KARELIA-AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

Jonne Mikael Jalonen

RANSOMWARELTA SUOJAUTUMINEN

Opinnäytetyö
Toukokuu 2017

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Toukokuu 2017** **Tietojenkäsittelyn koulutusohjelma** Karjalankatu 3 80220 JOENSUU (013) 260 600

Tekijä(t)
Jonne Mikael Jalonen

Nimeke
Ransomwarelta suojautuminen

Toimeksiantaja
Karelia-ammattikorkeakoulu

Tiivistelmä

Tämän opinnäytetyön aiheena on ransomwarelta suojautuminen. Toimeksiantajana on Karelia-ammattikorkeakoulu, joka halusi ohjeistusta ransomware-infektion varalle. Tavoitteena on antaa käyttökelpoisia ohjeita ransomwarelta suojautumiseen sekä selvittää, mitä varotoimia infektion varalle voi tehdä. Työssä käydään myös läpi erilaisia haittaohjelmia sekä muita hyökkäysmenetelmiä, jotka voivat aiheuttaa vaaraa verkossa liikuttaessa.

Työn pääpaino on ransomware-haittaohjelmissa, jotka pystyvät salaamaan infektoituneen tietokoneen tiedostot. Työssä käydään läpi, kuinka infektio saa alkunsa ja mitä infektion jälkeen tapahtuu. Toiminnallisessa osuudessa on pystytetty testiympäristö Virtual box -virtualisointiympäristöön, johon on asennettu Windows XP. Ympäristö infektoidaan ransomwarella, ja tällä pyritään havainnoimaan infektion etenemistä.

Opinnäytetyön lopputuloksena on kokoava paketti tietoa haittaohjelmista, erityisesti ransomwaresta.

Kieli suomi	Sivuja 30

Asiasanat

tietomurto, tietotekniikka, suojaus, työasema, tietokone, data, virus, ransomware, tietojenkäsittely, tietoturva

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2017
Degree programme in Business Information Technology

Karjalankatu 3
80220 JOENSUU
FINLAND
(013) 260 600

Author (s)
Jonne Mikael Jalonen

Title
Preventing Ransomware Infection

Commissioned by
Karelia University of Applied Sciences

Abstract

The subject of this thesis is defending against ransomware. This thesis is commissioned by Karelia University of Applied Sciences, who wanted instructions in case of a ransomware infection. The aim is to give useable instructions on defending against a ransomware infection and what to do in case of an infection. Thesis examines different kinds of malware and other ways of attacks one might come across on the internet.

The main focus of this thesis is ransomware, which can encrypt the files on the user's computer. We go through how the infection happens and what happens after it. In the practice-based part of this thesis we will infect a test environment composed of Virtual box and Windows XP. The aim is to show what happens in a ransomware infection.

The end product of this thesis is a tight information package about malware, especially about ransomware.

Language
Finnish

Pages 30

Keywords
It, safety, computers, malware, data, virus, ransomware, protection

Sisältö

1 Johdanto

Tämä opinnäytetyö keskittyy lunnashaittaohjelmiin, eritoten tiedostoja salaaviin ohjelmiin. Raportissa tarkastellaan myös muita haittaohjelmia ja käsitellään maailmalla tapahtuneita tietomurtoja. Aihe on varsin ajankohtainen, sillä tiedostoja salaavat lunnashaittaohjelmat, ransomwaret, tuntuvat nouseen otsikoihin viime vuosien ajan, ja niillä on erittäin suuri vaikutus varsinkin yrityksiin. joilla ei ole tarpeellisia varotoimia mahdollisen infektion varalle.

Työn tavoitteena on selvittää, kuinka ransomware toimii ja kuinka suojatutua siltä. Aihe syntyi omasta mielenkiinnosta aihealuetta kohtaan. Viimeaikaisten roskapostiongelmien seurauksena Karelia-ammattikorkeakoulu ryhtyi toimeksiantajaksi ja he halusivat ohjeistusta lunnashaittaohjelmien varalle. Tutkimusmenetelmänä tässä työssä on käytetty monimuotoista tutkimusmenetelmää – yhdistelmä toiminnallista ja teoreettista tutkimusta. Toiminnallisessa osuudessa infektoidaan virtuaalitietokone ransomwarella.

Tietomurtoja, joihin myös ransomware kuuluu, käsitellään toisessa luvussa. Siinä käydäänläpi muutamia isohkoja tietomurtoja, joita on vuosien saatossa tapahtunut, mitä eri haittaohjelmia on olemassa sekä muutamia esimerkkejä muista menetelmistä, miten tietomurto toteutetaan. Tässä luvussa käydään myös läpi, kuinka tietomurrosta saatuja tietoja voidaan mahdollisesti hyväksi-käyttää ja mitä rikosnimikkeitä tietomurrosta voidaan saada.

Ransomwarea käsitellään kolmannessa luvussa. Tässä kerrotaan, kuinka ransomware toimii yleisellä tasolla, kuinka mahdollinen infektio voidaan havaita, mitä mahdollisia suojautumiskeinoja on sekä kuinka turvata omat tiedostot mahdollista infektiota varten. Ennaltaehkäisy sekä vahinkojen minimointi -alaluvussa on listaus hyvistä toimintatavoista myös nopeaa lukua varten.

Neljäs luku on omistettu tutkimuksen toteutuksen kuvaukseen. Tässä luvussa kerrotaan tämän opinnäytetyön tutkimusongelma sekä käytetty

tutkimusmenetelmä. Lisäksi esitellään muutaman aiemman opinnäytetyön tuloksia tältä samalta aihealueelta.

Viidennessä luvussa selostetaan opinnäytetyön toiminnallisen osuuden toteutus ja esitellään erään ransomwaren infektio. Luvussa kerrotaan, mitä käyttäjä näkee, kun infektio on koneella, toisin sanoen, kuinka infektio etenee. Testi on tehty virtuaalitietokoneella, jotta omat tiedostoni eivät olisi vaarassa.

Viimeisessä luvussa on yhteenveto ja siinä arvioidaan opinnäytetyön toteutusprosessia ja lunnashaittaohjelmien tulevaisuutta.

2 Tietomurrot

Tässä luvussa tarkastellaan tietomurtoja nykypäivän perspektiivistä, mitkä ovat viimeisimmät suuret tietomurrot ja kuinka ne ovat vaikuttaneet murtojen kohteena olleisiin. Luvussa käydään lisäksi läpi, mitä monia tapoja on murtautua työasemalle sekä saastuttaa se erilaisilla haittaohjelmilla ja miten tietomurrosta pyritään hyötymään. Tietomurtoa tarkastellaan myös rikosprosessin näkökulmasta, mitä vastuita asianosaisilla on ja mitä mahdollisia rangaistuksia tekijä voi teostaan saada.

2.1 Tietomurrot nykypäivänä

Voi olla yllättävää joillekin kuulla tietomurtoja tai niihin verrattavissa olevia asioita tapahtuneen jo 1900-luvun alussa. Esimerkiksi vuonna 1903 pitkän kantaman lennättimen esittelytilaisuudessa ulkopuolinen pääsi lähettämään omia viestejä kyseisen lennättimen taajudella yleisölle. (Newscientist 2011.) Ei tule myöskään unohtaa toisen maailmansodan aikaisia koodinpurkuja, kuten saksalaisten Enigma-salauslaitteen koodin purkamista.

Nykyään työasemiin ja palvelimiin kohdistuvia hyökkäyksiä tapahtuu tietoverkkojen globaalista luonteesta johtuen kellon ympäri ympäri maailmaa, mikä myös hankaloittaa tekijöiden kiinnisaamista. Esimerkiksi palvelunestohyökkäyksiä tapahtuu päivittäin yli kaksi tuhatta ja hyökkäys voi kohdistua Kiinasta Englannissa sijaitseville palvelimille. (Digitalattackmap 2016.)

Vuosien saatossa on tapahtunut paljon isoja tietomurtoja, joissa on joutunut jopa useiden satojen miljoonien ihmisten ja yritysten tietoja vääriin käsiin. (Information is beautiful 2016.)

JPMorgan Chase

JPMorgan Chase -pankin tietoverkkoon tunkeutui ulkomaalaisia hakkereita kesäkuussa 2014. Aluksi vaikutti siltä, että hakkerit olivat saaneet käsiinsä listan pankin käyttämistä ohjelmistoista, etsineet niiden haavoittuvaisuudet ja niiden avulla päässeet tunkeutumaan sen verkkoon. (Goldstein, Perloth & Silver-Greenberg 2014.)

New York Timesin (Corkery, Goldstein & Perloth & 2014.) myöhemmän artikkelin mukaan murto kuitenkin tapahtui paljon yksinkertaisempaa reittiä pitkin. Hakkerit olivat saaneet erään työntekijän käyttäjätunnukset tietoonsa ja pankilla oli vielä yksi palvelin, jota ei ollut päivitetty käyttämään kaksivaiheista tunnistautumista, minkä takia hakkerit pääsivät palvelimen sisään. Hakkereilla oli siis suora pääsy palvelimen tiedostoihin ja he saivatkin sieltä reilustia tietoja varastettua. Hakkerit varastivat yhteensä 83 miljoonan asiakkaan tietoja, joihin kuului henkilöasiakkaiden lisäksi myös pienyrityksiä. Murrossa vuoti pankkitunnusten nimiä, osoitteita, puhelinnumeroita ja sähköpostiosoitteita. Mitään henkilötunnuksia tai salasanoja väärin käsiin ei kuitenkaan joutunut.

Sony Playstation Network

Playstation Network- ja Qriocity-palveluiden palvelimille hyökättiin19.4.2016. Murrossa varastettiin 77 miljoonan käyttäjän tietoja. Palvelimet olivat alhaalla

kolmen viikon ajan, jonka aikana Sonyn pelikonsoleiden verkko-ominaisuuksia ei voinut käyttää. Katkon aikainen tiedotus aiheutti käyttäjille suuttumusta. (Phillips 2016.)

Palveluiden käyttäjät olivat ensimmäisen viikon ajan epätietoisia siitä, mitä oikeasti oli tapahtunut, sillä Sony ilmoitti vasta 26.4 käyttäjien yksityistietojen joutuneen vaaraan. Nämä yksityistiedot sisälsivät muun muassa nimiä, sähköpostiosoitteita, salasanoja sekä käyttäjätunnuksia ja syntymäaikoja, eikä Sony ollut vielä varma olivatko käyttäjien luottokorttitiedot myös vuotaneet. (Phillips 2016.)

Sony ei ole paljastanut, kuinka hyökkäys toteutettiin, mutta on puhuttu Sonyn silloisen tietoturvajärjestelmien olleen vanhentuneita ja niiden mahdollistaneet hyökkäyksen. (Phillips 2016.)

Ulkoministeriö

Vuonna 2013 paljastui jo useamman vuoden aikana tapahtunut tietomurto ulkoministeriön verkosta. Puolustusvoimien Viestikoelaitos sai vihjeen Ruotsin signaalitiedustelulaitokselta mahdollisesta tietomurtoepäilystä ja asiaa selvitettiin kolme kuukautta ennen kuin asiaan saatiin varmuus. (Huhtanen 2014.)

Haittaohjelmana toimi kehittynyt vakoiluohjelma Uroburos, joka on tehokas jälkien peittämisessä. Ohjelmisto oli kytkeytynyt ulkoministeriön julkiseen verkkoon ja vienyt alimman turvaluokituksen viranomaistietoja, joita pystyi tietojen suuren määrän ansioista käyttämään tiedonlouhintaan. Samaa haittaohjelmaa on käytetty myös usean muun maan vakoiluun. (Huhtanen 2014.)

Yahoo, 2014

Syyskuussa 2016 paljastui yksi isoimmista tapahtuneista tietovuodoista, kun Yahoo ilmoitti, että 2014 vuonna ainakin 500 miljoonan käyttäjän tiedot olivat

joutuneet hakkereiden käsiin. Tiedot sisälsivät muun muassa nimiä, sähköpostiosoitteita, syntymäaikoja, tiivistettyjä salasanoja, kryptattuja ja kryptaamattomia turvakysymyksiä ja niiden vastauksia. Yahoo sanoo hakkereiden olleen valtion sponsoroimia. (Leswing 2016.)

2.2 Haittaohjelmat

Haittaohjelmia on monenlaisia, mutta yhteistä niille on, että ne tunkeutuvat käyttäjän tietokoneelle ilman lupaa ja useimmiten ne myös pyrkivät toimimaan salaa. Haittaohjelmat on voitu tehdä ilman mitään sen kummempaa tarkoitusta kuin mielipahan aiheuttaminen, mutta rikolliset voivat hyödyntää haittaohjelmia esimerkiksi urkkimiseen tai kiristämiseen.

Alla on listattuna erilaisia haittaohjelmatyyppejä, joita on monia erilaisia.

Virukset

Virukset ovat ohjelmistossa piilossa olevia haitallisia koodinpätkiä, jotka aktivoituvat, kun niiden isäntäohjelmaa suoritetaan. Useimmiten virukset pyrkivät aiheuttamaan suoraa vahinkoa käyttäjälle, joko poistamalla tiedostoja koneelta tai muuttamalla niiden toiminnallisuutta monistaen samalla infektoitunutta ohjelmaa. (Krutz & Vines 2008, 483.)

Symantec (2015) sanoo viruksen olevan pieni ohjelma, joka muuttaa tietokoneen toimintoja ilman käyttäjän tietoa ja lupaa. Viruksella on kaksi kriteeriä, jotka ovat, että sen tulee suorittaa itsensä itsenäisesti osana toisen ohjelman ajoa ja että sen tulee monistaa itseään toisiin ohjelmistoihin.

Madot

Symantecin (2015) mukaan madot ovat haittaohjelmia, jotka monistavat itseään ilman isäntäohjelmistoa, joskin madot ovat monesti Word- tai Excel-tiedoston sisällä. Salakavala mato voikin tuhoisasti lisääntyä koko verkkoinfran sisällä, jos sitä ei huomata ajoissa. Madot voivat korruptoida tiedostoja, varastaa salassa

pidettäviä tietoja sekä myös asentaa työasemalle muita ohjelmistoja kuten troijalaisia (Krutz & Vines 2008, 488). Tietokone on hyvä pitää päivitettynä, sillä madot usein käyttävät hyväkseen muiden ohjelmistojen tietoturva-aukkoja.

Troijalainen

Troijalainen on luotettavalta vaikuttava ohjelmisto, joka kuitenkin sisältää haitallista koodia ja suorittaa käyttäjälle tuntemattomia ja ei-toivottuja toimintoja, esimerkiksi lähettää tietoja käyttäjän verkkoliikenteestä eteenpäin. Troijalainen ei kuitenkaan monista itseään, kuten madot ja virukset. (Symantec 2015; Krutz & Vines 2008, 169 – 170.)

Malwarebytes-tietoturvasivuston artikkelin (2013) mukaan troijalaiset voidaan jakaa eri tyyppeihin sen mukaan, mitä ne pyrkivät tekemään.

- *Takaovi-t*roijalaiset *(RAT, remote access trojan)* jättävät jälkeensä uhrin tietokoneelle takaoven, jonka kautta hyökkääjä pääsee jatkossa käsiksi infektoituneelle tietokoneelle. Infektoitunutta tietokonetta voidaan käyttää esimerkiksi välityspalvelimena, palvelunestohyökkäyksen tekoon tai anonyymina palvelimena.
- *Tuhoisat* troijalaiset pyrkivät aiheuttamaan vahinkoa uhrin käyttöjärjestelmälle esimerkiksi salaamalla tiedostot ja pyytämällä maksua purkua vastaan (ks. ransomware) tai poistamalla tietoturvaohjelmistoja käytöstä.
- *Salasanan varastajat* pyrkivät välittämään käyttäjätilien tiedot hyökkääjälle. (Ks. Keylogger)
- *Tiputtaja* asentaa lisää haittaohjelmia käyttäjän tietokoneelle.
- *Vakoojat* ovat troijalaisia, jotka on erityisesti suunniteltu vakoiluun, ja niitä voi olla hyvinkin hankala paljastaa.
- *ArcBomb-troijalaiset* pyrkivät kaatamaan tai hidastamaan tietokoneen pakkaamalla ison kasan tiedostoja pieneen pakettiin, jonka purkaminen syö valtaisan määrän järjestelmän resursseja.

- *SMS-troijalaiset* kohdistuvat mobiililaitteisiin ja lähettävät sms-viestejä maksullisiin numeroihin.

2.3 Murtotekniikat

Tässä luvussa esitellään tekniikoita, joita hyökkääjä voi käyttää yrittäessään murtautua työasemalle tai aiheuttaa muuten vahinkoa yrityksen tietoresursseille.

Porttiskannaus

Porttiskannauksessa yhdistetään kohdeverkon TCP- ja UDP-portteihin pyrkimyksenä selvittää näissä toimivat palvelut ja ohjelmistot. Yleensä järjestelmissä on 65 535 eri porttia, ja ne voivat olla joko auki, kiinni tai filtteröitynä. Avonainen portti ottaa vastaan kutsuja, kiinni oleva portti taas ei ja filtteröity portti on suojattuna esimerkiksi palomuurin toimesta. (Krutz & Vines 2008, 95–96.)

Jokaisella portilla on oma tehtävänsä. Esimerkiksi portti #53 huolehtii domain-nimien muuntamisesta verkkoa selattaessa (Speedguide 2016.).
Porttiskannauksen toteuttamiselle on tehty monia eri ohjelmistoja ja tässä opinnäytetyössä käytetään ilmaista, useaa käyttöjärjestelmää tukevaa Nmap-porttiskanneria.

Porttiskannaus on laiton tietomurron yritys, josta voidaan rikoslain 38:8 §:n mukaan tuomita sakkoihin tai maksimissaan kahdeksi vuodeksi vankilaan. (Poliisi 2016a)

SQL-injektio

SQL-injektio on yksi yleisistä verkkosivustojen haavoittuvuuksista ja siinä hyökkääjä kirjoittaa SQL-koodia esimerkiksi web-lomakkeen syötekenttään odottaen, että palvelin mahdollisesti toteuttaa tämän käskyn. Mikäli SQL-

injektion mahdollisuutta ei ole otettu huomioon, voi syötekentän kautta jopa poistaa kokonaisia SQL-tauluja tai saada käyttäjien tietoja esille. (W3schools 2016.)

Esimerkki haavoittuvasta SQL-lauseesta ohjelmistokoodin sisällä:
txtUsername = getRequestString("Username");
*SELECT * FROM Users WHERE username = + txtUsername;*

Tähän injektoitunut lause voi näyttää seuraavalta, ja se voi pudottaa Users-taulun, poistaen käyttäjien tiedot:
SELECT * FROM Users WHERE Username = David; DROP TABLE Users;

Keylogger

Keylogger voi olla joko fyysinen lisäosa näppäimistön ja tietokoneen välissä tai ohjelmisto, joka pyörii koko ajan taustalla. Se tallentaa käyttäjän näppäimistön kaikki painallukset ja joko lähettää tiedot eteenpäin verkon välityksellä tai tallentaa tiedot paikallisesti. Keylogger-ohjelmisto on todennäköisintä saada troijalaisen sähköpostiliiteen mukana. (Krutz & Vines 2008, 149–150.)

Palvelunestohyökkäys

Palvelunestohyökkäyksellä on tarkoitus estää legitiimien käyttäjien pääsy tietojärjestelmään käyttäen erilaisia tekniikoita, jotka ylikuormittavat kohdejärjestelmän palvelinresurssit. Hyökkääjän ei edes tarvitse päästä kohdejärjestelmän sisään toteuttaakseen hyökkäyksen vaan kohdepalvelimelle voidaan lähettää esimerkiksi niin paljon kutsuja, ettei palvelin pysty käsittelemään niitä ja menee epäkuntoon. (Krutz & Vines 2008, 207-208.)

Varsinkin hajautetut palvelunestohyökkäykset, joissa bottiverkko kohdistetaan tiettyä kohdetta kohti, ovat erittäin yleisiä, ja niitä tapahtuu joka päivä. (Digital Attack Map 2016.)

Resursseja vievien tekniikoiden lisäksi on myös verkkoprotokollia hyväksi käyttäviä hyökkäyksiä, joissa lähetetään vääränlaisia paketteja kohdeverkkoon. Näiden lisäksi on myös ohjelmiston logiikkaan kohdistuvia hyökkäyksiä. (Krutz & Vines 2008, 208.)

Exploit Kit

Exploit kitit ovat, nimensä mukaankin, eräänlaisia haittaohjelman levityspaketteja. Luotettavalla sivustolla on tietoturva-aukko jonka kautta hyökkääjä on saanut syötettyä omaa haitallista koodia. Tämä koodi uudelleen ohjaa käyttäjän toiselle sivulle, jossa tunnistetaan käyttäjän tietokoneessa olevat tietoturva-aukot ja näitä hyväksi käyttäen asennetaan haittaohjelma. (Viestintävirasto 2016.)

Exploit kitit käyttävät hyväkseen muiden ohjelmistojen tietoturva-aukkoja, joten ohjelmistot tulisi aina pitää mahdollisimman ajan tasalla. Selaimen lisäosat voi myös laittaa pois päältä, mikä vähentää infektion mahdollisuutta.

2.4 Yksityistietojen hyväksikäyttö

Thomas Holt, rikosoikeuden professori Michiganin yliopistossa, kertoo Theconversation.com -sivuston artikkelissaan (2016) kuinka varastetun tiedon myynti tapahtuu. Holt kertoo, kuinka varastettuja tietoja käytetään muun muassa luottokorttitietojen tapauksessa rahasiirtoihin ja ostoihin, sosiaalisen median tietojen kanssa varastetulla käyttäjätunnuksella voidaan kiristää oikeaa omistajaa, käyttää tietoja tarkennettuihin hyökkäyksiin tiettyä henkilöä kohti tai lisätä tietyn henkilön näkyvyyttä antamalla tälle valefaneja varastetuista käyttäjätunnuksista.

Holtin (2016) artikkelissa kerrotaan tietojen myynnin tapahtuvan yleisten nettikauppojen tapaisissa paikoissa, joissa käyttäjät voivat arvioida toisiaan, kuinka tyytyväisiä olivat kaupankäyntiin ja saatuun tuotteeseen. Tämän avulla pyritään pitämään kaupankäynti luotettavana, sillä poliisille ei tietenkään voi

mennä näissä asioissa valittamaan, jos ostaja ei saakaan tuotettaan. Luottamuksella on siis iso merkitys kauppaa tehdessä.

Candid Wueest kirjoittaa Symantecin virallisessa blogissa (2014) varastettujen tietojen sekä verkkohyökkäysten hinnasta ja kuinka niiden hinta on muuttunut vuosien saatossa. Hän kertoo, kuinka varastettuja sähköpostilejä on saanut ostettua vuonna 2007 4–30 dollarin hintaan ja artikkelin kirjoittamisen aikaan on voinut saada 1000 tiliä 0,50–10 $ hintaan, joten hinnat ovat vaihdelleet vuosien aikana suuresti. Luottokorttitietojen hinnat eivät ole kuitenkaan kokeneet samanlaista isoa hintojen ailahtelua, ja 2014 vuonna niitä pystyi saamaan 0.10-20 $ hintaan kun 2008 hintahaitari oli 0.85–30 $ väliä. Wueestin mukaan hyökkäysten ja haittaohjelmien hinnat pyörivät kymmenistä dollareista jopa tuhansiin asti, esimerkiksi hintahaitari palvelunestohyökkäyksellä on 10–1000 $ ja SpyEye-haittaohjelman voi liisata kuudeksi kuukaudeksi 150–1250$:lla. Hyökkääjällä ei siis tarvitse edes olla tietoteknistä tietämystä, vaan hyökkäyksen voi vain tilata omasta verkkokaupastaan.

2.5 Rikosprosessi

Tässä luvussa tarkastellaan palveluntarjoajan vastuita sekä mitä mahdollisia rikosnimikkeitä sekä rangaistuksia liittyy tietotekniikkarikoksiin.

Vastuut

Käsiteltäessä henkilötietoja palvelun tarjoajan tulee muistaa olevansa vastuussa niiden ylläpidosta ja turvaamisesta, josta on myös henkilötietolaissa säädetty henkilörekisterien osalta seuraavanlaisesti:

> Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä

käsittelyn merkitys yksityisyyden suojan kannalta. (Henkilötietolaki 32. §.)

Yksityishenkilö taas on vastuussa aina itselleen omasta tietoturvasta ja siihen liittyvästä käyttäytymisestä verkossa. Yritysten on myös tärkeää luoda työntekijöilleen kattava tietoturvaohjeistus sekä valvoa sen noudattamista. Mahdollisista tietoturvaohjeistuksista ja hyvistä käytänteistä puhutaan luvussa 4.5 Riskien minimointi.

Rangaistukset

Nykypäivän digitalisoituneessa yhteiskunnassa tietotekniikka on olennainen osa jokapäiväistä elämäämme, joten myös rikollisuus tietoverkossa on lisääntynyt. Näitä tietotekniikkarikoksia ovat tietotekniikkaan ja tietoverkkoihin kohdistuvat rikokset sekä näitä hyväksi käyttävät rikokset. (Poliisi 2016b). Rikoslain (19.12.1889/39) 38 luvussa käydään läpi tieto- ja viestintärikoksia ja esittelen tässä sen luvun osuvimmat rikokset. Tässä kappaleessa esitetyt pykälät ovat kaikki rikoslain 38. luvusta, ellei toisin mainita.

Viestintäsalaisuuden loukkauksessa (3. §.), henkilö avaa toiselle tarkoitetun suojatun viestin joko purkamalla suojauksen tai jollain muulla teknisellä tavalla. Rikos täyttyy myös, jos hankkii tiedon televerkossa tai tietojärjestelmässä välitettävänä olevan televiestin sisällöstä tai sen vastaanottamisesta tahi lähettämisestä. Rangistus tästä on sakko tai enintään kaksi vuotta vankeutta ja pelkkä yritys on rangaistava. Rikos muuttuu törkeäksi (4. §.), mikäli henkilö käyttää hyväkseen asemaansa sähköisen viestinnän tietosuojalaissa tarkoitetun teleyrityksen palveluksessa tai muuta luottamusasemaa, teko on erityisen suunniteltu tai siinä käytetään siihen suunniteltua tai muunneltua ohjelmistoa ja jos kohteena oleva viesti on erityisen luottamuksellinen tai teko loukkaa huomattavasti yksityisyyden suojaa.

MTV julkaisi vuonna 2014 uutisen, jossa mieshenkilö oli tuomittu törkeästä viestintäsalaisuuden rikkomisesta vakoiltuaan vaimonsa tietokonetta noin viiden kuukauden ajan avioeroprosessin ollessa meneillään. Mies oli asentanut Spy-Agent-nimisen ohjelmiston, jolla pystyi seuraamaan tietokoneen tapahtumia ja

sai näin vaimonsa sähköpostiosoitteiden salasanat. Mies oli lukenut ja tallentanut useita kymmeniä vaimonsa sähköposteja, saatuja tietoja tämä oli lähettänyt myös vaimonsa vanhemmille. Mies sai 30 päivän ehdollisen vankeusrangaistuksen, hänet määrättiin maksamaan ex-vaimolleen korvauksia 2000 euroa sekä tämän 2700 euron oikeudenkäyntikulut. (Sipilä 2014.)

Tietoliikenteen häirinnässä (5. §.) henkilö häiritsee tai estää postiliikennettä tai tele- tai radioviestinnässä käytettävän laitteen toimintaa. Rangaistuksena on sakko tai enintään kaksi vuotta vankeutta. Törkeäksi rikos muuttuu, kun henkilö käyttää erityistä luottamusasemaansa rikoksen tekoon.

Helsingin Sanomat raportoi heinäkuussa 2015 17-vuotiaan nuoren saaneen 2 vuoden ehdollisen tuomion kymmenistä tuhansista törkeistä tietomurroista, tietoliikenteen häirinnästä, törkeästä petoksesta ja törkeästä viestintäsalaisuuden loukkauksesta. Poika menetti myös valtiolle tietokoneensa, jolla oli nämä rikokset suorittanut sekä rahanpesurikoksessa olleet 6 558 euroa, hän myös joutui valvontaan. Tuomiota lieventämässä oli pojan nuori ikä, joka oli 12–13 vuotta rikosten tekoaikaan sekä esitutkinnan aikainen vankeus, jota kesti 1 kuukauden. Nuorukaista epäillään myös useista muista tietoverkkorikoksista. (Kerkelä 2015)

3 Ransomware

Ransomware eli kiristyshaittaohjelmat ovat nousseet varsinkin viime vuosina otsikoihin. Ne ovat ohjelmia, jotka salaavat saastuneen koneen tiedostot ja kertovat antavansa salausavaimen, jolla omat tiedostot saa takaisin, rahaa vastaan. Usein nämä ransomwaret väittävät poliisin lukinneen tietokoneen lapsipornografian takia ja tietokoneen lukituksen saa pois, kun on maksanut sakon. Ransomwaren salaus on erittäin vahva ja ainut tapa saada tiedostot takaisin on palauttaa varmuuskopio tai maksaa rahasumma ja toivoa saavansa salausavain. (Poliisi, CERT-FI & F-Secure Oyj 2016.)

Ransomware-haittaohjelmien muunnoksia on löydetty yli 120 eri versiota, joista osa on kokonaisten rikollisjengien hallinnoimia ja toiset taas yksityishenkilöiden ostamia. Osana selittävänä tekijänä ransomwaren jatkuvalle nousulle voi olla Hidden Tear -haittaohjelman lähdekoodin julkaiseminen avoimeksi, mikä on luonut pohjan useille muille ransomware-haittaohjelmille. (Ward 2016.)

3.1 Toiminta

Crypto-Ransomware-haittaohjelmia on yli sataa erilaista versiota, joten tässä kappaleessa pyritään kuvaamaan sen toimintaa yleisemmällä tasolla. Kaikille niille on kuitenkin yhteistä tiedostojen salaaminen.

3.1.1 Infektion saaminen

Ransomware on mahdollista saada sähköpostissa liitetiedoston kautta. Nämä sähköpostiviestit pyrkivät saamaan käyttäjän lataamaan liitteet sosiaalisella manipuloinnilla, eli toisin sanoen sanomalla liitteessä olevan jotain käyttäjälle hyödyllistä. (O'Brien & Morparia 2016.)

Toinen tapa saada infektio on exploit kitin kautta, jossa hyökkääjä on lisännyt haitallista koodia tavalliselle verkkosivustolle. Tämä koodi voi uudelleen ohjata toiselle sivustolle tai selvittää käyttäjän tietoturva-aukot ja infektoi näitä hyväksi käyttäen tietokoneen. Myös muut haittaohjelmat voivat asentaa ransomwaren käyttäjän tietokoneelle. (O'Brien & Morparia 2016.)

3.1.2 Infektion jälkeen

Kun infektio on alkanut, ransomware pyrkii poistamaan Windowsin tilannevedokset, jottei salattuja tiedostoja pystytä tätä kautta tuomaan takaisin. Tämän jälkeen haittaohjelma kopioi ohjelmansa moneen paikkaan ja asettaa ohjelmiston suoritettavaksi heti käynnistyksen yhteydessä. Ransomwaren exe

-tiedosto voi olla randomisoidulla nimellä useassa paikassa ja vielä randomisoidussa kansiossa, mikä tekee sen löytämisesta hankalaa. (Sophos 2015.)

Ransomware ottaa yhteyttä komentopalvelimeen lähettäen sinne tietokoneen tiedot ja aloittaa tiedostojen salaamisen vastauksen saatuaan. Salaus on erittäin vahva, käytännössä mahdoton purkaa ilman salausavainta, jota säilytetään hyökkääjän omalla palvelimella. Kun tiedostojen salaus on tehty, tulee tietokoneen hakemistoihin, mahdollisesti kaikkiin joissa salattuja tiedostoja on, tiedosto, jossa kerrotaan, kuinka käyttäjä voi saada itselleen käyttöoikeuden takaisin tiedostoihinsa. (Symantec 2016.)

3.2 Havaitseminen

Ransomware poikkeaa muista haittaohjelmista niin, että se ei pyri toimimaan hiljaa vaan päinvastoin se pyrkii saamaan käyttäjän huomion itseensä, jotta haittaohjelma saisi uhrin maksamaan (Rashid 2016.). Ransomware voi ilmoittaa itsestään ponnahdusikkunoilla (Zamora 2016a.) ja, kuten edellisessä kappaleessa on kerrottu, ransomware luo infektiosta tiedottavan tiedoston useisiin paikkoihin ympäri koneen hakemistoja.

Kuvassa 1 on esimerkki ransomwaren luomasta ilmoituksesta.


README_FOR_DECRYPT.txt — Edited

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to https://fiwf4kwysm4dpw5l.onion.to (IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN THIS LINK: http://fiwf4kwysm4dpw5l.onion)
2. Use 1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof as your ID for authentication
3. Pay 1 BTC (~407.47$) for decryption pack using bitcoins (wallet is your ID for authentication - 1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof)
4. Download decrypt pack and run

---> Also at https://fiwf4kwysm4dpw5l.onion.to you can decrypt 1 file for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)

Kuva 1. Ransomwaren ilmoitus (Kuva: Palo Alto Networks 2016.)

Kuvasta käy ilmi, että tiedostot on salattu erittäin vahvalla 2048-bittisellä RSA -salauksella, joka tekee sen purkamisesta ilman salausavainta erittäin haastavaa. Hieman alempana näkyy, että maksu tapahtuu bitcoin-cryptovaluuttaa käyttäen, jolla hyökkääjä pyrkii salaamaan jälkensä. Käyttäjän tulee siis ostaa itselleen bitcoin, tai enemmän mikäli odottelu nostaa maksua. On hyvä myös huomata tiedoston nimi, joka on isoin huutavin kirjaimin kirjoitettu ”READ_FOR_FOR_DECRYPT”, eli suomeksi ”lue minut salauksen purkamiseksi.” Viestin kieli ja ulkoasu voi vaihdella sen mukaan missä päin maailmaa infektio tapahtuu (Sophos 2015.).

3.3 Ennaltaehkäisy

Ransomwaren-haittaohjelman ennaltaehkäisyyn voi käyttää samoja varotoimia kuin muidenkin haittaohjelmien kanssa. Verkkoon kytkettyjen ja muutenkin dataa vaihtavien laitteiden kanssa tulee toimia järkevästi ja miettiä voiko datan lähteeseen luottaa. Ei tule luottaa tuntemattomiin sähköposteihin, jotka sisältävät liitteitä eikä myöskään tutuilta tulleisiin liitteisiin silloin kun heiltä ei odota saavansa mitään liitettä. Voisi sanoa ransomwaren välttämiseen pätevän samat neuvot kuin muidenkin haittaohjelmien kanssa.

- **Asenna internetselaimeen adblocker-ohjelmisto.** Adblocker-ohjelmistot estävät internet-selaimessa näytettävien mainosten esittämisen. Kim Zetter sanoo Wired-sivuston artikkelissaan (2016), kuinka Internet-sivun mainos voi olla kompromisoitu ja sisältää väylän haittaohjelmien pääsylle työasemalle.
- **Ole tarkkana saapuneiden sähköpostiviestien kanssa.** Zetter sanoo samaisessa artikkelissa phishing-hyökkäysten olevan hakkeroijien pääkeino työasemien infektoimisessa. Sähköpostiin tulee infektion sisältävä liitetiedosto tai linkki sivustolle, jonka kautta infektio tulee.
- **Pidä ohjelmistojen päivitykset ajan tasalla.** Wendy Zamora (2016b) kertoo Malwarebytes-tietoturvayrityksen blogissaan, kuinka ohjelmistojen päivitykset korjaavat tietoturva-aukkoja, joita mahdollinen hyökkääjä voi käyttää hyväkseen.

- **Poista ohjelmat, joita et käytä.** Käyttämättömät ohjelmat voivat olla jo vanhentuneita ja ne ovat turhia infektiovektoreita. Tietoturva-aukot voivat olla varsin suuriakin, mikäli ohjelmiston tuki on loppunut eikä sille enää tehdä tietoturvapäivityksiä. (Zamora 2016b.)
- **Valkolistaa sallitut ohjelmistot.** Tämä on siis mustanlistan vastakohta. Vain järjestelmänvalvojan tekemässä listassa olevat ohjelmistot voidaan asentaa. Tämä auttaa estämään haittaohjelmien asentumista ja helpottaa myös organisaation työasemien ylläpitoa. (Zetter 2016.).
- **Käytä tarvittavia tietoturvaohjelmia ja muista myös päivittää ne.** Tietoturvaohjelmat ohjelmat pitävät tietokoneen suojattuna ja auttavat myös poistamaan infektion sen saatuaan (Zamora 2016b.). Virustorjuntaohjelmien viruskannat tulee myös päivittää usein, jotta se pystyy tunnistamaan ja torjumaan tuoreimpia uhkia.
- **Pysy poissa epäilyttäviltä internetsivuilta ja varo mitä lataat.** Mikäli sivusto ei näytä luotettavalta, sen mainokset vaikuttavat huijauksilta ja sivusto aukaisee pop-up-ikkunamainoksia, kannattaa sivulta lähteä pois, sillä sieltä saattaa saada viruksia. Sama asia myös tiedostoja ladattaessa eri lähteistä, sillä tiedosto voi sisältää mitä tahansa sen nimestä huolimatta, joten mikäli et luota tiedostoon ja sen alkuperään, älä lataa sitä. (Phelp 2016.)
- **Näytä tiedostopäätteet.** Ransomwaren sisältävä tiedosto voi olla nimettynä tavallisen näköiseksi PDF-tiedostoksi ”tiedosto.pdf”, mutta kun käyttöjärjestelmän laittaa näyttämään tiedostopäätteet, voi kyseinen tiedosto oikeasti ollakin ”tiedosto.pdf.exe”. Se ei olekkaan tekstitiedoston vaan ajettava tiedosto, joka asentaa haittaohjelman tietokoneelle. (No More Ransom 2017.)

3.4 Vahinkojen minimointi (Infektion tapahtuman varalle)

Mikäli työasema saa ransomware-infektion, pystyy siihen kuitenkin vielä valmistautumaan etukäteen ja minimoimaan mahdolliset vahingot. Alla on listattuna neuvoja, jotka voivat auttaa mahdollisen infektion varalle.

- **Muista tehdä varmuuskopiota tärkeistä tiedostoista.** Tiedostoja kannattaa varmuuskopioida päivittäin, jolloin voidaan minimoida tärkeiden tiedostojen häviäminen infektion tapahtuessa ja kaikkien tiedostojen ollessa lukittuna. (Zetter 2016.)
- **Pidä varmuuskopiot erossa muusta järjestelmästä.** Ransomwaret käyvät läpi koneen hakemistot ja mikäli varmuuskopioita säilyttävä palvelin on yhdistettynä infektoituneeseen koneeseen, ransomware salaa siellä olevat varmuuskopiotkin. (Zetter 2016.)
- **Vahva käyttäjäoikeuksien hallinta.** Salli käyttäjien päästä vain heille tarkoitettuihin kansioihin käsiksi, mikä hallitsee infektion leviämistä. Mikäli käyttäjällä ei ole oikeutta avata kansiota, ransomwarenkaan ei pitäisi sen sisälle päästä. (Sherman 2015.)
- **Ota Infektoitunut työasema heti kokonaan verkosta irti.** Kun infektoitunut kone otetaan verkosta irti, infektio ei pääse leviämään verkon yli muihin koneisiin jotka saattavat ottaa siihen yhteyttä. Tämä koskee myös bluetoothia ja muita yhteydenottomenetelmiä. (Zetter 2016.)
- **Googlaa infektio.** Ransomwareja on monia erilaisia, ja joidenkin salaukseen on jo löydetty purkukeinoja, kuten Tesla Cryptin tapauksessa, jossa sen luojat paljastivat salausavaimet. Tutkijat olivat myös löytäneet haavoittuvuuden Tesla Cryptin ensimmäisestä versiosta. Internetistä saattaa löytyä keino purkaa tiedostojen salaus. (Snow 2016.)
- **Älä maksa lunnaita.** Ei ole mitään varmuutta, että hyökkääjä purkaisi tiedostot saatuaan lunnaat. Käyttäjä voi myös, maksavana uhrina, joutua tämän jälkeen lisäkiristyksen kohteeksi. (Sherman 2015.)

4 Tutkimuksen toteutus

Haittaohjelmista ja tietoturvasta löytyy suuri määrä aikaisempia opinnäytetöitä vuosien varrelta. Esimerkkinä ota Eetu Salmisen työn vuonna 2012; Tietoturvaohjeistus Fujitsu Finland Oy:n käyttötukeen. Työ oli tarkoitettu tukemaan käyttötukihenkilöä tämän päivittäisessä työssä, sekä toimimaan

perehdytyksessä apuna uusille työntekijöille. Opinnäytetyön teoriaosuuden pohjalta Salmi loi Fujitsulle tietoturvaohjeistuksen, joka on salattu ulkopuolisilta. Päälähteenä hän on käyttänyt Esko Vainikan tietoturvakurssin lähdemateriaaleja, mutta myös erilaista kirjallisuutta sekä tietoturvastandardeja.

Karri Koski julkaisi oman opinnäytetyönsä nimeltään ”Tietoturva – Ilmaiset virustorjuntaohjelmat testissä” vuonna 2012. Koski testaa ilmaisia virustorjuntaohjelmia Windows XP- ja Windows 7 -ympäristöissä Virtual box-virtualisointiohjelmistoa hyväksikäyttäen, kuten tässäkin opinnäytetyössä on tehty. Teoriaosuudessa hän käy läpi erilaisia haittaohjelmia ja kuinka virustorjuntaohjelmat pystyvät tunnistamaan niitä. Koski on käyttänyt sähköisiä lähteitä, muun muassa Wikipediaa ja virusturvaohjelmistojen kotisivuja.

Tutkimusongelmana tässä opinnäytetyössä on, kuinka ransomware toimii ja kuinka suojautua siltä. Toimeksiantajan osalta työn tavoitteena on laatia ohjeistus lunnashaittaohjelmien varalle. Aihe on nykyisin varsin ajankohtainen, koska ransomware-haittaohjelmat ovat tulleet tietoisuuteen vasta joitain vuosia sitten. Materiaalia löytyy internetistä paljon, sillä onhan erilaisia haittaohjelmia, ransomwaret mukaan lukien, aivan lukematon määrä, joten olen rajannut aiheen koskemaan salaavia lunnashaittaohjelmia.

Tässä opinnäytetyössä on käytetty teoreettista sekä empiiristä tutkimusmenetelmää, eli kyseessä on monimenetelmäinen opinnäytetyö. Olen etsinyt opinnäytetyön aiheesta tietoa useista eri lähteistä ja näistä koonnut tietoperustaa tälle työlle. Jyväskylän yliopiston humanistinen uiedekunta (2015a) määritteleekin teoreettisen tutkimuksen seuraavalla tavalla:

> Teoreettisessa tutkimuksessa ei havainnoida tutkimuskohteita välittömästi, vaan kohteesta pyritään hahmottamaan käsitteellisiä malleja, selityksiä ja rakenteita aiemman tutkimuskirjallisuuden pohjalta.

Opinnäytetyön toiminnallinen osuus, jossa havainnoidaan ransomware-infektion kulkua, taipuu empiirisen tutkimuksen puolelle. Jyväskylän yliopiston (2015b) internetsivuilla sanotaankin, että empiirisessä tutkimuksessa tutkimustuloksia saadaan tekemällä konkreettisia havaintoja tutkimuskohteesta.

En tietoisesti valinnut mitään tutkimusmenetelmää tälle opinnäytetyölle, vaan enemmänkin alitajuisesti ajauduin teoreettiseen tutkimusmenetelmään. Se malli myös tuntui soveltuvan tällaiseen, teoreettisen informaation jakoon tarkoitettuun työhön. Tietysti olisi voinut olla hyödyllistä miettiä tarkemmin erilaisia tutkimusmenetelmiä ennen kirjoittamisen aloittamista, mutta myös tähän valintaan olen tyytyväinen.

5 Tietokoneen infektointi

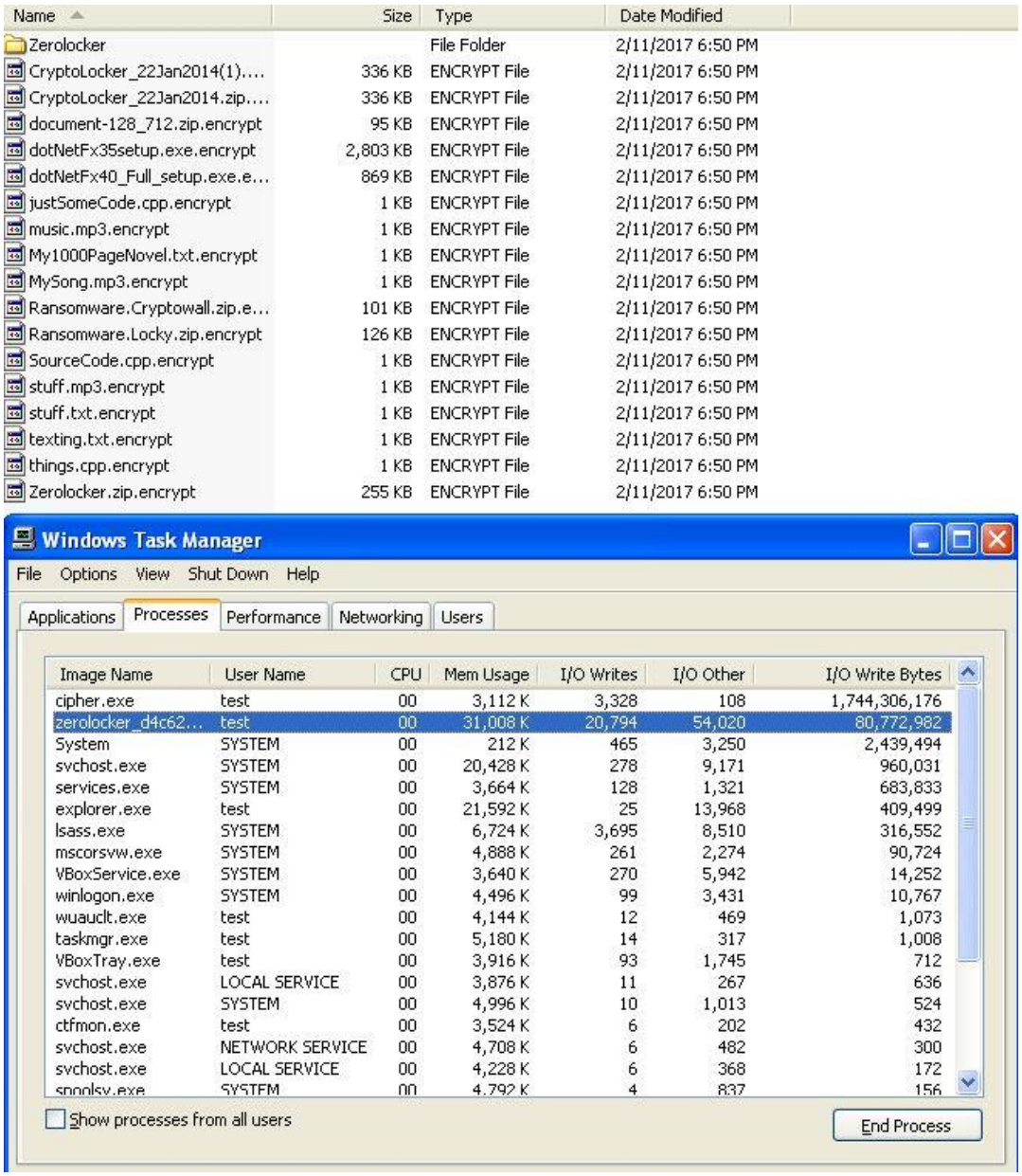
Tässä kerron toiminnallisesta osuudesta missä tein testin, jossa hankin itselleni ransomware-infektion. Käytin hyväksi virtuaalikonetta, jotta oman tietokoneeni tiedostot eivät olisi vaarassa. Latasin Oraclen Virtual Box -virtualisointiohjelmiston, ja käytin sen sisällä Windows XP-käyttöjärjestelmää.

Tarvitsin Microsoftin .NET Framework -ohjelmistokomponenttikirjaston 3.5 –version, jotta ransomware pystyi ajamaan itsensä. Latasin Cryptowall –ransomwaren Github repositoriosta ytisf/TheZoo, joka sisältää useita eri haittaohjelmistoja.

Purin saadun zip-paketin, joka sisälsi kaksi tiedostoa 1002.exe ja 1003.exe. Ajoin ensimmäisenä mainitun tiedoston ja sain pop-up-ikkunan, joka pyysi ajamaan toisen tiedoston nimeltään D2E9ED9C8B.exe ja tämä tiedosto näkyi myös Windowsin Task Managerin prosessien hallinnassa. Mitään ei kuitenkaan tapahtunut ja kokeilin toista haittaohjelmaa.

Latasin samasta paikasta ZeroLocker -nimisen ransomwaren. Ohjelman ajettuani oli muutaman minuutin kuluttua tiedostojen perässä .encrypted -pääte tiedostot oli nyt salattu. Todensin tämän avaamalla luomani tekstitiedoston ja näin sen sisältämän tekstin muuttunen sekamelskaksi. Kuvassa 2 voi Task Managerissa nähdä zerolocker_d4c62... (merkkisarja jatkuu pitkälle).exe- sekä cipher.exe -ohjelmat, jotka haittaohjelma on tehnyt aktiiviseksi. Kuvassa näkyy myös salatut tiedostot. Voi myös huomata kuinka paljon zerolocker.exe- ja

varsinkin cipher.exe -ohjelmilla on kirjoitusoperaatioita, voi siis olettaa cipher.exe-ohjelmiston hoitavan tiedostojen salauksen.



Name	Size	Type	Date Modified
Zerolocker		File Folder	2/11/2017 6:50 PM
CryptoLocker_22Jan2014(1)....	336 KB	ENCRYPT File	2/11/2017 6:50 PM
CryptoLocker_22Jan2014.zip....	336 KB	ENCRYPT File	2/11/2017 6:50 PM
document-128_712.zip.encrypt	95 KB	ENCRYPT File	2/11/2017 6:50 PM
dotNetFx35setup.exe.encrypt	2,803 KB	ENCRYPT File	2/11/2017 6:50 PM
dotNetFx40_Full_setup.exe.e...	869 KB	ENCRYPT File	2/11/2017 6:50 PM
justSomeCode.cpp.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
music.mp3.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
My1000PageNovel.txt.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
MySong.mp3.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
Ransomware.Cryptowall.zip.e...	101 KB	ENCRYPT File	2/11/2017 6:50 PM
Ransomware.Locky.zip.encrypt	126 KB	ENCRYPT File	2/11/2017 6:50 PM
SourceCode.cpp.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
stuff.mp3.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
stuff.txt.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
texting.txt.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
things.cpp.encrypt	1 KB	ENCRYPT File	2/11/2017 6:50 PM
Zerolocker.zip.encrypt	255 KB	ENCRYPT File	2/11/2017 6:50 PM

Kuva 2. Task Manager sekä salatut tiedosto

Salaamisen jälkeen Windows uudelleen käynnisti itsensä ilman käyttäjän syötettä. Hieman ennen uudelleen käynnistystä ohjelma kuitenkin loi RECOVER YOU FILES.exe tiedoston, joka pysyi työpöydällä joitain kymmeniä sekunteja ennen katoamistaan. Myös juuri ennen uudelleen käynnistystä välähti sekunnin ajan ikkuna, jossa lukon kuva. Mitään ilmoituksia tai viestejä ei kuitenkaan tapahtuneesta tullut uudelleen käynnistyksen jälkeen, joten minulla ei olisi ollut mahdollisuutta maksaa lunnaita saadakseni tiedostoja takaisin.

Luultavasti jotain meni pieleen haittaohjelman ajon aikana, ehkä se ei saa yhteyttä etäpalvelimelle tai virtuaalikone aiheuttaa sille jotain ongelmaa.

C-aseman juureen oli luotu ZeroLocker –hakemisto, joka sisälsi yhden tiedoston: address.dat. Tämä tiedosto sisälsi yli kolmekymmentä merkkiä pitkän sattumanvaraiselta vaikuttavan merkkijonon. Tämän hakemiston sisällä tulisi kuitenkin olla enemmän tiedostoja sekä ZeroRescue.exe, joka purkaa salauksen (Grinler 2014.). Jotain siis todellakin meni pieleen haittaohjelmiston ajon aikana ja se joutui terminoimaan ajon kesken kaiken.

Asensin Microsoftin Windows Defender -virusturvaohjelmiston ja ajoin skannauksen sen jälkeen, kun tiedostot oli salattu. Defender ei löytänyt virusta uusimmilla viruskannoillakaan.

6 Yhteenveto

Opinnäytetyön aiheen miettimisen aloitin keväällä 2016, ja työstämisen aloitin saman vuoden kesällä. Alkuperäisenä aiheena oli kirjoittaa työasemalle murtautumisesta, eri keinoista ja menetelmistä. Toiminnallisessa osuudessa olisin eri työkaluja hyväksikäyttäen yrittänyt murtautua tietokoneelle. Vaihdoin aiheen kuitenkin tähän nykyiseen marraskuussa 2016. Alkuperäinen tutkimusaihe osoittautui liian laajaksi kokonaisuudeksi ja tarve oli rajata aihealuetta.

Aluksi opinnäytetyön edistyminen oli hidasta, mutta rakenteen ja tutkimusongelman päivityksen jälkeen työ alkoi taas edistyä, vaikka samaan aikaan tein myös töitä. Tammikuussa 2017 sain sitten oman alan töitä, ja muutin eri paikkakunnalle. Tilanne aiheutti tietysti katkon kirjoittamisessa joksikin aikaa, mutta siitä huolimatta pyrin kirjoittamisessa olemaan järjestelmällinen. Ennen kirjoittamisen alkua loin opinnäytetyölle pohjan valmiiden otsikoiden ja alaotsikoiden muodossa, joihin sitten aloin kirjoittamaan

sisältöä, ”lihaa luurangon ympärille”. Samalla pyrin keskittymään kerralla vain yhteen kappaleeseen/asiaan, ja sen tehtyäni siirtymään sitten seuraavaan.

Eri lähteitä tässä opinnäytetyössä on käytetty varsin laajalti, joista suurin osa on sähköisiä, mutta kirjallisuuttakin löytyy. Lähdeviittauksissa olen pyrkinyt käyttämään luotettavia lähteitä, pääosin tunnettuja uutissivustoja, sekä myös tietotekniikkaan keskittyneitä sivuja. Blogeja olen myös käyttänyt, joskin blogien käyttämisen lähteenä olen rajannut ainoastaan tietoturvayritysten virallisiin blogeihin, joka tuo blogin informaatioon omanlaisensa auktoriteetin verrattuna internetin tusinablogeihin. Lähteistä löytyy myös yksi keskustelupalstan viesti, jonka olen ottanut mukaan, koska viestin luoja on erään tietotekniikkasivuston perustaja.

Tätä opinnäytetyötä voi pitää eräänlaisena oppaana, joka pyrkii kertomaan haittaohjelmista yleisesti ja paneutuu tarkemmin ransomwaren toimintaan ja sen välttämiseen. Toki ohjeet ovat kelpoja välttämään muitakin haittaohjelmia. Suurimmaksi osaksi ohjeiden tulisi palvella kaikkia niin yksittäisiä käyttäjiä kuin myös organisaatioita, vaikkakin ransomwaren tuoma uhka yrityksille on yksittäistä käyttäjää paljon suurempi.

Uskon ohjeista olevan hyötyä, silloin kun käyttäjä miettii, kuinka välttää haittaohjelmia. Ohjeet auttavat myös pitämään tiedostoja turvassa, mikäli ohjetta varmuuskopioinnista on noudatettu. Tiivistettynä voisi sanoa tärkeimpien ohjeiden olevan käyttäjän tarkkaavaisuus, ettei avaa epämääräisiä linkkejä ja sähköpostin liitetiedostoja sekä myös käyttäjän käyttöoikeuksien rajaus käyttöjärjestelmässä. Kannattaa myös pitää varmuuskopioita ajan tasalla, ja pitää huoli, että varmuuskopioiden tallennuspaikka ei ole yhteydessä tietokoneeseen.

Työn toiminnallinen osuus ei ehkä informaatioltaan ole kovin kattava, mutta uskon sen olevan kohtalaisen mielenkiintoinen lisä. Oli kuitenkin mielenkiintoista huomata siinä, kuinka virusturvaohjelma ei löytänyt mitään infektiota koneesta, vaikka haittaohjelma oli salannut tiedostoja. Olin jo aikaisemmin, ennen opinnäytetyön aloittamista kuullutkin, että

virusturvaohjelmat eivät välttämättä tunnista ransomware-infektiota, joten täysin yllättynyt en tästä ollut.

Opinnäytetyötä tehdessä opin tietysti aihealueesta, josta kirjotin, mutta myös isomman suunnittelun vaativasta kirjoitustyönteosta ja siitä, kuinka tärkeää on alussa olla selkeä kuva, mistä aloittaa kirjoittamaan, jotta kirjoitustyö sujuisi sulavasti. On ihan luonnollista, että asiat alkavat tekijälle tarkentumaan kirjoittamisen aikana. Opin, että kirjoitusprosessiin olisi hyvä asettaa aikarajoja. Asetin itselleni aikarajat vasta keväällä 2017, jolloin lyhyen ajan sisällä sain raportista kirjoitettua suurimman osan. Ilman ”deadlinea” kirjoittaminen etenee enemmän inspiraation mukaan.

Jos pitäisi miettiä, mitä tekisin toisin, niin olisi hyvä olla paremmin lukkoon lyöty aihe ennen kirjoittamisen aloittamista. Olisi myös hyvä olla jonkinlaista aikataulutusta, esimerkiksi tietty luku kirjoitettu tiettyyn päivämäärään mennessä, tai jokin tietty sivumäärä. Uskoisin deadlinejen asettamisen pitävän kirjoitusprosessin paremmin hallussa. Toisin voisi myös tehdä, että ottaisi jonkin yrityksen tähän mukaan, ja tekisi työn suoraan heidän it-tuelle saaden heiltä myös palautetta ja toiminnalisen osuuden toteutus heidän oikeissa järjestelmissä eikä virtuaalikoneella, tai vaihtoehtoisesti infektoisi virtuaalikoneiden verkon. Pitäisi myös olla paljon enemmän aikaa tällöin opinnäytetyön toteutukseen. Sanoisin opinnäytetyön onnistuneen kohtalaisesti myös näinkin. Työssä on hyödyllistä ja käytettävää informaatiota, ja uskon sen olevan helposti ymmärrettävässä muodossa kirjoitettu ilman tietoteknistä sanakirjaakin.

Uskon tietoturvan olevan tulevaisuudessa kasvavassa roolissa, kun arkipäivän laitteisiin saadaan älyä. Tekniikka kehittyvät, samalla kehittyy myös erilaiset suojausmenetelmät, mutta myös haittaohjelmat pysyvät kehityksessä koko ajan mukana. Ransomwaret alkavat käyttämään uusia vahvempia salausmenetelmiä, kun entiset saadaan jo purettua uusilla tekniikoilla. Tämän takia tulevaisuudessakin ennaltaehkäisy on tärkeässä asemassa, ja käyttäjän on oltava varuillaan tietoverkossa liikuttaessa.

Lähteet

Arntz, P. 2013. What are Trojans?. https://blog.malwarebytes.com/cybercrime/2013/06/what-are-trojans/. 3.10.2016.

Beaver, K. 2012. Hacking for Dummies (4). For Dummies. Hoboken: John Wiley & Sons.

Corkery, M. Goldstein, M. & Perloth, N. 2014. Neglected Server Provided Entry for JPMorgan Hackers. http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified. 6.10.2016.

Goldstein, M. Perloth, N. & Silver-Greenberg, J. 2014. JPMorgan Chase Hacking Affects 76 Million Households. http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/. 5.9.2016.

Google Ideas & Arbor Networks Inc. 2016. Digital Attack Map (Internetpalvelu). http://digitalattackmap.com. 4.9.2016.

Grinler. 2014. ZeroLocker - a new destructive encrypting ransomware. 15.8.2014 klo.17.25. https://www.bleepingcomputer.com/forums/t/544555/zerolocker-a-new-destructive-encrypting-ransomware/. 11.2.2017.

Holt, Thomas. 2016. Buying and selling hacked passwords: How does it work? . https://theconversation.com/buying-and-selling-hacked-passwords-how-does-it-work-60894. 11.10.2016

Huhtanen, J. 2016. Ulkoministeriöön vuonna 2013 iskenyt vakoiluohjelma vei tietoja "rekkalasteittain". http://www.hs.fi/kotimaa/a1411735620888?jako=684e1b1b69f7abe692b64d3b82e2ae7b. 19.19.2016.

Information is Beautiful. 2016. World's Biggest Data Breaches. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. 5.9.2016.

Jyväskylän Yliopisto. 2015a. Teoreettinen tutkimus. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/teoreettinen-tutkimus. 6.4.2017.

Jyväskylän Yliopisto. 2015b. Empiirinen tutkimus. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus. 6.4.2017.

Kerkelä, L. 2015. Espoolais-nuorukainen sai ehdollista vankeutta yli 50 000 tietomurrosta. http://www.hs.fi/kotimaa/a1436234526466. 27.9.2016.

Koski, K. 2012. Tietoturva - ilmaiset virustorjuntaohjelmat testissä. Turun ammattikorkeakoulu. Tietojenkäsittely koulutusohjelma. Opinnäytetyö. http://urn.fi/URN:NBN:fi:amk-2012061212551. 4.4.2017

Krutz, R. L. & Vines, R. D. 2008. CEH Prep Guide : The Comprehensive Guide to Certified Ethical Hacking. Indianapolis: Wiley.

Leswing, K. 2016. Yahoo confirms major breach — and it could be the largest hack of all time.. http://uk.businessinsider.com/yahoo-hack-by-state-sponsored-actor-biggest-of-all-time-2016-9. 26.9.2016

Marks, P. 2011. Dot-dash-diss: The gentleman hacker's 1903 lulz. https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/. 5.10.2016.

No More Ransom. 2017. Prevention Advice. https://www.nomoreransom.org/prevention-advice.html. 29.3.2017

Phelps, J. 2010. How to Avoid Malware. http://www.pcworld.com/article/210891/malware.html. 19.3.2017.

Phillips, T 2016. Five years ago today, Sony admitted the great PSN hack. http://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today. 19.9.2016

Poliisi. CERT-FI & F-Secure Oyj. 2016. LOOK OUT FOR RAN$OMWARE. http://www.ransomware.fi/. 28.8.2016.

Poliisi. 2016a Tietotekniikkarikosten tunnusmerkistöjä . https://www.poliisi.fi/rikokset/tietotekniikkarikollisuus/tietotekniikkarikosten_tunnusmerkist%C3%B6ja. 21.9.2016.

Poliisi. 2016b. Tietotekniikkarikollisuus . https://www.poliisi.fi/rikokset/tietotekniikkarikollisuus. 27.9.2016.

Rashid, F. 2016. How to tell if you've been hit by fake ransomware . http://www.infoworld.com/article/3062552/security/how-to-tell-if-youve-been-hit-by-fake-ransomware.html. 2.2.2017.

Refsnes Data. 2016. SQL Injection http://www.w3schools.com/sql/sql_injection.asp. 21.9.2016.

Salmi, E. 2012. Tietoturvaohjeistus Fujitsu Finland Oy:n käyttötukeen. Turun ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö. http://urn.fi/URN:NBN:fi:amk-2012120418215. 4.4.2017.

Sherman, M. 2016. Ransomware Do's and Don'ts: Protecting Critical Data 18.2.2016. https://www.symantec.com/connect/blogs/ransomware-dos-and-donts-protecting-critical-data. 27.3.2017.

Sipilä, J. 2014. Aviomies vakoili vaimonsa tietokonetta kuukausia http://www.mtv.fi/uutiset/rikos/artikkeli/aviomies-vakoili-vaimonsa-tietokonetta-kuukausia/4562404. 30.10.2016

Snow, J. 2016. Bye-bye, TeslaCrypt: Grand finale 19.5.2016. https://blog.kaspersky.com/teslacrypt-master-key/12160/. 29.3.2017.

Sophos. 2015 The current state of ransomware: TorrentLocker. https://blogs.sophos.com/2015/12/23/the-current-state-of-ransomware-torrentlocker/.19.12.2016.

Speed Guide Inc. 2016. Port 53 Details. http://www.speedguide.net/port.php?port=532 20.9.2016.

Symantec. 2016. Ransom.Cryptowall. https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99&tabid=2. 18.12.2016.

Symantec. 2015. What is the difference between viruses, worms, and Trojans? https://support.symantec.com/en_US/article.TECH98539.html. 28.8.2016.

Ward, M. 2016. 'Alarming' rise in ransomware tracked. http://www.bbc.com/news/technology-36459022. 25.11.2016.

Viestintävirasto. 2015. [Teema] Exploit kit - tehokas haittaohjelmien levittäjä. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/03/ttn201503061108.html. 18.12.2016.

Wueest, C. 2015. Underground black market: Thriving trade in stolen data, malware, and attack services. https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services. 17.10.2016.

Zamora, W. 2016a. How to tell if you’re infected with malware . https://blog.malwarebytes.com/101/2016/05/how-to-tell-if-youre-infected-with-malware/ 8.2.2017.

Zamora, W. 2016b. 10 easy ways to prevent malware infection (Blogi).. https://blog.malwarebytes.com/101/2016/08/10-easy-ways-to-prevent-malware-infection/. 15.3.2017.

Zetter, K. 2016. 4 Ways to Protect Against the Very Real Threat of Ransomware https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/. 15.3.2017.