#kybersää 12/2018

#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 03/2018: Office 365 -tunnuksia kalastellaan aktiivisesti

- Suomalaisten yritysten ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä on kuluvan vuoden aikana varastettu. Vakava varoitus aiheesta on edelleen voimassa. Varoituksen taso laskettiin lokakuussa kriittisestä (punainen) vakavaksi (keltainen).
- Käyttäjätunnuksia ja salasanoja on kalasteltu sähköpostitse ja huijaussivujen avulla. Lokakuun lopulla nähtiin viestejä, joissa kalastelulinkki toimitettiin pdf-liitetiedoston sisällä.
- Hyökkääjät voivat ohittaa käyttäjän monivaiheisen tunnistamisen (MFA), jos ylläpitäjät ovat asettaneet Office 365:n tukemaan kirjautumista myös vanhoilla sovelluksilla (ns. legacy support).
- Hyökkääjät kirjautuvat käyttäjätileille ja seuraavat yritysten sähköpostiliikennettä. He pyrkivät saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia.
- Kyberturvallisuuskeskus antoi asiasta varoituksen 11.6.2018. Lisätietoja: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

#kybersää 12/2018

Palvelunestot

- Jouluviikolla palvelunestohyökkäyksiä havaittiin tavallista enemmän, mutta niiden vaikutukset jäivät silti vähäisiksi.
- Suurimmat yksittäiset hyökkäykset ovat olleet volyymiltaan yli 40 Gbit/s.

Haittaohjelmat & haavoittuvuudet

- Kohdennettu Ryuk-kiristyshaittaohjelma on häirinnyt muun muassa useiden yhdysvaltalaisten sanomalehtien painamista.
- Internet Explorerista on korjattu haavoittuvuus tavallisen päivitysrytmin ulkopuolella.

Huijaukset & kalastelut

- Office 365 -tietojenkalastelu leviää nyt myös SharePoint -sivujen avulla.
- Uusia tekstiviestihuijauksia ulkomaisten pankkien ja Suomen Postin nimissä.

Vakoilu

- SUPO kertoi Suomeen kohdistuvan aktiivista kybervakoilua.
- Joulukuussa uutisoitiin teollisuusvakoilusta, joka ulottui myös Suomeen sekä EU:n diplomaattiviestinnän vakoilusta.

Verkkojen toimivuus

- Vakavia häiriöitä on ollut enemmän kuin viime vuonna, mutta niiden kestot ovat lyhentyneet.
- Merkittävien häiriöiden kokonaismäärä laskussa.

IoT

- Mirai–bottiverkon uhreja myös Suomessa
- Orangen modeemeista vuotanut huomattava määrä tunnuksia.

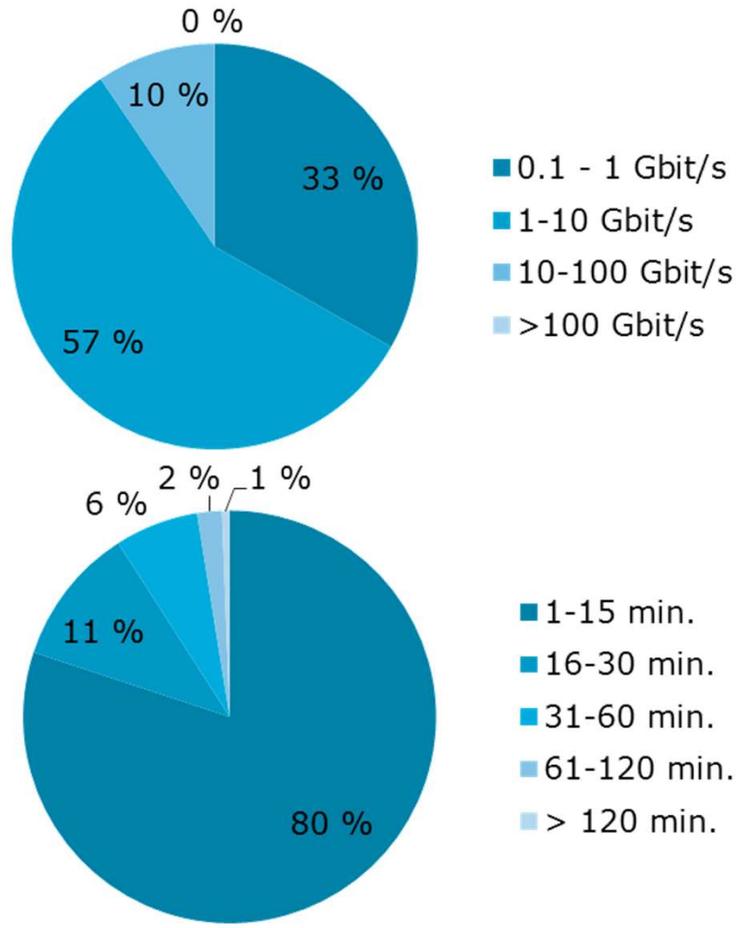
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu:

- Lyhyet alle 15 minuutin 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.

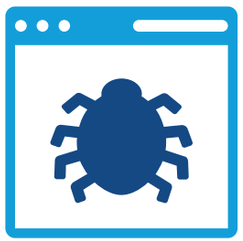
Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä. Lähde: teleyritykset

2018/Q4:	**2018/Q3:**	**2018/Q2:**
n. 45 Gbit/s (kesto 6 min)	n. 89 Gbit/s (kesto 30 min)	n. 37 Gbit/s (kesto 8 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2018/Q4. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu

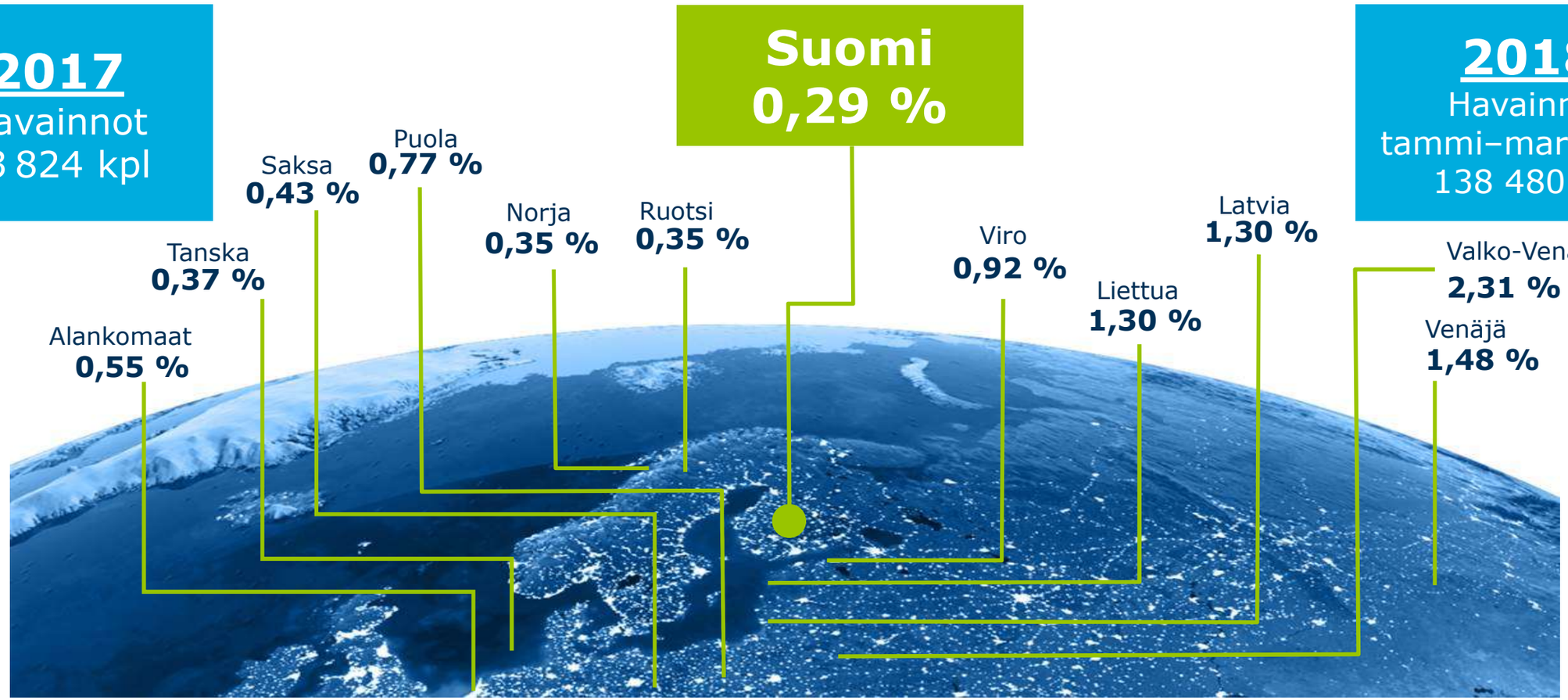


- **Jouluviikolla palvelunestohyökkäysten aktiviteetti kasvoi**
  - Kyberturvallisuuskeskukseen raportoitiin useista palvelunestohyökkäyksistä valtionhallintoa ja yksityistä sektoria vastaan. Hyökkäysten vaikutukset jäivät kuitenkin vähäisiksi.
  - Hyökkäysten volyymit ovat olleet pääosin 5-10 Gbit/s, mutta suurimmat yksittäiset hyökkäykset ovat olleet 40 Gbit/s luokkaa.
  - Hyökkäysten kestot ovat olleet poikkeuksellisen pitkiä. Pahimmillaan hyökkäykset ovat kestäneet liki 10 tuntia.
- **Viimeaikaisia trendejä**
  - Tällä hetkellä yleisin hyökkäystekniikka on internetiin avoimiksi asetettujen CLDAP-hakemistopalveluiden hyödyntäminen hyökkäysten vahvistamiseksi.
  - Nämä palvelimet sijaitsevat pääasiassa Suomen ulkopuolella.

Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl



2018
Havainnot
tammi–marraskuu
138 480 kpl

Vuoden 2018 tietoturvapoikkeamien havaintomäärää nostaa pienreitittimien haittaohjelmatartunnat

Haittaohjelmat

- **Haittaohjelmatilanne Suomessa**
  - Suomessa määrällisesti eniten havaintoja kotireitittimiin ja muihin IoT-laitteisiin tarttuneista haittaohjelmista.
- **Sähköpostin liitetiedostot yhä yleisin kanava levittää haittaohjelmia**
  - Sähköpostin liitetiedostot ovat olleet yleisin haittaohjelmien levitystapa jo muutaman vuoden ajan.
  - Joulukuussa uutena levitystapana näkyi organisaation oman Sharepoint-palvelun käyttö haitallisten tiedostojen jakamiseen, jotka ovat ohjanneet käyttäjän tietojenkalastelusivulle.
- **Magento-verkkokauppa-alustoja murretaan edelleen**
  - Murretuissa verkkokaupoissa käytetyt maksukorttitiedot päätyvät rikollisille.
  - Erään tietoturvatutkijan mukaan n. 7 000 Magento-alustaa käyttävää verkkokauppaa on murrettu viimeisen 6 kuukauden aikana. Julkisuuteen ovat tulleet muun muassa Ticketmaster, British Airways ja Newegg.
  - Kyberturvallisuuskeskuksen tiedossa on ainakin yksi havainto myös Suomesta.

Haavoittuvuudet

- **PHP version 5 tuki loppui 31.12.2018**
  - » Löytyviä uusia haavoittuvuuksia ei enää korjata.
  - » PHP:n vanhoja versioita käytetään yhä laajasti tuotantoympäristöissä.
  - » Linux-jakelut saattavat tarjota rajoitettua tukea tietyille paketoimilleen versioille.

- **Internet Explorer –selaimesta on korjattu haavoittuvuus tavallisesta päivitysrytmistä poiketen**
  - » Haavoittuvuutta on käytetty muun muassa kohdistetuissa hyökkäyksissä.
- **SQLite-tietokantakirjastosta on löytynyt haavoittuvuus, joka altistaa hyvin suuren määrän erilaisia ohjelmistoja hyväksikäytölle**
  - » Haavoittuvuus vaikuttaa muun muassa vanhempiin Chrome-selaimen versioihin.

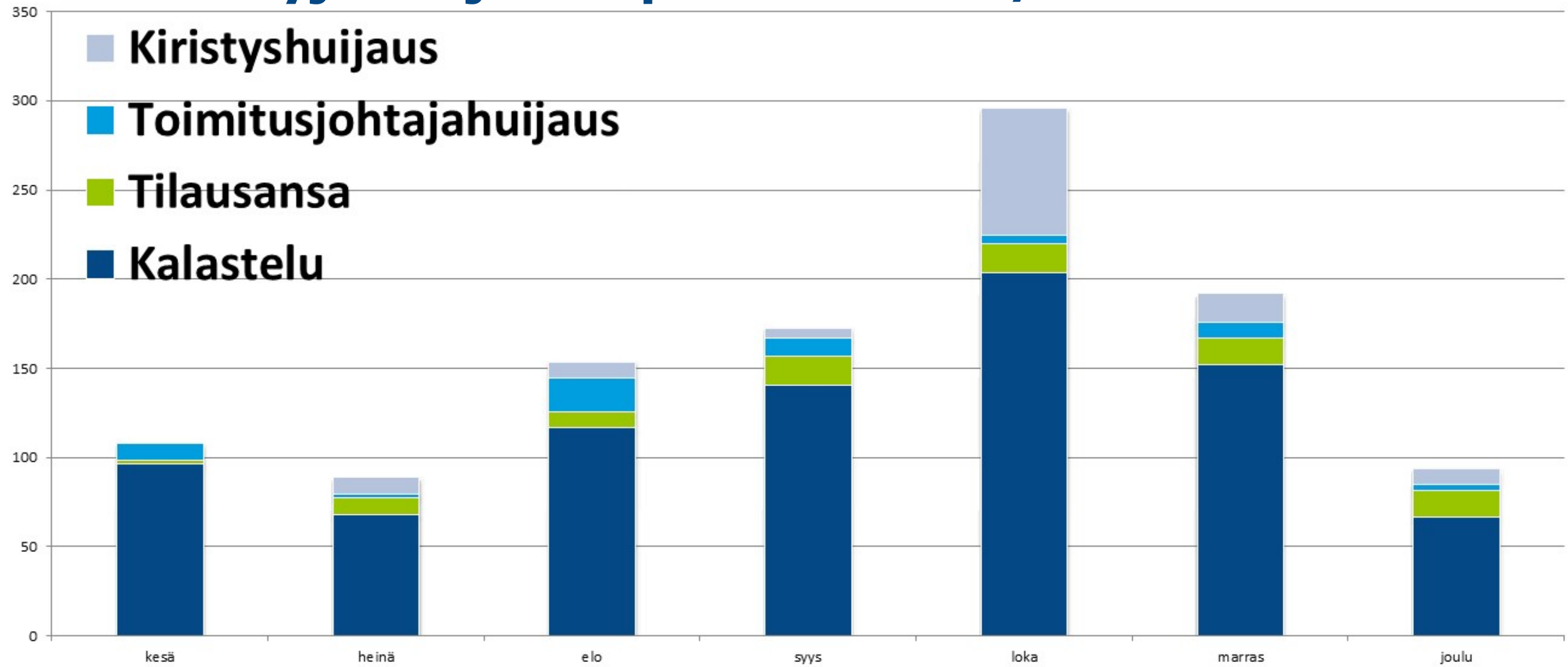
- **Viime kuukausina Windowsista on julkaistu säännöllisesti nollapäivähaavoittuvuuksia yksittäisellä Twitter-tilillä**
  - » Pääasiassa haavoittuvuudet ovat mahdollistaneet käyttövaltuuksien korottamisen paikallisesti.

Tietomurrot ja tietovuodot

- **Ryuk-niminen kohdennettu kiristyshaittaohjelma on aiheuttanut laajoja vahinkoja useassa yrityksessä**
  - » Haittaohjelma häiritsi muun muassa useiden yhdysvaltalaisten sanomalehtien painamista sekä erään pilvipalvelutarjoajan toimintaa.

Huijaukset & kalastelut

Käsiteltyjä huijaustapauksia 2018/06–12



Huijaukset

- **Office 365 -tunnusten kalastelu sai uusia muotoja**
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Uutena hyökkäystapana murretut SharePoint-sivut johdattavat uhrin kalastelusivulle.
  - Kalastelun avulla murrettuja sähköpostitilejä käytetään mm. laskutushuijauksiin, vakoiluun ja uusien kalasteluviestien lähetykseen.
  - Kaksivaiheinen kirjautumistapa Modern Authentication suositellaan ottamaan käyttöön pakotetusti niin, ettei sitä voi kiertää vanhemmilla päätelaitteilla.

- **Tekstiviestihuijaukset lisääntyneet selvästi**
  - Tekstiviestillä lähetetään nykyään paljon sellaisia tavallisia huijauksia, joita aiemmin levitettiin vain sähköpostitse.
  - Tilausansat, sijoitushuijaukset, rahanpesu ja kaikenlaiset huijausyritykset yrittävät nostaa uskottavuuttaan tekstiviestinä.
  - Älypuhelimilla linkkien klikkailu onnistuu yhtä helposti tekstiviestistä, sähköpostista ja verkkosivuilta.
- **Kiristyshuijauksia aikuisviihdeteemalla**
  - Kiristyksen uhreja säikytellään väittämällä, että kiristäjä on saanut pääsyn uhrin laitteeseen ja vakoillut tämän tekemisiä. Kiristäjä väittää saaneensa käsiinsä arkaluontoista materiaalia, mutta se on kaikki huijausta.
- **Tietoja yritetään kalastella tunnettujen pankkien ja tuotemerkkien nimissä**
  - Apple ID -tunnuksia kalastellaan jälleen. Myös pankkien, PayPalin ja Netflixin nimissä kalasteltiin maksukorttitietoja.
  - Tilausansoihin houkuteltiin kuluttajia paljon mm. Ikean ja Gigantin tuotenimillä.

Vakoilu

Verkkovakoilutilanteessa ajankohtaista

APT10-ryhmän vakoilu ulottui myös Suomeen	Yhdysvallat kertoo Suomen olleen yksi niistä maista, joissa toimiviin yrityksiin APT10-ryhmän tekemät tietomurrot ovat ainakin liittyneet. Kiinaan julkisuudessa yhdistetty ryhmä pääsi Yhdysvaltojen mukaan käsiksi uhriorganisaatioiden tietoihin palveluntarjoajan kautta.
SUPO kertoi Suomeen kohdistuvan kybervakoilun olevan aktiivista	Suojelupoliisin kansallisen turvallisuuden katsauksen mukaan Suomeen kohdistuu aktiivista kybervakoilua. SUPO myös arvioi kybervakoilun ja -hyökkäysten kohdistuvan jatkossa yhä useammin myös varsinaisia kohteita lähellä oleviin tahoihin.
EU:n diplomaatti-viestintää vakoiltiin jopa vuosien ajan	Hakkereiden epäillään vakoilleen EU:n diplomaattisähkeitä vuosien ajan ja päässeen käsiksi jopa tuhansiin alemman salaustason viesteihin. Järjestelmään päästiin tiettävästi käsiksi tietojenkalastelukampanjan avulla.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

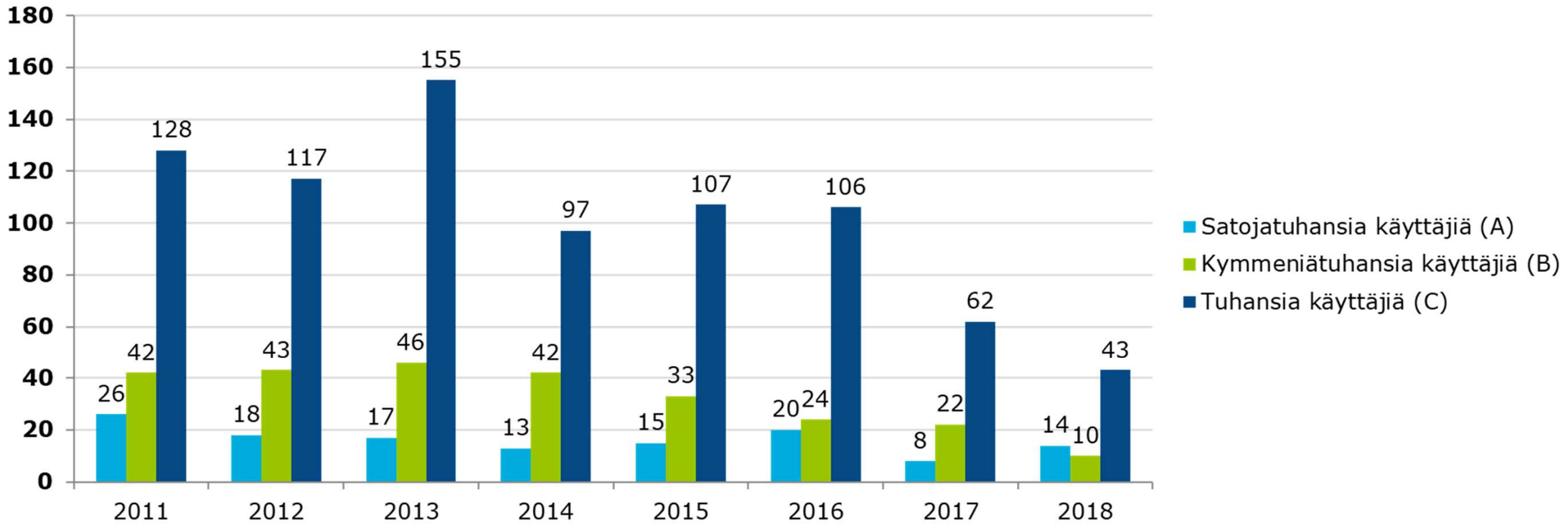
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018

Vakavuus	Lukumäärä
A-luokka	14
B-luokka	10
C-luokka	43
Kaikki häiriöt (Q1–Q3)	**287 725**

Merkittävien häiriöiden määrä jatkaa laskuaan. Vakavimpia A-luokan häiriöitä on ollut kesän aikana paljon, mutta se vaikuttaa sattumalta.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta vuodessa. Niiden määrä riippuu teleyrityksen tilastointitavasta.

IoT

Esineiden internet (IoT)

- **Mirai–bottiverkon uhreja myös Suomessa**
  - » Pitkään IoT-laitteita saastuttanut bottiverkko jatkaa toimintaansa.
  - » Uusi variantti, Miroi-haittaohjelma hyödyntää ThinkPHP haavoittuvuutta versioissa 5.0.23, sekä 5.1.31
- **Ranskassa ja Espanjassa yli 19000 modeemista on tunnukset vuotaneet**
  - » Orangen modeemeissa oleva haavoittuvuus on havaittu 2012.
  - » Haavoittuvuus on vakava, sillä sen lähiverkon tunnuksen avulla voi löytää salasanan lisäksi myös verkon sijainnin.

Tietoturva-alan kehitys

Ajankohtaiset oikeudelliset asiat: EU

- **EU:n televiestintäuudistus ("EECC-direktiivi")**
  - Säädös on julkaistu EU:n virallisessa lehdessä ja se on tullut voimaan, ks. https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1545208883302&uri=CELEX:32018L1972
  - Jäsenvaltioiden on annettava tarvittavat kansalliset säädökset viimeistään 21.12.2020, josta alkaen niitä tulee myös noudattaa.
  - Tarvittavat muutokset tehdään Suomessa pääasiassa sähköisen viestinnän palveluista annettuun lakiin (917/2014) LVM:n käynnistämässä säädöshankkeessa.
- **"Kyberturvallisuusasetus"**
  - Asetuksesta on päästy poliittiseen yhteisymmärrykseen. Seuraavaksi se on hyväksyttävä virallisesti Euroopan parlamentissa ja EU:n neuvostossa. Hyväksymisen jälkeen se julkaistaan EU:n virallisessa lehdessä ja se tulee heti voimaan.
  - Asetuksella vahvistetaan EU:n kyberturvallisuusvirasto ENISAn mandaattia sekä perustetaan EU:n laajuinen kyberturvallisuuden sertifiointikehys.
  - Ks. lisää http://europa.eu/rapid/press-release_IP-18-6759_fi.htm

Ajankohtaiset oikeudelliset asiat: kotimaa

- **Voimaan tulleet lait** (mm.):
  - Laki Liikenne- ja Viestintävirastosta (935/2018) ja muut LVM:n hallinnonalan virastouudistukseen kuuluvat lait
    - Säädökset tulivat pääasiassa voimaan 1.1.2019.
    - **Liikenne- ja viestintävirasto** Traficom aloitti toimintansa 1.1.2019 kun Viestintävirasto, Liikenteen turvallisuusvirasto Trafi sekä Liikenneviraston tietyt toiminnot yhdistyivät. Ks. lisää https://www.traficom.fi
    - **Kyberturvallisuuskeskuksen** toiminta pysyy ennallaan uudessa Liikenne- ja viestintävirastossa, ks. lisää https://kyberturvallisuuskeskus.fi
  - Sähköisen viestinnän palveluista annetun lain muutos (1266/2018)
    - Muutos liittyy EU:n yleistä tietosuoja-asetusta (GDPR) täydentävään lainsäädäntökokonaisuuteen, johon kuuluu myös uusi Tietosuojalaki (1050/2018).
    - Uusi 145 a § oikeuttaa teleyritykset käsittelemään rikoksiin liittyviä henkilötietoja; samalla puhelinliittymän markkinoinnin kieltävän 201 §:n voimassaoloa jatkettiin.
    - Säädökset tulivat voimaan 1.1.2019.

Ajankohtaiset oikeudelliset asiat: kotimaa

- **Eduskunnassa** (mm.):
  - Valtioneuvoston selonteko tietopolitiikasta ja tekoälystä (VNS 7/2018 vp)
  - Hallituksen esitys laeiksi vankeuslain ja tutkintavankeuslain, pakkokeinolain ja rikoslain 6 luvun 13 §:n muuttamisesta (HE 222/2018 vp)
    - HE:ssä ehdotetaan lisättäväksi vankeuslakiin ja tutkintavankeuslakiin säännökset, joiden nojalla RISEllä olisi toimivalta puuttua (esim. radiosignaaliin vaikuttavalla teknisellä laitteella) miehittämättömän kulkuneuvon liikkumiseen vankilan alueella tai yläpuolella.
  - Hallituksen esitys kansallisen turvallisuuden huomioon ottamista alueiden käytössä ja kiinteistönomistuksissa koskevaksi lainsäädännöksi (HE 253/2018 vp)
  - Tunnistus- ja luottamuspalvelulain muutos (HE 264/2018 vp)
    - HE:ssä selkeytetään vahvan sähköisen tunnistamisen luottamusverkostoon kuuluvien palveluntarjoajien sopimuksentekovelvoitetta ja ehdotetaan enimmäishinnan alentamista tukkutasolla.
  - Hallituksen esitys laeiksi sähköisen viestinnän palveluista annetun lain ja julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain muuttamisesta (HE 226/2018)
    - Lakimuutoksilla mahdollistetaan laajakaistainen viranomaisviestintäpalvelu, jolla korvataan nykyinen viranomaisradioverkkoon (VIRVE) perustuva kapeakaistainen viranomaisviestintäpalvelu.
    - Eduskunta hyväksyi lakiesityksen muutettuna ennen joulua, tasavallan presidentti ei ole vielä vahvistanut lakia.

Ajankohtaiset oikeudelliset asiat: kotimaa

- **Virastossa**:
  - » Tunnistuspalveluiden arviointikriteeristön päivitys käynnistetty
    - Virasto on antanut vahvan sähköisen tunnistuspalvelun tarjoajien vaatimustenmukaisuuden arvioinnista kaksi ohjetta (211/2016 ja 215/2016).
    - Virasto käynnisti marraskuun lopussa ohjeiden päivityksen. Mallikriteeristöön lisätään mobiilisovelluksien kriteeristö.
    - Päivitystyöhön on kutsuttu kaikille avoin työryhmä, ks. lisää https://kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen -> valmisteluasiakirjat.
- **Muuta**:
  - » Luonnos hallituksen esitykseksi laeiksi ydinenergialain ja turvallisuusselvityslain 21 §:n muuttamisesta on lausuttavana lausuntopalvelu.fi:ssä 16.1.2019 saakka
    - Esitysluonnos sisältää lennokkien ja miehittämättömien ilma-alusten torjuntaan ydinvoimalaitoksilla liittyvät toimivaltuussäännöksiä.

Kyberasioihin liittyvää uutisointia maailmalta

Suojelupoliisin mukaan **Suomea vastaan kohdistuva vieraiden valtioiden tiedustelutoiminta jatkuu aktiivisena lähivuosina**. Kybervakoilu ja -hyökkäykset kohdistuvat vastaisuudessa yhä enemmän kohdeorganisaatioita lähellä oleviin, vähemmän tietoturvatietoisiin toimijoihin.

Useat maan ovat kieltäneet kiinalaisomisteisten yhtiöiden teknologian käyttämisen maiden kriittisissä infrastruktuureissa tai valtionhallinnon työntekijöillä. Yhtiöiden pääsy esimerkiksi 5G-teknologian tekniikan ytimiin tai valtionhallinnon työtekijöiden käyttöön halutaan estää, sillä Kiinan lainsäädännön kerrotaan edellyttävän kaikkien kiinalaisten yritysten tukevan maan tiedustelutoimintaa.

Tietoturvayhtiö McAfee kertoi joulukuussa huolestuttavista haittaohjelmahavainnoistaan, joissa myös **suomalaiseen ydinvoimayhtiöön oli onnistuttu hyökkäämään**. Stukin asiantuntijan mukaan aiemminkaan suomalaisissa ydinvoimaloissa ei ole törmätty kyberhyökkäyksiin harmittomaksi jääneitä palomuurien koputteluja lukuun ottamatta.

Haittaohjelma viivytti useiden suurten amerikkalaisten päivälehtien julkaisua. Medioista mm. LA Times, New York Times sekä Wall Street Journal joutuivat haittaohjelman kohteeksi. Haittaohjelman epäillään tulleen ulkomailta.

TRAFICOM
Kyberturvallisuuskeskus

Liikenne- ja viestintäviraston kyberturvallisuuskeskus

Viestintävirasto, Liikenteen turvallisuusvirasto Trafi ja osa Liikennevirastoa yhdistyivät Liikenne- ja viestintävirasto Traficomiksi 1.1.2019. Vuosina 2014 - 2018 toimimme osana Viestintävirastoa.

etunimi.sukunimi@traficom.fi

www.kyberturvallisuuskeskus.fi

@CERTFI