TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 2019

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

rauhallinen

huolestuttava

vakava

Kybersää syyskuu 2019

Verkkojen toimivuus

- Merkittävien toimivuushäiriöiden määrä yli kaksinkertaistui
- Erica- ja Apotti-järjestelmät kärsineet viestiliikenteen häiriöistä
- Osa sovellustason palvelunesto-hyökkäyksistä on vaikeampi torjua

Vakoilu

- Ilmailusektorista kiinnostunut teollisuusvakoiluryhmä hyödyntää yritysten tärkeitä kumppaneita murtautumisessa.
- Haavoittuvat etäyhteysratkaisut ovat kiinnostava kohde valtiollisille toimijoille.

Haittaohjelmat ja haavoittuvuudet

- Haavoittuvien Microsoftin etätyöpöytä-sovelluksien hyväksikäyttöön on julkaistu helppokäyttöinen työkalu
- Sähköpostitse on jaettu erityisesti tietoja varastavia ja etäkäytön mahdollistavia haittaohjelmia.

Tietomurrot ja -vuodot

- Murrettuja verkkosivustoja käytetty kalastelusivujen ylläpitoon.
- Yksityisen henkilön Facebook-tilin haltuun saaminen mahdollisti yrityksen nimissä esiintymisen Facebookissa.

Huijaukset ja kalastelut

- Kaksi laajaa SMS-tilausansahuijauskampanjaa
- FBI:n koordinoima kansainvälinen verkkohuijareiden pidätysoperaatio

IoT ja automaatio

- 5G Cyber Security Hackathon Oulussa 29.11-1.12.2019.
- Satori Botnetin operaattori tunnustanut syyllisyytensä.
- IoT-verkoston tapahtuma Traficomilla 12.11, aiheina Asumisen IoT ja Tietoturvamerkki.

Varoitus 02/2019: Windows RDS:n haavoittuvuuksia hyödynnetään tietomurroissa

Windows-käyttöjärjestelmän Remote Desktop Service -toteutuksesta (RDS, etätyöpöytäsovellus) on löytynyt useita kriittisiä haavoittuvuuksia. Haavoittuvuudet mahdollistavat **matomaisesti leviävien haittaohjelmien** toteuttamisen. Havaintoja haavoittuvuuksien hyödyntämisestä on tehty sekä Suomessa että ulkomailla.

Varoitus koskee Windows-palvelinten ja -työasemien **ylläpitäjiä** sekä organisaatioita, jotka käyttävät etätyöpöytäpalvelua. Ylläpitäjien tulee asentaa Windowsin **ohjelmistopäivitykset** viipymättä tai rajoittaa haavoittuvuuksien käyttömahdollisuuksia muilla keinoin.

Microsoft on julkaissut RDS-toteutusta koskevia tietoturvapäivityksiä: BlueKeep-haavoittuvuus korjattiin jo toukokuun 2019 käyttöjärjestelmäpäivitysten yhteydessä. Elokuun tietoturvapäivitysten yhteydessä korjattiin kaksi uutta kriittistä haavoittuvuutta RDS-toteutuksesta.

Julkaisimme varoituksen 14.8.2019. **Varoitus poistettiin** 8.10., mutta uhka ei suinkaan ole kokonaan poistunut:

https://www.kyberturvallisuuskeskus.fi/fi/microsoftin-etatyopoyta-sovelluksen-haavoittuvuuksia-hyodynnetaan-tietomurroissa

Julkaisuhetkellä Suomessa oli noin 4500 haavoittuvaa järjestelmää avoinna internetiin.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

2

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

3

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Oulussa järjestetään maailman ensimmäinen 5G-Hackathon, jossa valkohattuhakkerit kohentavat tietoturvaa.

2. Kyberturvallisuuskeskus julkaisi harjoitusoppaan yhdessä Huoltovarmuuskeskuksen kanssa.

3. Varajärjestelmien säännöllinen testaaminen ja käytön harjoittelu auttaa varautumaan odottamattomiin vikatilanteisiin.

Tietoturvan kehitystarpeet

1. Pitkään tiedossa olevien haavoittuvuuksien korjaamatta jättäminen lisää hyväksikäytön riskiä.

2. Tietojärjestelmien häiriöitä aiheutuu laite- ja ohjelmistovioista, sekä erityisesti huolto- ja korjaustöiden yhteydessä tapahtuneista odottamattomista vikatilanteista.

3. Tekstiviestit yleistyvät huijausten ja tilausansojen välineinä. Lähettäjätiedot on helppo väärentää uskottavan näköiseksi.

Verkkojen toimivuus

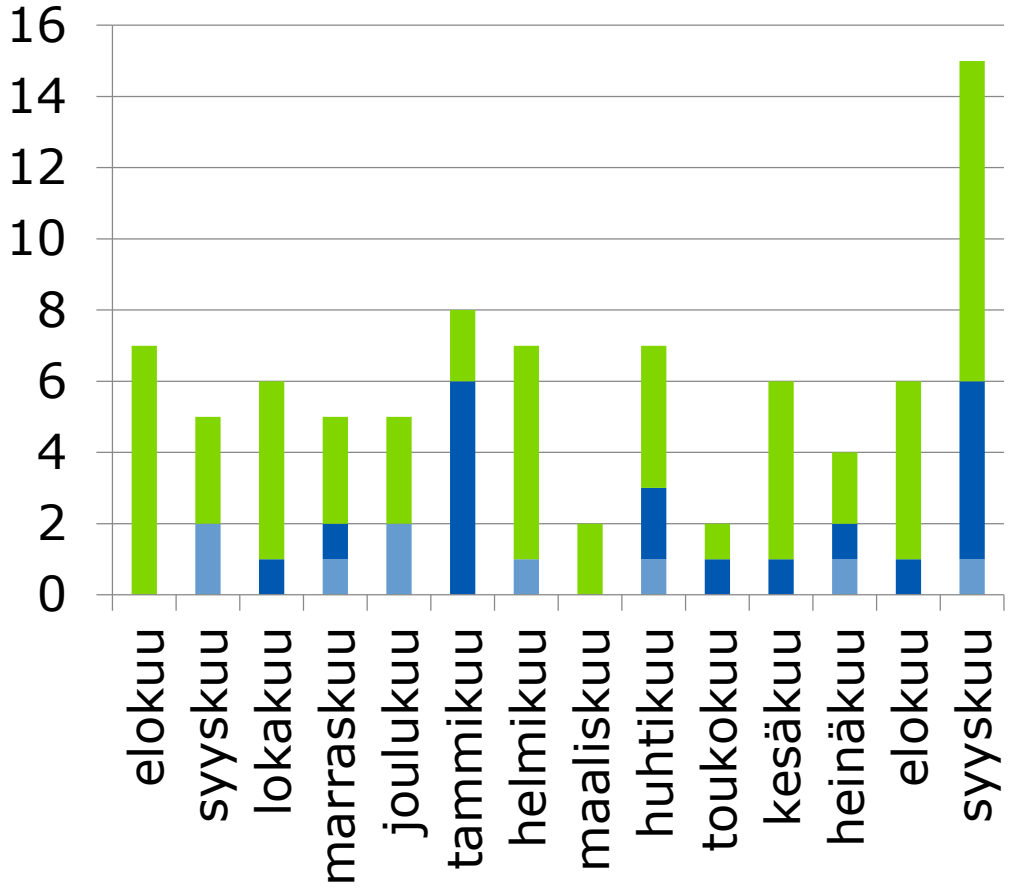
Verkkojen toimivuus

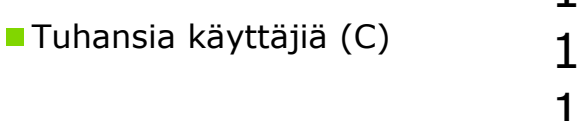
- Yleisten viestintäpalveluiden merkittävien toimivuushäiriöiden määrä kasvoi selvästi syyskuussa.
  - Syyskuussa oli 15 merkittävää häiriötä. Tyypillisesti niitä on ollut 6 kappaletta kuukaudessa.
  - Häiriöiden syissä korostuivat laite- ja ohjelmistoviat, sekä erityisesti huolto- ja korjaustöiden yhteydessä tapahtuneet odottamattomat vikatilanteet.
  - Myös varajärjestelmien toimimattomuus johti useaan häiriötilanteeseen
- Hätäkeskusjärjestelmä Erica on toistuvasti kärsinyt verkkoliikenteen häiriöistä
  - https://www.112.fi/ajankohtaista/uutiset/2/0/hatakeskuslaitos_tarkentaa_ylen_uutisointia_-_yhteysongelmat_johtuvat_valtion_turvallisuusverkosta_78333
- Potilastietojärjestelmä Apotti Vantaalla päivän ajan poissa käytöstä tietoliikennekuidun katkettua
  - https://www.hs.fi/kaupunki/art-2000006252723.html

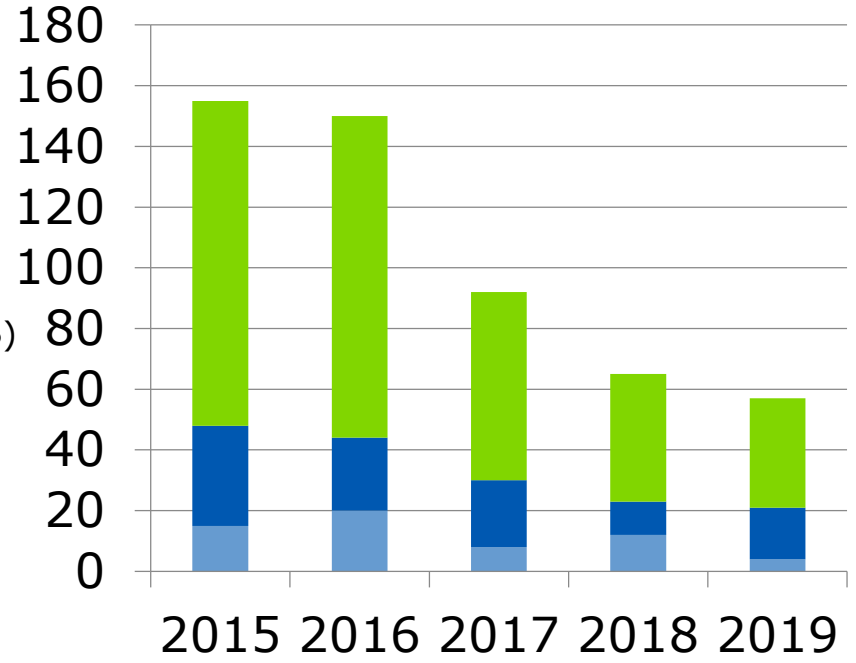
Verkkojen toimivuus

- Sovellustason palvelunestohyökkäys aiheutti häiriöitä saman konesalin kaikille asiakkaille
  - HTTP-hyökkäysliikennettä yli 3000 osoitteen bottiverkosta useana päivänä yli viikon aikana
- Operaattorin verkkolohkon moneen eri osoitteeseen kohdistunut massahyökkäys on häirinnyt eteläafrikkalaisen operaattorin toimintaa laajasti.
  - Leveän rintaman palvelunestohyökkäys on operaattorille yksittäistä hyökkäystä vaikeampi torjua ja aiheuttaa vakavia seurauksia.

Merkittävien toimivuushäiriöiden määrä







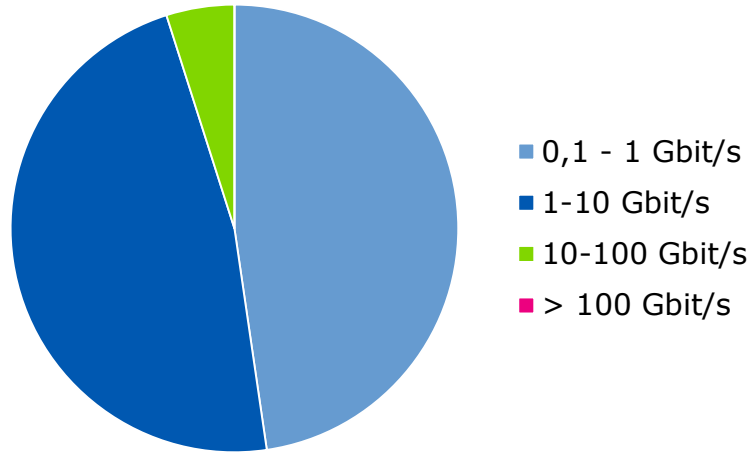
Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta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

Palvelunestohyökkäykset ja niillä uhkailu

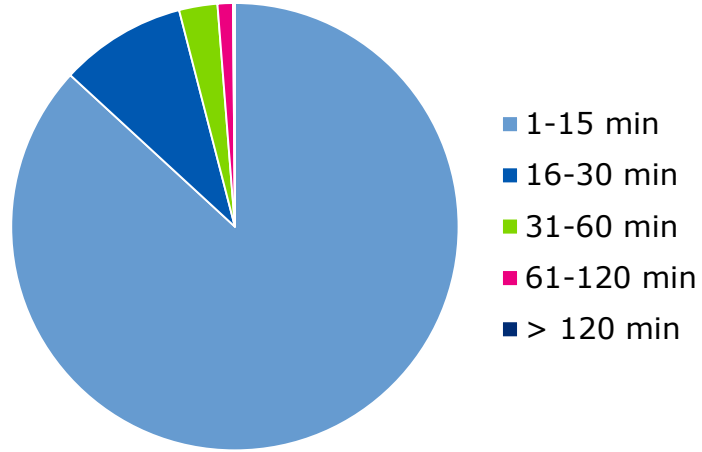
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (87 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin puolet havainnoiduista yli 100Mbit/s hyökkäyksistä on volyymiltään 1-10 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 10 Gbit/s hyökkäyksiä havaitaan Suomessa liki päivittäin.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Kyberturvallisuuskeskukselle ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

2019/Q3:	2019/Q2:	2019/Q1:
n. 39 Gbit/s	n. 79 Gbit/s	n. 162 Gbit/s
(kesto 64 min)	(kesto 4 min)	(kesto 9 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

Vakoilu

Vakoilutilanteessa ajankohtaista

Ilmailusektori teollisuusvakoilun kohteena

Teollisuusvakoiluun keskittyvä kiinalaisryhmä on kohdistanut mielenkiintoaan ilmailusektoriin. Ryhmä on pyrkinyt tunkeutumaan muun muassa lentokonevalmistaja AirBusin järjestelmiin. Tietoturvayhtiö Contextin mukaan ryhmä tunkeutuu varsinaiseen kohteeseensa tämän tärkeiden kumppaniyhtiöiden kautta.

Haavoittuvat etäyhteysratkaisut houkuttelevia kohteita

Valtiolliset toimijat etsivät kohteekseen yritysten käyttämiä haavoittuvia etäyhteysratkaisuja. Verkkolehti ZDNetin lähteiden mukaan tätä on tehnyt esimerkiksi Kiinaan liitetty APT5-ryhmä.

APT28-ryhmä paransi haittaohjelmiensa naamiointia

APT28-ryhmä, joka tunnetaan myös esimerkiksi nimellä Fancy Bear, on kehittänyt Zebrocy-haittaohjelmaperheeseensä uusia osia. Ryhmän tuorein latauskomponentti on esimerkiksi tehty Nim-kielellä. Uusia komponentteja on paranneltu siten, että tietoturvatuotteet eivät havaitsisi niitä yhtä helposti.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmahavaintomme

Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	Muodostavat merkittävän osan Suomessa tehdyistä havainnoista	
Kiristyshaittaohjelmat	Kiristyshaittaohjelmien osalta tilanne Suomessa rauhallinen	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia yritetään levittää aktiivisesti mm. sähköpostin välityksellä	
Louhijat	Louhijahavainnot vähentyneet merkittävästi	
Tietoja varastavat haittaohjelmat	Levittämisyrityksistä jonkin verran havaintoja. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti.	
Mobiilihaittaohjelmat	Mobiilihaittaohjelmatapauksista on joitain havaintoja.	

Haittaohjelmat

- Sähköpostiin liitettyjen tai linkitettyjen haittaohjelmien levitys jatkuu aktiivisena.
  - Sähköpostitse on jaettu syyskuussa erityisesti tietoja varastavia haittaohjelmia sekä etäkäytön mahdollistavia haittaohjelmia.
- Haavoittuvuuksia skannataan ja pyritään hyödyntämään aktiivisesti haittaohjelmien levitykseen.
- Verkkosivuille injektoiduista ja sitä kautta leviävistä haittaohjelmista sekä haitallisista selainlisäosista on havaintoja.

Haavoittuvuudet

- Microsoftin etätyöpöytä-sovelluksen haavoittuvuuden hyväksikäyttöön on julkaistu myös työkalu (Varoitus 2/2019)
  - Julkaistun Metasploit-moduulin avulla haavoittuvuuden etäkäyttö onnistuu helposti
- Exim-sähköpostipalvelimen haavoittuvuuden hyväksikäytöstä on epäilyjä ja syyskuun aikana on löydetty Eximistä muitakin haavoittuvuuksia. (Haavoittuvuus 15/2019)
- vBulletin-ohjelmiston, jota käytetään mm. keskustelusivustojen ylläpidossa, nollapäivähaavoittuvuus mahdollistaa sivujen kaappauksen. Päivitys on nyt saatavilla.
- Uusi iOS-jailbreak julkaistu (Haavoittuvuus 17/2019)
  - Vaatii fyysisen pääsyn laitteeseen ja haavoittuvuuteen ei ole olemassa korjausta, koska se on järjestelmäpiirisarjan toteutuksessa.

Tietomurrot ja -vuodot

Tietomurrot ja -vuodot

- Muutamia murrettuja .fi–päätteisiä verkkosivuja käytetty muun muassa kalastelusivujen ylläpitoon.
  - Tietomurroissa käytettiin todennäköisesti hyväksi WordPress-julkaisualustassa olevaa päivittämätöntä haavoittuvuutta.
- Yksittäisiä Facebook-tilejä päätynyt vääriin käsiin sähköpostin vanhenemisen takia.
  - Yritysten Facebook-tileille on päästy yritystiliin linkitetyn yksityisen facebook-tilin kautta.
  - Yksityiset Facebook-tilit on saatu haltuun tileissä olleen sähköpostiosoitteen vanhentumista hyväksikäyttäen. Tunkeutuja rekisteröi vanhentuneen sähköpostin itselleen ja pystyi sitä kautta nollaamaan kohteena olleen Facebook-tilin salasanan.
  - Facebook-tilin haltuun saaminen mahdollisti yrityksen nimissä esiintymisen sosiaalisessa mediassa.
- Office 365 –tietomurtoja ilmoitetaan päivittäin.
  - Poistimme yli vuoden voimassa olleen Office 365 –varoituksen. Varoitus poistettiin, koska uusia hyväksikäyttömenetelmiä ei ole lähiaikoina ilmennyt. Office 365 -aiheiset tietojenkalastelut ja tietomurrot jatkuvat, kuten ennenkin. Kehotamme käyttäjiä varovaisuuteen.
  - Meille ilmoitetaan ainoastaan murto-osasta Suomessa tapahtuvista Office 365 –tietomurroista. Esimerkiksi yhtä tietomurtoa selvitettäessä esille tuli neljä muutakin uhriorganisaatiota.

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.

Huijaukset ja kalastelut

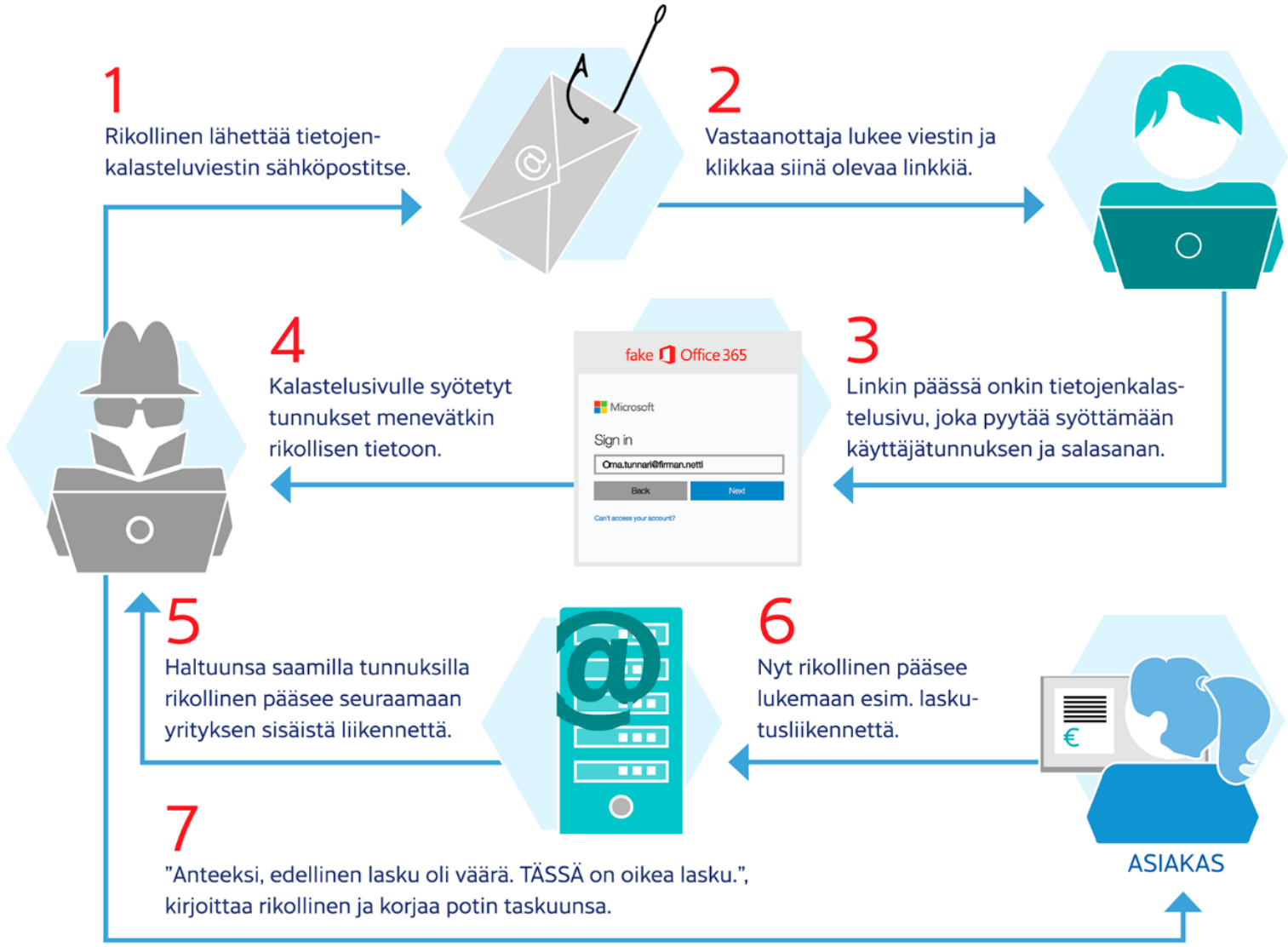
Huijaukset ja kalastelut

- Kaksi laajaa SMS-tilausansakampanjaa: Postin ja Sokoksen nimissä
- Lahjakorttihuijaukset toimitusjohtajahuijauksen muotona
- Pornokiristyksiä: huijarit ovat ottaneet QR-koodeja käyttöön lunnaiden maksua varten.
- Veronpalautuksia on yritetty huijata väärälle edunsaajalle

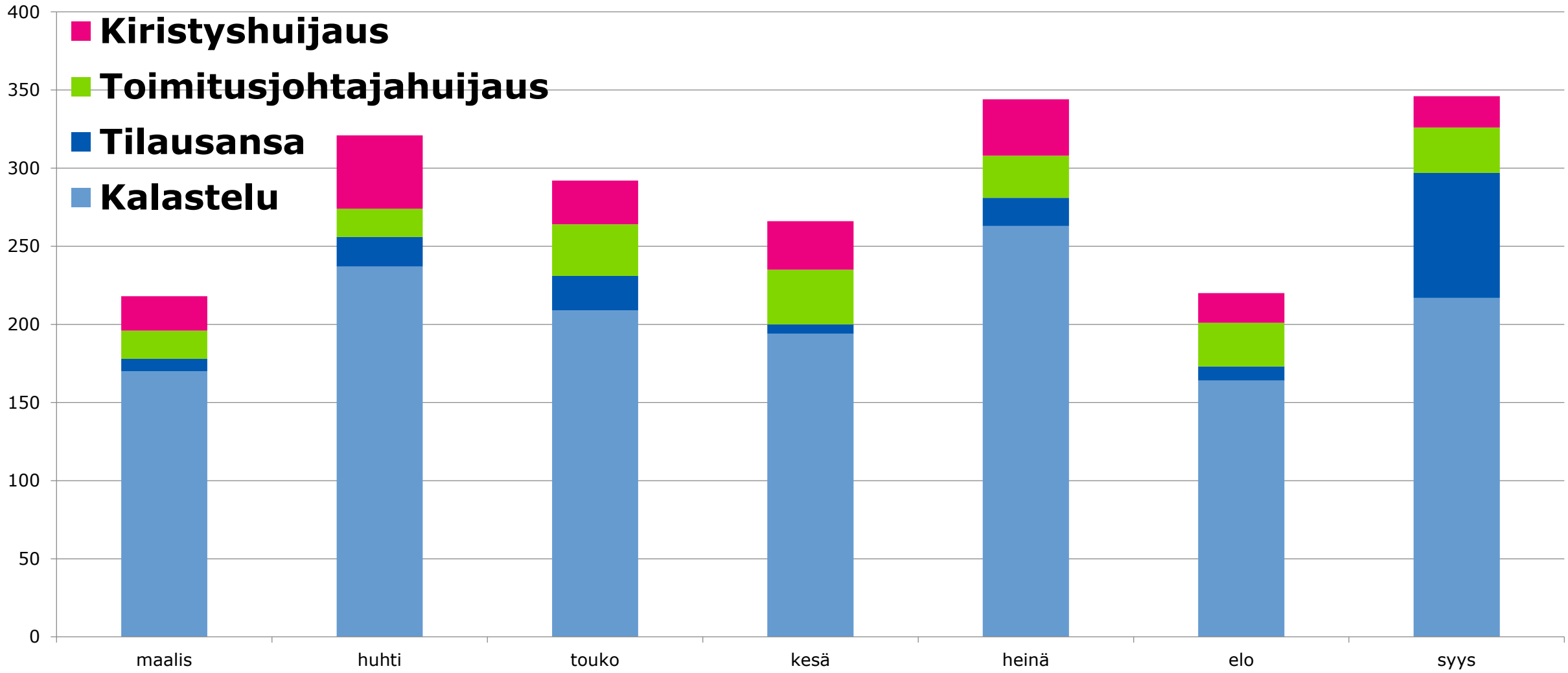
Operaatio reWired:

- 281 verkkohuijarin pidätystä ympäri maailmaa: USA, Nigeria, Turkki, Ghana...
- FBI:n koordinoimassa monen maan operaatiossa tehtiin laajaa poliisiyhteistyötä.

Office 365 –huijauksen vaiheet



Käsiteltyjä huijaustapauksia 2019/03–09



IoT ja automaatio

IoT ja automaatio

- 29.11-1.12.2019 järjestetään Oulussa 5g Hackathon (EU-puheenjohtajamaana toimiva Suomi saa kunnian toimia maailman ensimmäisen 5G:n kyberturvallisuutta luotaavan hackathonin isäntänä. 5G Cyber Security Hackathonin näyttämönä toimii Oulun yliopiston Tellus Innovation Arena.
- Aiemmin kiinni otettu Satori-botnetin operaattori on tunnustanut syyllisyytensä.
  - Ainakin osa aiemmin IoT-laitteisiin kohdistuneista Mirai-perheen varianttia operoitu tätä kautta.
- Tervetuloa IoT-verkoston tapaamiseen 12.11.2019 - teemoina Tietoturvamerkki ja asumisen IoT.
  - Paikkana : Liikenne- ja viestintävirasto Traficom, Erik Palménin aukio 1, Helsinki

Tietoturva-alan kehitys

Oikeudelliset asiat 1/2

- Liikenne- ja viestintäviraston määräysluonnos 66 A teletoiminnan häiriötilanteista lausuttavana 1.11.2019 saakka (määräyksen päivittäminen)
  - Lakiteknisiä ja määräystekstiä selkeyttäviä muutoksia (esim. lainsäädäntöviittaukset ajan tasalle)
  - Lukujen 4 (Ilmoittaminen Liikenne- ja viestintävirastolle) ja 5 (Tilastointi) velvoitteita joukkoviestintäpalvelujen kannalta sovellettaisiin jatkossa vain Yleisradion julkisen palvelun ja useita eri yleisöryhmiä palvelevien televisio-ohjelmistojen siirtämiseen ja lähettämiseen
  - Määräyksen 6 §:ää kevennettäisiin siten, että sähköisellä ilmoitusjärjestelmällä tai sähköpostitse ilmoittamisen lisäksi teleyrityksen tulee ilmoittaa asiasta puhelimitse vain tilanteen havaitessaan (ns. alkuilmoitus)
  - Määräyksen 15 ja 17 §:iin lisätäisiin mahdollisuus ilmoittaa palvelunestohyökkäyksistä hyödyntäen viraston tarjoamaa nk. DDoS-ilmoitusrajapintaa
  - Luvun 5 tilastointia koskevia velvoitteita kevennettäisiin poistamalla valtaosa nykyisistä tilastointivaatimuksista

Oikeudelliset asiat 2/2

- Sähköisen tunnistuspalvelun arviointiohje 211/2019 O on julkaistu
  - Ohjeessa on kyse vahvojen sähköisten tunnistuspalvelujen auditoinnin tueksi laaditusta mallikriteeristö
  - Uutena mukana on mobiilitunnistusratkaisuille erityiskriteeristö
  - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_S%C3%A4hk%C3%B6isen_tunnistuspalvelun_arviointiohje_211_2019_O.pdf
- EU:n sähköisen viestinnän tietosuojasta-asetuksen ("ePrivacy") valmistelu neuvoston teletyöryhmässä jatkuu

Kyberasioihin liittyvää uutisointia maailmalta

Kiristyshaittaohjelmat piinaavat maailmalla

- Kiristyshaittaohjelmat aiheuttavat huomattavia taloudellisia tappioita ja häiriöitä tuotannolle.
- Kiristyshaittaohjelmatapaus maksoi esimerkiksi tanskalaiselle terveysteknologiavalmistaja Demantille 95 miljoonaa dollaria.
- Yhdysvalloissa myös sairaaloiden ja koulupiirien uutisoitiin joutuneen kiristyshaittaohjelmien uhreiksi.
- https://www.zdnet.com/article/ransomware-incident-to-cost-danish-company-a-whopping-95-million/
- https://www.zdnet.com/article/some-victorian-hospitals-are-offline-after-ransomware-hit/

Euroopan kyberturvallisuus-kuukausi alkoi

- Lokakuussa vietetään Euroopan kyberturvallisuuskuukautta. Teemakuukauden tavoitteena on tarjota arjen tietoja ja taitoja kyberturvallisuudesta sekä fiksuja älylaitteiden hankinta- ja käyttötapoja.
- Myös Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on mukana kyberkuukauden tapahtumissa.
- https://cybersecuritymonth.eu/
- https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month

Toimitusjohtajahuijaukset yleistyvät ja kehittyvät

- FBI raportoi, että kolmen vuoden aikana sille ilmoitettujen sähköpostihuijausten rahallinen arvo ylitti 26 miljardia dollaria. Summa sisältää sekä onnistuneet huijaukset että huijausyritykset.
- Tyypillisesti rikollinen pääsee käsiksi murretulle sähköpostitilille, jonka kautta hän pyytää rahansiirtoa tai maksutietojen vaihtamista, mutta myös tilitietojen muuttamiseen tähtäävät palkanmaksuhuijaukset ovat yleistyneet.
- https://www.ic3.gov/media/2019/190910.aspx

Kiitos.

kyberturvallisuuskeskus.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus