Otto Laitinen

ÄLYPUHELIMIIN KOHDISTUVAT KYBERUHKAT JA NIILTÄ SUOJAUTUMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Laitinen, Otto
Älypuhelimiin kohdistuvat kyberuhkat ja niiltä suojautuminen
Jyväskylä: Jyväskylän yliopisto, 2019, 30 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Seppänen, Ville

Älypuhelimet kehittyvät jatkuvasti ja niiden käyttäjämäärät ovat suuressa kasvussa. Älypuhelimien käyttäjämäärät ovat kuitenkin houkutelleet alalle huomattavan määrän kyberrikollisuutta. Tämä tutkielma toteutettiin kirjallisuuskatsauksena, jonka tarkoituksena on vastata kahteen tutkimuskysymykseen, millaisia kyberuhkia älypuhelimiin kohdistuu ja millä tavoin älypuhelimiin kohdistuvilta kyberuhkilta voidaan suojautua? Tutkielmassa kävi ilmi, että älypuhelimiin kohdistuvien kyberuhkien määrä on jatkuvassa kasvussa ja niiden tehokkuus on parantunut viimeisten vuosien aikana. Älypuhelimiin kohdistuvista kyberuhkista suurin osa on haittaohjelmia nimeltä troijalainen. Tutkielmassa selviää myös, että älypuhelimiin suunnattujen haittaohjelmien kehittäjien motiivina on kasvavissa määrin raha, minkä takia älypuhelimien kyberuhkat suuntautuvat yhä enemmän käyttäjien henkilökohtaisiin tietoihin ja pankkipalveluihin. Tutkielmassa todetaan, että tehokkain ja yksinkertaisin tapa suojautua kyberuhkia vastaan on käyttää mahdollisimman monimutkaista suojakoodia ja asentaa laitteen käyttöjärjestelmäpäivitykset mahdollisimman pian niiden julkaisun jälkeen. Tutkielmassa kuitenkin käy ilmi, että tänä päivänä on tärkeää käyttää myös mobiilitietoturvaa käyttäjän yksityisyyden suojaamiseksi.

Asiasanat: älypuhelin, haittaohjelma, kyberturvallisuus, kyberuhka, tietoturva

ABSTRACT

Laitinen, Otto
Cyber threats on smartphones and how to protect against them
Jyväskylä: University of Jyväskylä, 2019, 30 pp.
Information Systems, Bachelor's Thesis
Supervisor: Seppänen, Ville

Smartphones are constantly evolving, and the number of the users is increasing. However, the high number of the smartphone users has attracted a significant amount of cybercrime to the industry. This thesis was conducted as a literature review to answer two research questions, what kind of cyber threats fall on smartphones and how can cyber threats to smartphones be defended? The study revealed that the number of cyber threats to smartphones has been steadily increasing and their efficiency has improved over the last few years. The most popular cyber threat to smartphones is a malicious program called trojan. This thesis also shows that the motive of malware developers has increasingly been money, which is why smartphone cyber threats are increasingly targeted to users' personal information and banking services. This thesis states that the most effective and simple way to protect against cyber threats is to use as complicate security code as possible and installing the system updates right away after they are released. However, the thesis shows that nowadays it is important to use mobile security service to protect user's privacy.

Keywords: smartphone, cyber security, cyber threat, information security, malware

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Puhelin ei ole enää pelkästään laite, jolla soitetaan. Älypuhelin on edistynyt tietojenkäsittely-ympäristö, joka voi sisältää kaiken digitaalisen informaation sen käyttäjästä ja jopa avaimet käyttäjän kotiin sekä pääsyn kaikkiin laitteisiin, jotka on liitetty verkkoon. Tämän takia älypuhelimien käyttäjien tulisi tiedostaa, kuinka suurta vahinkoa mobiilihaittaohjelmilla voidaan saada aikaan. Mobiilikäyttöjärjestelmistä on tullut täydellinen esimerkki fyysisen ja digitaalisen maailman yhdistymisestä. (Davis & Samani, 2018.) Julkisen hallinnon neuvottelukunta -JUHTA:n (2014) mukaan mobiililaite on mukana kannettava laite, jossa on internetselain ja johon pystyy asentamaan erilaisia sovelluksia. Mobiililaitteista suosituin ja käyttäjämäärän kasvultaan suurin laite on älypuhelin (Statista, 2017a; Statista, 2017b; Statista, 2018) ja sen takia tässä tutkielmassa keskitytään juuri älypuhelimiin kohdistuviin kyberuhkiin sekä niiltä suojautumiseen. Tutkielmassa on käytetty mainintaa mobiililaitteisiin kohdistuvista haittaohjelmista ja mobiiliuhkista silloin, kun lähteessä ei ole eritelty sitä mihin mobiililaitteeseen uhka kohdistuu. Älypuhelin on kuitenkin mobiililaite, jolloin mobiililaitteisiin kohdistuvat uhkat kohdistuvat myös älypuhelimiin. Tässä tutkielmassa painotetaan erityisesti älypuhelimiin kohdistettuja haittaohjelmia, joiden tarkoituksena voi olla esimerkiksi laitteen käyttäjän toimintojen vakoilu tai laitteen hidastaminen ja laitteessa olevan datan vaurioittaminen (Peng, Yu, & Yang, 2014).

Älypuhelimeen kohdistuva kyberuhka ei kuitenkaan aina ole haittaohjelma. Kyberuhkan voi aiheuttaa myös esimerkiksi suojaamaton, langaton verkkoyhteys tai hakkerin luoma vertaisverkko, jonka avulla kyberrikollinen voi seurata älypuhelimella tehtäviä toimintoja saastuttamatta käyttäjän laitetta. (Davis & Samani, 2018; Leavitt, 2014.) Ensimmäiset varsinaiset älypuhelimet tulivat markkinoille vuonna 1999, kun japanilainen NTT DoCoMo julkaisi i-mode järjestelmän, joka mahdollisti sähköpostin sekä internetselaimen käytön puhelimella (Islam & Want, 2014). Suurin mullistus älypuhelimien kehityksessä tapahtui vuonna 2007, jolloin yhdysvaltalainen Apple julkaisi ensimmäisen iPhonen (Islam & Want, 2014). Tämän jälkeen älypuhelimien kehitys on ollut erittäin nopeaa ja kehityksen uskotaan jatkuvan myös tulevaisuudessa. Onkin ennustettu, että älypuhelimet tulevat korvaamaan esimerkiksi perinteiset tieto-

koneet laitteina, jotka voidaan kytkeä telakan avulla erillisiin näyttöihin ja näppäimistöihin. (Islam & Want, 2014.)

Älypuhelimien käyttäjämäärien kasvu on lisännyt myös negatiivisia vaikutuksia ja esimerkiksi houkutellut alalle kasvavan määrän rikollisuutta (Becher, Freiling, Hoffmann, Holz, Ullenbeck & Wolf, 2011; Jiang & Zhou, 2012; Leavitt, 2011; Maslennikov, 2011; Peng, ym., 2014; Rastogi, Chen & Jiang, 2014; Wright, Dawson, & Omar, 2012). Tässä tutkielmassa tarkastellaan millaisia ovat älypuhelimiin kohdistuvat kyberuhkat ja mitä haittaohjelmia mobiililaitteiden keskuudessa on. Lisäksi tässä tutkielmassa käydään läpi, miten älypuhelimiin kohdistuvilta kyberuhkilta voidaan suojautua. Tutkielmassa myös kartoitetaan älypuhelimien haittaohjelmien kehitystä ja kasvua. Tämä tutkielma pyrkii vastaamaan kahteen tutkimuskysymykseen:

- Millaisia kyberuhkia älypuhelimiin kohdistuu?
- Millä tavoin älypuhelimiin kohdistuvilta kyberuhkilta voidaan suojautua?

Tämä tutkielma toteutettiin kirjallisuuskatsauksena. Tutkielman lähdekirjallisuus koostuu enimmäkseen tieteellisistä artikkeleista sekä konferenssijulkaisuista, mutta tutkielma sisältää myös lähdeaineistoa verkkosivuilta sekä raporteista. Yhdeksi tärkeimmistä lähteistä muodostui yhdysvaltalaisen virusten ja haittaohjelmien torjuntaan keskittyneen yrityksen, McAfeen vuoden 2018 mobiiliuhkaraportti. Lähdemateriaalin keräämiseen käytettiin IEEE- ja ACM-tietokantoja sekä Google – ja Google Scholar -hakukoneita. Hakusanoina käytettiin tutkielman avainsanoja. Aiheeseen liittyvien tieteellisten julkaisuiden määrä oli yllättävän rajallinen ja suurin osa tieteellisistä artikkeleista oli yli viisi vuotta vanhoja. Tästä syystä uusin tieto löytyi juurikin vuotuisista uhkaraporteista.

Tutkielma on jaettu neljään lukuun, eli johdantoon, kahteen sisältölukuun sekä yhteenvetoon. Ensimmäisessä sisältöluvussa käydään läpi älypuhelimen määritelmä sekä lyhyesti älypuhelimen historia ja kehitys, jonka jälkeen määritellään kyberturvallisuus käsitteenä. Tämän jälkeen käsitellään älypuhelimiin kohdistuvia kyberuhkia sekä haittaohjelmia. Toisessa sisältöluvussa käydään läpi, miten älypuhelimiin kohdistuvilta kyberuhkilta tulisi suojautua ja millainen tietous älypuhelimien käyttäjillä on laitteisiin kohdistuvista kyberuhkista. Yhteenvedossa käydään läpi tutkielman pääasiat ja pyritään vastaamaan tutkimuskysymyksiin.

2 ÄLYPUHELIMET, KYBERTURVALLISUUS JA KYBERUHKAT

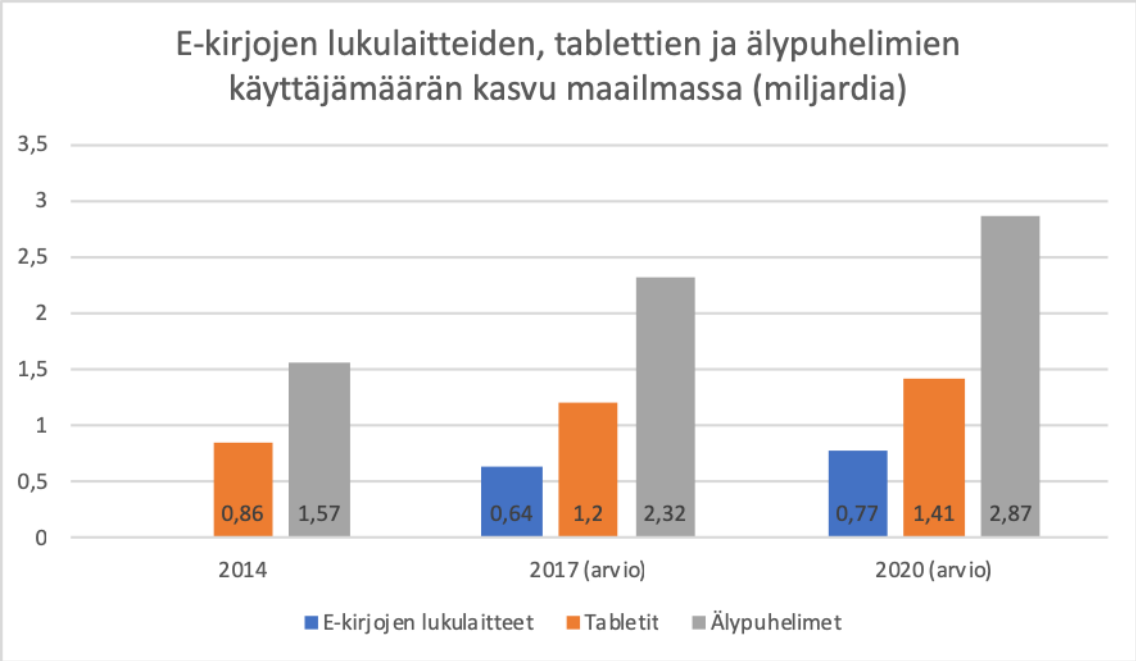
Älypuhelimet ovat kehittyneet huomattavasti viimeisen kymmenen vuoden aikana ja nykypäivänä ne sisältävätkin paljon samoja toimintoja, mitä tietokoneet. Älypuhelimien käyttäjämäärät ovat myös kasvaneet huomattavasti ja sen oletetaankin lähes kaksinkertaistuvan vuodesta 2014 vuoteen 2020, 1,57 miljardista käyttäjästä 2,87 miljardiin käyttäjään (Statista, 2017a). Tässä luvussa määritellään käsite älypuhelin, käydään läpi älypuhelimien historiaa ja tärkeimmät kehitysvaiheet, määritellään käsite kyberturvallisuus sekä paneudutaan siihen, millaisia kyberuhkia ja haittaohjelmia älypuhelimiin kohdistuu.

2.1 Älypuhelimet

Julkisen hallinnon tietohallinnon neuvottelukunta –JUHTA (2014) määrittelee mobiililaitteen laitteeksi, joka on mukana kannettava ja siihen on asennettavissa sovelluksia tai siinä on internetselain. Mobiililaitteita ovat esimerkiksi älypuhelimet, tabletit, e-kirjojen lukulaitteet sekä älypuhelimien ja tablettien välille asennettavat älylaitteet (Julkisen hallinnon tietohallinnon neuvottelukunta – JUHTA, 2014). Tarkasteltaessa kolmen eri mobiililaitteen käyttäjämäärän kasvua maailmanlaajuisesti, jotka ovat älypuhelin, tabletti sekä e-kirjojen lukulaite, kuviosta 1 huomataan että älypuhelimien käyttäjämäärä sekä käyttäjämäärän kasvu niin suhteellisesti kuin määrällisestikin on huomattavasti suurin (Statista, 2017a; Statista, 2017b; Statista, 2018). Tästä syystä tässä tutkielmassa keskitytään juuri älypuhelimien kyberuhkiin ja niiltä suojautumiseen. Älypuhelimien ensiaskeleet tapahtuivat 1990-luvulla, jolloin esiteltiin IBM:n (International Business Machines Corporation) Simon, Nokian Communicator ja Qualcommin PdQ, joissa yhdistyivät tietojenkäsittelyn sekä matkapuhelimen toiminnallisuudet (Islam & Want, 2014). Nämä puhelimet olivat kuitenkin ennemmin matkapuhelimia lisäominaisuuksilla, koska niistä puuttuivat esimekiksi internetselain ja pääsy sähköpostiin, jotka ovat älypuhelimille tyypillisiä toimintoja. Vuonna 1999 tämä kuitenkin muuttui, kun japanilainen NTT DoCoMo julkaisi i-mode

järjestelmän, joka mahdollisti sähköpostien lukemisen ja C-HTML-kielellä kirjoitettujen internetsivujen selaamisen matkapuhelimella. (Islam & Want, 2014.) Suurin mullistus älypuhelimien kehityksessä tapahtui vuonna 2007, jolloin Apple julkaisi ensimmäisen iPhonen ja siinä toimivan iOS käyttöjärjestelmän. Apple avasi App Storen vuonna 2008, josta ladattavat sovellukset luovat huomattavasti uusia tapoja käyttää älypuhelinta. Samana vuonna Google julkaisi Android -käyttöjärjestelmän ja sille oman sovelluskauppansa, jonka jälkeen Android ja iOS ovat olleet johtavia älypuhelimien käyttöjärjestelmiä. (Islam & Want, 2014.) Vuonna 2018 tuli täyteen kymmenen vuotta siitä, kun Apple App Store sekä Google Play on avattu. Vaikka älypuhelimien sovelluskauppakonsepti ulottuu aina Symbian käyttöjärjestelmän aikoihin asti, kuten Nokia ja Ericsson puhelimiin, voidaan Applen sekä Googlen luomia sovelluskauppoja pitää tämän päivän sovelluskauppojen esimerkkeinä. Näiden kymmenen vuoden aikana, molemmat yritykset ovat joutuneet selvittämään turvallisuuteen liittyviä tapauksia, samalla kun jatkavat kamppailua julkaisujen jälkeisten ongelmien kanssa. (Davis & Samani, 2018.)

Älypuhelimien käyttäjämäärät ovat kasvaneet huomattavasti viimeisten vuosien aikana (kuvio 1). Kuten kuviosta 1 on nähtävissä, tulevat älypuhelimien käyttäjämäärät arvioiden mukaan lähes kaksinkertaistumaan vuodesta 2014 vuoteen 2020. Ennusteiden mukaan älypuhelimet tulevat korvaamaan perinteiset tietokoneet laitteina, jotka voidaan telakoida erillisiin näyttöihin ja näppäimistöihin (Islam & Want, 2014). Älypuhelimet ovat suosituimpia laitteita internetsivujen selailussa, sähköpostin ja sosiaalisen median käyttämisessä sekä verkkokauppaostosten tekemisessä. Tämä johtuu yksinkertaisesti siitä, että älypuhelimet ovat tarpeeksi pienikokoisia kannettavaksi aina mukana ja näin ollen niitä voi käyttää lähes aina ajasta ja paikasta riippumatta. Älypuhelimien suosion kasvu on kuitenkin houkutellut alalle myös kyber- ja tietoturvarikollisia. (Becher, ym., 2011; Jiang & Zhou, 2012; Leavitt, 2011; Maslennikov, 2011; Peng, ym., 2014; Wright, ym., 2012.)



KUVIO 1 E-kirjojen lukulaitteiden, tablettien ja älypuhelimien käyttäjämäärän kasvu maailmassa (Statista, 2017a; Statista, 2017b; Statista, 2018).

2.2 Kyberturvallisuus

Sana kyber jakaa ihmisten mielipiteitä hyvinkin voimakkaasti, eikä sanalle löydy suomen kielessä vakiintunutta määritelmää. Kyber-sana on lähtöisin kreikan kielen sanasta kybereo, joka tarkoittaa suomen kielellä opastaa, ohjata, hallita. (Limnéll, 2014.) Limnéllin (2014) mukaan suomen kielen sana kyber on johdettu englannin kielen sanasta cyber, joka viittaa virtuaalitodellisuuteen, tietokonekulttuuriin ja informaatioteknologiaan, joihin myös tässä tutkielmassa kybersanalla viitataan. Lisäksi Limnéll (2014) mainitsee, että sanaa kyber käytetään harvoin yksinään, vaan se esiintyy lähes aina määrittelevänä osana yhdyssanaa.

Kyberturvallisuus on määritelty Merriam-Webster sanakirjan mukaan toimenpiteinä, jotka suoritetaan tietokoneen tai tietokonejärjestelmän suojaamiseksi luvatonta käyttöä tai hyökkäystä vastaan (Merriam-Webster, 2019; Von Solms & Van Niekerk, 2013). The International Telecommunication Unionin mukaan kyberturvallisuus koostuu työkaluista, menettelytavoista, turvallisuuskäsitteistä, turvallisuustoimenpiteistä, ohjeistuksesta, riskienhallinnan lähestymistavoista, harjoittelusta, parhaista käytänteistä, vakuuksista sekä teknologioista, joita voidaan käyttää suojaamaan kyberympäristöä, sekä organisaation ja käyttäjän varoja. Kyberturvallisuuden tarkoituksena on varmistaa organisaation turvallisuusominaisuuksien saavuttaminen ja ylläpito sekä suojata käyttäjien varat ja tiedot kyberympäristössä merkittäviltä turvallisuusriskeiltä. (Von Solms & Van Niekerk, 2013.) Sanastokeskus TSK:n mukaan kyberturvallisuus on tila, jossa kyberympäristössä oleviin kriittisiin infrastruktuureihin tai muihin kyberympäristöstä riippuvaisiin toimintoihin kohdistuvat riskit ja uhkat ovat

kontrolloitavissa (Sanastokeskus TSK, 2017). Tästä voidaankin huomata, että myös kyberturvallisuudelle on useita erilaisia määritelmiä, jotka täydentävät toisiaan.

2.3 Älypuhelimiin kohdistuvat haittaohjelmat ja kyberuhkat

Tässä alaluvussa käsitellään älypuhelimien haittaohjelmia ja älypuhelimiin kohdistuvia kyberuhkia. Sanastokeskus TSK:n mukaan kyberuhka on kybertoimintaympäristöön kohdistuva haitallinen tapahtuma, joka toteutuessaan vaarantaa kybertoimintaympäristöstä riippuvaisen toiminnon. Sanastokeskus TSK:n mukaan haittaohjelman tarkoituksena on luoda laitteen käyttäjän kannalta ei-haluttuja toimintoja tietojärjestelmissä tai sen osissa. Haittaohjelmia ovat siis esimerkiksi madot, troijalaiset ja virukset ja haittaohjelmat luovat älypuhelimien käyttäjille kyberuhkia, mutta kyberuhka ei aina välttämättä ole haittaohjelma. Leavitt (2011) kertoo artikkelissaan, kuinka kasvava älypuhelimien käyttö on lisännyt mobiililaitteiden kyberturvallisuusriskejä. Markkina-analyysiyrityksen ABI Researchin mukaan maailmassa on ollut vuonna 2010 370 miljoonaa älypuhelinta (Leavitt, 2011). Virusten ja haittaohjelmien torjuntaan erikoistuneen, yhdysvaltalaisen yrityksen McAfeen teettämästä McAfee Labsin uhkaraportista vuoden 2010 viimeiselle neljännekselle huomataan, että älypuhelimiin suunnattujen haittaohjelmien määrä oli kasvanut 46 prosenttia edelliseen vuoteen verrattuna (Leavitt, 2011). Seuraavaksi käydään läpi yleisimpiä älypuhelimien haittaohjelmia, jonka jälkeen käsitellään älypuhelimiin kohdistuvia kyberuhkia erilaisina ilmiöinä.

2.3.1 Älypuhelimiin kohdistuvat haittaohjelmat

Mobiililaitteille suunnattuja haittaohjelmia on ollut olemassa jo pitkään. Vuonna 2004 löydettiin ensimmäinen älypuhelimelle suunnattu mato Cabir, joka toimi Symbian-käyttöjärjestelmässä. Cabir levisi hyödyntäen Bluetooth-yhteyttä ja yksi sen aiheuttamista ja parhaiten tunnetuista epidemioista tapahtui Helsingissä yleisurheilun maailmanmestaruuskilpailuissa vuonna 2005. (Leavitt, 2005; Peng, ym., 2014.) Bluetoothin käyttäminen haittaohjelman levittämiseen on kuitenkin harvinaista (Leavitt, 2011). Vuoden 2010 lopussa mobiilihaittaohjelmista oli löytynyt 153 eri ryhmää (families) ja yli 1000 eri versiota (modifications), ja samalla haittaohjelmien tartuntamäärä oli lähes kaksinkertaistunut 17 kuukauden aikana (Peng, ym., 2014). Vuoden 2010 elokuussa Kaspersky Lab löysi ensimmäisen Androidille suunnatun troijalaisen, joka nimettiin Troijan-SMS.AnroidOS.FakePlayer.a:si (FakePlayer). FakePlayer naamioitui mediasoittimeksi, joka tämän jälkeen lähetti tekstiviestejä tiettyihin numeroihin ilman käyttäjän lupaa, aiheuttaen näin käyttäjälle mahdollisia lisäkustannuksia. (Maslennikov, 2011; Peng, ym., 2014.) Vuonna 2010 Juniper MTC:n havaitsemista mobiilihaittaohjelmista suurin osa oli suunnattu SymbianOs- ja J2ME-perusteisiin laitteisiin, mutta vuonna 2011 yritys huomasi haittaohjelmista suu-

ren osan siirtyneen Android-pohjaisiin laitteisiin (Peng, ym., 2014). Kaspersky Labin keräämän tiedon mukaan, vuonna 2012 Android-haittaohjelmia oli 126 ryhmää ja 4139 versiota, kun samaan aikaan J2ME-haittaohjelmia oli 63 ryhmää ja 1682 versiota ja Symbian-haittaohjelmia oli 111 ryhmää ja 435 versiota (Peng, ym., 2014).

Yksi McAfeen merkittävimmistä löydöistä vuoden 2018 mobiiliuhkaraportissa oli Androidille suunnattu Grabos-kampanja (Davis & Samani, 2018). Grabos-kampanjan tarkoituksena oli tyrkyttää haitallisia ohjelmia pahaa aavistamattomille käyttäjille. Grabos-kampanjan huijausmuoto tunnetaan nimellä payper-download -huijaus. (Davis & Samani, 2018.) Kokonaisuudessaan 144 sovellusta Google Play -kaupassa tunnistettiin osaksi kampanjaa, jonka jälkeen ne poistettiin kaupasta. Arvion mukaan sovelluksia ladattiin kampanjasta 17,5 miljoonaan älypuhelimeen, ennen kuin kampanja saatiin lakkautettua. (Davis & Samani, 2018.)

McAfeen vuoden 2018 mobiiliuhkaraportin mukaan, haittaohjelmakampanjoita on kohdistettu Google Play -kaupan käyttäjiin lähes heti sen avaamisesta lähtien: ensimmäisestä Droid09 nimisestä pankkitroijalaisesta (banking trojan) viimeisimpiin mainostenklikkaushuijauksiin (ad-click fraud) kehitettyihin sovelluksiin ja Bitcoinin piilolouhintasovelluksiin, jotka tänä päivänä saastuttavat Google Play -kauppaa viikko toisensa jälkeen (Davis & Samani, 2018). Vuosien aikana saastuneiden laitteiden määrä on kasvanut mahdollisesti jopa miljooniin, samalla kun McAfee on löytänyt uusia, aggressiivisia haittaohjelmakampanjoita (Davis & Samani, 2018). Android-käyttöjärjestelmä on säilynyt houkuttelevana alustana haittaohjelmien kehittäjille. Suurimpia houkutteita luovat sen yli kaksi miljardia käyttäjää sekä Androidin suhteellisen avoin sovelluskauppa. McAfee löysi vuoden 2017 aikana 30 % enemmän uhkaavia ryhmiä Google Play -kaupasta kuin edellisenä vuotena, mikä tekee virallisesta Google Play -kaupasta epäturvallisen käyttäjilleen. (Davis & Samani, 2018.) Applenkaan käyttäjät eivät ole täysin turvassa, koska esimerkiksi ”kuolleet sovellukset” (dead apps) aiheuttavat kyberuhkia. Kuolleista sovelluksista puhuttaessa tarkoitetaan sitä, että Applen havaitessa turvallisuuteen tai yksityisyyteen liittyvän ongelman, yritys poistaa sovelluksen kaikessa hiljaisuudessa App Storesta ilman mitään julkista ilmoitusta. (Davis & Samani, 2018.) Tämä altistaa miljoonien käyttäjien laitteita haittaohjelmille, joiden alkuperäisenä kohteena ovat kehitystyöntekijät samoin kuin lähdekoodivuodoille, mikä puolestaan auttaa hakkereita ymmärtämään paremmin, miten he voivat hyötyä saastuneesta laitteesta (Davis & Samani, 2018).

Pengin ym. (2014) mukaan, suurimmat syyt sille, miksi haittaohjelmien määrä mobiililaitteissa kasvaa ovat:

- Älypuhelimien hinnat laskevat ja yhä useampi jälleenmyyjä on osallisena älypuhelimien tuotannossa.
- Androidin perustuminen avoimeen lähdekoodiin mahdollistaa haittaohjelmien kirjoittajien syvemmän tutustumisen mobiilialustoihin.
- Älypuhelimien käyttäjät tallentavat suuria määriä henkilökohtaista dataa laitteisiinsa. Tämä houkuttelee haittaohjelmien kehittäjiä, jotka hyötyvät taloudellisesti identiteettivarkauksista tai pankkikorttien väärinkäytöistä.

- Älypuhelimien ja tietokoneiden ohjelmointi on samankaltaista, siksi haittaohjelmien kehittäjien on helppo siirtyä tietokoneympäristöstä älypuhelimiin.

Mobiililaitteiden haittaohjelmat on luokiteltu samalla tavalla kuin tietokoneissa, sillä niiden toimintaperiaate on sama. Mobiililaitteisiin kohdistuvia haittaohjelmia ovat esimerkiksi virukset, madot, troijalaiset, vakoiluohjelmat, takaovet (backdoor) sekä bottiverkot (Peng, ym., 2014). Seuraavaksi käydään läpi tarkemmin älypuhelimiin kohdistuvia haittaohjelmia ja niiden toimintatapoja.

Virus on haittaohjelma, joka asentuu laitteen järjestelmään joko ohjelmiston tai laitteiston kautta käyttäjän huomaamatta, minkä jälkeen se kiinnittää itsensä johonkin tiedostoon. Tämän jälkeen virus aloittaa itsensä kopioimisen ja tehtävän suorittamisen, johon se on ohjelmoitu. Virus saattaa vaurioittaa ohjelmistoa tai dataa, tai se saattaa suorittaa palvelunestohyökkäyksiä. (Peng, ym., 2014.)

Mato on haittaohjelma, joka tarttuu laitteen järjestelmään ilman käyttäjän tiedostamista. Toisin kuin virus, mato pystyy leviämään automaattisesti laitteesta laitteeseen ilman käyttäjän toimenpiteitä. Mato kopioi itseään ja voi lähettää jopa tuhansia kopioita itsestään jokaisesta tartunnan saaneesta laitteesta, esimerkiksi hyödyntäen käyttäjän sähköpostia. Madoilla voi olla tuhoisia vaikutuksia internetliikenteeseen, internetsivuihin tai käyttäjän omaan laitteeseen. (Peng, ym., 2014.)

Vakoiluohjelma kerää tietoa käyttäjän laitteesta, jonka jälkeen tieto luovutetaan usein kolmannelle osapuolelle (Peng, ym., 2014). Vakoiluohjelman avulla hakkerit voivat internetin välityksellä kaapata laitteen, joka mahdollistaa puheluiden salakuuntelun, tekstiviestien ja sähköpostien lukemisen ja jopa käyttäjän sijainnin paikantamisen GPS:n avulla (Leavitt, 2011). Vakoiluohjelma voi myös luoda laitteeseen piilotetun tukiaseman, jonka avulla hakkeri voi avata laitteen mikrofonin ilman, että laite soi. Tämän avulla hakkeri tai kolmas osapuoli pystyy kuuntelemaan laitteen lähellä käytävät keskustelut. (Leavitt, 2011.) Vakoiluohjelman avulla hakkeri pystyy myös esimerkiksi hankkimaan käyttäjän pankkikorttitietoja, salasanoja, keräämään yhteystietoja, seuraamaan internetkäyttäytymistä tai selaamaan laitteen tiedostoja (Peng, ym., 2014).

Troijalainen on haittaohjelma, joka naamioituu vaarattomaksi ohjelmaksi. Käyttäjän ladattua ja aktivoitua troijalaisen, se voi hyökätä laitteeseen useita kertoja. Troijalainen voi poistaa tiedostoja, avata pop-up ikkunoita, varastaa tietoja tai levittää muita haittaohjelmia, kuten viruksia. Troijalaiselle on myös tavallista luoda takaovia, joiden avulla hakkereilla on pääsy tartunnan saaneeseen laitteeseen (Peng, ym., 2014; Vashisht, Gupta, Singh & Mudgal, 2016). Takaovi on haittaohjelma, jonka avulla hakkeri pystyy saamaan etähallinnan saastuneeseen laitteeseen (Peng, ym., 2014). Tämän avulla hakkeri voi käytännössä varastaa kaiken laitteella olevan datan ja käyttää laitetta omiin tarkoituksiinsa. Älypuhelimista puhuttaessa, haitallinen sovellus on lähes aina troijalainen (Leavitt, 2011; Peng, ym., 2014; Vashisht, ym., 2016). Esimerkki älypuhelimen troijalaisesta on Androidille suunnattu Soundminer, joka pystyy kaappaamaan henkilökohtaisia tietoja laitteen mikrofonin avulla. Vuonna 2011 troijalainen oli suomalaisen tietoturvayhtiö F-Secure Lab's Q4 2011 Mobile Threat Reportin

mukaan suurin uhka mobiililaitteille kattaen jopa 74 % haittaohjelmista (Peng, ym., 2014). Tästä voidaan päätellä, että juurikin haitalliset sovellukset ovat suuri, elleivät jopa suurin uhka mobiililaitteille.

Bottiverkko antaa hyökkääjille mahdollisuuden saada etähallintaan joukon saastuneita laitteita (Leavitt, 2011; Peng, ym., 2014). Hyökkääjät käyttävät bottiverkkoja usein käynnistääkseen DDoS-hyökkäyksiä, lähettääkseen suuria määriä roskapostia tai kerätäkseen henkilökohtaisia tietoja (Peng, ym.,2014). Bottiverkolla tapahtunut laitteen saastuminen on usein peräisin sähköpostista, haitallisesta sovelluksesta tai internetsivulta (Leavitt, 2011). Leavittin (2011) mukaan, helpoin tapa hyökkääjälle hyötyä bottiverkosta, on ottaa saastunut laite hallintaan ja lähettää sillä joko teksti- tai multimediaviestejä palvelunumeroihin, jotka tuovat lisäkustannuksia laitteen omistajalle. Yllä käsitellyt älypuhelimiin kohdistuvat haittaohjelmat ja niiden kuvaukset löytyvät tiivistetysti seuraavan sivun taulukosta (taulukko 1).

TAULUKKO 1 Haittaohjelmat (Leavitt, 2011; Peng, ym., 2014; Vashisht, ym., 2016)

Haittaohjelma	**Kuvaus**
Virus	Asentuu järjestelmään ja kiinnittyy johonkin tiedostoon, jonka jälkeen aloittaa itsensä kopioimisen ja tehtävän suorittamisen, mihin se on ohjelmoitu.
Mato	Asentuu järjestelmään ja aloittaa itsensä kopioimisen. Pystyy leviämään laitteesta laitteeseen ilman käyttäjän toimenpiteitä.
Vakoiluohjelma	Kerää tietoa käyttäjän laitteesta, jonka jälkeen tieto usein luovutetaan kolmannelle osapuolelle.
Troijalainen	Naamioituu vaarattomaksi ohjelmaksi, mutta aktivoiduttuaan aloittaa muiden haittaohjelmien levittämisen tai luo takaovia. Älypuhelimien selkeästi yleisin haittaohjelma.
Takaovi	Takaoven avulla saa etähallinnan laitteesta, jolloin hakkeri pystyy varastamaan kaiken laitteessa olevan datan ja käyttämään laitetta omiin tarkoituksiinsa.
Bottiverkko	Antaa hyökkääjälle mahdollisuuden ottaa etähallintaan joukon saastuneita laitteita.

2.3.2 Älypuhelimiin kohdistuvat kyberuhkat ilmiöinä

Ihmiset luottavat saamiinsa mainoksiin esimerkiksi sosiaalisessa mediassa enemmän mobiililaitteilla kuin tietokonetta käyttäessä, ja siksi haittaohjelmat ja niiden leviäminen on vaarallisempaa mobiililaitteissa. Etenkin bottiverkkojen käyttö sekä tietojen kalastelu ovat suuri uhka mobiililaitteille. (Leavitt, 2011.) Symantec'sin vuonna 2011 teettämän Internet Security Threat Reportin mukaan yli puolet sen hetkisistä Android-käyttöjärjestelmään suunnatuista uhkista keräsi laitteen dataa tai seurasi käyttäjän toimintoja (Morrow, 2012).

McAfeen vuoden 2018 mobiiliuhkaraportin mukaan vuoden 2017 yleisin Google Play -kaupan käyttäjiin kohdistuva petostapa oli ad click fraud -haittaohjelmat, jotka kattoivat 36 % Google Play -kaupassa esiintyvistä haittaohjelmista (Davis & Samani, 2018). Ad click fraud -haittaohjelmat tai ad click -troijalaiset ovat haittaohjelmia, jotka esittävät tarjoavansa jotakin palvelua, mutta samanaikaisesti avaa taustalla mainoksia tuottaen rahallista hyötyä sovelluksen kehittäjälle (Davis & Samani, 2018). Toisiksi suurin Google Play -kaupan haittaohjelmaluokka vuonna 2017 oli vakoiluohjelmat 23 %, kolmantena bottiverkot 22 %, neljäntenä pankkitroijalaiset 12 %, viidentenä kryptovaluuttojen piilolouhintasovellukset 5 % ja kuudentena rootkitit eli piilohallintaohjelmat 2 %. Kaikki haittaohjelmaluokat rootkit pois lukien ovat olleet kasvussa edelliseen vuoteen verrattuna. Maailmanlaajuinen piikki kryptovaluuttojen louhintaan kohdistuvissa haittaohjelmissa tapahtui suunnilleen samaan aikaan, kun Bitcoinin suurin arvonnousu tapahtui. (Davis & Samani, 2018.)

Vuoden 2018 mobiiliuhkaraportin mukaan, McAfee havaitsi vuonna 2017 Google Play -kaupassa enemmän mobiililaitteille suunnattuja haittaohjelmia kuin edellisinä vuosina (Davis & Samani, 2018). Puolueettomat, haittaohjelmia mittaavat testit osoittavat, että Google Play -kaupan sisäinen haittaohjelmia paljastava Google Play Protect -ohjelma ei onnistunut havaitsemaan tai puolustautumaan yleisimpiäkään haittaohjelmakampanjoita vastaan (Davis & Samani, 2018).

Haittaohjelmien kokonaismäärän kasvu on ollut huomattavaa (Davis & Samani, 2018). McAfeen vuoden 2018 mobiiliuhkaraportin mukaan haittaohjelmien kokonaismäärä on kasvanut vuoden 2015 viimeisestä neljänneksestä vuoden 2017 kolmanteen neljännekseen noin 7,5 miljoonasta yli 20 miljoonaan. Samalla aikavälillä havaittiin keskimäärin 1,5-2 miljoonaa haittaohjelmaa vuosineljänneksessä, mutta vuoden 2017 kolmannessa neljänneksessä havaittiin yli 2,5 miljoonaa uutta mobiilihaittaohjelmaa. Suurin osa McAfeen vuonna 2017 havaitsemista mobiilihaittaohjelmista oli ad click -troijalaisia. (Davis & Samani, 2018.)

Haittaohjelmien kehittäjien motiivina on kasvavissa määrin raha ja tästä syystä haittaohjelmien kehittäjät pyrkivät keksimään yhä enemmän keinoja, joilla rahallistaa toimialaa (Davis & Samani, 2018). Selkeänä merkkinä tästä voidaan pitää sitä, että haittaohjelmien kehittäjät ovat siirtäneet perinteisiä, tietokoneille suunnattuja pankkitroijalaisten ja kiristysohjelmien vektoreita mobii-

lialustoille (Davis & Samani, 2018). Mobiilihaittaohjelmat ottivat ensiaskeleensa kohti toimialan rahallistamista käyttäen pitkän matkan huijauspuheluita sekä -tekstiviestejä (Davis & Samani, 2018). Aasiassa on tänä päivänä yleistä, että haittaohjelmat voivat periä saastuneilta laitteilta hyvinkin pieniä summia, kuten vain muutamia jenejä ja tästä johtuen käyttäjät saattavat huomata, että jokin on vialla vasta useiden kuukausien päästä. Kiinan poliisi on nimennyt tämän monkey suck -huijaukseksi. (Davis & Samani, 2018.) Toinen tapa tuottaa rahaa mobiilihaittaohjelmilla on ollut Itä-Euroopassa suositumpi smash-and-grab -strategia. Siinä on tarkoituksena saastuttaa laite, jonka jälkeen suoritetaan kertaluontoinen noin 45-100:n Yhdysvaltain dollarin arvoinen maksusuoritus. (Davis & Samani, 2018.) Tämän uskotaan luoneen pohjan mobiilikiristysohjelmille, joiden kohteina ovat käyttäjät Pohjois-Amerikassa ja jotka tänäkin päivänä ovat pääosin Itä-Eurooppalaisten haittaohjelmien kehittäjien luomia ja operoimia. (Davis & Samani, 2018.) McAfeen arvion mukaan vuonna 2010 tuottavimmalla haittaohjelmakampanjalla oli potentiaalia tehdä tulosta 100 000:n ja 300 000:n dollarin väliltä. Nykyisen arvion mukaan, tänä päivänä täysin kehittynyt haittaohjelmakampanja, joka hyödyntää ad click -huijausta, pay-per-download -huijausta, tai laajalle levinnyttä pankkitroijalaista, voi tuottaa tulosta 1-2:n miljoonan Yhdysvaltain dollarin edestä. Jos mobiilihaittaohjelmat jatkavat kehittymistään samaan malliin, niiden voidaan olettaa tekevän miljarditulosta vuoteen 2020 mennessä. (Davis & Samani, 2018.)

McAfee Labs havaitsi yli 16 miljoonaa mobiilihaittaohjelmatartuntaa pelkästään vuoden 2017 kolmannella neljänneksellä, mikä on lähes kaksi kertaa suurempi määrä kuin vuotta aiemmin (Davis & Samani, 2018). Mobiiliuhkia on havaittu ympäri maailmaa, mutta suurimmat tartuntamäärät on löydetty Venäjältä, Etelä-Koreasta ja Kiinasta. Kaikilla näillä tartunta-aalloilla on yhteys, haittaohjelmien kehittäjien halu ansaita rahaa. (Davis & Samani, 2018.) Ajan saatossa perinteiset huijausmuodot, kuten lisämaksutekstiviestit ja maksupetokset ovat korvaantuneet bottiverkko-ad fraudeilla, pay-per-download huijauksilla ja kryptovaluuttojen louhintahaittaohjelmilla, joilla voidaan tehdä miljoonien tulosta. Lisäksi kryptovaluuttahaittaohjelmissa on havaittu 70 prosentin ja mobiililaitteille suunnatuissa pankkitroijalaisissa on havaittu 60 prosentin määrällinen kasvu vuosien 2017 ja 2018 aikana. (Davis & Samani, 2018.) McAfee on löytänyt yhdessä esimerkissään piraattiversioita laillisista sovelluksista, joita voidaan käyttää mainostulojen tuottamiseen (Davis & Samani, 2018). Piraattiversiosovellusten kehittäjät voivat myös myöhemmin myydä kehittäjäoikeudet rikollisille organisaatioille, jotka käyttävät niitä haitta- ja vakoiluohjelmien levittämiseen. Molemmissa tapauksissa piraattisovellusten kehittäjien motiivina on rahan tuottaminen. (Davis & Samani, 2018.) McAfee ennustaakin, että kyberrikollisten suuntaamat hyökkäykset mobiililaitteille tulevat tasaisesti kasvamaan samalla, kun rikollisten taidot hyödyntää haittaohjelmia ja muuttaa niitä rahaksi kasvavat (Davis & Samani, 2018).

Pankkitroijalaisista esimerkkeinä voidaan pitää McAfeen löytämiä Marcher- ja LokiBot-haittaohjelmia (Davis & Samani, 2018). Marcher-haittaohjelma hyödyntää Android-käyttöjärjestelmän automaattiseen asennukseen liittyviä haavoittuvuuksia. Marcher-haittaohjelma saastutti miljoonia Google Play -kaupan käyttäjien laitteita tekeytymällä laillisiksi sovelluksiksi, kuten media-

soittimiksi, peleiksi tai järjestelmän apuohjelmiksi. (Davis & Samani, 2018.) Pankkitroijalaisista edistyksellisimpänä voidaan kuitenkin pitää LokiBot-haittaohjelmaa. LokiBot-haittaohjelma sisältää kaikki Marcher-haittaohjelman ominaisuudet, mutta niiden lisäksi siinä on myös kryptokiristysohjelman ominaisuuksia sekä muita haitallisia toimintoja. LokiBot-haittaohjelma pystyy salaamaan tiedostoja, lukitsemaan laitteita, ja lähettämään valeilmoituksia, joilla se voi huijata käyttäjän avaamaan verkkopankkisovelluksen sekä antaa hyökkääjälle mahdollisuuden imitoida uhrin IP-osoitetta, jota hyökkääjä voi käyttää muihin petollisiin tarkoituksiin. (Davis & Samani, 2018.) LokiBot-haittaohjelma on kohdistettu yli sataa rahoituslaitosta vastaan ympäri maailmaa ja McAfee arvioi sen tuottaneen lähes kahden miljoonan Yhdysvaltain dollarin tuotot piilohallintaohjelmamyynnillä (Davis & Samani, 2018).

Pankkitroijalaiset ovat hyökänneet niin suurin kansainvälisiin pankkeihin, kuin pienempiinkin pankkeihin (Davis & Samani, 2018). Pankkitroijalaiset ovat käyttäneet levitäkseen erityisesti mobiililaitteisiin suunniteltuja mobiilisovelluksia tai tietojenkalastelukampanjoita (Davis & Samani, 2018). Tästä esimerkkinä on suurimpiin korealaisiin pankkeihin suunnattu, Android-käyttöjärjestelmällä toimiva, MoqHao -haittaohjelma. MoqHao -haittaohjelma leviää tekstiviestien välityksellä ja pyytää vastaanottajaa vahvistamaan tilinsä valokuvalla itsestään. Sen jälkeen, kun viestin vastaanottaja on avannut haitallisen linkin, ohjelma asentaa valeverkkopankkisovelluksen käyttäjän laitteeseen. Tämän jälkeen haittaohjelma hakee laitteesta kaikki viralliset verkkopankkisovellukset ja poistaa ne. (Davis & Samani, 2018.) Perinteisten pankkien lisäksi, kryptovaluuttalompakot ovat olleet hyökkääjien kohteena. Vuonna 2018 McAfee on havainnut jopa 80 prosentin määrän kasvun haittaohjelmissa pelkästään liittyen Bitcoinin louhintaan. (Davis & Samani, 2018.)

Sosiaalisen median käyttö on lisääntynyt jatkuvasti ja kuten aiemmin on mainittu, on myös mobiililaitteiden määrä kasvanut ja sosiaalisen median suosituin selaamistapa on mobiililaite (Leavitt, 2014). Tästä syystä hakkerit ovat ryhtyneet hyödyntämään sosiaalista mediaa mobiilihaittaohjelmien levityksessä. Ihmiset luottavat sosiaalisessa mediassa näkemiinsä linkkeihin, jotka ovat heidän ystäviensä sosiaalisen median sivuilla, jolloin he klikkaavat niitä. Linkin avaaminen voi johtaa edellä mainittujen haittaohjelmien asentumiseen tai identiteettivarkauksiin. (Leavitt, 2014.) Sosiaalinen media on myös helpottanut tietojen kalastelua, sillä sosiaalinen media sisältää jo valmiiksi suuren määrän henkilökohtaista tietoa. Tietojen kalastelua mobiililaitteiden käyttäjiltä helpottaa myös se, että kalastelu on mahdollista ei vain sähköpostin, mutta myös tekstiviestien avulla. (Leavitt, 2014.)

Koska älypuhelin on todennäköisimmin aina käyttäjän mukana, on suojaamattomista langattomista verkoista tullut kyberuhka älypuhelimien käyttäjille, etenkin maissa, joissa mobiilidatan käyttö ei ole tavallisesti rajoittamatonta. Suojaamatonta langatonta verkkoyhteyttä käyttäessä, hakkeri voi salakuunnella ja hallita käyttäjän verkkoliikennettä. Hakkeri voi myös luoda vertaisverkon, joka näyttää käyttäjälle tarjoavan hyvän yhteyden. Tämä houkuttelee käyttäjää yhdistämään verkkoon, jolloin hakkeri voi seurata uhrin verkkoliikennettä hänen tietämättään ja urkkia arkaluontoisia tietoja, kuten verkkopankkitunnuksia ja pankkikorttien numeroita. (Davis & Samani, 2018; Leavitt, 2014.) Suojaamat-

tomien langattomien verkkoyhteyksien ja vertaisverkkojen on huomattu olevan erittäin vaarallisia, sillä käyttäjien on tutkittu olevan varomattomampia lomaillessaan. Unplugging Travel Survey -kysely osoittaa, että alle puolella matkailijoista on tapana tarkistaa internetyhteyden turvallisuus, vaikka yli puolet vastaajista tietää, kuinka langattoman verkkoyhteyden turvallisuus tarkistetaan. (Davis & Samani, 2018.)

McAfeen uhkaraportin mukaan yksi suurimmista huolenaiheista on kohdennettujen hyökkäysten (targeted attacks) siirtyminen mobiililaitteisiin (Davis & Samani, 2018). Tietokoneissa kesti kaksikymmentä vuotta, että kohdennettujen haittaohjelmien määrä ylitti kaksi miljoonaa kappaletta, mutta mobiililaitteissa sama määrä ylittyi viidessä vuodessa (Davis & Samani, 2018). McAfeen mobiilitutkimusryhmä on löytänyt takaovi-haittaohjelman, jonka oletetaan olevan kyberrikollisryhmä Lazarus Groupin ensimmäinen yritys siirtyä mobiiliympäristöön. Lazarus Group on kyberrikollisryhmä, jonka uskotaan olevan kytköksissä Pohjois-Korean hallitukseen. Lazarus Group on aiemmin tullut tunnetuksi WannaCry-kiristysohjelmasta, jolla se lamaannutti Yhdistyneen Kuningaskunnan julkisen terveydenhoitojärjestelmän ja tuhansia muita organisaatioita vuonna 2017. (Davis & Samani, 2018.)

Bring Your Own Device, lyhennettynä BYOD ja suomennettuna tuo oma laite, on yhä suositumpi käytäntö yrityksissä ja tähän käytäntöön lukeutuvat mukaan myös älypuhelimet (Ghosh, Gajar & Rai, 2013; Morrow, 2012). BYOD tarkoittaa käytännössä sitä, että yritysten työntekijät käyttävät omia henkilökohtaisia laitteitaan työntekoon sekä päästäkseen käsiksi yritysten resursseihin (Ghosh, ym., 2013). Tämä taas johtaa siihen, että yhä useammat työntekijät, liikekumppanit ja asiakkaat käyttävät yritysten informaation ja datan tarkasteluun laitteita, jotka eivät ole yritysten vastuulla. Koska BYOD-laitteet eivät ole yritysten IT-osastojen vastuulla, ne aiheuttavat turvallisuusriskejä kuten tietovarkauksia, tietovuotoja sekä säännösten seuraamatta jättämistä. Lisäksi yrityksien on vaikeampi hallita ja seurata BYOD-laitteiden käyttöä, kuin laitteita jotka yritykset omistavat itse. (Morrow, 2012.) Infoneticsin vuonna 2012 teettämän kyselyn mukaan lähes jokainen kyselyyn vastannut yritys on löytänyt haittaohjelmia yritysten työntekijöiden käyttämiltä mobiililaitteilta. Tämän lisäksi 64 prosenttia vastaajista kertoo arkaluontoista tai patentoitua dataa sisältävän laitteen kadonneen tai tulleen varastetuksi, mutta vain harvalla vastaajista löytyi ratkaisu laitteiden suojaamiseksi. (Morrow, 2012.)

3 ÄLYPUHELIMIEN KYBERUHKILTA SUOJAUTUMINEN

Älypuhelimiin kohdistuvien kyberuhkien määrän ja tehokkuuden kasvu on johtanut siihen, että älypuhelimien sekä sovelluskauppojen kehittäjät, kuten Google ja Apple ovat panostaneet yhä enemmän laitteiden turvallisuuteen (Davis & Samani, 2018). Lisäksi erilaiset tietoturvayhtiöt, kuten McAfee ja F-Secure ovat kohdistaneet työtään älypuhelimiin (Davis & Samani, 2018; Peng, ym., 2014). Tämän lisäksi esimerkiksi Suomen Viestintäviraston Kyberturvallisuuskeskus on laatinut ohjeen, joka antaa tietoturvaan liittyviä vinkkejä matkapuhelimen käyttöön (Viestintävirasto Kyberturvallisuuskeskus, 2014). Tässä luvussa käsitellään sitä, miten älypuhelinta tulisi käyttää, jotta laitteen käyttö olisi mahdollisimman turvallista ja käyttäjän yksityisyys olisi parhaiten suojattu. Lisäksi tässä luvussa käsitellään älypuhelimien käyttäjien valmiuksia suojautua kyberuhkia vastaan ja käydään läpi, millä tavoin älypuhelimien käyttäjät ymmärtävät laitteisiin kohdistuvat kyberuhkat.

3.1 Kyberuhkilta suojautuminen

Tässä alaluvussa käydään läpi erilaisia tapoja, joilla älypuhelimien kyberuhkilta tulisi suojautua. Kaikissa älypuhelimissa, niin yritysten kuin yksityisten henkilöiden käytössä olevissa, tulisi käyttää suojakoodia. (Vashisht, ym., 2016; Viestintävirasto Kyberturvallisuuskeskus 2014). Älypuhelimen suojakoodi voi olla piirrettävä kuvio, numerosarja tai kirjainyhdistelmä (Viestintävirasto Kyberturvallisuuskeskus, 2014). Älypuhelimessa käytettävän suojakoodin tulee olla mahdollisimman monimutkainen, jotta laitteen avaaminen ulkopuolisten toimesta olisi riittävän haastavaa (Viestintävirasto Kyberturvallisuuskeskus, 2014). Aiemmin mainittujen suojakoodien lisäksi älypuhelimeen on myös saatavilla biometrisiä tunnistustapoja, joilla älypuhelimen lukituksen saa avattua (Kunda & Chishimba, 2018). Biometrisistä tunnistustavoista yleisimpiä ovat sormenjälki- ja kasvojentunnistus. Näiden lisäksi käyttäjän on myös mahdollista ottaa tietyissä puhelimissa käyttöön äänitunnistus, jolloin puhelimen lukituksen saa

avattua äänikomennolla tai silmän värikalvon eli iiriksen tunnistus, jolloin älypuhelimen lukitus avautuu, kun laite tunnistaa käyttäjän iiriksen (Kunda & Chishimba, 2018).

Laitteen ohjelmisto- ja tietoturvapäivitykset tulee asentaa mahdollisimman pian niiden julkaisemisen jälkeen. Älypuhelimessa käytettävät sovellukset kannattaa myös pitää päivitettyinä (Viestintävirasto Kyberturvallisuuskeskus, 2014). Tietyssä pisteessä älypuhelimen elinkaarta laitteen ohjelmisto- ja tietoturvapäivitykset lopetetaan (Viestintävirasto Kyberturvallisuuskeskus, 2014). Tästä esimerkkinä Applen älypuhelinmalli iPhone 5, johon ei ole mahdollista asentaa 19.7.2017 julkaistua iOS 10.3.3 käyttöjärjestelmäpäivitystä uudempaa versiota (Apple, 2018). Tämä altistaa älypuhelimen entistä enemmän tietoturvauhkille, jolloin on syytä harkita uuden laitteen hankkimista (Viestintävirasto Kyberturvallisuuskeskus, 2014). Davisin ja Samanin (2019), Vashishtin ym. (2016) ja Viestintäviraston Kyberturvallisuuskeskuksen (2014) mukaan jokin virustorjunta ja tietoturvaohjelma kannattaa asentaa älypuhelimeen tekemään laitteen käytöstä turvallisempaa. Viestintäviraston Kyberturvallisuuskeskus (2014) kuitenkin huomauttaa, että laitteen lisäturvallisuutta tarjoavia sovelluksia ladatessa kannattaa noudattaa erityistä varovaisuutta ja käyttää ainoastaan tunnettujen yritysten palveluita.

Käyttäessä langattomia yhteyksiä, esimerkiksi Bluetoothia, kannattaa se käytön aikana pitää näkymättömänä muille laitteille, jolloin ulkopuoliset eivät pysty muodostamaan yhteyttä laitteeseen käyttäjän tietämättä (Vashisht, ym., 2016). Langattomat yhteydet, kuten Bluetooth, WLAN, GPS ja NFC kannattaa pitää pois päältä aina kun ne eivät ole käytössä (Vashisht, ym., 2016; Viestintävirasto Kyberturvallisuuskeskus, 2014). Tämä ei ainoastaan lisää laitteen turvallisuutta, vaan myös vähentää älypuhelimen akun kulumista (Viestintävirasto Kyberturvallisuuskeskus, 2014). Langatonta internetverkkoa käytettäessä tulisi käyttää ensisijaisesti salasanasuojattua verkkoa (Vashisht, ym., 2016). Jos älypuhelinta käyttää WLAN-verkossa, jossa ei ole salasanasuojausta, tai jos älypuhelinta käytetään ulkomailla, tulisi käyttäjällä olla käytössään VPN-palvelu (Viestintävirasto Kyberturvallisuuskeskus, 2014). Virtuaalinen yksityisverkko (Virtual Private Network, VPN) on virtuaalisesti rakennettu yksityisverkko, jonka avulla kaikki VPN-palvelussa olevat laitteet näyttävät ulkoisesti toimivan samassa verkossa. VPN-palvelua käytettäessä kaikki verkkoliikenne kulkee kyseisen yksityisverkon kautta, mikä mahdollistaa turvallisen internetyhteyden. (Venkateswaran, 2001.) McAfeen vuoden 2018 mobiiliuhkaraportin (Davis & Samani, 2018) mukaan VPN-palvelu ei kuitenkaan yksin riitä. McAfeen vuoden 2018 mobiiliuhkaraportin mukaan laajasti käytetystä WPA2 salausprotokollasta on löytynyt uusi KRACK-haavoittuvuus. KRACK-haavoittuvuus antaa hyökkääjälle mahdollisuuden seurata laitteen ja reitittimen välistä liikennettä, vaikka liikenne olisikin salattu, ellei käytössä ole HTTP-protokolla, joka sekoittaa dataa. (Davis & Samani, 2018.) McAfeen mobiiliuhkaraportin mukaan noin 41 prosenttia Android-laitteista oli haavoittuvaisia, vaikka olisikin käyttänyt suojattua verkkoyhteyttä (Davis & Samani, 2018). McAfeen vuoden 2018 mobiiliuhkaraportin mukaan tämä haavoittuvuus alleviivaa sitä, että käyttäjän on tärkeää käyttää myös mobiilitietoturvaa, eikä pelkästään VPN-yhteyttä turvatakseen verkkoliikenteensä (Davis & Samani, 2018).

Älypuhelimen sovellukset kannattaa aina ladata käyttöjärjestelmävalmistajan ylläpitämästä sovelluskaupasta tai tunnetulta, luotettavalta verkkosivulta (Vashisht, ym., 2016; Viestintävirasto Kyberturvallisuuskeskus, 2014). Esimerkki sovelluksesta, jonka voi ladata Android-laitteille ainoastaan tunnetulta ja luotettavalta verkkosivulta on suomalaisen Veikkaus Oy:n kehittämä Veikkaus-sovellus, joka helpottaa Veikkaus Oy:n tarjoamien rahapelien pelaamista mobiililaitteilla. Sovellus ei ole ladattavissa Google Play –sovelluskaupasta, sillä sovelluskauppaan ei ole sallittua lisätä rahapelaamista mahdollistavia sovelluksia. (Veikkaus, 2019.) Viestintäviraston Kyberturvallisuuskeskus (2014) huomauttaa, että käyttöjärjestelmien valmistajatkaan eivät pysty estämään kaikkien haitallisten sovellusten lisäämistä sovelluskauppoihin, jolloin myös näistä saattaa löytyä haittaohjelmia. Useat älypuhelimien sovellukset vaativat pääsyoikeuksia esimerkiksi kameraan, sijaintipalveluihin tai yhteystietoihin. Hyväksyessä älypuhelimen vaatimia oikeuksia käyttäjän tulee noudattaa erityistä varovaisuutta ja harkita, mitä oikeuksia kyseinen sovellus todellisuudessa tarvitsee toimiakseen. (Vashisht, ym., 2016; Viestintävirasto Kyberturvallisuuskeskus, 2014.) Esimerkiksi askelmittarisovelluksen ei lähtökohtaisesti pitäisi tarvita oikeuksia yhteystietojen tarkasteluun (Viestintävirasto Kyberturvallisuuskeskus, 2014).

Myydessä tai luovuttaessa älypuhelimen toiselle käyttäjälle, tulee laitteessa mahdollisesti käytössä ollut pilvipalvelu poistaa, laitteen muisti ja erillinen muistikortti tyhjentää sekä palauttaa laite tehdasasetuksille. Tällä tavoin käyttäjä varmistaa, ettei hänen henkilökohtaiset tietonsa päädy laitteen uuden omistajan haltuun. (Viestintävirasto Kyberturvallisuuskeskus, 2014.) Ostettaessa käytetyn älypuhelimen, kannattaa suorittaa samat toimenpiteet kuin luopuessa omasta laitteesta. Erityistä huomiota tulisi kiinnittää siihen, onko laite liitettynä edellisen käyttäjän pilvipalveluun, jonka kautta uuden käyttäjän henkilökohtaiset tiedot voivat mahdollisesti päätyä edellisen älypuhelimen omistajan haltuun. (Viestintävirasto Kyberturvallisuuskeskus, 2014.) Käytettynä myytävä älypuhelin saattaa olla myös varastettu. Tällaista on syytä epäillä, jos laite on huomattavasti halvempi kuin muut markkinoilla olevat samanlaiset laitteet, laitteen pääsykoodia ei ole tiedossa, laitteessa on myyjälle tuntemattomien ihmisten tietoja tai laite on lukittu. (Viestintävirasto Kyberturvallisuuskeskus, 2014.)

Viestintäviraston Kyberturvallisuuskeskuksen mukaan älypuhelimessa voidaan epäillä olevan haittaohjelma, jos käytettäessä ilmenee jokin seuraavista tapauksista:

- laitteen käyttö on hidastunut, eikä laitteen uudelleen käynnistäminen korjaa tilannetta
- laitteen akku alkaa äkillisesti kulua huomattavasti nopeammin kuin aiemmin
- laitteen käyttöjärjestelmä alkaa kaatuilla
- laitteen verkkoliikenne kasvaa äkillisesti ilman, että käyttäjä on muuttanut verkkotoimintaansa
- laitteen käyttäjä ohjataan väärille verkkosivuille tai hän saa ylimääräisiä mainoksia
- laitteen käyttäjä vastaanottaa roskapostia tai käyttäjän yhteyshenkilöt ilmoittavat saavansa käyttäjältä viestejä, joita käyttäjä ei itse ole lähettänyt.

3.2 Käyttäjien valmius suojautua kyberuhkilta

Tässä alaluvussa käsitellään älypuhelimien käyttäjien valmiutta suojautua älypuhelimiin kohdistettuja kyberuhkia vastaan. Älypuhelimien automaattitunnistimien on kehotettu ilmoittamaan edistyneille käyttäjille, jos sovelluksen vaatimat oikeudet heikentävät käyttäjän turvallisuutta tai yksityisyyttä (Mylonas, Kastania & Gritzalis, 2013). Mylonasin ym. (2013) mukaan on kuitenkin epäselvää, onko älypuhelimien turvallisuuteen liittyvien ratkaisujen tekeminen tarpeellista älypuhelimien peruskäyttäjille. Tutkimukset ovat myös osoittaneet, että peruskäyttäjät eivät pysty tekemään älypuhelimen turvallisuuteen liittyviä päätöksiä eikä heillä ole riittävää taitoa hallinoidakseen laitteen turvallisuuteen liittyviä asetuksia asiaankuuluvasti (Mylonas, ym., 2013). Mylonasin ym. tekemän haastattelututkimuksen mukaan on havaittavissa, että älypuhelimien käyttäjillä on selkeitä puutteita laitteen tietoturvan tuntemuksessa. Tutkimukset osoittavat, että älypuhelimiin asennettavien sovellusten latausmäärät korreloivat positiivisesti sovellusten vaatimien pääsyoikeuksien kanssa (Chia, Yamamoto & Asokan, 2012; Mylonas, ym., 2013). Tämä tarkoittaa siis sitä, että mitä suositumpi älypuhelimeen ladattava sovellus on, sitä todennäköisemmin sovellus vaatii pääsyoikeuksia laitteen eri osa-alueille, jotka voivat vahingoittaa laitteen ja laitteen käyttäjän turvallisuutta sekä yksityisyyttä. Tästä voidaankin päätellä, että vaikka älypuhelimen sovellus olisi suosittu sovelluskaupassa, se ei tarkoita automaattisesti sitä, että sovellus kunnioittaisi käyttäjän yksityisyyttä (Mylonas, ym., 2013). Mylonasin ym. (2013) teettämät tutkimukset osoittavat, että älypuhelimien käyttäjillä on tapana jättää huomioimatta sovelluksen maine, toisten käyttäjien arvostelut sekä sopimus- ja turvallisuusviestit sovellusta ladattaessa. Tämän lisäksi älypuhelimien käyttäjillä ei ole riittävää ymmärrystä riskeistä, joita eri oikeuksien antaminen älypuhelimien sovelluksille voi lisätä (Mylonas, ym., 2013).

Vaikka Mylonasin ym. (2013) tekemistä havainnoista voidaan todeta, että älypuhelimien käyttäjien tietoisuus turvallisuusriskeistä älypuhelinsovelluksia ladatessa on heikko, älypuhelimien käyttäjät ovat tutkitusti huolestuneita omasta yksityisyydestään ja turvallisuudestaan älypuhelimia käytettäessä. Chin, Porter, Sekar ja Wagner (2012) ovat huomanneet tutkimuksessaan, että käyttäjät ovat enemmän huolissaan heidän älypuhelimiensa kuin kannettavien tietokoneidensa yksityisyyden säilymisestä. Tämän lisäksi käyttäjät ovat pelokkaampia suorittamaan yksityisyytensä kannalta arkaluontoisia toimintoja ja raha-asioitaan älypuhelimillaan kuin kannettavilla tietokoneillaan (Chin, ym., 2012). Chin ym., (2012) teettämän tutkimuksen mukaan älypuhelimien käyttäjät ovat huolissaan laitteiden varastamisesta ja datan häviämisestä, haitallisista sovelluksista sekä langattomissa verkoissa tapahtuvista hyökkäyksistä. Tutkimuksessa kävi myös ilmi, että pelko langattomissa verkoissa tapahtuvista hyökkäyksistä johtuu suurilta osin väärinkäsityksistä, jotka liittyvät siihen, miten langattomien verkkojen viestintä toimii.

McAfeen vuoden 2018 mobiiliuhkaraportista käy ilmi, että turvallisuus on kaikista suurin huolenaihe, niin Applella kuin Googlellakin. Tämä näkyy selkeästi investointien määrästä alustojen lujittamiseksi aina komponenttitasolta sovelluskauppoihin. Vaikka suunta haittaohjelmien torjumiseksi onkin ollut oikea, lisää työtä tarvitaan edelleen. (Davis & Samani, 2018.)

4 YHTEENVETO

Tämän tutkielman tavoitteena oli kirjallisuuskatsauksen avulla kartoittaa, millaisia kyberuhkia älypuhelimiin kohdistuu, miten niiltä voidaan suojautua ja mikä on käyttäjien sekä valmistajien valmius suojautua kyberuhkia vastaan. Tutkielma jaettiin neljään lukuun, joista luvuissa kaksi ja kolme pyrittiin vastaamaan kahteen tutkimuskysymykseen:

- Millaisia kyberuhkia älypuhelimiin kohdistuu?
- Millä tavoin älypuhelimiin kohistuvia kyberuhkia vastaan voidaan suojautua?

Tutkielmassa määriteltiin, mikä on älypuhelin ja tehtiin katsaus älypuhelimien historiaan sekä kehitykseen. Tutkielmassa myös todettiin, että älypuhelimien määrä on suuressa kasvussa ja niiden kehitys on nopeaa. Oletuksena onkin, että tulevaisuudessa älypuhelimet tulevat esimerkiksi korvaamaan perinteiset tietokoneet laitteina, jotka voidaan telakoida erillisiin näyttöihin ja näppäimistöihin (Islam & Want, 2014). Tutkielmassa määriteltiin myös termit kyber ja kyberturvallisuus, sekä käytiin läpi älypuhelimiin kohdistuvia kyberuhkia ja haittaohjelmia. Tutkielmassa kävi ilmi, että älypuhelimiin kohdistettujen haittaohjelmien määrä on ollut jatkuvassa kasvussa jo vuodesta 2010. Tutkielmassa määriteltiin älypuhelimiin kohdistuvien haittaohjelmien nimiä ja samalla kävi ilmi, että älypuhelimiin kohdistuvat haittaohjelmat on nimetty samalla tavalla kuin tietokoneisiin suunnatut haittaohjelmat, sillä niiden toimintaperiaate on sama. Suurin muutos haittaohjelmien kehittämisessä on ollut se, että haittaohjelmien kehittäjät pyrkivät tänä päivänä yhä enemmän tuottamaan rahallista hyötyä haittaohjelmillaan. Tästä voidaan päätellä, että haittaohjelmien kehittäminen on yhä ammattimaisempaa ja haittaohjelmien aiheuttamat vahingot ovat jatkuvasti suurempia.

Tutkielmassa ilmeni vastauksena ensimmäiseen tutkimuskysymykseen, että tänä päivänä monet älypuhelimiin kohdistuvat kyberuhkat ovat sovelluskaupoissa esiintyviä haittaohjelmakampanjoita, joiden avulla yhtä haittaohjelmaa voidaan levittää suurella volyymilla useiden erilaisten haitallisten ohjelmien avulla (Davis & Samani, 2018). Haittaohjelmat eivät kuitenkaan ole ainut

kyberuhka, joka älypuhelimiin kohdistuu. Haittaohjelmien lisäksi esimerkiksi tietojen kalastelu sosiaalisessa mediassa tai suojaamattoman langattoman internetyhteyden tuomat riskit ovat suuria uhkia älypuhelimien käyttäjille (Davis & Samani, 2018; Leavitt, 2014).

Luvussa kolme käsiteltiin sitä, miten edellä mainittuja kyberuhkia vastaan tulisi suojautua. Samassa luvussa käsiteltiin myös käyttäjien sekä valmistajien valmiuksia suojautua kyberuhkia vastaan. Toinen tutkimuskysymys tarkasteli sitä, millä tavoin älypuhelimiin kohistuvia kyberuhkia vastaan voidaan suojautua. Tutkielmassa todettiin, että käyttäjä voi suojautua älypuhelimeen kohdistuvilta kyberuhkilta:

- käyttämällä mahdollisimman monimutkaista suojakoodia
- asentamalla laitteen ohjelmisto- ja tietoturvapäivitykset mahdollisimman pian niiden julkaisun jälkeen
- käyttämällä älypuhelimessa jotakin tietoturva- ja viruksentorjuntaohjelmaa
- pitämällä langattomat yhteydet näkymättöminä muille laitteille ja kytkemällä ne pois päältä, silloin kun niitä ei enää käytä
- käyttämällä VPN-palvelua salasanasuojaamattomia langattomia internetyhteyksiä käytettäessä
- lataamalla älypuhelimiin tarjolla olevat sovellukset käyttöjärjestelmävalmistajan tarjoamasta sovelluskaupasta tai tunnetuilta, luotettavilta verkkosivuilta
- noudattamalla erityistä varovaisuutta antaessa eri käyttöoikeuksia älypuhelimen sovelluksille
- poistamalla laitteessa olleet pilvipalvelut, tyhjentämällä laitteen muistin sekä muistikortin ja palauttamalla laitteen tehdasasetuksille silloin, kun luovuttaa älypuhelimen uudelle käyttäjälle tai vastaanottaa käytetyn älypuhelimen.

Tutkielmassa käsiteltiin myös sitä, millainen on käyttäjien ja valmistajien tämän hetkinen valmius suojautua kyberhyökkäyksiä vastaan ja kartoitettiin, miten hyvin kuluttajat ymmärtävät älypuhelimien kyberuhkia. Tutkielmassa todettiin, että käyttäjien taito suojautua kyberuhkia vastaan on puutteellista, mutta käyttäjät ovat silti huolestuneita älypuhelimiensa turvallisuudesta ja yksityisyydestä. Käyttäjien suhtautumisesta älypuhelimien kyberuhkia kohtaan löytyi varsin vähän tieteellistä tutkimusta ja aiheeseen liittyvät julkaisut olivat yli viisi vuotta vanhoja. Tämä antaakin tutkielman tekijälle syytä paneutua aiheeseen tarkemmin, esimerkiksi pro gradu -tutkielman muodossa.

Tutkielmassa kävi ilmi, että kyberrikollisuus on jatkuvassa nousussa älypuhelimien saralla. Ihmiset käyttävät yhä enemmän älypuhelimia asioihin, joihin he aikaisemmin käyttivät tietokoneita. Loogisesti tämä houkuttelee alalle myös rikollisuutta. Varsinkin haittaohjelmien määrä ja tehokkuus ovat kasvaneet huomattavasti viimeisen kymmenen vuoden aikana, mistä voidaan ennustaa niiden myös kasvavan tulevaisuudessa. Moni älypuhelimen käyttäjä luottaa

liikaa siihen, että laitteeseen ei voi tulla haittaohjelmatartuntaa, vaikka varsinkin Android-käyttöjärjestelmän kohdalla tilanne on jo melko huolestuttava.

Tämä tutkielma antaa lisää syitä perehtyä siihen, mitä mobiilihaittaohjelmat pahimmillaan käyttäjälleen aiheuttavat ja onko näitä uhkia vastaan keinoja suojautua. Esimerkiksi Shacklefordin (2016) mukaan, viruksentorjuntaohjelmista on tullut yhä vähemmän hyödyllisiä, sillä monet viruksentorjuntatyökalut keskittyvät ainoastaan hyvin tunnettujen ja laajalle levinneiden haittaohjelmien havaitsemiseen, vaikka tuntemattomammat ja pienemmät haittaohjelmat voivat luoda samanlaisen riskin. Tämä antaa syyn tutkia tarkemmin, mitä keinoja älypuhelimien käyttäjille tarjotaan, jotta he voivat suojautua kyberuhkilta.

Lisäksi tutkielma herättää mielenkiintoa seuraamaan sitä, miten tulevaisuudessa siirtyminen perinteisistä tietokoneista kokonaan mobiililaitteisiin vaikuttaa haittaohjelmien ja kyberuhkien kehitykseen ja osaavatko silloin jo älypuhelimien käyttäjät suojautua paremmin näitä vastaan.

LÄHTEET

Apple. (2018) Apple security update. Haettu 21.1.2019 osoitteesta https://support.apple.com/en-us/HT201222

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices Teoksessa IEEE Symposium on Security and Privacy (96-111).

Chia, P. H., Yamamoto, Y., & Asokan, N. (2012). Is this app safe?: a large scale study on application permissions and risk signals Teoksessa Proceedings of the 21st international conference on World Wide Web (311-320). ACM.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. Teoksessa Proceedings of the eighth symposium on usable privacy and security. Washington: Advancing Science, Serving Society.

Davis, G., Samani, R. (2018). The Next 10 Years (McAfee Mobile Threat Report Q1, 2018). McAfee Mobile.

Davis, G., Samani, R. (2019). Mobile Malware Continues to Increase in Complexity and Scope (McAfee Mobile Threat Report Q1, 2019). McAfee Mobile.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. Journal of Global Research in Computer Science, 4(4), 62-70.

Islam, N., & Want, R. (2014). Smartphones: Past, present, and future. IEEE Pervasive Computing, 13(4), 89-92.

Jiang, X., & Zhou, Y. (2012). Dissecting android malware: Characterization and evolution. In 2012 IEEE Symposium on Security and Privacy (95-109). IEEE.

JUHTA – julkisen hallinnon tietohallinnon neuvottelukunta. (2014). JHS-suositukset: JHS 190 julkisten verkkopalvelujen suunnittelu ja kehittäminen. Haettu 11.10.2017 osoitteesta http://docs.jhssuositukset.fi/jhs-suositukset/JHS190/JHS190.pdf.

Kunda, D., & Chishimba, M. (2018). A Survey of Android Mobile Phone Authentication Schemes. Mobile Networks and Applications, 1-9.

Leavitt, N. (2005). Mobile phones: the next frontier for hackers? Computer, 38(4), 20-23.

Leavitt, N. (2011). Mobile security: finally a serious problem? Computer, 44(6), 11-14.

Limnéll, J. (2014). Kyber rantautui Suomeen. Aalto yliopiston julkaisusarja 12/2014

Maslennikov, D. (2011). Mobile malware evolution: An overview, part 4. Haettu 13.3.2019 osoitteesta https://www.securelist. com/en/analysis/204792168/Mobile _ Malware _ Evolution _ An _ Overview _ Part_4

Merriam-Webster Dictionary Cybersecurity. Haettu 14.3.2019 osoitteesta https://www.merriam-webster.com/dictionary/cybersecurity

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. Network Security, 2012(12), 5-8.

Mylonas, A., Kastania, A. & Gritzalis, D. (2013). Delegate the Smartphone User? Security Awarness in Smartphone platforms. Computers & Security Volume 34, May 2013. 47–66.

Peng, S., Yu, S., & Yang, A. (2014). Smartphone malware and its propagation modeling: A survey. IEEE Communications Surveys & Tutorials, 16(2), 925-941.

Rastogi, V., Chen, Y., & Jiang, X. (2014). Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks. IEEE Trans. Information Forensics and Security, 9(1), 99-108.

Sanastokeskus TSK ry. (2019a). Haettu 10.4.2019 osoitteesta http://www.tsk.fi/tepa/fi/haku/haittaohjelma

Sanastokeskus TSK ry. (2019b). Haettu 10.4.2019 osoitteesta http://www.tsk.fi/tepa/fi/haku/kyberuhka

Sanastokeskus TSK ry. (2017). Haettu 16.10.2017 osoitteesta http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&height=156&qfind=kyberturvallisuus

Shackleford, D. (2016). Using Analytics to Predict Future Attacks and Breaches. *Sans.*

Statista (2017a) Number of smartphone users worldwide from 2014 to 2020. Haettu 28.1.2019 osoitteesta https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Statista (2017b) Number of tablet users worldwide from 2013 to 2021. Haettu 28.1.2019 osoitteesta https://www.statista.com/statistics/377977/tablet-users-worldwide-forecast/

Statista (2018) eBooks worldwide. Haettu 28.1.2019 osoitteesta https://www.statista.com/outlook/213/100/ebooks/worldwide

Vashisht, S., Gupta, S., Singh, D., & Mudgal, A. (2016). 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016), 41-44.

Veikkaus (2019) Veikkaus sovellukset. Haettu 21.1.2019 osoitteesta https://www.veikkaus.fi/fi/sovellukset

Venkateswaran, R. (2001). Virtual private networks. IEEE potentials, 20(1), 11-15.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102

Viestintävirasto Kyberturvallisuuskeskus. (2014). Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön. Haettu 18.1.2019 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf

Wright, J., Dawson, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smart phones. Journal of Information Systems Technology and Planning, 5(14), 40-60.