TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 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 maaliskuu 2021

Tietomurrot ja -vuodot

- Exchange-tilanne on vakiintunut ja rauhoittunut maaliskuun alkupuolen jälkeen.
- Facebookista vuonna 2019 varastettuja tietoja on päätynyt julkisuuteen, joukossa on myös suomalaisten käyttäjien tietoja.

Huijaukset ja kalastelut

- OmaPosti-teemaiset huijaustekstiviestit ovat edelleen jokapäiväinen kiusa.
- Teknisen tuen huijauspuhelut piinaavat yhä suomalaisia – enimmäkseen englanniksi, mutta joskus myös huonolla suomella.

Haittaohjelmat ja haavoittuvuudet

- BazarLoader-haittaohjelmaa levitetään sähköpostin välityksellä. Kampanja tunnetaan myös nimellä ”BazarStrike”.
- OmaPosti-teemaiset tekstiviestit johtavat joissain tapauksissa myös haittaohjelmaan.

Automaatio ja IoT

- Verkkolaitevalmistaja Ubiquitin taustajärjestelmiin on tehty merkittävä tietomurto.

Verkkojen toimivuus

- Viisi merkittävää toimivuushäiriötä.
- Valtakunnallisten digitaalisten terveyspalveluiden käyttäjien tunnistamisessa toistuvia toimivuushäiriöitä.
- Etäopetusympäristöjen häirintä palvelunestohyökkäyksellä ei ole harmitonta hupia, vaan johtaa rikostutkintaan.

Vakoilu

- Eduskuntaan kohdistuneen tietomurron taustalla oli Suojelupoliisin mukaan APT31-operaatio.
- Useat Kiinaan linkitetyt APT-ryhmät ovat olleet viime aikoina aktiivisia eri puolilla maailmaa.

Kuukauden tunnuslukuja

194

MAALISKUUN AIKANA SAAPUNUTTA POIKKEAMIENHALLINTAILMOITUSTA, JOISSA EXCHANGE-TARKENNE.

1

HELMI-MAALISKUUN TAITTEESSA JULKAISTU HAAVOITTUVUUS MICROSOFTIN EXCHANGE-PALVELIMISSA OLI VAKAVA!

0

MAALISKUUN LOPUSSA TEKEMÄMME KARTOITUKSEN MUKAAN AVOIMENA VERKKOON NÄKYVIÄ PÄIVITTÄMÄTTÖMIÄ EXCHANGE-PALVELIMIA.

Poistimme varoituksen 1/2021 Exchange-palvelimen haavoittuvuuksia käytetään aktiivisesti hyväksi

- Julkaisimme punaisen varoituksen 3.3.2021. Päivitimme varoituksen 23.3. keltaiseksi, koska kyseessä ei ollut enää kriittinen tilanne. Varoitus päätettiin poistettiin 14.4, koska varoitukselle ei ole enää tarvetta.
- Kyberturvallisuuskeskus antaa noin 1-5 varoitusta vuoden aikana, eikä varoituksia anneta kevein perustein.
- Haavoittuvuuksien avulla hyökkääjät pääsivät sähköpostipalvelimen avulla uhrien sähköpostitileille. Tämän jälkeen hyökkääjät ovat asentaneet haittaohjelman, jonka avulla he ovat vahvistaneet jalansijaa uhrin ympäristössä.
- Suuri osa organisaatioista on tehnyt päivitykset haavoittuviin palvelimiin sekä aloittanut tietoturvatutkinnan tekemisen. tällä hetkellä verkkoon ei näy havaintojemme mukaan avoimia haavoittuvia palvelimia .fi-osoitteissa
- Katso lisää:

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 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.

↑ *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

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

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 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.

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.

- 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

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

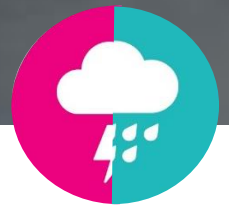
Lokitietojen puutteellisuus on riski monessa organisaatiossa.
Poikkeamatilanteita ei kyetä havainnoimaan ja selvittämään mikäli oikeiden järjestelmien tai sovellusten lokitietoja
ei kerätä, seurata ja säilytetä riittävän kauan.

- 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

- Exchange-tapauksen osalta on Suomessa saavutettu vakaa tilanne maaliskuun lopussa
  - Kyberturvallisuuskeskuksen tiedossa olevien murtojen määrä on 31.3. ollut: 74
  - Kontaktoidut organisaatiot: 253
  - Havaittujen haavoittuvien palvelinten määrä tällä hetkellä: 0
  - Tämän hetken arviomme mukaan akuuttivaihe on ohi, jonka vuoksi laskimme varoituksen punaisesta keltaiselle tasolle 23.3.
    https://www.kyberturvallisuuskeskus.fi/fi/varoitus-exchangen-hyvaksikaytetty-haavoittuvuus

ANALYYSI

- Toimitusketjujen hallinta on monimutkaista, monien tuotteiden ja palveluiden toimitusketjut sisältävät useita eri vaiheita, maantieteellisiä sijainteja ja paljon toimijoita
- Kyberriskienhallinnassa tulisi muistaa puhua myös toimitusketjuihin liittyvistä uhista

Tietomurrot ja -vuodot

- Facebookin vuonna 2019 varastettuja tietoja julkaistu
  - Henkilötietojen vaarantumisen vuoksi tapauksessa on lievä identiteettivarkauden riski.
  - Tiedossa ei ole vuodettu esimerkiksi luottokorttitietoja, henkilötunnusta eikä Facebookin salasanaa.
  - Vuodetut tiedot ovat pitkälti julkisia tietoja, pois lukien puhelinnumerot.
  - Tällä hetkellä ei ole helppoa tapaa tarkastaa, ovatko omat tiedot vuotaneiden tietojen joukossa.
  - Julkaisimme aiheeseen liittyvän Tietoturva Nyt! –artikkelin https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/facebookin-vuonna-2019-varastettuja-tietoja-julkaistu-mukana-14-miljoonan-suomalaisen

ANALYYSI

- Julkaisussa on mukana ainoastaan niitä tietoja, joita henkilö on itse lisännyt profiiliinsa, salasanat eivät ole mukana listalla
- Huijauspuheluiden ja -tekstiviestien määrä voi lisääntyä, kun tiedot ovat saatavilla kootusti ja puhelimen käytössä tuleekin olla tavallistakin valppaampi

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 näkyvin huijausaalto oli OmaPosti-teemainen tekstiviestikampanja. Huijaustekstiviestejä lähetettiin taas tuhansittain.
- Teknisen tuen puheluhuijauksia soitettiin paljon. Enimmäkseen puhelut olivat englanniksi, mutta maaliskuun erikoisuutena saatiin useita huonolla suomella soitettuja huijauspuheluita.
- Vilpilliset valeverkkokaupat väittivät myyvänsä maihinnousukenkiä, vaatteita, polkupyöriä ja muuta tavaraa, mutta oikeasti kalastelivat vain luottokorttitietoja.

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

- Office 365 -sähköpostitunnuksia kalastellaan edelleen, mutta niillä tehtävät tietomurrot ovat vähentyneet maaliskuussa 2021. Pakottaminen kaksivaiheiseen tunnistautumiseen on osoittautunut tehokkaimmaksi yksittäiseksi keinoksi vähentää tunnuskalastelulla tehtyjä tietomurtoja.
- COVID19-huijausteema nosti suosiotaan. Koronavirusteemaa käytettiin luottokorttitietojen ja käyttäjätunnusten kalasteluun sekä rokotekyselyn mukana levitettiin haittaohjelmaa. 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.

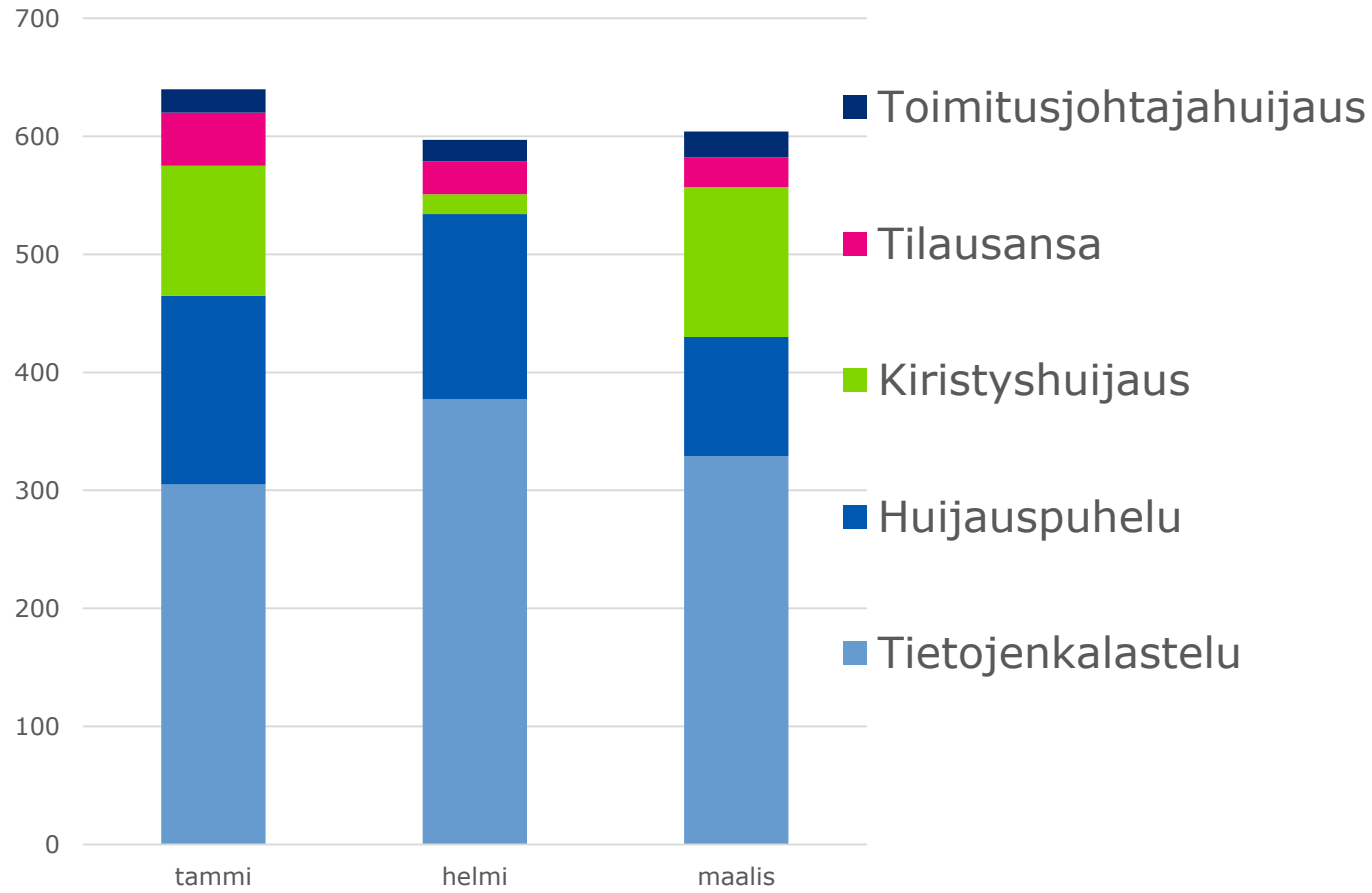
Teknisen tuen huijaukset jatkuvat

- Microsoftin nimissä soittelevat puhelinhuijarit jatkavat edelleen suomalaisten kuluttajien kiusaamista.
- Huijarimikrotuki haluaa asentaa etähallintaohjelman uhrin työasemalle. Etähallintaohjelmia asennetaan myös puhelimiin, minkä avulla huijari pääsee hallitsemaan uhrin puhelinta ja varastamaan sieltä tietoja.
- Tuntemattomaan numeroon vastaaminen ei ole vaarallista eikä siitä koidu kuluja. Soittajalle ei kuitenkaan pidä kertoa pankkitunnuksia, salasanoja eikä henkilötietoja.

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 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 aihealueen merkittävimmät julkaisut ja havainnot sekä annetaan toimenpidesuosituksia ja linkkejä lisätietoihin.

Haittaohjelmat

- OmaPosti-teemainen huijauskampanja jatkuu
  - Tekstiviesti sisältää linkin, viesti kehottaa allekirjoittamaan ja tarkistamaan OmaPostin kautta paketin
  - Kampanja on hyvin aktiivinen ja Kyberturvallisuuskeskus on saanut asiasta kasvavissa määrin ilmoituksia
  - Kampanjassa pyritään asentamaan FakeCop/FakeSpy-haittaohjelma Android-puhelimiin tai kytkeä Apple-tileihin toistuva mobiililaskutus
  - Saastuneet puhelimet saattavat lähettää edelleen tekstiviestejä niin kotimaahan kuin ulkomaillekin

ANALYYSI

- Ethän avaa viesteissä tulevia linkkejä harkitsematta. Vastaan voi tulla haittaohjelmia, tietojenkalastelua ja tilausansoja. Älä syötä tietojasi nettisivustoille, joiden aitoudesta et ole varma.
- Muista pyytää apua ja kysyä neuvoja, kehotamme myös kertomaan ilmiöstä tuttaville. Mikäli ilmiö ei ole itselle uusi, voi tietoisuuden levittäminen kuitenkin tavoittaa jonkun, jolle se onkin ennestään tuntematon.

Haavoittuvuudet

- Haittaohjelmaa levitetään roskapostilla (malspam)
  - Kyseessä on vanha kampanja, josta kerroimme helmikuussa
  - Viesti käyttää teemoinaan muun muassa asiakasvalituksia ja COVID-aiheisia irtisanomisilmoituksia. Kampanjasta käytetään myös nimeä "BazarStrike".
  - Hyökkääjä on ollut aktiivisena sisällä verkossa ja päässyt laajentamaan tunkeutumistaan
  - Kyberturvallisuuskeskuksen tietojen mukaan tarkoituksena on kiristyshaittaohjelman levittäminen verkkoon – näistä emme kuitenkaan saaneet ilmoituksia

ANALYYSI

- Tarkasta lokeista onko organisaatiostasi liikennöity tunnistetietojen mukaisiin komentopalvelinosoitteisiin
- Eristä saastunut työasema verkosta mahdollisimman pian ja tarkasta onko hyökkääjä onnistunut laajentamaan tunkeutumistaan

Maaliskuun haavoittuvuusjulkaisut

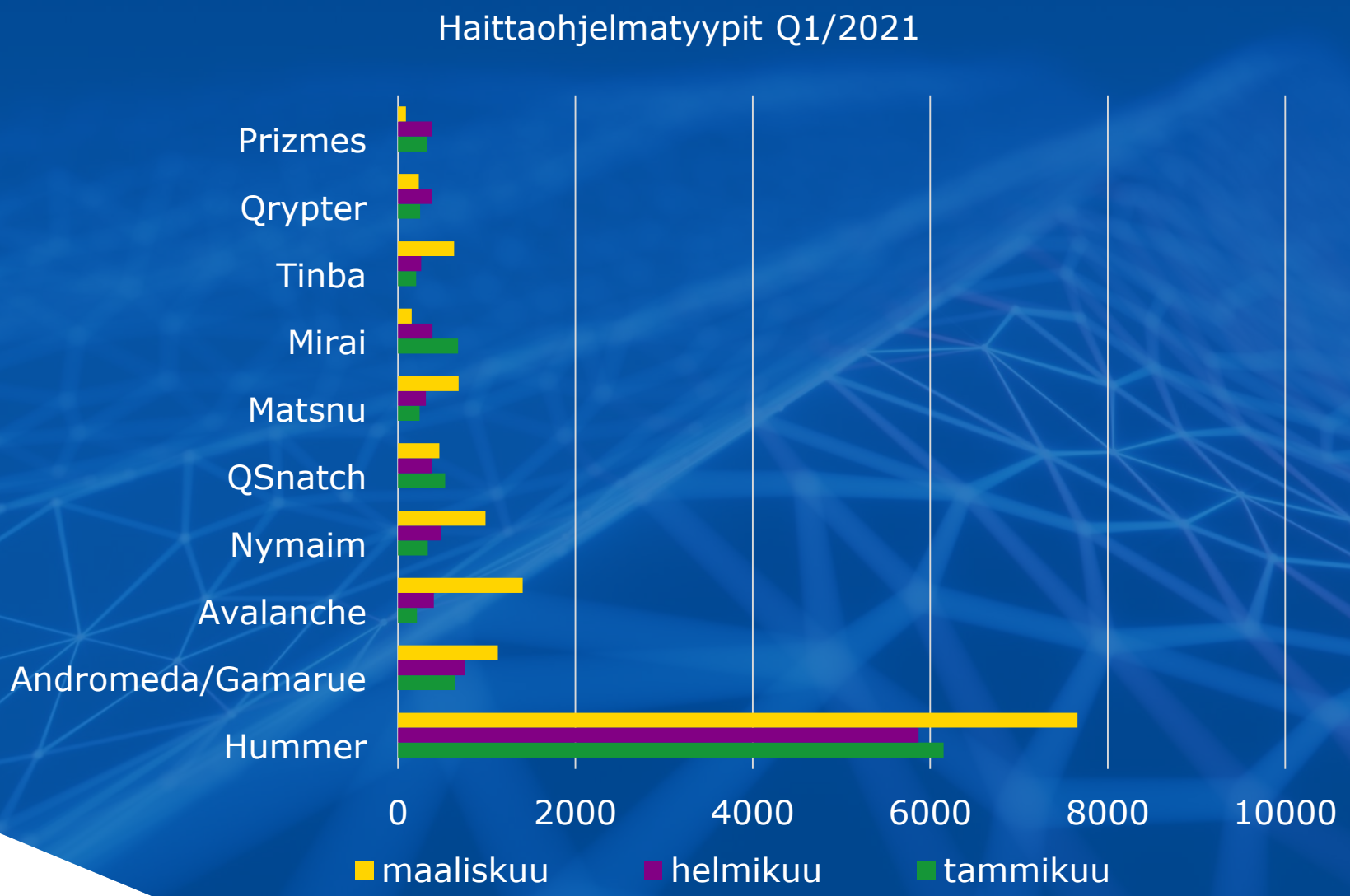
- Microsoft korjasi kriittisiä haavoittuvuuksia Exchange Serverissä (7/2021)
  - Hyväksikäyttö on ollut erittäin nopeaa ja laajamittaista
  - Käsitelty tarkemmin Tietomurrot ja –vuodot -osiossa
- Windows DNS-palvelimen haavoittuvuus mahdollistaa komentojen suorittamisen etänä (8/2021)
- Internet Explorer ja Edge-selaimien muistin korruptoitumishaavoittuvuus (9/2021)
- F5-laitteissa useita kriittisiä haavoittuvuuksia (10/2021)

- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

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

Haittaohjelmahavainnot



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.

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

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

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.

IoT

- Verkkolaitetoimittaja Ubiquitin taustajärjestelmiin on tehty merkittävä tietomurto
  - Murtautuja oli onnistunut saamaan haltuunsa pääkäyttäjäoikeudet palveluntarjoajan käyttämiin pilvipohjaisiin taustajärjestelmiin
  - Järjestelmien lokitus oli puutteellista, mikä vaikeutti todellisten vahinkojen arviointia
  - https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/

ANALYYSI

- Useimmat IoT-ekosysteemit hyödyntävät pilviteknologiaa
- Kyberhyökkäys IoT-palveluntarjoajan taustainfrastruktuuriin voi aiheuttaa huomattavia vaikutuksia laajan käyttäjäjoukon tietoturvaan, vaikka yksittäinen käyttäjä itse olisi huolehtinut oman IoT-laitteensa paikallisen verkkoympäristön tietoturvallisuudesta
- Tietomurto voi vaikuttaa merkittävästi yrityksen liiketoimintamahdollisuuksiin ja maineeseen

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

- Viisi merkittävää toimivuushäiriötä.
  - Useimmat niistä vaikuttivat muutamaan tuhanteen käyttäjään kerrallaan.
- Telia Inmics-Nebula otti Exchange-sähköpostipalvelunsa useiksi päiviksi irti internetistä.
  - Maaliskuun alussa julki tulleiden Microsoft Exchange -ohjelmiston haavoittuvuuksien hyväksikäyttö aiheutti vakavan uhkan palveluiden tietoturvalle.
  - https://www.inmicsnebula.fi/fi/tiedotteet/microsoft-exchange-palvelut-jalleen-kaytettavissa
- Australialaisen TV-kanava Channel Ninen lähetys katkesi kyberhyökkäyksen vuoksi.
  - Hyökkäyksen tekotavasta ja vaikutuksista ei ole julkisuudessa tietoja.
  - https://www.bbc.com/news/world-australia-56554641

ANALYYSI

- Yleisten viestintäpalveluiden merkittäviä häiriöitä oli tavanomainen määrä. Vaikutukset jäivät suhteellisen pieniksi.
- Tietoturvan häiriö voi aiheuttaa myös toimivuushäiriön, kuten Exchangen haavoittuvuudet ja Channel Ninen tapaukset osoittivat.

ICT-palveluiden toimivuus

- Valtakunnallisissa Terveyskylä-palveluissa häiriöitä maaliskuun alkupuolella.
  - Häiriö vaikutti mm. koronarokotusten ja -testausten ajanvarausten käyttämiseen. Syynä oli tekninen vika HUS:n tunnistautumispalveluissa.
  - https://www.tivi.fi/uutiset/tv/c9246f37-dd9a-4c1e-b7eb-461ccccbdf5e
- Useat Microsoftin pilvipalvelut ja Facebookin palvelut olivat estyneet maaliskuussa ympäri maailmaa.
  - Microsoftin palveluiden häiriö johtui Azure-palvelun käyttäjien tunnistamista koskeneesta vikatilanteesta. Lisätietoja: https://www.zdnet.com/article/microsofts-latest-cloud-authentication-outage-what-went-wrong/
  - Facebook ei ole julkaissut tietoja palveluidensa häiriöiden syystä. Reutersin lyhyt uutinen: https://www.reuters.com/article/us-facebook-outages-idUSKBN2BB232

ANALYYSI

- HUS:n operoimissa digitaalisissa terveyspalveluissa on ollut useita häiriöitä maaliskuun aikana. Digitaalisesti tarjottavien terveyspalveluiden lisääntyessä niiden häiriötkin vaikuttavat yhteiskuntaan entistä enemmän.
- Käyttäjien tunnistaminen on herkkä ja tärkeä osa tietojärjestelmien turvallisuutta.

Palvelunestohyökkäykset

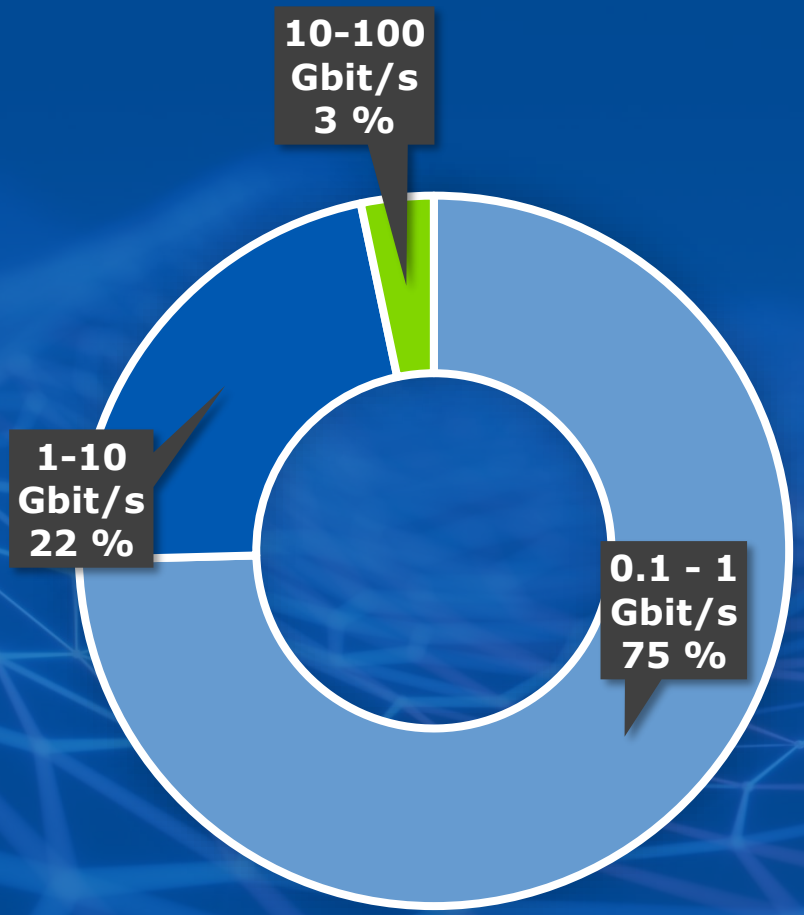
- Maaliskuussa saimme ilmoituksia palvelunestohyökkäyksistä eri sektoreilta, joilla oli myös vaikutuksia organisaatioiden toimintaan.
- Olemme saaneet ilmoituksia, missä sovellustason (http) palvelunestohyökkäyksillä on ollut vaikutuksia palveluihin.
  - Hyökkäykset voivat mennä mitigaatiopalveluidenkin ohi pienen voluumin vuoksi.
- Etäopiskeluympäristöihin kohdistuneet palvelunestohyökkäysten yritykset taas kasvussa.
  - Koronatilanteen aiheuttama etäopetukseen siirtyminen on aiheuttanut lieveilmiönä kasvua etäopiskeluympäristöihin kohdistuneissa haitantekoyrityksissä. Ilmiö huomattiin ensimmäisen kerran jo viime keväänä.
  - Etäopiskeluympäristöihin on kohdistunut etenkin palvelunestohyökkäyksiä, joilla pyritään lamauttamaan opiskeluympäristö. Tällä vaikeutetaan ympäristöä käyttävien oppilaiden ja opettajien työskentelyä. Vaikka merkittäviä vaikutuksia ei ole aiheutunut, myös palvelunestohyökkäysten yritykset aiheuttavat lisätöitä järjestelmien ylläpitäjille.

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

- 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

- Suojelupoliisin mukaan eduskuntaan kohdistuneen kyberhyökkäyksen taustalla oli APT31-nimellä kutsuttu operaatio. APT31 on aiemmin yhdistetty maailmalla muun muassa Yhdysvaltojen presidentinvaaleihin liittyneeseen mahdolliseen kybervakoiluun sekä Saksan julkishallintoon kohdistuneisiin kartoitus- ja tunkeutumisyrityksiin.
  - Myös Kyberturvallisuuskeskus on tehostanut valvontaansa Suojelupoliisin toimittamien tietojen avulla.
- Asiasta on käynnissä esitutkinta Keskusrikospoliisilla. KRP tutkii tapausta epäiltynä törkeänä tietomurtona, törkeänä vakoiluna ja törkeänä viestintäsalaisuuden loukkauksena. KRP kertoi selvittävänsä APT31-toimijan yhteyttä tietomurtoon.
- Eduskunta kertoi tietomurrosta vuodenvaihteessa. Sen mukaan joidenkin sähköpostitilien tietoturva vaarantui tietomurrossa ja näiden tilien joukossa oli myös kansanedustajien tilejä.

ANALYYSI

- Suojelupoliisi on varoittanut vakoilun painopisteen siirtyneen aiempaa enemmän tietoverkkoihin koronapandemianvuoksi. Esimerkiksi vuosikatsauksessaan Supo kertoi, että vuoden 2020 aikana havaittiin poikkeuksellisen intensiivisiä kybervakoiluyrityksiä, jotka kohdistuivat Suomen ulko- ja turvallisuuspoliittisen päätöksenteon valmisteluun: https://vuosikirja.supo.fi/vakoilun-painopiste-verkkoon

Vakoilu

- Kiinasta käsin toimivien APT-ryhmien aktiivisuudesta tuli maaliskuussa runsaasti uusia tietoja.
  - Useat Kiinaan linkitetyt ryhmät ottivat ESET:n mukaan työkalupakkiinsa aiemmin tänä vuonna julki tulleen Microsoft Exhange -haavoittuvuuden hyödyntämisen. Tähän joukkoon kuuluvat ESET:n mukaan ainakin Tick, Calypso, LuckyMouse (tunnetaan myös nimillä APT27 ja Emissary Panda) ja Winnti Group (tunnetaan myös nimellä APT41).
  - Recorded Future -tietoturvayhtiö kertoi RedEcho-nimisen APT-ryhmän yrittäneen tunkeutua Intian sähköverkkoon.
  - Tietoturvayhtiö Kasperskyn tutkijat kertoivat erityisesti Japaniin kohdistuneesta APT-kampanjasta, jonka ne linkittävät APT10-toimijaan.
  - Lisäksi Mustang Panda on pyrkinyt McAfeen mukaan varastamaan tietoja 5G-tekgnologiasta.

ANALYYSI

- Microsoft Exchangeen liittyvä vakava haavoittuvuus kuvaa hyvin nykypäivänä vallitsevaa tilannetta, johon organisaatioiden on hyvä varautua: yksi toimija hyödynsi aiemmin tuntematonta haavoittuvuutta jo ennen sen löytämistä, mutta sen lisäksi haavoittuvuuden julkitulon jälkeen haavoittuvuuden hyödyntäminen yleistyi nopeasti sekä kyberrikollisen että valtiollisten kybertoimijoiden keskuudessa. Organisaatioiden on varauduttava siihen, että ne pystyvät ketterästi reagoimaan uusiin, nopeasti nouseviin tietoturvauhkiin.

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

Liikenne- ja viestintäministeriö pyytää lausuntoja sähköisen viestinnän välitystietojen säilyttämistä koskevasta arviomuistiosta

- LVM pyytää näkemyksiä siitä, tarvitaanko kansalliseen sääntelyyn muutoksia ottaen huomioon unionin tuomioistuimen hiljattain antamat säilytysvelvollisuutta koskevat ennakkoratkaisut (viimeisimpänä asiassa C-746/18)
- Ks. lisätietoa LVM:n nettisivuilta: https://www.lvm.fi/-/arviomuistio-sahkoisen-viestinnan-valitystietojen-sailyttamisesta-lausunnoille-1263339
- LVM:n lausuntopyyntö lausuntopalvelussa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=8087aa19-7e03-4d3f-a292-ad2bc6a8bd90

Tunnistuslain muutokset tulivat voimaan 1.4.2021 (lait 230/2021 ja 231/2021)

- Muutoksilla jatketaan ensitunnistamisen ketjuttamisen hintasääntelyä 31.3.2023 asti, poistetaan yleisen henkilötietosääntelyn kanssa päällekkäistä sääntelyä ja asetetaan liikenne- ja viestintävirastolle uusi tehtävä koota vuosittain tilastotietoa sähköisen tunnistamisen markkinasta.

Hallituksen esitysluonnos ilmailulain ja ilmailun osalta liikenteen palveluista annetun lain, sähköisen viestinnän palveluista annetun lain ja rikoslain muutoksista lausunnoille

- Lausuntoaika päättyy 20. toukokuuta 2021.
- https://www.lvm.fi/-/ilmailulainsaadantoon-liikenteen-turvallisuutta-koskevia-tasmennyksia-1265588
- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=7c7db681-a721-4ce3-8f49-e130bf0b2221

Oikeudelliset asiat

Valtiovarainministeriön digitaalisen henkilöllisyyden kehittämishankkeessa laadittu arviomuistio on lausuttavana lausuntopalvelussa 30.4.2021 saakka.

ANALYYSI

- Liikenne- ja viestintävirasto on laatinut yhdessä kilpailu- ja kuluttajaviraston kanssa hankkeelle selvityksen sähköisen tunnistamisen nykytilasta.
- Traficomin tutkimuksia ja selvityksiä 2/2021 Sähköisen tunnistamisen markkinat https://www.traficom.fi/sites/default/files/media/publication/S%C3%A4hk%C3%B6isen_tunnistamisen_markkinat_-_S%C3%A4hk%C3%B6inen%20tunnistaminen%20turvallisen%20asioinnin%20mahdollistajana%2017%2003%202021p.pdf
- Valtiovarainministeriön lausuntopyyntö lausuntopalvelussa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=938337e8-306d-4737-bc4b-02bd2911f308&respondentId=9b962629-c21d-4f34-8064-56f40f1d6658

Oikeudelliset asiat

- YK:n alaisen UNECE:n E-säännöt koskien ajoneuvojen kyberturvallisuutta ja niiden hallintajärjestelmää sekä ohjelmistopäivityksiä ja niiden hallintajärjestelmää tulivat voimaan 22.1.2021.

ANALYYSI

- E-sääntö nro 155 – Yhdenmukaiset vaatimukset, jotka koskevat ajoneuvojen hyväksyntää kyberturvallisuuden ja sen hallintajärjestelmän osalta, ks. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:42021X0387&from=FI
  - EU:ssa pakollisiksi uusille ajoneuvotyypeille 7.7.2022 ja kaikille uusille ajoneuvoille 7.7.2024.
- E-sääntö nro 156 – Yhdenmukaiset vaatimukset, jotka koskevat ajoneuvojen hyväksyntää ohjelmistopäivitysten ja niiden hallintajärjestelmän osalta, ks. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX%3A42021X0388&from=FI
- Lisätietoja tyyppihyväksynnän pohjana olevasta sääntelystä, ks. https://www.traficom.fi/fi/liikenne/tieliikenne/tyyppihyvaksynta/saantely

Arjen kyberturvallisuus – maaliskuu

Facebookin vuonna 2019 varastettuja tietoja julkaistu - mukana 1,2 miljoonan suomalaisen tiedot

- Facebookista vuonna 2019 varastetut tiedot on uutisoinnin mukaan julkaistu internetissä hakkerifoorumilla. Tietoja on yhteensä 533 miljoonasta ihmisestä, joista suomalaisia on reilut 1,2 miljoonaa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/facebookin-vuonna-2019-varastettuja-tietoja-julkaistu-mukana-12-miljoonan-suomalaisen

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

Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä

- Huijarit ovat jälleen aktivoituneet aikuisviihdeteemaisten eli "pornokiristys" -huijausviestien lähettelyssä. Ne ovat huijausta, eikä huijareille pidä missään nimessä maksaa lunnaita.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pornokiristyksia-runsaasti-liikkeella-ala-usko-huijarien-vaitteita

Etäopiskeluympäristöihin kohdistuneet palvelunestohyökkäysten yritykset taas Kasvussa

- Koronatilanteen aiheuttama etäopetukseen siirtyminen on aiheuttanut lieveilmiönä kasvua etäopiskeluympäristöihin kohdistuneissa haitantekoyrityksissä. Ilmiö huomattiin ensimmäisen kerran jo viime keväänä.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/etaopiskeluymparistoihin-kohdistuneet-palvelunestohyokkaysten-yritykset-taas-kasvussa

Ajankohtaista Kyberturvallisuuskeskuksesta

Timanttiteko-palkinto 2020 Kyberturvallisuuskeskukselle

- Turvallisuuskomitea on myöntänyt vuoden 2020 Timanttiteko-palkinnon Kyberturvallisuuskeskukselle Yhteiskunnan turvallisuusstrategian tavoitteiden esimerkillisestä edistämisestä.
- Lue lisää: https://www.erillisverkot.fi/timanttiteko-palkinto-2020/

Traficomin vuosi 2020: varmistimme koronavuonna ihmisten, datan ja tavaroiden sujuvan ja turvallisen liikkumisen

- "Paransimme liikenteen ja digiyhteiskunnan toimintavarmuutta ja turvallisuutta Suomessa. Kyberturvallisuus nousi vuonna 2020 yhä strategisempaan rooliin kansalaisten palvelujen, yritysten tietojen ja toimitusketjujen suojaamisessa", painottaa Traficomin pääjohtaja **Kirsi Karlamaa**.
- Liikenne- ja viestintävirasto Traficom julkaisi Traficomin vuosi 2020 –katsauksen. Lue Lisää: https://www.traficom.fi/fi/ajankohtaista/traficomin-vuosi-2020-varmistimme-koronavuonna-ihmisten-datan-ja-tavaroiden-sujuvan

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio pähkinänkuoressa

- Haavoittuvuuskoordinaation tehtävänä on avustaa haavoittuvuuden tai vakavan ohjelmistovirheen löytäjää parempaan yhteistyöhön ohjelmistovalmistajien ja järjestelmäintegraattoreiden kanssa.
- Haavoittuvuusjulkaisujemme neljännessä osassa esittelemme Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatiota. Tutustu toimintaamme esimerkkitapausten kautta. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

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