Maaliskuu | 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 varastetaan edelleen. Varoitus aiheesta on ollut voimassa kesästä 2018. Kyberturvallisuuskeskus julkaisi huhtikuun alussa oppaan Office 365 -tuotteiden tietoturvaominaisuuksista, joiden käyttöä suositellaan.

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.

Käyttäjätunnuksia ja salasanoja kalastellaan sähköpostitse ja huijaussivujen avulla. Yksi viimeaikainen menetelmä on ollut toimittaa kalastelulinkki pdf-liitetiedoston sisällä. Monivaiheinen tunnistaminen (MFA) voidaan myös ohittaa, jos Office 365 on asetettu tukemaan kirjautumista myös vanhoilla sovelluksilla (ns. legacy support).

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

Julkaisimme oppaan uhkan torjumiseksi: https://www.kyberturvallisuuskeskus.fi/fi/node/2532

TRAFICOM

Top 5 -kyberuhat

1

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdistetuissa hyökkäyksissä ja vakoilussa.

2

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Tietoturvan laiminlyönnit altistavat esimerkiksi häiriöille.

3

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

4

Edistyneemmät rikollisryhmät etsivät kohteikseen isoja organisaatioita, joiden toimintaa haittaamalla voidaan yrittää kiristää huomattavia summia rahaa.

5

Puutteellinen elinkaaren- ja lokienhallinta heikentää organisaatioiden kykyä havaita ja reagoida poikkeamiin.

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

TRAFICOM

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Ilmoituskynnyksen madaltuminen tietoturva-asioissa ja varmuuden vuoksi ilmoittaminen kehittää varautumista ja parantaa tietoturvaa.

2. Ylen Docstop: Team Whack -dokumenttisarja tuo tietoturvan lähelle arkea ja avaa aihetta ymmärrettävällä tavalla.

3. Varautuminen palvelunestohyökkäyksiin on parantunut, eikä niillä saada näkyviä vaikutuksia aikaa yhtä helposti.

Tietoturvan kehitystarpeet

1. Tietomurtojen ja -vuotojen taustalta löytyy usein yksinkertaisia syitä ja helposti paikattavia puutteita, eli perusta ei useinkaan ole kunnossa.

2. Tietojenkalastelu koskettaa kaikkia ja on jatkuvaa: siihen pitää varautua niin yritysmaailmassa, tutkimus- ja oppilaitoksissa kuin julkishallinnossakin.

3. Tietoturvaan liittyvässä vastuunjaossa on usein puutteita tai roolit eivät ole kaikille osapuolille selvät.

TRAFICOM

Kybersää maaliskuu 2019

Verkkojen toimivuus

- Toimivuushäiriöiden määrä väheni tammi-helmikuuhun verrattuna.
- Useissa Euroopan maissa on havaittu palvelunestohyökkäyksiä, joiden tarkoituksena oli vaalihäirintä.
- Kotimaassa palvelunestohyökkäysten tilanne oli rauhallinen.

Tietomurrot & -vuodot

- Norsk Hydroon kohdistunut tietomurto aiheutti suuret taloudelliset tappiot.
- Kalasteltuja tunnuksia (esim. Office 365) käytetään usein nopeasti tietomurroissa.

Haittaohjelmat & haavoittuvuudet

- Paljon kriittisiä haavoittuvuuksia päivitettäväksi.
- Ransomware-toiminta kehittyy.

Vakoilu

- Myös laitevalmistajia hyödynnetään toimitusketjuhyökkäyksissä.
- Suojelupoliisin tietoon tuli vuonna 2018 useita verkkovakoilutapauksia, joiden taustalla on todennäköisesti ollut valtiollinen taho.

Huijaukset ja kalastelut

- Tietojenkalasteluun on räätälöity entistä uskottavampia portaaleja.
- Toimitusjohtajahuijaukset ovat taas nousussa, ja niissä on käytetty murrettuja Office 365 -sähköpostitilejä.

IoT ja automaatio

- 20 % ICS-laitteiden haavoittuvuuksista on kriittisiä.
- Fidelixin taloautomaatiojärjestelmissä haavoittuvuuksia, Aiheetta käsitelty YLE:n Docstop: Team Whack –ohjelmassa.
- Suomessa paljon julkiseen internetiin näkyviä IoT-laitteita.


Verkkojen
toimivuus
TRAFICOM

Verkkojen toimivuus

Maaliskuussa toimivuushäiriöiden määrä laski

- Tammi- ja helmikuussa yleisissä viestintäpalveluissa oli tavanomaista enemmän toimivuushäiriöitä.

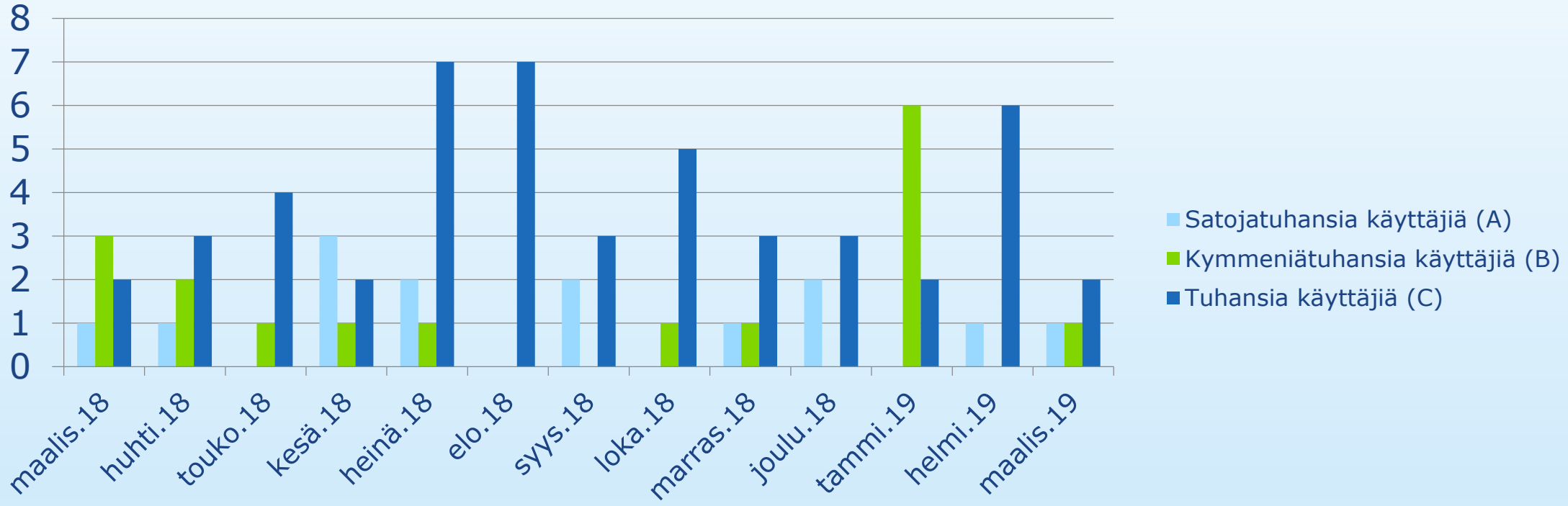
Maaliskuu oli palvelunestohyökkäysten osalta rauhallinen

- Kyberturvallisuuskeskukseen raportoitiin vain muutamasta palvelunestohyökkäyksestä.

Tulevat eduskunta- ja europarlamenttivaalit saattavat olla palvelunestohyökkäysten kohteena

- Useissa eurooppalaisissa maissa on vaalien yhteydessä nähty palvelunestohyökkäyksiä, joilla on pyritty häiritsemään mm. tulospalvelun tai puolueiden verkkosivujen toimintaa.

Merkittävien toimivuushäiriöiden määrä kuukausittain



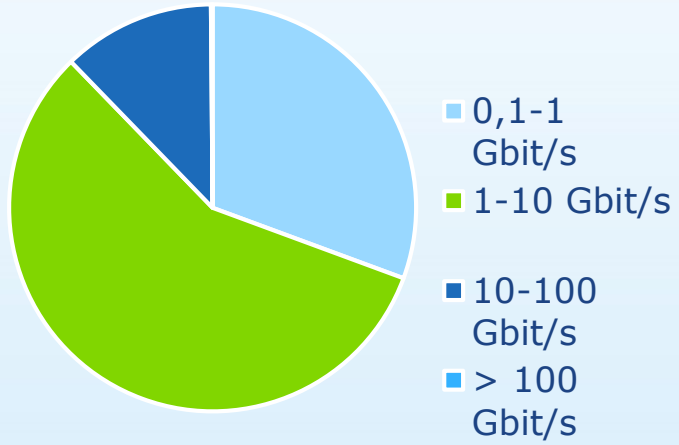
Tässä tilastossa on esitetty ainoastaan merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Teleyritykset korjaavat satoja pieniä toimivuushäiriöitä päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta vuodessa. Niiden määrä riippuu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

Palvelunestohyökkäykset ja niillä uhkailu

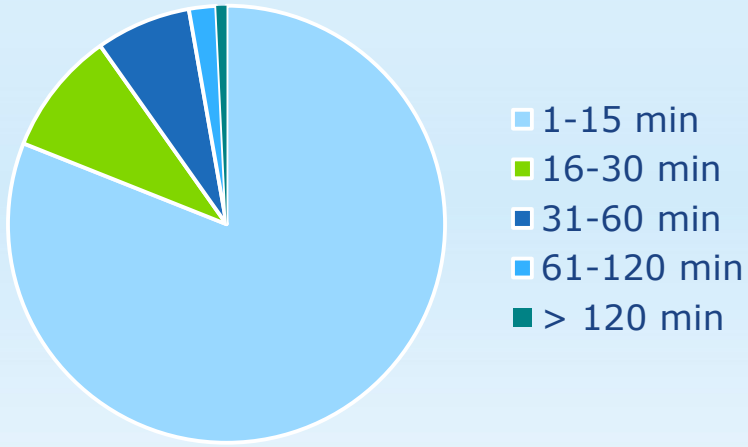
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (80 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 57 % kaikista nähdyistä hyökkäyksistä ovat volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 10 Gbit/s hyökkäysten osuus on kasvanut vuoden 2018 puolivälistä alkaen, ja niitä nähdään Suomessa jo päivittäin.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Viestintävirastoon ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

2019/Q1:	2018/Q4:	2018/Q3:
n. 162 Gbit/s (kesto 9 min)	n. 45 Gbit/s (kesto 6 min)	n. 89 Gbit/s (kesto 30 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.


Tietomurrot & -vuodot
TRAFICOM

Tietomurrot & -vuodot

- Office 365:n ja muiden pilvipalveluiden esimerkiksi kalastelulla haltuun saatuja tunnuksia käytetään tietomurroissa nopeasti tunnusten saamisen jälkeen.
- Maailmalla on ollut useita teollisuusyrityksiin kohdistuneita tietomurtoja.
  - Murtojen yhteydessä on käytetty varsin yleisiä tunkeutumistyökaluja, joiden avulla kohteeseen on asennettu kiristyshaittaohjelmia.
  - Tietomurrot ovat ns. Big Game Hunting toimintaa, jossa etsitään suuria toimijoita esimerkiksi kiristyksen kohteiksi. Norsk Hydro on tästä tunnetuimpana esimerkkinä.
- Avoimien etätyöpöytäyhteyksien (esim. RDP) käyttö tietomurroissa on yleistynyt. Murroissa hyödynnetään haltuun saatuja tunnuksia.
- Taloyhtio.info ja Tallier.info joutuivat tietomurron kohteeksi. Mahdollista tietovuotoa ja sen laajuutta selvitetään parhaillaan.

Suojautumisohjeita tietomurtojen varalta

- Käytä eri salasanaa jokaisessa palvelussa.
- Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot
- 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 merkittävän osan Suomessa tehdyistä havainnoista.	
Kiristyshaittaohjelmat	Kiristyshaittaohjelmahavainnot ovat vähentyneet, mutta on edelleen yksittäisiä havaintoja palvelinten tietoja salanneesta haittaohjelmasta.	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia on raportoitu muutamia tapauksia.	
Louhijat	Ei merkittävää louhija-aktiviteettia.	
Tietoja varastavat haittaohjelmat	Suomessa ei levitetä aktiivisesti käyttäjätunnuksia tai rahaliikenteen välitykseen liittyvien tietojen varastamiseen tähtääviä haittaohjelmia. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti.	
Mobiilihaittaohjelmat	Mobiilihaittaohjelmatapauksista on havaintoja.	

Haittaohjelmat

- Haitallista sisältöä sähköpostiliitteissä ja jaetuissa linkeissä.
- Aiemmin vähenemään päin ollut kiristyshaittaohjelmabisnes on löytänyt uusia muotoja:
  - "Big Game Hunting": Organisaation sisälle tunkeudutaan haavoittuvuuksien avulla ja pyritään levittämään haittaohjelmaa Active Directory:n (AD) avulla laajalle organisaatiossa.
  - Kiristyshaittaohjelmien leviäminen on tehostunut, ja niiden mukana tulee salasanoja varastavia ohjelmia.
  - Julkisuudessa olleen tiedon perusteella uhrit ovat maksaneet lunnaita enemmän kuin aiemmin, joten rikollinen liiketoiminta on kasvussa.
  - LockerGoga-kiristyshaittaohjelmasta useita havaintoja maailmalla.
- Uutisotsikoihin viittaavissa roskapostituskampanjoissa ohjataan vastaanottajia haittaohjelman sisältäviin linkkeihin.

Haavoittuvuudet

- Viime kuussa julkaistua WinRAR-pakkausohjelmiston haavoittuvuutta käytetään laajalti hyväksi eri kampanjoissa.
- Maaliskuun aikana on julkaistu paljon päivityksiä kriittisiin haavoittuvuuksiin eri ohjelmistoissa.
- Tutkijat löysivät uusia haavoittuvuuksia LTE-ympäristöistä.
  - Haavoittuvuuksia hyödyntämällä voidaan mm. estää palvelun saatavuus käyttäjiltä, väärentää tekstiviestejä tai vakoilla ja muuttaa tietoliikennettä.
- Google Chromen ja Microsoftin nollapäivähaavoittuvuuksia käytettiin yhdessä laajalti hyväksi. (CVE-2019-5786)
- Sveitsiläisestä online-äänestysjärjestelmästä löydettyä haavoittuvuutta hyödyntämällä voi yksi henkilö väärentää koko vaalituloksen.
- Useita kriittisiä haavoittuvuuksia Magento-verkkokauppa-alustassa, johon on saatavilla päivitykset. Lisätietoja: Haavoittuvuus 6/2019

Vakoilu

TRAFICOM

Vakoilutilanteessa ajankohtaista

Verkkovakoilu voi kohdistua myös kohdetta lähellä oleviin tahoihin

Suojelupoliisin kertoo vuosikirjassaan, että sen tietoon tuli vuonna 2018 useita verkkovakoilutapauksia, joiden taustalla on todennäköisesti ollut valtiollinen taho. Kohteina ovat olleet niin Suomen valtio kuin yritykset ja yksityishenkilötkin.

ASUS haittaohjelmalevityksen välikappaleena

Tietokonevalmistaja ASUSin päivityksiä jakelevan palvelimen kautta takaoven sisältävää ohjelmistoversiota arviolta puoleen miljoonaan laitteeseen. Hyökkääjät olivat kuitenkin kiinnostuneita vain noin 600 tunnistettiin MAC-osoitteiden perusteella ja joihin ladattiin toinen ha

Espanjan puolustusministeriö vakoilun kohteena

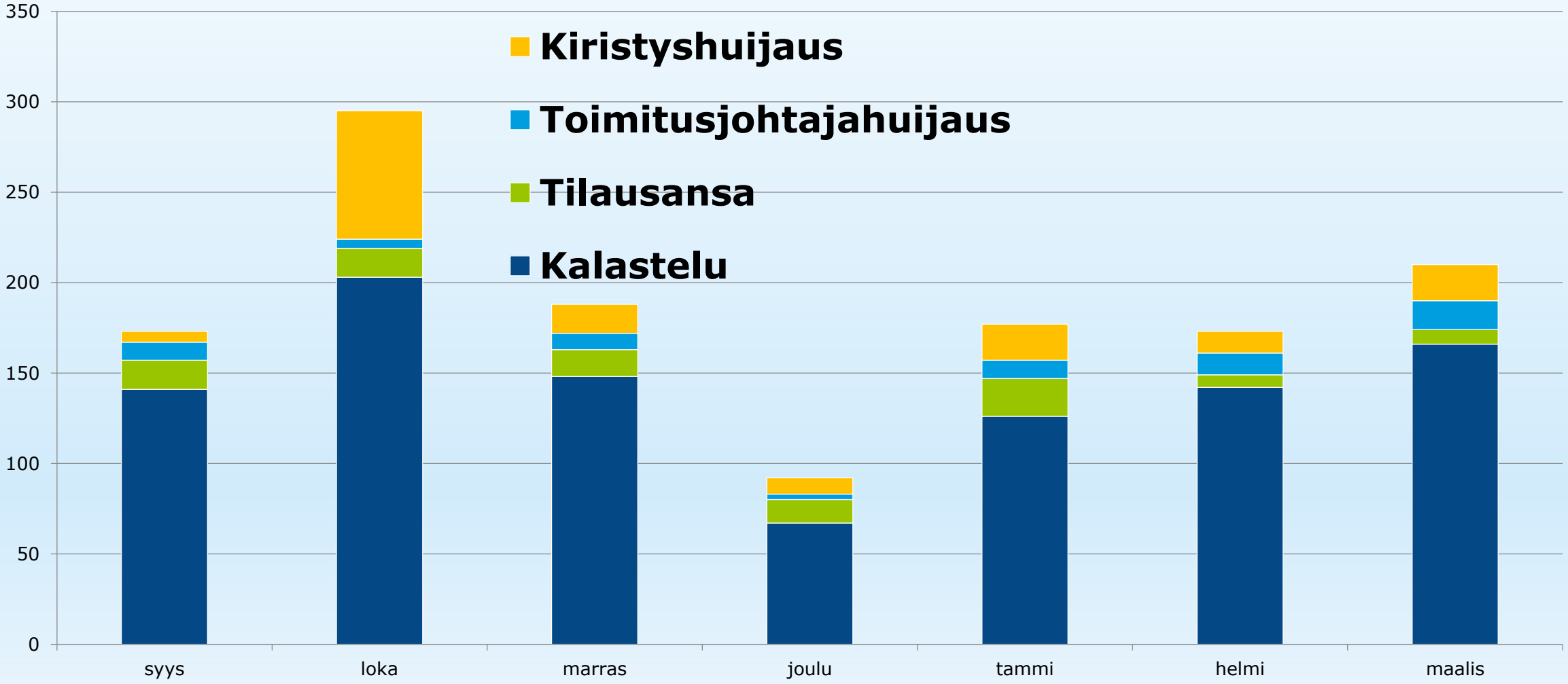
Espanjan puolustusministeriön verkossa havaittiin tietoa varastava haittaohjel Lehtitietojen mukaan haittaohjelman tavoitteena olisi ollut puolustusteknologi liittyvien tietojen varastaminen. Taustalla on epäilty olevan valtiollinen toimija


Huijaukset ja kalastelut
TRAFICOM

Huijaukset ja kalastelut

- Varoitus Office 365 -palvelun tietomurroista tietojenkalastelun avulla on edelleen aktiivinen. Viime aikoina kalasteluviesteissä on käytetty vilpillisiä Sharepoint-linkkejä ja eri tiedostonjakopalveluita.
  - Kyberturvallisuuskeskukselle raportoitiin maaliskuussa 50 tietojenkalastelun yritystä, 25 onnistunutta tietomurtoa ja 6 murretulla sähköpostitilillä tehtyä huijausta.
- Toimitusjohtajahuijaukset kohdistuvat kaikenlaisiin organisaatioihin kansainvälisistä pörssiyrityksistä pieniin kansalaisjärjestöihin. Maaliskuussa myös ministeriöt ja virastot ovat olleet laskuhuijausten kohteina.
- Yliopistojen ja tiedeyhteisöjen käyttäjätunnuksia kalastellaan suhteellisen paljon. Pääsy akateemisiin palveluihin on joissakin maissa virallisesti hankalaa, joten tunnuksilla on kysyntää pimeillä markkinoilla.
- Eri pankkien nimissä on jälleen lähetetty suuri määrä tietojenkalasteluviestejä, joilla rikolliset yrittävät saada haltuunsa pankkitunnuksia.
  - Kyberturvallisuuskeskus poisti verkosta 21 kalastelukampanjaan liittyvää verkkosivua.
  - Säästöpankin nimissä huijataan entistä uskottavammilla PSD2-direktiiviaiheisilla viesteillä.
- Apple ID -tunnusten kalastelu kääntyi alkuvuodesta taas nousuun.
- Sähköpostilla ja tekstiviesteillä on lähetetty linkkejä tilausansoihin, joissa kuluttajia houkutellaan Lidl:n lahjakortilla. Myös virtuaalivaluutta-aiheinen huijauskampanjointi on runsasta.

Käsiteltyjä huijaustapauksia 2018/09–2019/03



IoT ja automaatio

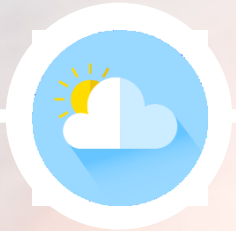
TRAFICOM

IoT ja automaatio

- 20 prosentissa teollisuusautomaatiolaitteista on kriittisiä haavoittuvuuksia.
  - Yli puolet teollisuusautomaatiojärjestelmistä löydetyistä haavoittuvuuksista arvioitiin vakaviksi tai kriittisiksi.

- Fidelixin taloautomaatiojärjestelmissä löydetty ja korjattu haavoittuvuuksia. Tapaus esitelty myös Ylen Docstop: Team Whack –ohjelmassa.

- Suomessa näkyy paljon kuluttajien IoT-laitteita, jotka on kytketty julkiseen internetiin.
  - Monien laitteiden huonon tietoturvan vuoksi niitä voidaan hyödyntää esimerkiksi palvelunestohyökkäyksiin, roskapostin lähettämiseen tai muuhun rötöstelyyn.
  - Esimerkki väärinkäytöstä Yhdysvalloissa: https://www.bitdefender.com/box/blog/iot-news/8-year-old-scared-death-hacked-nest-security-camera-warns-missile-attack/
  - Kannattaa estää internetistä tulevat yhteydenotot esimerkiksi kotireitittimen palomuuritoiminnolla. Kysy ohjeita internetpalveluntarjoajaltasi.



Tietoturva-alan kehitys

TRAFICOM

Oikeudelliset asiat – EU ja Eurooppa

- EU:n parlamentti on hyväksynyt ns. EU:n kyberturvallisuusasetuksen, joka etenee seuraavaksi neuvoston hyväksyttäväksi
  - http://www.europarl.europa.eu/news/fi/press-room/20190307IPR30694/ep-hyvaksyi-eu-n-kyberturvallisuuslain-ja-puuttuu-kiinan-teknologiauhkaan

- Euroopan tietosuojaneuvosto on lausunut mm. yleisen tietosuoja-asetuksen ja sähköisen viestinnän tietosuojalainsäädännön yhteensovittamisesta
  - https://tietosuoja.fi/artikkeli/-/asset_publisher/sahkoisen-viestinnan-tietosuojalainsaadanto-ja-vaalivaikuttaminen-euroopan-tietosuojaneuvoston-taysistunnon-teemoina

- EU:n komission on antanut suosituksen energia-alan kyberturvallisuudesta (EU) 2019/553
  - https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32019H0553&from=FI

- EU:n komissio on antanut radiolaitedirektiiviä täydentävän delegoidun asetuksen, joka koskee älypuhelimista hätäviestin mukana toimitettavien sijaintitietojen saataville asettamista
  - https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1554725962519&uri=CELEX:32019R0320

Oikeudelliset asiat – kotimaa

- Hyväksyttyjä lakeja
    - Eduskunta on hyväksynyt lain sotilastiedustelusta, lain tietoliikennetiedustelusta siviilitiedustelussa sekä niihin liittyvät lait.
    - Eduskunta on hyväksynyt lain julkisen hallinnon tiedonhallinnasta sekä siihen liittyvät lait.
- Säädöskokoelmassa julkaistuja
    - Laki sähköisen viestinnän palveluista annetun lain 304 §:n muuttamisesta (350/2019), voimaan 1.5.2019
        - datan vapaata liikkuvuutta tukevat viranomaistehtävät
    - Laki digitaalisten palvelujen tarjoamisesta (306/2019, ns. saavutettavuuslaki), voimaan 1.4.2019
        - laki koskee myös vahvan sähköisen tunnistuspalvelun tarjoajaa (3.1 §)
    - Laki Digi- ja väestötietovirastosta (304/2019), voimaan 1.1.2020
    - Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) muutokset (412/2019), voimaan 1.4.2019
        - https://www.lvm.fi/-/vahvaa-sahkoista-tunnistamista-koskevat-lakimuutokset-voimaan-1003082
- Muuta
    - Sähköisen viestinnän palveluista annetun lain kokonaisuudistus etenee.
        - Katso tallenne seurantaryhmän 1. kokouksesta -> https://www.youtube.com/watch?v=dyAx_r11iB0
    - Liikenne- ja viestintävirasto on tehnyt tulkintakannanoton ajokortin käytöstä tunnistusvälineen uusimis-, korvaamis- ja uudelleenaktivointitilanteissa (dnro Traficom/106/09.02.00/201, 25.3.2019).
    - Suomen kyberturvallisuusstrategia 2019 on ollut lausuttavana -> https://www.lausuntopalvelu.fi (suljetut)
    - Suojelupoliisin vuosikirjassa 2018 käsitellään mm. kybervakoilua -> https://www.supo.fi/julkaisut/esitteet

Kyberasioihin liittyvää uutisointia maailmalta

Suomi allekirjoitti aiejulistuksen nopean toiminnan kyberjoukkoihin osallistumisesta.

- Aiejulistuksen allekirjoitti puolustusministeri Jussi Niinistö työvierailullaan Liettuaan.
- Aiejulistuksen on allekirjoittanut seitsemän joukkoihin osallistuvaa, ja kuusi tarkkailijamaina osallistuvaa EU-maata.

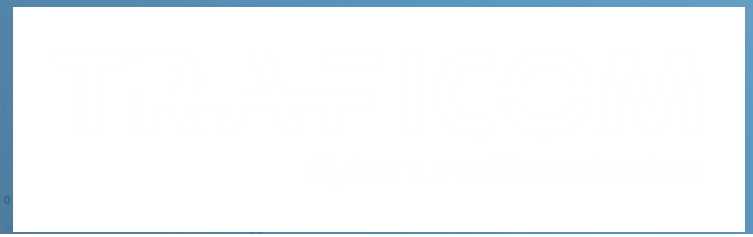
Ruotsi kehittää hyökkäyksellistä kyberkyvykkyyttä.

- Asiasta kertoo Ruotsin armeijan komentaja.
- Hyökkäyksiä harjoitellaan erillisessä harjoitusympäristössä.
- Kyberhyökkäysten harjoittelu on herättänyt kuitenkin keskustelua, sillä niiden tekeminen on lähtökohtaisesti laitonta.

Viron ulkomaantiedustelu julkaisi vuosikatsauksensa

- Katsaus käsittelee isolta osin Venäjää.
- Ulkomaantiedustelu arvioi, että europarlamenttivaalit ovat todennäköinen Venäjän vaikuttamisen kohde.
- Lisäksi katsauksessa linkitetään useita vuoden 2018 aikana julki tulleita kohdistettuja kyberhyökkäyksiä Venäjään.

TRAFICOM



www.kyberturvallisuuskeskus.fi

TRAFICOM