#kybersää 05/2018

#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 järjestelmät, kansainvälinen tiedonvaihto, uutiset ja muut julkiset lähteet

#kybersää 05/2018

Palvelunestot

- Toukokuussa palvelunestohyökkäyksiä havaittiin jonkin verran enemmän kuin aiempina kuukausina.
- Sovellustason hyökkäykset ovat yleistyneet.

Haittaohjelmat & haavoittuvuudet

- VPNFilter-haittaohjelma levisi yli 500 000 pienyritysreitittimeen ja verkkotallennuslaitteeseen ympäri maailman.
- Haittaohjelmia on alettu levittää .iqy-päätteisten liitetiedostojen avulla.

Huijaukset & kalastelut

- Microsoftin O365-sähköpostitilejä varastetaan. Varastettuja tunnuksia käytetään mm. toimitusjohtajahuijauksiin ja laskutuspetoksiin.
- Iso tilausansakampanja Postin nimissä.

Vakoilu

- VPNFilter-bottiverkko yhdistetty valtiolliseen toimijaan APT28.
- Turla-ryhmän on havaittu käyttävän avoimen lähdekoodin hyökkäystyökaluja.

Verkkojen toimivuus

- Toukokuussa vain kolme merkittävää häiriötä.
- Teleyritysten ja sähköverkkoyhtiöiden yhteistyö toimii hyvin myrskyn aiheuttamien vikojen korjaamisessa.

IoT

- Palvelunestohyökkäysten aiheuttamia kuluja hyökkäyksiin käytettyjen laitteiden omistajille on arvioitu.
- Hide and Seek -haittaohjelma selviää laitteen uudelleenkäynnistyksestä.

Toukokuussa kybersäässä salamoi Microsoftin Office 365 -sähköpostitilien varastelun vuoksi. Varastetuilla käyttäjätunnuksilla rikolliset tehtailevat toimitusjohtajahuijauksia ja valelaskuja. Vakavaksi tilanteen teki myös VPNFilter-haittaohjelma, joka levisi yli 500 000 pienyritysreitittimeen ja verkkotallennuslaitteeseen maailmanlaajuisesti. Kotimaisten verkkojen hyvä toimivuus rauhoitti kybersäätä.

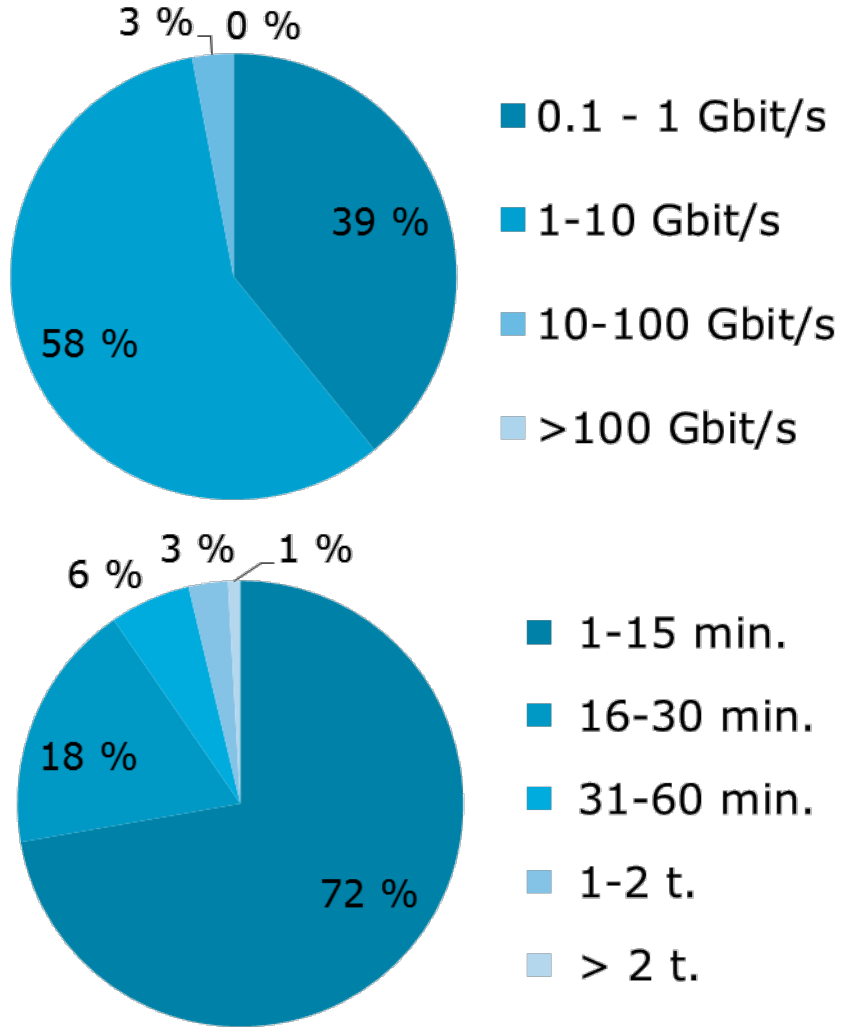
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu

- Lyhyet alle 15 min hyökkäykset ovat yleisimpiä (70 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 55 % 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/Q1:	**2017/Q4:**	**2017/Q3:**
n. 35 Gbit/s (kesto 7 min)	n. 57 Gbit/s (kesto alle 10 min)	n. 30 Gbit/s (kesto 12 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2018/Q1. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu

- **Palvelunestohyökkäyksiä on ilmoitettu Kyberturvallisuuskeskukseen jonkin verran enemmän kuin aiempina kuukausina**
  - Hyökkäyksiä sekä julkista että yksityistä sektoria vastaan on raportoitu aiempaa enemmän.
  - Hyökkäyksille ei ole yhteistä nimittäjää, kohteet ja tekotavat vaihtelevat.
- **Sovellustason hyökkäykset ovat yleistyneet hyökkäystyyppinä**
  - Tämä näkyy muu muassa CLDAP-reflektio-, Slowloris- ja WordPress pingback -hyökkäysten yleistymisenä.

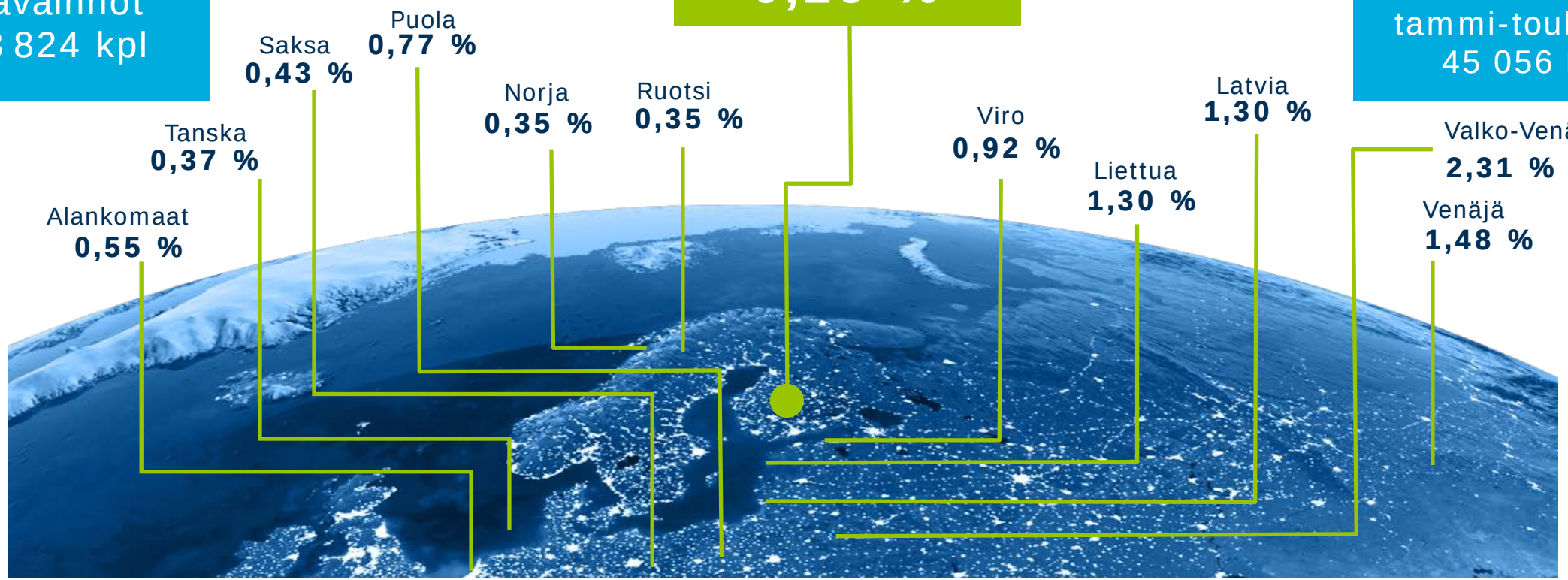
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-toukokuu
45 056 kpl



Vuoden 2018 alussa tietoturvapoikkeamahavaintoja tehtiin vuoden 2017 lopun maltillisen linjan mukaisesti, mutta havaintomäärä on kevään aikana kasvanut voimakkaasti.

Haittaohjelmat

- **VPNFilter-haittaohjelma levisi yli 500 000 pienyritysreitittimeen ja verkkotallennuslaitteeseen ympäri maailman**
  - Suomessa haittaohjelma ei ollut levinnyt laajalti, Kyberturvallisuuskeskuksen tiedossa on noin kymmenkunta uhria.
- **Haittaohjelmia on levitetty .iqy-päätteisten sähköpostin liitetiedostojen avulla**
  - Liitetiedosto avautuu Excelissä, joka käy lataamassa haitallista sisältöä tiedostoston viittaamasta verkko-osoitteesta.
- **Rikolliset ovat siirtyneet levittämään virtuaalivaluuttoja louhivia haittaohjelmia kiristyshaittaohjelmien sijaan**
- **Joulukuussa julkaistua tietoturvaohjelmistojen harhautusmenetelmää (Process Doppelgänging) on hyödynnetty kiristyshaittaohjelmassa**

Haavoittuvuudet

- **Adobe Reader -ohjelmistossa kriittinen haavoittuvuus**
  - Tätä hyödyntämällä ohjelmistokoodin ajaminen on mahdollista pdf-tiedoston avaavassa järjestelmässä.
- **Spectre-haavoittuvuudesta on julkaistu uusia variantteja**
  - Eivät ole kovin helposti hyödynnettävissä.
  - Uusia löydöksiä tehtäneen vielä lisää lähikuukausina.
- **POP SS -haavoittuvuus aiheutui virheellisistä kuvauksista Intelin prosessorin manuaaleissa**
  - Haavoittuvuus johti käyttöoikeuksien nostoon ja koodin suoritukseen paikallisesti.
- **Sähköpostiohjelmien PGP-liitännäiset käsittelivät PGP-viestejä virheellisesti**
  - Niin sanotun "eFail"-haavoittuvuuden vaikutukset jäivät vähäisiksi.

Huijaukset & kalastelut

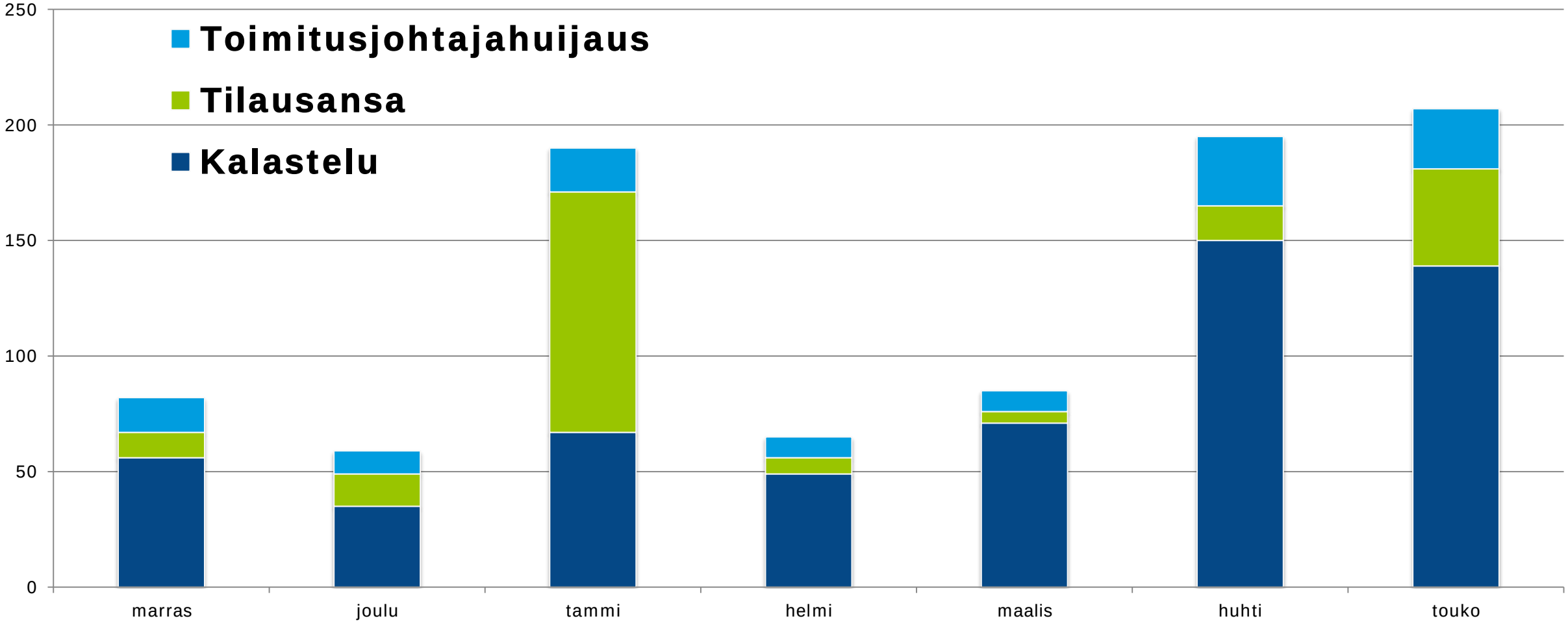
Huijaukset toukokuussa

- **Office 365 -sähköpostitunnuksia varastetaan jatkuvasti**
  - Tietojenkalastelu on lisääntynyt hälyttävästi.
  - Kaapattuja yritysten Office 365 -tunnuksia käytetään tietojenkalasteluun.
  - Sähköpostitse levitettävät tietojenkalastelusähköpostit saavat lisää uskottavuutta, jos ne on lähetetty aidosta sähköpostilaatikosta.
  - *Aiheesta julkaistu varoitus 11.6.18: https://www.viestintavirasto.fi/2018/varoitus-2018-03*

- **Toimitusjohtajahuijaukset lisääntyvät koko ajan**
  - Kaapatut Office 365 -tunnukset ovat yksi väline toimitusjohtajahuijauksien tekoon.
  - Laskutushuijaukset ovat myös onnistuneet, ja niissä menetetään merkittäviä rahasummia.
- **Postin nimissä levitetään tilausansoja**
  - Sähköpostissa kerrotaan saapuneesta lähetyksestä, joka on noudettava ennen kuin se palautuu lähettäjälle. Linkin takana onkin jotakin aivan muuta, esimerkiksi puhelimen arvonta.
  - Todellisuudessa luottokortilla sitoudutaan maksamaan kuukausittaista palvelua.

- **Tietoja yritetään kalastella tunnettujen pankkien nimissä**
  - OP-pankki, S-pankki ja Säästöpankki.
  - Myös Apple ID, Netflix- ja PayPal-tunnuksia yritetään kalastella.

Huijausyritykset 2017/11–2018/05



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

VPNFilter

Satoja tuhansia pienreitittimiä saastuttanut VPNFilter-haittaohjelma vaikuttaa olevan Venäjään yhdistetyn APT28-ryhmän käytössä.

Metasploit Turla

Venäjän tiedusteluviranomaisiin yhdistetyn Turla-ryhmän on havaittu hyödyntävän yleisesti käytössä olevaa Metasploit-tunkeutuistyökalua operaatioissaan.

Havainnointi- ja varoitusjärjestelmän (HAVARO) havainnot

Vuosi 2017

Vakavuus	Lukumäärä
Punainen	597
Keltainen	1 128
Vihreä	62 294
Yhteensä	**64 019**

Vuosi 2018
(tammi-toukokuu)

Vakavuus	Lukumäärä
Punainen	249
Keltainen	12 020
Vihreä	7 714
Yhteensä	**19 963**

Huhtikuussa tehtiin poikkeuksellisen paljon keltaisia havaintoja, jotka johtuivat tietoturvaheikkouksien skannailuista ja tunkeutumisyrityksistä.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

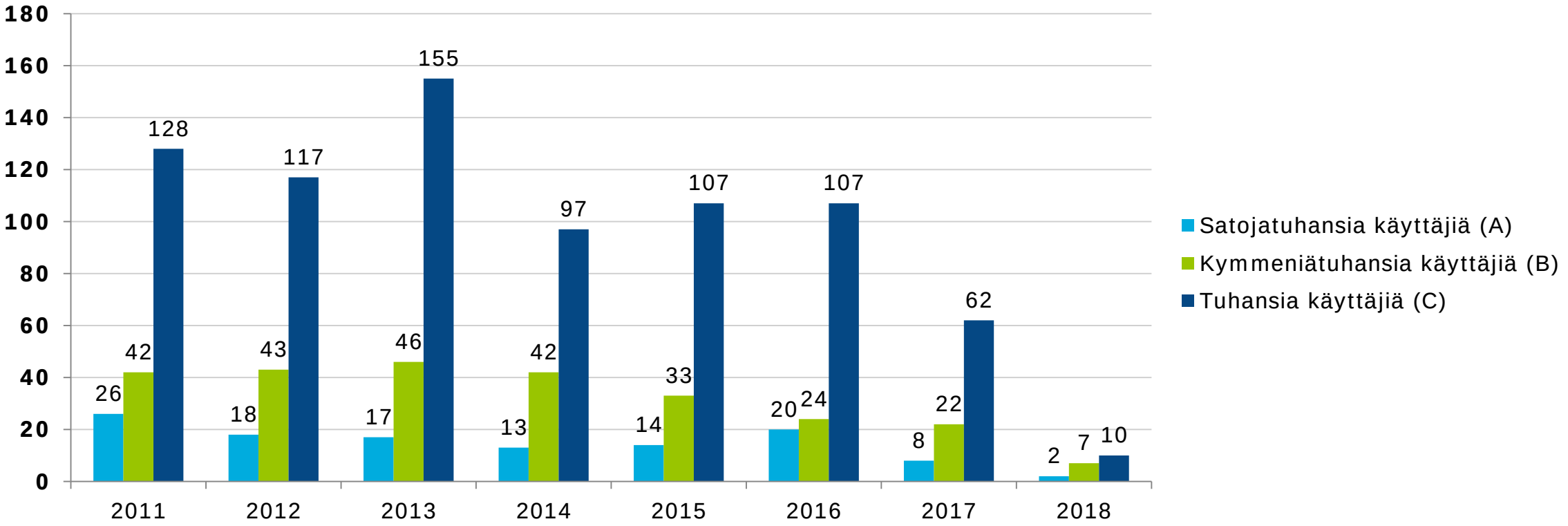
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018
(tammi-toukokuu)

Vakavuus	Lukumäärä
A-luokka	2
B-luokka	7
C-luokka	10
Kaikki häiriöt (1Q)	**96 732**

Alkuvuonna on ollut poikkeuksellisen vähän merkittäviä häiriöitä. Teleyritysten ja sähköverkkoyhtiöiden yhteistyö toimii hyvin myrskyjen aikana.

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) toukokuun yhteenveto

- **Haittaohjelmilla saastutetut IoT-laitteet aiheuttavat kuluja myös niiden omistajille**
  - » Tutkijat arvioivat kulut, joita hyökkäyksessä käytettyjen laitteiden omistajille aiheutui palvelunestohyökkäyksestä KrebsOnSecurity-sivustolle syksyllä 2016: keskimäärin 13,50 USD/hyökännyt laite.
  - » Erittäin vino kulurakenne: hyökkäyksen tilaaja maksoi bottiverkon hallitsijalle muutaman sata dollaria. KrebsOnSecurity-sivustoa puolustanut Akamai arvioi hyökkäyksen torjunnan maksavan miljoonia dollareita.
- **Hide and Seek -haittaohjelma selviää IoT-laitteen uudelleenkäynnistyksestä**
  - » Ensimmäinen laatuaan, ei varmasti viimeinen.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- **Verkko- ja tietoturvadirektiivi tuli sovellettavaksi 9.5.**
  - https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2018/velvollisuudetraportoidatietoturvaloukkauksistalaajenevateunverkko-jatietoturvadirektiivinnismyota9.5.2018.html
  - Viestintävirasto ja toimialakohtaiset valvovat viranomaiset jatkavat toimeenpanon valmistelua.
  - EU:n komission täytäntöönpanoasetus (EU) 2018/151 digitaalisten palveluiden turvallisuuden riskihallinnasta ja poikkeamien merkittävyyden arvioinnista tuli sovellettavaksi 10.5.2018 alkaen. Asetuksen kohteena pilvipalvelut, verkon markkinapaikat ja hakukoneet.
  - Jäsenvaltioiden yhteistyötä kehittäminen jatkuu muun muassa CSIRT-verkostossa.
- **Uusi siirtymäaikataulu TUPAS-tunnistuksen muutoksille**
  - Päivitetty Määräys 72A/2018 sähköisistä tunnistus- ja luottamuspalveluista on tullut voimaan 22.5.
  - Tunnistukseen on lisättävä sanomatason salaus.
  - Muutoksia vaaditaan sekä tunnistuspalvelun tarjoajan ja asiointipalvelun tarjoajan järjestelmiin.
  - Vaihtoehtoisesti TUPAS-protokollaa käyttävät toimijat voivat siirtyä toisen tietoturvavaatimukset täyttävän protokollan käyttämiseen (esim. SAML tai OIDC).

Ajankohtaiset lakiasiat

- **Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018 vp) on valiokuntakäsittelyssä**
  - Kansallinen laki täydentäisi EU:n yleistä tietosuoja-asetusta (GDPR).
- **Tiedustelulakipakettia koskevat hallituksen esitykset ovat valiokuntakäsittelyssä** (HE 198/2017 vp, HE 202/2017 vp ja HE 203/2017 vp)
- **Hallituksen esitys eduskunnalle laeiksi rajavartiolain ja ulkomaalaislain muuttamisesta sekä eräiksi niihin liittyviksi laeiksi on edelleen valiokuntakäsittelyssä** (HE 201/2017)
  - Laissa säädettäisiin mm. valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin.
- **Hallituksen esitys laiksi puolustusvoimista annetun lain muuttamisesta** (HE 72/2018) on annettu eduskunnalle 31.5.2018
  - Laissa säädettäisiin valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin.

Kyberuutisointia maailmalta

Cisco Systems Inc. varoitti 23.5., että yli 500 000 reititintä ja verkkotallennuslaitetta yli 50 maassa oli saastunut tasokkaalla VPNFilter-haittaohjelmalla. Mediassa on spekuloitu, että taustalla olisi Venäjän valtio ja kohteena mahdollisesti Ukraina. Haittaohjelmaa hyödyntämällä on mahdollista kuunnella reitittimien läpi kulkevaa liikennettä, myös salasanoja. Mahdollista myös kyberoperaation käynnistäminen ja teollisuusautomaation lähettämän liikenteen kuuntelu.

Isossa-Britanniassa kriittisen infrastruktuurin yrityksiä vaaditaan raportoimaan kyberuhkista, tietomurroista ja verkkohäiriöistä viranomaisille 72 tunnin kuluessa 23 miljoonan dollarin uhkasakon uhalla.

Papua-Uusi-Guinea estää pääsyn Facebookiin kuukauden ajaksi. Ministeriö pyrkii selvittämään, miten palvelua käytetään maassa. Media on nostanut esiin huolen siitä, että maa on siirtymässä Kiinan, Pohjois-Korean ja Iranin tielle, jossa ihmisten, yritysten ja yhteisöjen oikeuksia rajoitetaan merkittävästi.

Vakoilukampanja, jossa kohteena oli Thaimaa ja 16 muun maan kriittinen infrastruktuuri, on paljastunut. Tietoturvayhtiö McAfee varoitti, että operaatio GhostSecretin myötä kriittisen infrastruktuurin yritysten verkkoihin on saatu ujutettua haittaohjelma, joka varastaa ja lähettää tietoa operaation takana olevalle ryhmittymälle. Operaation epäillään olevan pohjoiskorealaisen Hidden Cobra -ryhmittymän käsialaa.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi