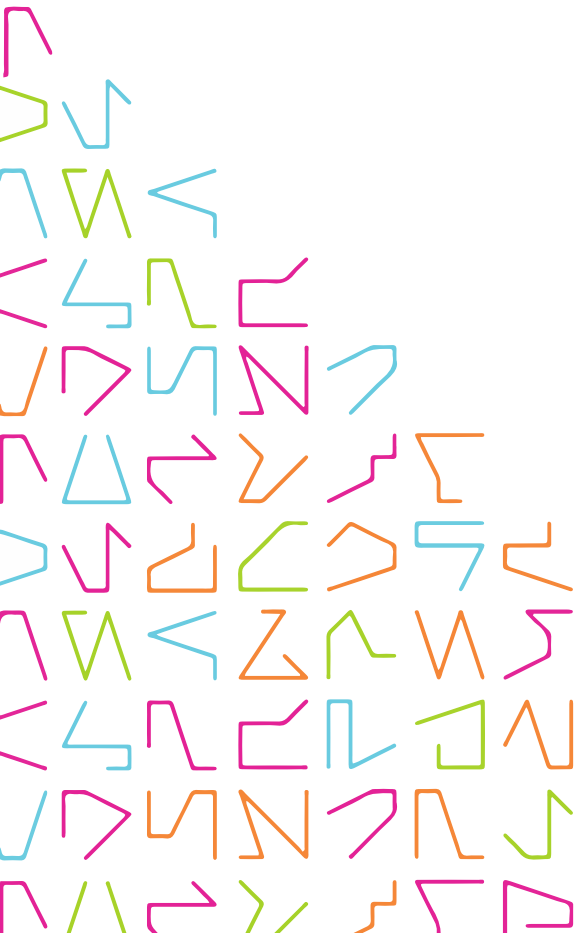
TAMPEREEN
AMMATTIKORKEAKOULU

ANDROIDIN TIETOTURVAUHAT JA NIILTÄ SUOJAUTUMINEN

Jukka Kemppainen



Opinnäytetyö
Toukokuu 2018
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

KEMPPAINEN JUKKA:
Androidin tietoturvauhat ja niiltä suojautuminen

Opinnäytetyö 37 sivua, joista liitteitä 2 sivua
Toukokuu 2018

Älypuhelimet ja tablet-laitteet ovat tietoturvan kannalta hankalin mahdollinen ympäristö. Ne on helppo hukata ja varastaa, laitteet eivät tahdo kestää arjen kolhuja ja niiden tietoturvaominaisuudet jättävät toivomisen varaa. Mobiililaitteissa on useita osapuolia: laitevalmistaja, käyttöjärjestelmä, sovellus, pilvipalvelu, operaattori ja niin edelleen. Käyttäjällä ei ole mitään keinoa varmistua kaikkien osien turvallisuudesta.

Työn alussa tutustutaan Android-käyttöjärjestelmään, jonka jälkeen tarkastellaan erinäisiä käyttöjärjestelmän käyttäjiä koskevia uhkia. Työssä esitetään suurimmat uhat ja neuvotaan, kuinka niitä vastaan voidaan suojautua.

Tämän opinnäytetyön tarkoituksena on koota ajankohtainen tietopaketti Android-järjestelmiä koskevista tietoturva-asioista. Tavoitteena on, että tämän työn lukija ymmärtää kuinka pieniltä tuntuvat asiat saattavat olla yllättävän tärkeitä tietoturvan kannalta.

Asiasanat: android, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

KEMPPAINEN JUKKA:
Android security threats and protection against them

Bachelor's thesis 37 pages, appendices 2 pages
May 2018

Smartphones and tablet devices are the most difficult environment for security. They are easy to miss and steal, devices do not endure everyday knockouts and their security features leaves room to improvement. Mobile devices have multiple parties: device manufacturer, operating system, application, cloud service, carrier, and so on. The user has no way of ensuring the security of all parts.

This thesis consists introduction to the Android operating system, look around largest threats which affect users of the operating system and guidance how to protect yourself against them.

The purpose of this thesis is to compile topical information pack on security issues in Android systems. The goal is that the reader of this thesis understands how even smallest things seem to be surprisingly important for security.

Key words: android, security

SISÄLLYS

LYHENTEET JA TERMIT

AOSP	Android Open Source Project. Androidin avoimen lähdekoodin projekti, johon kaikki Android käyttöjärjestelmät perustuvat.
APK	Android Application Package. Android-sovelluksen asennuspaketti.
EOL	End-of-Life. Kuvaa yleensä käytöstä poistuvaa laitetta.
OTA	Over the Air. Langattomasti Internetin välityksellä jaettava päivitys.
VPN	Virtual Private Network. Mahdollistaa maarajoitteiden kierron ja suojaa liikenteen.
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 JOHDANTO

Nykyajan älypuhelimet ovat teknisiltä ominaisuuksiltaan täysin rinnastettavissa tietokoneisiin, mutta useimmat käyttäjät eivät suojaa mobiililaitteitaan yhtä tehokkaasti kuin tietokoneitaan. Teoriassa älypuhelimet mahdollistavat jopa vaarallisemman tietoturvariskin kuin tietokoneet, koska älypuhelimet sisältävät enemmän sensoreita ja seuraavat käyttäjän toimintaa enemmän. Tämän seurauksena puhelin oppii tuntemaan käyttäjänsä paremmin ja puhelimesta tulee myös käyttäjälle apuväline jota ilman ei pärjäisi.

Älypuhelimet myös keräävät käyttäjän dataa ja jakavat sitä puhelinvalmistajalle, älypuhelimeen asennettujen sovellusten kehittäjille sekä muille kolmansille osapuolille käyttäjän sitä huomaamatta. Nykyään yhä suurempi osa datasta lähetetään myös eri pilvipalveluihin, vaikka käyttäjä ei sitä välttämättä tiedostaisi. Pienetkin sovellukset vaativat käyttäjältä monia oikeuksia toimiakseen kunnolla ja tällä tavoin sovelluskehittäjät saavat myytyä käyttäjän dataa mainostajille ja tällä tavoin tienaavat ilmaisilla sovelluksilla.

Älypuhelimiin kohdistuvat tietoturvariskit voidaan jakaa laitteistoista sekä ohjelmistoista löytyviin haavoittuvuuksiin. Suurin osa haavoittuvuuksista löytyy ohjelmistoista, sillä niitä on runsaasti enemmän eikä kaikkien sovelluksen laadunvalvontaan kiinnitetä välttämättä niin paljon kuin laitteistopuolella. Sovelluksia myös päivitetään laitteistoa enemmän, jonka seurauksia uusia haavoittuvuuksia voi syntyä.

Nykyajan älypuhelimista löytyy monenmoista käyttöjärjestelmää, mutta suurin osa älypuhelimesta käyttää Androidia käyttöjärjestelmänään. Suurin kilpailijalle Androidille on Applen iOS-käyttöjärjestelmä, joka löytyy vain Applen mobiililaitteista. Muita kilpailijoita ovat muun muassa Windows Phone, BlackBerry sekä monet erilaiset Linux-pohjaiset käyttöjärjestelmät. Päädyin tässä työssä käsittelemään kuitenkin Androidia sen markkinaosuuden ja avoimen ympäristön perusteella.

Tämän opinnäytetyön tarkoituksena on koota ajankohtainen tietopaketti Android-järjestelmiä koskevista tietoturva-asioista. Työssä esitetään suurimmat uhat ja neuvotaan, kuinka niiltä voidaan suojautua.

2 ANDROID-KÄYTTÖJÄRJESTELMÄ

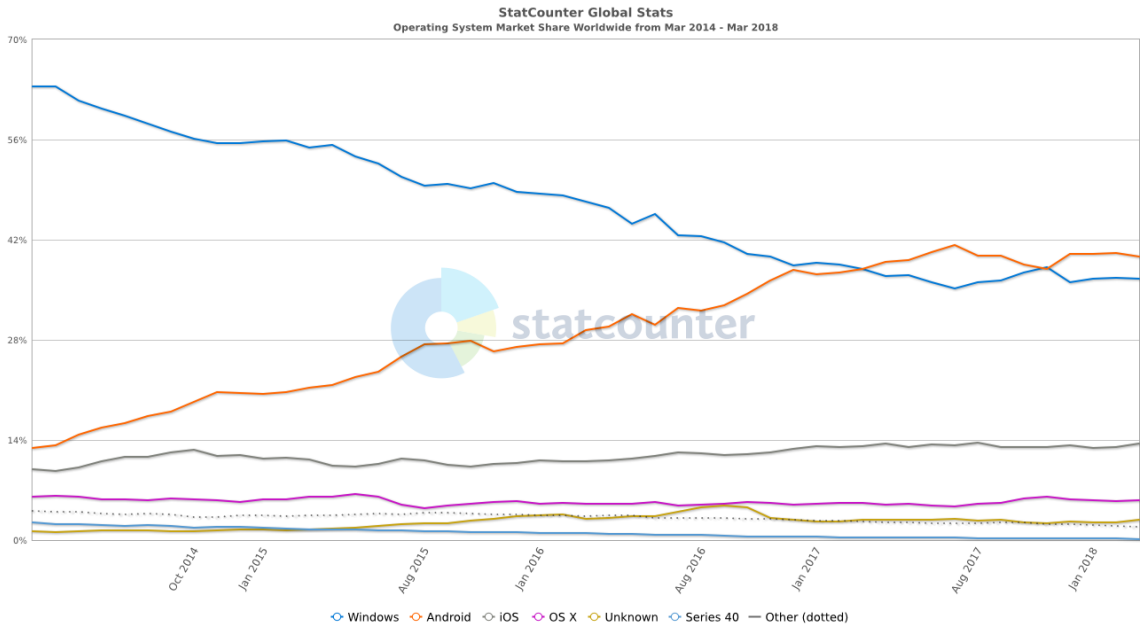
Tässä kappaleessa selvitetään hieman Androidin historiaa sekä käydään läpi asioita, jotka tekevät Android-puhelimesta uhan tietoturvan kannalta.

2.1 Taustaa

Vaikka yleisesti Androidia pidetään Googlen kehittämänä ja ylläpitämänä käyttöjärjestelmänä, väite pitää vain puoliksi paikkaansa. Vuonna 2003 perustettu Android Inc. kehitti käyttöjärjestelmän, josta piti tulla alun perin digikameroille suunniteltu, mutta koska markkinat olivat suuremmat puhelinmaailmassa, kehitys suuntautui niille markkinoille. Tästä Google kiinnostui vuonna 2005 saadakseen kilpailua silloista markkinajohtajaa Symbiania vastaan. Tällöin käyttöjärjestelmän ydin vaihdettiin myös Linux-pohjaiseksi.

Vuonna 2007 perustettiin Open Handset Alliance (OHA), jonka tarkoituksena oli muodostaa avoimet standardit mobiilimarkkinoille. Myös Androidin kehittäminen siirtyi tälle organisaatiolle. Yhteenliittymää koordinoi Google, mutta mukana oli myös tietoliikenneyrityksiä, ohjelmointifirmoja sekä komponentti- ja laitevalmistajia. Suurista yrityksistä mukana olivat muun muassa Sprint, T-Mobile, Intel, NVIDIA, Texas Instruments, HTC, Sony ja Samsung. Nykyään OHA sisältää 84 eri yritystä joiden tavoitteena on luoda Androidin käyttökokemusta yhä paremmaksi.

Ensimmäinen yleisesti saatavilla oleva Androidia käyttävä laite, HTC Dream, tuli markkinoille 23.9.2008 ja sen jälkeen markkinoille on tullut tuhansia uusia laitteita ja laskuissa on lähes mahdotonta pysyä mukana. Vuonna 2015 erilaisia Android-pohjaista laitteita oli maailmassa ainakin yli 24000 lähes 1300 valmistajalta. (Sawers, 2015)

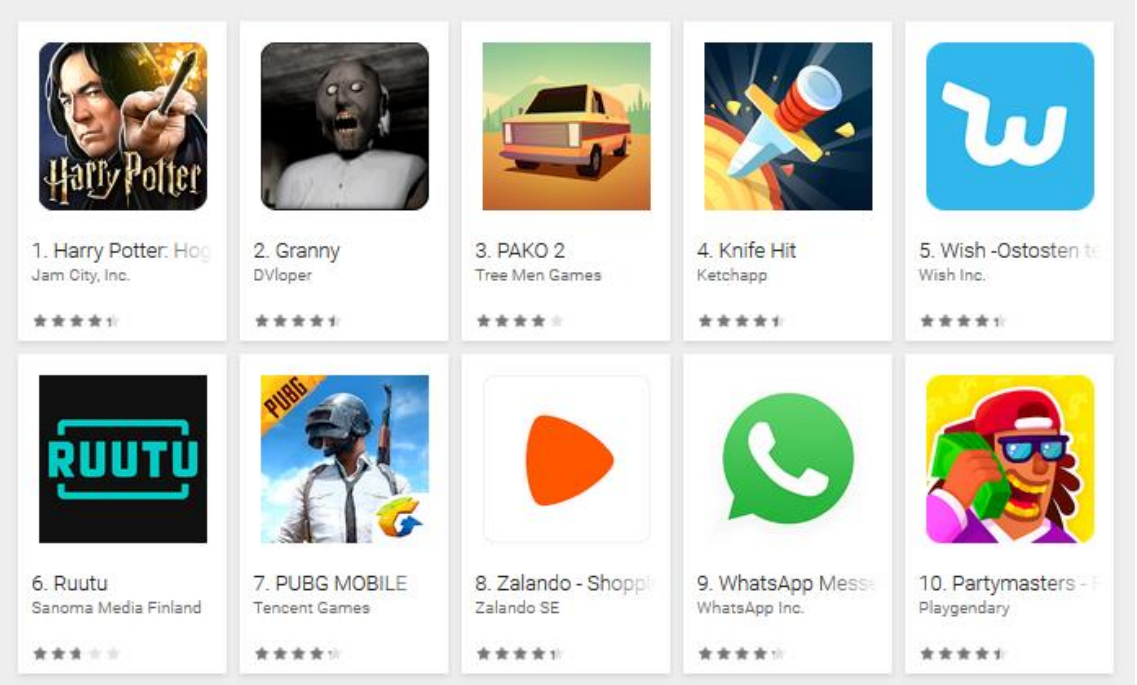


KUVA 1. Käyttöjärjestelmien markkinaosuudet 3/2014 – 3/2018 (Statcounter, 2018)

Kuten kuvasta 1 nähdään, vuonna 2018 Android on maailman käytetyin käyttöjärjestelmä. Aikaisemmin kärkisijaa pitänyt Windows on ollut tasaisessa laskussa ja menettänyt markkinaosuuttaan lähinnä Androidille vuodesta 2013 alkaen. Vielä tammikuussa 2013 Windowsin markkinaosuus oli yli 75 prosenttia ja Androidin 5.9 prosenttia. Android on kuitenkin kasvattanut osuuttaan merkittävästi viime vuosina ja maaliskuussa 2017 Android ohittikin Windowsin maailman suosituimpana käyttöjärjestelmänä. Siitä lähtien Android on pysynyt markkinajohtajana marraskuuta 2017 lukuun ottamatta. Huhtikuussa 2018 Androidin markkinaosuus oli mobiilikäyttöjärjestelmissä 75.66 prosenttia ja kaikissa käyttöjärjestelmissä 40.06 prosenttia. (Statcounter)

2.2 Sovellukset ja niiden hankinta

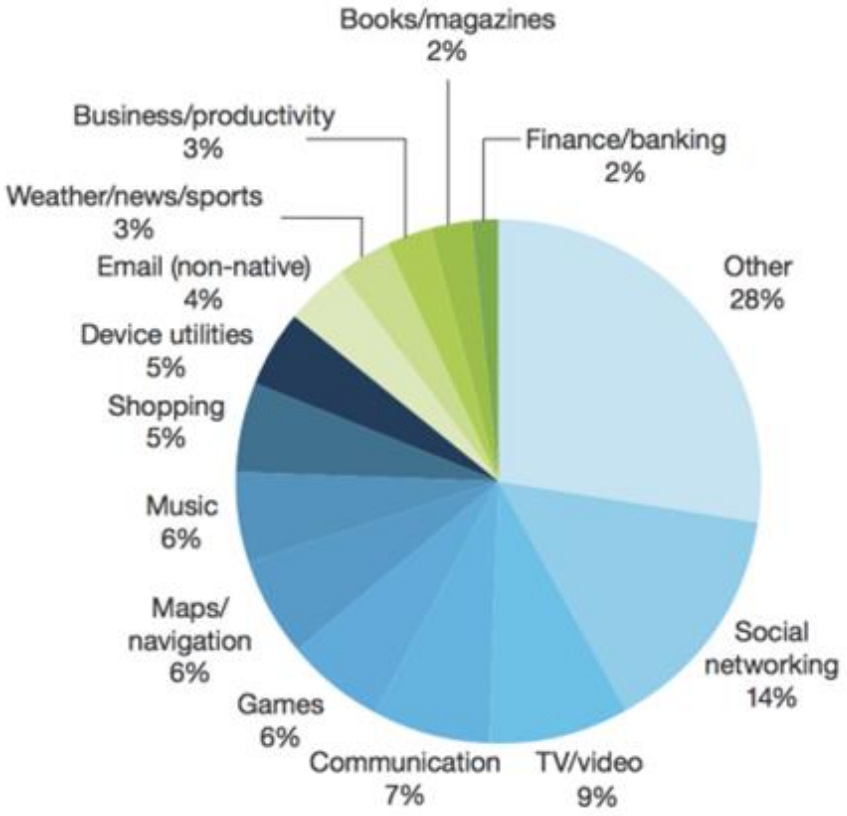
Nykypäivän mobiililaitteet ovat siis täysiperäisiä tietokoneita, joihin voidaan ladata erilaisia sovelluksia kuten tietokoneisiinkin. Laitteista löytyvät laitevalmistajasta riippuen eri määrä valmiiksi asennettuja sovelluksia, mutta käyttäjä joutuu useimmiten lataamaan käyttämänsä sovellukset itse puhelimeen. Nykyään monet laitevalmistajat haluavat tarjota käyttäjille mahdollisimman puhtaan Android-kokemuksen. Tämä saadaan, kun AOSP:n julkaisemaa Androidin lähdekoodia muokataan mahdollisimman vähän ja laitteeseen on esiasennettu vain ja ainoastaan Googlen sovellukset.



KUVA 2. Google Playn suosituimmat sovellukset huhtikuun lopussa 2018 (Google Play)

Suosituimpien sovellukset ovat esitetty kuvassa 2. Top10-listalta löytyy yleensä sen hetken hittipelit sekä sosiaalisen median sovellukset. Tässä listauksessa mukaan on päässyt pelien lisäksi myös verkkokaupat Wish sekä Zalando, suoratoistopalvelu Ruutu sekä pikaviestinpalvelu WhatsApp Messenger.

Keskimäärin Android-puhelimeen on asennettu 80 eri sovellusta, joista päivittäin käytössä on noin kymmentä. Sovellusten määrä eroaa huomattavasti eri maiden välillä, esimerkiksi Meksikossa puhelimeen on asennettu alle 70 sovellusta ja Japanissa vastaava lukema on yli 100. (Perez, 2017)

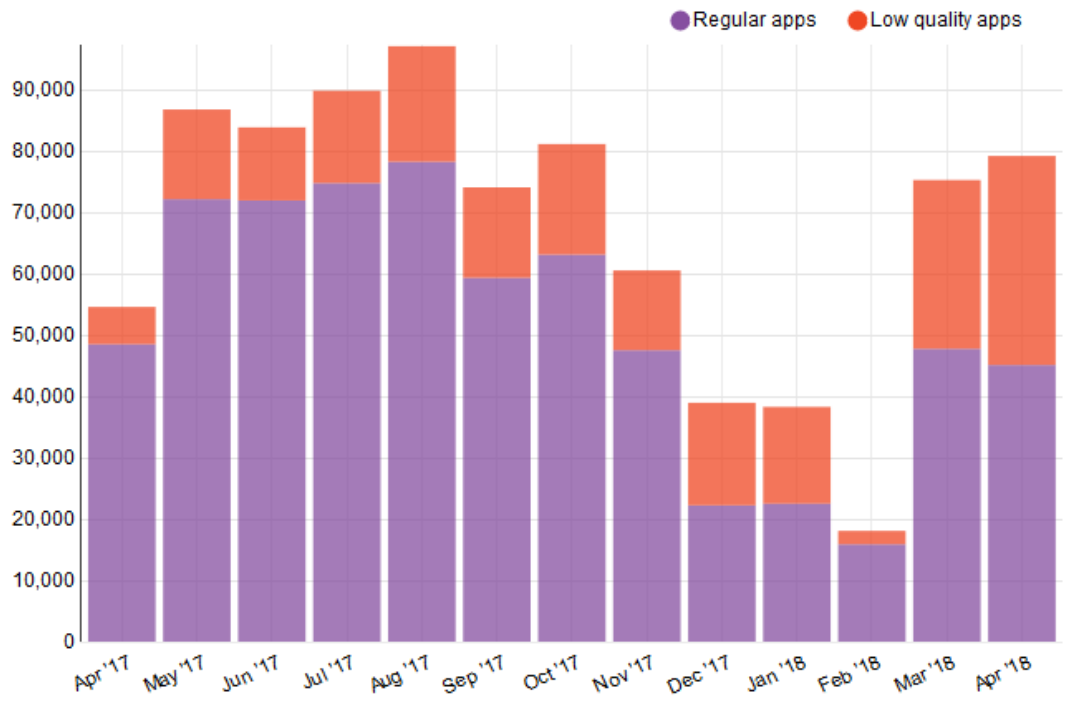


KUVA 3. Sovellusten jakautuminen aihepiireittäin (Perez, 2017)

Suosituin sovelluskategoria 14 prosentin osuudella kaikista sovelluksista on sosiaalisen median sovellukset joita seuraa erilaiset suoratoistopalvelut/videosovellukset. Kommunikointisovelluksiin kuuluvat muun muassa videopuhelusovellukset kuten Skype ja pikaviestinsovellukset kuten WhatsApp Messenger. Seuraavina tulevat musiikki- ja karttasovellukset sekä pelit 6 prosentin osuudella.

2.2.1 Google Play

Googlen omasta sovelluskaupasta, Google Playsta, löytyy nykyään niin sovellukset, musiikki, kirjat, elokuvat sekä myös laitekauppa. Sovelluksia kaupasta löytyy noin 3.7 miljoonaa kappaletta, joista AppBrainin mukaan noin 500 000 on huonolaatuisia sovelluksia, joista osa on myös mahdollisesti haitallisia. Osa Google Playn ominaisuuksista ei ole käytettävissä kaikissa maissa, esimerkiksi Suomessa puhelinten ostaminen Play kaupan välityksellä ei ole mahdollista.



KUVA 4. Uudet sovellukset Google Playssa kuukausittain 4/2017- 4/2018 (AppBrain)

Kuvasta 4 voidaan havaita, että sovelluksia tulee markkinoille kesäkuukausina huomattavasti enemmän kuin talvella ja odotettavissa onkin, että vuoden 2018 kesäkuukausina rikotaan 100 000 uuden sovelluksen kuukausiraja. Myös huonolaatuisten sovellusten määrä kasvaa räjähdysmaisesti kesäisin.

2.2.2 Muut kauppapaikat

Joissain maissa Googlen Play kauppa ei toimi kokonaisuudessaan. Tällaisia maita ovat muun muassa Kiina, Kuuba ja Iran, joissa sovellusten lataaminen ei ole mahdollista ilman geoblokkausta eli maarajoitteiden kiertämistä. Kiinassa Googlen sovelluskauppa onkin vasta seitsemänneksi suosituin sovellusten latauspaikka. Kiinan top10 sovelluskaupat on esitetty kuvassa 5.

KUVA 5. Suosituimmat Android-sovellusten kauppapaikat Kiinassa joulukuussa 2017. (TalkingData)

Kuten ylläolevasta kuvasta nähdään, monet kiinalaiset suuryhtiöt ovat perustaneet kilpailevia sovellusten kauppapaikkoja kerätäkseen kiinalaisten sovelluksiin käyttämää rahaa

omiin taskuihinsa. Kiinassa sovelluskauppa käy kuumimmin kuin koskaan ja vuonna 2017 sovelluksiin käytetty raha kasvoi 270 prosenttia vuoteen 2016 verrattuna CNBC:n tutkimuksen mukaan. Vuonna 2017 kiinalaiset kuluttivat yli 35 miljardia Yhdysvaltojen dollaria mobiilisovelluksiin.

360 Mobile Assistant on Kiinan toiseksi suurimman hakukoneen, Qihoon, tuote. Tencent puolestaan on Aasian arvokkain pörssiyhtiö, joka tunnetaan muun muassa WeChatin kehittäjänä. MIUI App Store on kiinalaisen elektroniikkavalmistajan Xiaomin oma sovelluskauppa. Huawei, Oppo, Vivo ja Meizu ovat puhelinvalmistajia ja Baidu on Kiinan suosituin hakukone. Wandouija on puolestaan Aasian toiseksi suurimman pörssiyhtiön Alibaban omistuksessa oleva sovelluskauppa.

2.2.3 APK-tiedostojen asennus

On olemassa myös sovelluksia, joita ei syystä tai toisesta löydy sovelluskaupoista vaan laitetaan jakoon esimerkiksi nettisivun kautta. Tällaisena esimerkkinä on Veikkauksen oma mobiilisovellus, jota ei saa laittaa Googlen Play kauppaan sen sisältämän vedonlyöntimahdollisuuden takia. Näiden sovellusten asentaminen on mahdollista lataamalla apk-tiedosto ja hyväksymällä laitteen asetuksista tuntemattomista laitteista tulevien sovellusten asentaminen (kuva 6).

KUVA 6. Tuntemattomien lähteiden hyväksyminen

Sovelluksen asentaminen onnistuu tämän jälkeen avaamalla apk-tiedosto tiedostohallinnan kautta ja seuraamalla ruudulle tulevia ohjeita. Sovelluksen päivittäminen on tämän jälkeen hieman haastavampaa kuin sovelluskaupasta hankituille sovelluksille, sillä uuden version joutuu aina lataamaan uudestaan eikä sovellusta saa suoraan päivitettyä OTA-yhteyden välityksellä.

2.3 Päivitykset

Tärkein ja helpoin tapa pitää haittaohjelmat pois laitteesta on pitää laite sekä sovellukset päivitettynä. Laitevalmistajat lupaavat yleensä laitteelle päivitykset kahdeksi vuodeksi, mutta tämä koskee lähinnä vain valmistajien lippulaivamalleja ja suosituimpia malleja. Halvempien tuotteiden tuki jää yleensä kauas tästä luvatusta kahdesta vuodesta ja voi olla, ettei laite saa päivityksiä ollenkaan. Usein päivitykset tulevan puhelimeen automaattisesti OTA:na, mutta jossain tapauksissa suuremmat päivitykset joudutaan asentamaan manuaalisesti. Päivitykset voi myös itse asentaa manuaalisesti lataamalla asennustiedoston valmistajan sivuilta, mikäli haluaa päivitykset mahdollisimman pian.

Play kauppa osaa päivittää sovellukset automaattisesti, mikäli käyttäjä sallii tämän. Tämä mahdollistaa sen, että kaikki sovellukset pysyvät päivitettyinä, vaikkei käyttäjä muistaisi aina välttämättä itse niitä päivittää.

TAULUKKO 1. Android-versiot huhtikuussa 2018 (Android developer)

Versio	Nimi	API	Markkinaosuus
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.4%
4.1.x	Jelly Bean	16	1.7%
4.2.x		17	2.2%
4.3		18	0.6%
4.4	KitKat	19	10.5%
5.0	Lollipop	21	4.9%
5.1		22	18.0%
6.0	Marshmallow	23	26.0%
7.0	Nougat	24	23.0%
7.1		25	7.8%
8.0	Oreo	26	4.1%
8.1		27	0.5%

Kuten yllä olevasta taulukosta nähdään, Android-päivitykset eivät saavuta loppukäyttäjiä nopealla tahdilla. Suosituin Android-versio on edelleen lokakuussa 2015 julkaistu Android 6.0 Marshmallow. Pelkkä Android-versio ei kuitenkaan kerro tietoturvapäivitysten tasosta. Osa valmistajista kuten Samsung ja Sony lupaa huippumalleilleen kuukausittaiset tietoturvapäivitykset, mutta suurin osa varsinkin pienemmistä ja vähemmän tunnetuista laitevalmistajista eivät tarjoa laitteilleen välttämättä mitään tukea laitejulkaisun jälkeen.

Jotkut valmistajat ovat lisäksi esittäneet päivittävänsä laitteiden tietoturvapäivitykset, mutta todellisuudessa vain muuttaneet päiväysten aikaleimaa ilman varsinaisia korjauksia. Saksalaiset SRL:n tutkijat havaitsivat, että tärkeimmistä älypuhelinvalmistajista Google, Sony ja Samsung tekivät parhaan tuloksen maksimissaan yhden korjauksen korjaamatta jättämisellä, OnePlus ja Nokia jättivät väliin yhdestä kolmeen korjausta. HTC, Huawei, LG ja Motorola jättivät kolme tai neljä korjauspäivitystä tekemättä, kun taas kiinalaiset valmistajat TCL ja ZTE jättivät enemmän kuin neljä. (Gibbs, 2018)

3 UHAT

Seuraavissa kappaleissa käsitellään, millaisia erilaisia uhkia Android-laitteeseen kohdistuu. Erilaisia uhkia on lukuisia eikä tässä työssä pystytä niitä kaikkia käymään läpi, joten seuraavissa kappaleissa on esitelty suurimmat ja tunnetuimmat uhat esimerkin.

3.1 Haavoittuvuudet

Haavoittuvuudella tarkoitetaan ohjelmistossa tai laitteistossa olevaa tietoturva-aukkoa, jota hyödyntämällä hyökkääjä pystyy ohittamaan puhelimen suojauksen ja siten pääsemään käsiksi laitteen dataan tai pahimmassa tapauksessa jopa hallitsemaan laitetta etäyhteyden välityksellä.

Haavoittuvuudet voidaan jakaa rautatason haavoittuvuuksiin ja ohjelmiston haavoittuvuuksiin. Vuonna 2018 neljä suurinta Android-käyttäjää koskevaa uhkaa ovat tsekkiläisen tietoturvayhtiön Avast Softwaren mukaan latausohjelmat, mobiilipankkeihin kohdistuvat malwaret, matkapuhelimien ransomwaret sekä huijaussovellukset.

Latausohjelmat ovat ohjelmistoja, jotka lataavat malwarea sovelluksen taustalla käyttäjän siitä tietämättä. Lataushetkellä käyttäjä on antanut sovellukselle luvan ladata tiedostoja taustalla sekä päästä käsiksi laitteen tietoihin. Näin malware pääsee selaamaan laitteen tietoja ja etsimään tietoja joilla voisi hyötyä taloudellisesti. Mahdollisesti jopa suurempi uhka on mobiilipankkeihin kohdistuvat malwaret, jotka keräävät käyttäjätunnuksia ja tunnuslukuja. Tällainen haittaohjelma oli muun muassa viime vuonna Android-laitteissa levinnyt BankBot. Tämä kyseinen ohjelma pystyi pankkitietojen lisäksi varastamaan sosiaalisen median käyttäjätunnuksia sekä urkkimaan laitteen sisältävää dataa.

Vuonna 2018 suuri uhka tulee olemaan ransomware-iskut. Viime vuoden toukokuussa maailmalle levisi WannaCry -haittaohjelma Windows-käyttöjärjestelmään ja saastutti muutamassa päivässä yli 200 000 tuhatta laitetta yli 150 maassa. Vastaavien haittaohjelmien uskotaan vuonna 2018 leviävän myös mobiililaitteisiin, sillä niitä on tällä hetkellä enemmän ja niiden tietoturva on heikommalla tasolla. Ransomware tarkoittaa iskua, jossa saastunut laite lukitaan ja vaaditaan lunnaita sen toiminnan palauttamiseksi (kuva 7).

KUVA 7. Esimerkki ransomware-iskusta (ArsTechnica)

Lisäksi huijaussovellusten määrä tulee kasvamaan suuresti tänä vuonna. Sovelluskaupoista löytyy tälläkin hetkellä lukuisia sovelluksia, jotka muistuttavat kirjoitusasultaan, kuvakkeeltaan sekä tiedoiltaan suosituimpia sovelluksia. Nämä huijaussovellukset saattavat myös toiminnaltaan näyttää esikuvaltaan, mutta todellisuudessa sovellukset sisältävät runsaasti malwarea ja saattavat jopa altistaa laitteeseen osaksi bottiverkkoa louhimaan kryptovaluuttoja.

Tietoturva-ala on tällä hetkellä muutoksen kourissa, kun uusi EU:n tietosuoja-asetus GDPR (*General Data Protection Regulation*) astuu voimaan toukokuussa 2018. Tämän seurauksena F-Securen toimitusjohtajan Mikko Hyppösen mukaan verkkorikollisuus tulee todennäköisesti kasvamaan ja lunnashyökkäyksen määrä nousemaan räjähdysmäisesti. Nämä hyökkäykset kohdistuvat pääosin yritykseen ja organisaatioihin, mutta myös yksityisellä henkilöllä pitäisi olla selvillä mitä muutoksia GDPR voi aiheuttaa omaan elämään.

3.2 Haittaohjelmat

Haittaohjelma, englanniksi malware, ei eroa normaalista ohjelmasta muuten kuin että sen tarkoitus on aiheuttaa ongelmia tartunnan saaneisiin laitteisiin. Nämä toimivat useammilla eri tavoilla, mutta usein niillä käyttäjän tietoja haltuun. Mobiilialustoilla nämä ohjelmat asentuvat laitteeseen ja naamioivat itsensä joksikin toiseksi sovellukseksi. Siten ne pääsevät livahtamaan käyttäjän huomaamatta laitteeseen. Tällaisen haittaohjelman tunnistaa helposti lukemalla sovelluksen arvostelut tai tarkastelemalla sovelluksen vaatimia oikeuksia. Yleensä haitallinen sovellus vaatii ainakin oikeuden päästä käsiksi laitteen sisältämiin lokitiedostoihin. Alla olevassa kuvassa eroaa vasemmanpuoleinen haitallinen malware sekä oikealla oleva alkuperäinen sovellus (kuva 8).

KUVA 8. Naamioitunut haittasovellus sekä alkuperäinen sovellus (VirusBulletin)

Tunnetuimpia haittaohjelmia ovat virukset ja madot. Tyypillisesti viruksia saadaan laitteelle sähköpostin kautta, ladattaessa tiedostoja internetistä tai pikaviestinohjelman välityksellä. Haittaohjelmien levittämiseen voidaan käyttää myös valheellisia linkkejä, jotka esitetään kiinnostavina. Linkin sisältämältä sivustolta löytyy yleensä ilmoitus, jossa pyydetään lataamaan puhelimelle sovellus, jonka kautta luvattu asia toimitetaan.

Vaikka virus ja mato käyttäytyvät samalla tavoin pyrkien keräämään ja varastamaan tietoja saastuneista laitteista on niiden toiminnassa yksi selkeä ero: Madot eivät tarvitse isäntäohjelmistoa toimiakseen vaan ne osaavat levitä laitteesta toiseen automaattisesti. Madot ovat kuitenkin nykyään vähentyneet palomuurien yleistymisen ja käyttöjärjestelmän nopeiden päivitysten seurauksena.

Myös troijalaiset ovat levinneet mobiilimaailmaan. Troijalainen on haittaohjelmista epätäsmällisin. Yleensä sitä käytetään ohjelmasta, joka viruksesta ja madosta poiketen ei levitä itseään eteenpäin. Nimitys voi tarkoittaa myös ohjelmaa, jonka hyödylliseltä näyttävän julkisivun takana on piilotettuja toimintoja. Nimitys tulee suuresta puuhevosesta, johon piiloutumalla kreikkalaiset sotilaat pääsivät Troijan muurien sisäpuolelle ja pystyivät valtaavan kaupungin. Troijalainen kykenee myös avaamaan palomuuriin aukkoja jolloin muut haittaohjelmat pääsevät sisälle laitteeseen (Järvinen 2012, 178).

3.3 Vakoiluohjelmat

Vakoiluohjelma eli urkintaohjelma, englanniksi spyware, on verkkouhkien kategoria, joka kuvaa haitallisia ohjelmia jotka on suunniteltu saastuttamaan järjestelmät ja aiheuttamaan laittomia aktiviteetteja niillä. Useimmissa tapauksissa, näiden uhkien toiminnallisuus riippuu niiden välittäjien aikomuksista: joitain vakoiluohjelmia voidaan käyttää keräämään henkilökohtaisia tietoja (kirjautumisnimet, salasanat ja muut henkilökohtaiset tiedot) ja lähettämään ne niiden omistajille takaoven välityksellä, kun taas toiset vakoiluohjelmavirukset voivat seurata uhrejaan ja kerätä tietoa heidän nettiselaamisestaan.

Vakoiluohjelmia käytetään seuraamaan ihmisiä ja heidän useimmiten vierailtuja sivuja sekä kuinka näillä sivuilla käyttäydytään. Näitä tietoja käytetään yleensä markkinoimaan ja mainostamaan eri osapuolia, joten vakoiluohjelma voi aiheuttaa sinulle myös suuren määrän roskapostia. On myös mahdollista, että vakooja seuraa käyttäjän toimia puhelimen ja mikrofonin välityksellä.

Vakoiluohjelma on nimenä hieman harhaanjohtava, sillä todellisuudessa monet ohjelmat seuraavat käyttäjän toimintaa ilman varsinaista vakoilua. Esimerkiksi Facebook ja Google keräävät käyttäjästä mielettömiä määriä tietoja seuraamalla puhelimen käyttöä ja varsin-

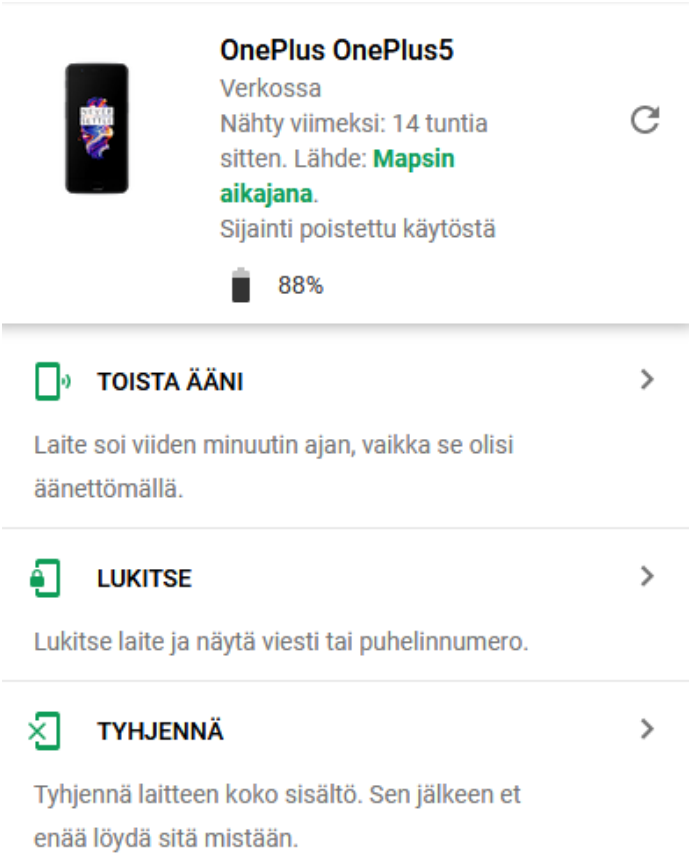
kin paikkatietoja. Sovelluskehittäjät jakavat usein tekemiään sovelluksia ilmaiseksi maksimoidakseen käyttäjämäärän. Saamalla runsaasti käyttäjiä voi kehittäjä myydä käyttäjän paikkatietoja mainostajille, jotta he voivat tarjota paikkakohtaisia mainoksia käyttäjälle.

Yksi tunnetuimmista vakoiluohjelmatyypeistä on keylogger eli näppäinnauhuri. Keylogger on tietokoneohjelma, joka kirjaa jokaisen näppäimen iskun ja tallentaa sen tiedostoon. Kun se on kerännyt tarvittavat tiedot, niin se siirtää ne internetin välityksellä ennalta määrätylle etäpalvelimelle.

Vaaralliset keyloggerit ovat aika samanlaisia kuin virukset ja troijalaiset. Hakkerit käyttävät niitä loukkaamaan käyttäjien yksityisyyttä. Lailliset keyloggerit, tunnetaan myös valvontatyökaluina, ovat kaupallisia tuotteita joita käyttävät vanhemmat, työnantajat ja opettajat. Ne kertovat mitä lapset tai työntekijät tekevät verkossa. Jopa lailliset ohjelmat toimivat ilman käyttäjän lupaa ja tietoa. Niitä voidaan käyttää myös vaarallisten henkilöiden puolesta ja sen takia niitä ei pidetä paljoakaan vaarattomampana kuin useita muitakaan loisia.

3.4 Fyysinen laite

Vaikka nykyään on kaikenlaisia haittaohjelmia, vakoiluohjelmia ja kaikenlaisia muita keinoja kerätä tietoja käyttäjästä kohdistuu suurin yksittäinen uhkakuva kuitenkin kadonneeseen laitteeseen. Tätä tapausta varten on hyvä varautua käyttämällä omassa laitteessaan tehokasta lukitusta sekä säätämällä asetukset siten, ettei ilmoitukset näy lukitusnäytössä. Mikäli puhelin kuitenkin sattuu häviämään, on Google kehittänyt siihen palvelun (kuva 9).



KUVA 9. Googlen paikanna puhelin -palvelu

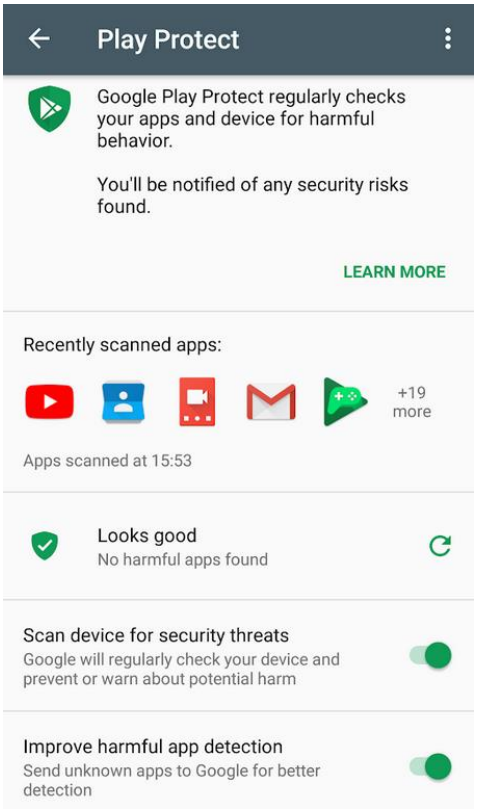
Aikaisemmin Android Device Managerina tunnettu palvelu uudistui vuonna 2017 ja uusien ominaisuuksien myötä nimettiin Paikanna puhelin -palveluksi osaksi Google Play Protect -kokonaisuutta. Tämä ominaisuus löytyy jokaisesta Android-puhelimesta, josta löytyy vähintään Android 4.4 ja johon on kirjauduttu Google-tilillä. Palvelun käyttö vaatii lisäksi, että laite on yhdistettynä internetiin. Näiden lisäksi laitteen tarkka paikannus vaatii myös GPS:n päällä olemista. Palvelu mahdollistaa paikkatietojen selaamisen lisäksi laitteeseen soittamisen, laitteen lukitsemisen sekä laitteen tietojen tyhjentämisen.

4 SUOJAUTUMINEN

Seuraavissa kappaleissa selvitetään, kuinka Android toimii aktiivisesti suojaten laitetta sekä esitellään erilaisia suojautumiskeinoja ja kuinka omat laitteet saa pidettyä turvassa haittaohjelmilta.

4.1 Google Play Protect

Vuonna 2017 esiteltiin Google Play Protect, jonka myötä sovellusten tarkkailu siirtyy käyttäjiltä enemmän koneoppivalle tekoälylle. Tämä toiminto toimii automaattisesti kaikissa laitteissa, jossa on Android 4.3 tai uudempi. Play Protect skannaa laitteen sovellukset läpi päivittäin ja käsittelee myös ne sovellukset, jotka ovat asennettu eri kauppapaikoista. Play Protect löytyy sisäänrakennettuna Play kaupasta (kuva 10).



KUVA 10. Google Play Protect

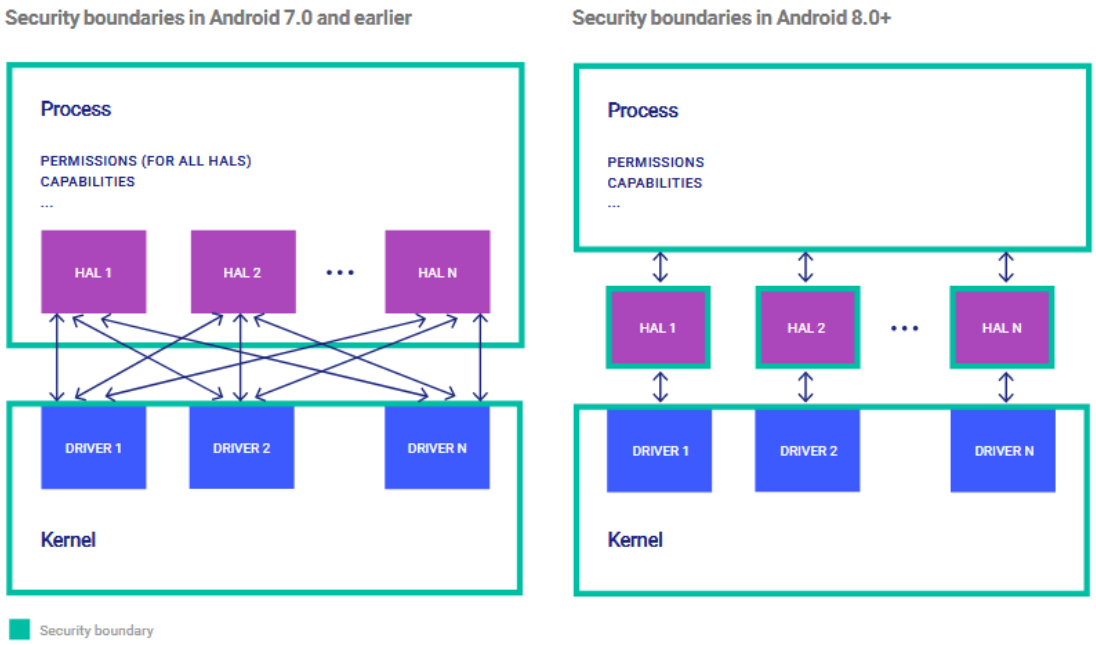
Google Play Protect -nimen lisäksi uutta on nyt mahdollisuus suorittaa skannaus myös itse haluttuna ajankohtana. Tämä onnistuu Google Play -sovelluskaupan Omat sovellukset ja pelit -osion kautta Päivitykset-välilehden ylälaidasta. Googlen mukaan Play Protect suojelee näin yli miljardia laitetta ja tarkistaa päivittäin yli 50 miljardia sovellusta. Play Protect voi varoittaa haitallisesta sovelluksesta jo ennen sen asentamista, minkä lisäksi vakavissa tilanteissa se voi jopa poistaa vaarallisia sovelluksia laitteesta.

4.2 Project Treble

Android 8.0 versiossa uutena ominaisuutena tuli Project Treble, jonka seurauksena laitteiden päivittäminen tulee yksinkertaistumaan. Treble tuo laitevalmistajille uuden rajapinnan Androidin lähdekoodin sekä piirivalmistajan toteutuksen välille. Uuden rajapinnan taustalla toimii Vendor Test Suite (VTS), joka tarkistaa toimittajan toteutuksen yhteensopivuuden.

Tämä erottaminen tekee laitteiden päivittämisestä uusille Android-versioille paljon helpompaa, koska se ei muokkaa laitevalmistajan muutoksia. Historiallisesti päivitykset olivat haastavia, kalliita ja aikaa vieviä laitevalmistajille omien käyttöjärjestelmämuokkausten vuoksi. Project Treblen myötä laitteita on helpompi päivittää, minkä pitäisi tarkoittaa nopeampia tietoturvakorjauksia ja Android-version päivityksiä.

Nopeammat ja helpommat päivitykset eivät ole Treblen ainoa turvallisuushyöty. Treblen modulaarisuus on suunniteltu parantamaan tietoturvaa muuttamalla laitteiston abstraktiokerrosten (HAL) toimintaa siten, että jokainen HAL valvoo yhtä rautatason ajuria (kuva 11).



KUVA 11. Uudistunut prosessihallinta Android Oreossa. (Google)

Eristetyt HAL:t noudattavat vähemmän etuoikeuden periaatetta ja tarjoavat kaksi erillistä etua. Jokainen HAL toimii omassa ympäristössään ja se voi valvoa vain omaa laitteistoajuriaan ja pääsee käsiksi vain niihin oikeuksiin, joita tehtävässä tarvitaan. Näin ollen jokainen HAL tekee oman työnsä eikä sotkeudu muihin ajureihin. Tämä auttaa prosesseja toimimaan nopeammin sekä turvallisemmin.

4.3 Antivirussovellukset

Paras ja luotettavin tapa suojautua haittaohjelmilta on ladata luotettava antivirusohjelma toimimaan taustasovelluksena. Tunnettuja sovelluksia ovat muun muassa Avira Antivirus Security, Norton Security and Antivirus, Bitdefender Antivirus Free, Avast Mobile Security sekä suomalaisen F-Securen Mobile Security. Näiden aktiivisesti puhelinta seuraavien ohjelmien lisäksi on olemassa erilaisia haittaohjelmaskannereita kuten esimerkiksi Malwarebytes Security.

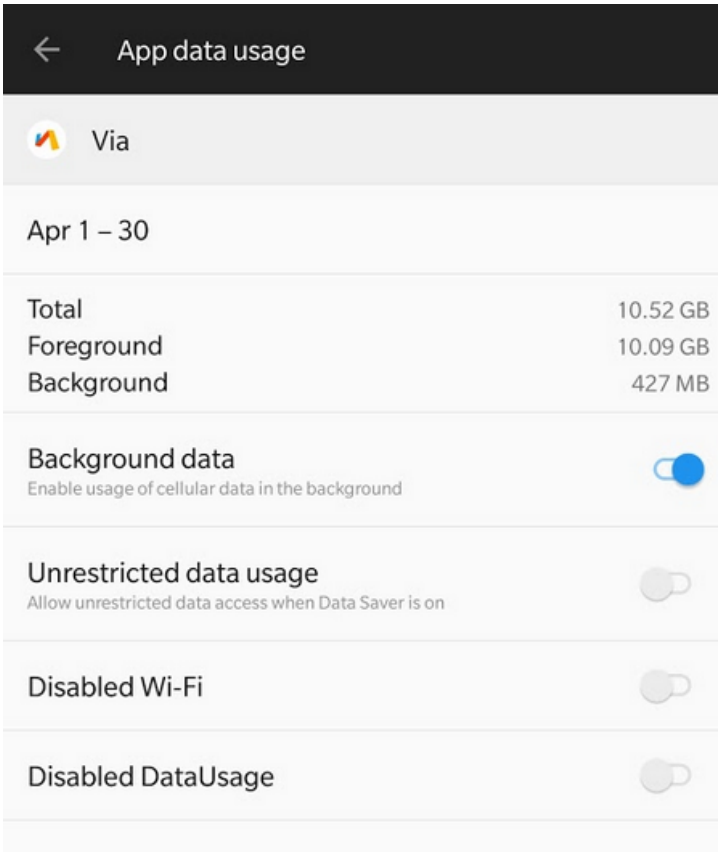
Virustorjuntaohjelmistoilla on kaksi perustilaa: staattinen tiedostojen tarkastustila sekä dynaaminen reaaliaikainen tila. Reaaliaikaisessa tilassa ohjelmisto tarkistaa uudet tiedostot ennen kuin käyttäjä avaa ne ja ehkäisee siten muiden tiedostojen saastumisen. Staattisessa tilassa käyttäjä voi puolestaan suorittaa muistin tarkistuksen tai valita tietyt kansiot/tiedostot tarkasteltavaksi. Kuukausittain ilmestyy jopa satoja uusia haittaohjelmia, ja siksi virustorjuntaohjelmistojen tietokantojen säännöllinen päivittäminen on tärkeää.

4.4 Palomuuri

Palomuuri on järjestelmä, joka toteutetaan joko ohjelmisto- tai laitteistopohjaisesti. Se valvoo verkkojen välillä kulkevaa tietoliikennettä ja suojaa tietokonetta ulkopuolelta tulevilta hyökkäyksiltä. Perusedellytyksenä on, että kaikki verkkoliikenne kulkee palomuurin läpi ja että ainoastaan haluttu verkkoliikenne päästetään läpi. Palomuuri estää lisäksi palveluihin kohdistuvat hyökkäykset sekä erilaisia reititys- ja lähdeosoitteen väärennykseen perustuvia hyökkäystapoja.

Hyvin konfiguroitu palomuuri suodattaa kaiken verkkoliikenteen ja oletusarvoisesti kieltää kaiken liikenteen. Suodatussäännöillä määritellään erikseen, mikä liikenne sallitaan ja mikä ei. Suodatussäännöt toimivat täten poikkeuksina oletussääntöön, jossa kaikki kielletään. Mikäli kaiken kieltävää oletussääntöä ei olisi, toimisi palomuuri ennemminkin reitittimen tavoin ja sallisi tällöin kaiken liikenteen. (Viljanen, 2018)

Vaikka palomuurit liitetään usein tietokoneverkkoihin, myös mobiililaitteeseen voi palomuurin asentaa. Androidissa on 7.0 päivityksen jälkeen myös sovelluskohtainen asetus, jonka avulla voi tietyn sovelluksen pääsyn internetiin estää silloin kun sovellus ei ole päällimmäisenä auki eli niin sanotusti tämä valinta estää taustaprosessien pääsyn internetiin.



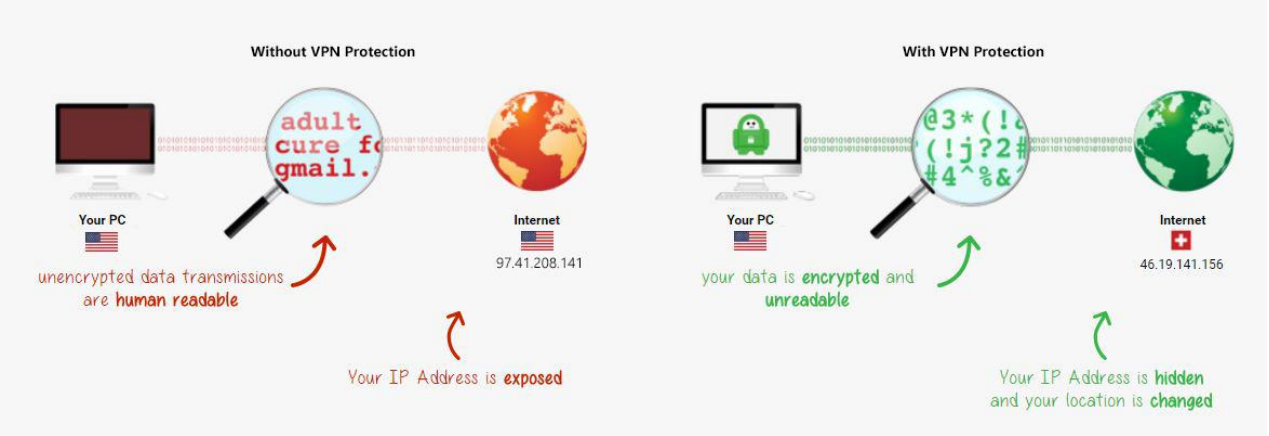
KUVA 12. Sovelluksen datan käyttö

Kuvassa 12 näkyy Via browser nimisen selaimen datan käyttö kuukauden ajalta. Tutkimuksen aikana taustadatan käyttö sallittiin ja huomattiin että kuukauden mittaisen tutkimusjakson aikana taustadataa kului 427 megatavua joka vastaa noin neljää prosenttia koko sovelluksen datankäytöstä. Tästä voidaan päätellä, että Via browserin prosessit eivät jää taustalle pyörimään pitkäksi aikaa vaan sammuu kun sovellus poistuu etualalta.

Jos taustaprosessien datan sulkeminen ei riitä, voi puhelimeen ladata erillisen palomuurisovelluksen, joka estää kokonaan valittujen sovellusten pääsyn internetiin. Näitä sovelluksia ovat muun muassa NoRoot Firewall, NetGuard sekä NetPatch Firewall.

4.5 VPN

Lyhenne VPN tulee sanoista Virtual Private Network. Suomeksi VPN käännetään virtuaaliseksi erillisverkoksi. VPN salaa dataliikenteesi tunnelointiprotokollaa hyödyntäen. Näitä tunnelointiprotokollia ovat muun muassa IPsec, L2TP, L2F sekä PPTP. Tietoliikenteesi kulkee putkessa suojatulle palvelimelle ja vasta sitten sivustolle tai sovellukseen, jonne olet menossa. Näin VPN hämärtää laitteesi fyysisen sijainnin. VPN-palvelin voi toki sijaita missä päin maailmaa tahansa (kuva 13).



KUVA 13. VPN:n hyödyt (Pinellas Computers)

Avoimet verkot ovat lähtökohtaisesti turvattomia. Myös salasanalla varustettu WLAN voi olla suojaton – esimerkiksi silloin, jos salasanaa jaellaan kaikille, vaikka kuppilan seinällä tai hotellin vastaanotossa. VPN:ää käytetäänkin yhä enemmän tiedonkeruulta suojautumiseen avoimissa verkoissa niin kotimaassa kuin reissussakin.

VPN:ää käyttäessäsi laitteesi näyttää sijaitsevan siellä, missä valitsemasi VPN-palvelin sijaitsee. Siksi oman maan nettisensuuria kiertävät ja laitonta sisältöä lataavat käyttävät VPN:ää. Lisäksi VPN auttaa suojautumaan mainostajia vastaan. Kun VPN on käytössä, mainostaja ei löydä käyttäjää yhtä helposti ja mainosten määrä vähenee. Matkustaessa nettiyhteyksiä sensuroivaan maahan, kuten Kiinaan tai Venäjälle, asentamalla VPN:n on mahdollista päästä selaamaan kotimaasi sivustoja ja käyttämään sosiaalista mediaa kuten normaalistikin.

VPN tunnetaan parhaiten maaestojen kiertämisestä. Aikaisemmin suoratoistopalvelu Netflixissä muiden maiden tarjontaan pääsi käsiksi valitsemalla VPN-palvelimen kyseisestä maasta. Nykyään monet sivustot rajoittavat tai estävät kävijöitä harhauttamasta maarajoituksia VPN:n avulla. Lisäksi maantieteellisten rajoitusten eli niin sanotun geoblokkauksen kiertäminen on esimerkiksi Netflixillä käyttöehtojen vastaista. (Solla, 2017)

4.6 Maalaisjärki

Vaikka tässä työssä on tullut esille monia erilaisia mahdollisia haittaohjelmia, sellaisen päätyminen omaan laitteeseesi on erittäin epätodennäköistä, jos pidät laitteesi ja sovelluksesi päivitettynä sekä käytät vain Googlen sovelluskauppaa. Googlen tilastojen mukaan haitallisen ohjelman lataamiseen Play kaupasta on 2 promillen mahdollisuus.

Hyvä keino suojautua uhkia vastaan on siis pitää huolta omista laitteistaan. Vaikka haittaohjelmat kehittyvät koko ajan ja uusia uhkia ilmenee, suurin uhka on silti fyysisesti kadonnut laite. Suojaamaton laite on unelmakohde datarosvolle. Pidämme laitteissamme useita eri sähköposteja, mukaan lukien työsähköpostit, sosiaalisen median käyttötilejä, pankkisovelluksia sekä muita arkaluontoista dataa sisältäviä sovelluksia. Jos laitetta ei ole suojattu, ulkopuolinen pääsee heti käsiksi tileihisi. Nykypäivänä monista laitteista löytyy biometrinen tunniste, kuten sormenjäljen lukija tai iirisskanneri. Jo pelkästään tätä käyttämällä hyökkääjä ei pääse suoraan laitteen tietoihin käsiksi.

Android on myös sisältänyt mahdollisuuden salata laitteen tiedot versiosta 2.3 lähtien. Tällöin laitteen dataan ei pääse suoraan käsiksi tietokoneeseen yhdistämällä, vaikka laite olisi sammutettuna. Versiosta 7.0 ylöspäin Android myös mahdollistanut tiedostokohtaisen salauksen.

Tärkeää on myös muistaa internetissä järjen käyttö; jos jokin asia vaikuttaa liian hyvältä, se on todennäköisesti huijausta. Soittamalla annettuun epäilyttävän näköiseen puhelinnumeroon et tule saamaan uusinta älypuhelinta tai lomamatkaa muutamalla eurolla. Myöskään asentamalla pop-up ikkunassa mainostettua sovellusta ei sinusta tule miljonääriä.

5 LAITTEEN END-OF-LIFE

Älypuhelimemme ovat tietoisia elämämme tärkeimmistä salaisuuksista. Sähköpostit, taloudelliset tiedot, yhteystiedot ja ehkä jopa riskialttiit valokuvat eivät ole sitä, mitä haluamme joutuvan vääriin käsiin. Tietoturvayhtiö Avast teki testin, jossa ostettiin 20 käytettyä Android-älypuhelinta ja testattiin, onko tietojen palauttaminen niistä mahdollista. Avastin työntekijät onnistuivat tunnistamaan neljää vanhaa omistajaa, jonka lisäksi laitteista saatiin palautettua tuhansia valokuvia, satoja sähköposteja, tekstiviestejä sekä yhteystietoja. (Pelegrin, 2014)

Mikään laite ei kestä ikuisesti ja jossain vaiheessa tulee vastaan tilanne, jolloin uusi laite korvaa vanhan ja vanhasta pitäisi päästä eroon. Seuraavissa kappaleissa käsitellään, kuinka vanha laite saadaan poistettua käytöstä, sitten ettei laitteen sisältämään dataan päästä enää jälkikäteen käsiksi.

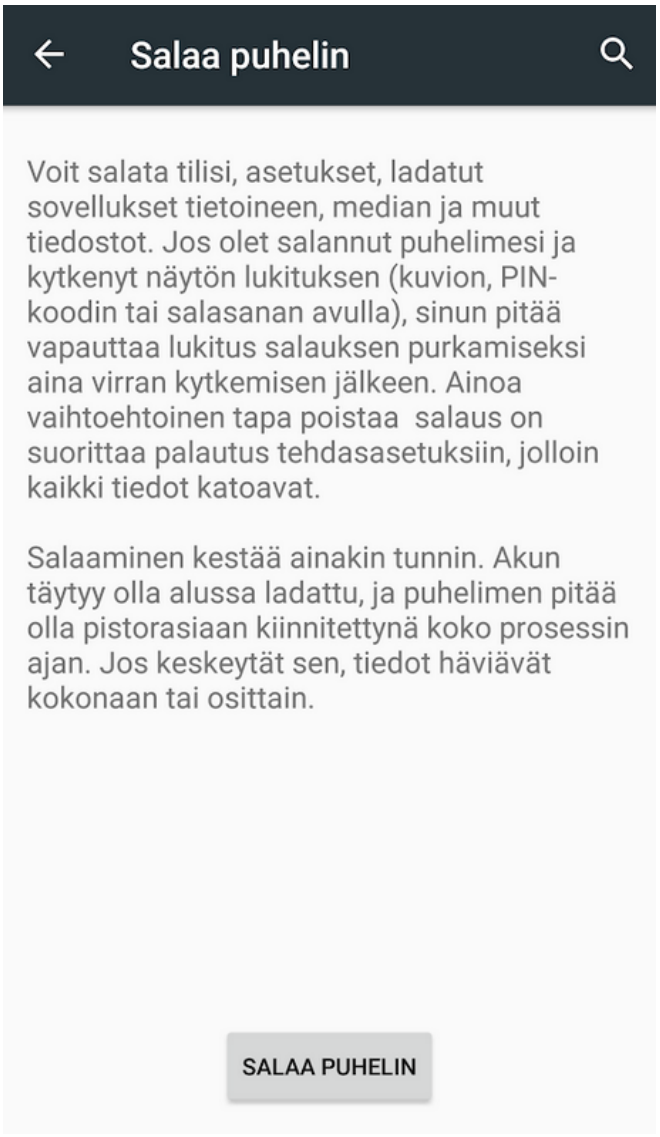
5.1 Tehdasasetusten palautus

Ensimmäinen askel laitteen tyhjentämiseen on ottaa mahdolliset turvalukitukset pois käytöstä, sillä nämä eivät häviä tehdasasetusten palautusta tehdessä. Lisäksi on järkevää poistaa Google-tili puhelimesta, sillä nollauksen jälkeen laite pyytää kirjautumaan aikaisemmin kirjautuneella olleella käyttäjätilillä ja ellei näitä kirjautustietoja ole olemassa, laite pysyy lukittuna. Lisäksi Samsungin laitteilla tulee poistaa laitteessa käytetty Samsung-tili.

Kun Android-laitteeseen palautetaan tehdasasetukset sen pitäisi pyyhkiä puhelimen sisältämän datan puhtaaksi, mutta se ei sitä tee. Se poistaa kaikki tiedot näkyvistä, mutta se ei oikeastaan korvaa niitä. Tällöin on mahdollista, että datan pystyy palauttamaan kolmannen osapuolen palautusohjelmistoja hyödyntäen. (Hill, 2017)

5.2 Tiedostojen uudelleenkirjoittaminen

Jotta voidaan olla varma, ettei puhelimen tietoja saada palautettua voidaan puhelimen tiedot salata ennen tehdasasetusten palauttamista. Android-puhelimet joissa on tehtaalta tullessa ollut Android 6.0 tai uudempi, pitäisi tämä olla jo tehty tehtaalla. Tämä onnistuu menemällä puhelimen asetuksiin ja valitsemalla sieltä suojausvälilehden alta salaa puhelin (kuva 14).



KUVA 14. Android-puhelimen salaaminen

Tiedot salattua voi puhelimen tehdasasetukset palauttaa ja laittaa laitteen kiertoon. Toki jos haluaa olla aivan varma, ettei kukaan pääse vanhaan dataan käsiksi, olisi hyvä uudelleenkirjoittaa data esimerkiksi Play kaupasta löytyvällä Secure Eraser -ohjelmalla. Ohjelmalla on kolme eri toimintaperiaatetta uudelleenkirjoittamisen suhteen. Olemassa oleva data voidaan korvata joko satunnaisilla merkeillä, 0-täytöllä tai F-täytöllä. Täytöt tarkoittavat, että olemassa oleva bittijono korvataan joko 0 tai F bitillä. Tämän toimenpiteen jälkeen vanhan datan palautamminen pitäisi olla mahdotonta.

6 POHDINTA

Langattomien laitteiden yleistyminen on avannut uusia tietoturvauhkia, sillä langattomissa laitteissa on ikävä kyllä paljon enemmän tietoturvariskejä kuin perinteisissä samaan paikkaan sidotuissa laitteissa. On tärkeää ohjeistaa ihmisiä mobiililaitteiden turvalliseen käyttöön.

Opinnäytetyön tavoitteena oli saada lisää tietoa Android-järjestelmästä, niiden tietoturvasta sekä vahvistaa aiempaa tietämystä. Tässä työssä halusin koota paketin, jonka lukemalla saa selville mitä heikko tietoturva voi tuottaa.

Tietoturva on todella laaja ja mielenkiintoinen osa-alue tietotekniikkaa. TAMK:ssa opintosuunnitelmaan kuului yksi tietoturvakurssi, josta kipinä aiheeseen syntyi. Tämän seurauksena suoritin myös Metropolia Ammattikorkeakoulun tarjoaman verkkokurssin kyberturvallisuuteen liittyen.

Opinnäytetyöstä käy ilmi, kuinka suuria vahinkoja huono tietoturva voi pahimmillaan aiheuttaa ja kuinka pienillä muutoksilla nämä vahingot voidaan estää. Tämän työn tekemisen aikana minulle tuli myös selväksi, että tahdon työskennellä tulevaisuudessa tietoturvan parissa ja seurata aihetta aktiivisesti.

LÄHTEET

Sawers, P. 2015.. Android fragmentation report: There are now 24,093 distinct devices, up 28% from last year. Luettu 30.3.2018. https://venturebeat.com/2015/08/05/fragmentation-report-there-are-now-24093-distinct-android-devices-up-78-from-last-year/

Statcounter. 2018. Operating System Market Share Worldwide. Luettu 4.5.2018. http://gs.statcounter.com/os-market-share

Android Developer. 2018. Google. Dashboards. Luettu 24.3.2018. https://developer.android.com/about/dashboards/index.html

Think With Google. 2016. Google/Ipsos. Luettu 27.4.2018. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjg5_SypdraAhVkOpoKHR_qAs4QFggmMAA&url=https%3A%2F%2Fwww.thinkwithgoogle.com%2F_qs%2Fdocuments%2F331%2Fhow-users-discover-use-apps-google-research.pdf&usg=AOvVaw3BDzPn8x9OXl9L_9lAp8zw

Perez, S. 2017. Report: Smartphone owners are using 9 apps per, 30 per month. Luettu 27.4.2018. https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/

Perez, S. 2015. Consumers Spend 85% Of Time On Smartphones In Apps, But Only 5 Apps See Heavy Use. Luettu 27.4.2018. https://beta.techcrunch.com/2015/06/22/consumers-spend-85-of-time-on-smartphones-in-apps-but-only-5-apps-see-heavy-use/?_ga=2.104543304.9115928.1524743128-444196237.1522151343

AppBrain. 2018. Number of Android Applications. Luettu 25.4.2018. https://www.appbrain.com/stats/number-of-android-apps

D'Onfro, J. 2018. Google is missing out on billions of dollars by not having an app store in China, new data shows. Google is missing out on billions of dollars by not having an app store in China, new data shows. Luettu 15.4.2018. https://www.cnbc.com/2018/01/17/google-misses-out-on-billions-in-china.html

Gibbs, S. 2018. Android phone makers skip Google security updates without telling users – study. Luettu 26.4.2018. https://www.theguardian.com/technology/2018/apr/13/android-phone-makers-skip-security-updates-users-smartphone-software-google

Škvor, M. 2018. Keeping your Android safe this year. Luettu 11.4.2018. https://blog.avast.com/keeping-your-android-safe-this-year

Goodin, D. 2016. Active drive-by exploits critical Android bugs, care of Hacking Team. Luettu 25.4.2018. https://arstechnica.com/information-technology/2016/04/active-drive-by-attacks-exploit-critical-android-bugs-care-of-hacking-team/

Hyppönen, M. 2017. EU:n tietosuoja-asetus ja sen vaikutukset - Mikko Hyppönen (F-secure) - #TietoturvallinenSuomi. YouTube-video. Julkaistu 17.5.2017. https://www.youtube.com/watch?v=XiMVzR7byFg

Järvinen, P. 2012. Arjen tietoturva – vinkit ja ratkaisut. 1. painos. Jyväskylä: Docendo.

Viljanen, V. 2018. Virusturva ja palomuuri. Luettu 29.4.2018. https://www.yksityisyydensuoja.fi/virusturva-ja-palomuuri

Solla, K. 2017. Digitreenit: Mikä ihmeen vpn? Se suojaa nettiyhteyttäsi avoimessa verkossa. Luettu 27.4.2018. https://yle.fi/aihe/artikkeli/2017/09/06/digitreenit-mika-ihmeen-vpn-se-suojaa-nettiyhteyttasi-avoimessa-verkossa

Pinellas Computers. 2017. ISP's Collecting and Selling Your Data: Protect Your Privacy with a VPN. Luettu 27.4.2018. https://www.pinellascomputers.com/blog-news/isps-collecting-and-selling-your-data-protect-your-privacy-with-a-vpn/

Android. 2018. Android Security 2017 Year In Review. Luettu 29.4.2018. https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Android. 2017. Encryption. Luettu 29.4.2018. https://source.android.com/security/encryption/

Hill, S. 2017. Selling your phone or tablet? Here's how to wipe your Android phone. Luettu 4.5.2018. https://www.digitaltrends.com/mobile/how-to-wipe-your-android-phone-or-tablet/

Pelegrin, W. 2014. Warning: Factory resetting your Android phone may not delete everything. Luettu 4.5.2018. https://www.digitaltrends.com/mobile/android-factory-reset-broken-avast/

LIITTEET

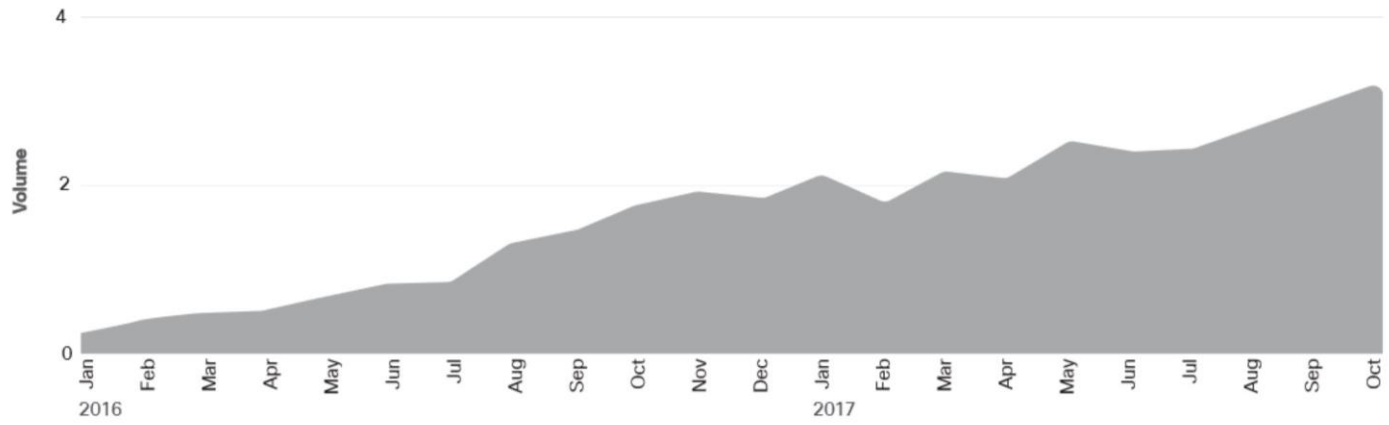
Liite 1. Ciscon tietoturvaraportin 2018 päätelmät

Conclusion

In the modern threat landscape, adversaries are adept at evading detection. They have more effective tools, like encryption, and more advanced and clever tactics, such as the abuse of legitimate Internet services, to conceal their activity and undermine traditional security technologies. And they are constantly evolving their tactics to keep their malware fresh and effective. Even threats known to the security community can take a long time to identify.

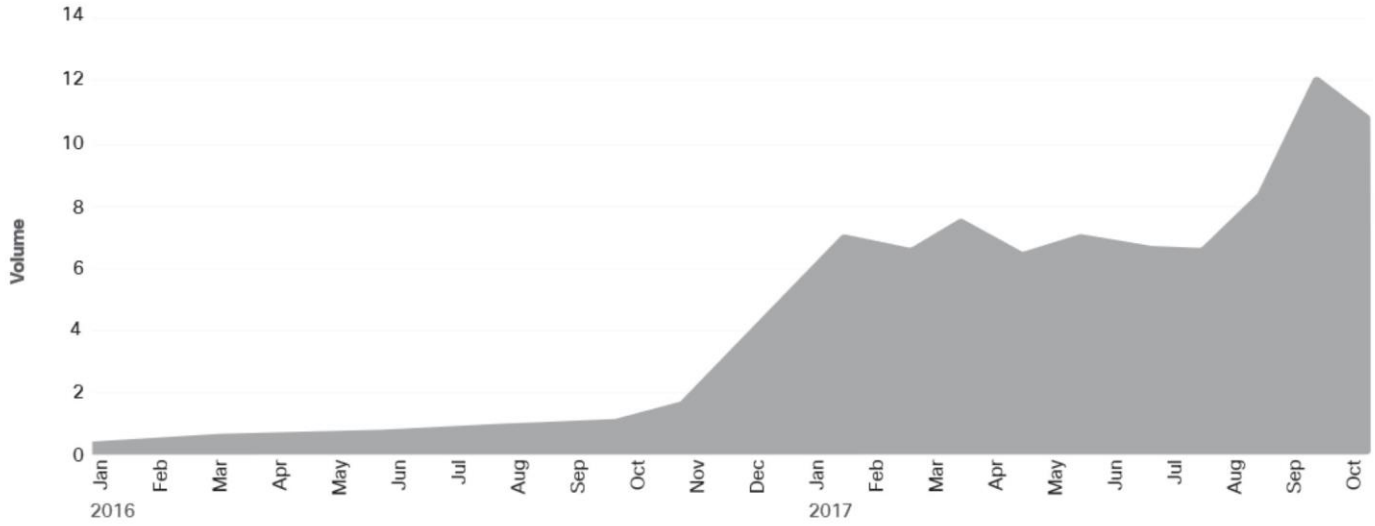
One reason defenders struggle to rise above the chaos of war with attackers, and truly see and understand what's happening in the threat landscape, is the sheer volume of potentially malicious traffic they face. Our research shows that the volume of total events seen by Cisco cloud-based endpoint security products increased fourfold from January 2016 through October 2017 (see Figure 58). "Total events" is the count of all events, benign or malicious, seen by our cloud-based endpoint security products during the period observed.

Figure 58 Total volume of events



Source: Cisco Security Research

Figure 59 Overall malware volume



Source: Cisco Security Research

Our security products also saw an elevenfold increase in overall malware volume during that same period, as Figure 59 shows.

Trends in malware volume have an impact on defenders' time to detection (TTD), which is an important metric for any organization to understand how well its security defenses are performing under pressure from the constant barrage of malware deployed by adversaries.

The Cisco median TTD of about 4.6 hours for the period from November 2016 to October 2017 helps to illustrate the ongoing challenge of identifying threats quickly in the chaotic threat landscape. Still, that figure is well below the 39-hour median TTD we reported in November 2015, after we first began tracking TTD, and the 14-hour median reported in the *Cisco 2017 Annual Cybersecurity Report* for the period from November 2015 to October 2016.[20]

The use of cloud-based security technology has been a key factor in helping Cisco to drive and keep its median TTD at a low level. The cloud helps to scale and maintain performance as both the volume of total events and malware targeting endpoints continues to increase. On-premises security solutions would struggle to offer the same flexibility. Designing one to scale that could handle more than 10 times the volume capacity of malicious events over a two-year period—and maintain or increase response times—would be a very difficult and costly undertaking for any organization.

Cisco defines "time to detection," or TTD, as the window of time between a compromise and the identification of a threat. We determine this time window using opt-in security telemetry gathered from Cisco security products deployed around the globe. Using our global visibility and a continuous analytics model, we are able to measure from the moment a malicious file is downloaded on an endpoint to the time it is determined to be a threat that was unclassified at the time of encounter.

"Median TTD" is the average of the monthly medians for the period observed.

20 *Cisco 2017 Annual Cybersecurity Report:* cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.