#kybersää 06/2018

#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 kevään 2018 aikana varastettu.
- 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.
- Lisätietoja:
  - https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2018/varoitus-2018-03.html

#kybersää 06/2018

Palvelunestot

- Kesäkuussa Kyberturvallisuuskeskukseen on ilmoitettu useista finanssisektoriin kohdistuvista palvelunestohyökkäyksistä.
- Hyökkäysten kokoluokat n. 10–35 Gbit/s.

Haittaohjelmat & haavoittuvuudet

- Gentoo-Linux-jakelun GitHubissa sijaitsevaan lähdekoodiin oli ujutettu haittaohjelma.
- TLBleed-haavoittuvuus Intelin suorittimissa voi mahdollistaa esimerkiksi salausavainten vuotamisen pilvipalveluympäristöissä.

Huijaukset & kalastelut

- Sähköpostitunnuksia kalastellaan ja kaapattuja tilejä käytetään esimerkiksi toimitusjohtaja-huijauksiin ja laskutuspetoksiin.
- Huijauksista koituu merkittäviä tappioita.

Vakoilu

- Suomi osallistuu EU Cyber Rapid Response Force -toimintaan.
- Kyberhyökkäykset Singaporeen lisääntyivät merkittävästi Trump-Kim-tapaamisen aikana.
- Olympic Destroyer löysi uusia kohteita.

Verkkojen toimivuus

- Häiriöitä on ollut vähän edellisiin vuosiin verrattuna.
- Kesäkuiset ukkospuuskat eivät aiheuttaneet merkittäviä toimivuushäiriöitä.

IoT

- Laivojen kyberturvallisuus retuperällä.
- VPNFilter on ilmeisesti vakoilutyökalu.
- BSI julkaisi havainnointisääntöjä TRITON-haittaohjelman liikenteen havaitsemiseksi.
- Kryptolouhijat tarttuvat myös IoT-laitteisiin.

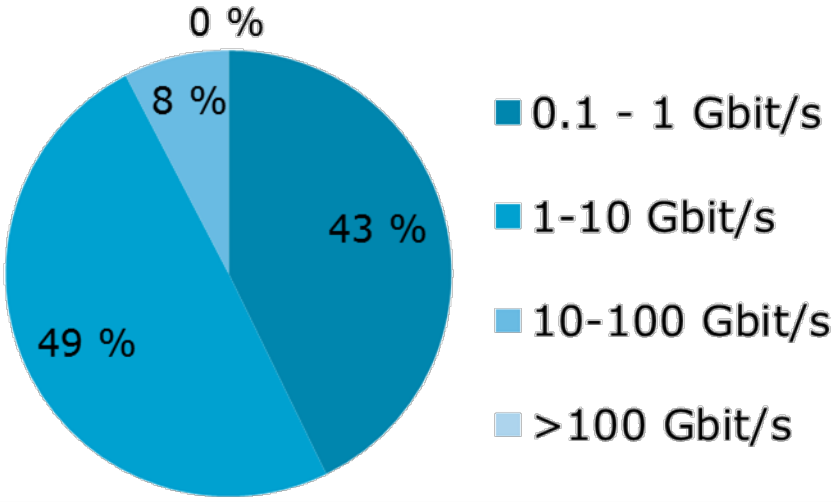
Palvelunestot

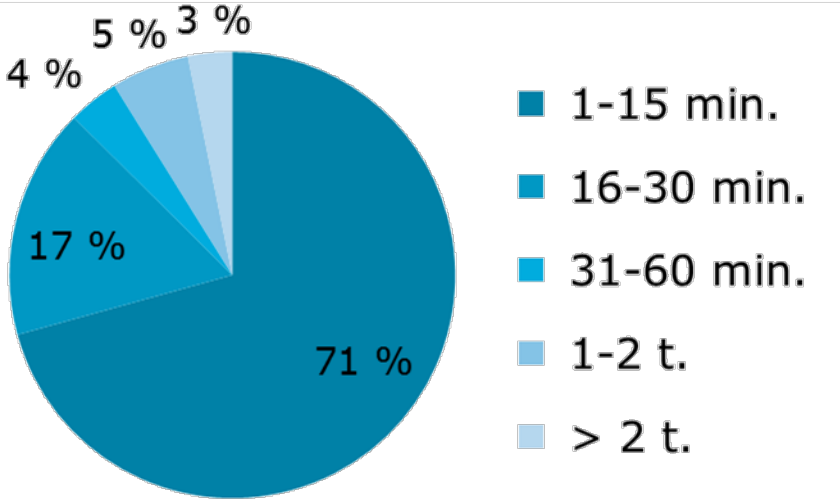
Palvelunestohyökkäykset ja niillä uhkailu:

- 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

- **Kesäkuussa Kyberturvallisuuskeskukseen on ilmoitettu useista finanssisektoriin kohdistuvista palvelunestohyökkäyksistä**
  - Hyökkäysten kokoluokat n. 10–35 Gbit/s ja koostuivat pääasiassa CLDAP- ja SYN FLOOD -tekniikoista.
  - Hyökkäykset onnistuttiin torjumaan, joten niillä ei ollut asiakkaille näkyviä vaikutuksia
- **Keinot suojautua suureen liikennemäärään perustuvilta palvelunestohyökkäyksiltä ovat kehittyneet**
  - Tästä syystä näitä keinoja hyödyntävien organisaatioiden palveluihin ei yleensä enää saada vaikutettua.
  - Rikolliset ovat siirtyneet yhä enemmän kuormittamaan kohteen resursseja, kuten laskentatehoa tai muistia.
  - Tällaisia hyökkäyksiä vastaan voi suojautua erilaisilla palvelimen säännöillä, joilla yksittäisen laitteen tekemiä kyselyitä voidaan rajoittaa.

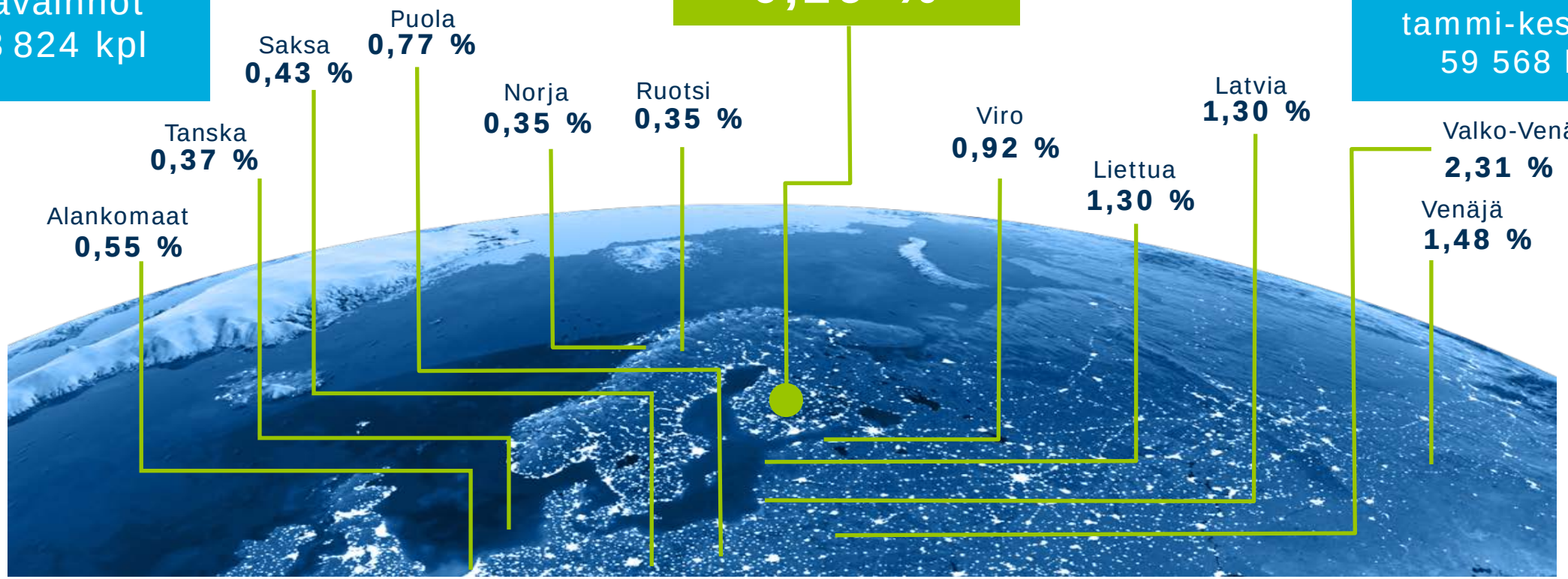
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-kesäkuu
59 568 kpl



Vuoden 2018 alussa tietoturvapoikkeamahavaintojen määrä jatkoi vuoden 2017 lopun maltillista linjaa, mutta kevään aikana havainnot ovat lisääntyneet voimakkaasti.

Haittaohjelmat

- **Gentoo-Linux-jakelun GitHubissa sijaitsevaan lähdekoodiin oli ujutettu haittaohjelma**
  - Git ei ole Gentoon pääasiallinen jakelukanava, joten vaikutukset jäivät pieniksi. Lisäksi haittaohjelma ei toiminut oikein.
  - Tapaus kuitenkin osoittaa jakelukanavan eheyden merkityksen.

- **Necurs-bottiverkko alkoi levittää haittaohjelmia .iqy-päätteisten sähköpostin liitetiedostojen avulla**
  - Liitetiedosto avautuu Excelissä, joka käy lataamassa tiedoston viittaamasta verkko-osoitteesta haitallista sisältöä.

- **Rikolliset ovat siirtyneet levittämään virtuaalivaluuttoja louhivia haittaohjelmia kiristyshaittaohjelmien sijaan**
- **Joulukuussa julkaistua tietoturvaohjelmistojen harhautusmenetelmää (Process Doppelgänging) hyödynnettiin kiristyshaittaohjelmassa**

Haavoittuvuudet

- **TLBleed-haavoittuvuus Intelin suorittimissa**
  - Samassa prosessoriytimessä suoritettavat prosessit voivat saada tietoa toistensa toiminnasta.
  - Tämä voi mahdollistaa esimerkiksi salausavainten vuotamisen pilvipalveluympäristöissä.
- **Zip Slip -haavoittuvuus koskee pakkauskirjastoja**
  - Sallii tiedostojen kirjoittamisen yllättäviin hakemistoihin hyökkääjän laatimaa tiedostopakettia purettaessa.
  - Haavoittuvuutta ei ole havaittu itsenäisissä tiedostonpakkausohjelmistoista, kuten WinZip tai gzip.
- **Cisco ASA**
  - Cisco ASA -palomuuri- ja VPN-tuotteen verkkopalvelimessa haavoittuvuus, jonka avulla sen saa palvelunestotilaan.
  - Tällöin käyttäjät eivät esimerkiksi voi muodostaa VPN-yhteyksiä tai liikennöidä palomuurin kautta.

Tietomurrot ja tietovuodot

- **Suomalaisyritysten Office 365 -tileille on murtauduttu useita kertoja**
  - » Johdon sähköpostitileille on asetettu postin uudelleen-lähetys rikollisten sähköpostiosoitteeseen.

- **Ticketmasterin käyttämän kolmannen osapuolen sovellustoimittajan asiakastukijärjestelmästä löydettiin haitallista ohjelmakoodia**
  - » Tietomurto on koskettanut alle viittä prosenttia (5%) maailmanlaajuisesta asiakastietokannasta
- **Adidaksen Yhdysvaltain verkkokauppa tietomurron kohteena**

Huijaukset & kalastelut

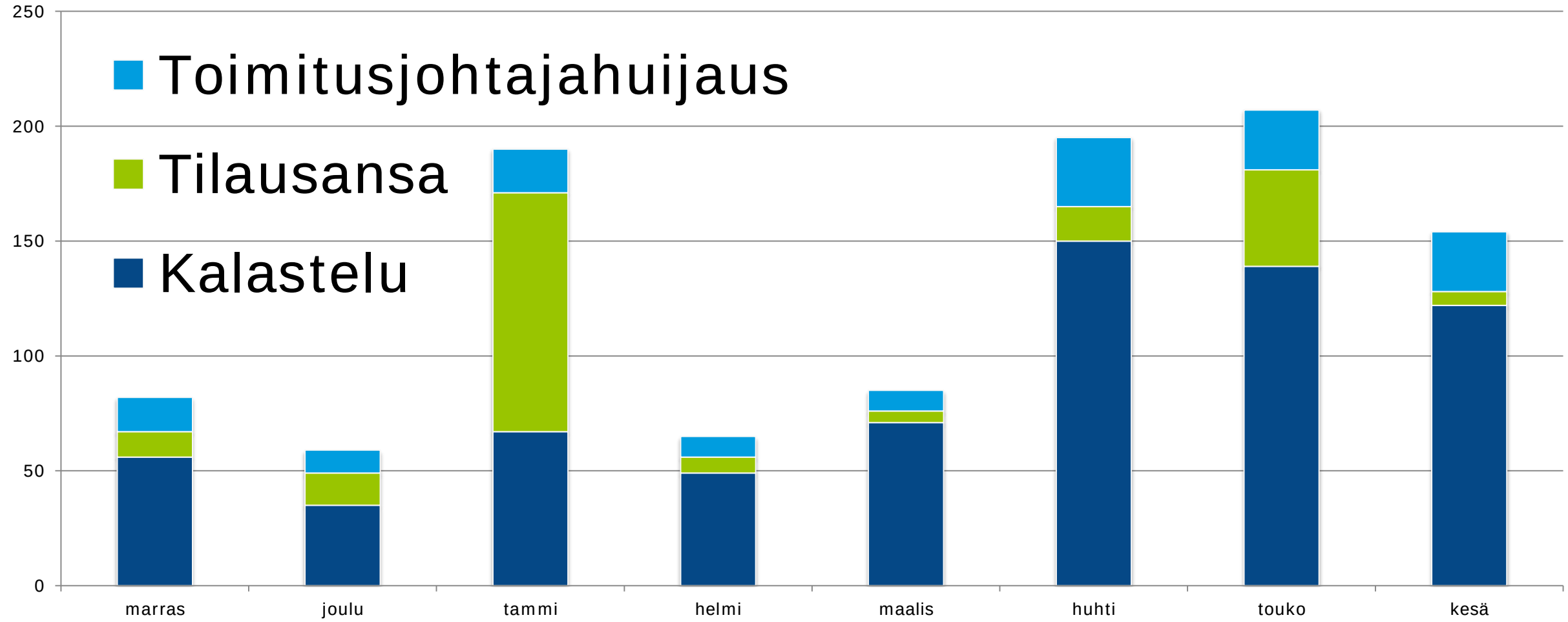
Huijaukset kesäkuussa

- **Office 365 -tunnusten kalastelusta kriittinen varoitus**
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Tilien sähköpostit edelleenlähetetään rikollisille, jotka voivat hyödyntää niitä mm. toimitusjohtajahuijauksiin ja teollisuusvakoiluun.
  - Petoksilla ja muilla rikoksilla tavoitellaan merkittävää rikoshyötyä.

- **Sähköpostihuijaukset ovat lisääntyneet**
  - Sekä yrityksiä että yksityisiä henkilöitä yritetään huijata monenlaisilla verukkeilla: lottovoitot, rahanpalautukset, yllättävät perinnöt, houkuttelevat työpaikat.
  - Virtuaalivaluutat ovat suosittuja verukkeita huijauksiin.
  - Myös katteettomat uhkailut ja perusteettomat kiristykset ovat tavallisia tapoja huijata rahaa.

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

Huijausyritykset 2017/11–2018/06



Vakoilu

Verkkovakoilussa ajankohtaista

EU Cyber Rapid Response Force	Suomi osallistuu Liettuan johtamaan EU Cyber Rapid Response Force -ryhmään, jonka tehtävä on avustaa jäsenvaltioita kyberloukkausten selvittelyssä.
Kyber-hyökkäyksiä Trump-Kim tapaamisen aikana	Trump-Kim-tapaamisen aikana kyberhyökkäykset Singaporeen lisääntyivät huomattavasti.
Olympic Destroyer löysi uusia kohteita	Talviolympialaisiin hyökännyt Olympic Destroyer -ryhmä on ottanut kohteekseen uusia tahoja Euroopassa ja Ukrainassa.

Havainnointi- ja varoitusjärjestelmän (HAVARO) havainnot

Vuosi 2017

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

Vuosi 2018
(tammi-kesäkuu)

Vakavuus	Lukumäärä
Punainen	258
Keltainen	12 148
Vihreä	8 664
Yhteensä	**21 070**

Tietoturvaheikkouksien skannailu ja tunkeutumisyritykset kasvattivat huhtikuun keltaisten havaintojen määrää poikkeuksellisen paljon. Kesäkuussa keltaiset havainnot ovat vähentyneet.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

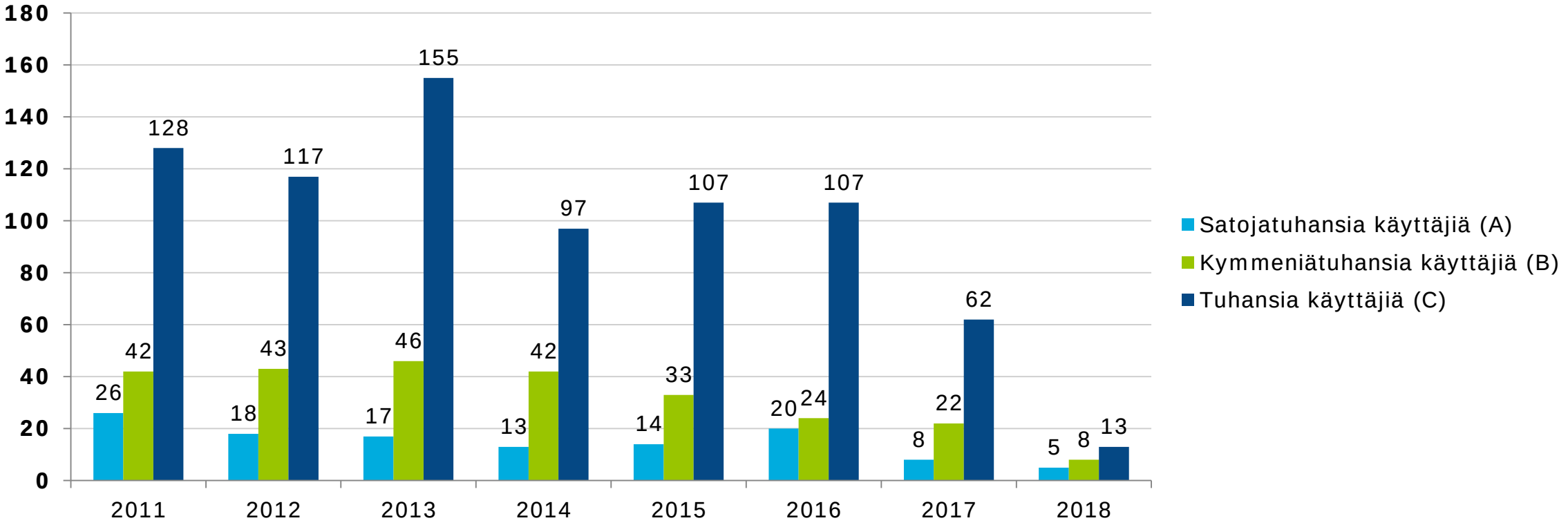
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018
(tammi-kesäkuu)

Vakavuus	Lukumäärä
A-luokka	5
B-luokka	8
C-luokka	13
Kaikki häiriöt (1Q)	**96 732**

Alkuvuonna on ollut poikkeuksellisen vähän merkittäviä häiriöitä. Kesäkuiset ukkospuuskat eivät aiheuttaneet merkittäviä häiriöitä viestintäpalveluille.

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)

- Laivojen kyberturvallisuus
  - » Tietoturvayhtiö Pen Test Partners on tutkinut laivojen navigointi- ja automaatiojärjestelmien haavoittuvuuksia.
  - » Laivojen navigointia voidaan häiritä ja laivoja ohjata luvatta.
  - » Tunnetut tietoturvakäytännöt suojaavat: segmentoi verkot, käytä vahvoja salasanoja, päivitä ohjelmistot.
- VPNFilter
  - » Haittaohjelmasta paljastui lisää hyökkäysominaisuuksia.
  - » Haittaohjelma ei vaikuta tavallisten rikollisten tekemältä vaan vakoilu- ja sabotaasityökalulta.
- Triconex ja TriStation
  - » Saksan BSI julkaisi havainnointisääntöjä väärinkäytösten havaitsemiseksi.
- Virtuaalivaluuttojen louhinta
  - » Myös IoT-laitteisiin tarttuvia louhintahaittaohjelmia on alkanut ilmestyä.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- **Verkko- ja tietoturvadirektiivin mukainen lainsäädäntö 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 mm. 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
- **Työryhmän ehdotus (SM009:00/2018) poliisilain 2 luvun muuttamisesta on lausuttavana 17.8.2018 saakka**
  - 2 lukuun lisättäisiin säännökset, joiden perusteella poliisilla olisi nykyistä kattavampi toimivalta puuttua lennokkien ja miehittämättömien ilma-alusten kulkuun.

Kyberuutisointia maailmalta

Saksa on linjannut, että kyberhyökkäyksiin voidaan jatkossa vastata sotilaallisesti joko kyberpuolustuksen tai tavanomaisin sotilaallisin keinoin. Päätöstä perustellaan sillä, että NATO on linjannut kyberulottuvuuden yhdeksi sotilaalliseksi toimintaympäristöksi maa-, meri- ja ilmatoimintaympäristön lisäksi.

Euroopan komissio kehottaa jäsenmaita aktiivisemmin nimeämään kyberhyökkäysten taustalla olevat tahot. Kehotuksen taustalla on halu nostaa kynnystä kyberhyökkäyksiin.

Yhdeksän EU-maata aikoo perustaa nopean toiminnan kyberjoukot. Liettua kertoi kesäkuussa, että mukaan yhteishankkeeseen ovat lähdössä Liettua, Kroatia, Viro, Alankomaat, Romania, Suomi, Ranska, Puola ja Espanja.

Ticketmasterin käyttämästä tietojärjestelmästä löydettiin haittaohjelma, joka on voinut johtaa asiakkaiden henkilö- ja maksutietojen vuotamiseen. Yhtiö kehotti asiakkaitaan vaihtamaan salasanansa ja tarkkailemaan tilitapahtumiaan.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi