#kybersää lokakuu 2017

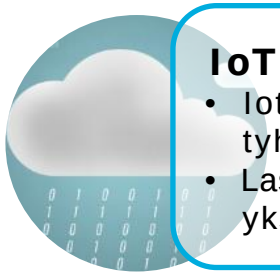
#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tarkoituksena on antaa lukijalle nopea kokonaiskuva siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

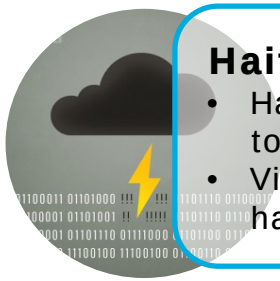
vakava

#kybersää 10/2017



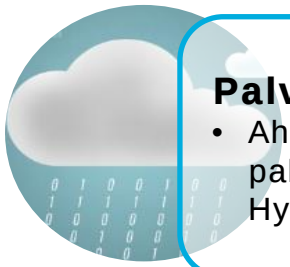
IoT

- Iot-laitteista koostuva Reaper-bottiverkko nousi tyhjästä, levisi nopeasti ja katosi äkillisesti.
- Lasten älyrannekellojen tietoturvassa ja yksityisyyden suojassa vakavia puutteita.



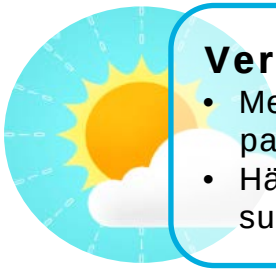
Haittaohjelmat & haavoittuvuudet

- Haittaohjelmien levitys Microsoft Officen DDE-toimintoa hyödyntämällä on yleistynyt.
- Viro uusi 750 000 henkilökorttia niistä löytyneen haavoittuvuuden vuoksi.



Palvelunestot

- Ahvenanmaalle kohdistuneet palvelunestohyökkäykset jatkuivat lokakuussa. Hyökkäykset häiritsivät palveluiden toimintaa.



Verkkojen toimivuus

- Merkittävä häiriö Lahden alueen TV-lähetyksissä parhaaseen katseluaikaan.
- Häiriöt yhä melko pieniä ja niitä esiintyy suhteellisen vähän.

Huijaukset & kalastelut

- Pankkitunnusten kalastelu jatkuu.
- Toimitusjohtajahuijaukset erittäin yleisiä.
- Kalasteltuja Office 365 -tunnuksia käytetään useissa erilaisissa huijauksissa.

Vakoilu

- APT28:n viimeisimmät spearphishing-kampanjat on havaittu lokakuussa.
- Bad Rabbit –haittaohjelmalla epäillään olevan kytköksiä valtiollisiin toimijoihin.

Lokakuu 2017 on ollut pilvinen

IoT-laitteista koostunut Reaper-bottiverkko toi taas esiin älylaitteiden tietoturvahaasteet. Päivittäminen ei ole yksinkertaista tai aina edes mahdollista kuluttajalle. Haavoittuvia IoT-laitteita on helppo hyödyntää mm. palvelunestohyökkäyksissä.

Salausjärjestelmien perusteellinen auditointi on tärkeää. Tämän osoitti Viron sähköisiin henkilökortteihin vaikuttanut haavoittuvuus.

Ajankohtaista

Kyberturvallisuusuutisointia maailmalta

- DDoS-hyökkäyksissä käytettyjen "stresser"-palvelujen määrä on kasvanut selvästi
- Google tarjoaa korkeariskisille asiakkailleen tehostettuja käyttäjätilin suojauspalveluja

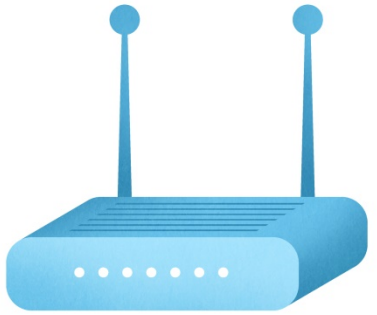
Lakiasioita

- NIS-direktiivin täytäntöönpanon valmistelu jatkuu kotimaassa ja EU:ssa
  - » HE laeiksi Euroopan Unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta (LVM/1616/03/2016) oli kuulemisella 20.10.2017 asti
  - » EU:n komissio valmistelee täytäntöönpanoasetusta digitaalisten palveluiden tietoturva- ja ilmoitusvaatimuksista
  - » Jäsenvaltioiden yhteistyötä kehitetään muun muassa CSIRT-verkostossa
- Tunnistus- ja luottamuspalvelulain (617/2009) vahvan sähköisen tunnistuspalvelun tarjoajia koskeva luottamusverkostosääntely tuli voimaan 1.5.2017
  - » Viestintävirasto on 5.10.2017 julkaissut 4 tulkintamuistiota tunnistuslain soveltamisesta.
  - » Tunnistuslakiin ehdotetut muutokset tulevat todennäköisesti voimaan vielä kuluvan vuoden aikana.
    - Ensitunnistamisen ketjuttamiselle enimmäishinnan asettaminen ja käytettävä menetelmä enimmäishinnan asettamiseksi.
    - Korjaus valvontamaksusäännökseen.

IoT

Esineiden internet (IoT) lokakuun yhteenveto

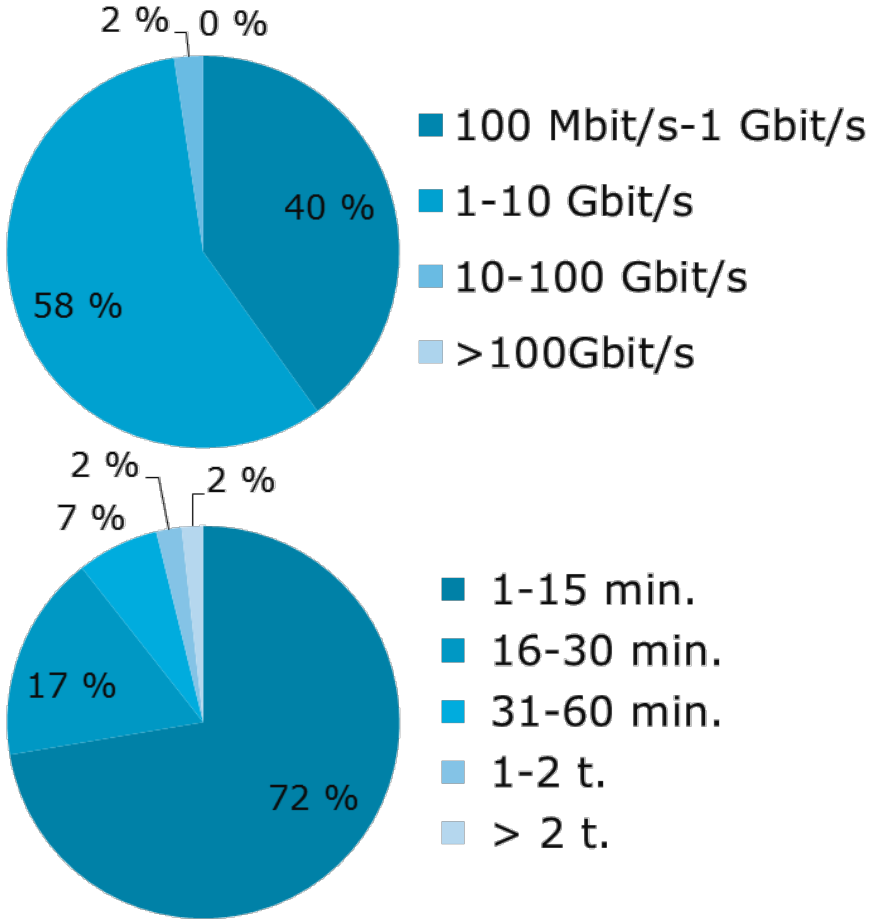
- Reaper/IoT_reaper/IoTroop-haittaohjelma ja -bottiverkko ilmestyi ja kasvoi nopeasti
  - » Havaittiin maailmalla ensimmäisen kerran lokakuussa 2017
  - » Leviää kuin Mirai: saastunut laite etsii lisää haavoittuvia laitteita. Hyödyntää leviämisessä ohjelmistohaavoittuvuuksia, ei tunnettuja salasanoja kuten Mirai.
  - » Ei havaintoja merkittävästä bottiverkon käytöstä tai havaintoja tartunnoista Suomessa.
  - » Bottiverkko katosi äkillisesti marraskuun alussa.
- Lasten älyrannekelloissa vakavia tietoturva- ja tietosuojariskejä
  - » Norjan kuluttajalautakunta tutki useita lapsille tarkoitettuja älykelloja. Kaikissa tutkituissa laitteissa oli selviä puutteita.
  - » Samoja tai samanlaisia laitteita myydään Suomessakin.



Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu

- Ahvenanmaa sai kokea palvelunestohyökkäyssarjan, joka oli volyymiltään ja kestoltaan merkittävä.
  - Hyökkäykset muun muassa hidastivat tai estivät useiden palveluiden toiminnan.
- Palvelunestohyökkäyksiä tehtailtu jälleen myös useisiin julkishallinnon kohteisiin. Aiheuttivat kuitenkin vain pieniä häiriöitä.
- Lizard Squadin väitetään kiristäneen palvelunestohyökkäyksillä Euroopassa.
  - Kiristyksen yhteydessä on tehty lyhyitä palvelunestohyökkäyksiä, volyymiltään n. 5 Gbit/s.
- Viimeaikojen suurimpia Suomessa havaittuja palvelunestohyökkäyksiä:
  - 2017/Q4: n. 57 Gbit/s (kesto alle 10 min)
    - Hyökkäys jatkui 20 Gbit/s volyymillä n. 2 tuntia
  - 2016: n. 280 Gbit/s (kesto 42 min)



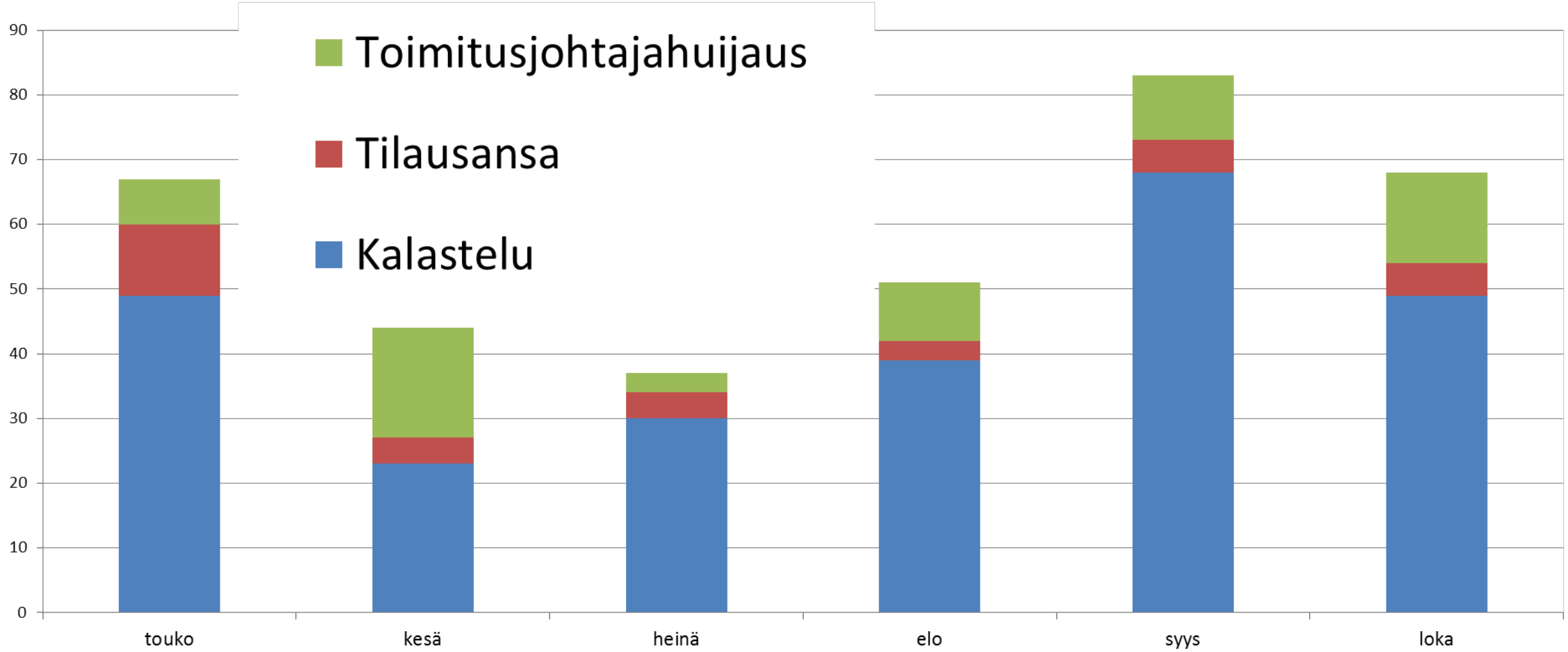
Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2017/Q3. Keräämme tilaston suoraan teleyrityksiltä. Lähde: Telia. Seuraava tilasto: tammikuussa 2018

Huijaukset & kalastelut

Huijaukset lokakuussa

- Toimitusjohtajahuijauksia yhä runsaasti liikkeellä.
- Tietoja yritetään kalastella pankkien, brändien ja viranomaisten nimissä.
  - » Nordea, Danske Bank ja S-pankki
  - » Apple ja PayPal
  - » Vero
- Office 365-tunnuksien avulla rikolliset yrittävät päästä yrityksen sisäverkkoon
  - » Samalla menetelmällä urkitaan tietoja, joita käytetään laskutushuijauksiin
- Tilausansoissa käytetty luvatta tunnettuja tuotemerkkejä
  - » Prisma, Posti ja Finnair
- Uusia huijauskohteita kehitellään jatkuvasti, nyt bitcoinit ovat suosittu teema.

Huijausyritykset 2017/05-10



Haittaohjelmat & haavoittuvuudet

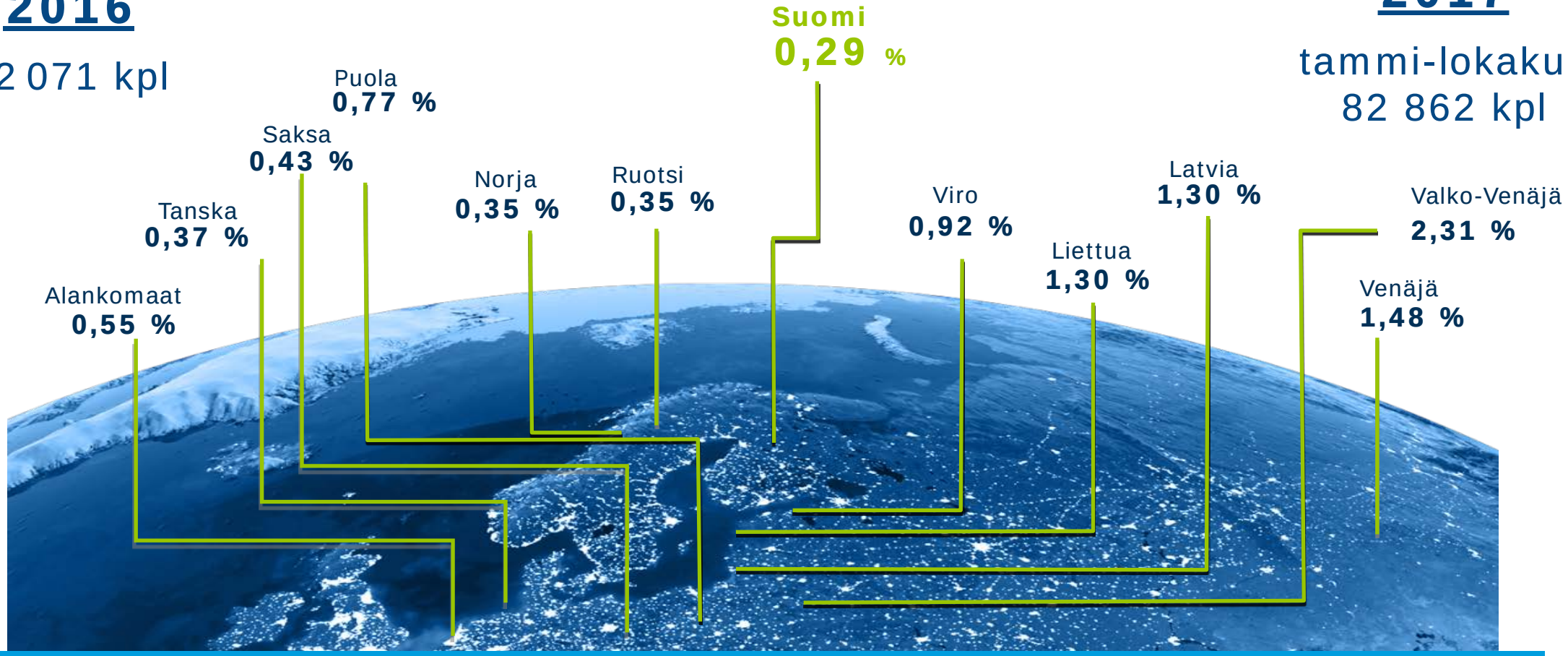
Havainnot tietoturvapoikkeamista suomalaisissa verkoissa

2016

82 071 kpl

2017

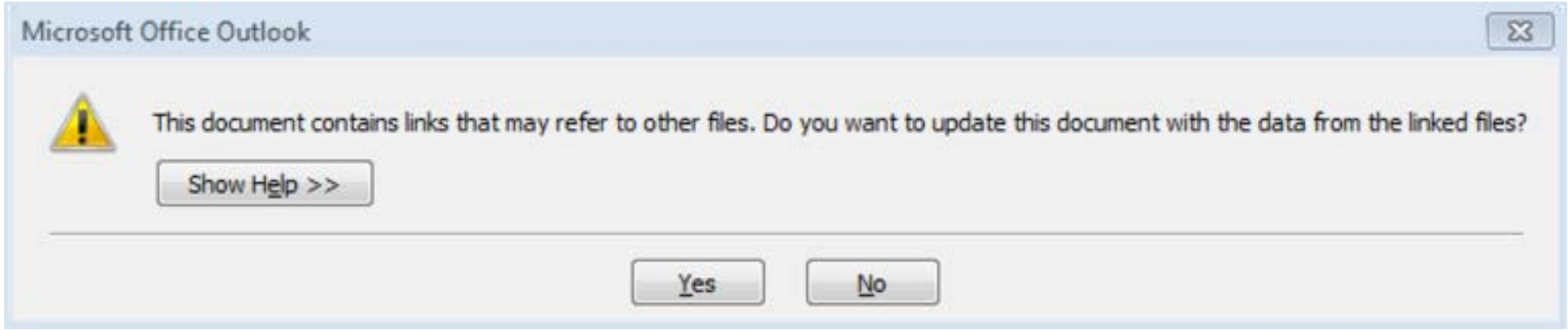
tammi-lokakuu
82 862 kpl



Havaintojen määrä on keskimäärin vuoden 2015 tasolla. Mirai-botin leviäminen marras-joulukuussa 2016 nosti lukemaa selvästi.

Haittaohjelmat ja haavoittuvuudet (1/2)

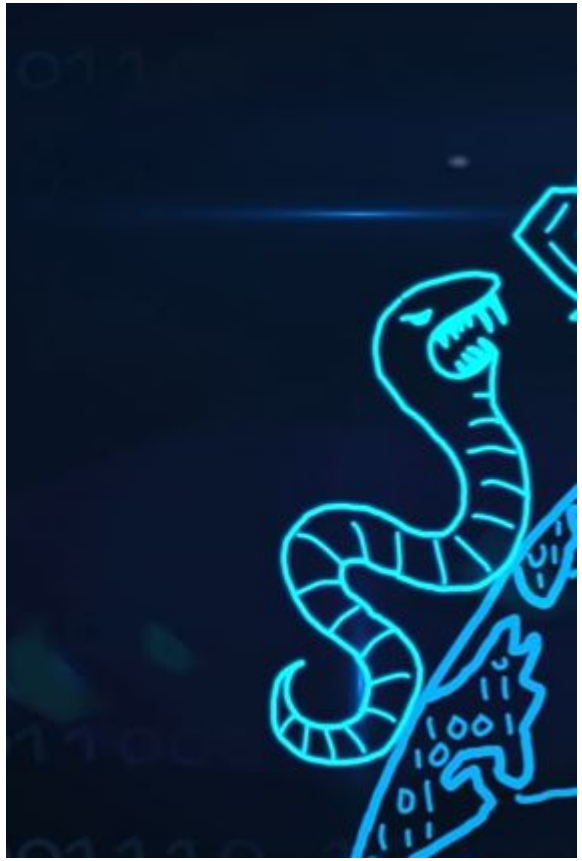
- WiFi-lähiverkkojen WPA2-salattu tietoliikenne voi paljastua hyökkääjälle. Ns. KRACK-haavoittuvuus osoittaa, että langattoman verkon salaukseen ei yksin voi luottaa. Esim. VPN antaa lisäsuojaa.
- Haittaohjelmien levitys Microsoftin Office-ohjelmistojen ja sähköpostin DDE-toimintoa hyödyntämällä on yleistynyt. Aiemmin sama tehtiin makroilla.



Kuva 1: DDE:tä voi hyödyntää hyväksymällä päivityksen oheisen kuvan mukaisesti.

Haittaohjelmat ja haavoittuvuudet (2/2)

- Bad Rabbit on uusin matomaisesti leviävä kiristyshaittaohjelma.
  - » Vaikuttanut pääasiassa Ukrainassa, Venäjällä, Turkissa ja Saksassa.
  - » Kasperskyn mukaan haittaohjelma oli saastuttanut n. 200 organisaatioita.
- Viro uusi 750 000 henkilökorttia haavoittuvuuden vuoksi
  - » RSA Infineon –piirin haavoittuvuuden seurauksena piirillä sijaitsevan varmenteen voi kloonata.
  - » Piiriä on käytetty myös passeissa, virkakorteissa ja tietokoneiden turvasiruissa.
  - » Haavoittuvuudella ei ole suuria vaikutuksia Suomessa, koska RSA-avaimia ei ole luotu kortilla missään esille tulleessa käyttökohteessa. Suomessa avaimet on luotu kortin ulkopuolella, ja siirretty kortille jälkikäteen.



Vakoilu

Verkkovakoilussa ajankohtaista

APT28	Uusin spearphishing-kampanja, jolla levitetään haitallista liitetiedostoa. Viestien aiheena on ollut mm. kyberturvallisuuskonferenssi.
Bellingcat	Bellingcat-tutkijayhteisön jäsenten Gmail-tunnuksia on yritetty kalastella. Huijausviesteissä on käytetty hyväksi Blogspot-palvelua.
Bad Rabbit	Lähinnä Venäjällä ja Ukrainassa levitetty Bad Rabbit –kiristyshaittaohjelma on yhdistetty kesän NotPetya-haittaohjelmaan

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi