

kybersää tammikuu 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



Kybersään kooste 12 kk

Ajanjakson merkittävimmät tietoturvapoikkeamat

Tietojenkalastelu

Apple ID –kalastelu jatkuu ja näyttää jääneen pysyväksi ilmiöksi.

Mirai

Haittaohjelma aktivoitunut uudestaan. Hyödyntää haavoittuvia IoT-laitteita.

NotPetya

Haittaohjelma levisi Ukrainasta ympäri maailmaa. Suomessa vaikutukset vähäisiä.

Apache Struts

Haavoittuvuutta hyödynnetään tietomurroissa.

Viron sähköiset henkilökortit

Viro päivitti 750 000 henkilökorttia haavoittuvuuden vuoksi.

Meltdown & Spectre

Vaikuttavat lähes kaikkiin tietokoneisiin, Riskinä erityisesti virtuaalipalvelinympäristöt

macOS root

MacOS High Sierra –käyttöjärjestelmässä normikäyttäjä saa helposti root-tunnuksen.

Maalis

Huhti

Touko

Kesä

Heinä

Elo

Syys

Loka

Marras

Joulu

Tammi

Helmi

2017

2018



WannaCry

Haittaohjelma levisi tehokkaasti organisaatioiden sisäverkoissa.

Palvelunestot

Hyökkäykset häiritsevät muun muassa sähköisiä reseptejä sekä –tunnistuspalveluita.

DDE-toiminto

Haittaohjelmia levitetään Microsoftin Office-ohjelmistojen DDE-elementin avulla.



WPA2 KRACK

Langattoman lähiverkon KRACK-haavoittuvuus vaatii päätelaitteiden päivittämistä.

kybersää 01 / 2018



Palvelunestot

- Alkuvuonna Suomessa havaittu kohtuullisen vähän.
- Hollannissa palvelunestohyökkäyksiä pankkeihin ja julkista sektoria vastaan.



Vakoilu

- Pohjois-Korea hyödynsi korjaamatonta haavoittuvuutta Flash Player –sovelluksessa.
- Hollannin tiedustelupalvelu murtautui venäläisten vakoilijoiden järjestelmiin.
- Tietomurto Norjan terveydenhuollon järjestelmiin.



Haittaohjelmat & haavoittuvuudet

- Meltdown- ja Spectre-hyökkäykset prosessorien kiusana.
- Virtuaalivaluuttoja louhivat haittaohjelmat ovat yleistyneet.
- Flashin 0-päivähaavoittuvuutta hyödynnetty.



Verkojen toimivuus

- Viestintäverkoissa on ollut hankalista sääolosuhteista huolimatta vain pieniä häiriöitä.
- Alkuvuoden tykkylumitilanne on häirinnyt verkkojen toimintaa Kainuussa.



Huijaukset & kalastelut

- Viestintäviraston pääjohtajan laskutushuijaus.
- S-Pankin nimissä tekstiviesti-huijauskampanja.
- Google ja Bitcoin uusimpia huijausteemoja.



IoT

- Satori-haittaohjelman ohjelmistokoodi on vuodettu Pastebin-tiedonjakopalveluun.
- Tutkijat varoittavat sairaaloiden kuvantamislaitteita vastaan suunnatuista kiristyshaittaohjelmahyökkäyksistä.

Tammikuun 2018 kybersää sakeni vuodenvaihteen haavoittuvuuksista

"Meltdown- ja Spectre-hyökkäyksiin julkaistut ohjelmistopäivitykset ovat olleet huonolaatuisia ja toimiessaankin ovat saattaneet hidastaa suorittimia."



Palvelunestot

Tilastojen valossa: palvelunestohyökkäykset ja niillä uhkailu

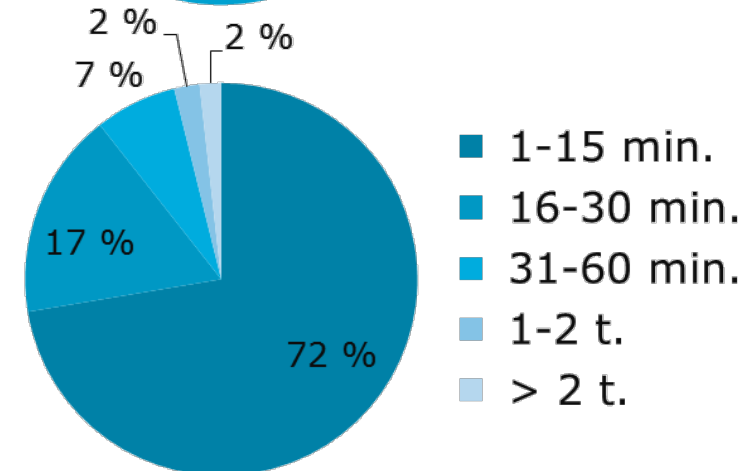
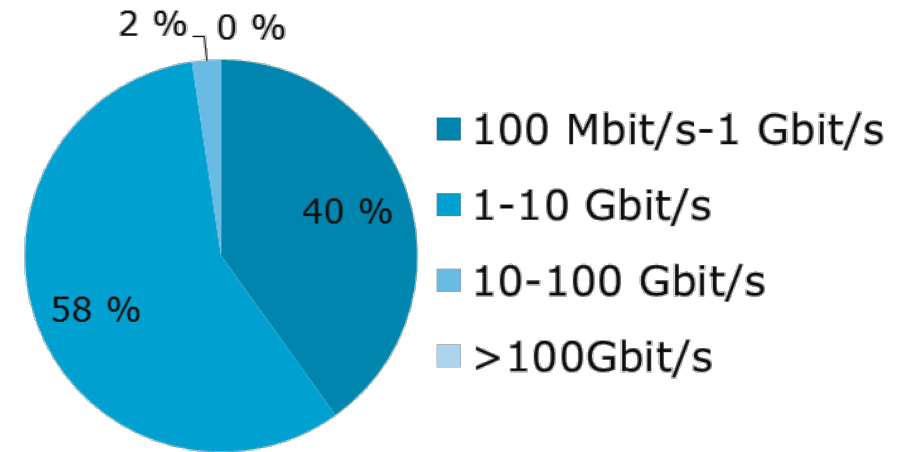
- Lyhyet alle 15 min hyökkäykset ovat yleisimpiä (72 %). Niitä nähdään tuhansia vuodessa.
- Noin 60 % kaikista nähdystä hyökkäyksistä on volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän suuruusluokan hyökkäyksiin riskiarviossaan.
- Myös yli 10 Gbit/s -hyökkäyksiä nähdään Suomessa useita viikoittain.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Viestintävirastoon ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

Lähiaikojen suurimpia Suomessa havaittuja palvelunestohyökkäyksiä

2017 / Q4:
n. 57 Gbit/s
(kesto alle 10 min)

2017 / Q3:
n. 30 Gbit/s
(kesto 12 min)

2017 / Q2:
n. 77 Gbit/s
(kesto 7 min)

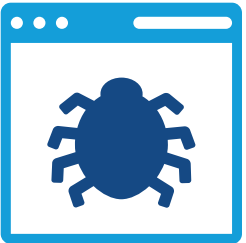


Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2017 / Q3. Keräämme tilaston suoraan teleyrityksiltä. Lähde: Telia. Seuraava tilasto: helmikuussa 2018

Ajankohtaista: palvelunestohyökkäykset ja niillä uhkailu



- Alkuvuonna Suomessa on ollut kohtuullisen rauhallista
 - Elinkeinoelämän keskusliitto joutui helmikuun alkupuolella palvelunestohyökkäyksen kohteeksi ja tiedotti asiasta esimerkillisesti.



- Hollannin pankkeihin ja julkiseen sektoriin kohdistui palvelunestohyökkäysten sarja tammikuun lopussa
 - Hyökkäykset tehtiin noin viikko sen jälkeen, kun Hollannin tiedustelupalvelu oli paljastanut yksityiskohtia kohdistettuja hyökkäyksiä tekevän APT29-ryhmän toiminnasta. Tämä aiheutti julkisuudessa epäilyjä APT29:n kostoiskusta.

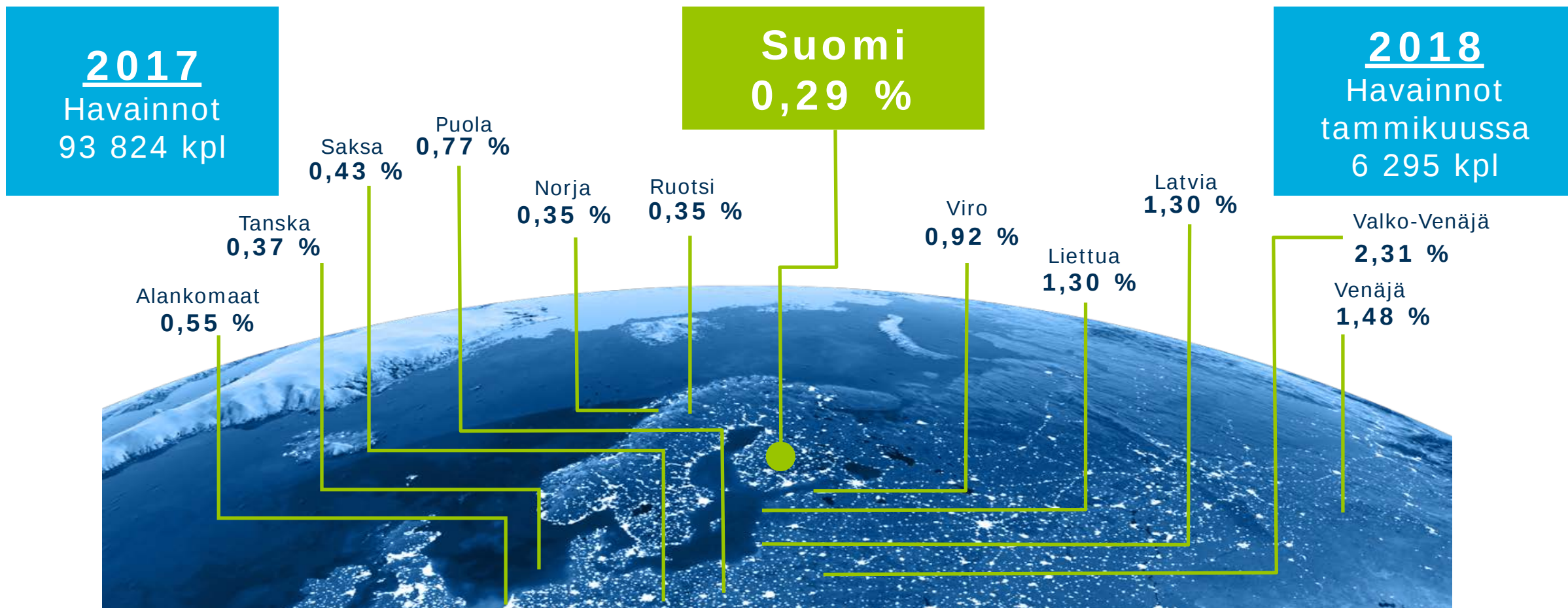


- Hollannin poliisi on kuitenkin helmikuun alkupuolella pidättänyt 18-vuotiaan nuorukaisen epäiltynä verottajaa vastaan tehdystä hyökkäyksestä. Poliisi tutkii parhaillaan onko epäilyllä osuutta myös pankkeja vastaan tehtyihin hyökkäyksiin.



Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

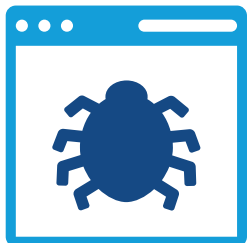


Poikkeamahavaintojen määrä oli vuonna 2017 samalla tasolla kuin 2016.

Haittaohjelmien ja haavoittuvuudet



- Meltdown- ja Spectre-hyökkäykset prosessorien kiusana
 - » Prosessoreiden haavoittuvuudet Meltdown- ja Spectre-hyökkäyksineen vaikuttavat lähes kaikkiin tietokoneisiin PC-koneista puhelimien ja palvelimiin.
 - » Kotikoneen suojana päivitetty käyttöjärjestelmät ja ohjelmistot, ohjelmisto- ja laitevalmistajien huolehdittava haavoittuvuuksien paikkaamisesta.
 - » Vaikutukset suurempia Intel- ja ARM-prosessoreihin, yksi hyökkäyksistä vaikuttaa myös AMD-prosessoreihin. Päivityksillä voi olla vaikutuksia erityisesti vanhempien Intel-prosessorien suorituskäyttöön.
 - » Päivitysongelmia AMD-prosessoreiden ja antivirustuotteiden kanssa.
 - » Ensimmäisiä viitteitä on nyt nähty, että haittaohjelmat hyödyntävät haavoittuvuuksia.



- Adobe Flash Player -ohjelmiston nollapäivähaavoittuvuutta on hyödynnetty kohdistetuissa hyökkäyksissä.
- Virtuaalivaluuttoja louhivat haittaohjelmat ovat yleistyneet maailmalla. Suomessakin nähty muun muassa Monerominer-haittaohjelmaa.



- Epäillyn tietomurron seurauksena Metsä Group antoi ennakkotiedon vuoden 2017 viimeisen neljänneksen liikevaihdosta.
- Microsoft Office –toimisto-ohjelmiston Equation Editor -apuohjelmasta löydettiin lisää haavoittuvuuksia, joita on hyödynnetty hyökkäyksissä. Haavoittuvuudet korjattiin tammikuun 2018 päivityksissä.



Huijaukset & kalastelut

Huijaukset ja tietojenkalastelut



- Tammikuussa 2018 alkoi mittava S-market-aiheinen huijauskampanja tekstiviesteitse
 - » Huijauslinkki johti tilausansa.
 - » Tekstiviestihuijaukset ovat yleistyneet alkuvuodesta merkittävästi.

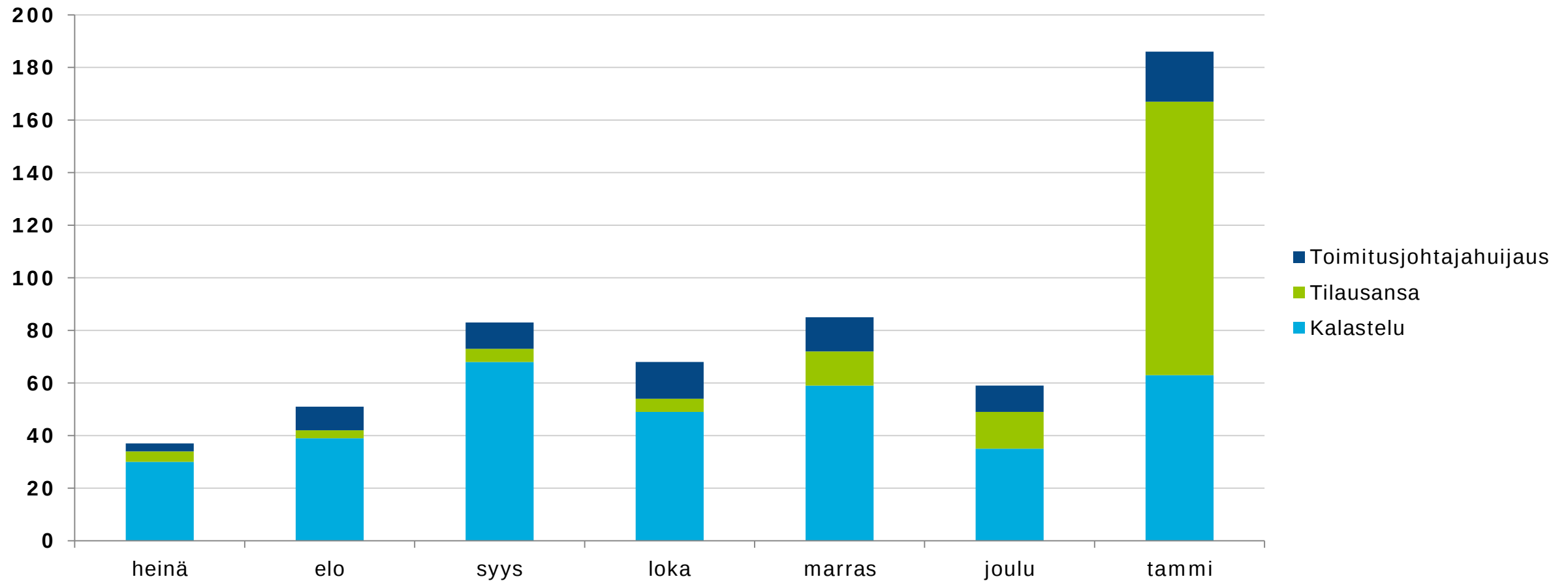


- Tietoja yritetään kalastella tunnettujen pankkien nimissä
 - » Nordea, POP-pankki, Aktia ja S-pankki olivat tammikuussa yleisimmät teemat.
- Googlen nimissä on lähetetty tekaistuja "palkintoja", joiden avulla kalastetaan käyttäjätunnuksia
- Bitcoinin varjolla yritetään monenlaisia huijauksia ja tietojenkalasteluja
- Vilpilliset verkkokaupat lisääntyivät joulusesongin alla. Tarkoituksena harhauttaa kuluttajia
 - » Edes ylätason verkkotunnus ".fi" ei ole kotimaisuuden tai luotettavuuden tae.



- Toimitusjohtajahuijaukset ovat edelleen yleisiä
 - » Maanantaina 22.1.2018 laskutushuijausta yritettiin myös Viestintäviraston pääjohtaja Karlamaan nimissä.
 - » Toimitusjohtajahuijauksia on nähty julkishallinnossa siinä missä muillakin sektoreilla.

Huijausyritykset 2017 / 07 – 2018 / 01





Vakoilu

Verkkovakoilussa ajankohtaista

Adobe Flash Player

Pohjois-Korea hyödyntää Adobe Flash Player -sovelluksen nollapäivähaavoittuutta kohdistetuissa hyökkäyksissään.

Hollannin tiedustelupalvelu

Hollannin tiedustelupalvelu vakoili venäläistä hakkeriryhmää, jota epäillään Yhdysvaltojen vaalien aikaisesta vaikuttamisesta.

Norjan SOTE-piirin tietomurto

Norjalaisen terveydenhoitoalueen tietojärjestelmiin on tehty laajamittainen tietomurto.



Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt (Q1-Q3)	345 787

2017 Q4 häiriöiden kokonaismäärä päivittyy maaliskuussa

Vuosi 2018 (tammikuu)

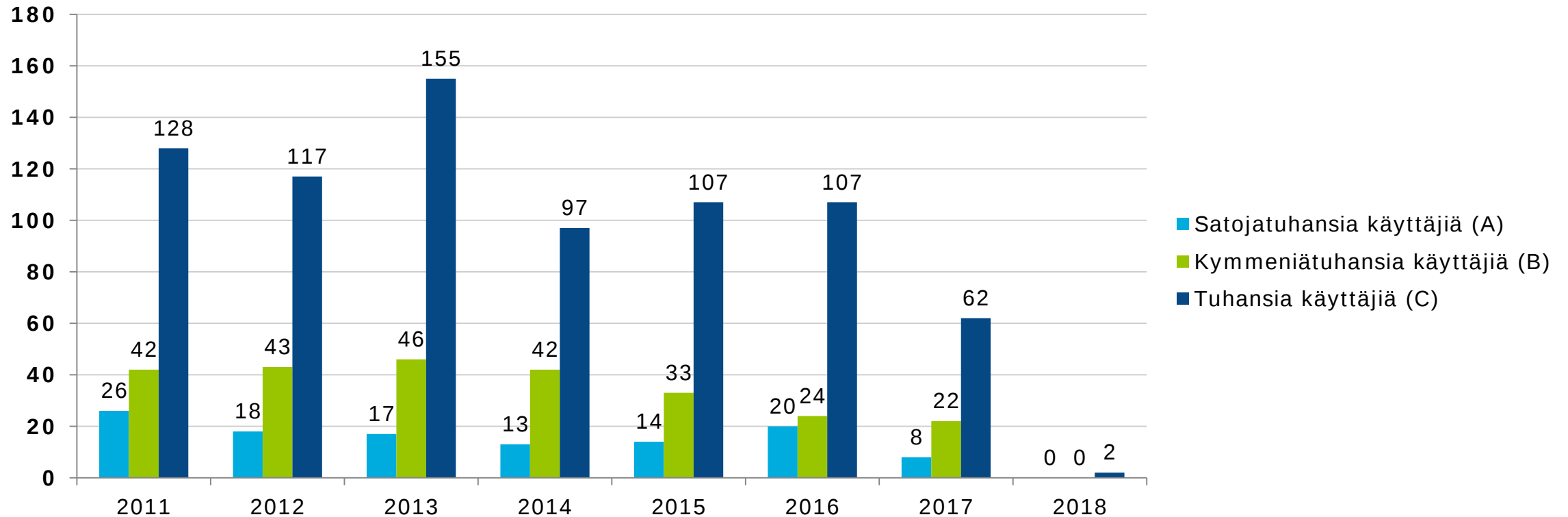
Vakavuus	Lukumäärä
A-luokka	0
B-luokka	0
C-luokka	2
Kaikki häiriöt	

2018 häiriöiden kokonaismäärä päivittyy myöhemmin



Tammikuussa 2018 on hankalista sääolosuhteista huolimatta välttytty vakavilta viestintäverkon häiriöiltä.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokan toimivuushäiriöt. Niitä on vuosittain 150–200. Pienempiä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–350 000 vuodessa.



IoT

Esineiden internet (IoT) tammikuun yhteenveto



- IoT-laitteissa leviävän Satori-haittaohjelman ohjelmistokoodi vuodettiin Pastebin-tiedonjakopalveluun

- » Satori leviää hyödyntämällä muun muassa Huaweiin laitteista löytyvää haavoittuvuutta.
- » Todennäköisesti vuodettu koodi poikii lukuisia Satoriin perustuvia muunnelmia. Ensimmäinen laajemmalle levinnyt muunnos on Jenx.



- Israelin yliopiston tutkijat varoittavat sairaaloiden tietokonetomografia- ja magneettikuvantamislaitteita vastaan suunnatuista kiristyshaittaohjelmista

- » Kuvantamislaitteet on yleensä kytketty sairaaloiden tietoverkkoon, jolloin ne ovat alttiita kehittyneille hyökkäyksille.
- » Laitteet ovat hyökkääjille houkutteleva kohde, koska niiden toiminta on keskeistä sairaalan toiminnan kannalta.



Tietoturva-alan kehitys

Ajankohtaiset lakiasiat



- NIS-direktiivin täytäntöönpanon valmistelu jatkuu kotimaassa ja EU:ssa
 - » Hallitus esitys voimassa olevien lakien muuttamisesta eduskunnan käsittelyssä.
 - » Komission täytäntöönpanoasetus digitaalisten palveluiden tietoturva- ja ilmoitusvaatimuksista julkaistu.
 - » Jäsenvaltioiden yhteistyötä kehitetään mm. CSIRT-verkostossa.
- Tunnistus- ja luottamuspalvelulain (617/2009) vahvan sähköisen tunnistuspalvelun tarjoajia koskeva luottamusverkostosäätely tuli voimaan 1.5.2017
 - » Lainmukaisen luottamusverkoston toimeenpano jatkuu.
 - » Tunnistuslakiin ehdotetut muutokset tulivat voimaan 15.12.2017.
 - Ensitunnistamisen ketjuttamiselle asetetaan enimmäishinta
 - Valvontamaksusäännöksen korjaus
 - » Virasto on aloittanut ensitunnistamisen ketjuttamisen enimmäishinnan asettamisprosessin
- Laki sähköisen viestinnän palveluista korvaa tietoyhteiskuntakaaren 1.6.2018 alkaen
- EU:n yleistä tietosuoja-asetusta (GDPR) aletaan soveltamaan 25.5.2018 alkaen
 - » Asetuksen toimeenpanosta ja valvonnasta vastaa Tietosuojavaltuutetun toimisto.
 - » Asetukseen liittyvä sähköisen viestinnän tietosuoja –asetus (ePrivacy) on edelleen valmistelussa EU:ssa.



Kyberasioihin liittyvää uutisointia maailmalta

Hollannin tiedustelupalvelu AIVD:n kerrotaan hakkeroineen venäläisen APT29-tai Cozy Bear-hakkeriryhmän järjestelmiin. Ryhmän väitetään olleen demokraatteihin kohdistuneen sähköpostimurtojen takana Yhdysvaltojen presidentinvaalien alla.

Ydinasejärjestelmien haavoittuvuuksia tutkinut brittiläinen ajatushautomo varoittaa, että sen tiedonkulkua voidaan manipuloida. Päättäjille voidaan esimerkiksi näyttää väärää tietoa, mikä voi pahimmillaan johtaa jopa tahattomaan ydinaseiden laukaisuun.

Japani liittyy Naton kyberpuolustuskeskukseen, joka sijaitsee Tallinnassa (NATO Cooperative Cyber Defense Center of Excellence (CCD COE)). Viron pääministeri Ratas toivotti Japanin lämpimästi tervetulleeksi.

Ison-Britannian hallitus on linjannut, että kriittisen infrastruktuurin yrityksiä uhkaa jopa 17 miljoonan punnan sakko, jos yritykset eivät rakenna tehokkaita suojauksia kyberhyökkäyksiä vastaan. Linjaus koskee muun muassa energia-, liikenne-, vesi- ja sosiaali- ja terveysalan yrityksiä



Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi
