#kybersää 04/2018

#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

Varoitus 01/2018: Suomalaisten selväkielisiä salasanoja paljastunut

- Helsingin Uusyrityskeskuksen ylläpitämään verkkopalveluun liiketoimintasuunnitelma.com on tehty tietomurto.
- Murron yhteydessä noin 130 000 käyttäjän käyttäjätunnukset ja selväkieliset salasanat ovat paljastuneet.
- Myös muita luottamuksellisia tietoja on voinut paljastua. Tietovuoto on käyttäjätilien määrällä mitattuna Suomen kolmanneksi suurin.
- Lisätietoja:
  - https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2018/varoitus-2018-01.html

#kybersää 04/2018

Palvelunestot

- Ilmoitettujen hyökkäysten määrä oli huhtikuun aikana Suomessa vähäinen.
- Yksi palvelunestohyökkäyksiä myyvä palvelu on poistettu verkosta kansainvälisen poliisioperaation seurauksena.

Haittaohjelmat & haavoittuvuudet

- Haavoittuuden avulla vietiin selväkielisiä salasanoja liiketoimintasuunnitelma.com -sivustolta
- Cisco ASA –tuotteissa oli vakava haavoittuvuus, joka mahdollisti VPN-verkkoon liittymisen virheellisellä asiakasvarmenteella.

Huijaukset & kalastelut

- Veikkauksen käyttäjätietoja kalasteltu puhelimitse
- Kaapattuja O365-sähköpostitilejä käytetään aktiivisesti huijauksiin
- Pankkitunnusten tietojenkalastelu lisääntyi roimasti

Vakoilu

- Amerikkalaisten hakkereiden vastaisku iranilaisia kohteita vastaan.
- Saksa syyttää Venäjää tietomurrosta valtionhallintoon
- Kiinalaisten vakoilijoiden menetelmiä paljastettu

Verkkojen toimivuus

- Hieman tavallista vähemmän merkittäviä häiriöitä.

IoT

- Industrial Internet Consortium julkaisi päivitetyt ohjeet IoT:n tietoturvan hyvistä käytännöistä.
- Microsoft julkaisi Azure Sphere -tuotteen turvallisten IoT-tuotteiden alustaksi.

Huhtikuussa 2018 korostuivat liiketoimintasuunnitelma.com –tietovuoto sekä Office 365 -tietojenkalastelun avulla tehdyt valelaskut.
Kelejä rauhoittivat toimivat viestintäverkot ja IoT:n hyvät käytännöt

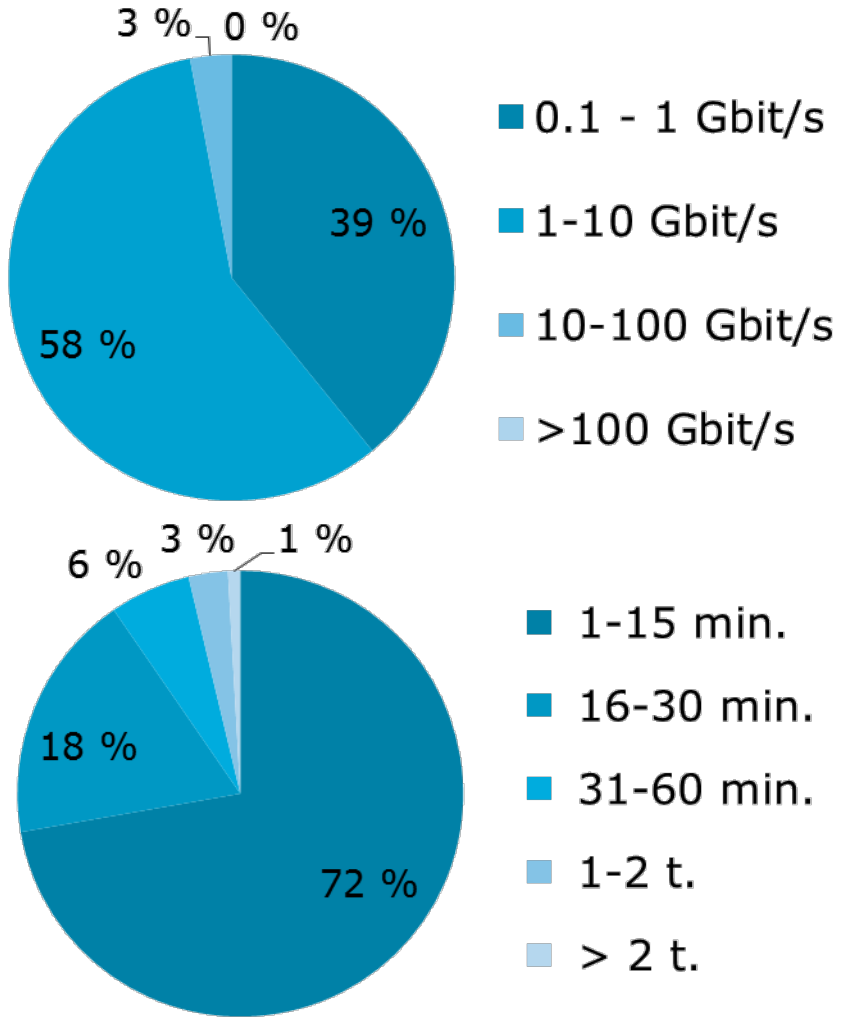
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu

- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (72 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 60 % 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 viimeaikoina 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

- Huhtikuussa Kyberturvallisuuskeskukseen raportoitiin kohtuullisen vähän palvelunestohyökkäyksiä
- Yhden organisaation sähköpostipalvelin palvelunestohyökkäyksen kohteena
  - Hyökkäys toteutettiin lähettämällä runsaasti sähköposteja kohteen sähköpostipalvelimelle.
  - Hyökkäys saatiin torjuttua mainepohjaisella estolistalla.
- Rikollisten pyörittämä webstresser.org-palvelu suljettiin verkosta kansainvälisen poliisioperaation seurauksena. Palvelun avulla on voinut tilata palvelunestohyökkäyksiä.
  - Verkossa on edelleen lukuisia niin sanottuja stresser- ja booter–palveluita, joista voi tilata maksullisen palvelunestohyökkäyksen haluamaansa verkko-osoitteeseen.

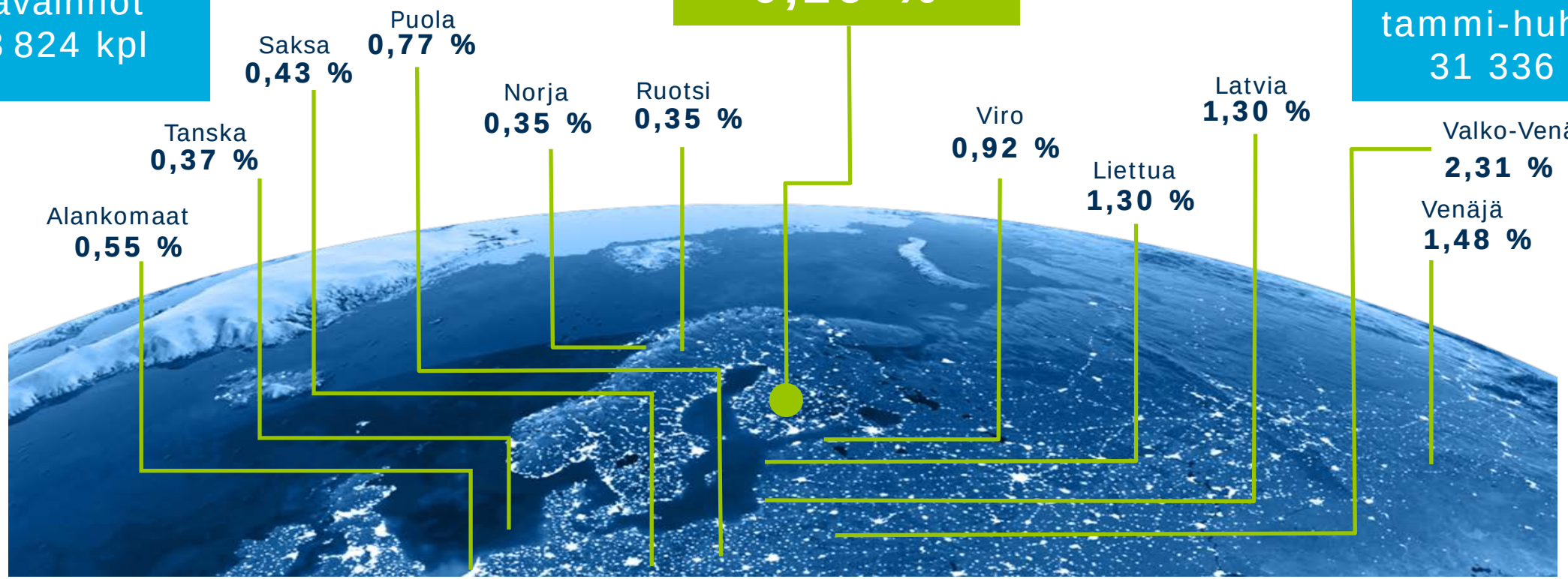
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-huhtikuu
31 336 kpl



Havaintojen määrät vuosina 2016 ja 2017 olivat samankaltaiset.
(*Lähde: Microsoftin SIR-raportti 22 "January-March", julkaistu elokuussa 2017*)

Haittaohjelmat ja haavoittuvuudet

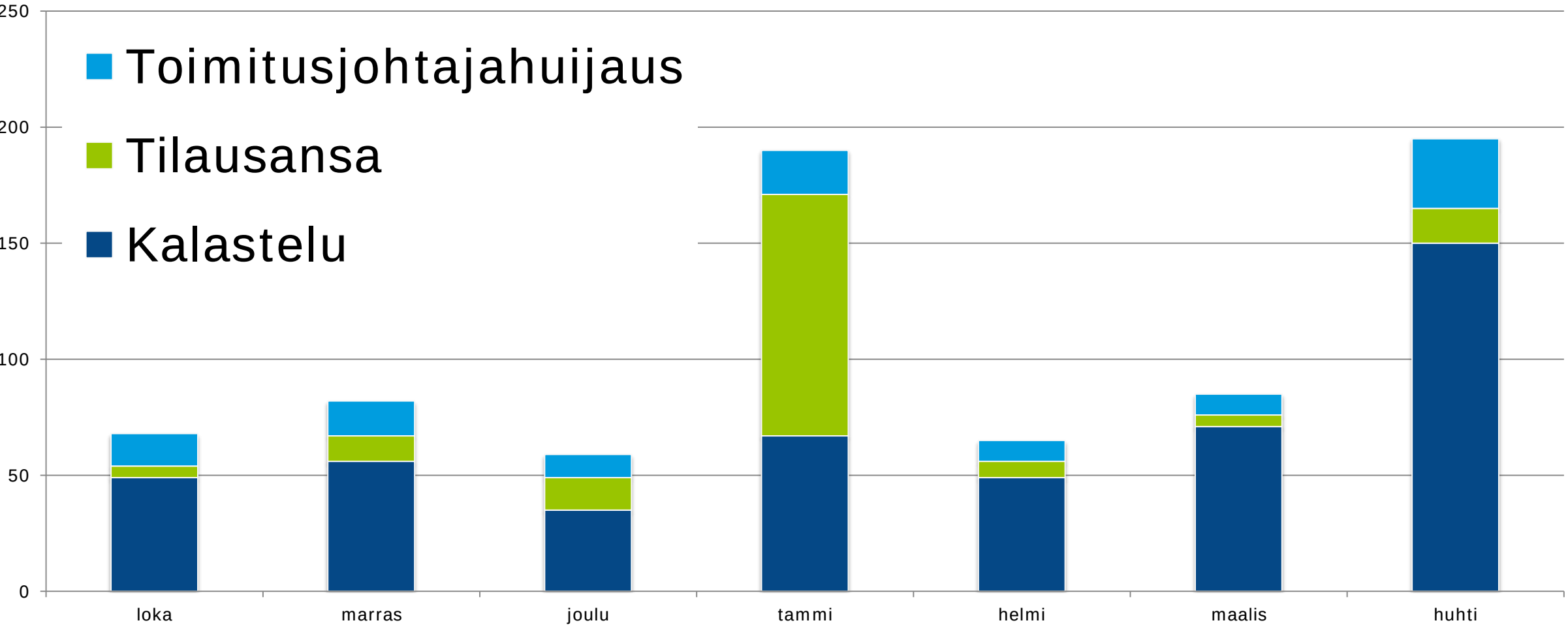
- Meltdown- ja Spectre-haavoittuvuuksien päivitysten laatu on parantunut, mutta uusista haavoittuvuuksista liikkuu jo huhuja
- Cisco ASA –tuotteissa oli haavoittuvuus, joka mahdollisti VPN-verkkoon liittymisen virheellisellä asiakasvarmenteella.
  - Haavoittuvuus on merkittävä, koska VPN-laitteita käytetään suojaamaan verkkoon pääsy vain sallituilta toimijoilta
- Joulukuussa julkaistua tietoturvaohjelmistojen harhautusmenetelmää (Process Doppelgänging) on hyödynnetty kiristyshaittaohjelmassa.
- Ohjelmistokomponenttien hallinta ohjelmistotuotannossa puhuttaa tällä hetkellä asiantuntijoita kansainvälisesti. Tavoitteena on edistää haavoittuvuuksien hallintaa alihankintaketjuissa.
- Rikolliset ovat siirtyneet levittämään virtuaalivaluuttoja louhivia haittaohjelmia kiristyshaittaohjelmien sijaan.

Huijaukset & kalastelut

Huijaukset huhtikuussa

- Asiakastietojen kalastelua puhelimitse Veikkauksen nimissä
  - Puhelimessa soittaja väittää olevansa Veikkauksen asiakaspalvelusta ja kertoo arvontavoitosta. Soitot ovat olleet huijauksia, joilla kalastellaan käyttäjätunnuksia Veikkauksen palveluun.
- Kaapattuja yritysten Office 365 -tunnuksia käytetään tietojenkalasteluun
  - Office 365 -sähköpostitunnuksia salasanoineen kalastellaan rikolliseen käyttöön. Sähköpostitse levitettävät tietojenkalastelusähköpostit saavat lisää uskottavuutta, jos ne on lähetetty aidosta sähköpostilaatikosta.
  - Kaapattuja sähköpostitunnuksia käytetään niin kutsuttuihin nigerialaishuijauksiin, toimitusjohtajahuijauksiin ja monenlaisiin laskutuspetoksiin.
- Tietoja yritetään kalastella tunnettujen pankkien nimissä
  - Huhtikuussa 2018 alkoi uusi laaja pankkiteemainen kalastelukampanja.
  - Myös ulkomaisia palveluita, kuten PayPal, HBO ja NetFlix, käytetään huijauksiin.
- Toimitusjohtajahuijauksia yhdistyksiin ja muihin organisaatioihin
  - Toimitusjohtajahuijauksia ilmoitettiin Viestintävirastoon huhtikuussa 2018 enemmän kuin kertaakaan aiemmin.

Huijausyritykset 2017/10–2018/04



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

"Don't mess with our elections"	Tuntematon ryhmittymä murtautui konesaleihin Iranissa ja jätti kohteisiin tekstin "Don't mess with our elections" sekä Yhdysvaltain lipun.
Saksa syyttää Venäjää	Saksa syyttää Venäjän tiedustelupalveluja murtautumisesta valtionhallinnon verkkoon.
Kiinalaisten vakoilijoiden työkaluja	Julkaistu raportti paljastaa vakoilijoiden menetelmiä.

Havainnointi- ja varoitusjärjestelmän (HAVARO) havainnot

Vuosi 2017

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

Vuosi 2018
(tammi-huhtikuu)

Vakavuus	Lukumäärä
Punainen	242
Keltainen	11665
Vihreä	6673
Yhteensä	**18 580**

Huhtikuussa oli poikkeuksellisen paljon keltaisia havaintoja, minkä syynä muun muassa tietoturvaheikkouksien skannailut ja tunkeutumisyritykset.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

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

Häiriöiden vakavuusluokat A-C perustuvat Viestintäviraston määräykseen 66 teletoiminnan häiriötilanteista.

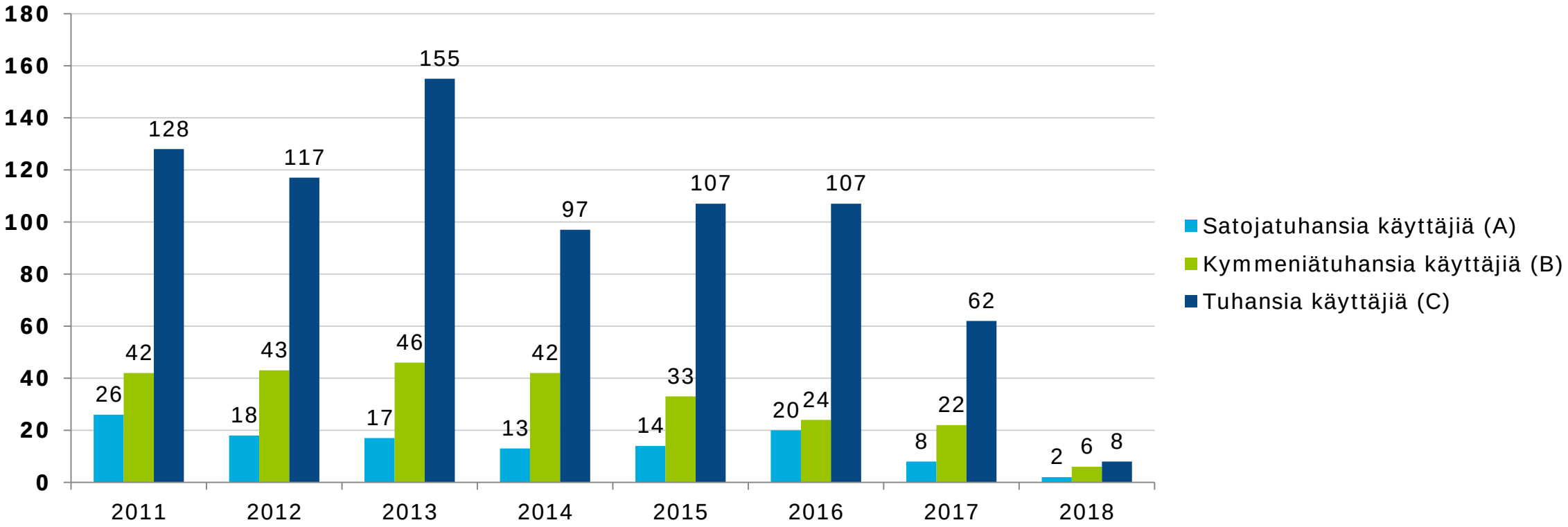
Vuosi 2018
(tammi-huhtikuu)

Vakavuus	Lukumäärä
A-luokka	2
B-luokka	6
C-luokka	8
Kaikki häiriöt	**Ei tiedossa**

Ensimmäisen vuosineljänneksen tilasto kaikista häiriöistä valmistuu toukokuun lopussa.

Teleyrityksiltä saatujen ilmoitusten mukaan alkuvuonna 2018 merkittäviä häiriöitä on esiintynyt tavallista vähemmän.

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 200 000–450 000 vuodessa.

IoT

Esineiden internet (IoT)

- **Industrial Internet Consortiumin (IIC) päivitetty opas kuvailee teollisen internetin IoT- päätelaitteiden tietoturvan hallintaa**
  - Endpoint security best practices
  - Industrial Internet of Things Volume G4: Security Framework
  - https://www.uusiteknologia.fi/2018/04/04/tarkea-opas-teollisuuden-iot-tietoturvaan/
- **Microsoftilta Azure Sphere -tuote turvallisten IoT-tuotteiden alustaksi**
  - Tuote koostuu Microsoftin omasta linux-ytimestä, uudenlaisesta mikropiiristä ja pilvipohjaisesta tietoturvapalvelusta. Tuotteen tavoite on suojata mikrokontrollereihin perustuvia IoT-laitteita tietoturvauhilta.
  - Tällä hetkellä ratkaisujen kehittämiseen tarkoitettu MediaTek MT3620 -piirilevy on ennakkotilattavissa ja toimitusten luvataan alkavan syyskuussa 2018.
  - https://azure.microsoft.com/en-us/blog/introducing-microsoft-azure-sphere-secure-and-power-the-intelligent-edge/
  - https://www.seeedstudio.com/MT3620-Development-Board-for-Azure-Sphere-p-3052.html

Tietoturva-alan lakiasiaa ja kansainvälisiä uutisia

Lakiasiat

- Verkko- ja tietoturvadirektiivin mukainen kansallinen lainsäädäntö voimaan 4.5.2018 ja sovellettavaksi 9.5. alkaen
  - Viestintävirasto ja toimialakohtaiset valvovat viranomaiset valmistelevat toimeenpanoa
  - 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
- Uusi siirtymäaikataulu TUPAS-tunnistuksen muutoksille
  - Tunnistukseen on lisättävä sanomatason salaus
  - Määräysmuutos tämän osalta on loppusuoralla ja päivitetty määräys annettaneen viikolla 19-20
  - 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)

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)
- Mm. rajavartiolain ja ulkomaalaislain muuttamista koskeva hallituksen esitys on valiokuntakäsittelyssä (HE 201/2017, http://intermin.fi/hybridiuhat)
  - Säädettäisiin mm. 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

Yhdysvallat ja Iso-Britannia varoittavat Venäjän käynnistämästä kyberoperaatiosta runkoverkkoja, reitittimiä ja palomuureja vastaan. Kyberhyökkäyksen sanotaan kohdistuvan sekä valtiolliseen että yksityiseen sektoriin tarkoituksena saada virtuaalinen jalansija kaikkeen kriittisessä verkkoinfrastruktuurissa liikkuvaan tiedonsiirtoon.

NATOn Kyberosaamiskeskuksen johtama kansainvälinen kyberturvallisuusharjoitus Locked Shields pidettiin Virossa. Yli 1000 asiantuntijaa 30 valtiosta osallistui harjoitukseen. Myös Suomi ja Ruotsi olivat mukana harjoituksessa.

Useissa maissa esiintyi vakavia verkkoliikenteen häiriöitä Ciscon valmistamien kytkinten haavoittuvuuden hyväksikäytön seurauksena. Hyökkäys lopetti kytkinten normaalin toiminnan ja asetti kytkimen ohjauspaneeliin näkyviin Yhdysvaltain lipun.

Saksan tiedustelupalvelun johtajan mukaan on erittäin todennäköistä, että Saksan parlamenttiin vuonna 2015 sekä Yhdysvaltain demokraattisen puolueen kansallisen komitean järjestelmiin vuonna 2016 tehdyt kyberhyökkäykset ovat venäläistä alkuperää. Venäjän valtio on kiistänyt syytteet.

Viestintävirasto
Kyberturvallisuuskeskus

cert@ficora.fi

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi