TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Kybersää

## Joulukuu 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 joulukuu 2019

### Verkkojen toimivuus

- Eräässä palvelunestohyökkäyksessä hyödynnettiin verkon aktiivilaitteen haavoittuvuutta hyökkäyksen teossa.
- Aapo-myrsky aiheutti vain vähän toimivuushäiriöitä.
- Vuosia jatkunut merkittävien häiriöiden määrän lasku pysähtyi.

### Vakoilu

- Iranin ja Yhdysvaltojen välinen kiristynyt poliittinen tilanne kasvattaa myös kyberiskujen ja -vakoilun riskiä.
- Kaksivaiheinen tunnistaminen ei pidä kybervakoojia ulkona järjestelmistä.

### Haittaohjelmat ja haavoittuvuudet

- Esimerkiksi Citrixin tuotteissa haavoittuvuus, johon ei ole päivitystä ja jota hyödynnetään hyökkäyksissä.
- Lokibot-haittaohjelmaa levitetty aktiivisesti sähköpostitse mm. Turun yliopiston nimissä.

### Tietomurrot ja -vuodot

- Office 365 tietomurto aiheutti kymmenien tuhansien tappiot suomalaiselle yritykselle.
- Varsin laaja Facebook-tunnusten tietomurto, joka ei kuitenkaan sisältänyt salasanoja tai maksukorttitietoja.

### Huijaukset ja kalastelut

- Tilausansojen tehtailu on automatisoitumassa.
- Tilausansoja levitellään tekstiviestein, sähköpostilla, mainoslinkeillä ja hakukoneoptimoinnilla.

### IoT ja automaatio

- Vuosittainen kartoitus paljasti yli tuhat suojaamatonta laitetta Suomessa.
- FBI:n suosittelee pitämään IoT-laitteet muista järjestelmistä eriytetyissä verkoissa.

# **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. Palvelunestohyökkäyksiä näkyy entiseen malliin, mutta niiden vaikutukset jäävät vähäisiksi. Pesurit ja muut torjuntakeinot näyttävät toimivan.

2. DNSSEC-tietoturvalaajennuksen käyttö parani Suomessa: Digitaalisten palveluiden käyttäminen turvallisemmaksi.

3. Tietoturvaharjoitusskenaariot julkaistiin. Skenaariot täydentävät aikaisemmin julkaistua Kyberharjoitusopasta.

## Tietoturvan kehitystarpeet

1. Tietojenkalasteluita ja tilausansoja tehtaillaan automatisoidusti. Organisaatioiden tulee kiinnittää huomiota henkilöstön kykyyn tunnistaa niitä.

2. DNSSECin käyttöönotto on hyvä alku. Tietoturvalaajennuksen käyttö tulisi vielä laajentua teleyrityksistä organisaatioiden verkkotunnusten nimipalvelimiin.

3. Ota järjestelmäpäivitykset osaksi rutiinia. Tunnettuja tietoturva-aukkoja hyödynnetään edelleen, kuten 2019 yleisin haittaohjelma WannaCry.

# Verkkojen toimivuus

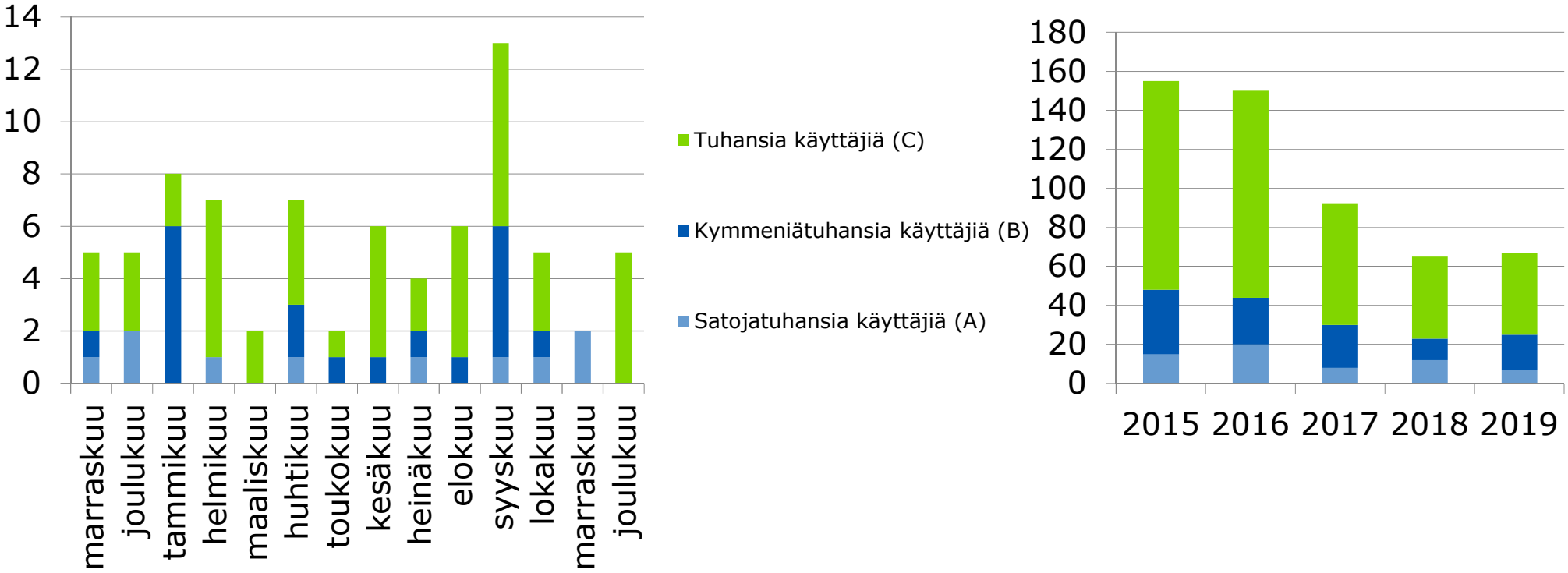
# Verkkojen toimivuus

- Joulukuussa viisi merkittävää toimivuushäiriötä
  - Tavanomainen määrä
- Aapo-myrsky 18.-19.12. aiheutti suhteellisen vähän toimivuushäiriöitä
  - Satoja mobiiliverkkojen tukiasemia oli sähköttä Kanta-Hämeestä Etelä-Karjalaan ja Keski-Suomen eteläosiin ulottuvalla alueella. Yhtenäisiä usean tukiaseman katveita oli kuitenkin vähän.
  - Hätäliikenne toimi koko ajan.
- Vuonna 2019 merkittävien toimivuushäiriöiden määrän väheneminen pysähtyi
  - 2016: 150 kpl. 2017: 92 kpl. 2018: 65 kpl. 2019: 67 kpl.

# Verkkojen toimivuus

- Joulukuussa raportointiin palvelunestohyökkäyksiä tavanomainen määrä.
  - Hyökkäyksiä toteutettiin mm. isolla määrällä UDP-paketteja sekä TCP SYN tulvalla.
  - Kohteina oli mm. julkishallintoa sekä media-alan yritys.
- Eräässä palvelunestohyökkäyksessä hyökkäys toteutettiin verkkolaitteen ohjelmistohaavoittuvuutta hyödyntämällä.
  - Haavoittuvuuden avulla hyökkääjät saivat laitteen uudelleenkäynnistymään toistuvasti, joka käytännössä aiheutti palvelunestotilan.

# Merkittävien toimivuushäiriöiden määrä



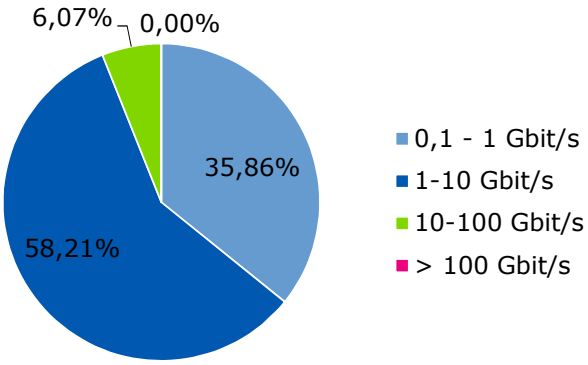

Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 65–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta vuodessa. Niiden määrä riippuu teleyrityksen tilastointitavasta.

# Palvelunestohyökkäykset ja niillä uhkailu

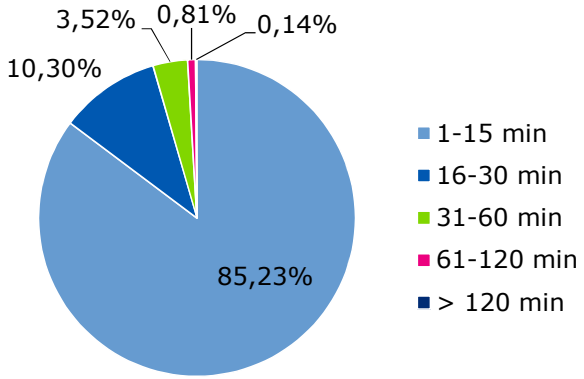
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (85 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Yli puolet havainnoiduista yli 100Mbit/s hyökkäyksistä on volyymiltään 1-10 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 10 Gbit/s hyökkäyksiä havaitaan Suomessa päivittäin.
- Tietoa palvelunestohyökkäyksistä kerätään suoraan teleyrityksiltä, koska Kyberturvallisuuskeskukselle ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

**Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)**

| 2019/Q4: | 2019/Q3: | 2019/Q2: |
|---|---|---|
| n. 54 Gbit/s | n. 39 Gbit/s | n. 79 Gbit/s |
| (kesto 8 min) | (kesto 64 min) | (kesto 4 min) |




Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.




Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

# Vakoilu

# Vakoilutilanteessa ajankohtaista

### Lähi-idän tilanne kasvattaa kyberiskun mahdollisuutta

Iranin ja Yhdysvaltojen välinen kiristynyt poliittinen tilanne kasvattaa kyberiskujen ja -vakoilun riskiä. Kyberhyökkäystä pidetään Iranin yhtenä mahdollisena keinona reagoida Yhdysvaltojen toimiin alueella. Yhdysvallat on varoittanut kohonneesta kyberriskistä sekä omalla maaperällään että sille tärkeissä kohteissa ulkomailla.

### Hakkeriryhmä ohittaa monivaiheisen tunnistamisen

Fox-IT varoittaa, että Kiinaan yhdistetty hakkeriryhmä on ohittanut kaksivaiheisen tunnistamisen viimeaikaisissa hyökkäyksissään. Fox-IT kutsuu operaatiota nimellä Wocao. Uhreina on ollut valtiollisia tahoja, palveluntarjoajia kuin organisaatioita lukuisilta eri toimialoilta.

### Microsoft otti haltuunsa hakkereiden verkko-osoitteita

Microsoft on ottanut haltuunsa lähes 50 pohjoiskorealaisten hakkerien käyttämää verkkotunnusta. Palvelut jäljittelivät Microsoftin palveluita, ja niiden avulla pyrittiin muun muassa kalastelemaan kohdistetusti tiettyjen Microsoftin asiakkaiden käyttäjätietoja.

# Haittaohjelmat ja haavoittuvuudet

# Haittaohjelmahavaintomme

| Haittaohjelmatyyppi | Tilanne | |
|---|---|---|
| IoT-haittaohjelmat | QSnatch-haittaohjelma muodostaa edelleen suuren osan Suomessa tehdyistä havainnoista, mutta havainnot laskussa marraskuuhun verrattuna. |  |
| Kiristyshaittaohjelmat | Kiristyshaittaohjelmissa tilanne Suomessa rauhallinen. |  |
| Etähallittavat haittaohjelmat (RAT) | Etähallittavia haittaohjelmia yritetään levittää edelleen sähköpostin avulla. Yksittäisistä haittaohjelmista pinnalla on Lokibot. |  |
| Louhijat | Ei merkittäviä louhijahavaintoja tässä kuussa |  |
| Tietoja varastavat haittaohjelmat | Levittämisyrityksistä vain vähän havaintoja. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti. |  |
| Mobiilihaittaohjelmat | Mobiilihaittaohjelmatapauksista on joitain havaintoja. |  |

# Haittaohjelmat

- Turun yliopiston nimissä lähetettiin 19.12. haitallisia sähköpostiviestejä, joiden liitteenä on ollut Lokibot-haittaohjelman. Lokibot-haittaohjelman eri versioita on muutenkin liikkeellä, mutta viestien määrä on laskussa.
- Mittavia lunnaita vaativa big game hunting –ilmiö jatkuu maailmalla voimakkaana.
  - Kyberturvallisuuskeskus on avustanut ulkomaisia sisarorganisaatioita Sodinokibi- (REvil) kiristyshaittaohjelman komentopalvelininfrastruktuurin kitkemisessä Suomesta
- Frankfurt am Main sulki IT-järjestelmänsä Emotet-haittaohjelmatartunnan takia. Maailmalla on muutenkin paljon Emotet-haittaohjelmaa liikkeellä.
- RavnAIR Group on joutunut kyberhyökkäyksen kohteeksi, joka on vaikuttanut erityisesti De Havilland Dash 8 –sarjan koneiden operointiin.

# Haavoittuvuudet

- Citrix Application Delivery Controller (ADC) sekä Citrix Gateway -tuotteista on löydetty haavoittuvuus, jota pyritään aktiivisesti hyväksikäyttämään. Hyökkääjän on mahdollista suorittaa kohdejärjestelmässä mielivaltaista ohjelmakoodia. Ensimmäiset päivitykset saatavilla arviolta 20. tammikuuta. (Haavoittuvuus 24/2019, TTN 13.1.2020)
- SSL VPN tuotteiden keväällä 2019 löydettyjä haavoittuvuuksia käytetään nyt aktiivisesti haittaohjelmien levittämiseen ja big game hunting -toimintaan. Koskee mm. Pulse Securen, Fortinetin SSL VPN tuotteita.
- TCP/IP-toteutuksista löydetty haavoittuvuus mahdollistaa saamaan tietoa VPN-yhteyksien tilasta ja liittämään dataa VPN-tunneloituun liikenteeseen (Haavoittuvuus 23/2019)
- Android-laitteita koskevaa StrandHogg-haavoittuvuutta hyödynnettiin haittaohjelmissa. (Haavoittuvuus 22/2019)

# Tietomurrot ja -vuodot

# Tietomurrot ja -vuodot

- Office 365 –tietomurroista koituu kustannuksia suomalaisyrityksille. Toisaalta jouluna ilmoitetut tietomurrot vähenivät.
  - Yksittäisen Office 365 –tietomurron seurauksena suomalaiselta yritykseltä onnistuttiin laskutuspetoksella huijaamaan kymmeniä tuhansia euroja. Rahoja ei onnistuttu palauttamaan uhrille.
  - Joulukuun alkupuolella Office 365 –tietomurtoilmoituksia tuli useita päivittäin, mutta joulun aikaan ilmoitukset loppuivat täysin yli viikoksi. Syynä ilmoitusten määrän vähenemiseen on todennäköisesti lomakausi.

- Joulukuun lopulla tuli julki 267 miljoonan Facebook-käyttäjän tietojen vuotaminen julkisuuteen.
  - Vuotaneita tietoja olivat käyttäjän nimi, Facebook-tunnus sekä puhelinnumero, muttei esimerkiksi salasanoja tai maksukortin tietoja vuotanut.
  - Vuodettuja tietoja ei todennäköisesti ole saatu tietomurron seurauksena, vaan ne on kerätty julkisesti saatavilla olleista rajapinnoista, käyttöehtojen vastaisesti.

# 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

# Tietojenkalastelut

- Office 365 -palvelun käyttäjätunnusten tietojenkalastelu jatkui joulukuussakin vilkkaana ja johti uusiin tietomurtoihin lähes päivittäin. Murrettuja tilejä käytettiin edelleen uusiin tietojenkalasteluihin.

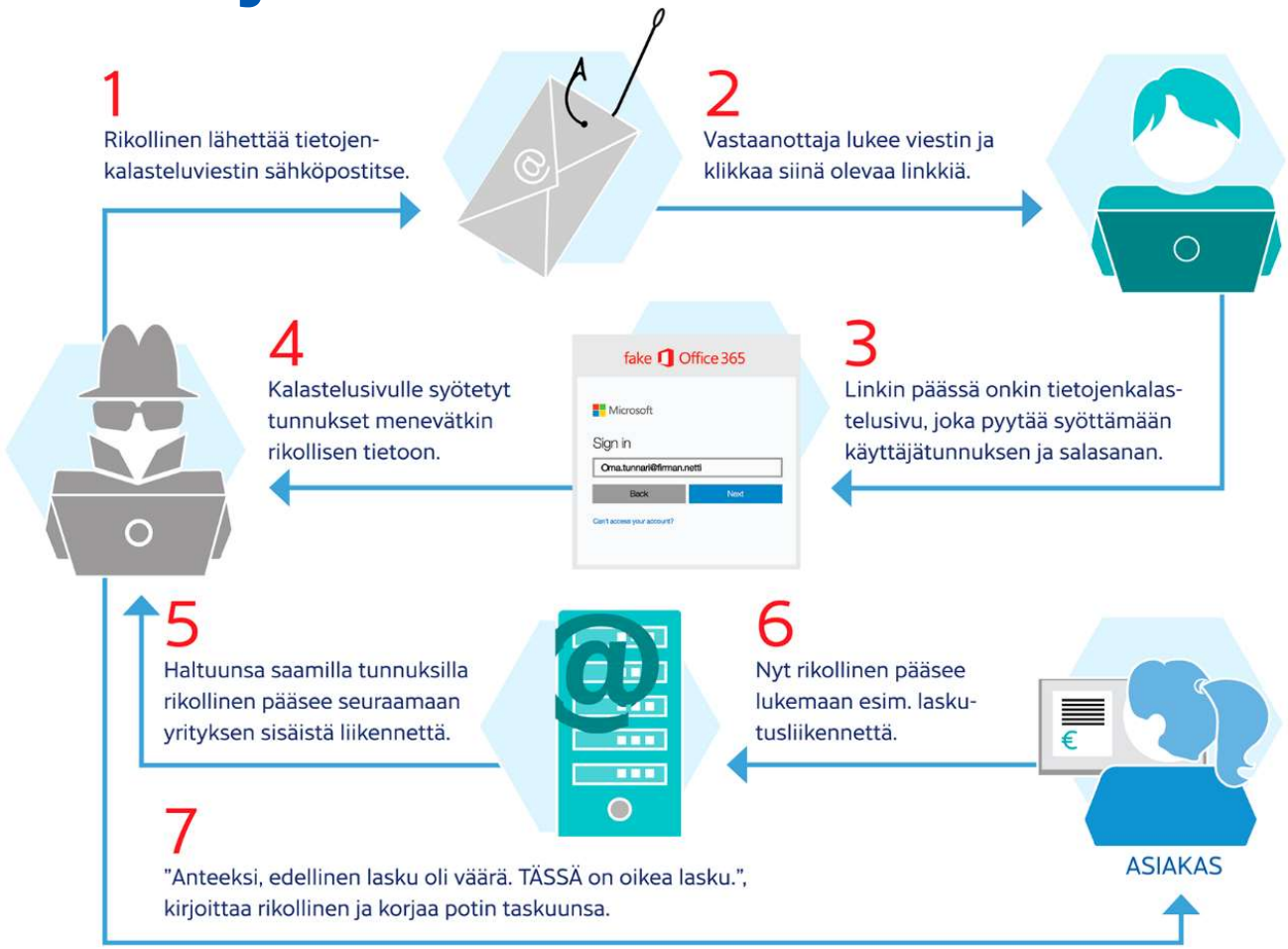
- Kaikkien kotimaisten liikepankkien pankkitunnuksia kalasteltiin aktiivisesti.
  - Lisäksi muut rahaliikennepalvelut, kuten PayPal kiinnostavat huijareita.

- Verkkopalveluista Netflix- ja LinkedIn-tunnuksia kalasteltiin runsaasti joulukuussa.

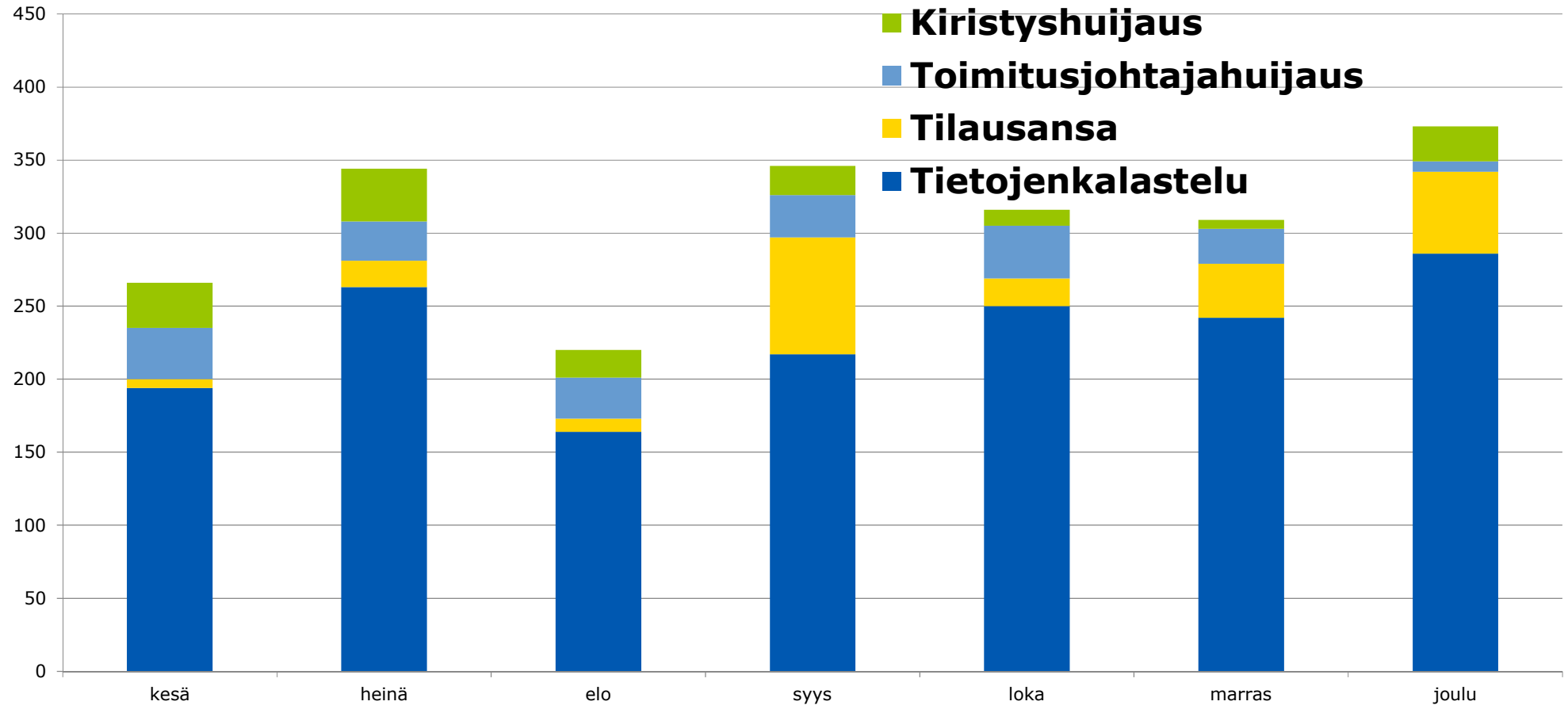
# Verkkohuijaukset

- Tilausansat tuntuvat olevan taas kasvussa
  - Tilausansoja levitetään runsain määrin tekstiviesteillä, sähköpostilla, verkkomainosten ja sosiaalisen median kautta.
  - Maksuttomiin verkkotunnuksiin perustetaan tuhansittain huijaussivustoja, joille käyttäjiä ohjataan hakukoneoptimoinnin kautta: melkein millä tahansa hakusanalla voi päätyä tilausansaan.
  - Tilausansojen ja muiden huijausten tehtailu verkkosivuille on automatisoitunut.
- Sijoitushuijauksia markkinoidaan ulkomaisista ja väärennetyistä puhelinnumeroista.
- Umpeutuvia verkkotunnuksia rekisteröidään mm. valeverkkokauppoihin ja erityyppisiin huijauksiin.

# Office 365 –huijauksen vaiheet



# Käsiteltyjä huijaustapauksia 2019/06–12



# IoT ja automaatio

# IoT ja automaatio

- Kyberturvallisuuskeskuksen vuosittainen automaatiolaitteiden tarkastus paljasti reilu tuhat laitetta, joista suurin osa lukeutuu rakennusautomaation piiriin. Raportti havaintoineen sekä suositukset ylläpitäjille: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hieman-yli-tuhat-automaatiolaitetta-suojaamattomana-suomalaisissa-verkoissa
- FBI on julkaissut joukon suosituksia IoT-laitteisiin liittyen.
  - Tarkastuslista: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hieman-yli-tuhat-automaatiolaitetta-suojaamattomana-suomalaisissa-verkoissa

# Tietoturva-alan kehitys

# Oikeudelliset asiat

- Kyberturvamerkin pohjana toiminutta teknistä spesifikaatiota muutetaan eurooppalaiseksi standardiksi, jonka lausuntokierros on käynnissä. ETSI 303645.
- Digi- ja väestötietovirasto aloitti toimintansa 1.1.2020, kun Väestörekisterikeskus, maistraatit ja Itä-Suomen aluehallintovirastossa toimiva Maistraattien ohjaus- ja kehittämisyksikkö yhdistyivät. Ks. tarkemmin https://dvv.fi/digi-ja-vaestotietovirasto
- 1.1.2020 voimaan tulleen tiedonhallintalain nojalla on annettu Valtioneuvoston asetus julkisen hallinnon tiedonhallintalautakunnasta (1338/2019). Asetus tuli voimaan 1.1.2020
- Euroopan Parlamentin ja Neuvoston päätös (EU) 2019/2071, annettu 5 päivänä joulukuuta 2019, Euroopan tietosuojavaltuutetun nimittämisestä, https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32019D2071&from=FI

# Kyberasioihin liittyvää uutisointia maailmalta

### Cloud Hopper

- Cloud Hopper on vuonna 2016 tietoisuuteen tullut, kiinalaisiin toimijoihin yhdistetty, yrityksiin kohdistunut laaja tietomurtosarja.
- WSJ:n mukaan tietomurron vaikutukset ovat olleet luultua laajemmat. Kokonaisuuteen liittyi useita pilvipalveluidentarjoajia, mm. Suomessa toimiva Tieto.
- Tiedon mukaan sen omissa järjestelmissä ei ollut merkkejä tietomurroista.
- https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061
- https://www.hs.fi/talous/art-2000006361021.html

### Alaskalainen lentoyhtiö kyberhyökkäyksen kohteena

- Alaskalainen RavnAir on joutunut keskeyttämään tietyn konetyyppiinsä lennot kyberhyökkäyksestä johtuen.
- Yhtiön tiedotteen mukaan se katkaisi yhteyden lentokoneiden ylläpitojärjestelmään ja sen varajärjestelmään kyberhyökkäyksen takia.
- Saman koneperheen lentokoneita on laajasti käytössä Euroopassa mm. airBalticilla, Air Icelandilla ja Eurowingsillä.
- https://www.flightglobal.com/fleets/network-attack-disrupts-ravnair-dash-8-fleet/135964.article

### Huawei kommentoi Supon toimintaa

- Huawein mukaan Yhdysvallat on levittänyt sen tuotteista väärää tietoa muiden maiden tiedusteluviranomaisille yli vuoden ajan – myös Supolle.
- Supon mukaan se muodostaa kantansa itse, oman tiedonhankinnan, analyysin ja kansainvälisen yhteistyön pohjalta.
- Supon päällikkö Antti Pelttari peräänkuuluttaa poliittisen keskustelun käymistä 5G:stä.
- https://www.is.fi/digitoday/tietoturva/art-2000006353678.html
- https://www.is.fi/digitoday/tietoturva/art-2000006348909.html

# Kiitos.

kyberturvallisuuskeskus.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus