#kybersää helmikuu 2018

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tarkoituksena on antaa lukijalle nopea kokonaiskuva siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

vakava

#kybersää 02/2018

Palvelunestot

- Hyökkäysten määrä lisääntyi Suomessa.
- Memcached-palvelua alettu käyttää hyökkäysten vahvistamiseen. Tuloksena historian voimakkain hyökkäys.

Haittaohjelmat & haavoittuvuudet

- WannaMine tarttui useiden organisaatioiden palvelimiin Suomessa.
- Rikolliset suosivat ja levittävät nyt virtuaalivaluuttoja louhivia haittaohjelmia.

Huijaukset & kalastelut

- Yhä yleistä: pankkitunnusten kalastelu ja toimitusjohtajahuijaukset.
- Saksalaisista puhelinnumeroista arveluttavia ja lyhyitä soittoja lukuisille suomalaisille.
- Kansalaisaloite-sivu kopioitu tilausansaksi.

Vakoilu

- Turla-ryhmä tunkeutui Saksan valtionhallintoon.
- USA ja UK uskovat Venäjän olevan NotPetya-haittaohjelman tekijä.
- Olympialaisten tietojärjestelmiä yritettiin tuhota.

Verkkojen toimivuus

- Vain kaksi merkittävää häiriötä helmikuussa.
- Vuoden 2017 kaikkien häiriöiden lukumäärä oli poikkeuksellisen korkea edellisvuosiin verrattuna. Viestintävirasto selvittää syytä.

IoT

- Teollisuusautomaatiojärjestelmässä ensimmäistä kertaa virtuaalivaluuttaa louhiva haittaohjelma. Vakavilta seurauksilta vältyttiin.
- IoT-haittaohjelmien kehittäminen kiinnostaa rikollisia edelleen.

Helmikuussa 2018 useita vakavia tietoturvaloukkauksia

Maailmalla tehtiin historian suurin palvelunestohyökkäys, josta vähäisesti merkkejä myös Suomessa. Suomessa organisaatioden palvelimiin tarttunut WannaMine-haittaohjelma hidasti palveluiden toimintaa. Saksan liittovaltion tietojärjestelmiin tehty kohdistettu hyökkäys paljastui.

Viestintävirasto julkaisi Tietoturvan vuosi 2017 -katsauksen https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2018/tietoturvanvuosi2017-julkaisu0012018j.html

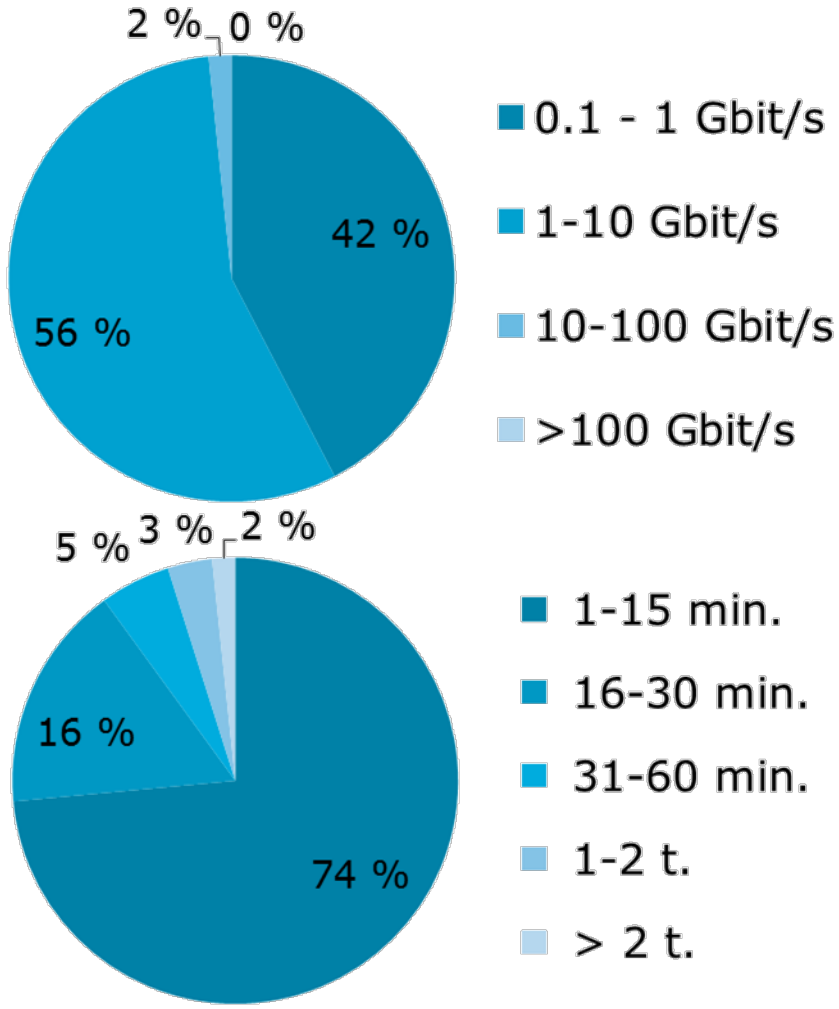
Palvelunestot

Palvelunestohyökkäysten volyymit

- Lyhyet alle 15 min hyökkäykset ovat yleisimpiä (72 %). Niitä nähdään tuhansia kappaleita vuodessa.
- Organisaatioiden kannattaa varautua riskiarvioissaan vähintään yli 1 Gbit/s volyymin hyökkäyksiin. Niiden osuus havaituista hyökkäyksistä on noin 60 %.
- Myös yli 10 Gbit/s hyökkäyksiä nähdään Suomessa useita viikoittain.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Viestintävirastoon ilmoitetaan hyökkäyksistä vain murto-osa.

Suurimpia Suomessa viimeaikoina havaittuja palvelunestohyökkäyksiä. Lähde: teleyritykset

2017/Q4:	**2017/Q3:**	**2017/Q2:**
n. 57 Gbit/s (kesto alle 10 min)	n. 30 Gbit/s (kesto 12 min)	n. 77 Gbit/s (kesto 7 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2017/Q4. Lähde: Telia. Seuraava tilasto: maaliskuussa 2018

Palvelunestohyökkäyksissä ajankohtaista

- Hyökkäysten määrä Suomessa lisääntyi selvästi helmikuun aikana
  - Elinkeinoelämän keskusliitto joutui helmikuun alkupuolella palvelunestohyökkäyksen kohteeksi ja tiedotti asiasta esimerkillisesti.
- Memcached-palvelun käyttö hyökkäysten vahvistamiseen keksittiin helmikuussa
  - Historian suurin hyökkäys on nyt 1,7 Tbit/s.
  - Kartoitimme yhdessä teleyritysten kanssa Suomessa internetiin näkyviä memcached-palveluita ja tiedotimme ylläpitäjiä palvelun suojaamisen tärkeydestä.

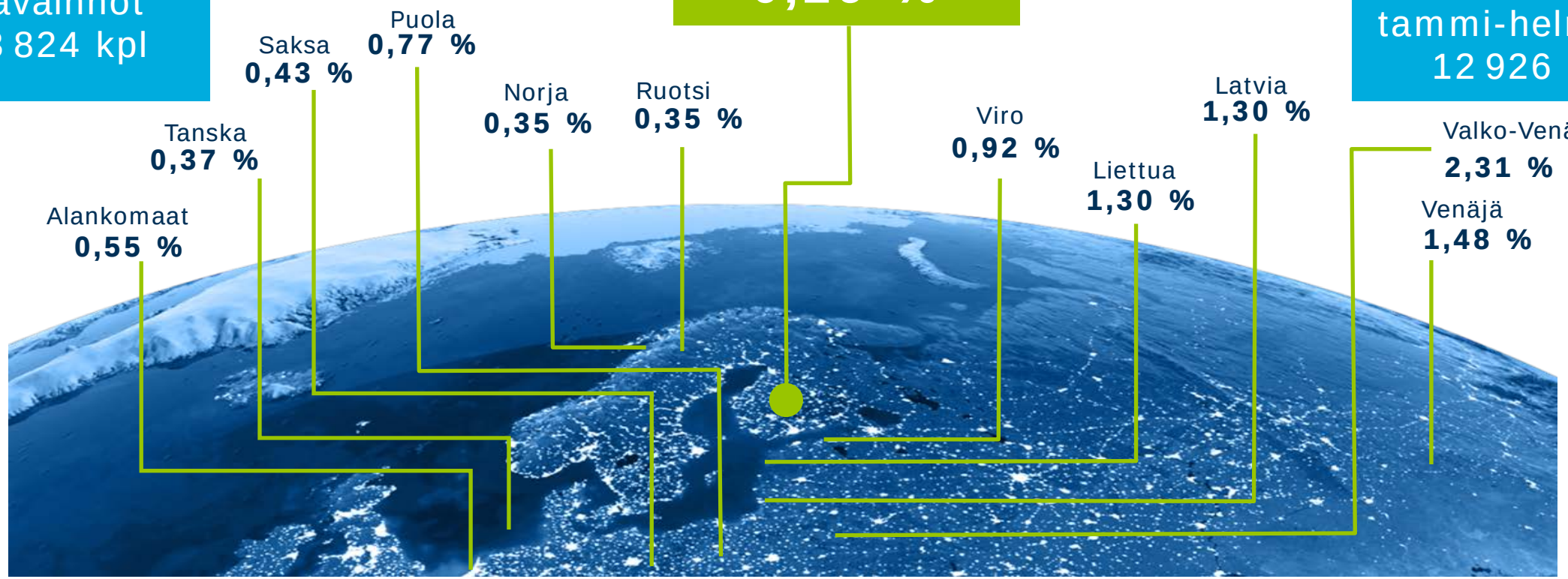
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-helmikuu
12 926 kpl



Havaintojen määrissä ei juuri eroavaisuuksia vuonna 2017 ja 2016.

Haittaohjelmien ja haavojen ajankohtaiset

- WannaMine-haittaohjelma tarttui Suomessakin useiden organisaatioiden palvelimiin
  - Leviämistapa on liki identtinen NotPetyan kanssa.
  - WannaMinen pääasiallinen käyttötarkoitus on virtuaalivaluutan louhiminen, mutta se varastaa myös käyttäjätunnuksia ja salasanoja.
- Tammikuussa julki tullutta Adobe Flashin haavoittuvuutta hyödynnettiin helmikuussa exploit kiteissä.
- Cisco ASA -palomuurien WebVPN-toiminnossa kriittinen haavoittuvuus, joka antaa hyökkääjälle mahdollisuuden suorittaa kohdejärjestelmässään omaa ohjelmakoodiaan ilman tunnistautumista.
- SAML-kirjastojen haavoittuvuutta hyödyntämällä voi esiintyä toisena käyttäjänä.
  - SAML-kirjastoja käytetään esimerkiksi verkkoselaimilla tehtävissä kertakirjautumisissa
- Kiristyshaittaohjelmien sijaan rikolliset ovat alkaneet levittää virtuaalivaluuttoja louhivia haittaohjelmia exploit kitien avulla.

Huijaukset & kalastelut

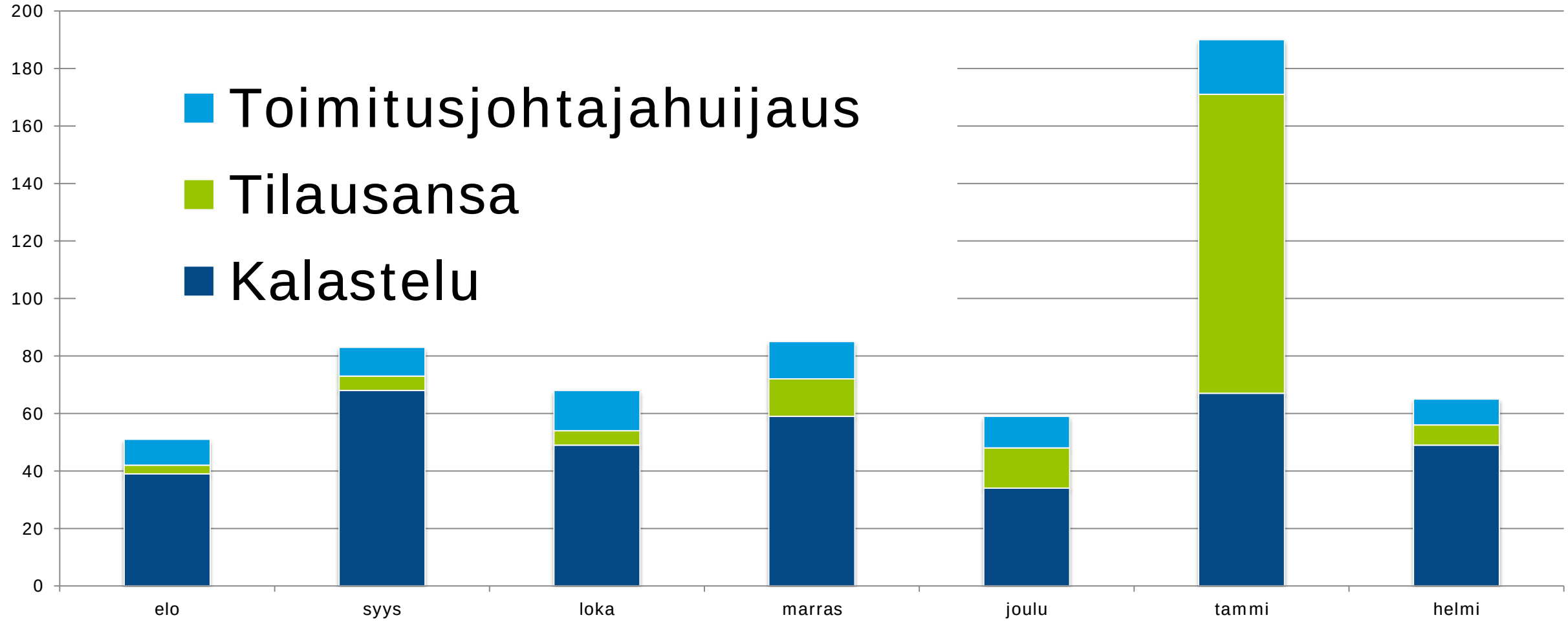
Helmikuun huijaukset

- Tietoja yritetään kalastella tunnettujen pankkien nimissä
  - Muun muassa POP, Aktia, Nordea, Danske, Bank of America.
- Suosittujen verkkopalveluiden tunnusten kalastelua
  - Office 365, OneDrive ja LinkedIn
  - Myös DHL:n, Elisan ja Finnairin nimissä on kalasteltu käyttäjätunnuksia ja luottokorttien numeroita.

- Kansalaisaloite-sivusto kloonattu tilausansaksi
  - Sivusto näytti eri sisällön Google-haun kautta tulleille kuin muuta kautta sivustolle tulleille.

- Saksasta +44-alkuisia puheluita lukuisille ihmisille
  - Puheluilla on todennäköisesti haluttu markkinoida sijoituksia, joiden laillisuus kyseenalaista.
  - Vuonna 2017 vastaavia puheluita soitettiin Iso-Britannian suunnasta.

Huijausyritykset 2017/08–2018/02



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

Saksa

Saksan valtiohallinnon tietoverkkoon on tunkeuduttu. Venäläisen Turla-ryhmän uskotaan olevan tunkeutuja.

NotPetya

Iso-Britannia ja Yhdysvallat syyttävät Venäjän asevoimia kesällä Ukrainassa levinneestä NotPetya-valekiristyshaittaohjelmasta.

Olympic Destroyer

Olympialaisten tietojärjestelmiin tunkeuduttiin ja niiden toimintaa yritettiin estää.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

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

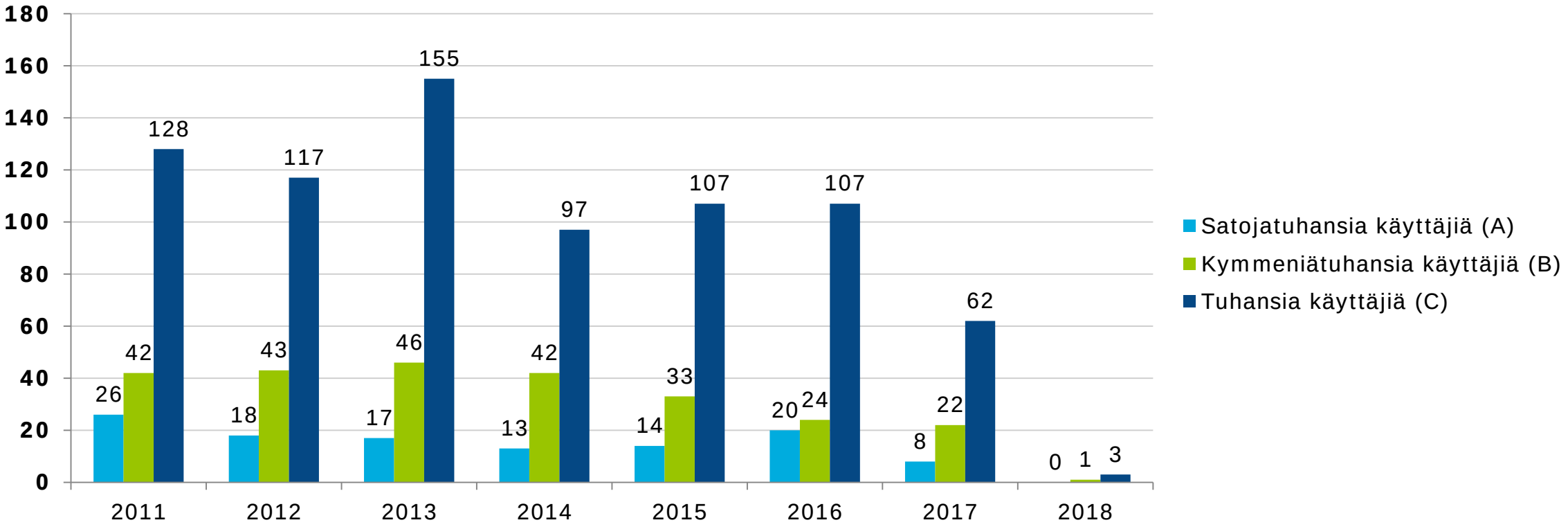
Vuosi 2018
(tammi-helmikuu)

Vakavuus	Lukumäärä
A-luokka	0
B-luokka	1
C-luokka	3
Kaikki häiriöt	**Ei tiedossa**

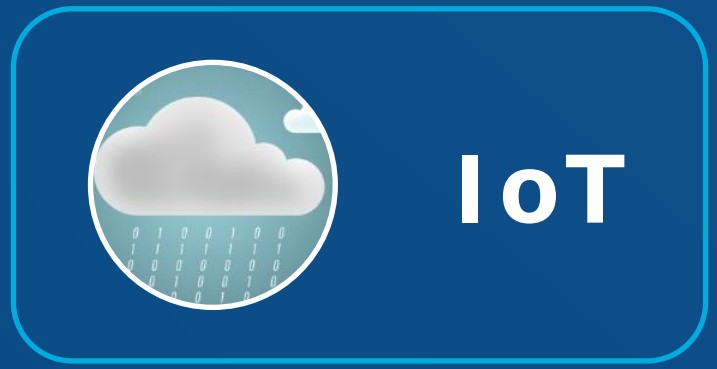
Ensimmäisen vuosineljänneksen tilasto kaikista häiriöistä valmistuu huhtikuun lopussa.

Kotimaiset viestintäverkot toimivat melko hyvin myös helmikuussa. Kaikkien häiriöiden lukumäärä oli huomattavan suuri 2017. Selvitämme asiaa.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokkien toimivuushäiriöt. Niitä on vuosittain 100–200. Pienempiä häiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–350 000 vuodessa.


IoT

Esineiden internet (IoT) helmikuun yhteenveto

- Haittaohjelma eurooppalaisen vesilaitoksen automaatiojärjestelmässä
  - Tammikuun 2018 alussa järjestelmään tarttui kryptovaluuttaa louhiva haittaohjelma. Tämä on ensimmäinen dokumentoitu kerta, kun automaatiojärjestelmään on tarttunut tällainen haittaohjelma.
  - Haittaohjelma hidasti automaatiojärjestelmää, mutta ei ehtinyt aiheuttaa vakavaa häiriötä vesilaitoksen toiminnalle.
  - Katso Tietoturvayhtiö Radiflow'n raportti Detection of a Crypto-Mining Malware Attack at a Water Utility http://radiflow.com/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/.
- Rikolliset kehittävät vanhoja IoT-haittaohjelmia
  - Muiden muassa Satori- ja OMG-haittaohjelmia on helmikuun aikana täydennetty uusilla leviämis- ja hyökkäyskeinoilla. Rikolliset yhä kiinnostuneita IoT:stä.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- NIS-direktiivin täytäntöönpanon valmistelu jatkuu kotimaassa ja EU:ssa
  - HE 192/2017 vp laeiksi Euroopan Unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta on käsiteltävänä eduskunnassa
  - EU:n komissio antoi 30.1.18 täytäntöönpanoasetuksen (EU) 2018/151 digitaalisten palveluiden turvallisuuden riskihallinnasta ja poikkeamien merkittävyyden arvioinnista. Asetusta sovelletaan pilvipalveluihin, verkon markkinapaikkoihin ja hakukoneisiin 10.5.2018 alkaen.
  - Jäsenvaltioiden yhteistyötä kehitetään muun muassa CSIRT-verkostossa
- Viestintävirasto valmistelee siirtymäaikataulun jatkamista TUPAS-tunnistuksen muutoksille
  - Tunnistukseen on lisättävä sanomatason salaus
  - Tämä tehdään muuttamalla kevään aikana määräystä 72/2016
  - Valmisteluun toivotaan erityisesti sähköisten asiointipalveluiden osallistumista, koska muutokset vaikuttavat niihin
  - Lisätietoja hankkeesta ja osallistumisesta: https://www.viestintavirasto.fi/ohjausjavalvonta/lausuntopyynnottiedoksiannotkyselyt/lausuntopyynnot/viestintavirastonkommenttipyyntokutsujamuistiotunnistusmaarayksen72tupas-muutoksesta.html

Ajankohtaiset lakiasiat

- Hallitus on esittänyt uuden tietosuojalain säätämistä henkilötietojen käsittelyä koskevaksi yleislaiksi (http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta)
  - Tietosuojalaki 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)
- Muun muassa rajavartiolain ja ulkomaalaislain muuttamista koskeva hallituksen esitys valiokuntakäsittelyssä (HE 201/2017, http://intermin.fi/hybridiuhat)
  - Säädettäisiin esimerkiksi valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin

- Puolustusministeriön työryhmämietintö miehittämättömän ilmailun lainsäädännön kehittämisestä turvallisuuden näkökulmasta ollut lausuttavana 31.1.2018 asti
  - https://www.defmin.fi/ajankohtaista/tiedotteet/2017/puolustusministerion_tyoryhmamietinto_miehittamattoman_ilmailun_lainsaadannon_kehittamisesta_turvallisuuden_nakokulmasta_valmistui.8915.news

Kyberasioihin liittyvää uutisointia maailmalta

Olympialaisten organisaatiota vastaan hyökättiin haittaohjelma **OlympicDestroyerillä**. Haittaohjelma pyrkii tuhoamaan tietokoneille tallennettuja tietoja.

Väestörekisterikeskus avasi haavoittuvuuspalkinto-ohjelman. Mukaan ilmoittautuneet haavoittuvuustutkijat voivat saada rahapalkintoja suomi.fi-verkkopalvelusta löytämistään haavoittuvuuksista, jotka ne raportoivat vastuullisesti VRK:lle.

Venäjän turvallisuuspalvelu FSO sai uusia valtuuksia tietoturvauhkien ja informaatiovaikuttamisen torjuntaan ja "valtion politiikan toteuttamiseen kansainvälisen tietoturvan alalla"

UNICEF vetoaa lasten edun asettamiseksi digitaalipolitiikan keskiöön. Joka kolmas internetin käyttäjä on lapsi tai nuori. Lapset ovat erityisen alttiita internetin haitallisille ilmiöille.

Viestintävirasto
Kyberturvallisuuskeskus

cert@ficora.fi

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi