#kybersää 07/2018

#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 02/2018: Office 365 -tunnuksia kalastellaan aktiivisesti

- Suomalaisten yritysten työntekijöiden sähköpostitunnuksia ja -viestejä on kuluvan vuoden aikana varastettu. Aiheesta annettu punainen varoitus oli voimassa myös heinäkuussa. Varoitus on elokuussa laskettu kriittisestä (punainen) vakavaksi (keltainen).
- Tietojenkalastelu on useissa tapauksissa kohdistunut organisaatioiden johtoon ja maksuliikenteestä vastaaviin henkilöihin.
- Käyttäjätunnuksia ja salasanoja on kalasteltu sähköpostitse ja huijaussivujen avulla.
- Kalastelluilla tunnuksilla on kirjauduttu yritysten Office 365 -sähköpostitileille ja pyritty seuraamaan yritysten sähköpostiliikennettä, saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia.
- Lisätietoja:
  - https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2018/varoitus-2018-03.html

#kybersää 07/2018

Palvelunestot

- Heinäkuussa palvelunestohyökkäyksiä kohdistui muun muassa pankkisektoriin ja julkishallintoon.
- Hyökkäysten kokoluokat noin 10 – 35 Gbit/s.
- Hyökkäykset on saatu pääosin torjuttua.

Haittaohjelmat & haavoittuvuudet

- Avoimista palvelinten hallintaliittymistä raportoitiin 300 laitteen omistajalle.
- Suorittimista raportoitiin uusia haavoittuvuuksia.
- Urheilukellojen mahdollistamista tietovuodoista uutisoitiin runsaasti.

Huijaukset & kalastelut

- Pornokiristyskampanja tehosti uskottavuuttaan uhrille kuuluvalla salasanalla, joka oli lähtöisin vanhasta tietovuodosta.
- Sähköpostitunnuksia kalastellaan ja näin kaapattuja tilejä käytetään uusiin huijauksiin.

Vakoilu

- Microsoft kertoi jo havainneensa hyökkäyksiä Yhdysvaltain syksyn vaaleihin.
- US-CERT kertoi Venäjän hyökkäyksistä sähköverkkoyhtiöihin.

Verkkojen toimivuus

- Häiriöitä on ollut vähän edellisiin vuosiin verrattuna.
- Kesän aikana on ollut 5 vakavaa häiriötä. Ne ovat olleet melko lyhyitä ja johtuneet toisistaan riippumattomista syistä.

IoT

- Hide 'n Seek -botti leviää nyt myös yleiskäyttöisiin tietokoneisiin.
- Lukuisat IoT-laitteet haavoittuvia DNS rebinding -hyökkäykselle. Linkin klikkaaminen voi lähettää komentoja sisäverkon IoT-laitteille.

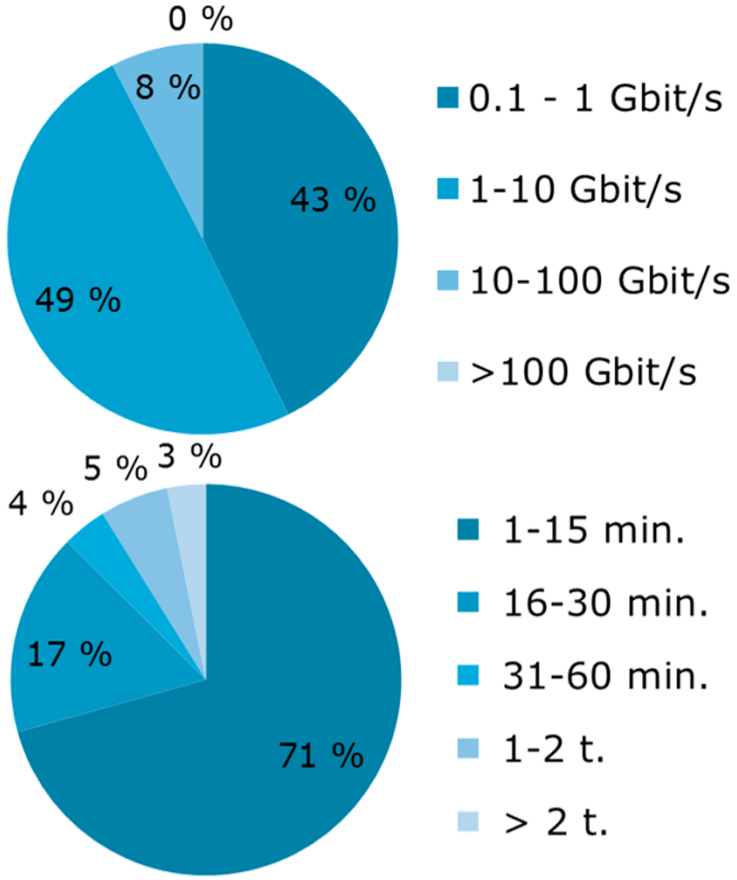
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu:

- Lyhyet alle 15 min 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.

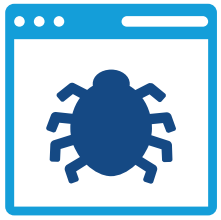
Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä. Lähde: teleyritykset

2018/Q2:	**2018/Q1:**	**2017/Q4:**
n. 37 Gbit/s (kesto 8 min)	n. 35 Gbit/s (kesto 7 min)	n. 57 Gbit/s (kesto alle 10 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2018/Q2. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu



- Finanssisektoria vastaan kohdistuu säännöllisesti jonkin verran palvelunestohyökkäyksiä, joiden maksimivolyymi vaihtelee 10–35 Gbit/s. Näitä volyymiltaan suuria hyökkäyksiä tehdään CLDAP- ja SYN FLOOD -tekniikoilla. Pääsääntöisesti nämä hyökkäykset voidaan torjua eikä niistä aiheudu merkittävää haittaa.
  - Palvelunestohyökkäyksiä on siirrytty tekemään enenevässä määrin myös HTTP FLOOD -tekniikalla, jossa WWW-palvelinta yritetään kuormittaa suurella määrällä HTTP-kyselyitä ja joiden torjuminen on vanhempia tekniikoita haastavampaa, sillä normaali selailuliikenne näyttää samalta tai sillä voidaan kuormittaa palvelinta tehokkaammin.
- Julkishallinnon palveluihin on raportoitu kohdistuneen SYN FLOOD -palvelunestohyökkäyksiä suuruudeltaan 15-24 Gbit/s.
  - Hyökkäykset on enimmäkseen torjuttu, mutta suurimmat ovat jonkin verran häirinneet palveluiden toimintaa.
- Suuriin liikennemääriin perustuvat palvelunestohyökkäykset eivät yleensä enää häiritse palveluita sellaisissa yrityksissä, joissa on otettu käyttöön tehokkaampia suojauskeinoja.
  - Rikolliset ovat siirtyneet yhä enemmän kuormittamaan kohteen resursseja, kuten laskentatehoa tai muistia.

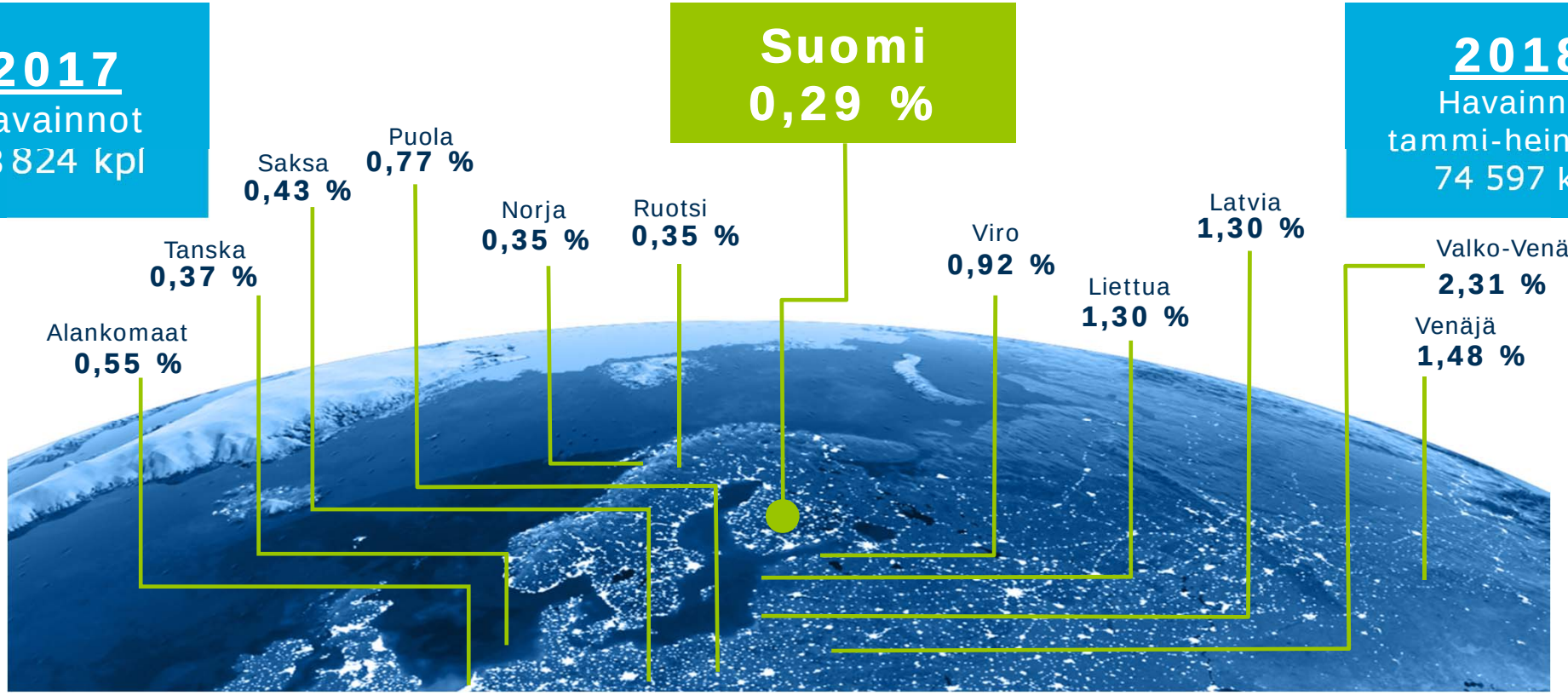
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

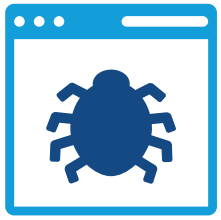
Suomi
0,29 %

2018
Havainnot
tammi-heinäkuu
74 597 kpl



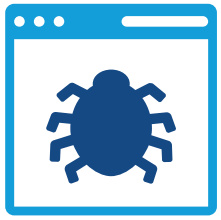
Vuoden 2018 alussa tietoturvapoikkeamahavaintojen määrä jatkoi vuoden 2017 lopun maltillista linjaa, mutta on kevään aikana lähtenyt voimakkaaseen kasvuun.

Haittaohjelmat ja haavoittuvuudet



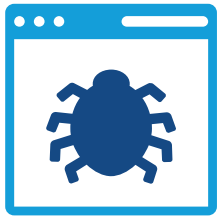
- 18 000 laitteen bottiverkko luotiin vuorokaudessa hyödyntäen Huawei-kotireitittimen haavoittuvuutta.
  - Koti- ja pienyritysreitittimissä raportoidaan edelleen haittaohjelmia myös Suomessa.
- Oracle WebLogic -haavoittuvuuteen julkaistiin valmis hyväksikäyttömenetelmä, jota raportoidusti käytettiin hyökkäyksissä.
  - Haavoittuvuuden avulla hyökkääjä pystyy ottamaan haltuunsa haavoittuvan palvelimen ilman salasanaa.
  - Edellistä WebLogicin haavoittuvuutta käytettiin cryptominereiden levittämiseen.
  - Hyökkäyksiä ei raportoitu Suomessa.
- Androidin ADB-vianselvitystoiminnon kautta levitettiin Satori-haittaohjelmaa verkkoon avoimena olleen portin kautta.
  - Satori on Mirai-haittaohjelman muunnos, jota voidaan Mirain tavoin käyttää bottiverkkojen muodostamiseen ja edelleen palvelunestohyökkäyksiin.

Haavoittuvuudet



- Sähköverkkojen ohjauksessa käytetystä laitteesta löydettiin useita kriittisiä haavoittuvuuksia.
  - Kyse on Martem TELEM-GW6/GWM –laitteesta.
- Dellin, HP:n ja Supermicron palvelinten hallintapaneeleita oli avoimina julkiseen verkkoon.
  - Avoimena olivat Dellin iDRAC-, HP:n iLO- ja Supermicron IPMI-palvelimet. Yhteensä noin 300 hallintapaneelin ylläpitäjään on otettu yhteyttä.
  - HP:n iLO-hallintapaneelin versiosta 4 löydettiin kirjautumisen ohittamisen mahdollistava haavoittuvuus.
- Useiden Bluetooth-laitteiden liikenteen salaustoteutuksista löydettiin toteutusvirheitä, joiden avulla salaus voidaan purkaa.
- Toukokuussa julkaistuista Spectre-varianteista julkaistiin yksityiskohtia ja hyökkäysten estokeinoja. Uudet variantit SpectreRSB ja NetSpectre jatkavat prosessorihaavoittuvuuksien kavalkadia.
- Runsaasti päivityksiä, joissa korjattiin useita kriittisiä haavoittuvuuksia: mm. Cisco, Oracle, Juniper, Apple, SAP, Adobe ja Microsoft julkaisivat päivityspakettinsa.

Tietomurrot ja tietovuodot



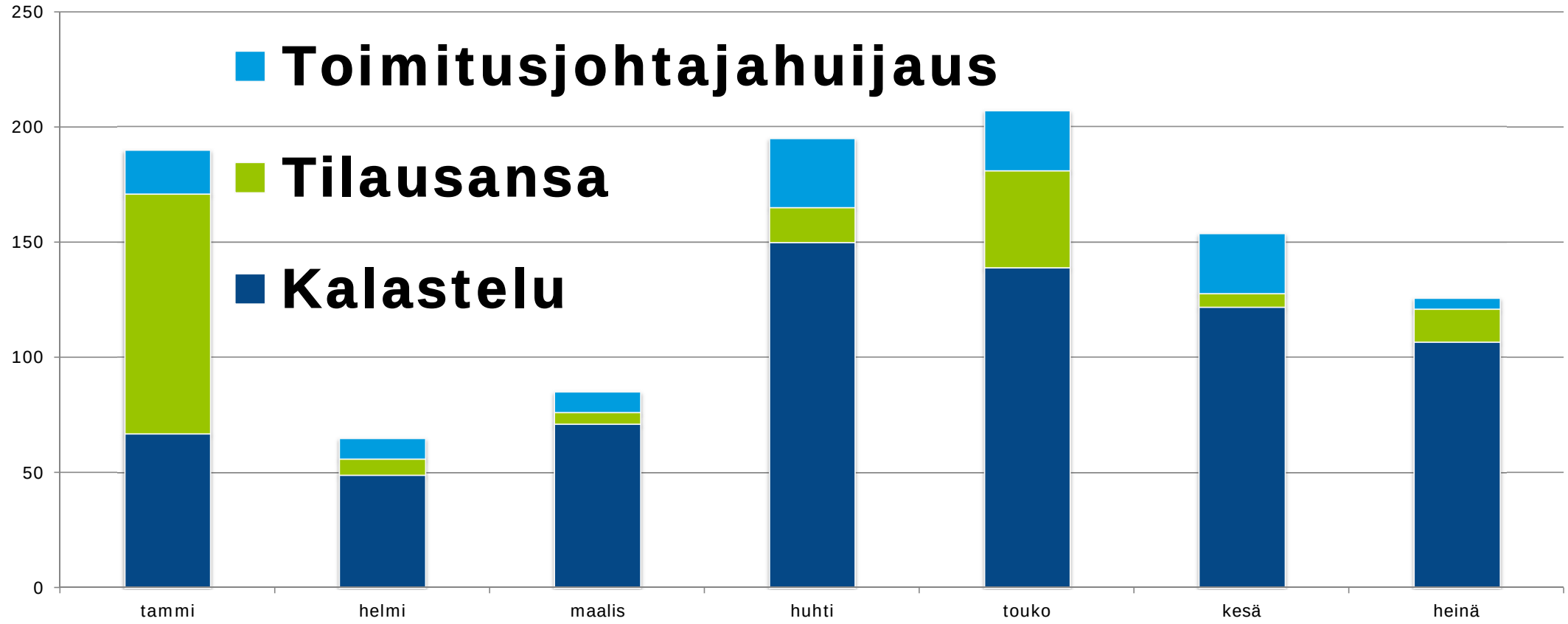
- Suomalaisten yritysten Office 365 -tileille on tehty useita tietomurtoja, joiden seurauksena sähköposti-tileille on asetettu postin uudelleenlähetys rikollisten sähköpostiosoitteeseen.
- US-CERT julkaisi varoituksen hyökkäyksistä toiminnaohjausjärjestelmiin (ERP-järjestelmät).
- Identiteettivarkaussuojaa myyvän Lifelock-yrityksen järjestelmistä raportoitiin tietovuodoille altistava haavoittuvuus. Yrityksen mukaan tietovuotoja ei kuitenkaan ollut tapahtunut.
- Urheilukellovalmistajien järjestelmistä löydettiin eriasteisia tietovuotoja mahdollistavia heikkouksia.
  - » Uutisoinnissa esiin nostetun Polarin lisäksi heikkouksia löydettiin Endomondon, Runkeeperin ja Stravan järjestelmistä.

Huijaukset & kalastelut

Huijaukset heinäkuussa

- Office 365 -tunnusten kalastelu on jatkunut
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Tilien sähköpostit edelleenlähetetään rikollisille, jotka voivat hyödyntää niitä mm. toimitusjohtajahuijauksiin ja teollisuusvakoiluun.
  - Petoksilla ja muilla rikoksilla tavoitellaan merkittävää rikoshyötyä.
- Kiristyskampanja säikäyttää paljastuneella salasanalla
  - Kiristysviestissä väitetään, että uhrin tietokone on saatu haltuun ja kameralla on kuvattu käyntejä pornosivustolla. Väitteet ovat huijausta.
  - Kiristäjä vaatii tuhansien dollarien lunnaita bitcoineina siitä hyvästä, ettei paljastaisi arkaluontoisia tietoja.
  - Sähköpostiviestissä on usein jostakin vanhasta tietovuodosta löydetty salasana, joka kiinnittää huomion ja lisää uskottavuutta.
  - Maailmanlaajuinen kiristysviestikampanja tuotti rikollisille kymmeniä tuhansia jo ensimmäisellä viikolla.
- Tietoja yritetään kalastella tunnettujen pankkien nimissä.
  - Nordea, Danske Bank, OP-pankki, S-pankki ja Säästöpankki ovat yleisiä teemoja.
  - Myös Apple ID-, Netflix- ja PayPal-tunnuksia yritetään kalastella.

Huijausyritykset 2018/01–07



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

Microsoft havaitsi hyökkäyksiä vaaleihin

Microsoft kertoi havainneensa tunkeutumisyrityksiä Yhdysvaltojen syksyn vaalien ehdokkaiden tietojärjestelmiin

US-CERT kertoi Venäjän tunkeutumisista sähköverkkoihin

US-CERT piti webinaarin, jossa paljasti yksityiskohtia siitä, miten venäläiset toimijat tunkeutuivat yhdysvaltalaisiin sähköverkkoyhtiöihin

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

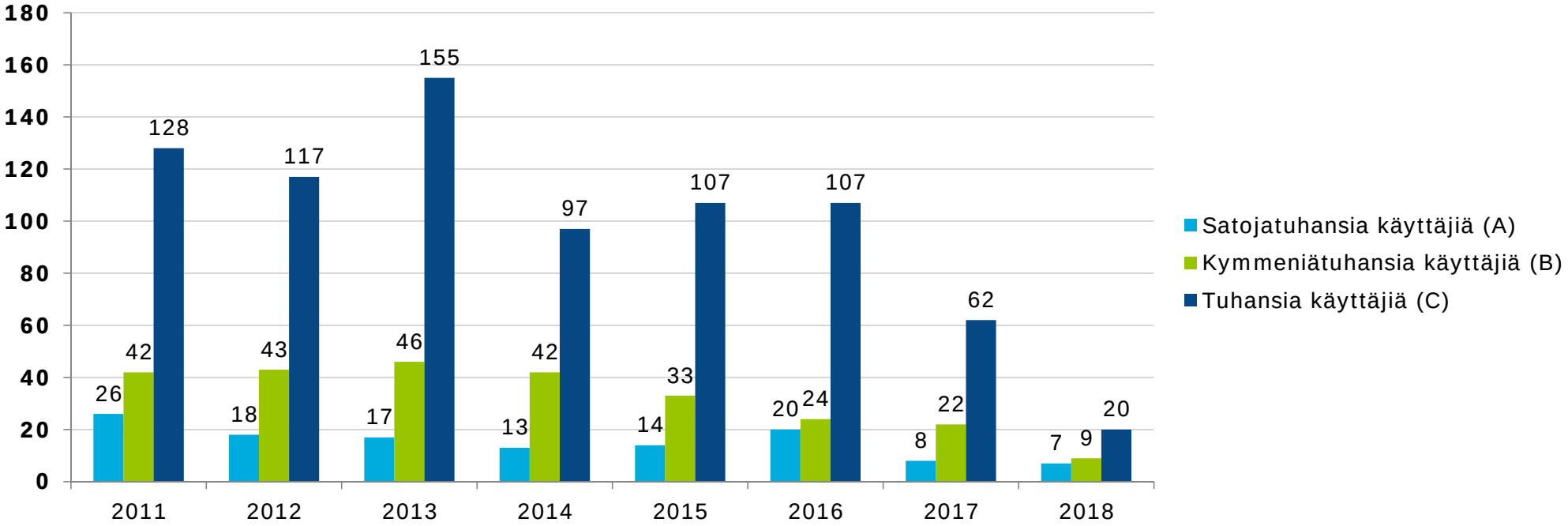
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018
(tammi-heinäkuu)

Vakavuus	Lukumäärä
A-luokka	7
B-luokka	9
C-luokka	20
Kaikki häiriöt (1Q)	**96 732**

Alkuvuonna on ollut poikkeuksellisen vähän merkittäviä häiriöitä. Vakavimpia A-luokan häiriöitä on ollut kesän aikana paljon, mutta se vaikuttaa sattumalta.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokan toimivuushäiriöt. Niitä on vuosittain 100–200. Pienempiä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 vuodessa.

IoT

Esineiden internet (IoT) heinäkuun yhteenveto

- Hide 'n Seek (HNS) -bottiverkko leviää sekä IoT-laitteisiin että tietokantapalvelimiin
  - » Teknisesti kehitysaskel ei ole suuri, mutta hyökkääjän toimintatavan muutos on merkittävä.
  - » HNS-botti myös käyttää omaa vertaisverkkoa komentokanavana ja selviää IoT-laitteen uudelleenkäynnistyksestä. Molemmat ominaisuudet ovat uusia IoT-haittaohjelmissa.
- Lukuisat IoT-laitteet ovat haavoittuvia klassiselle DNS rebind -hyökkäykselle
  - » Hyökkääjän antaman linkin klikkaaminen tietokoneella voi lähettää komentoja sisäverkon IoT-laitteille.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- Eurooppalainen sähköisen viestinnän säännöstö
  - » Jäsenmaat hyväksyivät EU:n televiestintäuudistuksen (*European Electronic Communications Code, EECC*) 29.6.2018 .
  - » Säännöksillä mm. tuetaan 5G-verkkojen ja muiden seuraavan sukupolven teknologioiden nopeaa ja laajaa käyttöönottoa, parannetaan ja yhtenäistetään sähköisten viestintäpalvelujen kuluttajansuojaa sekä luodaan julkinen varoitusjärjestelmä**,** jonka kautta kansalaisille voidaan lähettää kohdennettuja varoituksia hätätilanteista.
  - » Kun sovitut säädöstekstit on viimeistelty, on ne vielä hyväksyttävä virallisesti parlamentissa ja neuvostossa sekä julkaistava EU:n virallisessa lehdessä, minkä tapahtunee vuoden lopulla.
  - » Ks. lisää http://www.consilium.europa.eu/fi/press/press-releases/2018/06/29/telecoms-reform-to-bolster-better-and-faster-connectivity-across-eu-approved-by-member-states/
- Tiedonhallintalaki
  - » Valtiovarainministeriössä on valmisteltavana uusi tiedonhallinnan yleislaki, jonka on tarkoitus kattaa tiedonhallinnan suunnittelu- ja kuvausvelvollisuudet, tietoturvallisuusvaatimukset, asian- ja palvelunhallinnan rekisteröinnin perusteet sekä tietoaineistojen säilyttämistä ja arkistointia koskevat säännökset julkisessa hallinnossa.
  - » Hallituksen esityksen luonnos lähetettäneen lausuntokierrokselle elokuun puolivälissä, ja siitä järjestetään esittelytilaisuus syyskuun alussa, ks. https://vm.fi/tiedonhallintalain-valmistelu.

Ajankohtaiset lakiasiat

- Tiedustelulakipakettia koskevat hallituksen esitykset ovat edelleen valiokuntakäsittelyssä (HE 198/2017, 199/2017, HE 202/2017 ja HE 203/2017).
- Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018) on valiokuntakäsittelyssä.
- Hallituksen esitys laeiksi rajavartiolain ja ulkomaalaislain muuttamisesta sekä eräiksi niihin liittyviksi laeiksi on edelleen valiokuntakäsittelyssä (HE 201/2017).
  - » Laissa säädettäisiin mm. valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin.
- Hallituksen esitys laiksi puolustusvoimista annetun lain muuttamisesta (HE 72/2018) on valiokuntakäsittelyssä.
  - » Laissa säädettäisiin valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin.
- Hallituksen esitys laiksi Liikenne- ja viestintäviraston perustamisesta, Liikennevirastosta annetun lain muuttamisesta ja eräiksi niihin liittyviksi laeiksi (HE 61/2018) on valiokuntakäsittelyssä.

Ajankohtaiset lakiasiat

- Luonnos hallituksen esitykseksi laeiksi sähköisen viestinnän palveluista annetun lain ja julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain muuttamisesta on lausuttavana 15.8.2018 saakka.
  - » Lakiehdotuksilla mahdollistettaisiin uudenlaisen laajakaistaisen mobiilin viranomaisviestintäpalvelun tarjoaminen palvelumallilla, jossa verkko-operaattorina toimii kilpailutuksen perusteella valittu kaupallinen teleyritys ja palveluoperaattorina Suomen Erillisverkot Oy (ERVE) tai sen tytäryhtiö.
- Työryhmän ehdotus poliisilain 2 luvun muuttamisesta on lausuttavana 17.8.2018 saakka (SM009:00/2018).
  - » Lukuun lisättäisiin säännökset, joiden perusteella poliisilla olisi nykyistä kattavampi toimivalta puuttua lennokkien ja miehittämättömien ilma-alusten kulkuun.
- Oikeusministeriössä valmisteltu hallituksen esityksen luonnos vankeuslain, tutkintavankeuslain ym. muuttamisesta on lausuttavana 31.8.2018 saakka.
  - » Uusien säännösten nojalla Rikosseuraamuslaitoksella olisi toimivalta puuttua miehittämättömän kulkuneuvon liikkumiseen vankilan alueella tai sen yläpuolella, jos se olisi välttämätöntä vankilan järjestyksen ja turvallisuuden ylläpitämiseksi.

Kyberasioihin liittyvää uutisointia maailmalta

Suojelupoliisin mukaan **tulevaisuuden uhkat ovat virtuaalimaailmassa**. He arvioivat, että tulevaisuuden terroristi on "innovatiivinen diginatiivi", joka verkostoituu ja myös toimii virtuaalimaailmassa. Suojelupoliisin mukaan viranomaisten on välttämätöntä lähestyä ilmiötä kokonaisvaltaisesti ja siirtää torjuntatoimet siihen maailmaan, jossa nuoret elävät. Suojelupoliisi osallistui Suomi Areenan keskusteluihin paneelissa, jossa pohdittiin tulevaisuuden uhkia.

Pentagon on listannut venäläisiä ja kiinalaisia ohjelmistovalmistajia, joiden **palveluita ei suositella ostettavan**. Tämä Do Not Buy -lista muodostettiin siksi, että ohjelmistojen kerrotaan jättävän täyttämättä kansallisen turvallisuuden vaatimuksia. Useiden listalla olevien yritysten kerrotaan toimivan yleisten puolustusteollisuudessa ja puolustushallinnossa käytössä olevien standardien vastaisesti.

Yhdysvaltojen julkishallintoon lähetettiin useita kirjeitä, joiden sisältämässä **CD-levyssä levitettiin haittaohjelmaa**. Levyt oli lähetetty Kiinasta. CD-levyjen lähettäminen on totutusta poikkeava tapa levittää haittaohjelmaa, jotka nykypäivänä tulevat usein sähköpostitse.

Suositun pikaviestinsovellus **Telegramin viestiliikenne onnistuttiin kaappaamaan** Iranin valtionhallinnon ylläpitämissä viestintäverkoissa. Myös sisältö onnistuttiin ilmeisesti kaappaamaan. Kaappausten uskotaan liittyvän maassa oleviin protesteihin, joiden tietoja ja teemoja jaetaan Telegramin kautta.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi