#kybersää 09/2018

#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 ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä on kuluvan vuoden aikana varastettu, ja kriittinen varoitus aiheesta on edelleen voimassa. Varoitus laskettiin hetkellisesti vakavaksi (keltainen), mutta nostettiin syyskuussa takaisin kriittiseksi (punainen).
- Käyttäjätunnuksia ja salasanoja on kalasteltu sähköpostitse ja huijaussivujen avulla. Kyberturvallisuuskeskukselle on tehty ilmoituksia myös monivaiheisen tunnistautumisen (MFA) ohittamisesta. Syyskuussa yleistyivät myös turvapostilta näyttävät kalasteluviestit.
- Kalastelluilla tunnuksilla on kirjauduttu Office 365 -tileille ja pyritty seuraamaan yritysten sähköpostiliikennettä, saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia.
- Kyberturvallisuuskeskus antoi asiasta varoituksen 11.6.2018. Lisätietoja: https://www.viestintavirasto.fi/2018/varoitus-2018-03

#kybersää 09/2018

Palvelunestot

- Palvelunestohyökkäys häiritsi jälleen suomi.fi -verkkopalvelun toimintaa.
- Suomalaiseen yritykseen kohdistui erittäin suuri, n. 90 Gbit/s -volyymin hyökkäys.

Haittaohjelmat & haavoittuvuudet

- Kotireitittimien haittaohjelmahavainnot nousussa myös Suomessa.
- Magecart-hyökkäyksellä on varastettu asiakas- ja luottokorttitietoja useista verkkokaupoista.

Huijaukset & kalastelut

- Office-sähköpostitunnuksia kalastellaan nyt myös väärennetyillä turvaposti-ilmoituksilla.
- OmaVero-teemalla kalasteltiin maksukorttitietoja.

Vakoilu

- USA nimesi pohjoiskorealaisen hakkerin.
- Saksan turvallisuuspalvelu huolissaan kyberpommeista.
- FireEye varoittaa Iranin kyberhyökkäyksistä.

Verkkojen toimivuus

- Vakavimman luokan häiriöitä ollut enemmän kuin viime vuonna. Häiriöt ovat kuitenkin olleet lyhyitä.
- Muita häiriöitä suhteellisen vähän.

IoT

- OWASP top 10 -lista IoT-haavoittuvuuksista auttaa valmistajia välttämään virheitä.
- IoT-haittaohjelmat leviävät myös muille alustoille.
- Satori-bottiverkon tekijäksi epäilty pidätettiin.

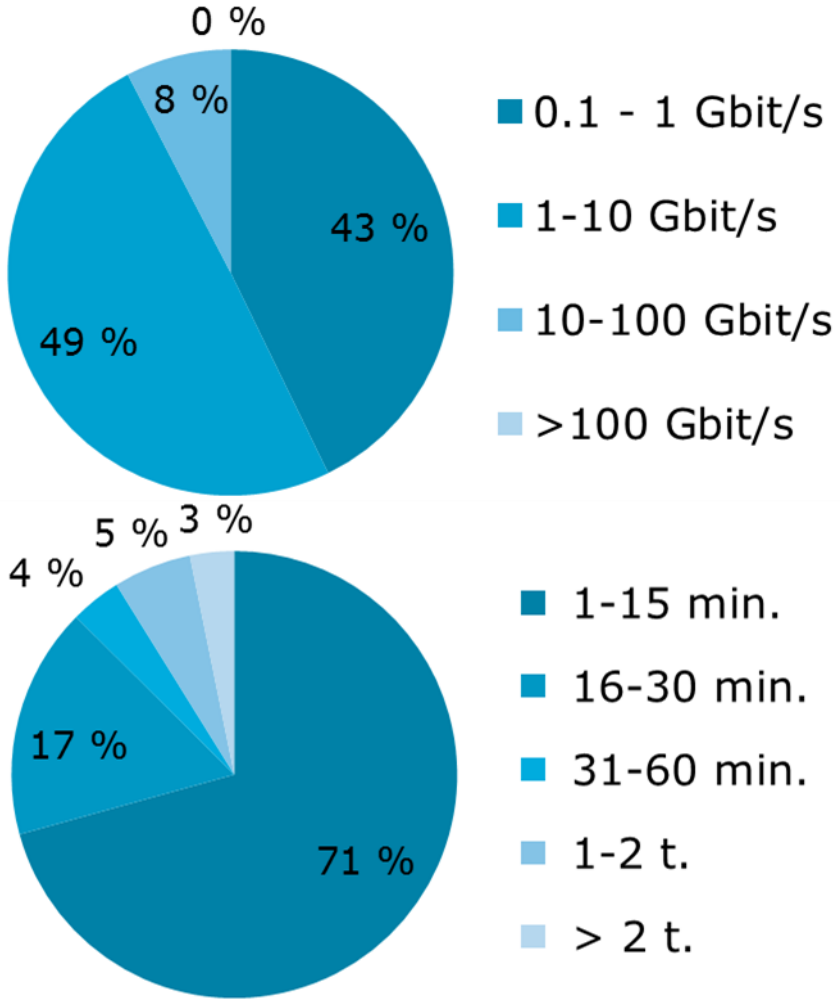
Palvelunestot

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/Q3:	**2018/Q2:**	**2018/Q1**
n. 89 Gbit/s (kesto 30 min)	n. 37 Gbit/s (kesto 8 min)	n. 35 Gbit/s (kesto 7 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2018/Q2. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu

- Suomi.fi-verkkopalvelua vastaan tehtiin syyskuussa palvelunestohyökkäys, joka aiheutti katkoksia ja hitautta palvelun toiminnassa.
  - Hyökkäys vaikutti myös sivustoihin, jotka hyödyntävät suomi.fi-tunnistautumista. Esimerkiksi Poliisin ja Verohallinnon palveluihin kirjautumisessa oli ongelmia hyökkäyksen aikana.
  - Edellisen kerran palvelunestohyökkäykset häiritsivät suomi.fi-palvelun toimintaa elokuussa.
  - Samaan aikaan päällä ollut Elisan puhelinvaihdepalvelun vika ei liittynyt suomi.fi- tai muuhun palvelunestohyökkäykseen.
- Erittäin suuri palvelunestohyökkäys suomalaista yritystä vastaan.
  - Hyökkäyksen tekniikkana oli mm. DNS- sekä memcached-amplifikaatio.
  - Maksimissaan voimakkuus oli 89 Gbit/s ja 8 Mpps.
- Palvelunestohyökkäyksiä on siirrytty tekemään enenevässä määrin ns. HTTP FLOOD -tekniikalla, jossa WWW-palvelinta kuormitetaan suurella määrällä HTTP-kyselyitä.
  - Torjuminen on perinteisiä hyökkäystekniikoita haastavampaa, sillä HTTP FLOOD -kyselyt näyttävät normaalilta selainliikenteeltä. HTTP FLOOD -hyökkäyksellä voidaan myös kuormittaa palvelinta tavanomaista hyökkäystä tehokkaammin.
  - Silti myös perinteiset amplifikaatiohyökkäykset ovat yhä yleisiä. Viime aikoina on näkynyt erityisen paljon memcached- ja DNS-amplifikaatiotekniikoilla toteutettuja hyökkäyksiä.

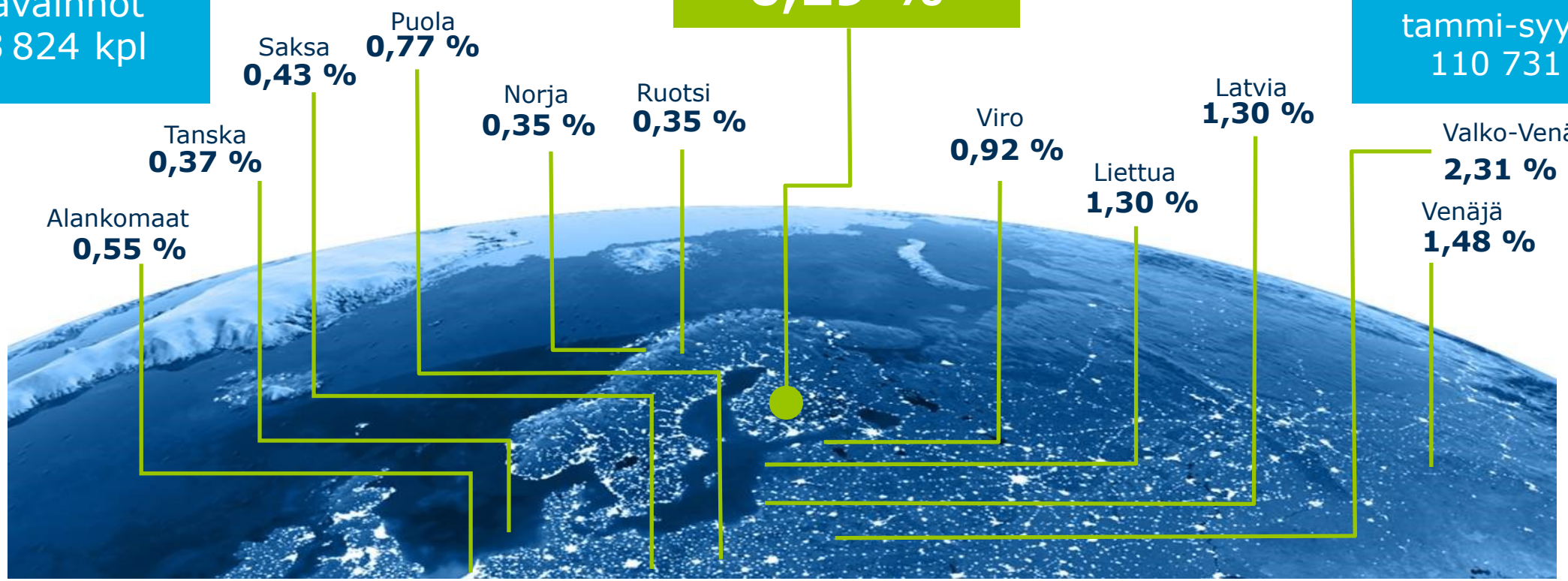
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-syyskuu
110 731 kpl



Vuoden 2018 toukokuusta alkaen tietoturvapoikkeamahavaintojen määrä on kasvanut pienreitittimien haittaohjelmatartuntojen vuoksi

Haittaohjelmat

- Kotireitittimien haittaohjelmahavainnot ovat nousussa Suomessa.
  - Suomalaisia kotireitittimiä on toukokuusta 2018 alkaen saastunut haittaohjelmalla, joka on tarttunut luultavasti jonkin haavoittuvuuden tai väärän konfiguraation seurauksena.
  - Saastunut kotireititin yrittää levitä eteenpäin liikennöimällä portteihin, jotka ovat tyypillisiä Mirai-sukuisilla haittaohjelmilla.
- Magento-verkkokauppa-alustoja on murrettu, ja ne on laitettu varastamaan asiakas- ja luottokorttitietoja.
  - Tässä nk. Magecart-hyökkäyksessä verkkokauppaan asetetaan haitallinen ohjelmakoodi, joka oston yhteydessä siirtää asiakas- ja maksukorttitiedot kaupan lisäksi myös verkkorikollisille.
  - Erään tietoturvatutkijan mukaan n. 7000 Magento-alustaa käyttävää verkkokauppaa on murrettu viimeisen 6 kk aikana. Julkisuuteen ovat tulleet mm. Ticketmaster, British Airways ja Newegg.

Haavoittuvuudet

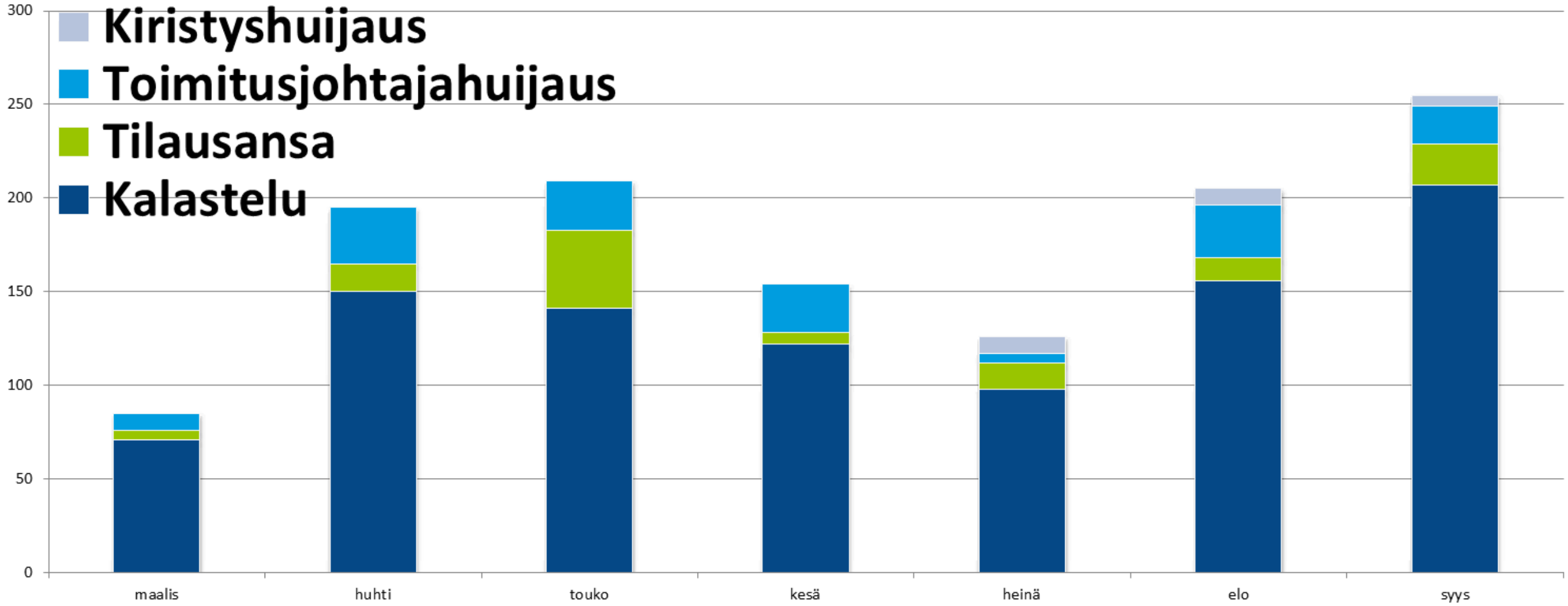
- Linuxista ja FreeBSD:stä viime kuussa paljastunut TCP- ja IP-pakettien pilkkomiseen liittyvä haavoittuvuus koskee myös Windows-käyttöjärjestelmää.
  - » Haavoittuvuuden avulla hyökkääjä voi toteuttaa palvelunestohyökkäyksen haavoittuvaan laitteeseen.
  - » Haavoittuvuus koskee myös useiden verkkolaitevalmistajien tuotteita.
  - » Toistaiseksi ei ole näyttöä haavoittuvuuden hyväksikäytöstä palvelunestohyökkäyksissä.

Huijaukset & kalastelut

Huijaukset syyskuussa

- Office 365 -tunnusten kalastelu sai uusia muotoja turvapostissa.
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Kalasteluun käytetään myös organisaatioiden omia turvapostiviestejä sekä sellaiseksi naamioituja väärennettyjä turvaposti-ilmoituksia.
  - Sähköposteja vakoillaan ja niistä saatuja tietoja käytetään huijauksiin ja vakoiluun.
- Verottajan nimissä kalasteltiin maksukorttitietoja.
  - OmaVero-nimelle väärennetyt huijausviestit houkuttelivat kansalaisia veronpalautuksilla.
- Kiristyskampanja säikäyttää paljastuneella salasanalla.
  - Heinäkuussa alkanut kiristyshuijaus jatkui läpi koko elo- ja syyskuun. Kiristysviestissä väitetään, että uhrin tietokone on saatu haltuun ja kameralla on kuvattu käyntejä aikuisviihdesivustolla. Väitteet ovat huijausta.
  - Huijauksen uskottavuutta on lisätty liittämällä viestiin uhrin vanha salasana. Salasana on oikea, mutta se on peräisin jostain vuosia vanhasta tietovuodosta eikä liity kiristyskampanjaan, aikuisviihteeseen tai työaseman käyttäjätunnuksiin.
  - Lokakuussa alkoi uusi kiristyskampanja konekäännetyllä suomella samasta aiheesta, mutta näihin viesteihin ei oltu liitetty vuotaneita salasanoja.
- Tietoja yritetään kalastella tunnettujen pankkien ja tuotemerkkien nimissä.
  - Apple ID -tunnusten kalastelu lisääntyi elo-syyskuussa. Myös pankkien ja Netflixin nimissä kalasteltiin maksukorttitietoja.
  - Tilausansoihin houkuteltiin kuluttajia paljon mm. Prisman, Gigantin, Finnkinon ja Shellin tuotenimillä.

Käsiteltyjä huijaustapauksia 2018/03–09



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

USA nimesi Lazarus-ryhmän hakkerin	Yhdysvallat syyttää pohjoiskorealaista miestä osallisuudesta Lazarus-ryhmän tekemiin tietomurtoihin.
Saksan turvallisuus-palvelu on huolissaan "kyberpommeista"	Saksan turvallisuustiedustelupalvelun (BfV) johtaja on huolissaan kriittisen infrastruktuurin tietojärjestelmiin piilotetuista "kyberpommeista".
FireEye varoittaa Iranin kyberhyökkäyksistä	Tietoturvayhtiö FireEye pitää mahdollisena, että Iranin tekemät tietomurrot liittyvät sabotaasien valmisteluun.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

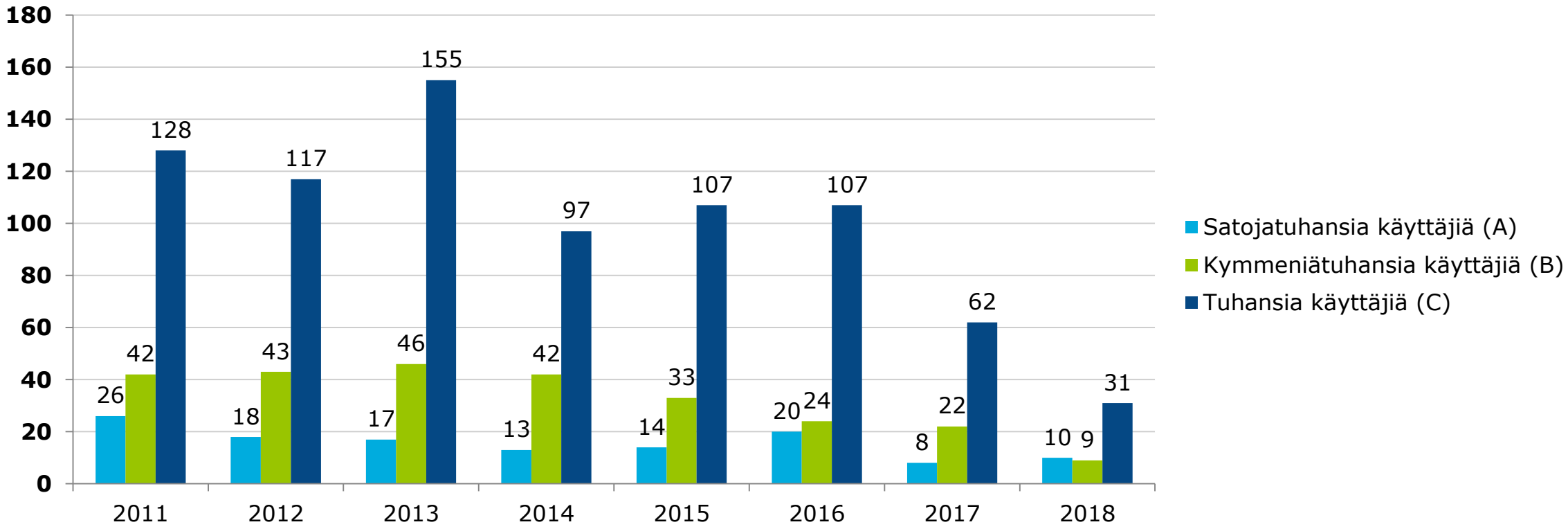
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018
(tammi-syyskuu)

Vakavuus	Lukumäärä
A-luokka	10
B-luokka	9
C-luokka	31
Kaikki häiriöt (Q1–Q2)	**208 026**

Alkuvuonna on ollut poikkeuksellisen vähän merkittäviä häiriöitä. Vakavimpia A-luokan häiriöitä on ollut kesän aikana paljon, mutta se vaikuttaa sattumalta.

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), syyskuun yhteenveto

- OWASP-yhteisön top 10 -lista IoT-tuotteiden haavoittuvuuksista.
  - » Listan luonnos on julkisesti kommentoitavana.
  - » OWASP:n listat haavoittuvuuksista ja niiden korjauskeinoista ovat hyvin suosittuja ja käytännönläheisiä.
  - » Lista auttaa IoT-tuotteiden tekijöitä välttämään tyypillisiä virheitä.
- IoT-haittaohjelmat leviävät muihinkin kuin IoT-laitteisiin.
  - » Hide and Seek -bottiverkko saastuttaa myös Android-laitteita.
  - » Mirai- ja Gafgyt-haittaohjelmiin on ilmestynyt ominaisuuksia, joilla ne voivat tarttua tiettyihin yritysten suosimiin palvelinohjelmistoihin.
  - » Bottiverkkoja käytetään erityisesti palvelunestohyökkäyksiin.
- Yhdysvalloissa poliisi on pidättänyt Satori-bottiverkon tekijäksi epäillyn miehen.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- EU:n televiestintäuudistus (*EECC*)
  - Sisällöstä sovittu, käynnissä tekstien hiominen ja edessä virallinen hyväksyntä sekä julkaisu EU:n virallisessa lehdessä, minkä tapahtunee vuoden lopulla → 2 v. täytäntöönpanoaika.
- Valiokuntakäsittelyssä:
  - Tiedustelulakipakettia koskevat esitykset (HE 198/2017, 199/2017, 202/2017 ja 203/2017).
    - Eduskunta hyväksyi 3.10.2018 ehdotuksen perustuslain 10 §:n muuttamisesta kiireellisenä sekä itse ehdotuksen.
  - EU:n yleistä tietosuoja-asetusta täydentävää lainsäädäntöä koskeva esitys (HE 9/2018).
  - Esitys laiksi Liikenne- ja viestintäviraston perustamisesta ym. (HE 61/2018).
    - Ehdotusta täydentävä esitys (HE 104/2018) on annettu eduskunnalle.
  - Esitykset rajavartiolain ja ulkomaalaislain muuttamisesta (HE 201/2017) sekä puolustusvoimista annetun lain muuttamisesta (HE 72/2018) .
    - Valtuudet puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin.
  - Valtioneuvoston kirjelmä (U 33/2018 vp) eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston asetukseksi ja direktiiviksi koskien lainvalvontaviranomaisten rajat ylittävää pääsyä sähköiseen todistusaineistoon rikosasioissa ("e-Evidence").

Kyberasioihin liittyvää uutisointia maailmalta

Vaalien turvallisuus puhuttaa monissa maissa. Tanska julkaisi suunnitelman kyberuhkien torjumiseksi vaalien alla ja peruutti sähköisen äänestämisen käyttämisen vaikuttamisriskeihin vedoten. Myös Indonesian viranomaiset varoittavat 2019 vaaleihin kohdistuvista mahdollisista kyberuhkista. Ruotsin SÄPO raportoi valtionhallintoon ja poliittisiin organisaatioihin kohdistuneista hyökkäyksistä.

Europolin mukaan valtiollisten toimijoiden tekemät kyberhyökkäykset ovat kasvussa. Europolin mukaan on entistä vaikeampaa sanoa onko tekijä rikollisryhmittymä, valtiollinen toimija vai amatööri. Tekijät suosivat yhä vähemmän satunnaisia hyökkäyksiä ja keskittyvät kohdennetumpiin hyökkäyksiin, jolloin mahdollinen hyöty on suurempi.

Saksalaiset energiayhtiöt varautuvat kyberhyökkäykseen maan viranomaisten antaman varoituksen jälkeen. Saksan tietoturvavirasto BSI varoitti kesällä siitä, että Euroopan energiaverkkojen pimentäminen on varteenotettava uhkakuva. Virasto varoitti kaikkia energiayhtiöitä ja kertoi jo nyt näkyvästä palomuurien kokeilusta.

Virossa kutsuttiin maan poliitikot kyberturvallisuuskoulutukseen. Kutsut liittyvät Viron Riigikogun ja Euroopan parlamentin vaaleihin 2019.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi