#kybersää 08/2018

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

rauhallinen

huolestuttava

vakava

Kybersään lähteinä ovat vastaanottamamme ilmoitukset, omat järjestelmämme, kansainvälinen tiedonvaihto, uutiset ja muut julkiset lähteet

Varoitus 02/2018: Office 365 -tunnuksia kalastellaan aktiivisesti

- Suomalaisten yritysten työntekijöiden sähköpostitunnuksia ja -viestejä on kuluvan vuoden aikana varastettu. Punainen varoitus aiheesta oli voimassa myös heinäkuussa. Varoitus on elokuussa laskettu kriittisestä (punainen) vakavaksi (keltainen).
- Tietojenkalastelu on useissa tapauksissa kohdistunut organisaatioiden johtoon ja maksuliikenteestä vastaaviin henkilöihin.
- Käyttäjätunnuksia ja salasanoja on kalasteltu sähköpostitse ja huijaussivujen avulla.
- Kalastelluilla tunnuksilla on kirjauduttu yritysten Office 365 -sähköpostitileille ja pyritty seuraamaan yritysten sähköpostiliikennettä, saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia.
- Kyberturvallisuuskeskus antoi asiasta varoituksen 11.6.2018, joka on edelleen voimassa. Lisätietoja: https://www.viestintavirasto.fi/2018/varoitus-2018-03

#kybersää 08/2018

Palvelunestot

- Palvelunestohyökkäys häiritsi suomi.fi – verkkopalvelun toimintaa
- Suomalaiselta yritykseltä kiristetty 1 BTC palvelunestohyökkäyksen lopettamiseksi

Haittaohjelmat & haavoittuvuudet

- Kotireitittimien haittaohjelmahavainnot nousussa myös Suomessa
- Useita kriittisiä haavoittuvuuksia eri ohjelmistoissa, joihin on julkaistu myös hyväksikäyttömenetelmiä.

Huijaukset & kalastelut

- Office-sähköpostitunnuksia kalastellaan ja kaapattuja tilejä käytetään edelleen huijauksiin.
- Apple ID-, Netflix-, PayPal- ja verkkopankki-tunnuksia kalastellaan säännöllisesti

Vakoilu

- Ruotsin vaaleihin yritetään kybervaikuttaa
- Tutkinta yhdistää APT10-ryhmän Kiinan turvallisuusministeriöön
- Raportti kyberuhkista Saksan sähköverkkoon

Verkkojen toimivuus

- Häiriöitä on ollut vähän edellisiin vuosiin verrattuna.
- Kesän aikana muutamia kaapelikatkoksista johtuneita merkittäviä häiriöitä.

IoT

- Faksien laiteohjelmistoista löytyi haavoittuvuus, jolla faksi voidaan kaapata puhelinyhteydellä.
- Haavoittuvia 3D-tulostimia suojaamattomina kiinni internetissä.

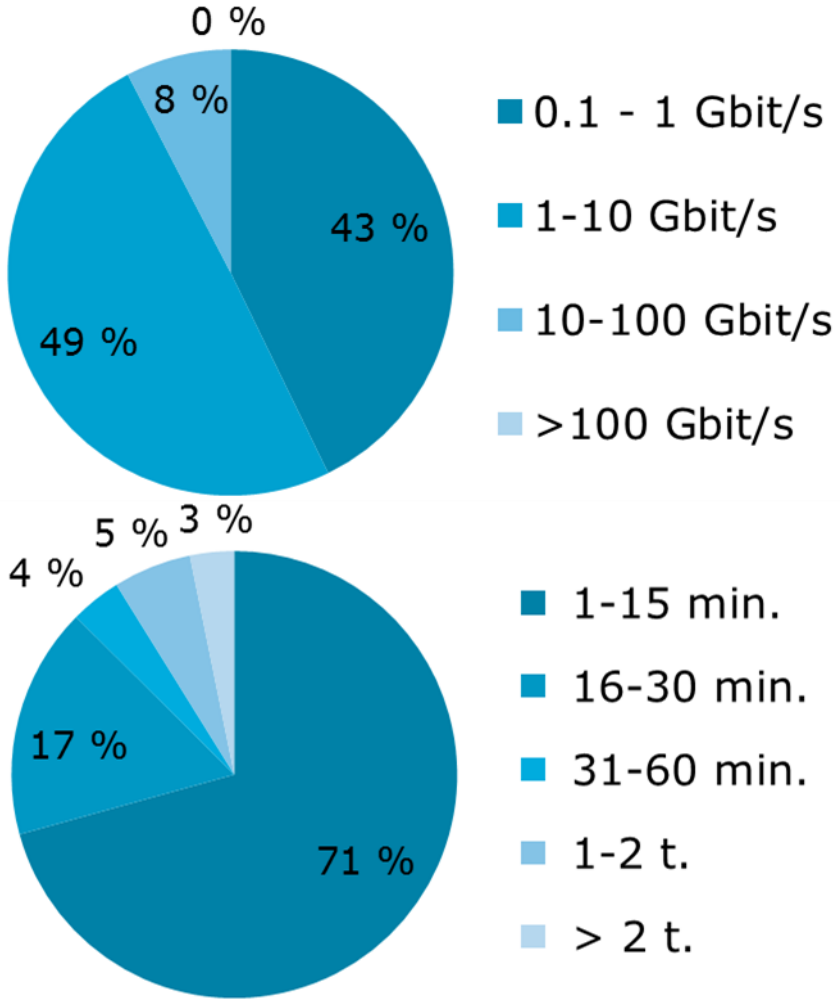
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu:

- Lyhyet alle 15 min hyökkäykset ovat yleisimpiä (71 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 57 % kaikista nähdyistä hyökkäyksistä ovat volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Myös yli 10 Gbit/s hyökkäyksiä nähdään Suomessa useita viikoittain.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Viestintävirastoon ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä. Lähde: teleyritykset

2018/Q2:	**2018/Q1:**	**2017/Q4:**
n. 37 Gbit/s (kesto 8 min)	n. 35 Gbit/s (kesto 7 min)	n. 57 Gbit/s (kesto alle 10 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2018/Q2. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu

- Suomi.fi -verkkopalvelua vastaan tehtiin elokuussa palvelunestohyökkäys, joka aiheutti katkoksia ja hitautta palvelun toiminnassa.
  - Hyökkäys vaikutti myös sivustoihin, jotka hyödyntävät suomi.fi –tunnistautumista. Esimerkiksi Poliisin ja Verohallinnon palveluihin kirjautumisessa oli ongelmia hyökkäyksen aikana.
- Kyberturvallisuuskeskuksen tietoon on tullut suomalaiseen yritykseen kohdistunut palvelunestohyökkäys, mihin liittyi myös kiristysviesti.
  - Rikolliset kiristivät yritykseltä 1 Bitcoinia, eli noin 6300 euroa, jotta hyökkäys loppuisi.
  - Hyökkäys oli toteutettu HTTP FLOOD -tekniikalla
- Espanjan keskuspankkia vastaan tehtiin elokuun lopussa palvelunestohyökkäys, joka vaikutti julkisen verkkosivun toimintaan.
- Palvelunestohyökkäyksiä on siirrytty tekemään enenevässä määrin ns. HTTP FLOOD -tekniikalla, jossa WWW-palvelinta kuormitetaan suurella määrällä HTTP-kyselyitä.
  - Torjuminen on perinteisiä hyökkäystekniikoita haastavampaa, sillä HTTP FLOOD -kyselyt näyttävät normaalilta selainliikenteeltä. HTTP FLOOD –hyökkäyksellä voidaan myös kuormittaa palvelinta tavanomaista hyökkäystä tehokkaammin.

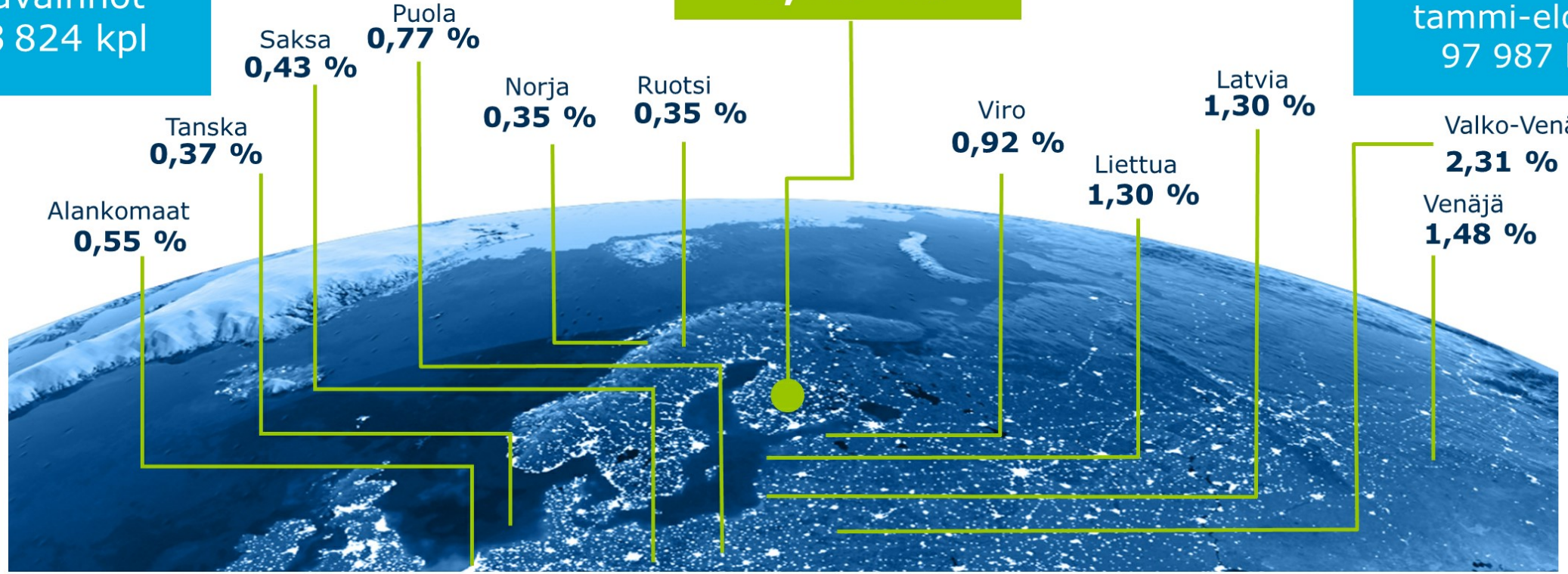
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-elokuu
97 987 kpl



Vuoden 2018 toukokuusta alkaen tietoturvapoikkeamahavaintojen määrä on kasvanut pienreitittimien haittaohjelmatartuntojen vuoksi

Haittaohjelmat

- Kotireitittimien haittaohjelmahavainnot nousussa Suomessa
  - Suomalaisia kotireitittimiä on toukokuusta 2018 alkaen saastunut haittaohjelmalla, joka on tarttunut luultavasti jonkin haavoittuvuuden tai väärän konfiguraation seurauksena.
  - Saastunut kotireititin yrittää levitä eteenpäin liikennöimällä portteihin, jotka ovat tyypillisiä Mirai-sukuisilla haittaohjelmilla.
- Magento- verkkokauppa-alustoja on murrettu ja ne on laitettu varastamaan asiakas- ja luottokorttitietoja.
  - Erään tietoturvatutkijan mukaan n. 7000 Magento-alustaa käyttävää verkkokauppaa on murrettu viimeisen 6 kk aikana

Haavoittuvuudet

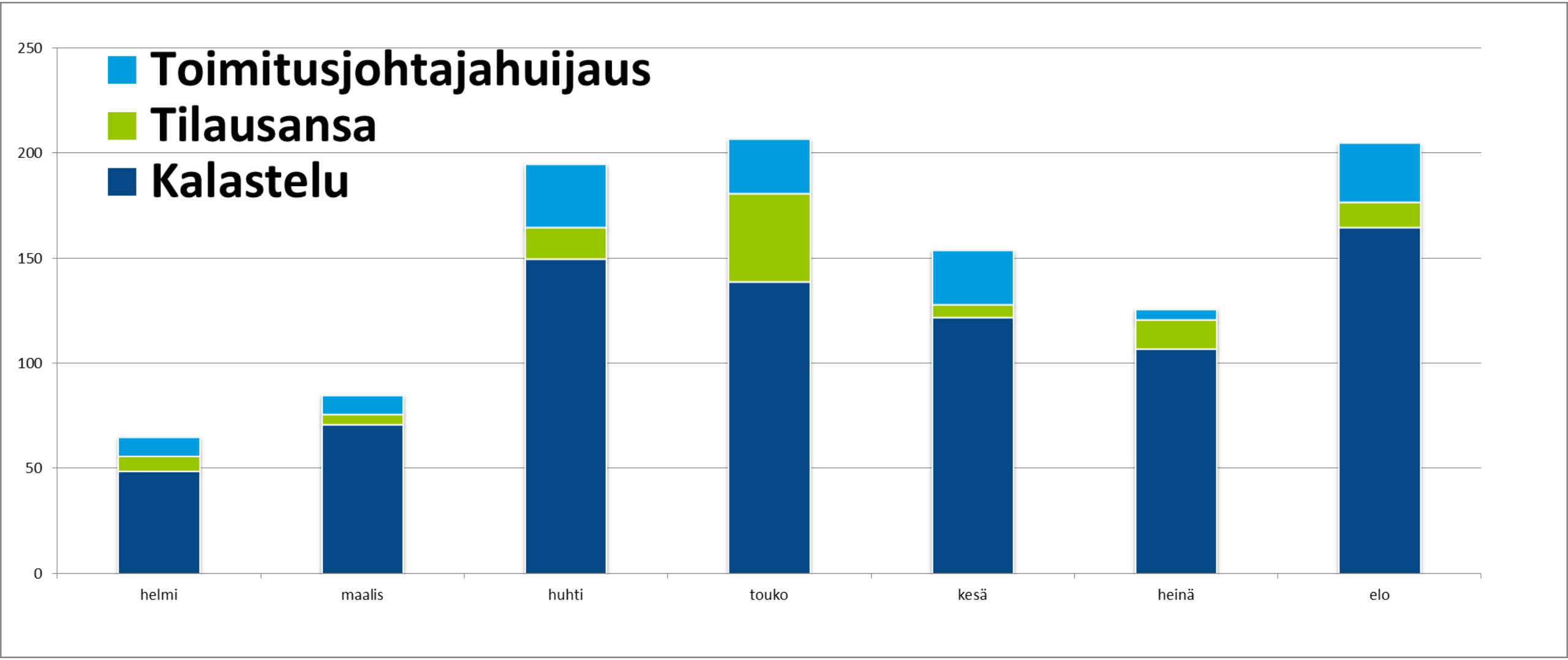
- Kyberturvallisuuskeskus järjesti suomalaisten haavoittuvuustutkijoiden tapaamisen 30.8. Päivän kestäneessä seminaarissa haavoittuvuustutkijat käsittelivät tuoreita haavoittuvuuslöydöksiä ja niiden käsittelyä. Tapaamiseen osallistui noin 70 henkeä.
- Linuxista ja FreeBSD:stä on löydetty TCP- ja IP-pakettien pilkkomiseen liittyvä haavoittuvuus, jonka avulla hyökkääjä voi aiheuttaa palvelunestohyökkäyksen.
- Apache Struts -sovelluskehyksestä löydettiin jälleen kriittinen haavoittuvuus ja siihen on myös julkaistu hyväksikäyttömenetelmä. Haavoittuvuutta on hyödynnetty tietomurroissa.
- Microsoft korjasi Windows-järjestelmistä task scheduler -haavoittuvuuden, jonka avulla paikallinen käyttäjä voi laajentaa käyttöoikeuksiaan järjestelmätasolle.
- Oracle korjasi tietokannastaan haavoittuvuuden, joka salli tietokantapalvelimen haltuunoton etäkäyttöisesti.
- Intel-prosessoreista löydettiin haavoittuvuus, jossa samalla suorittimella ajettavat ohjelmat voivat saada tietoa toistensa toiminnasta. Haavoittuvuus koskee erityisesti monen käyttäjän järjestelmiä, kuten virtualisoituja ympäristöjä ja pilvipalveluja.

Huijaukset & kalastelut

Huijaukset elokuussa

- Office 365 -tunnusten kalastelu on jatkunut
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Tilien sähköpostit edelleenlähetetään rikollisille, jotka voivat hyödyntää niitä mm. toimitusjohtajahuijauksiin tai teollisuusvakoiluun.
  - Petoksilla ja muilla rikoksilla tavoitellaan merkittävää rikoshyötyä.
- Kiristyskampanja säikäyttää paljastuneella salasanalla
  - Heinäkuussa alkanut kiristyshuijaus jatkui läpi koko elokuun. Kiristysviestissä väitetään, että uhrin tietokone on saatu haltuun ja kameralla on kuvattu käyntejä aikuisviihdesivustolla. Väitteet ovat huijausta.
  - Huijauksen uskottavuutta lisää, että huijari väittää tietävänsä uhrin salasanan. Salasana on ihan oikea, mutta se on jostain vuosia vanhasta tietovuodosta eikä liity aikuisviihteeseen tai työaseman käyttäjätunnuksiin.
  - Kiristäjä vaatii lunnaita bitcoineina siitä hyvästä, ettei paljastaisi arkaluontoisia tietoja. Lunnaat olivat aluksi tuhansia dollareita, mutta elokuun lopulla huijari vaati enää alle 500 dollaria.
- Tietoja yritetään kalastella tunnettujen pankkien ja tuotemerkkien nimissä
  - Apple ID -tunnusten kalastelu lisääntyi elokuun lopulla.
  - Prisma-aiheisia tilausansoja on lähetetty suuria määriä.
  - OP-pankki ja S-pankki ovat yleisiä teemoja. Myös Netflix- ja PayPal-tunnuksia yritetään kalastella.

Huijausyritykset 2018/02–08



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

Ruotsin vaaleihin yritetään kybervaikuttaa	Turvallisuuspoliisi SÄPÖ on havainnut Ruotsin parlamenttivaaleihin kohdistuvaa kybervaikuttamista.
APT10 –ryhmän takana on Kiinan turvallisuus-ministeriö	Julkaistu tutkinta syyttää Kiinan turvallisuusministeriön oleva toimijan APT10 takana, joka on tunkeutunut useiden ICT-palvelutarjoajien verkkoihin.
Raportti Saksan sähköverkkoon kohdistuvista kyberuhista	Saksalaisten asiantuntijoiden mukaan on mahdollista, että hakkerit lamauttaisivat sähkönjakelun koko Euroopan laajuisesti.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

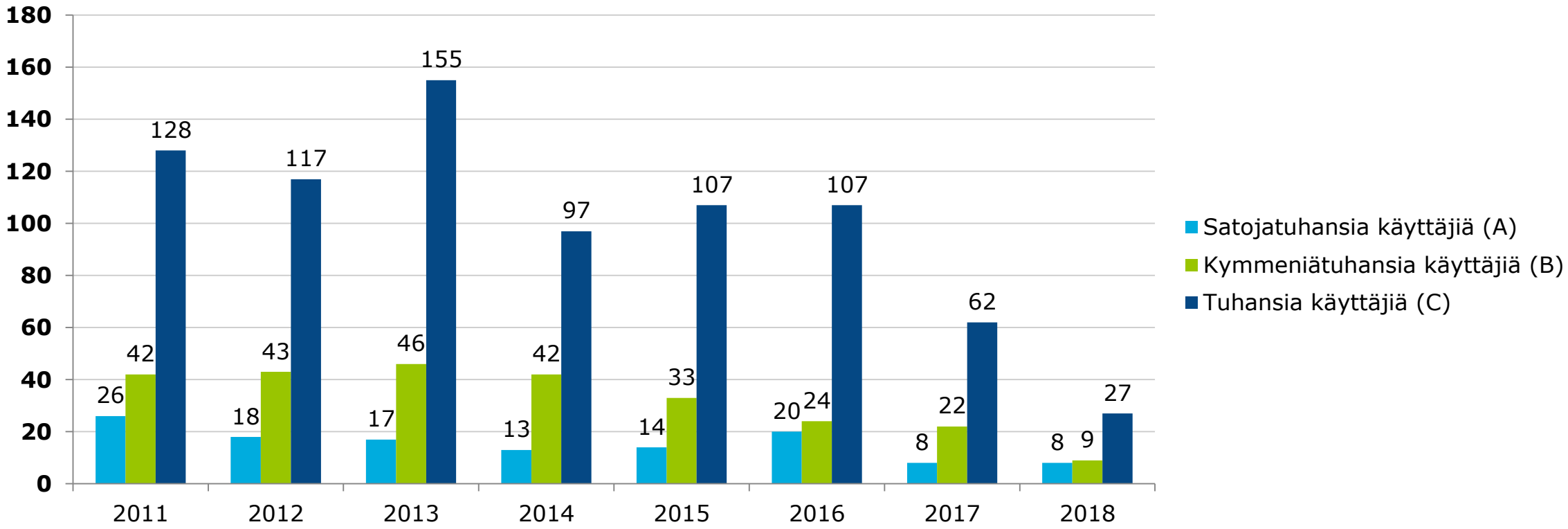
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018
(tammi-elokuu)

Vakavuus	Lukumäärä
A-luokka	8
B-luokka	9
C-luokka	27
Kaikki häiriöt (Q1–Q2)	**208 026**

Alkuvuonna on ollut poikkeuksellisen vähän merkittäviä häiriöitä. Vakavimpia A-luokan häiriöitä on ollut kesän aikana paljon, mutta se vaikuttaa sattumalta.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokan toimivuushäiriöt. Niitä on vuosittain 100–200. Pienempiä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 vuodessa.

IoT

Esineiden internet (IoT) heinäkuun yhteenveto

- Faksien haavoittuvuudet.
  - » HP:n valmistamien monitoimitulostinten ja faksien laiteohjelmistoista löytyi haavoittuvuus. Korjaava ohjelmistopäivitys on saatavilla
  - » Laitteen voi kaapata hallintaansa puhelinyhteyden kautta. Hyökkääjän täytyy vain tietää haavoittuvan faksin puhelinnumero.
  - » Haavoittuvuus toimii myös väylänä sisäverkon suojausten ohi.
  - » Tietoturvatutkijat uskovat, että vastaavia haavoittuvuuksia on myös muiden valmistajien faksilaitteissa sekä fakseja käsittelevissä ohjelmistoissa.
- Suojaamattomat 3D-tulostimet
  - » Internetiin kytkettyjen 3D-tulostinten suojaamattomia hallintakäyttöliittymiä löytyy runsaasti hakukoneilla.
  - » Hyökkääjä voi esimerkiksi varastaa tulostimesta tulostusohjeita tai katsella useissa tulostimissa olevaa webbikameraa.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- Sisällöstä sovittu: Eurooppalainen sähköisen viestinnän säännöstö
  - Jäsenmaat hyväksyivät EU:n televiestintäuudistuksen (*European Electronic Communications Code, EECC*) 29.6.2018. Tekstien viimeistelyn jälkeen direktiivi on vielä hyväksyttävä virallisesti sekä julkaistava EU:n virallisessa lehdessä, minkä tapahtunee vuoden lopulla.
  - Ks. lisää http://www.consilium.europa.eu/fi/press/press-releases/2018/06/29/telecoms-reform-to-bolster-better-and-faster-connectivity-across-eu-approved-by-member-states/

- Lausunnolla: Tiedonhallintalaki
  - VM:ssä valmisteltu hallituksen esityksen luonnos on parhaillaan lausuntokierroksella ja siitä järjestetään esittelytilaisuus 14.9.2018 Ks. https://vm.fi/tiedonhallintalain-valmistelu.

- Valiokuntakäsittelyssä:
  - Tiedustelulakipakettia koskevat esitykset (HE:t 198/2017, 199/2017, 202/2017 ja 203/2017)
  - EU:n yleistä tietosuoja-asetusta täydentävää lainsäädäntöä koskeva esitys (HE 9/2018)
  - Esitys laiksi Liikenne- ja viestintäviraston perustamisesta, Liikennevirastosta annetun lain muuttamisesta ym. (HE 61/2018)
  - Esitykset rajavartiolain ja ulkomaalaislain muuttamisesta (HE 201/2017) sekä puolustusvoimista annetun lain muuttamisesta (HE 72/2018) --> laeissa säädettäisiin mm. valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin

Kyberasioihin liittyvää uutisointia maailmalta

Uusi saksalaisraportti pyrkii arvioimaan kriittiseen infrastruktuuriin kohdistuvia kyberuhkia. Raportin mukaan **yksittäisten energiaa toimittavien saksalaisyhtiöiden jakelun lamauttaminen heijastuisi kaikkialle Eurooppaan**, sillä yhtiöt ovat verkostoituneet ulkomaille ja toimittavat sähköä useisiin EU-maihin.

Israel perusti kyberpuolustuskeskuksen turvaamaan lentokenttää. Ben-Gurion lentokentän suojaksi perustettiin kyberpuolustuskeskus sen jälkeen, kun lentokentän ICT-infrastruktuuria vastaan tehtyjen kyberhyökkäysten määrä nousi merkittävästi.

Viro ajaa kyberturvallisuusasioiden nostamista YK:n turvallisuusneuvostoon. Viron presidentti Kersti Kaljulaid kertoo maan hakevan kiertäväksi jäsenvaltioksi edistääkseen kyberturvallisuusasioita sekä nostaakseen tekoälyn YK:n turvallisuusneuvoston käsittelyyn.

Viro varoittaa, että vuonna 2019 järjestettäviin **europarlamenttivaaleihin saattaa kohdistua kyberhyökkäys**. Myös Valkoisen talon turvallisuusneuvonantaja John Bolton varoittaa Venäjän, Kiinan, Iranin ja Pohjois-Korean **mahdollisista vaikuttamisyrityksistä Yhdysvaltain välivaaleissa 2018**.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi