen markkinasta ja tarjonnasta sääntelyn vaikutusten seuraamista, sähköisen tunnistamisen markkinoiden ohjaamista ja lainsäädännön kehittämistä varten.
- Ks. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_237+2020.aspx ja https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/LiVM_6+2021.aspx

# ISO 27002 ohjeistus kommentoitavana

- Tietoturvan hallintajärjestelmästandardi ISO 27001:n vaatimuksia tarkentava ohjeistus ISO 27002 on uusittavana. Standardiluonnos on nyt kansainvälisellä lausuntokierroksella, ja siihen voi tutustua ja ottaa kantaa maksutta. Lausuntoaika päättyy 1.4.2021.

- Standardiluonnokseen pääsee tutustumaan täältä, palveluun tulee rekisteröityä: https://lausunto.sfs.fi/Home/Details/1282

# Arjen kyberturvallisuus – helmikuu

## Väärennettyjä puheluita teknisen tuen nimissä

- Suomalaisille organisaatioille ja yksityisille henkilöille on tullut runsaasti puheluita, joissa soittaja esiintyy teknisenä tukena. Soittaja väittää että uhrin tietokoneella on tietoturvaongelma ja pyytää avaamaan koneen korjatakseen sen.
- Ilmiö on vaivannut jo yli vuoden ajan, mutta on edelleen ajankohtainen!
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/rikolliset-kalastelevat-verkkopankkitunnuksia-hakutulosten-avulla

## Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus

- Postin nimissä lähetetään runsaasti huijauksia tekstiviestien välityksellä.
- Älä avaa viesteissä tulevia linkkejä harkitsematta, koska vastaan voi tulla haittaohjelmia, tietojenkalastelua ja tilausansoja.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

## Iäkkäiden tietoturvasta pitää huolehtia

- Kyberturvallisuuskeskuksen vt. ylijohtaja Sauli Pahlman toi esille Helsingin Sanomien mielipidekirjoituksessa ikäihmisten digitaidot.
- Viranomaisilla on oma roolinsa. Lisäksi haastamme digitaitoisia ihmisiä miettimään, miten itse voi auttaa lähellä olevaa ikäihmistä turvalliseen sähköiseen asiointiin.
- https://www.hs.fi/mielipide/art-2000007826142.html

## Hurjana vuonna 2020 kyberturvallisuus kosketti kaikkia

- Miltä näytti Tietoturvan vuosi 2020? Vastaamon tietomurto, pandemia ja etätyöt, Koronavilkku-sovellus, Emotet-haittaohjelma ja teknisen tuen huijauspuhelut tekivät kybervuodesta hurjan. Myös 5G:n tietoturva ja turvallisuussääntelyn muutostarpeet puhututtivat. Kertaa keskeiset käänteet katsauksestamme ja löydä eväät parempaan kyberturvallisuusvuoteen 2021.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hurjana-vuonna-2020-kyberturvallisuus-kosketti-kaikkia

# Ajankohtaista Kyberturvallisuuskeskuksesta

## Galileo Innovation Challenge antoi puhtia uusille innovaatioille

- Galileo Innovation Challenge keräsi vuonna 2019 kymmeniä osallistujia eri puolilta maailmaa Helsinkiin. Soitimme kolmelle tapahtumaan osallistuneelle tiimille ja kysyimme, mitä heille nykyään kuuluu.
- Esimerkiksi veneilijöiden Boato-sovellus on viittä vaille valmis ja Missing-Link tunnistaa ja paikantaa langattomia häiriölähteitä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/galileo-innovation-challenge-antoi-puhtia-uusille-innovaatioille

## Tunnetko tunkeutumisen laajentamisen

- Kirjoitimme juttusarjaa tunkeutumisen laajentamisesta, jonka osat 1 ja 2 on julkaistu.
- Suomi on osa globaaleja tietoverkkoja. Tämän seurauksena myös Suomeen ja suomalaisiin kohdistetaan tietomurtoja, joissa pyritään tunkeutumisen laajentamisen keinoin luomaan hyökkääjälle mahdollisimman edullinen asema ja työrauha.
- Lue lisää:
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-1
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-2

## Tonttu-projektit - uusien menetelmien toteutettavuustestaus

- Julkaisimme uuden sivun, jossa kerromme Tonttu kokeiluista
- Tonttu on kokeilumalli, jossa on useita erilaisia pilotteja. Pilottien avulla esimerkiksi testataan kevyitä ja skaalautuvia menetelmiä organisaatioiden suojattavien kohteiden tunnistamiseksi, niihin liittyvän tietoturvatiedon jakamiseksi, ja erityissuojattavien verkkojen eristyksen testaamiseksi.
- Tutustu sivuun:
- https://www.kyberturvallisuuskeskus.fi/fi/tonttu

# 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