Helmikuu | 2019

# #KYBERSÄÄ

**#kybersää** kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

**rauhallinen**

**huolestuttava**

**vakava**

TRAFICOM

# Varoitus 02/2018: Office 365 -tunnuksia kalastellaan aktiivisesti

Suomalaisten yritysten ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä on varastettu jo pitkään. Vakava (keltainen) varoitus aiheesta on ollut voimassa kesästä 2018.

Käyttäjätunnuksia ja salasanoja on kalasteltu sähköpostitse ja huijaussivujen avulla. On nähty viestejä, joissa kalastelulinkki toimitettiin pdf-liitetiedoston sisällä. Monivaiheinen tunnistaminen (MFA) voidaan ohittaa, jos Office 365 on asetettu 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. Varastettuja tunnuksia käytetään erilaisiin laskutuspetoksiin.

Ajantasaisimmat tiedot varoituksesta verkkosivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

TRAFICOM

# Top 5 -kyberuhat

**1**

Loppukäyttäjät haksahtavat tietojenkalasteluun. He avaavat liitetiedostoja, klikkaavat linkkejä ja toimivat muutenkin miettimättä.

**2**

Palveluja keskitetään ja ulkoistetaan ilman suunniteltuja ja testattuja vararatkaisuja tai selkeitä sopimuksissa määriteltyjä vastuita.

**3**

Avoimeen verkkoon liitetään laitteita, joiden tietoturvaa tai suojaamista ei ole huomioitu.

**4**

Laitteiden ja järjestelmien tietoturvan puutteellinen elinkaaren hallinta. Tietoturvariskeillä ei ole nimettyä omistajaa.

**5**

Organisaatioiden kyky hallita kokonaistilannekuvaa ja reagoida poikkeamiin on usein puutteellista lokienhallinnan vajavaisuudesta johtuen.

**Top 5 -kyberuhkiin nostetaan Kyberturvallisuuskeskuksen näkökulmasta merkittävimpiä pidemmän aikavälin ilmiöitä.**

TRAFICOM

# Kybersään johtopäätökset

## Tietoturvan edistyminen

1. Rohkeilla käytössä olevien järjestelmien testauksilla organisaatio pystyy kehittämään omaa varautumistaan kyberhäiriöitä vastaan.

2. Avoimuus kertoo tilanteen hallinnasta. Tietoturvaloukkauksen kohde varoittaa esimerkillään muita ja saa apua.

3. Vaalien sujuvuuden varmistamisessa on huomioitu myös kyberturvallisuus sekä Suomessa että EU:ssa.

## Tietoturvan kehitystarpeet

1. Lokien hallinta on organisaation ”teknistä kirjanpitoa”. Sen merkitys poikkeamien selvityksessä on keskeistä.

2. Rikolliset tekevät verkko-osoitteiden tarkoituksellisilla muunnoksilla huijauksista entistä tehokkaampia. Varautuminen teknisin ja koulutuksellisin keinoin huomioitava kaikilla tasoilla.

3. Vastuuta ei voi ulkoistaa. Toimitusketjujen kautta tehtyjä hyökkäyksiä paljastuu säännöllisesti. Havainnointia on kehitettävä.

TRAFICOM

# Kybersää helmikuu 2019

### Verkkojen toimivuus

- Helmikuu oli palvelunestohyökkäysten kannalta rauhallinen.
- Viestintäpalveluiden merkittäviä häiriöitä ollut alkuvuonna hieman tavallista enemmän.

### Tietomurrot & -vuodot

- Ruotsissa suuri terveystietojen tietovuoto.
- Maltalaiseen Bank of Valletta – pankkiin tehtiin tietomurto, jonka avulla siirrettiin n. 13 miljoonaa euroa ulkomaisille tileille.

### Haittaohjelmat & haavoittuvuudet

- Sähköpostilla levitetään pakattuja tiedostoja, jotka sisältävät dokumentiksi naamioidun haittaohjelman.
- Drupal-sisällönhallintaohjelmistossa oli kriittinen haavoittuvuus.

### Vakoilu

- IT-palveluntarjoajien kautta toteutettavat hyökkäykset ovat uhka, johon organisaatioiden täytyy varautua.
- Australiassa kerrottiin poliittisiin toimijoihin kohdistuneesta tietomurrosta.

### Huijaukset ja kalastelut

- Toimitusjohtajahuijaukset ovat taas lisääntyneet, ja niissä on käytetty murrettuja Office 365 -sähköpostitilejä.
- Julkisuuteen nousi suomalaiseen pörssiyritykseen kohdistunut 7 miljoonan euron huijaus.

### IoT ja automaatio

- Internetiin yhdistettävien radiolaitteita koskevat säädökset etenevät hyväksyttäviksi 2020 mennessä.
- ETSI on julkaissut viitekehysmallin IoT-laitteiden turvallisuuden huomiointiin kehitysvaiheessa.

TRAFICOM

# Verkkojen toimivuus

TRAFICOM

# Verkkojen toimivuus

## Merkittäviä toimivuushäiriöitä oli helmikuussa hieman normaalia enemmän

- Merkittäviä häiriöitä oli seitsemän. Yksi häiriö koski koko Suomea ja loput vaikuttivat muutaman kunnan alueella.
- Tammi- ja helmikuussa on ollut yhteensä 15 merkittävää häiriötä.

## Helmikuu oli palvelunestohyökkäysten kannalta rauhallinen

- Saimme muutamia ilmoituksia ns. sovellustason palvelunestohyökkäyksistä, jotka oli toteutettu tekemällä lukuisia HTTP-kyselyitä kohdepalvelimelle.

## LähiTapiola testasi omia palveluitaan palvelunestohyökkäyksiltä suojautumiseksi

- Testi antoi hyvää oppia omien palveluiden suojaamisesta LähiTapiolalle sekä yhteistyökumppaneille.

## Viimeaikaisia trendejä palvelunestohyökkäyksissä

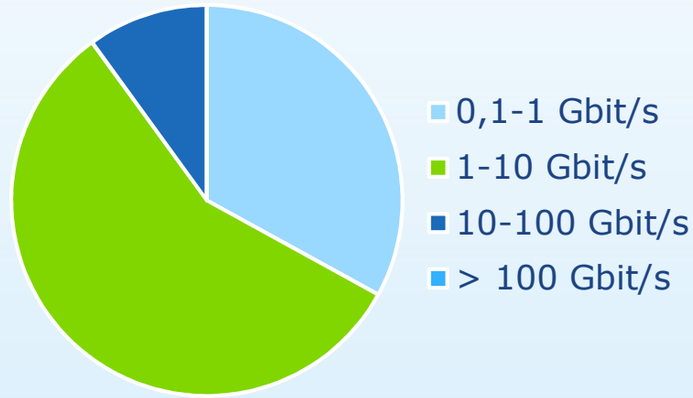
- Internetin avoimia palvelimia hyödyntävien verkkoliikenteen vahvistushyökkäysten lisäksi on muutaman kuukauden tauon jälkeen ilmoitettu myös sovellustason hyökkäyksistä.

# Palvelunestohyökkäykset ja niillä uhkailu

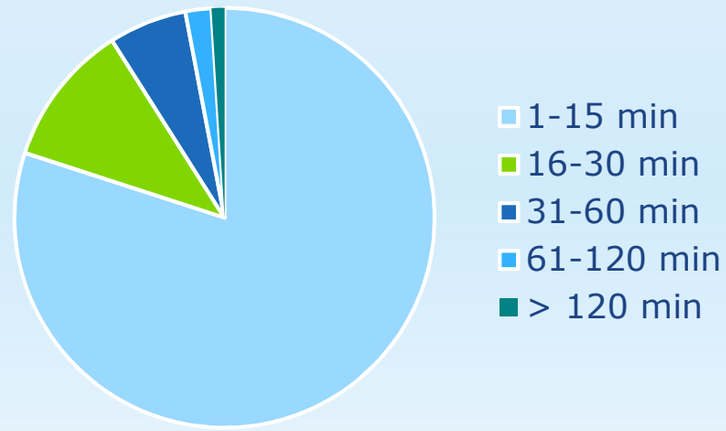
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (80 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 57 % kaikista nähdyistä hyökkäyksistä ovat volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Myös yli 10 Gbit/s hyökkäyksiä nähdään Suomessa useita viikoittain.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Liikenne- ja 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 | n. 89 Gbit/s | n. 37 Gbit/s |
| (kesto 6 min) | (kesto 30 min) | (kesto 8 min) |




Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.




Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

TRAFICOM


Tietomurrot & -vuodot
TRAFICOM

# Tietomurrot & -vuodot

- Kyberturvallisuuskeskus sai useita ilmoituksia murretuista verkkosivuista.
- Ruotsissa on paljastunut tietovuoto, jossa verkkoon avoimesti kytketystä palvelimesta on ollut saatavilla 2,7 miljoonaa puhelutallennetta, jotka sisälsivät ihmisten terveys- ja henkilötietoja.
- Maltalaiseen Bank of Valletta -pankkiin tehtiin tietomurto, jonka avulla siirrettiin noin 13 miljoonaa euroa ulkomaisille tileille.

# Suojautumisohjeita tietomurtojen varalta

- Käytä eri salasanaa jokaisessa palvelussa.
- Säilytä salasanoja turvallisesti.
- Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen vääriin käsiin.
- Käytä monivaiheista tunnistamista, jos käyttämissäsi palveluissa sellainen on mahdollista.

# Haittaohjelmat & haavoittuvuudet

TRAFICOM

# Kyberturvallisuuskeskuksen tekemät haittaohjelmahavainnot

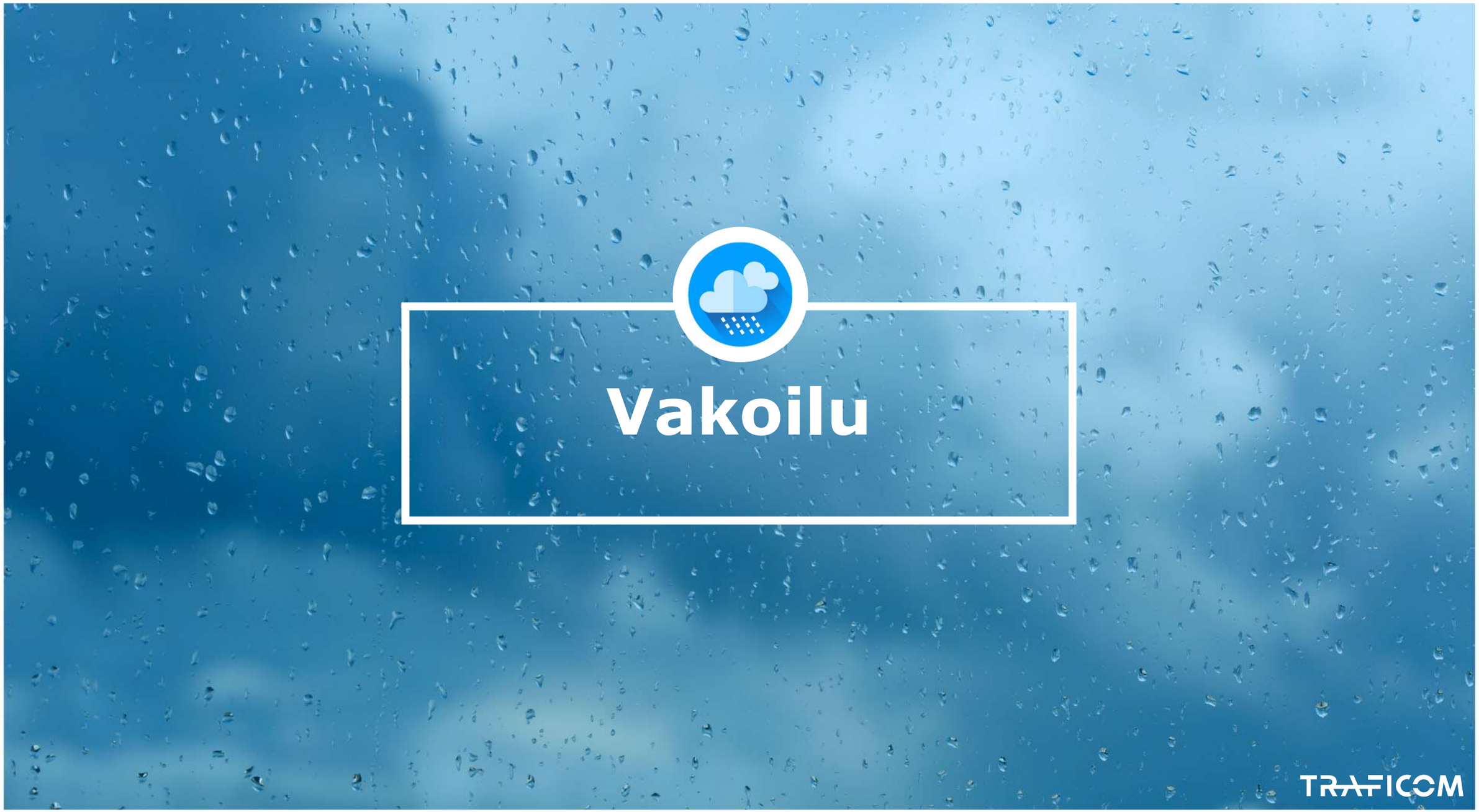
| Haittaohjelmatyyppi | Tilanne | |
|---|---|---|
| IoT-haittaohjelmat | Muodostavat edelleen merkittävän osan Suomessa tehdyistä havainnoista. |  |
| Kiristyshaittaohjelmat | Kiristyshaittaohjelmista ei tehty ilmoituksia helmikuussa Kyberturvallisuuskeskukseen, mutta muutamia tapauksia on havaittu. |  |
| Etähallittavat haittaohjelmat (RAT) | Etähallittavia haittaohjelmia levitetään mm. sähköpostin liitetiedostoina ja myös Kyberturvallisuuskeskuksella on useita havaintoja niistä. |  |
| Louhijat | Ei merkittävää louhija-aktiviteettia. |  |
| Tietoja varastavat haittaohjelmat | Suomessa ei levitetä aktiivisesti käyttäjätunnuksia tai rahaliikenteen välitykseen liittyvien tietojen varastamiseen tähtääviä haittaohjelmia. Tunnuksia kuitenkin kalastetaan aktiivisesti. |  |
| Mobiilihaittaohjelmat | Mobiilihaittaohjelmatapauksia ei ole raportoitu Kyberturvallisuuskeskukseen, mutta niistä on yksittäisiä havaintoja. |  |

# Haittaohjelmat

- Helmikuussa ei tehty merkittäviä haittaohjelmahavaintoja.
- Sähköposti on yleisin kanava levittää haittaohjelmia.
  - Tällä hetkellä suosittua on levittää RAR-pakattua tiedostoa, jonka sisällä on dokumentiksi naamioitu tiedosto, joka todellisuudessa suorittaa haittaohjelman.
  - Tiedosto voi olla joko suoraan sähköpostin liitteenä tai sähköpostissa voi olla linkki esim. Google Docsiin tai vastaavaan pilvipalveluun, jossa tiedosto on ladattavissa.
  - Sähköposti ja sen liitetiedostot ovat olleet yleisin haittaohjelmien levitystapa jo muutaman vuoden ajan.

# Haavoittuvuudet

- Drupal-sisällönhallintaohjelmistossa oli kriittinen haavoittuvuus, jonka avulla järjestelmään pystyi tietyin reunaehdoin murtautumaan.
- WinRAR-pakkausohjelmistossa oli haavoittuvuus, joka mahdollisti haitallisen tiedoston purkamisen hyökkääjän määrittämään kansioon.
  - Haavoittuvuutta on hyödynnetty purkamaan haitallinen tiedosto Windowsin startup-kansioon, josta se suoritetaan seuraavan kirjautumisen yhteydessä.
- Konttiteknologioiden pohjalla käytettävässä runc-työkalussa oli haavoittuvuus, jota hyväksikäyttämällä hyökkääjä pystyy korottamaan oikeuksiaan hallitsemansa kontin sisällä päästen alla lepäävään järjestelmään käsiksi.
- TLS 1.2 -salausprotokollasta löytyi haavoittuvuus, joka mahdollistaa salatun liikenteen osittaisen purkamisen osassa TLS 1.2 -yhteyksissä, mikäli hyökkääjä pystyy muokkaamaan verkkoliikennettä.
  - TLS-protokollan yleisimmät käyttökohteet ovat suojattu verkkoselailu HTTPS-protokollalla, sekä sähköpostiyhteyden salaaminen.
  - Hyökkääjä pystyy onnistuessaan purkamaan salatusta yhteydestä yhden tavun kerrallaan.
- Useiden eri valmistajien PDF-lukijoiden varmenteiden tulkinnassa on ilmennyt haavoittuvuuksia. Haavoittuvuudet mahdollistavat digitaalisesti allekirjoitetun PDF-tiedoston sisällön muokkaamisen ilman, että sovellus varoittaa asiasta.


Vakoilu
TRAFICOM

# Vakoilutilanteessa ajankohtaista

### Kohdistettu hyökkäys ICT-palveluntarjoajan järjestelmiin

Norjalaisen ohjelmistotalon ja ICT-palveluntarjoajan Visman kautta yritettiin tiettävästi päästä käsiksi Visman asiakkaiden tietoihin ja järjestelmiin. Visman tuotteita käytetään yleisesti myös Suomessa.

### Australian parlamentti ja puolueet vakoilun kohteena

Australiassa paljastui parlamenttiin ja merkittäviin poliittisiin puolueisiin kohdistunut vakoilutapaus. Hyökkäys alkoi tiettävästi haitallisen sähköpostin liitetiedoston avaamisesta ja jatkui etenemisellä muihin saman verkon laitteisiin.

### Sharpshooter-kampanjan takana sittenkin Lazarus-ryhmä

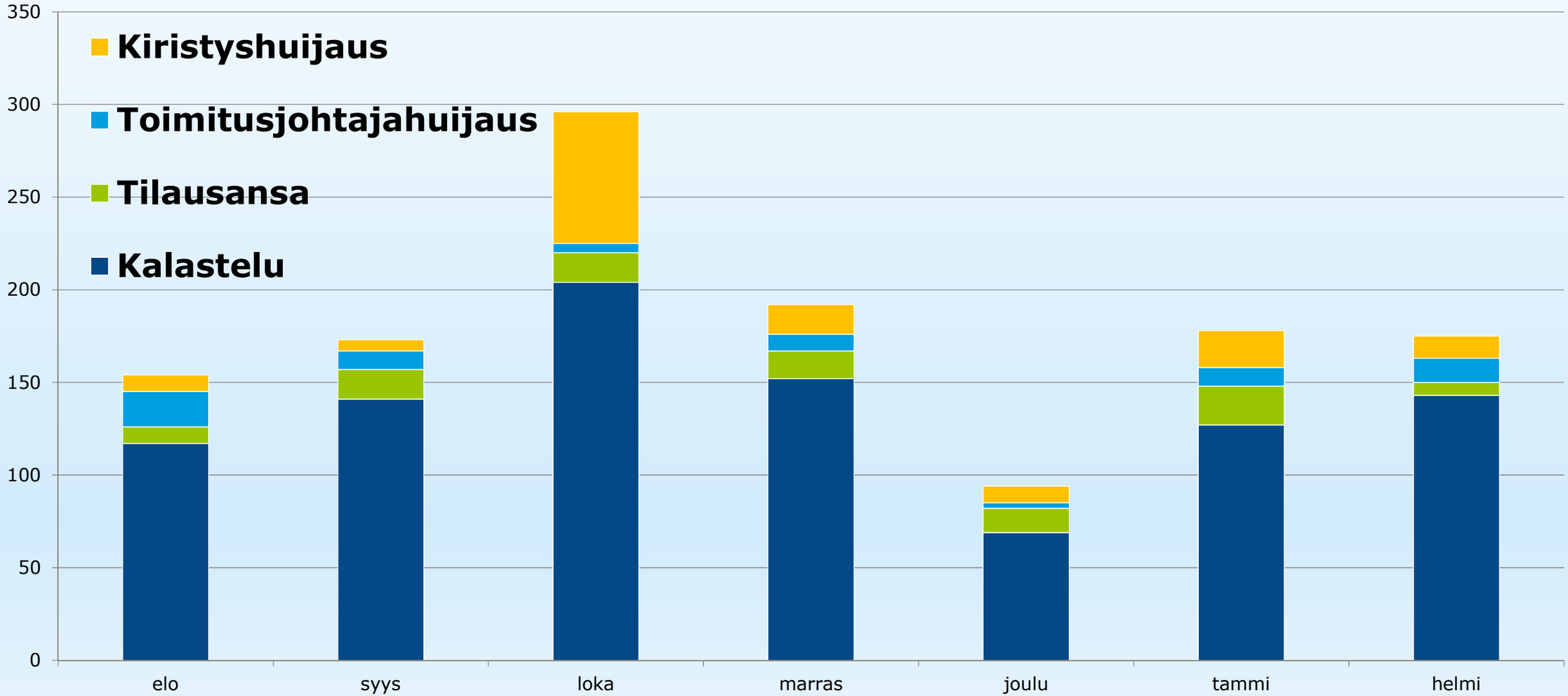
Tietoturvayhtiö McAfeen mukaan vuoden 2018 lopulla julki tulleen haittaohjelmakampanjan taustalla oli sittenkin Pohjois-Koreaan liitetty Lazarus-ryhmä. Aiemmin yhtiö arvioi, että kyse olisi ollut harhautusyrityksestä.


Huijaukset ja kalastelut
TRAFICOM

# Huijaukset ja kalastelut

- Teknologiayhtiö Telesten tytäryhtiön epäillään joutuneen rikoksen kohteeksi. Huijarit saivat mm. identiteettivarkauden avulla Telesten tytäryhtiön siirtämään noin 7 miljoonaa euroa.
- Varoitus Office 365 -palvelun tietomurroista tietojenkalastelun avulla on edelleen aktiivinen. Kalasteluviestien apuvälineinä on käytetty mm. PDF-liitteitä, turvaposteja ja Sharepoint-linkkejä.
  - Rikollisten käyttöön saatuja sähköpostitilejä käytetään aktiivisesti toimitusjohtajahuijauksiin ja laskutuspetoksiin.
- Toimitusjohtajahuijauksia yritetään aktiivisesti kaikenlaisiin organisaatioihin: yritysten lisäksi virastot, julkishallinnon toimijat, yhdistykset, rahastot, säätiöt ja oppilaitokset ovat huijausyritysten kohteina. Huijari esiintyy organisaation johtajana ja pyytää suorittamaan tekaistun maksusuorituksen ulkomaille.
- Sekä suomalaisten että ulkomaisten pankkien nimissä lähetetään edelleen paljon tietojenkalasteluviestejä, joilla pyritään huijaamaan pankkitunnuksia.
  - Säästöpankin nimissä lähetetyt PSD2-direktiiviaiheiset viestit vaikuttavat uskottavilta, mutta niiden linkki johtaa tietojenkalastelusivulle.

# Käsiteltyjä huijaustapauksia 2018/08–2019/02



# IoT ja automaatio

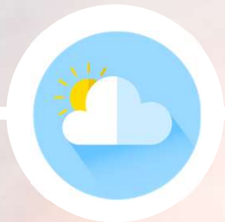
TRAFICOM

# IoT ja automaatio

Internetiin yhdistettävien radiolaitteita koskevat säädökset etenevät hyväksyttäviksi 2020 mennessä.

- Erityissäädös ohjelmistopohjaiset internetiin liitettäviin radioihin lasten suojelemiseksi.
  - Yksityisyyden suoja ja petoksilta suojaaminen /yhdistetyt lelut ja älykellot, keskittyy lasten suojaamiseen, RED 3(3)(e) ja (f)
- Uudelleenkonfiguroitavat radiolaitteet, RED 3(3)(i) ja 4(f) säädös hyväksytään 2020 ensimmäisellä neljänneksellä.

- ETSI on julkaissut viitekehysmallin IoT-laitteiden turvallisuuden huomiointiin kehitysvaiheessa.
  - Tekninen asiakirja luo pohjaa turvalliselle kehittämiselle kattaen useita eri osa-alueita.
  - Myös Kyberturvallisuuskeskus käyttää mallia soveltuvilta osin tulevan IoT-laitteen suositus-merkinnän kanssa.



# Tietoturva-alan kehitys

TRAFICOM

# Sähköinen tunnistus

- Suomessa laajassa käytössä oleva TUPAS-tunnistusprotokolla tulee tiensä päähän.
- Vahvaa sähköistä pankkitunnistusta käyttävät verkkopalvelut tulee päivittää käyttämään uusia, turvallisia protokollia 1.10.2019 mennessä.
- Liikenne- ja viestintäviraston tekemän kyselyn (4.3.2019) mukaisesti luottamusverkoston toimijoiden tarjolla olevat rajapinnat oheisessa taulukossa.
- Lähes kaikki pankit ovat toteuttaneet OpenID Connect –protokollan, joka on myös tuettu kaikkien välityspalveluiden kautta.
- Osa välineiden tarjoajista välittää myös muiden tunnisteita. Ajantasainen lista tästä.

| **Tunnistusvälineen tarjoajat** | Palveluntarjoaja rajapinta | | | |
|---|---|---|---|---|
| | SAML | OIDC | ETSI | Muu |
| Aktia | | x | | Tupas* |
| Danske Bank | | x | | |
| Handelsbanken | | x | | Tupas* |
| Nordea | | x | | |
| Oma Säästöpankki | | x | | Tupas* |
| Osuuspankki | x | | | |
| Pop Pankki | | x | | Tupas* |
| S-Pankki | | x | | |
| Säästöpankki | | x | | Tupas* |
| Ålandsbanken | | x | | |
| | | | | |
| DNA | | x | x | |
| Elisa | | | x | Tupas* |
| Telia | x | x | Rajoitet. | |
| | | | | |
| **Puhtaat välityspalvelut** | | | | |
| | | | | |
| Checkout | | x | | |
| NETS | | x | | SAML 1.1 |
| Signicat | x | x | | |

*) siirtymäaikana

ETSI = natiivi mobiilivarmennerajanpinta

TRAFICOM

# Oikeudelliset asiat (1/2)

- Liikenne- ja viestintäministeriön on käynnistänyt hankkeen sähköisen viestinnän palveluista annetun lain uudistamiseksi
  - ks. https://www.lvm.fi/-/laki-sahkoisen-viestinnan-palveluista-uudistustyon-alle-996625
- Opetus- ja kulttuuriministeriö on julkaissut suositukset tekijänoikeuden kirjevalvontaan
  - ks. https://minedu.fi/tekijanoikeuksien-valvonta
- 1.2.2019 voimaan tullutta lainsäädäntöä:
  - Laki tiedustelutoiminnan valvonnasta (121/2019)
    - Lailla järjestetään siviili- ja sotilastiedustelun laillisuusvalvonta sekä säädetään eräistä parlamentaarisen valvonnan yksityiskohdista
  - Laki sähköisen viestinnän palveluista annetun lain muuttamisesta (52/2019) ja laki julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain muuttamisesta (53/2019)
    - Mahdollistetaan laajakaistainen viranomaisviestintäpalvelu, jolla korvataan nykyinen viranomaisradioverkkoon perustuva kapeakaistainen viranomaisviestintäpalvelu
- Vahvistetut lait:
  - Laki rajavartiolain muuttamisesta (9/2019) ym.
    - Lakimuutoksella mm. annetaan rajavartiomiehelle oikeus puuttua miehittämättömän ilma-aluksen ja lennokin lennätykseen tarvittaessa voimakeinoja tai teknisiä toimenpiteitä käyttäen; voimaan 1.4.2019
- Valiokuntakäsittely päättynyt:
  - Hallituksen esitykset siviili- sotilastiedustelua koskeviksi lainsäädännöiksi (HE 202/2017 ja HE 203/2017) ja tunnistus- ja luottamuspalvelua koskevan lain muuttamiseksi (HE 264/2018); ks. lisää www.eduskunta.fi

# Oikeudelliset asiat (2/2)

- Valiokuntakäsittelyssä ollut mm.:
  - Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi (HaVM362018 vp HE 202/2017 vp)
  - Hallituksen esitys kansallisen turvallisuuden huomioon ottamista alueiden käytössä ja kiinteistönomistuksissa koskevaksi lainsäädännöksi (HE 253/2018)
  - Valtioneuvoston selonteko tietopolitiikasta ja tekoälystä (VNS 7/2018)
  - Hallituksen esitys laeiksi vankeuslain ja tutkintavankeuslain, pakkokeinolain ja rikoslain 6 luvun 13 §:n muuttamisesta (HE 222/2018)
  - Hallituksen esitys laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta (HE 264/2018)
  - Hallituksen esitys laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi (HE 284/2018)
  - Valtioneuvoston selvitys: Eurooppalainen lähestymistapa disinformaation torjuntaan verkossa (E 39/2018 vp – E-jatkokirje 31/2018 vp)
  - Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta (U 102/2018 vp)
  - Hallituksen esitys laiksi sähköisen viestinnän palveluista annetun lain 304 §:n muuttamisesta (HE 318/2018, "datan vapaa liikkuvuus")

# Kyberuutisointia maailmalta

Useat Euroopan maat ovat raportoineet ulkomaisten toimijoiden tekemästä vaikuttamisesta kansallisissa vaaleissa viime vuosina. Mm. Ruotsi, Bulgaria ja Moldova ovat raportoineet kyberhyökkäyksistä vaalijärjestelmiinsä. Muun muassa Bulgaria on ilmaissut huolensa Europarlamenttivaaleihin kohdistuvasta kybervaikuttamisen uhkasta.

YK:n alainen siviili-ilmailujärjestö ICAO kertoo olleensa kyberhyökkäyksen kohteena. Organisaatio peitteli tapahtunutta kuukausien ajan yrittäen selvittää tilannetta, samaan aikaan levittäen palvelimiltaan haittaohjelmaa lentoteollisuuden keskuudessa. Ongelman laajuutta selvitetään.

Huaweihin liittyvät riskit puhututtavat laajasti. Useat länsimaat, kuten Tšekki, ovat asettaneet rajoituksia Huawein käytölle maan kriittisessä infrastruktuurissa, mutta esimerkiksi Britanniassa asiaa pohditaan laajemmin. Korkean tason asiantuntijat haluaisivat tuoda keskusteluun tutkimustulosten puuttumisen Huawein epäillystä vakoilusta Kiinan hyväksi.

Venäjä valmistelee eristäytymistä muusta internetistä. Suvereeniksi internetiksi kutsuttu lakimuutos on viety Venäjän parlamentin alahuoneeseen, jossa sen oletetaan menevän läpi. Lain myötä Venäjällä pystytään tehokkaammin estämään kielletyillä sivuilla vierailu, sekä sulkemaan epäkunnioittavaa ja virheellistä tietoa julkaisevia sivustoja.

TRAFICOM

Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi

TRAFICOM