#kybersää syyskuu 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

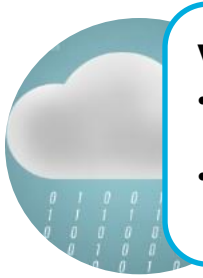
vakava

#kybersää 09/2017

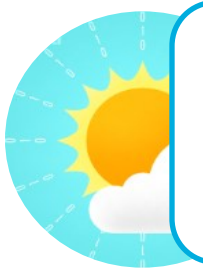
Palvelunestot
- Ahvenanmaalla useissa palveluissa katkoja, koska paikallisiin palvelimiin kohdistui sarja jykeviä palvelunestohyökkäyksiä.

Haittaohjelmat & haavoittuvuudet
- Miljoonat kuluttajat saivat haittaohjelmatartunnan Avastin CCleaner-ohjelmistopäivityksen yhteydessä.
- Viron henkilökorteista löydetty tietoturvapuutteita.

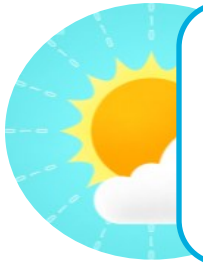
Huijaukset & kalastelut
- Pankkitunnusten kalastelu jatkuu sekä pankkien, verottajan, poliisin että Apple ID:n nimissä.
- Toimitusjohtajahuijaukset jatkuvat yleisinä.
- Tilausansoissa käytetään tunnettuja tuotemerkkejä, mm. Prisma, Finnair ja Gigantti.



Vakoilu
- Valko-Venäjää yritettiin vakoilla Zapad 2017 – sotaharjoitusaiheisilla viesteillä.
- CCleaner-sovelluksen saastuttamisen tarkoituksena oli tunkeutua teknologiayrityksiin.



Verkkojen toimivuus
- Elokuun tapaan myös syyskuussa merkittäviltä häiriöiltä vältyttiin.



IoT
- IoT-laitteiden hyödyntäminen roskapostin levittämisessä lisääntynyt.
- Älylaitteita tullaan hyödyntämään rikollisissa tarkoituksissa myös jatkossa, keinot monipuolistuvat.

Syyskuu 2017 on ollut pilvinen

"Syyskuussa nähtiin vakavia haavoittuvuuksia sekä tietomurtoja suuriin kansainvälisiin yrityksiin. Kotimaassa vakava palvelunestohyökkäys häiritsi tietoliikenneyhteyksiä Ahvenanmaalla."

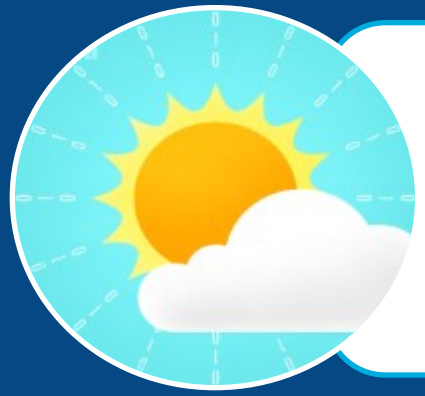
Ajankohtaista

Kyberturvallisuus-uutisointia maailmalta

- Vuonna 2013 tapahtuneessa internetyhtiö Yahoon palvelinmurrossa rikolliset saivat käsiinsä tietoa, joka koski yhteensä 3 miljardia käyttäjätiliä. Aiemmin Yahoo oli tiedottanut tietomurron koskeneen miljardia käyttäjätiliä.
- Suomi ja Yhdysvallat perustavat yhteisen kyberturvallisuuden tutkimuskeskuksen Oulun yliopiston yhteyteen.
- Euroopan unioni päivittää kyberturvallisuusstrategiaansa: tähtäin on pidemmällä tulevaisuudessa, ja luottamusta yhteiseen EU:n digitaaliseen markkina-alueeseen halutaan tukea.
- Yhdysvaltalaiselta luottokorttiyhtiö Equifaxilta on varastettu ainakin 143 miljoonan asiakkaan henkilötietoja.

Ajankohtaiset lakiasiat

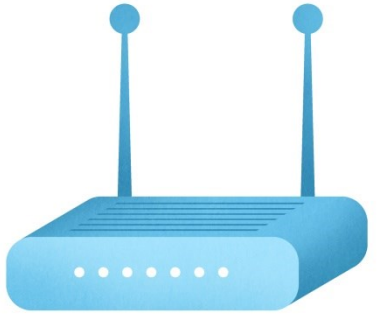
- NIS-direktiivin täytäntöönpanon valmistelu jatkuu kotimaassa ja EU:ssa
  - » HE laeiksi Euroopan Unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta (LVM/1616/03/2016) oli kuulemisella 20.10.2017 asti.
  - » EU:n komissio valmistelee täytäntöönpanoasetusta digitaalisten 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.
  - » HE tunnistuslain muuttamisesta on valiokuntakäsittelyssä.
    - Tunnistuslain enimmäishintaa koskeva sääntely laajennettaisiin koskemaan kaikkia tunnistustapauksia mukaan lukien ensitunnistus.
    - Korjaus valvontamaksusäännökseen.



IoT

Esineiden internet (IoT) -yhteenveto

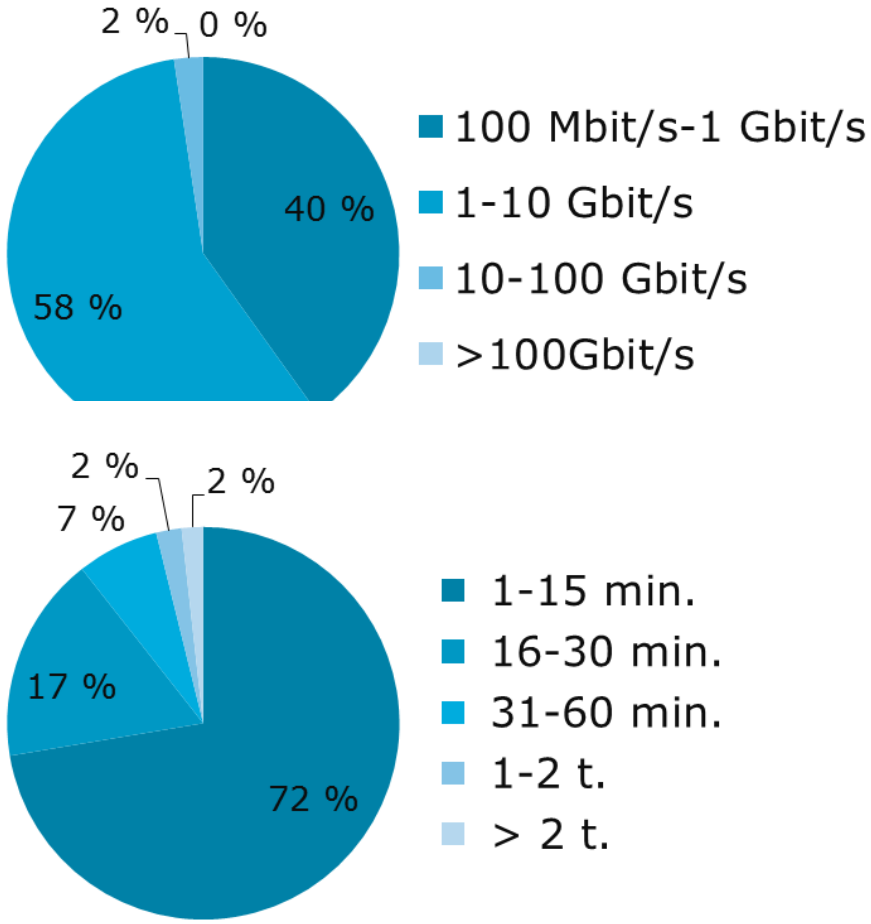
- IoT-laitteiden käyttö myös massamaisiin roskapostilähetyksiin lisääntyy jatkuvasti
  - Haittaohjelman sisältävä laite voi lähettää keskimäärin 400 roskapostia päivässä.
  - Eniten saastuneita laitteita on Brasiliassa ja Yhdysvalloissa. Seuraavaksi Venäjällä, Intiassa, Meksikossa ja muutamissa Euroopan maissa.
- Verkkorikolliset testaavat puutteellisesti suojattujen Netgear-valmistajan reitittimien avulla käyttäjätunnus-salasanapareja useisiin verkkopalveluihin - tiedot on saatu aiempien tietomurtojen yhteydessä
  - Uusilla murroilla voidaan jatkaa vastaavaa hyökkäystä uusiin kohteisiin ilman, että hyökkääjää saadaan estettyä.
- Mirai samantyyppisine boteineen ja matoineen on pysyvä ilmiö
  - Ilmiö myös yleistynee, koska kaikkia helposti hyödynnettävien ohjelmistojen salasanoja ei vielä ole löydetty.
  - Niin kauan kun markkinoilla myydään haavoittuvia laitteita eivätkä valmistajat paranna tuotteidensa laatua, ongelma tulee jatkumaan.
  - Kuluttajat eivät juurikaan voi ongelmaa ehkäistä, sillä salasanoja ei usein voi vaihtaa.
  - Kuluttajan on myös hankala saada tietoa siitä, kuinka laiteiden tietoturvaa on testattu.



Palvelunestot

Palvelunestohyökkäykset ja nii[illegible]

- Ahvenanmaahan kohdistui sarja palvelunestohyökkäyksiä, jotka olivat suuria ja pitkäkestoisia
  - Hyökkäykset vaikuttivat useiden palveluiden toimintaan.
  - Samanaikaisesti käynnissä Ruotsin isännöimä Aurora-sotaharjoitus ja Venäjän Zapad-sotaharjoitus
- Kelaa vastaan jälleen palvelunestohyökkäyksiä, jotka aiheuttivat vain pieniä häiriöitä
- Etelä-Suomen Median lehtien verkkosivut olivat nurin useita tunteja palvelunestohyökkäyksen vuoksi
- Suurimpia Suomessa viimeaikoina havaittuja palvelunestohyökkäyksiä:
  - 2017/Q3: n. 30 Gbit/s (kesto 12 min)
  - 2017/Q2: n. 77 Gbit/s (kesto 7 min)
  - 2016: n. 280 Gbit/s (kesto 42 min)



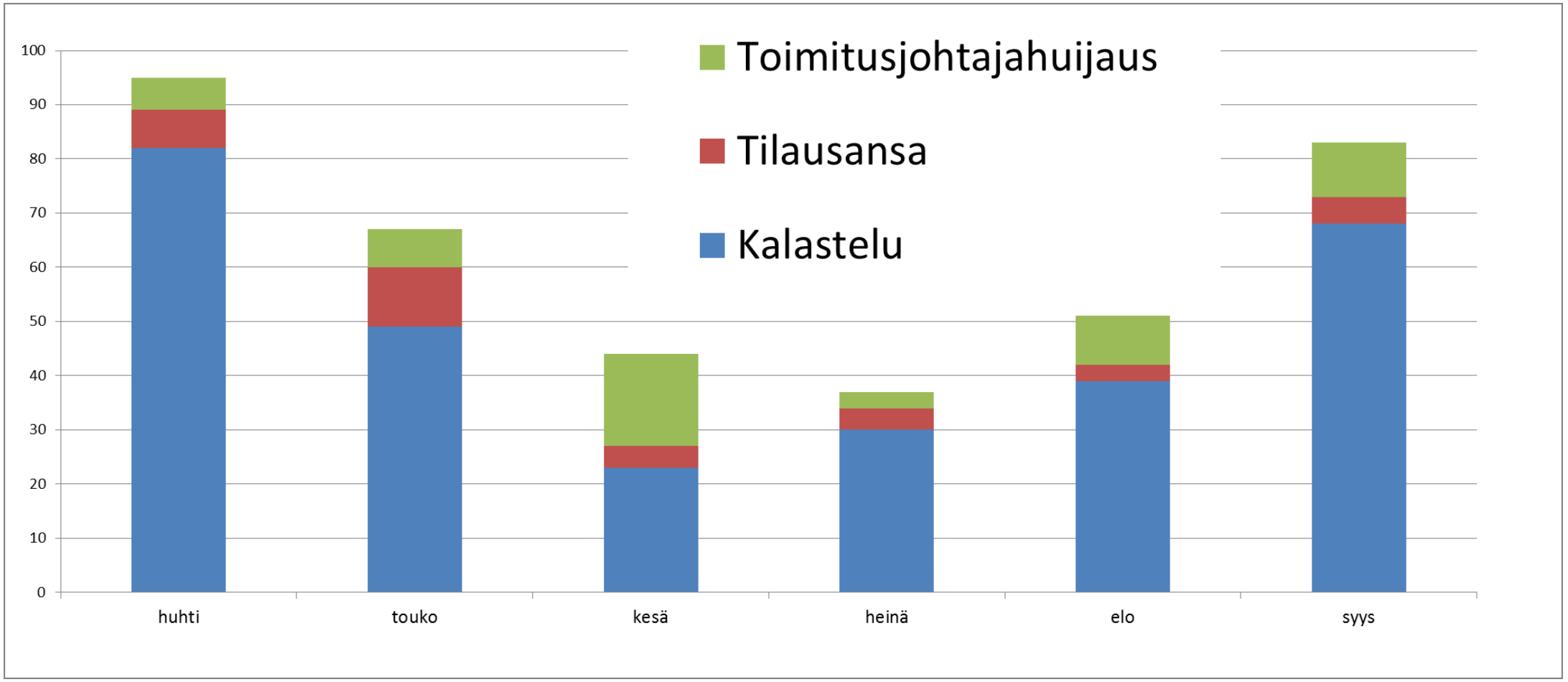
Suomeen k
kestot 2017/Q3. Keräämme tilaston suoraan teleyrityksiltä.
Lähde: Telia. Seuraava tilasto: tammikuussa 2018

Huijaukset & kalastelut

Huijaukset

- Tietoja yritetään kalastella Nordean, Danske Bankin, Aktian ja S-pankin ja verottajan nimissä
  - » PayPal-, Dropbox- ja Apple ID -tunnuksiakin udellaan.
- Poliisina esiintyvät huijarit yrittävät saada tietoonsa uhrien tunnuksia sähköpostiviestien avulla
- Toimitusjohtajahuijaukset ovat edelleen yleisiä
- Tilausansoja liikkeellä. Niissä käytetty luvatta tunnettuja tuotemerkkejä (esim. Prisma, Gigantti ja Finnair)

Huijausyritykset 2017/04-09

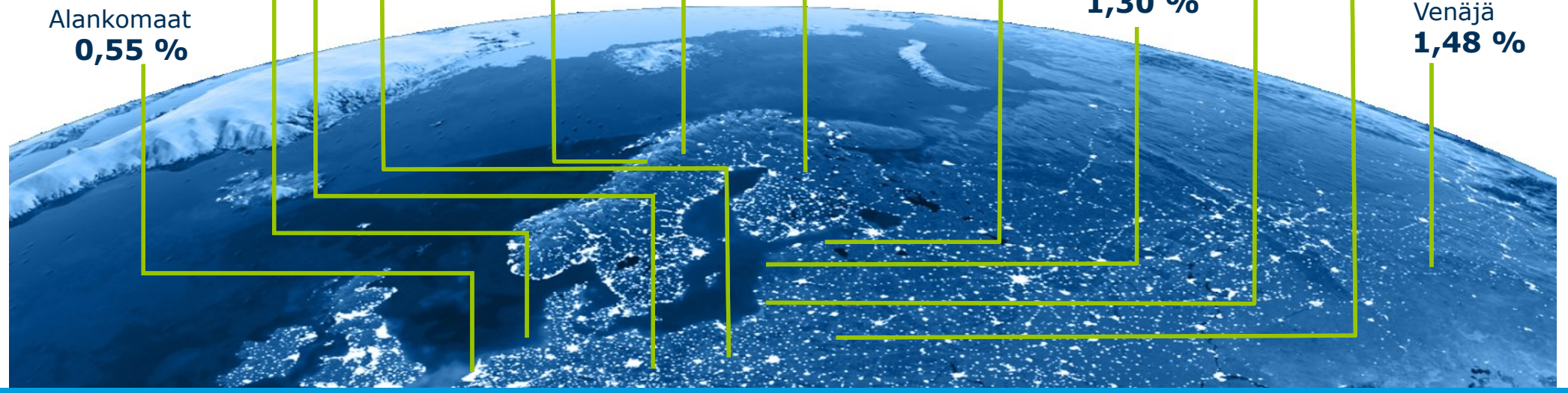


Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2016

Havainnot
82 071 kpl



Alankomaat **0,55 %**
Tanska **0,37 %**
Saksa **0,43 %**
Puola **0,77 %**
Norja **0,35 %**
Ruotsi **0,35 %**
Suomi **0,29 %**
Viro **0,92 %**
Liettua **1,30 %**
Latvia **1,30 %**
Venäjä **1,48 %**
Valko-Venäjä **2,31 %**

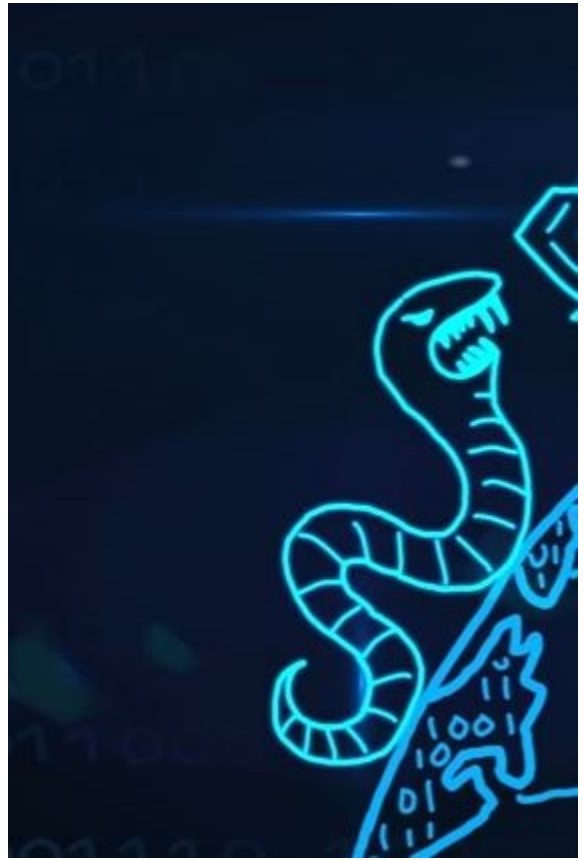
2017

Havainnot tammi-syyskuu
76 290 kpl

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

Haittaohjelmat ja haavoittuvuudet

- Avastin CCleaner-ohjelmistoon oli ujutettu haittaohjelma, joka tarttui ohjelmistopäivitysten yhteydessä miljoonille kuluttajille
- Apache Struts –palvelinohjelmistosta löytyi vakava haavoittuvuus, jota on hyödynnetty palvelinten tietomurroissa
  - » Vastaavaa Struts-haavoittuvuutta käytettiin yhdysvaltalaisen Equifax-yrityisen tietomurrossa, jossa vuodettiin n. 140 miljoonan kuluttajan henkilötiedot.
- Viron sähköisistä henkilökorteista löydettiin tietoturvahaavoittuvuus
- Trickbot–pankkihaittaohjelmaa käytetään taas aktiivisesti, tällä kertaa kohteena suomalaispankkien asiakkaat. Tartuntoja on havaittu toistaiseksi vähän
- Dnsmasq-ohjelmistossa vakava haavoittuvuus, jonka avulla hyökkääjä voi muun muassa saada kohteensa koneen haltuun
  - » Dnsmasqin avulla lähiverkon koneille jaetaan verkkonimet, joilla niihin voi yhdistää IP-osoitteiden sijaan.



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

Valko-Venäjä	Valko-Venäjää yritetty aktiivisesti verkkovakoilla Zapad-aiheisin viestein.
Lähi-itä	Tietoturvayhtiöt ovat julkaisseet useita julkisia raportteja erityisesti Persianlahden alueelle kohdistuneista verkkovakoilutapauksista.
CCleaner	Työasemahallinnan apusovelluksen päivitykseen oli ujutettu haitallinen komponentti. Varsinaisena kohteena olivat ilmeisesti useat globaalit teknologiayritykset.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi