TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 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 toukokuu 2021

Tietomurrot ja -vuodot

- Kesän kynnyksellä Office 365 – tietomurtoilmoituksia on alkanut jälleen tulla enemmän
- Ulkomailla on ollut useita merkittäviä tietomurtoja joissa tietomurtoon on yhdistetty myös kiristyshaittaohjelma

Huijaukset ja kalastelut

- Tekstiviestihuijaukset saastuttivat suomalaisten puhelimet. Räjähdysmäisesti levinnyt FluBot-haittaohjelma varastaa myös pankkitietoja.
- Suomenkieliset kiristyshuijaukset aktivoituivat jälleen loppukuusta.

Haittaohjelmat ja haavoittuvuudet

- Mobiililaitteisiin kohdistuvat haittaohjelmat ovat olleet aktiivisia
- Julkaisimme Flubotista Keltaisen varoituksen 4.6.
- Microsoftin kuukausittaisessa päivityspaketissa julkaistiin korjaukset 55 haavoittuvuut joista 4 oli kriittistä

Automaatio ja IoT

- Colonial Pipelinen toimistoverkon kiristyshaittaohjelmatartunta vaikutti myös tuotantojärjestelmiin
- Traficomin IoT-tietoturvavaatimuksia käsittelevän webinaarin tallenne saatavilla

Verkkojen toimivuus

- Toukokuussa Suomessa vain kolme merkittävää toimivuushäiriötä
- Salesforcen palveluiden käyttökatko johtui inhimillisestä virheestä
- Toukokuussa meille ilmoitettujen palvelunestohyökkäysten määrä väheni, mutta hyökkäysten koko oli ennätysluokassa.

Vakoilu

- APT29-ryhmä on lähettänyt kohdistettuja haitallisia sähköposteja isolle joukolle vastaanottajia.
- Yhdysvaltojen NSA:ta syytetään virkamiesten ja poliitikkojen vakoilusta Saksassa, Ranskassa, Ruotsissa ja Norjassa Tanskan kautta vuosina 2012–2014.

Kuukauden tunnuslukuja

260 GBIT/S

MEILLE ILMOITETTIIN MAHDOLLISESTI SUURIMMASTA PALVELUNESTOHYÖKKÄYKSESTÄ SUOMESSA TÄHÄN ASTI.

1

KUUN VAIHTEESSA JULKAISIMME KELTAISEN VAROITUKSEN TEKSTIVIESTITSE LEVITETTÄVISTÄ ANDROID-HAITTAOHJELMISTA.

8

KERÄSIMME KAHDEKSAN VINKKIÄ ERI LÄHTEISTÄ TUOTANTOJÄRJESTELMIEN SUOJAAMISEKSI.

Varoitus 2/2021 Tekstiviestitse levitettävät Android-haittaohjelmat

- Julkaisimme keltaisen varoituksen 4.6.2021
- Pakettiteemaisia huijausviestejä lähettävä FluBot-kampanja on aktivoitunut Suomessa.
- Haittaohjelma on kohdistettu kaikille, joilla on käytössään Android-laite ja matkapuhelinliittymä. Tekstiviestit saapuvat myös muihin laitteisiin, mutta .apk-asennuspaketti ei toimi esimerkiksi iPhonella.
- Kyberturvallisuuskeskus on aiemmin tänä vuonna viestinyt FakeCop/FakeSpy -haittaohjelmasta, joka toimii samankaltaisesti kuin FluBot.
- Lue koko varoitus: https://www.kyberturvallisuuskeskus.fi/fi/tekstiviestitse-levitettavat-android-haittaohjelmat

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

- Office 365 -kalasteluviestejä käytetään jälleen aktiivisesti murtautumiseen
  - Kaapattuja sähköpostitilejä käytetään uusien kalasteluviestien lähetykseen ja sähköpostiliikenteen varastamiseen
  - Myös teollisuus-, energia- ja terveydenhuoltosektoreilla on ollut liikkeellä tietomurtoihin johtanut tietojenkalastelukampanja
  - Vuonna 2020 ensimmäisen viiden kuukauden aikana ilmoituksia tuli 538
  - Vuonna 2021 ensimmäisen viiden kuukauden aikana ilmoituksia tuli 368

ANALYYSI

- Monivaiheisen tunnistautumisen käyttöönotto estää suurimman osan tunnuskalastelun avulla tehdyistä tietomurroista
- Monipuoliset suojaukset, lokituksen seuranta, päätelaitteiden hallinta ja henkilöstön koulutus ovat avaintekijöitä suojautumisessa

Tietomurrot ja -vuodot

- Tietomurtojen yhteydessä käytetään usein myös kiristyshaittaohjelmia
  - Rikollisryhmä WIZARD SPIDER hyökkäsi Irlannin terveysministeriötä ja sitten Irlannin terveysviranomaista (HSE) vastaan
  - Hyökkäys ministeriön järjestelmiin saatiin torjuttua ennen kuin rikolliset ehtivät käynnistää tiedostojen salaamisen sekä HSE:n että ministeriön tietokoneilta löytyi lunnasvaatimus
  - Irlannin pääministeri on sanonut, että maa ei aio maksaa lunnaita
  - Hyökkäys tunnistettiin ministeriössä torstai-iltapäivästä 13.5. ja ministeriö pystyi torjumaan sen ennen kuin rikolliset ehtivät käynnistää tiedostojen salaamisen
  - Rikolliset ehtivät kuitenkin jättää ministeriön tietojärjestelmiin kiristysviestin, jossa ministeriötä vaaditaan maksamaan lunnaat, jotta se saisi salauksen purkamiseen tarvittavat tiedot

ANALYYSI

- Irlannin julkinen sairausvakuutus ja terveydenhuolto, Health Service Executive (HSE) pyörittää sekä rahoittaa Irlannin julkista terveydenhuoltoa terveysministeriön puolesta
- Kiristyshaittaohjelmista toipuminen on hidasta ja tilanteen selvittämiseen kuluu pitkiä aikoja, puolustavan tahon tulee varmistaa, että kaikki järjestelmät voidaan turvallisesti ottaa taas käyttöön. Varmuuskopiot ovat avainasemassa toipumisen varmistamisessa.

Tietomurrot ja -vuodot

- Colonial Pipelinen tietomurto ja kiristyshaittaohjelma
  - Colonial Pipeline on USA:n suurin polttoaineen siirtojohtoja operoiva yritys
  - Rikollisryhmä Darkside teki 7.5. kohdennetun kiristyshaittaohjelmahyökkäyksen yrityksen toimistoverkkoon
  - Yritys sammutti suojaamistoimenpiteenä koko tietoverkkonsa, minkä vuoksi myös polttoaineen siirto pysähtyi

ANALYYSI

- Bloombergin 4.6. julkaiseman artikkelin mukaan Colonial-tapauksen taustalla oli useita syitä
- Tietomurrossa hyödynnettiin vanhaa tunnusta, jota ei oltu poistettu käytöstä, vaikka sen käyttö oli lopetettu
- VPN oli käytössä ilman MFA:ta ja näyttäisi siltä, että sama salasana on ollut käytössä muissakin palveluissa
- Tietoturva-asioissa hyvin kunnossa pidetyt perusasiat voivat pelastaa monelta ongelmalta

Tietomurrot ja -vuodot

- Colonial Pipeline ja lunnaiden maksaminen
  - Yritys maksoi rikollisille 4,4 M$ lunnaat ja sai purkutyökalun
  - 8.6. esimerkiksi YLE uutisoi, että Yhdysvaltojen oikeusministeriö on saanut takaisin valtaosan Colonial Pipeline -putkiyhtiön hakkereille maksamista lunnasrahoista

ANALYYSI

- Lunnaiden maksamiseen päädyttiin tässä tapauksessa, mutta päätös ei Colonial Pipelinen toimitusjohtajan mukaan ollut helppo
- Yleisesti lunnaiden maksamista ei suositella, sillä ne maksamalla ei välttämättä saa purkuavainta ja maksaminen ylläpitää rikollisten liiketoimintaa
- On myös mahdollista, että lunnaiden maksamisesta joutuu maksamaan tuntuvia sakkoja (USA:ssa jopa 20 M$, jos rikollisryhmittymälle tai maalle on asetettu pakotteita)

Huijaukset ja kalastelut

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

Huijaukset ja kalastelut

- Tekstiviestien käyttö on yleistynyt huijausviesteissä huomattavasti
  - SMS-huijausviestejä lähetettiin OmaPostin nimissä toukokuussa jälleen runsaasti.
  - Uusi SMS-kampanja eri kuriiripalveluiden nimissä noudattaa samaa kaavaa kuin aiemmat, mutta sisältää uuden ja vieläkin vaarallisemman FluBot-haittaohjelman.
- Pankkikalastelua tehdään entistä taitavammin.

TIETOJENKALASTELUN MONET KASVOT

- Pankkitietoja, maksukorttitietoja, henkilötietoja ja kirjautumistietoja kalastellaan hyvin monenlaisilla eri verukkeilla.
- Tyypillisin kalasteluviesti väittää, että uhrin tunnus tai tili jäädytetään tai sopimus on päättymässä, klikkaa tästä jos haluat jatkaa tiliä. Toinen yleinen kalasteluviesti vetoaa virhetilanteeseen tai muuhun ongelmaan, joka pitää korjata klikkaamalla.
- Korona-aiheiset huijausviestit vetoavat nyt karanteeniteemaan, rokotustodistukseen tai koronatesteihin.
- Käyttäjätunnuksia kalastellaan myös elokuvapalveluiden, verkkokauppojen, tiedostojenjakopalveluiden ja kokousohjelmistojen tilille.

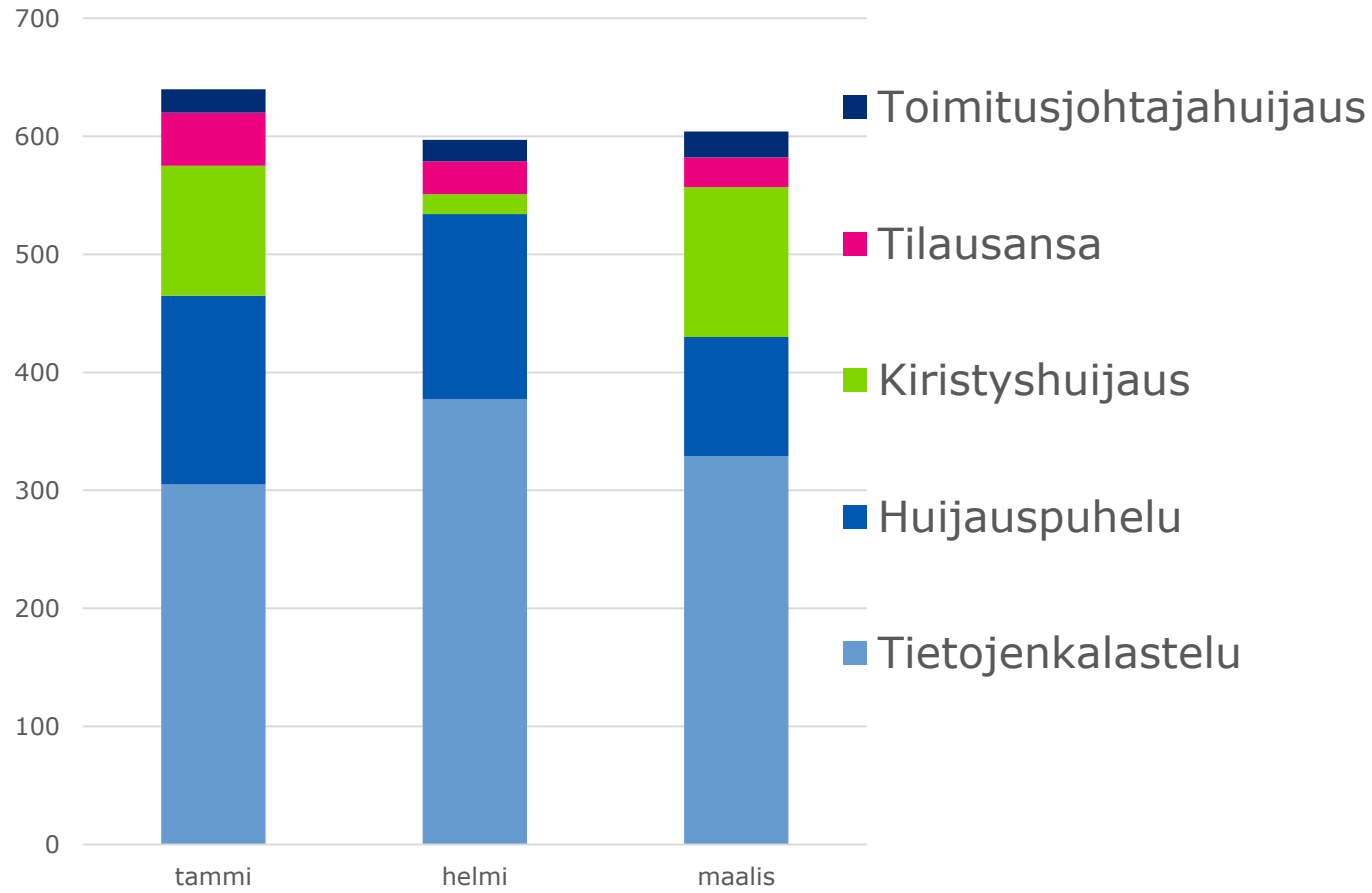
Kiristyshuijauksia sähköpostitse

- Sähköpostitse levitettiin jälleen runsain mitoin kiristyshuijauksia.
  - Huijausviesteissä keksittiin väitteitä, joiden mukaan uhri on katsellut pornoa ja hakkeri on kuvannut sitä tietokoneen kameralla. Vanhoja tuttuja pornokiristyksiä on terästetty jostakin vanhasta tietovuodosta löydetyllä salasanalla.
  - Huijausviesteissä käytettiin kömpelöä suomen kieltä. Geneerisissä huijauksissa suomen kieli ei ole kaikkein tyypillisin, mutta tässä huijauskampanjassa on jaksettu panostaa erikielisiin huijausviesteihin.
  - Virastolle raportoitiin samoja huijauksia toukokuussa myös englanniksi, tanskaksi ja turkiksi.

SOSIAALISEN MEDIAN TUNNUKSIA KALASTELLAAN

- Sosiaalisen median tunnuksen kaksivaiheista tunnistautumista koetetaan ohittaa tekstiviestikoodeja kalastelemalla.
- Hyökkääjä koettaa kirjautua tilille, jolla on kaksivaiheinen kirjautuminen käytössä, ja kyselee kirjautumiskoodia tekstiviestillä.
- Jos olet ottanut kaksivaiheisen kirjautumisen käyttöön Googlessa, WhatsAppissa, Facebookissa tai Twitterissä, varo jakelemasta kirjautumiskoodeja kenellekään!

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

- Mobiililaitteisiin kohdistuvat haittaohjelmat ovat olleet aktiivisia kevään aikana
  - Aktiivinen Fakecop/Fakespy-haittaohjelman levityskampanja, vuonna 2021: 607 ilmoitusta
    - OmaPostin nimissä tehtävä huijauskampanja vaikuttaa Android- ja iPhone-käyttäjiin
    - Haittaohjelmalla saastunut puhelin voi lähettää tuhansittain tekstiviestejä ja aiheuttaa liittymälle tuntuvia kustannuksia
  - Android-haittaohjelma Flubot:sta julkaistiin Keltainen varoitus 4.6.
    - Haittaohjelmaa levitetään DHL- ja UPS-teemoilla saapuvien tekstiviestien välityksellä

ANALYYSI

- FakeCop-haittaohjelma tarttuu Android-puhelimiin vain, jos käyttäjä sen erikseen hyväksyy. Tuntemattomista lähteistä tulevia .apk-pakettien asentamisia ei pitäisi hyväksyä.
- Omaa puhelinnumeroa, luottokorttitietoja tai mitään muita omia tunnuksia ei pidä syöttää harkitsemattomasti nettisivuille tai verkkopalveluihin
- Tarkastathan aina, että vierailemasi verkko-osoite on oikeasti sen organisaation osoite, jossa uskotkin vierailevasi

Haavoittuvuudet

- Microsoftin kuukausittaisessa päivityspaketissa julkaistiin korjaukset 55 haavoittuvuuteen, joista 4 oli kriittistä
- SAP:lta tuli päivityspaketti kuuteen haavoittuvuuteen ja Adobelta 43 paikkausta 12 eri tuotteeseen
- Haavoittuvuuksiin julkistettiin korjauksia myös Siemensin ICS-laitteisiin
- Pulse Secure julkaisi uuden hallintakomponenttihaavoittuvuuden
- Useat verkkolaitevalmistajat julkaisivat artikkeleita FragAttack -haavoittuvuudesta, joka vaikuttaa useisiin langattomiin verkkolaitteisiin (WiFi)

ANALYYSI

- Vuodesta 2003 alkaen joka kuukauden toisena tiistaina on "Patch Tuesday". Silloin esimerkiksi Microsoft julkaisee turvallisuuteen vaikuttavien haavojen korjauspäivitykset Windowsille, Officelle ja muille liitännäisille tuotteille.
- Päivitysaikataulu mahdollistaa paremman ennakoinnin ja suunnittelun, kun päivityksiä osataan odottaa tiettynä päivänä. Useat muutkin toimijat kuten Adobe, SAP ja Cisco ovat ottaneet käyttöönsä saman aikataulun.

Toukokuun haavoittuvuusjulkaisut

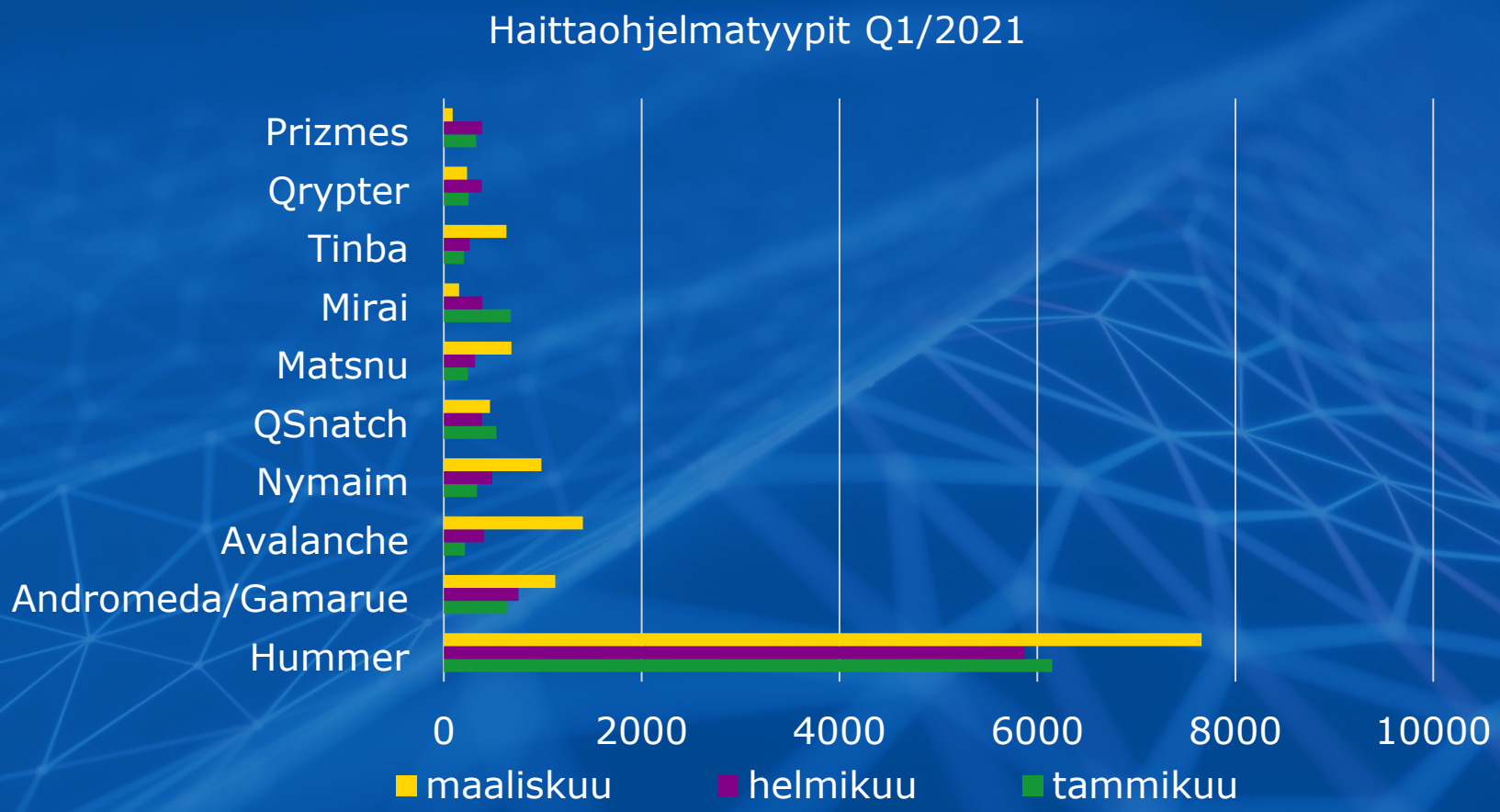
- Dellin Windows-laitteissa vakava haavoittuvuus (13/2021)
- Exim-sähköpostiohjelmistossa kriittisiä haavoittuvuuksia (14/2021)
- Adobe korjasi kriittisen haavoittuvuuden Adobe Acrobatissa ja Readerissa (15/2021)
- Wi-Fi-laitteiden toteutuksista on löytynyt haavoittuvuuksia (16/2021)
- Apple korjasi haavoittuvuuksia laitteissaan - päivitä heti (17/2021)

- Lue lisää: www.kyberturvallisuuskeskus.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

Autoreporterin 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 sekä monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.

Automaatio

- Colonial Pipeline hallinnoi Yhdysvaltain suurinta polttoaineen siirtoon tarkoitettua putkilinjastostoa. Heidän toimistoverkkojensa järjestelmät joutuivat kiristyshaittaohjelman uhriksi (katso Kybersään Tietomurrot ja -vuodot -osio).
- Yritys sulki varotoimenpiteenä myös polttoaineensiirtolinjastonsa.

ANALYYSI

- Kriittisimmätkään tuotantojärjestelmät (OT) ovat harvoin täysin eriytettyjä toimistojärjestelmistä (IT), vaikka tällainen olisi haluttua.
- Myös IT:n ja OT:n välissä sijaitsevan tuotannonohjausjärjestelmän (Manufacturing execution system, MES) suojaamiseen on kiinnitettävä huomiota, sillä ilman sitä mm. reseptien, laadun, tehokkuuden ja materiaalien kuljetuksien seuranta ja hallinta voivat hankaloitua.

Automaatio

- Kasasimme alle muutamia nostoja viimeaikoina julkaistusta tuotantojärjestelmien suojausvinkeistä:
  - Tunnista IT-puolelta OT-puolelle jaetut järjestelmät ja niiden väliset yhteydet, jotka ovat kriittisiä ja välttämättömiä toiminnan jatkuvuuden kannalta. Onko kaikilla vastuullinen omistaja? Mieti, miten luottamus eri AD-järjestelmien välillä on hoidettu.
  - Tutki, miten kriittisimpien järjestelmien eristäminen ja eriyttäminen on toteutettu ja pitävätkö ne. Rakenna OT-puolelle oma DMZ.
  - Tunnista myös muut kuin kriittisimmät tuotantojärjestelmät ja monitoroi verkkoliikennettä OT-puolella.
  - Selvitä, mitä tuotantojärjestelmistä näkyy Internetiin ja miten niiden etähallinta on toteutettu. Minimoi hyökkäyspinta-ala.
  - Selvitä, mitä minimissään vaaditaan, jotta käyttäjä (tai rikollinen) pääsee käsiksi tuotantoympäristöön etänä.
  - Selvitä, miten järjestelmien asetusten ja päivitysten hallinta on toteutettu. Onko tärkeimmistä resursseista “kultaiset” varmuuskopiot tallessa esimerkiksi kassakaapissa?
  - Harjoittele säännöllisesti poikkeamatilanteita ja varmista sekä testaa palautuminen sellaisista. Suunnittele, miten jatkuvuus taataan manuaalisesti, mikäli tuotantojärjestelmät eivät ole käytettävissä.
  - Testaa säännöllisesti, miten tietoturvakontrollit kuten hyväksyttyjen sovellusten listat toimivat.

IoT

- Traficom järjesti 26.5. webinaaritilaisuuden IoT-laitteiden tietoturvavaatimusten ja -sertifiointien kehittymisestä
  - Tilaisuuteen osallistuivat Traficomin lisäksi F-Securen, EU-komission, Singaporen ja Iso-Britannian kyberturvallisuusviranomaisten ja Signifyn (Philips Lighting) edustajat
  - Webinaaritallenne on katseltavissa osoitteessa: https://www.youtube.com/watch?v=NApgNblKuWs

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 kolme merkittävää toimivuushäiriötä.
  - Katkos internetyhteyksissä Järvenpäässä 7.5., vaikutuksia muutamalle tuhannelle asiakkaalle.
  - Yritysten vaihdepalveluissa oli häiriö, joka vaikutti alle tunnin mobiiliittymien saapuviin puheluihin.
  - Radiokanavalla oli reilun tunnin katkos viikonloppuyönä.
- Häiriöiden vaikutukset olivat suhteellisen pieniä ja useimmissa toukokuun merkittävissä häiriöissä alkusyy oli ylläpitotyössä tehty virhe.

ANALYYSI

- Yleisten viestintäpalveluiden toimivuus Suomessa on ollut alkuvuoden 2021 aikana hyvä. Merkittäviä toimivuushäiriöitä on ollut 23 kappaletta, mikä ennustaisi koko vuoden summaksi noin 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

- Salesforcen palveluiden käyttökatko johtui inhimillisestä virheestä
  - 11.5. Salesforcen palvelimille tehtiin muutostyö, joka esti asiakkaiden pääsyn osaan palveluista.
  - Saatavuudesta vastaava johtaja kertoi, kuinka inhimillisestä virheestä johtuen työntekijä päätyi tekemään muutoksia vikatilanteessa koko tuotantoympäristöön.
  - Myös Salesforcen palveluiden tilasta asiakkaille kertova sivu meni alas vikatilanteen vuoksi.

ANALYYSI

- Suurissa pilvipalveluissa on viime aikoina ollut kuukausittain maailmanlaajuisesti vaikuttaneita häiriöitä. Niiden toistumiseen kannattaa varautua esimerkiksi häiriötilanteiden toimintatapoja suunnittelemalla ja harjoittelemalla.
- On syytä muistaa, että vaikka asioihin on varauduttu hyvin - voi esimerkiksi inhimillinen virhe suurella toimijalla aiheuttaa maailmanlaajuisen palvelukatkon.

Palvelunestohyökkäykset

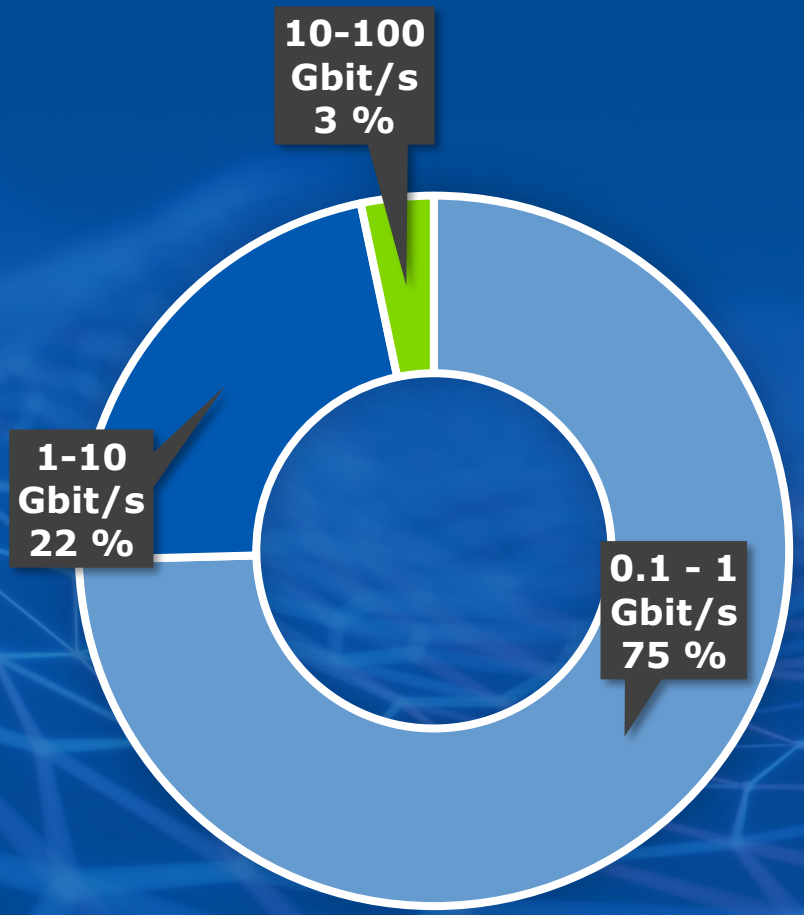
- Toukokuussa meille tulleiden ilmoitusten määrä väheni, mutta hyökkäysten koko oli ennätysluokassa.
  - Meille ilmoitettiin mahdollisesti suurimmasta palvelunestohyökkäyksestä Suomessa tähän asti: 260Gbit/s.
  - Hyökkäys oli kestoltaan noin 15 minuuttia ja mitigaatiopalvelut torjuivat sen.
  - Tiedossamme on myös yli 100Gbit/s hyökkäys toukokuussa, jonka kesto oli useita tunteja.
  - Viime aikoina olemme saaneet jälleen tietoomme kiristysviesteistä palvelunestohyökkäyksiin liittyen. Toistaiseksi uhattuja suurempia hyökkäyksiä ei ole nähty, mutta kiristysviestin lähettämisen lisäksi kiristäjä on voinut tehostaa viestiä uhattua pienemmällä palvelunestohyökkäyksellä.

ANALYYSI

- Organisaatioiden tulee tietää mitkä palvelut ovat heille tärkeitä, ja mitkä tulisi suunnitella toimimaan myös mahdollisen palvelunestohyökkäyksen aikana.
- Noin 25% hyökkäyksistä (Q1/2021) Suomessa oli kooltaan yli 1Gbit/s. Viime kuussa meille ilmoitettujen hyökkäysten perusteella skaala ulottuu siis jopa 260Gbit/s tasolle asti.

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

- APT29-ryhmä on lähettänyt kohdistettuja, haitallisia sähköposteja isolle joukolle vastaanottajia. Asiasta kertonut Microsoft kutsuu ryhmää nimellä NOBELIUM.
  - Laaja sähköpostikampanja toteutettiin toukokuun lopussa. Viestit sisälsivät haitallisia linkkejä, jotka oli yritetty naamioida käyttämällä välikappaleena aitoa markkinointisähköpostipalvelua.
- Operaation aiemmat vaiheet ovat Microsoftin mukaan olleet vähäeleisempiä.
  - Tammikuussa kohteille lähetettiin viestejä, joiden tarkoituksena oli ainoastaan seuranta – tällöin viesteillä ei välitetty haitallista sisältöä.
  - Seuraavassa vaiheessa kohteille lähetettiin sähköpostiviestejä, joiden tavoitteena oli saada uhri avaamaan haitallinen HTML-tiedosto, joka johti tiettyjen käyttäjän toimenpiteiden jälkeen siihen, että laitteelle asentui komentokanavayhteyden mahdollistava ohjelmisto.
- APT29 on viime aikoina yhdistetty julkisuudessa mm. SolarWinds Orion -hallintatyökaluun kohdistuneen murron avulla toteutetuista kohdeorganisaatioihin tunkeutumisista.

ANALYYSI

- Valtiolliset toimijat voivat hyödyntää legitiimejä palveluita osana operaatioitaan esimerkiksi kiertääkseen kohdeorganisaation tietoturvakontrolleja tai vaikeuttaakseen havainnointia.

Vakoilu

- Ruotsin yleisradioyhtiön SVT:n ja Tanskan radion DR:n mukaan Yhdysvaltojen turvallisuusvirasto NSA olisi vakoillut poliitikkoja ja virkamiehiä useissa Euroopan maissa Tanskan kautta vuosina 2012–2014.
  - Kohteina oli uutisoinnin mukaan poliitikkoja ja virkamiehiä Saksassa, Ranskassa, Ruotsissa ja Norjassa.
  - Mediat perustavat tietonsa sisäpiirilähteiden antamiin tietoihin Tanskan sotilastiedustelun salassa pidettävästä sisäisestä tutkinnasta, jossa selvitettiin NSA:n Tanskan kautta tekemään valvontaa. Tanskan syytetään mahdollistaneen Yhdysvalloille pääsyn tietoliikenteen solmukohdan seuraamiseen Tanskassa.
- Tanskan asevoimien tiedustelun ja NSA:n yhteistyön sisällöstä on uutisoitu viime syksystä lähtien.
  - Aiemmin syksyllä uutisoitiin, että Tanskan asevoimien tiedustelupalvelu olisi avustanut Yhdysvaltoja Tanskan sisällä tapahtuneessa seurannassa.
  - Loppuvuodesta 2020 puolestaan uutisoitiin, että Yhdysvallat olisi kohdistanut vakoilua tanskalaiseen ja ruotsalaiseen puolustusteollisuuteen.

ANALYYSI

- Ainakin Ruotsi ja Norja ovat vaatineet Tanskalta selvitystä väitteistä.
- Koska uutisointi pohjautuu sisäpiirilähteisiin, on tietojen paikkansapitävyyttä vaikea vahvistaa.

Vakoilu

- Muissa kybervakoilu-uutisissa esiin nousivat jälleen mm. VPN-ratkaisuihin ja verkko-laitteisiin liittyvien haavoittuvuuksien hyödyntäminen kohdistetuissa hyökkäyksissä.
  - Yhdysvallat kertoi, että valtiolliseen toimintaan linkittyvä taho oli murtautunut yhdysvaltalaisten kuntien järjestelmiin Fortinetin Fortigaten murtamisen avulla.
  - FireEye löysi uusia haittaohjelmia, joita on käytetty Pulse Connect Secureiden murtoihin liittyvässä operaatiossa.
- Lisäksi toukokuussa uutisoitiin muun muassa Kiinaan liitetyn, mahdollisesti uuden APT-ryhmän pyrkineen vakoilemaan venäläistä puolustusteollisuutta. Kohteena oli sukellusveneitä Venäjän laivastolle suunnitteleva toimija.
- Venäläinen operaattori Rostelecom ja FSB:n alainen NKTsKI puolestaan kertoivat Venäjän valtionhallintoon kohdistuneesta kybervakoiluyrityksestä.

ANALYYSI

- Verkkolaitteet sekä verkon ja verkkoyhteyksien turvalliseen toteutuksen liittyvät ratkaisut ovat edelleen houkutteleva kohde kybervakoilun näkökulmasta.

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

- Määräys viestintäverkon kriittisistä osista on julkaistu ja tullut voimaan 20.5.2021
- Määräystä sovelletaan yleiseen teletoimintaan sekä sähköisen viestinnän palveluista annetun lain (917/2014) 244 a §:n 2 momentissa tarkoitettuihin yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitettyyn erillisverkkoon.

ANALYYSI

- Taustalla sähköisen viestinnän palveluista annetun lain (917/2014) eli viestintäpalvelulain muutos 1.1.2021:
  - ”Viestintäverkkolaitetta ei saa käyttää yleisen viestintäverkon kriittisissä osissa, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta. Tämä käyttökielto koskee tilanteita, joissa käytöllä mahdollistettaisiin ulkomainen tiedustelutoiminta tai toiminta, jolla häirittäisiin, lamautettaisiin tai muuten vahingollisella tavalla vaikutettaisiin Suomen tärkeisiin etuihin, yhteiskunnan perustoimintoihin tai kansanvaltaiseen yhteiskuntajärjestykseen”
  - Määräyksen tavoitteena on täsmentää, mitä yleisen viestintäverkon tai kriittisen erillisverkon tyypillisiä teknisiä osia viestintäpalvelulain määrittelemä kriittinen osa käsittää.
  - Linkki: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-maarittelee-viestintaverkon-kriittiset-osat

Oikeudelliset asiat

- Avaruusohjelma-asetus
  - EU:n avaruusohjelma-asetus on tullut voimaan 12.5.2021. Samana päivänä myös EU:n avaruusohjelmavirasto EUSPA aloitti toimintansa.
  - EU:n avaruusohjelma-asetuksella perustetaan EU:n avaruusohjelma sekä EU:n avaruusohjelmavirasto sekä säädetään Galileo- ja EGNOS-satelliittinavigointijärjestelmistä, Copernicus-maanhavainnointijärjestelmästä, avaruustilannetietoisuudesta sekä GOVSATCOM-satelliittiviestintäpalvelusta.
  - Linkki: https://data.consilium.europa.eu/doc/document/PE-21-2021-INIT/fi/pdf

Oikeudelliset asiat

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
  - Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä hyväksytty eduskunnassa 28.5.2021.
  - Laki velvoittaa kaikki sosiaali- ja terveydenhuollon toimijat liittymään valtakunnalliseen Kanta-palveluun.
  - Omatietovarannon tarkoituksena olisi mahdollistaa kansallinen tietovaranto henkilöiden omille hyvinvointitiedoille niin, että henkilö voisi hyödyntää hyvinvointitietojaan erilaisissa hyvinvointisovelluksissa sekä luovuttaa niitä palvelunantajille hyödynnettäväksi sosiaali- ja terveyspalveluja antaessaan.
  - Tietojärjestelmän tai hyvinvointisovelluksen saa ottaa tuotantokäyttöön ja liittää valtakunnallisiin tietojärjestelmäpalveluihin, kun se on läpäissyt Kansaneläkelaitoksen koordinoiman yhteentoimivuuden testauksen ja tietoturvallisuuden arviointilaitos on antanut sitä koskevan tietoturvallisuuden arviointia koskevan todistuksen eli sertifioinnin.
  - Lue lisää: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_212+2020.pdf

Arjen kyberturvallisuus - toukokuu

Etenkin iäkkäät menettävät nyt rahojaan verkkorikollisille - menetykset yhteensä jo 2,1 miljoonaa

- Kevät 2021 on ollut verkkorikollisten kulta-aikaa. Uhrit ovat menettäneet rahojaan jo 2,1 miljoonaa euroa.
- Jokaisen on nyt syytä olla varovainen ja huolellinen asioidessaan verkkopankissa ja hyväksyessään maksuja.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/etenkin-iakkaat-menettavat-nyt-rahojaan-verkkorikollisille-menetykset-yhteensa-jo-21

Julkaisimme vakavan varoituksen Android-haittaohjelmien levityksestä tekstiviestitse

- Haittaohjelmien saastuttamilta laitteilta voidaan varastaa esimerkiksi salasanoja ja muita tietoja.
- Saastuneita laitteita käytetään myös lähettämään haittaohjelmaa eteenpäin.
- https://www.kyberturvallisuuskeskus.fi/fi/Varoitus_TTN_0621

Stop, slow & go

- Digiturvataitoja on hyvä alkaa opettaa lapsille mahdollisimman varhain, jotta niistä tulee luonnollinen osa lapsen elämää.
- Lasten on tärkeä harjoitella myös digiliikenteen osalta, mikä asiat ovat kiellettyjä (STOP), mietityttäviä (SLOW) tai sallittuja (GO).
- Sivustolle on koottu ohjeita opettajille sekä vanhemmille https://suojellaanlapsia.fi/digiliikenteessa/ammattilaisille/

Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä

- Ilmiö on ollut pitkään pinnalla jo Suomessa eikä näytä laantumisen merkkejä.
- Liikkeellä on nyt runsaasti aikuisviihdeteemaisia kiristysviestejä. Viestit ovat huijausta, eikä niihin tarvitse reagoida. 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

Traficom määrittelee viestintäverkon kriittiset osat

- Viestintäverkon kriittisenä osana pidetään verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.
- Määräys viestintäverkon kriittisistä osista auttaa verkkojen omistajia tulkitsemaan täsmällisemmin, mitä yleisen viestintäverkon tai kriittisen erillisverkon tyypillisiä teknisiä osia viestintäpalvelulain määrittelemä kriittinen osa käsittää.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-maarittelee-viestintaverkon-kriittiset-osat

Ovatko suomalaiset yritykset valmiita älylaitteiden tietoturvavaatimuksiin?

- Älylaitteiden tietoturva mietityttää laitevalmistajia, laitemyyjiä ja kuluttajia.
- Suomessa otettiin käyttöön vapaaehtoinen älylaitteiden tietoturvallisuudesta kertova Tietoturvamerkki vuoden 2019 lopussa.
- Parhaillaan EU:ssa käydään keskustelua älylaitteiden vapaaehtoisista ja velvoittavista vaatimuksista.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ovatko-suomalaiset-yritykset-valmiita-alylaitteiden-tietoturvavaatimuksiin

CERT-FI 20 vuotta: Näin rakennettiin kotimaisen tietoturvan perustuksia

- On aika aloittaa pienet etkot, kun CERT-toimintomme täyttää vuodenvaihteessa 20 vuotta.
- Suomalainen Computer Emergency Responce Team on pitänyt tietoturvastamme huolta nuorukaisen iän verran. Nykyisen Tilannekeskuksemme, tietoturvapäivystyksemme ja tietoturva-asiantuntijuutemme juuret ovat CERT-FI:ssä.
- Tutustu juttusarjan ensimmäiseen osaan

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