Atte Söderlund

Mobiililaitteiden haittaohjelmat

Tietotekniikan kandidaatintutkielma

18. joulukuuta 2013

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Atte Söderlund

Yhteystiedot: atanauso@student.jyu.fi

Työn nimi: Mobiililaitteiden haittaohjelmat

Title in English: Mobile phone malwares

Työ: Kandidaatintutkielma

Sivumäärä: 24+0

Tiivistelmä: Mobiiliuhkien yleistyessä on syytä vähän kartoittaa, mitä haittaohjelmia mobiilipuolelle on jo tullut. Tässä kirjallisuus kartoituksessa tavoite oli yksinkertaisesti kartoittaa nykyisiä mobiilihaittaohjelmia, joista suurimpana alueena ovat troijalaiset.

Avainsanat: Mobiili, haittaohjelma, troijalainen, virus, uhka

Abstract: While mobile threats are coming part of our every day life, it is important that we survey those threats that are already here. Objective of this paper was to simply survey mobile malware, where the biggest part is toijans.

Keywords: Mobile, malware, troijan, virus, threat

Kuviot

Taulukot

Sisältö

1 Johdanto

Mobiililaitteet ovat yleistymässä hurjalla vauhdilla ja lisäksi niiden tehot ovat kasvaneet niin isoiksi, että niistä on tullut rikollisten mielenkiinnon kohde tuottaa erilaisia haittaohjelmia. (Delac, Silic ja Krolo 2011) Mobiililaitteista on tullut PC:n kaltaisia tehonlisäyksen vuoksi, joten on luontevaa, että PC maailman haittaohjelmat siirtyvät mobiilipuolelle. Laitteitakin on tullut ihmisille enemmän, minkä voi päätellä taulukosta 1. Pelkästään vuoden 2011 ja 2012 ensimmäisten neljännesten välillä mobiiliuhkat ovat yli kaksinkertaistuneet (F-secure 2013a). Vaikka mobiiliuhkat kattaakin huijaukset mukaan, voi raportista (F-secure 2013a) huomata, että suurin osa näistä uhista on troijalaisia, joka on yksi haittaohjelmaalalaji. Vielä 10 vuotta sitten mobiilihaittaohjelmat olivat harvinaisia ja ne alkoivatkin kehittyä oikeastaan vasta 2004. (Hyppönen 2007)

Taulukko 1. Vuosien 2012 ja 2013 toisen neljänneksen älypuhelimien myynti maailmanlaajuisesti. (Tuhatta yksikköä) Gartner.com

Yhtiö	2013 Yksiköt	2Q13 Markkinaosuus (%)	2Q12 Yksiköt	2Q12 Markkinaosuus (%)
Apple	31 899,7	14,2	28 935,0	18,8
LG Electronics	11 473,0	5,1	5 827,8	3,8
Lenovo	10 671,4	4,7	4 370,9	2,8
ZTE	9 687,6	4,3	6 331,4	4,1
Muut	90 213,6	40,0	62 704,0	40,8
Yhteensä	225 326,2	100,0	153 772,9	100,0

Taulukossa 2 on puhelimien, ei vain älypuhelimien, myynti, joten jos sitä vertaa taulukkoon 1, nähdään, että myydyistä puhelimista noin puolet on älypuhelimia. Tämä on hyvinkin merkittävä osuus, koska älypuhelimet maksavat varsin paljon ja köyhemmissä maissa kaikilla ei välttämättä ole varaa älypuhelimeen.

Yrityksien varsinkin tulisi panostaa tietoturvaan, ja vaikka suurin osa on tehnyt tietoturvadokumentin yritykselle, se ei edes puolissa yrityksistä kata mobiilitietoturvaa (Goode 2010). Yritys voi tehdä suuret tappiot, jos vaikka sen uutuustuotteen tietoja joutuu vääriin käsiin,

Taulukko 2. Vuosien 2012 ja 2013 toisen neljänneksen mobiilipuhelimien myynti maailmanlaajuisesti. (Tuhatta yksikköä) Gartner.com

Yhtiö	2013 Yksiköt	2Q13 Markkinaosuus (%)	2Q12 Yksiköt	2Q12 Markkinaosuus (%)
Samsung	107 526,0	24,7	90 432,1	21,5
Nokia	60 953,7	14,0	83 420,1	19,9
Apple	31 899,7	7,3	28 935,0	6,9
LG Electronics	17 016,4	3,9	14 345,4	3,4
ZTE	15 280,7	3,5	17 198,2	4,1
Huawei	11 275,1	2,6	10 894,2	2,6
Lenovo	10 954,8	2,5	6 821,7	1,6
TCL Comm.	10 134,3	2,3	9 355,7	2,2
Sony Mobile Comm.	9 504,7	2,2	7 346,8	1,7
Yulong	7 911,5	1,8	4 016,2	1,0
Muut	152 701,5	35,1	147 354,60	35,1
Yhteensä	435 158,4	100,0	420 120,0	100,0

ja juuri sen vuoksi juuri yritysten pitäisi herätä ja tehdä jotain asialle. Tätä tilannetta ei auta yhtään nykytrendi siitä, että otetaan oma puhelin työpaikalle. Esimerkiksi, kun työpuhelinta käyttää viihdekäytössä eli siihen asentaa erilaisia sovelluksia, voi helposti tulla ladanneeksi haitallisen ohjelman ja sitä kautta myös yrityksen tietoturva on uhattuna.

Haittaohjelmille alttein alusta on Android, jolle on jo monenlaisia haittaohjelmia. Vuoteen 2012 alttein tai toiseksi alttein haittaohjelmille on ollut Symbian-alusta. Symbianille on vain muutamia haittaohjelmia vuonna 2013, mutta aikaisempina vuosina osuus on ollut paljon suurempi. (F-secure 2013a; Hyppönen 2007) Vuoteen 2010 Symbian johti uhissa, mutta on menettänyt kyseenalaista asemaansa (F-secure 2011). Tämä todennäköisesti johtuu siitä, että Symbian ei ole enää suosituin alusta.

Windows Mobilelle, iOS:lle ja BlackBerrylle on vain muutamia uhkia (F-secure 2013a). Android nousi vuonna 2010 kärkeen uhkissa kuin heittämällä ja sattuukin olemaan suosituin alusta tällä hetkellä (F-secure 2011; Gartner 2013). Sen vuoksi on rikollisille parempi kes-

kittyä Android-alustalle kuin jollekin toiselle mobiilialustalle. Teoriaa todistaa se, että kun Symbian aikoinaan oli suosituin mobiilialusta, niin suurin osa haittaohjelmista kehitettiin sille. (Coursen 2007)

Koska haittaohjelmat ovat lähinnä Androidille kehitettyjä, tässä kirjallisuuskartoituksessa käydään enemmän läpi Androidin haittaohjelmia ja samasta syystä varsinkin troijalaistyyppisiä haittaohjelmia. (F-secure 2013a)

Tässä kirjallisuuskartoituksessa tutkimuskysymys on: Minkälaisia tai mitä mobiilihaittaohjelmia on liikkeellä tällä hetkellä. Eli tehtävänä on kartoittaa nykyisiä mobiililaitteiden, mutta lähinnä älypuhelimien haittaohjelmia.

Kirjallisuuskartoituksessa ei kuitenkaan oteta huomioon ennen vuotta 2006 julkaistuja artikkeleita, koska tuolloin vain lähinnä spekuloitiin mobiiliuhkien yleistymisestä sen sijaan, että niistä olisi konkreettista tutkimustietoa. Lisäksi mobiilialustat ovat muuttuneet paljon vuodesta 2006 ja toisista on kasvanut suositumpia kuin toisista. Sen vuoksi käsittelen vanhempia artikkeleita kriittisemmin.

Otan huomioon vain F-securen tekemät raportit, enkä muiden tietoturvayhtiöiden, koska näiden välillä on erilaisia nimeämiskäytäntöjä, jolloin joillakin haittaohjelmilla voi olla eri nimet.

Luvussa 2 käsitellään vain hyvin pintapuolisesti pääkohtia mobiiliuhkien alkuvaiheesta eli ensimmäisestä sukupolvesta vuosina 2004 – 2009. Lähinnä siksi, että ne on hyvä kuitenkin tietää, mutta niillä ei ole kuitenkaan välttämättä ole suoraa yhteyttä nykypäivän haittaohjelmiin, koska tekniikka on kehittynyt paljon ja uusia käyttöjärjestelmiä on tullut markkinoille. Käyttäjätkin ovat luultavasti tulleet tietoisemmiksi vaaroista ja osaavatkin varmasti myös siten ennaltaehkäistä tartuntoja.

Luvussa 3 taas käsitellään enemmän lähinnä vuoden 2010 ja sen jälkeen tulleita haittaohjelmia, jotka ovat jo toisen sukupolven haittaohjelmia. Nämä ovat tärkeitä tässä kartoituksessa, koska tässä on ihan viime vuosien haittaohjelmat, jotka kertovat, missä mennään haittaohjelmapuolella ja mahdollisesti viittovat, mihin suuntaan ollaan menossa.

Sen jälkeen luvussa 4 käsitellään vuotta 2013, jolloin jo kolmannen sukupolven haittaohjel-

mia ilmestyi. Luku on hyvin samanlailla kuin viime vuosien haittaohjelmia luvussa 3.

Viimeisenä on yhteenveto kirjallisuuskartoituksen tuloksista. Luvussa tiivistetään havaintoja, joita kirjallisuuskatsauksen perusteella on tehty ja tarkastellaan niitä.

2 Mobiililaitehaittaohjelmien ensimmäinen sukupolvi: Cabir, Commwarrior

Hyppönen 2007 mukaan jo vuonna 2007 oli yli 370 mobiilivirusta, ja että Cabir ja Commwarrior virukset olivat levinneet yli 30 maahan. Ensimmäiset haittaohjelmat olivatkin viruksia, joista ensimmäinen Symbianille oli vuonna 2004 löydetty Cabir-virus, joka on varsin harmiton, mutta laajalle levinnyt. Cabir-virus leviää Bluetoothin kautta, ja se on varsin primitiivinen virus, mutta vuonna 2007 siitä löydettiin vähintään 15 eri varianttia. (Coursen 2007)

Virus on haittaohjelma, jonka päätarkoitus on levitä. Virukset kuitenkin voivat aiheuttavat kaikenlaista haittaa, mutta levitäkseen laajalle, niiden pitää yleensä olla huomaamattomampia.

Tästä on hyvä huomata se, että puhelimet itsessään mahdollistivat virusten levityksen eli tukivat Bluetoothia, joka ei ollut tarpeeksi turvalliseksi kehitetty. Puhelimien ominaisuudet siis kehittyivät ja samalla myös käyttäjämäärät kasvoivat. Käyttäjämäärän kasvaessa taas on ymmärrettävää, että osajoukko puhelimien omistajista olisi niin sanotusti ajattelemattomampia puhelimen käyttäjiä, jotka mahdollistavat tällaisien viruksien leviämisen. Tämän viruksen kohdalla ei olisi tarvinnut kuin pitää Bluetooth suljettuna koko ajan ja virus ei olisi koskaan päässyt puhelimeen. Siksi olisi hyvä vielä lisätä ominaisuuksien kehittymisen lisäksi yhdeksi syyksi käyttäjien tyhmyys tai oikeastaan tietämättömyys – kun ei ole tietoa, ei voi varautuakaan.

Commwarrior taas on ensimmäinen löydetty virus, joka leviää MMS-viestien eli multimediaviestien avulla, mutta voi myös levitä Bluetoothin tai sähköpostin kautta. Commwarrior oli kohdistettu Symbian Series 60 -älypuhelimille. Koska MMS-viestien lähettäminen maksaa puhelimen omistajalle tai ainakin liittymän omistajalle, on Commwarrior todella ikävä virus, joka voi käydä kalliiksi uhrille. (Hyppönen 2007)

Cardtrap on ensimmäinen löydetty virus, joka yrittää saastuttaa myös Windows-käyttöjärjestelmän tietokoneita (Hyppönen 2007). Tämä on merkittävää siksi, että mobiililaitteet ovat jo tietokoneen kaltaisia, pieniä, taskuun mahtuvia tietokoneita. Siten on myös ymmärrettävää, että

haittaohjelmien tarttuminen molempien välillä olisi varsin helppo toteuttaa ja sitä kautta siitä tulisi suosittu levitysmuoto. Täten myös mobiilivirusten määrä voi kasvaa merkittävästi. On huomion arvoista, että PC:lle tai mobiililaitteelle suunnitellut haittaohjelmat eivät toimi toisissaan, vaan ne on pitänyt suunnitella toimimaan molemmille yhtä aikaa, mikä on ilmeisesti osoittautunut ongelmaksi.

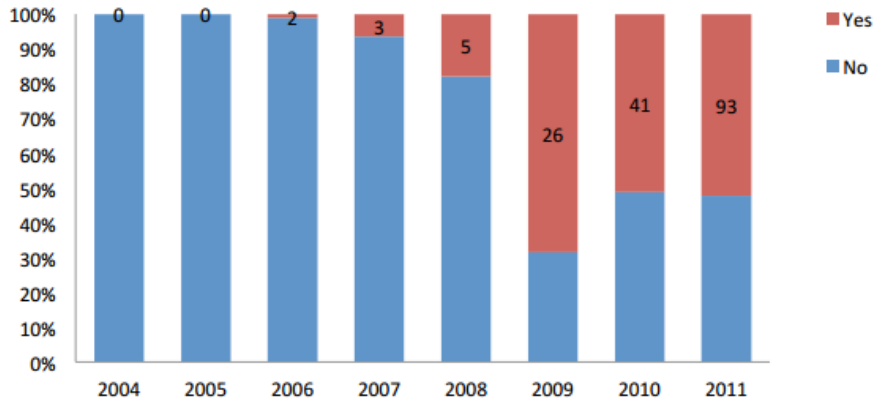
	Year								
Type	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**Total**
Garbage			8						8
Riskware			1		1	8	1	10	21
Spyware			5	15	6		2	4	32
Trojan	11	105	160	23	13	24	47	136	519
Virus	14	19	17	6					56
Worm				2	8	6	22		38
Hack-Tool							4	9	13
Backdoor							3		3
Monitoring-Tool							1	14	15
Application								5	5
Total	**25**	**124**	**191**	**46**	**28**	**38**	**80**	**178**	**710**

Kuvio 1. Haittaohjelmien kehitys 2004-2011. (F-secure 2011)

Kuviosta 1 voi nähdä, että virukset eivät olleet ainoita haittaohjelmia vuonna 2004, sillä troijalaisiakin löydettiin vain muutama vähemmän ja jo seuraavana vuonna troijalaisia oli paljon enemmän kuin viruksia. Viruksia ei löydetty kuvion 1 mukaan enää vuonna 2008 yhtään ja viruksien tilalle olisi tulleet madot (englanniksi: worm), mutta näistä ei ole mainintaa missään lähteissä ja siten voidaan olettaa, että ne eivät ole kehittyneet kovinkaan haitallisiksi.

Symbianin ollessa suosittu alusta, sille tehtiin paljon enemmän haittaohjelmia kuin muille alustoille. Kun taas Androidista kasvoi suosituin, sille ilmestyi kertaheitolla moninkertaisesti haittaohjelmia. (Hyppönen 2007) Tämä ei kuitenkaan ole mitenkään uusi ilmiö, sillä se on huomattu myös tietokonepuolella, jossa Windows varmasti johtaa haittaohjelmien luvuissa. Onhan se loogistakin, että haittaohjelmia tehdään sinne, missä ne voivat varmimmin tarttua.

Kuten kuviosta 2 voidaan huomata, ensimmäisenä tulivat pelkästään haittaa tekevät haittaohjelmat. Haitta ei välttämättä ollut suurta, mutta jokainen haittaohjelma vaikuttaa jotenkin puhelimeen, ja se voidaan laskea haitaksi. Vasta vuonna 2009 haittaohjelmien tekijöitä alkoi motivoida tuotto, mikä on varsin myöhään. Toisaalta tämä ei myöskään ole kovin yllättävää



Kuvio 2. Tuotolla motivoidut haittaohjelmat 2004-2011. (F-secure 2011)

siinä mielessä, että ensin on luontevaa vain testailla haittaohjelmia ja sen jälkeen muokata niitä siten, että niillä voidaan saada voittoa. Aika nopeasti kuitenkin kehitys vei siihen, että raha ratkaisi noin joka toisessa haittaohjelmassa.

Alkuvaiheessa haittaa on tuotettu melko helpoilla tavoilla. On lähetetty viestejä, jotka maksavat uhrille. On poistettu tiedostoja tai varastettu salasananoja. Kaikkea tällaista haittaa, joka on todella kiusallista, koska matkapuhelimessa voisi kuvitella olevan nykyaikana paljon henkilökohtaista tavaraa, kuten kuvia, videoita ja yhteystietoja. Tämänkaltaista haittaa tekevien haittaohjelmien toteutus ei pitäisi olla kovinkaan vaikeaa, sillä pelkästään tiedostojen poistaminen ei vaadi kovinkaan montaa koodiriviä.

3 Mobiililaitehaittaohjelmien toinen sukupolvi: Boxer, Zeus, DroidKungFu

Alkuajan tapaan myös viime vuodet ovat olleet kasvuvaihetta haittaohjelmille, mutta on hyvä huomata oikea niin sanottu buumi eli huippusuhdanne vuosina 2009 ja 2010, jolloin Androidista tuli suosittu. (F-secure 2011, 2012d, 2013b) Mielenkiintoista on huomata, että tuottoa tavoittelevat haittaohjelmatehtailijat ovat kasvamassa. Vuosina 2010 – 2012 tuottoa tavoittelevat ja muutoin motivoituneet haittaohjelmatehtailijat ovat jakautuneet tasaisesti. (F-secure 2012d) Vuoden 2013 kolmannen neljänneksen luvut ovat paljon enemmän tuotolla motivoituneiden puolella: noin 81 prosenttia (F-secure 2013b).

Vuonna 2011 ja 2012 yksi isoimmista haittaohjelmaperheistä oli Boxer. (F-secure 2011, 2012a, 2012b, 2012c, 2012d) Mutta jostakin syystä Boxer ei esiintynyt F-Securen vuoden 2013 ensimmäisen neljänneksen raportissa ollenkaan. Vuoden 2013 kolmannen neljänneksen raportissa se sen sijaan esiintyy 15:sta eniten löydetyn ja tunnistetun haittaohjelmalistassa. (F-secure 2013a, 2013b)

Boxer haittaohjelmat, joka useimmissa vuoden 2012 F-Securen raporteissa esiintyy, on yleensä troijalainen, joka tuottaa rahaa rikollisille lähettämällä tilausviestejä eri palveluihin. (F-secure 2012a, 2012b, 2012c, 2012d) Boxer.D on kuitenkin riskihaittaohjelma (englanniksi: riskware), joka vain lähettää tekstiviestejä puhelimen eri yhteystietoihin. Troijalaisia, jotka tuottavat voittoa, käsitellään lähemmin luvussa 3.1.2.

Troijalaiset ovat haittaohjelmia, jotka esittävät jotain toista: mahdollisesti ohjelmaa. Nimitys tulee Troijan hevosesta. Troijalaiset ovat siitä ikäviä, että ne esittävät toista sovellusta, ehkä jopa oikeasti toimivaa sovellusta, mutta tekevät haittaa taustalla, niin tällöin käyttäjä ei välttämättä huomaa, että mobiililaite on saastunut.

Symbianin haittaohjelmat jatkavat ilmestymistään vielä vuonna 2013, vaikkakin ovat ainakin osuutena vähentyneet selvästi kulta-aikakaudestaan. (F-secure 2012c, 2013a) Symbianille tehdään vielä merkittävä osuus haittaohjelmista. F-secure 2012c raportissa kerrotaan, "Vuonna 2012 kolmannessa neljänneksessä havaittiin Symbianille 21 uutta perhettä ja va-

rianttia."ja "yleisesti Symbian troijalaiset matkivat järjestelmäpäivitystä tai aitoa sovellusta."

Symbian-haittaohjelmat ovat melko samanlaisia Android-alustan haittaohjelmien kanssa. Tartunta metodit ovat vain vähän erilaiset, mutta rahanhankintametodit ovat samat eli suosituimpana tilaustekstiviestit (englanniksi: premium-rate SMS), joista enemmän luvussa 3.1.2. Suurin osa haittaohjelmista on vielä rahaa tekeviä ja alkujaan Kiinasta. Esimerkkeinä voi mainita Fakepatch.A- ja Foliur.A -haittaohjelmat. (F-secure 2012c)

Artikkelissa Felt et al. 2011 on jaettu uhkat kolmeen kategoriaan: haittaohjelmat, vakoiluohjelmat ja harmaat ohjelmat. Tämä on kyllä hyvä jaottelu, mutta esimerkiksi F-Securen jaottelun mukaan nuo kaksi jälkimmäistä on samat, joka on F-Securen ei-toivottuja ohjelmia (englanniksi: potentialy unwanted software). Onkin parempi jakaa haittaohjelmia enemmän, koska selvästi troijalaiset ovat suurin osa haittaohjelmissa, mutta sen voi jakaa kahteen osaan: voittoa tuottavat (rahalla motivoidut-) ja muuten motivoidut -haittaohjelmat.

3.1 Troijalaiset

Vuonna 2012 trendi troijalaisissa muuttui merkittävästi. Aikaisemmin troijalaiset eivät yleensä toimineet oikeasti vaan esimerkiksi asennettu internetselainsovellus ei suostunut toimimaan antaen virheilmoituksen. Sitten käyttäjät hakivat hakukoneella virheilmoituksen ja saivat tietää sovelluksen olevan haittaohjelma. Vuonna 2012 tehtiin enemmän toimivia troijalaisia, jolloin käyttäjät eivät saaneetkaan enää tietää saastuneesta puhelimestaan niin helposti. (F-secure 2012a)

Kuten kuviosta 2 voi huomata, tuotto motivoi vasta 2009 vähintään yhtä paljon kuin muut motiivit. Sama trendi jatkui seuraavinakin vuonna ja sen vuoksi merkittävimmät troijalaiset ovatkin tuottoa tuottavia. Tuottoa voidaan tuottaa kahdella suositulla tavalla: tuotolla motivoidut- ja muulla tavalla motivoidut troijalaiset.

3.1.1 Voittoa tuottamattomat troijalaiset

F-secure 2011 raportissa mainitaan vuoden 2011 merkittävimpinä haittaohjelmina muun muassa FakeNetflic ja FakeBattScar. FakeNetflic on troijalainen, joka yrittää varastaa uh-

rin Netflix-tunnuksen ja salasanan. FakeNetflic esittää Netflixin mobiilisovellusta ja käyttäjän syöttäessä tunnuksensa sisäänkirjautumisruutuun tunnukset lähtevätkin rikollisille. FakeBattScar on myös troijalainen, mutta se esittää puhelimen akun kestoa parantavaa sovellusta. Oikeasti sovellus ottaa yhteyden palvelimeen ja lähettää tietoa puhelimesta samalla, kun se esittää mainosta.

3.1.2 Voittoa tuottavat troijalaiset

Rikollisilla on olemassa kaksi suosittua tapaa tuottaa rahaa mobiilitroijalaisilla tai mobiili- ja tietokonetroijalaisten yhdistelmällä.

Ensimmäisenä on SMS-viestein tilausviestinä (englanniksi: premium-rate SMS) siten, että tilataan jotain tekstiviestillä, ja siten rikolliset saavat tuottoa. Yleensä tällaisen huijauksen huomaa vasta laskusta. (F-secure 2012d) Tällaiset huijaukset voitaisiin poistaa kokonaan, jos jokainen maa asettaisi lainsäädäntönsä siten, että on laitonta tehdä tilauksia tekstiviestein. On vain epärealistista ajatella, että ihan kaikki maat sitoutuisi asettamaan tällaista lakia tai valvomaan sitä. Sen sijaan operaattorit voisivat estää tekstiviestien lähettämisen tällaisiin palveluihin, joka on mahdollista toteuttaa ja varmaankin ainakin osa operaattoreista toimii tällä tavalla.

Toisena metodina on pankkitroijalaiset, jotka voivat tuottaa todella isot tappiot uhrilleen. Vuoden 2012 loppupuolella löydetty Citmo.A toimii kuten aiemmat Zitmo ja Spitmo eli se varastaa mobile Transaction Authentication Numberin (mTAN), jonka pankki lähettää tekstiviestillä asiakkaalle validoidakseen transaktion. Täten troijalainen voi lähettää rahaa uhrin tililtä minne vain. (F-secure 2012d) Zitmoa tavataan myös Blackberryllä (F-secure 2012c).

Vuonna 2012 tuli myös yksi uudenlainen haittaohjelma, RootSmart.A. RootSmart oli mutkikas haittaohjelma, joka keräsi ensin tietoja puhelimesta. Tämän jälkeen tuli fiksu osuus: RootSmart niin sanotusti roottasi puhelimen eli hankki itselleen root-oikeudet sallien sen tehdä, jos ei mitä vaan puhelimessa, niin ainakin melkein mitä vain. RootSmart ei ole voittoa tuottava välttämättä, mutta siinä on esimerkiksi ominaisuus, että sen voi laukausta lähettämään tilaustekstiviestejä tai katsomaan maksullisia videoita. (F-secure 2012a)

DroidKungFu.H on myös root-oikeuden hankkiva troijalainen. DroidKungFu on vain erittäin vaikea poista puhelimesta, koska se tekee muutoksia muun muassa systeemikansioon. (F-secure 2012a)

Ensimmäinen niin sanottua drive by -metodia käyttävä troijalainen tavattiin vuonna 2012 toukokuussa. Trojan-Proxy:Android/NotCompatible.A, joka pystyi saastuttamaan puhelimen saastuneen internetsivuston avulla, ja jos puhelin oli asetettu sallimaan sovelluskaupan ulkopuoliset asennukset. Puhelimesta tuli täten osa bottiverkkoa. (F-secure 2012b)

Vuonna 2012 kolmannella neljänneksellä löydetty FinSpy on mielenkiintoinen troijalainen siinä mielessä, että se on monelle alustalle: Android, Symbian, Windows Mobile ja IOS. FinSpy on mobiiliversio FinFisher-troijalaisesta. FinSpy vakoilee muun muassa Skype-kommunikointia, tarkkailee puhelimen sijaintia, nauhoittaa näppäinpainallukset ja ottaa näyttökuvia eli screen shotteja. (F-secure 2012c)

Eurograbber-troijalainen taas saastutetaan ensin tietokoneelle, jonka jälkeen se houkuttelee uhrin saastuttamaan myös mobiililaitteensa. Yhdessä ne voivat tyhjentää uhrin pankkitiliä, mutta kuitenkin siten, että se ei herätä huomiota. Eurograbber onnistuikin varastamaan yli 47 miljoonaa Yhdysvaltain dollaria vuonna 2012. (F-secure 2012d)

3.2 Ei-toivotut sovellukset

Nämä ei-toivotut sovellukset (englanniksi: potentialy unwanted software) ovat eräänlaisia haittaohjelmia, vaikka eivät ole ainakaan F-Securen määritelmän mukaan haittaohjelmia (F-secure 2011). Mutta koska ne tuottavat haittaa käytäjälle, on luontevaa kutsua niitä haittaohjelmiksi.

Ei-toivotut sovellukset tuottavat siis haittaa puhelimen käyttäjälle erilaisin tavoin. Useimmat haitat liittyvät puhelimen SMS-viestien lähettämisominaisuuteen ja puhelimeen tallennettujen numeroiden sotkemiseen tai hyväksi käyttämiseen. Tällaisia ovat myös tarkkailutyökalut, joilla voidaan vakoilla puhelimia. (F-secure 2011) Esimerkiksi lapsien valvontaan tehtyjä tarkkailutyökaluja myydään ihan yleisesti ja tällaiset haittaohjelmat ovat ehkä jopa hyviä. Se, että onko tällainen tarkkailu eettisesti hyväksyttävää edes tai varsinkaan oman lapsen

kohdalla, on toinen asia.

Ei-toivottuja sovelluksia on kutsuttu myös nimellä harmaat ohjelmat tai -sovellukset (Felt et al. 2011), mutta ei-toivottu on hieman kuvaavampi nimi. Lisäksi harmaat ohjelmat eivät sisällä vaikoulutyökaluja tai -haittaohjelmia.

Yksi tällainen ei-toivottujen haittaohjelmien muoto on riskihaittaohjelmat (englanniksi: riskware), jotka eivät välttämättä tee mitään pahaa puhelimessa. Tällaisena haittaohjelmana esimerkkinä voidaan mainita Anudown.A, joka sovellus, joka tekee itselleen pikakuvakkeen Androidin aloitusruutuun ja sovellukseen tulee useita, isoja päivityksiä, jotka ovat turhia. Täten käyttäjälle tulee mahdollisia verkonkäyttölaskuja. (F-secure 2011) Laskua ei kuitenkaan tule, jos on kiinteä yhteys eli lasku on sama joka kuukausi riippumatta siitä, kuinka paljon internetyhteyttä käyttää.

Ei-toivotut sovellukset ovat olleet kasvussa ja vuoden 2013 kolmannen neljänneksen haittaohjelmista ei-toivotut sovellukset saavat 39 prosentin osan. (F-secure 2013b) Siksi onkin todennäköistä, että tulevaisuudessa näemme paljon enemmän tämänkaltaisia, pääosin vain ei-rahallista haittaa tekeviä haittaohjelmia.

4 Mobiililaitehaittaohjelmien kolmas sukupolvi: Chuli, PerkeSecuApp, Pincer

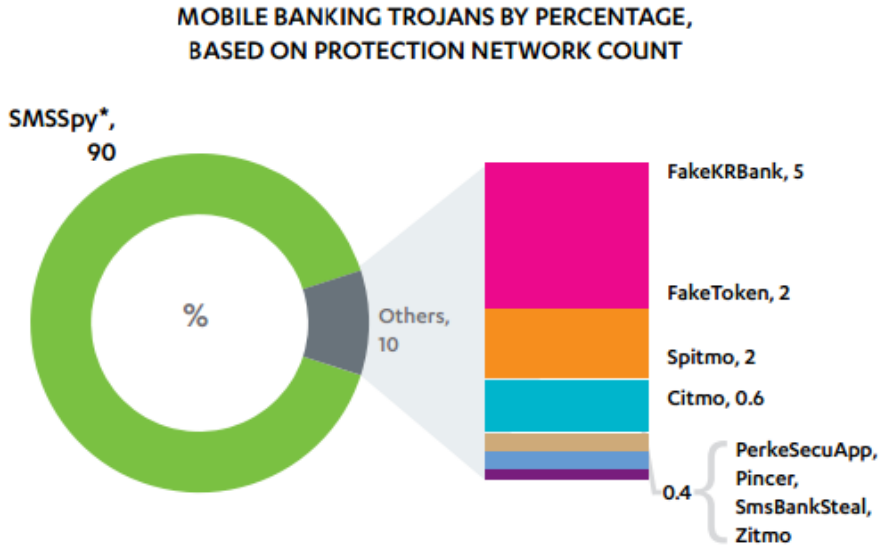
F-secure 2013a raportissa mainitaan nimeltä kaksi haittaohjelmaa: Stels ja PerkeSecuApp.A. Stels on jo vuonna 2012 löydetty troijalainen nimellä SmsSpy.K, joka levisi venäjänkielisenä. Stels oli ensin tilaustekstiviesteihin keskittynyt haittaohjelma, mutta sitten sitä muutettiin toimimaan roskaposti-modulina ja sitä levitetään nyt bottiverkossa. Stels siis vain lähettää paljon tekstiviestejä, joiden sisältö ohjaa vastaanottajaa haitalliselle sivustolle, jossa käyttäjää kehotetaan lataamaan Flash Player, joka oikeasti antaa troijalaiselle oikeudet soittaa puheluita. Stels tekee voittoa soittamalla kaukopuheluita, kun puhelimen omistaja on nukkumassa. (F-secure 2013a)

On paljon tapoja haittaohjelmalta huijata käyttäjää antamaan oikeudet tehdä puhelimessa jotain, kuten käyttää sijaintia tai soittaa puheluita. Usein tällaiset naamioidaan joksikin säännöiksi, jotka pitää hyväksyä. Tulemme varmasti näkemään lisää tällaisia luovempia ratkaisuita saada käyttäjä hyväksymään jotain, mitä ei oikeasti haluaisi.

PerkeSecuApp.A on pankkitroijalainen, mutta ei kuitenkaan ole uudenlainen sellainen. Se on paremmin varusteltu pankkitroijalainen, joka matkii Zeus-troijalaista. Mielenkiintoisen Perkeleestä tekee se, että se on kehitystyökalu, jolla voi tehdä oman PerkeSecuAppinsa, mutta myös se, että tämän kaltaisia haittaohjelmia on ollut vaikea saada. Nyt kuitenkin se on tuotu myös halvemmille markkinoille eli käytännössä kaikkien saataville haittaohjelmamarkkinoilla. (F-secure 2013a)

Kuvion 3 mukaan PerkeSecuApp ei kuitenkaan ole kovin laajalle levinnyt vielä ja toiseksi isoimmallakin on vain 5 prosenttiyksikön osuus. SmsSpy.F on ainakin yksi kyseisistä varianteista, joka kuviossa näkyy SmsSpy-perheen prosenteissa. SmsSpy perheessä käytetään myös tilaustekstiviestejä, mutta ainakin F-variantti on pankkitroijalainen, joka käyttää mTanin varastamista. (F-secure 2012b, 2013a)

Pankkitroijalaisiin tuli myös uusi metodi vuoden 2013 alkupuolella. Pincer.A pystyy murtamaan kahden vaiheen suojauksen (englanniksi: two-factor authentication). Tämä tapahtuu



Kuvio 3. Mobiilipankkitroijalaiset prosentuaalisesti. (F-secure 2013b)

vähän samanlailla kuin mTanin varastaminen, mutta tässä tapauksessa puhelimen pitää vielä lähettää tekstiviestin. (F-secure 2013b) Pankit käyttävät kahden vaiheen suojausta internet-pankin transaktioissa.

Vuoden 2013 alkupuolella oli myös muita mielenkiintoisia haittaohjelmia, kuten Chuli.A ja SmSilence.A. Kohdistetut hyökkäykset ovat ottamassa ensiaskeliaan jo vuonna 2013 ja siitä esimerkkinä on nämä kaksi troijalaista. Chuli on kohdistettu ihmisoikeusaktivisteille ja se kerää heidän tietojaan, kuten yhteystietoja, GPS-sijainnin, puheluhistorian ja tallennetut tekstiviestit. Tällaisen haittaohjelman kohderyhmää on helppo muokata ja sen vuoksi tämä haittaohjelma voi tulevaisuudessa olla todella vaarallinen, vaikka on se sitä jo nyt. (F-secure 2013a)

Vaikka Suomessa olevat ihmisoikeusaktivistit ovat melko turvassa niin on helppo kuvitella, kuinka joissakin Aasian maissa ihmisaktivisteja ei kohdella kovinkaan hyvin. F-secure 2013a raportissakin mainitaan, että on vain ajan kysymys, koska valtioihin ja hallintoihin aletaan kohdistaa hyökkäyksiä.

SmSilence.A kuitenkin jo kohdistaa hyökkäyksensä eteläkorealaisiin, koska tämä troijalainen on kiinnostunut vain +82-suuntanumeroiden tekstiviesteistä, joka on Etelä Korean suun-

tanumero. SmSilence asettaa prioriteettinsa niin korkealle, että se näkee tekstiviestin ensimmäisenä. Sen jälkeen se lähettää viestin sisällön ja lähettäjän puhelinnumeron etäpalvelimelle ja estää kaikki huomautukset uudesta viestistä, eikä käyttäjä huomaa, että hänelle on tullut uusia viestejä puhelimeensa. (F-secure 2013a)

F-secure 2013b raportin mukaan vuonna 2013 ennen kolmatta neljännestä ei ole löydetty yhtään uutta haittaohjelmaa muille alustoille kuin Androidille. Kolmas neljännes on siitä mielenkiintoinen, että tuotolla motivoidut haittaohjelmat ottavat selvästi isoimman osuuden. Tämä johtuu luultavasti siitä, että tilaustekstiviestimetodiin perustuvat haittaohjelmat kuten FakeInst, OpFake ja PremiumSms ovat kasvussa.

Mielenkiintoinen työkalu, jolla voi sijoittaa haittaohjelmakoodia oikeisiin sovelluksiin on Androrat APK binder, jolla sisällytetään oikeaan toimivaan sovellukseen AndroRAT-etäyhteystyökalu. Siten hyökkääjä voi kerätä tietoa saastutetusta puhelimesta ja käyttää kameraa sekä mikrofonia ja lähettää esimerkiksi tekstiviestejä sekä soittaa puheluita. (F-secure 2013b)

Toinen tapa käyttää aitoa sovellusta hyväksi on käyttää mainosmoduulia, joka ohjaa käyttäjiä saastutetuille sivustoille (F-secure 2013b). Koska haittaohjelmat eivät ole sovelluksessa, tällaisia sovelluksia on vaikea pitää poissa Googlen sovelluskaupasta ja siten myös tartuntoja tulee paljon.

5 Yhteenveto

Kirjallisuuskartoitusta tehdessä kävi ilmi, että jostakin ihmeellisestä syystä suurin osa artikkeleista oli vuosilta 2005-2008. Ilmeisesti mobiilivirukset olivat silloin jo tiedostettu, ja niitä alettiin tutkia. On kuitenkin huono, että uudempia tutkimuksia ei löydä ainakaan helpolla, koska tämä on varsin keskeinen aihe tällä hetkellä, kun katsoo kuinka mobiiliuhkat ovat kasvussa. (Hyppönen 2007)

Paras lähde on F-securen mobile threat reportit. Esimerkiksi F-secure 2012d raportti, jossa kerrotaan yhteenveto vuodesta 2012 ja verrataan ainakin vähän edellisten vuosien tuloksiin ja sen vuoksi kyseinen raportti oli erittäin hyvä yleiskuvan saamiseksi. Onkin suositeltavaa, että jos haluaa yksityiskohtaisempaa tietoa haittaohjelmista, tutustuu näihin raportteihin paremmin.

Kirjallisuuskartoituksen perusteella haittaohjelmien kärjessä ovat troijalaiset, mutta kaikki on alkanut viruksista, jotka levisivät puhelimen omien ominaisuuksien välityksellä, joista tärkeimmät viruksille olivat Bluetooth ja MMS-viestit. (F-secure 2013a, 2012d; Coursen 2007) Nykyään on kuvioon tullut myös niin sanotut ei-toivotut sovellukset, jotka koostuvat muun muassa vakoiluhaittaohjelmista, riskihaittaohjelmista ja seurantatyökaluista. (F-secure 2013b) Näistä seurantatyökalut ei varsinaisesti ole haittaohjelma, mutta muut ei-toivotut sovellukset ovat selvästi haittaa tuottavia ohjelmia ja siksi haittaohjelmia.

Haittaohjelmat varastavat yleensä puhelimesta tietoja, vaikka tekisivät paljon muutakin haittaa. Moni haittaohjelma lähettää puhelimesta erilaisia tietoja, kuten Google-accountin tietoja tai itse puhelimen tietoja kuten IMEI- ja IMSI numeroita. IMEI-koodia käytetään muun muassa matkapuhelimien tunnistamiseen verkossa. Näillä voi rikolliset tehdä rahaa joko itse käyttämällä tietoa tai myymällä sitä esimerkiksi mainontaa harjoittaviin yrityksiin tai epämääräisempiin ryhmittymiin.

Troijalaiset on selvästi suurin haittaohjelmien osa. Toisena tulee ei-toivotut haittaohjelmat, kun niitä tässä kirjallisuuskartoituksessa pidetään haittaohjelmana. Haittaohjelmat ovat jo useamman vuoden jakautuneet voittoa tuottaviin ja tuottamattomiin puoliksi. Joistakin voittoa tuottamattomista haittaohjelmista voi tai on muokattu sitten voittoa tuottavia. Jos trendi

pysyy samana, tulemme näkemään yhä enemmän haittaohjelmia, koska raha on varmasti suurimpana syynä haittaohjelmien nykykasvuun.

Vaarallisin troijalaisten metodi on root-oikeuden hankkiminen, koska se käytännössä antaa haittaohjelmalle oikeuden tehdä mitä vain. Myös käyttäjän itse tekemä niin sanottu roottaus on vaarallista, koska silloin, jos käyttäjä lataa saastuneen ohjelman puhelimeensa, se saa oikeuden tehdä paljon enemmän. Tällaisille rootatuille puhelimillekin on tehty omat haittaohjelmansa. (Felt et al. 2011)

2012 oli kovaa aikaa haittaohjelmapuolella sillä vielä NotCompatible.A-haittaohjelma ilmestyi joka käytti tartuttamiseen niin sanottua drive by -metodia eli saastutettu websivusto tartutti puhelimet suoraan, joissa oli asetuksissa sallittu sovelluskaupan ulkopuolisten ohjelmien asennus. Tämä tarkoitti jo sitä, että ilman mitään käyttäjän hyväksyntää, muuta kuin tuo asetus, pystyi haittaohjelma tulemaan puhelimeen, kun yleensä haittaohjelmat tarvitsevat luvan käyttäjältä.

Rahan hankintaan on olemassa kaksi suosittua tapaa. Suosituin varmasti on lähettää puhelimella tilaustekstiviestejä (englanniksi: premium SMS), joilla rikolliset saa tuottoa. Näistä todisteena ovat esimerkiksi Boxer-haittaohjelman perhe, joita on löydetty monena vuonna havaituista haittaohjelmalistoilta kärkisijoilta. Monet muut haittaohjelmat kuitenkin käyttävät ihan samaa metodia, vain numero, johon viesti lähetetään ja viestin sisältö muuttuvat. (F-secure 2012a, 2012b) Voittoa havittelemattomat haittaohjelmat eivät ole kehittyneet juurikaan tai ainakaan saman verran kuin voittoa havittelevat. Ehkä ne ovatkin vain askel, kun haittaohjelmatehtailijat siirtyvät mobiilipuolelle ja raha alkaa houkuttaa.

Toiseksi tavaksi on kivunnut tietokonepuolelta tutumpi pankkitroijalaiset. Vuonna 2012 näitä alkoi ilmestyä ainakin sellaisia, joissa metodina on niinkin yksinkertainen tapa kuin vain varastaa mobile Transaction Authentication Numberin (mTAN), joka tulee tekstiviestillä ja jolla validoidaan pankkitilin transaktioita. Pitää kuitenkin muistuttaa, että nämä mobiilipankkitroijalaiset eivät ole tavallaan se, joka varastaa vaan oikeasti rahat vie tietokoneelle saastutettu troijalainen, joka vain käyttää tätä mobiilitroijalaista hyväksi, koska osa pankeista käyttää ylimääräistä suojaa mTanin muodossa.

Nykyisin myös kaksivaiheinen suojaus pystytään murtamaan. Pankkien ohella, myös monet

palvelut, kuten Facebook ja Google käyttävät kaksivaiheista suojausta.

Ne haittaohjelmat, joilla ei rahaa tehdä, eivät jakaudu näin helposti suosittuihin metodeihin. Moni haittaohjelma varastaa puhelimen tietoja tai tuhoaa tietoja. Pelkästään itsensä näyttäminen käyttäjälle on myös suosittua. Tämä tapahtuu vaikka soittoäänen tai taustakuvan vaihtamisella.

Vuosi 2013 jatkui siitä mihin 2012 jäi eli uusia perheitä ja variantteja tulee kasvavalla tahdilla. Samoja metodeja käytettiin eli tilaustekstiviestejä, kaukopuheluita ja pankkitroijalaisten mTanin varastamista. Perkele oli erittäin huono uutinen muiden kuin rikollisten kannalta, koska se on varsin kehittynyt pankkitroijalainen, joka on nyt useimpien käytettävissä. Uutena metodina voidaan myös mainita se, että kohdennetut hyökkäykset ovat alkaneet ottaa ensiaskeliaan mobiilipuolella. Chuli-troijalainen on varsin hyvä esimerkki siitä, mihin ollaan menossa ja miten vaarallisia troijalaiset voivat oikeasti olla.

Myös Androrat APK binder on hyvä esimerkki siitä, että mobiilihaittaohjelmat alkavat olla jo varsin kehittyneitä ja mutkikkaita. Rikolliset oppivat ovelimmiksi ja hyökkäystavat monipuolistuvat, vaikka itse päämetodit eivät ole muuttuneet paljon.

Androrat on kehitystyökalu, kuten on myös Perkele. Näillä pyritään tekemään haittaohjelmien tekeminen helpoksi tai ainakin helpommaksi. Tämähän käytännössä tarkoittaa sitä, että haittaohjelmien määrä tulee kasvamaan.

Lähteet

Coursen, Shane. 2007. “Mobile Malware: The future of mobile malware”.

Delac, G, M Silic ja J Krolo. 2011. “Emerging security threats for mobile platforms”.

Felt, Adrienne Porter, Matthew Finifter, Erika Chin, Steven Hanna ja David Wagner. 2011. “A Survey of Mobile Malware in the Wild”.

F-secure. 2011. *Mobile threats report Q4 2011.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202011.pdf`, viitattu 1.11.2013.

———. 2012a. *Mobile threats report Q1 2012.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q1%202012.pdf`, viitattu 1.11.2013.

———. 2012b. *Mobile threats report Q2 2012.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q2%202012.pdf`, viitattu 1.11.2013.

———. 2012c. *Mobile threats report Q3 2012.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q3%202012.pdf`, viitattu 1.11.2013.

———. 2012d. *Mobile threats report Q4 2012.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf`, viitattu 1.11.2013.

———. 2013a. *Mobile threats report Q1 2013.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013.pdf`, viitattu 1.11.2013.

———. 2013b. *Mobile threats report Q3 2013.* Saatavilla WWW-muodossa, `http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf`, viitattu 12.11.2013.

Gartner. 2013. *Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time.* Saatavilla WWW-muodossa, `http://www.gartner.com/newsroom/id/2573415`, viitattu 1.11.2013.

Gilbert, Peter, Byung-Gon Chun, P. Cox Landon ja Jaeyeon Jung. 2011. “Vision: automated security validation of mobile apps at app markets”.

Goode, Alan. 2010. “Mobile Security: Managing mobile security: How are we doing?”

Hyppönen, Mikko. 2007. *State of cell phone malware in 2007.* Saatavilla WWW-muodossa, `https://www.usenix.org/legacy/event/sec07/tech/hypponen.pdf`, viitattu 1.11.2013.