TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 2019

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

vakava

Varoitus 01/2019: Eximin haavoittuvuutta käytetään aktiivisesti hyväksi

Olemme saaneet useita ilmoituksia Exim-sähköpostipalvelimen haavoittuvuutta hyväksikäyttävästä tietomurroista. Haavoittuvuus ei koske uusinta 4.92 ohjelmistoversiota. Vanhemmat ohjelmistoversiot ovat haavoittuvia.

Haavoittuvuutta hyväksikäyttämällä hyökkääjä voi suorittaa komentoja kohdejärjestelmässä. Havaituissa tapauksissa hyökkääjä on yleensä asentanut palvelimelle takaoven myöhempää käyttöä varten sekä asettanut palvelimen louhimaan virtuaalivaluuttaa.

Eximin oletuskonfiguraatiossa haavoittuvuuden hyväksikäyttö on tämänhetkisten tietojen mukaan hankalaa. On kuitenkin hyvin todennäköistä, että joissakin palvelinympäristöissä Eximin oletusasetuksia on muutettu sellaisiksi että hyväksikäyttö verkon yli on mahdollista helpommin.

Ajantasaisimmat tiedot varoituksesta:

https://www.kyberturvallisuuskeskus.fi/fi/exim-sahkopostipalvelimen-haavoittuvuuden-avulla-tehdaan-tietomurtoja

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/useita-exim-sahkopostiohjelmistoa-kayttavia-palvelimia-murrettu-suomessa

Varoitus 02/2018: Office 365-tunnuksia kalastellaan aktiivisesti

Suomalaisten yritysten ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä varastetaan edelleen. Varoitus aiheesta on ollut voimassa kesästä 2018. Kyberturvallisuuskeskus julkaisi huhtikuun alussa oppaan Office 365 -tuotteiden tietoturvaominaisuuksista, joiden käyttöä suositellaan.

Hyökkääjät kirjautuvat käyttäjätileille ja seuraavat yritysten sähköpostiliikennettä. He pyrkivät saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä tai kalastelevat muiden työntekijöiden tai yhteistyökumppanien tunnuksia.

Käyttäjätunnuksia ja salasanoja kalastellaan sähköpostitse ja huijaussivujen avulla. Yksi viimeaikainen menetelmä on Azuren pilvipalveluissa tehtävä kalastelu, joka on todella hyvin toteutettu. Monivaiheinen tunnistaminen (MFA) voidaan myös ohittaa, jos Office 365 on asetettu tukemaan kirjautumista myös vanhoilla sovelluksilla (ns. legacy support).

Annoimme varoituksen 11.6.2018, joka on edelleen voimassa.
https://www.viestintavirasto.fi/2018/varoitus-2018-03

Julkaisimme oppaan uhkan torjumiseksi:
https://www.kyberturvallisuuskeskus.fi/fi/node/2532

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä. Verkkoon liitetään laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet ovat puutteellisia.

2

Edistyneemmät rikollisryhmät etsivät kohteikseen isoja organisaatioita, joiden toimintaa haittaamalla voidaan yrittää kiristää rahaa.

3

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

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Tietoturvan laiminlyönnit altistavat esimerkiksi häiriöille.

5

Puutteellinen elinkaaren- ja lokienhallinta heikentää organisaatioiden kykyä havaita ja reagoida poikkeamiin.

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Nopea reagointi ja omien verkkojen havainnointi suojaavat mahdollisilta Big game hunting -hyökkäyksiltä.

2. Pilvipalveluiden tietoturvallisuutta voidaan nyt arvioida Pilvipalveluiden turvallisuusarviointikriteeristön avulla.

3. Europarlamenttivaalit sujuivat häiriöittä, vaikka maailmalla nähtyjen uhkakuvien takia valmiutta nostettiin.

Tietoturvan kehitystarpeet

1. Päivittämättömiä järjestelmiä murretaan toistuvasti. Päivitysten merkitys korostuu, kun aikajänne haavoittuvuuden löytämisestä hyväksikäyttöön lyhenee.

2. Yleisesti käytettyjen haittaohjelmien avulla voidaan saada suuryrityksistäkin jalansija. Big game hunting -ryhmät valikoivat uhrien joukosta kaikkein rahakkaimmat.

3. Toimitusjohtajahuijausten lisäksi palkanlaskentaan ja henkilöstöhallintoon on kohdistettu huijauksia.

Kybersää toukokuu 2019

Verkkojen toimivuus

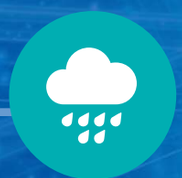
- Vain kaksi merkittävää toimivuushäitiötä. Myrskyt eivät vaikuttaneet merkittävästi.
- Palvelunestorintamalla oli rauhallista. Myös europarlamenttivaalit sujuivat ilman tietoliikenteen häirintää.

Vakoilu

- Vuodetun asiakirjan mukaan EU:n Moskovan lähetystö oli tietomurron kohteena.
- Iso-Britannia ilmoitti ottavansa kovemman linjan valtiollisten kyberoperaatioiden estämiseksi.

Haittaohjelmat ja haavoittuvuudet

- Bluekeep-haavoittuvuus voi johtaa itsenäisesti ja nopeasti leviävään haittaohjelmaepidemiaan.
- Big game hunting -ryhmät hyödyntävät yleisiä haittaohjelmia. Hyökkäys johtaa pahimmillaan liiketoiminnan keskeytymiseen tai sen häiriintymiseen.



Tietomurrot ja -vuodot

- Varsin tyypillinen tietomurtokuukausi.
- Julkisesti verkossa olevien päivittämättömien palveluiden hyväksikäyttö on erittäin yleistä.

Huijaukset ja kalastelut

- Lähestyvä lomakausi sijaisuuksineen lisää jälleen toimitusjohtaja-huijausten uhkaa.
- Palkanlaskijoille lähetetyillä huijausviesteillä yritetään muuttaa palkkatilejä huijarin tiliksi.

IoT ja automaatio

- Taloautomaatiotuotteista paljastui yli sata haavoittuvuutta.
- Tutkijat murtautuivat ja onnistuivat manipuloimaan lentokoneiden lentoa tukevia järjestelmiä.
- Vastuulliset käytännöt tietoturvapuutteista ilmoittamisessa leviävät.

Verkkojen toimivuus

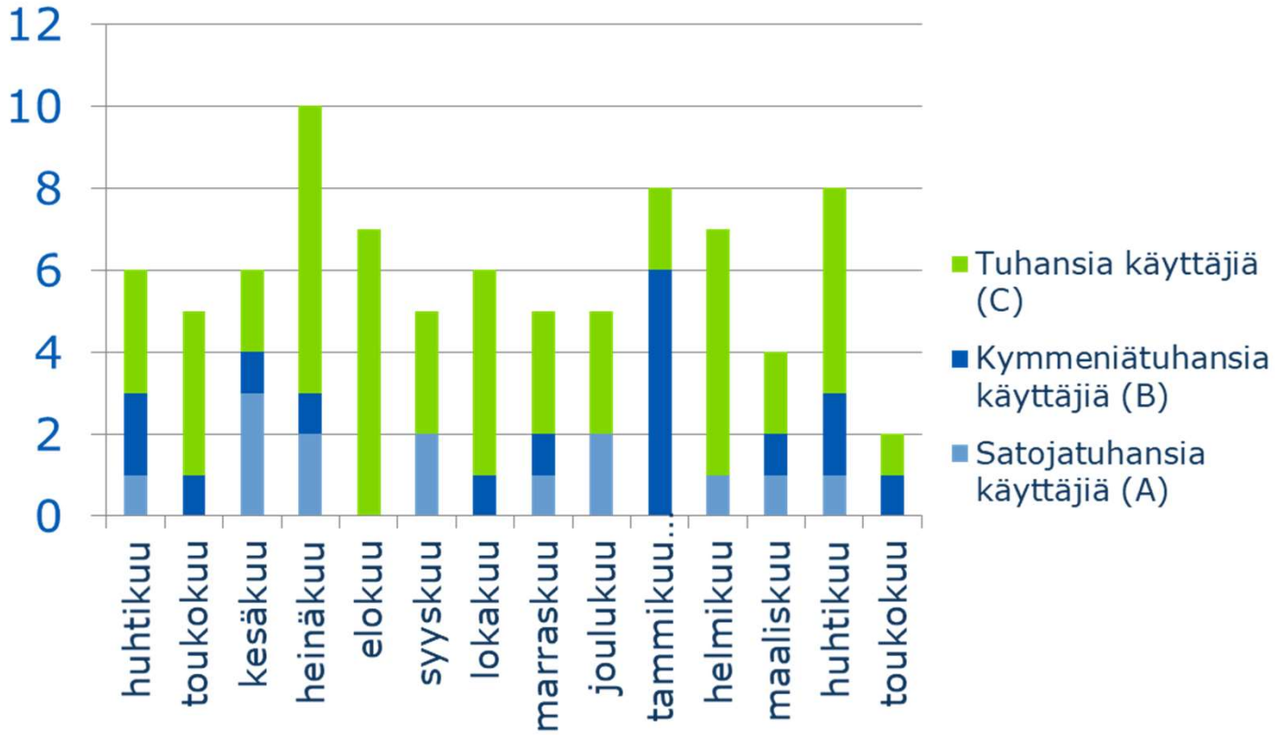
Verkkojen toimivuus

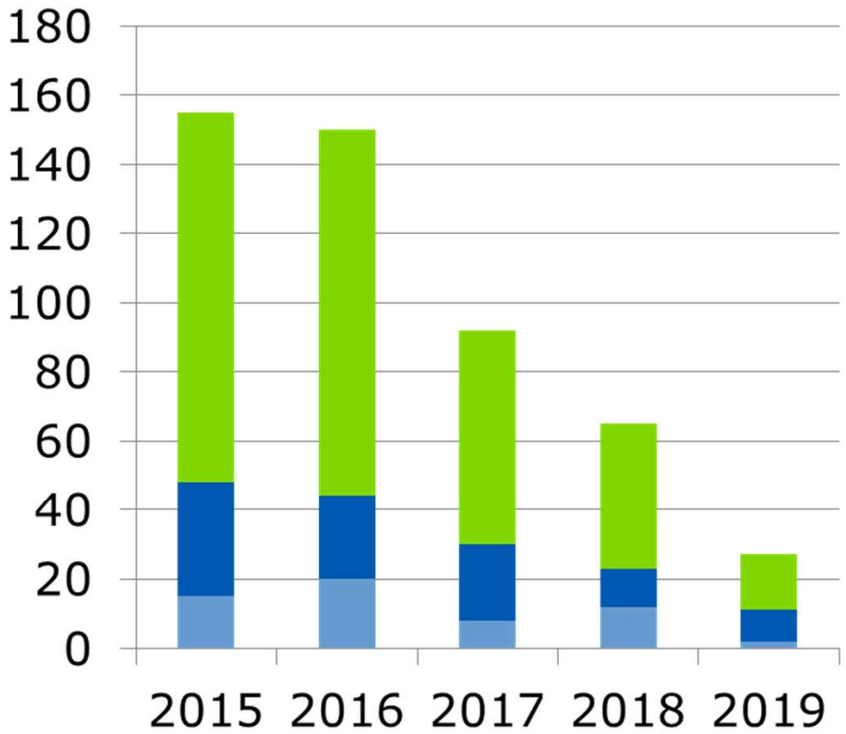
- Toukokuussa oli vain kaksi merkittävää toimivuushäiriötä
  - Häiriöt vaikuttivat lähinnä matkaviestinpalveluihin.
- Kesämyrskyt 30. ja 31.5. eivät aiheuttaneet merkittäviä toimivuushäiriöitä
  - Kymmenittäin matkapuhelinverkkojen tukiasemia kärsi sähkökatkoista, mutta yhtenäisiä katvealueita ei muodostunut.
  - Sähköverkkourakoitsijat saivat palautettua sähköt ripeästi.

Verkkojen toimivuus

- Palvelunestohyökkäysten suhteen kuukausi oli rauhallinen
  - Suomalainen kunta raportoi pienestä hyökkäyksestä koulun järjestelmään.
- Europarlamenttivaalit sujuivat rauhallisesti
  - Sekä Suomessa että muualla Euroopassa vaalit sujuivat tällä kertaa ilman havaintoja tietoliikenteen tai vaalijärjestelmien häirinnästä.
  - Viranomaiset olivat sekä eduskuntavaalien että europarlamenttivaalien aikana varautuneet häirintään.
- Palvelunestohyökkäysten voimakkuudet ovat kasvaneet
  - Yli 10 Gbit/s hyökkäyksiä nähdään Suomessa jo päivittäin.
  - Hyökkäysten aiheuttamista häiriöistä ei kuitenkaan ole raportoitu Kyberturvallisuuskeskukselle tavanomaista enempää. Tämä saattaa johtua parantuneista suojautumiskeinoista.

Merkittävien toimivuushäiriöiden määrä





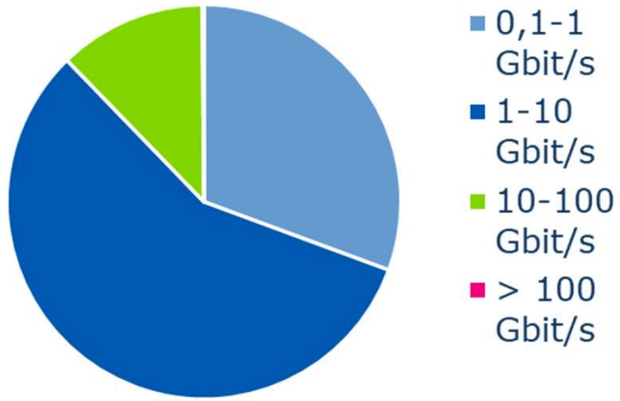
Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta vuodessa. Niiden määrä riippuu teleyrityksen tilastointitavasta.

Palvelunestohyökkäykset ja niillä uhkailu

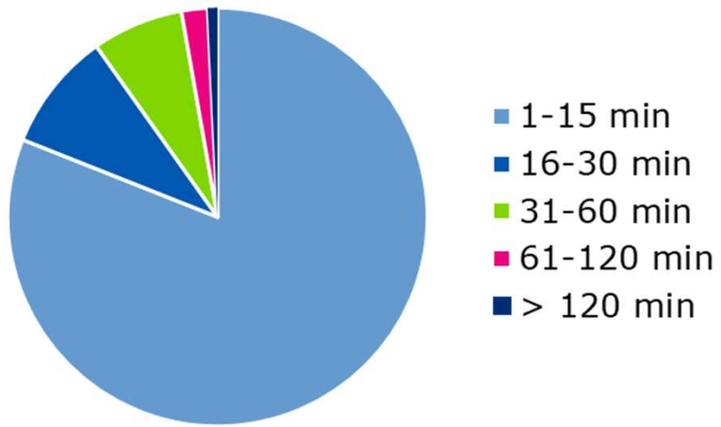
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (80 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 57 % kaikista nähdyistä hyökkäyksistä ovat volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 10 Gbit/s hyökkäysten osuus on kasvanut vuoden 2018 puolivälistä alkaen, ja niitä nähdään Suomessa jo päivittäin.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Kyberturvallisuuskeskukselle ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

2019/Q1:	2018/Q4:	2018/Q3:
n. 162 Gbit/s	n. 45 Gbit/s	n. 89 Gbit/s
(kesto 9 min)	(kesto 6 min)	(kesto 30 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

Vakoilu

Vakoilutilanteessa ajankohtaista

EU:n Moskovan lähetystössä paljastui tietomurto

Vuodetun asiakirjan mukaan Euroopan unionin Moskovan lähetystö olisi ollut kybervakoilun kohteena vuoden 2017 helmikuusta tähän kevääseen asti. EU:n ulkosuhdehallinto on kertonut tutkivansa asiaa.

Iso-Britannia ilmoitti vastaavansa verkkovakoiluun

Iso-Britannian ulkoministeri kertoi maan varautuvan vastaamaan Venäjän verkkovakoiluun aktiivisemmalla lähestymistavalla. Britannia on myös ilmoittanut kasvattavansa hyökkääjien toimintaa aktiivisesti haittaamaan pyrkivän kyberyksikön vahvuutta.

Kiinalaisryhmä hyökkäsi Lähi-itään

Tietoturvayhtiö Palo Alto Networksin mukaan Kiinan valtioon liitetty Emissary Panda -ryhmä tunkeutui valtionhallinnon organisaatioiden järjestelmiin ainakin kahdessa Lähi-idän maassa. Hyökkäyksessä käytettiin hyväksi Microsoftin Sharepointissa paljastunutta ja sittemmin korjattua haavoittuvuutta.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmahavaintomme

Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	Muodostavat merkittävän osan Suomessa tehdyistä havainnoista	
Kiristyshaittaohjelmat	Muutamia havaintoja kiristyshaittaohjelmista	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia raportoitu muutamia tapauksia	
Louhijat	Louhijoita levitetty haavoittuvuuksien avulla palvelimille	
Tietoja varastavat haittaohjelmat	Levittämisyrityksistä jonkin verran havaintoja. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti.	
Mobiilihaittaohjelmat	Mobiilihaittaohjelmatapauksista joitain havaintoja	

Haittaohjelmat

- Big game hunting -toimijat hyödyntävät laajasti levitettäviä haittaohjelmia päästäkseen sisälle kohdeorganisaation verkkoon
  - Hyödynnettyjä haittaohjelmia muun muassa Emotet, Qbot ja Trickbot.
  - Muualla Euroopassa kohteeksi on valikoitunut erityisesti pieniä ja keskisuuria yrityksiä.
  - https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes
- Verkkosivuilta luottokorttitietoja keräävää Magecart-kampanjaa on havaittu viime aikoina myös Suomessa
  - Murretulle verkkosivustolle lisätään tietoja keräävä ohjelmakoodi.
  - Hyökkääjät ovat hyödyntäneet myös puutteellisesti suojattuja Amazon S3 -tiedostosäilöjä.

Big Game Hunting

Maailmalla on yleistynyt ilmiö, jota kutsutaan nimellä *Big Game Hunting* (suom. kirj. ”suurriistan metsästys”). Toiminnalle ominaista on, että rikollinen toimija tunkeutuu organisaation järjestelmiin, levittäytyy organisaation verkossa ja käynnistää kiristyshaittaohjelman siten, että tiedostojen salaus haittaa organisaation toimintaa vakavasti tai jopa lamauttaa sen.

Salauksen jälkeen organisaatiolta kiristetään lunnaita salauksen purkamiseksi. Kohteita yhdistää perinteisesti hyvä maksukyky tai toiminnan jatkumisen aikakriittisyys. Esimerkiksi tammikuussa kohteiksi joutui ranskalainen Altran ja maaliskuussa norjalainen Norsk Hydro. Yhdysvalloissa useat kunnat ja aluehallinnot ovat myös olleet kohteina.

Samaan ilmiöön liittyy useita eri kiristyshaittaohjelmia, kuten LockerGoga, SamSam, Ryuk ja MegaCortex. Organisaation järjestelmiin tunkeutuminen puolestaan voi alun perin tapahtua käyttäen hyväksi haavoittuvia verkkoon avoimia palveluita, haitallisilla sähköpostien liitetiedostoilla tai esimerkiksi onnistuneen tietojenkalastelun avulla.

Ilmiö on hyvä huomioida riskiarvioissa. Muun muassa murtautumisen ja levittäytymisen havaitsemiseksi on hyvä varmistua siitä, että jo hankittujen ratkaisujen tietoturvaominaisuuksia hyödynnetään kattavasti. Varautumista suunnitellessa on syytä huomioida myös, että rikolliset voivat pyrkiä vaikeuttamaan toipumista salaamalla myös esimerkiksi varmuuskopiot ja käyttövaltuushallinnan.

Haavoittuvuudet 1/2

- Microsoftin etätyöpöytäratkaisun kriittiseen RDS/RDP-haavoittuvuuteen (BlueKeep) on saatavilla julkinen palvelunestotilan mahdollistava esimerkkikoodi. Lisäksi on olemassa ei-julkisia hyväksikäyttömenetelmiä, joilla palvelimella saadaan suoritettua haitallista koodia verkon yli järjestelmätason oikeuksin.
- Intelin suorittimista löydetty uusia ennakoivaan suoritukseen liittyviä haavoittuvuuksia. ZombieLoad-, Fallout- ja RIDL-hyökkäyksiksi nimetyt keinot ovat hyväksikäyttömekanismiltaan Spectre-haavoittuvuuksia vastaavia.
- Windows 10 -käyttöjärjestelmään julkaistiin uusia käyttövaltuuksia korottavia nollapäivähaavoittuvuuksia.
- Cisco IOS XE versiossa 16 löydetty useita haavoittuvuuksia, joiden yhteiskäytöllä hyökkääjä voi ohittaa laiteohjelmiston tarkistukset ja korvata laiteohjelmiston haitallisella versiolla verkon yli.

Haavoittuvuudet 2/2

- Exim-sähköpostipalvelimista löydettiin haavoittuvuus, joka mahdollistaa komentojen suorittamisen. Haavoittuvuudelle on julkaistu paikallinen hyväksikäyttömenetelmä. Haavoittuvuutta voi hyödyntää myös verkon yli, mutta hyväksikäyttökoodi ei ole vielä julkinen.
- Julkisesti internetiin avoinna olevien palveluiden haavoittuvuuksia käytetään hyväksi yhä useammin. Tässä kuussa on tullut esille useiden haavoittuvuuksien hyväksikäyttötapauksia.
  - Sharepoint- ja MySQL-haavoittuvuuksia on jo hyväksikäytetty ja myös BlueKeep-haavoittuvuutta tullaan todennäköisesti hyväksikäyttämään, kun hyväksikäyttökoodi tulee yleisesti saataville.
  - Suosittelemme etenkin internetiin avoinna olevien palveluiden päivitysten pitämistä ajan tasalla sekä mahdollisuuksien mukaan estämään internetistä suoran pääsyn palveluihin.

Tietomurrot ja -vuodot

Tietomurrot ja -vuodot

- Microsoft Office 365 -tietomurtoja tapahtuu edelleen säännöllisesti
  - Murretuille tileille saapuvat sähköpostit lähetetään edelleen usein ulkoiseen sähköpostiin, mistä hyökkääjä voi etsiä tietoja esimerkiksi hyvin toteutettuihin laskutushuijauksiin.
  - Murrettuja tilejä käytetään myös huijaussivustoille osoittavien linkkien jakamiseen.
- Viime kuukauden aikana tietomurroissa on yleistynyt julkisesti verkkoon olevien palveluiden haavoittuvuuksien hyväksikäyttö
  - Sharepoint-haavoittuvuutta käytetään hyväksi myös Suomessa. Haavoittuvuuteen helmikuussa julkaistu korjaus osoittautui puutteelliseksi, jonka takia huhtikuun lopussa julkaistiin toinen korjaus. Haavoittuvuuden käytön estäminen edellyttää molempien päivitysten asentamista.
  - Useampi tietoturvatoimija on kehittänyt esimerkkikoodin Microsoftin RDP/RDS-etätyöpöytäratkaisussa olevaan haavoittuvuuteen. Haavoittuvuuden hyväksikäytöstä ei kuitenkaan nähty toukokuussa viitteitä.
  - Päivittämättömät julkaisujärjestelmät ovat usein verkkorikollisten kohteena, koska se on varsin helppo tapa saada julkaistua haitallista materiaalia julkisilla internet-sivuilla.
- Maailmalla uutisoitiin yksittäisten laajojen tietomurtojen aiheuttaneen jopa kymmenien miljoonien eurojen tappioita yrityksille alkuvuoden aikana

Suojautumisohjeita tietomurtojen varalta

- Käytä eri salasanaa jokaisessa palvelussa.
- Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot.
- Säilytä salasanoja turvallisesti.
- Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen vääriin käsiin.
- Käytä monivaiheista tunnistamista, jos käyttämissäsi palveluissa sellainen on mahdollista.

Huijaukset ja kalastelut

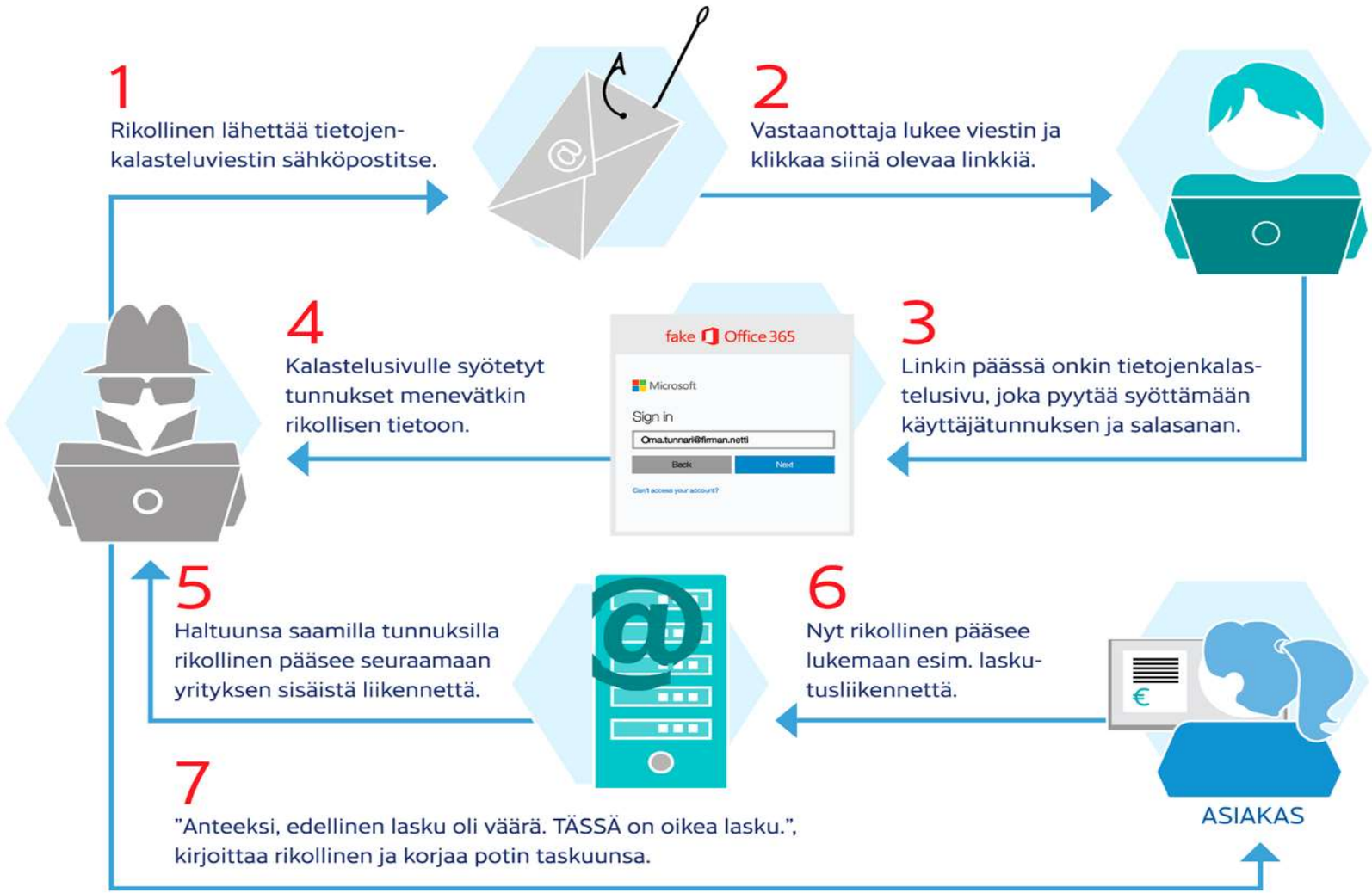
Huijaukset ja kalastelut

- Kesä ja lomakausi tuovat tullessaan laskutuspetoksia
  - Toimitusjohtajahuijaukset yleistyvät kesällä, kun lomakausina maksuja hyväksyvät sijaiset tai kesätyöntekijät.
  - Toimitusjohtajahuijauksissa johtajan nimiin väärennetyillä viesteillä yritetään saada organisaation tilinhaltijaa siirtämään rahaa huijarin tilille.
- Uudenlaiset maksupetokset kohdistuvat palkanmaksuun
  - Nyt huijari lähettää työntekijän nimissä palkanlaskijalle tai henkilöstöhallintoon sähköpostin, jolla yritetään vaihtaa palkanmaksutietoja siten, että palkka maksetaan huijarin tilille.

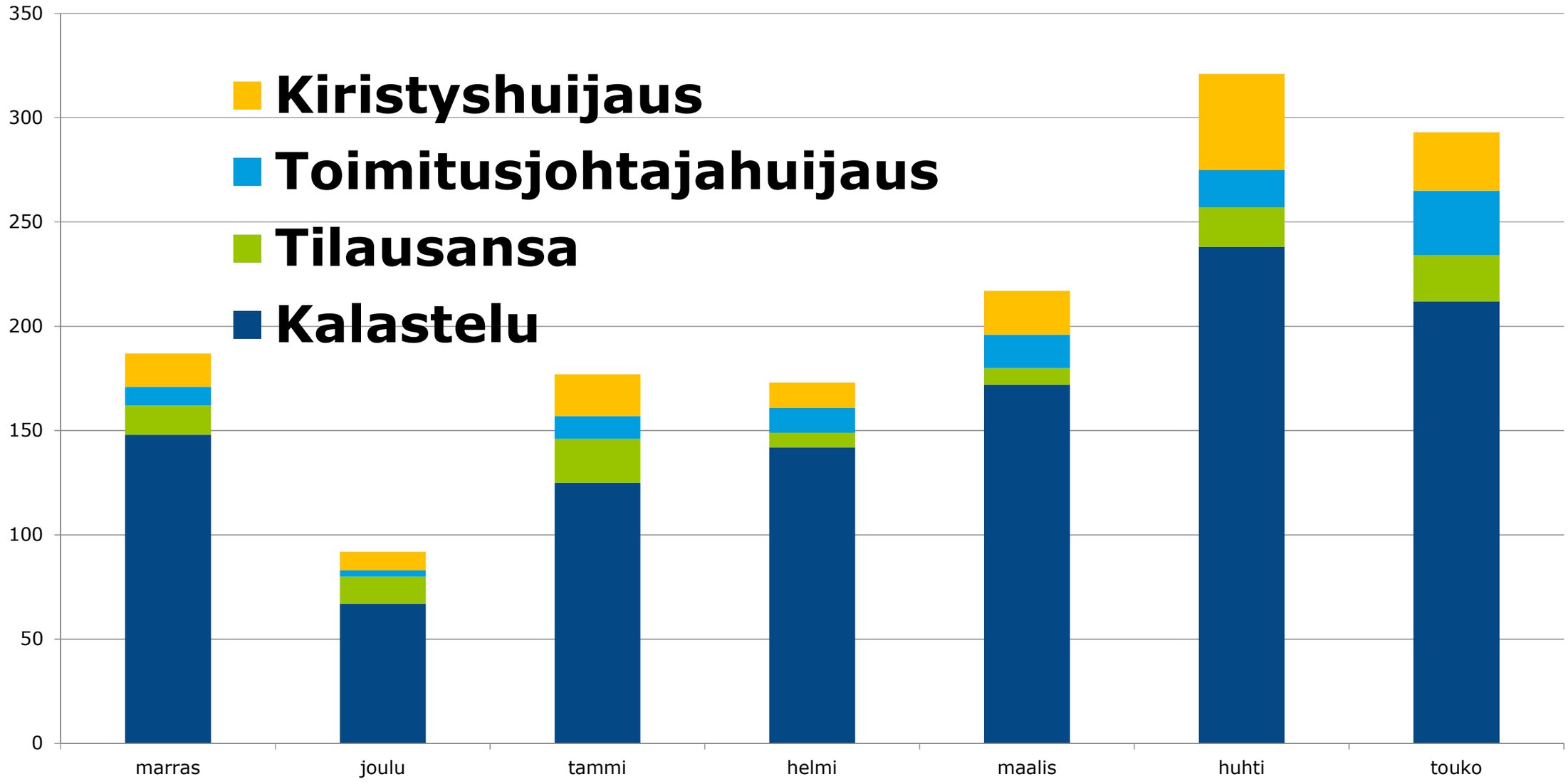
Huijaukset ja kalastelut

- Vuoden voimassa ollut varoitus Office 365 -palvelun tietomurroista tietojenkalastelun avulla poistetaan kesäkuussa 2019
  - Kalastelun uhka ei kuitenkaan ole poistunut.
  - Julkaisimme kattavan ohjeen Office 365 -ympäristön suojaamiseen: https://www.kyberturvallisuuskeskus.fi/fi/node/2532
  - Tiedostonjakopalveluita käytetään levittämään vilpillisiä PDF-tiedostoja ja linkkejä kalastelusivuille.
- Pornokiristyksiä tehtaillaan edelleen aktiivisesti
  - Huijari käyttää uhkailuun vanhoja salasanavuotoja, väärennettyä sähköpostia tai muita keinoja, mutta väitteet ovat valetta.
- Uudenlainen kiristäjä uhkaa pilata uhrin maineen roskapostitulvalla, ellei uhri maksa 0,5 BTC.

Office 365 –huijauksen vaiheet



Käsiteltyjä huijaustapauksia 2018/11–2019/05



IoT ja automaatio

IoT ja automaatio

- Tietoturvatutkija löysi yleisistä taloautomaatio- ja kulunvalvontatuotteista yli sata haavoittuvuutta.
- Northwestern Universityn tutkijat murtautuivat lentokoneiden lentoa tukeviin järjestelmiin ja onnistuivat manipuloimaan lentoa.
- Vastuulliset käytännöt automaatiojärjestelmien tietoturvapuutteista ilmoittamisessa leviävät. Esimerkkiä on näyttänyt esimerkiksi Remod Oy.
- SANSin blogikirjoituksessa seitsemän hyvää käytäntöä teollisuusautomaatiojärjestelmän tietoturvatilanteen tehokkaaseen arviointiin.

Tietoturva-alan kehitys

Oikeudelliset asiat 1/2

- EU:n sähköisen viestinnän tietosuojasta-asetuksen ("ePrivacy") valmistelu on kesken, ja sitä edistettäneen Suomen EU-puheenjohtajakaudella syksyllä 2019.

- EU:n komissio on julkaissut ohjeet muiden kuin henkilötietojen vapaan liikkuvuuden (asetus (EU) 2018/1807) suhteesta EU:n tietosuojalainsäädäntöön.
  - http://europa.eu/rapid/press-release_IP-19-2749_fi.htm

- EU:n kyberturvallisuusasetus (EU) 2019/881 on julkaistu EU:n virallisessa lehdessä ja tulee voimaan 27.6.2019.
  - https://eur-lex.europa.eu/legal-content/EN-FI/TXT/?uri=CELEX:32019R0881&from=EN
  - Asetus on jäsenvaltioissa suoraan sovellettavaa velvoittavaa lainsäädäntöä, ja sillä vahvistetaan:
    - EU:n kyberturvallisuusvirasto ENISA:n tavoitteet, tehtävät ja organisatoriset näkökohdat (pysyvä mandaatti), sekä
    - Kehys eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamiselle.

Oikeudelliset asiat 2/2

- Sähköisen viestinnän palveluista annetun lain (917/2014) uudistaminen EU:n sähköisen viestinnän säännöstön (”telepaketti”, ”EECC”) voimaansaattamiseksi
  - Työ on jatkunut ja seurantaryhmän kokousten videotallenteet löytyvät LVM:n kanavalta YouTubesta.
    - https://www.youtube.com/channel/UCcVp5kxaimHcSMo8_A66Sgg
- Tiedustelulait sekä niitä täydentävät valtioneuvoston asetukset tulivat voimaan 1.6.2019.
  - Poliisilain (872/2011) uusi 5 a luku siviilitiedustelusta (581/2019)
  - Laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019)
  - Laki sotilastiedustelusta (590/2019)
    - Sisältävät säännöksiä mm. teleyritysten avustamisvelvollisuudesta, teleyrityksille maksettavasta korvauksesta sekä teleyrityksen säilyttämien tietojen käyttämisestä
- Vuosipäiviä
  - EU:n yleinen tietosuoja-asetus (”GDPR”) ollut sovellettavana jo vuoden verran.
    - Lue lisää tietosuojasta https://tietosuoja.fi/
  - EU:n verkko- ja tietoturvadirektiivin ("NIS-direktiivi") voimaanpaneva kansallinen lainsäädäntö ollut voimassa vuoden. Lue lisää https://www.kyberturvallisuuskeskus.fi/fi/nis-direktiivi

Kyberuutisointia maailmalta

Valtionhallinnon toimijat harjoittelijat kybertapahtumia ja yhteistoimintaa

- Jyväskylässä järjestettiin toukokuussa viikon kestänyt valtionhallinnon kyberharjoitus KYHA19vh.
- Lähes sata valtionhallinnon toimijaa harjoitteli kyberuhilta suojautumista Kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTECissä. Harjoitusta tuli myös Turvallisuuskomitean sihteeristö.
- Jyväskylän harjoituksessa luotiin arkitodellisuutta vastaavia kyberturvallisuustilanteita. Osa tiimeistä toimii hyökkääjinä, toiset puolustautuivat.

EU:lle valtuudet rangaista vakaviin kyberhyökkäyksiin osallistuneita hakkereita

- EU päätti toukokuussa, että mistä päin tahansa maailmaa tehtyjen vakavien kyberhyökkäysten tekijöitä voidaan rangaista.
- Rangaistusmallit voivat olla esimerkiksi varojen jäädyttämistä ja matkustuskielto Schengen-alueelle.
- Toimivalta yhtenäistää Iso-Britanniassa ja Hollannissa käytössä olleita diplomaattisia toimintoja, joita esimerkiksi Italia on aiemmin vastustanut.
- Toimilla pyritään ennalta ehkäisemään tulevia kyberhyökkäyksiä.

Iso-Britannia kertoo varoittaneensa kuuttatoista Nato-maata venäläisperäisestä hakkeroinnista

- Iso-Britannia kertoo kuuttatoista maata koskevista varoituksesta ilmenneen viimeisen 18 kuukauden aikana.
- Iso-Britannian kansallinen kyberturvallisuuskeskus kertoo, että varoituksia on annettu myös muihin kuin Nato-maihin.
- Tavoitteena raportoidaan olleen kriittisen infrastruktuurin haavoittuvuuksien kartoittaminen.