Opinnäytetyö (AMK)

Tietojenkäsittely

2021

Jan Stockfelt

WANNACRY JA SEN VAIKUTUKSET TIETOTURVAAN

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely tradenomi

2021 | 44 sivua

Jan Stockfelt

WannaCry ja sen vaikutukset tietoturvaan

Tämän opinnäytetyön tavoitteena oli selvittää, mikä on WannaCry-kiristyshaittaohjelma ja miksi se oli niin merkittävä vuonna 2017 tapahtuneessa verkkohyökkäyksessä. Opinnäytetyön tavoitteena oli myös selvittää, miten WannaCryn aiheuttama hyökkäys vuonna 2017 vaikutti yritysten tietoturvakäytäntöihin.

Opinnäytetyön tutkimuksessa käytettiin pääsääntöisesti hyväksi tietoturvayritysten (F-Secure, Sophos ja Kyberturvallisuuskeskus) tietoturvaraportteja ja artikkeleita, joita analysoimalla tutkin kiristyshaittaohjelmien kehitystä. Tämän lisäksi aineistoa saatiin erilaisista artikkeleista ja tutkimuksista, missä on seurattu yritysten rahankäyttöä tietoturvatuotteisiin ja -palveluihin.

Opinnäytetyön tuloksena saatiin informaatiota kiristyshaittaohjelmien käytön kehityksestä vuosina 2018–2020 ja vastauksen, ovatko yritykset alkaneet käyttämään lisää resursseja tietoturvatuotteisiin ja -palveluihin.

Johtopäätöksinä voi todeta, että kiristyshaittaohjelmistot ovat kehittyneet ja yleistyneet, mutta samanaikaisesti yritykset panostavat yhä suurempia summia tietoturvapalveluihin ja -tuotteisiin.

Asiasanat:

tietoturva, haittaohjelma, verkkohyökkäykset, media, kiristysohjelma

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Business Information Technology

2021 | 44

Jan Stockfelt

WannaCry and its implications for information security

The aim of this thesis was to find out what is the WannaCry ransomware and why was it so significant in the 2017 cyberattack. Thesis aim was also to find out how the attack caused by WannaCry in 2017 affected companies’ information security practices.

The research of the thesis mainly utilized security reports and articles of the cybersecurity companies (F-Secure, Sophos and the Finnish National Cyber Security Center), which I was able to analyze to examine the development of the ransomware. In addition to these, material was obtained from various articles and studies where companies’ spending on the information security products and services has been monitored.

The results of the thesis were information on the development of the use of blackmail malware in 2018-2020 and an answer to whether companies have started to invest more resources into information security.

In conclusion, ransomware has evolved and become more widespread in use, while companies are investing more resources into security services and products.

Keywords:

information security, malware, cyber-attacks, media, ransomware.

Sisältö

Käytetyt lyhenteet ja sanasto

Bitcoin	Bitcoin on avoimen lähdekoodin sähköinen kryptovaluutta.
IoT	Internet of Things eli IoT, on Internetiin kytketty laite. Esimerkiksi IP-kamera tai sensorit.
Kryptolouhinta	Kryptolouhinta on tapa saada luotua kryptovaluuttaa, kuten bitcoinia.
Skripti/Script	On sarja valmiiksi kirjoitettuja automaattisia komentoja tai toimintoja tietokoneelle. Käytetään helpottamaan tai nopeuttamaan toistuvien komentojen toteutusta.

1 Johdanto

Kiristysohjelmistojen käyttö on massiivisesti kasvanut viimeisen neljän vuoden aikana. Pelkästään vuoden 2021 aikana on nähty räjähdysmäinen ero hyökkäysyritysten määrässä, ja näillä näkymin 2021 tulee olemaan suurin vuosi kiristysohjelmistojen aiheuttamissa hyökkäyksissä verrattuna aikaisempiin vuosiin. Kiristyshaittaohjelmistot ovat todettu toimivaksi tavaksi hyökätä yrityksiä ja vaikkapa eri valtioiden tietojärjestelmiä vastaan. (Seals 2021.)

Tämän opinnäytetyön tavoitteena on selvittää, mitä ovat kirityshaittaohjelmistot, mikä on WannaCry-kiristyshaittaohjelma ja millaisia vaurioita WannaCry aiheutti vuonna 2017 tapahtuneessa laajassa verkkohyökkäyksessä. Tutkin myös mahdollisia ongelmia, jotka saattoivat edesauttaa hyökkäyksen onnistumisessa.

Opinnäytetyössä pyrin myös selvittämään, miten yritysten tietoturvakäytännöt ovat muuttuneet vuoden 2017 jälkeen. Ovatko yritykset paremmin varautuneet vastaavanlaiseen hyökkäykseen vai onko kenties vielä isoja puutteita tietoturvakäytännöissä?

Opinnäytetyössä on myös selvitetty, mikä on kiristyshaittaohjelmisto sekä kiristysohjelmistojen historiaa ja toiminnallisuutta. Kiristyshaittaohjelmistojen historiaa tutkin AIDS, Cryptolocker ja Locky haittaohjelmistojen avulla. Lopulta esitän ajankohtaisia korjausehdotuksia, joiden avulla pyritään estämään kiristyshaittaohjelmistojen vapaa leviäminen tietojärjestelmän sisällä.

Opinnäytetyön lähteinä on pääsääntöisesti käytetty materiaalia, joka löytyy Internetistä ja jonka on mieluiten julkaissut joku tunnettu tietoturvatalo, kuten McAffee, F-Secure, Kaspersky jne. Näin pyrin varmistamaan, että materiaali on tarkkaa ja ajankohtaista.

2 Kiristyshaittaohjelma

Kiristyshaittaohjelma (engl. Ransomware) on haittaohjelmien alalahkoon kuuluva ohjelmisto, jonka tavoitteena on päästä käyttäjän tai yrityksen tietojärjestelmään. Tietojärjestelmä voi tässä tapauksessa olla esimerkiksi yksittäisen henkilön tietokone tai yrityksen tietokanta. Tietojärjestelmään päästyään ohjelman tehtävänä on salata tärkeitä tiedostoja, ohjelmistoja tai muuta kriittistä dataa, jolloin tietokoneen käyttäminen estyy tai muilla tavoin hankaloituu. Tämän jälkeen hyökkääjä pyrkii kiristämään lunnaita vastineeksi siitä, että tiedostojen salaus avataan. Lunnasvaatimukset tehdään usein bitcoin kryptovaluutta käyttäen johtuen siitä, kuinka vaikeata virtuaalivaluutan siirtoja on seurata verrattuna normaaliin rahaliikenteeseen. (McAfee LLC, 2018.)

Yrityksiä vastaan on myös kehittynyt variaatio ransomwaresta, jota kutsutaan englantilaisella nimellä ”extortionware”. Molemmat ohjelmistot toimivat samalla periaatteella, mutta ohjelmistojen tavoitteet ovat hieman erilaiset. Exortionwaren tehtävänä on urkkia selville yrityksen salaisuuksia, esimerkiksi varastamalla, huijaamalla tai muilla tavoin vakoilemalla. Tiedostoja ja tietokantoja ei yleensä salata, jotta ohjelmisto pystyy leviämään ja toimimaan mahdollisimman pitkään huomaamatta. Lopulta, kun hyökkääjät ovat mielestään varastaneet tarpeeksi informaatiota tai tarpeeksi tärkeätä informaatiota, ottavat he yhteyttä yritykseen ja uhkaavat paljastaa varastetut salaisuudet, ellei lunnaita makseta. Vaikka tämän tyyppinen hyökkäys ei yleensä aiheuta mitään isompia tuhoja tietojärjestelmille, on yritysten salaisuuksien leviäminen silti ongelmallista, ja välillä erittäin haitallista kilpailun kannalta. (Daniels 2021.)

2.1 Historia

Kiristyshaittaohjelmistojen historiaa voidaan seurata vuoteen 1989 asti, jolloin ensimmäinen tunnettu kiristyshaittaohjelmisto eli AIDS troijalainen tavattiin. Tässä kappaleessa pyrin käymään läpi erilaisten kiristyshaittaohjelmistojen historiaa ja kehitystä. Vaikka kappaleen nimi on historia, en pyri käymään läpi

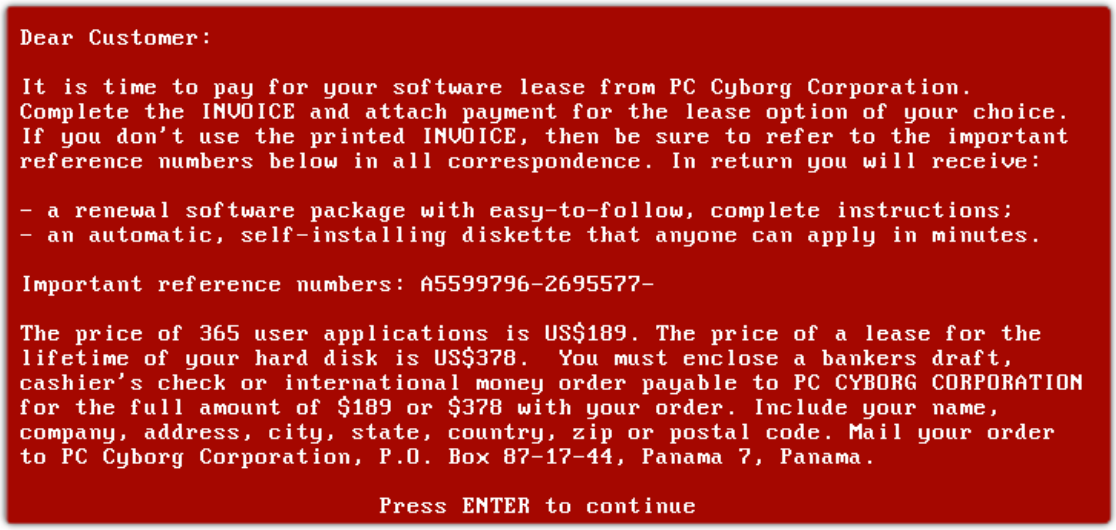
jokaista mahdollista variaatiota kyseisistä ohjelmistoista, vaan sen sijaan pyrin nopeasti katsomaan läpi omasta mielestä mielenkiintoisimpia tapauksia, jotka ovat tapahtuneet ennen WannaCryn ilmestymistä. Näiden esimerkkien avulla saadaan peruslähtökohta, sille mitä kiristyshaittaohjelmat ovat kykeneviä tekemään ja millaisia tuhoja näillä pystytään aiheuttamaan.

2.1.1 AIDS Troijalainen haittaohjelma

AIDS Troijalaista voidaan pitää ensimmäisenä tunnettuna kiristysohjelmistona, joka on päässyt merkittävästi leviämään käyttäjien tietokoneissa. Alkuperäisesti vuonna 1989 levitettyä haittaohjelmaa pidetäänkin tästä syystä vanhimpana tunnettuna kiristyshaittaohjelmistona. AIDS Troijalaista levitettiin postittamalla käyttäjille AIDS/HIV virustautiin liittyvää kyselylevykettä. Levyke sisälsi myös AIDS Troijalaisen, jonka tehtävänä oli salata osia uhriksi joutuneen käyttäjän tietokoneesta, jolloin tietokoneen käyttö estyi tai muilla tavoin häiriintyi. Levykkeitä epäillään joutuneen noin 20 000 ihmisen postituslistalle. (VirusBulletin 1990.)

AIDSin toiminta perustuu käyttäjän luottoon liittyen levykkeen sisältämään ohjelmistoon. Levykettä asennettaessa ei käyttäjälle heti ilmene, että olisi tehnyt jotakin väärin. AIDS Troijalainen on ohjelmoitu tavalla, jolla se pitää kirjaa tietokoneen uudelleenkäynnistysmäärästä, ja jos uudelleenkäynnistysmäärä ylittää sallitun rajan alkoi ohjelmisto salaamaan osia käyttäjän tietokoneesta. (VirusBulletin 1990.)

Uudelleenkäynnistyksen rajat saattoivat vaihdella, mutta yleensä noin 90 käyttökerran jälkeen alkaa ohjelmiston varsinainen toiminta. Käyttökertojen määrän ylittyessä, ohjelmisto pyrkii piilottamaan ja salaamaan kaiken tiedon C: aseman sisältä. Tämän jälkeen käyttäjälle näytetään ilmoitusta, että ohjelmiston lisenssiaika on päättynyt ja pyydetään uusimaan lisenssi (Kuva 1). Jos lisenssiä ei makseta, ei myöskään tietokoneen tiedostoja avata. (Bates 1990.)



Kuva 1. AIDS troijalainen aktivoitunut: (Popp 1989).

AIDS ohjelmiston heikkoudeksi paljastui lopulta tämän yksinkertainen tapa salata tiedostoja, ja ohjelmiston käyttämän salauksen heikkolaatuisuus. Salauksen heikkouteen vaikutti merkittävästi se, että haittaohjelma ei pyri salaamaan koko tiedoston sisällä olevaa dataa, vaan pelkästään tiedoston nimen ja tämän käyttämän tiedostopäätteen. Tiedostot myös asetettiin piilotetuiksi, mutta lopulta itse tiedostojen sisällä olevaan dataan ei kosketa ja se on yhä luettavissa. Ohjelmiston levittäminen oli myös erittäin hidasta verrattuna nykyaikaisiin kiristyshaittaohjelmiin, johtuen tarpeesta lähettää fyysisiä levykkeitä postitse käyttäjille. (Bates 1990.)

Haittaohjelman poistamista varten on luotu ohjelmistot AIDSOUT ja CLERAID. AIDSOUT on ohjelma, jonka avulla käyttäjä pystyy poistamaan haittaohjelmiston koneeltaan. CLEARAID on ohjelma, jonka avulla voidaan avata jo salatut tiedostot ilman, että kiristäjälle tarvitsee maksaa lunnasrahoja. (Bates 1990.)

2.1.2 Cryptolocker-kiristyshaittaohjelma

Cryptolocker on vuonna 2013 levinnyt Troijalainen kiristyshaittaohjelmisto, jota levitettiin osana Gameover Zeus- bottiverkon hyökkäyksiä. Cryptolocker yleensä saapui tietokoneelle sähköpostin liitetiedostona, jonka käyttäjä on ladannut taikka

avannut. Cryptolockerin kohteena ovat vain Windows-käyttöjärjestelmää käyttävät tietokoneet ja laitteet, ja esimerkiksi Mac-laitteissa haittaohjelma ei toiminut. Cryptolockerin uskotaan iskeneen yli 230 000 tietokoneeseen, ja mahdollisesti onnistunut saamaan yli 27 miljoonan dollarin edestä lunnasrahoja. (Kaspersky 2018.) (Department of justice 2014.)

Cryptolockerin sisältävän liitteen käynnistyessä pyrkii haittaohjelma etsimään tiedostoja tietokoneen kovalevyltä, medialaitteilta kuten USB-tikuilta ja ulkoisilta kovalevyilta, sekä etsimään mahdollisia verkkolevyjä tai pilvipalveluita mihin tietokone on mahdollisesti yhteydessä. Tämän jälkeen haittaohjelmisto pyrkii salaamaan tiedostot löydetyistä lähteistä käyttäen epäsymmetristä salausta. Epäsymmetrisessä salauksessa luodaan yksi julkinen ja salainen avain, joita käytetään joko tiedostojen salaamiseen tai avaamiseen. Hyökkääjät salaavat tiedostot käyttäen julkista avainta, mutta ottavat itse talteen kiristystä varten salaisen avaimen. Salaisen avaimen käyttö on ainoa tapa saada avattua salatut tiedostot. Tämän jälkeen ohjelma näyttää lunnasikkunan uhriksi joutuneelle käyttäjälle, jossa uhataan, että salainen avain tuhotaan, ellei lunnaita makseta ennen määräajan loppumista (Kuva 2). (Kaspersky 2018.)

Kuva 2. Cryptolockerin lunnasikkuna (Grigorik 2017).

Haittaohjelmaa levitettiin Gameover ZeuS -bottiverkkoa käyttäen. Bottiverkolla tarkoitetaan Internetiin kytkettyjä laitteita, jotka ovat saastuneet haittaohjelman tartunnan vuoksi. Saastuneita laitteita pystytään tämän jälkeen käyttämään koordinoidusti nettihyökkäystoimintaa varten. Gameover Zeus -bottiverkon avulla pystyttiin lähettämään päivittäin roskapostia tuhansilla laitteilla, ja täten tehokkaasti levittämään Cryptolockeria. (Belcic 2020) (Cybersecurity & infrastructure security agency 2014.)

Cryptolockerin poistaminen on yksinkertaista. Haittaohjelman tultua yleiseen tietoon pystyi perinteinen virustorjuntaohjelmisto tunnistamaan ja poistamaan haittaohjelmiston. Ongelmaksi monille tulikin, että haittaohjelmiston poistaminen ei avaa jo Cryptolockerin salaamia tiedostoja, vaan ainoastaan salaisen avaimen saaminen pystyy takaamaan tiedostojen täydellisen palauttamisen. (Belcic 2020.)

Haittaohjelman leviäminen saatiin pysäytettyä, kun useat tietoturvayhtiöt ja valtioiden lainvalvojat alkoivat tekemään yhteistyötä, jolla Gameover Zeus -bottiverkko saataisiin suljettua. Vuonna 2014 Yhdysvaltain oikeusministeriö ilmoitti, että Gameover Zeus -bottiverkon komento- ja ohjauspalvelimet oli saatu hallintaan, joka tehokkaasti pysäytti haittaohjelman leviämisen. (Department of justice 2014.)

Vaikka alkuperäinen versio Cryptolockerista ei ole toiminnassa, on kyseisestä haittaohjelmasta olemassa lukuisia erilaisia versioita ja jäljitelmiä, jotka ovat yhä toiminnassa. (Belcic 2020.)

2.1.3 Locky-kiristyshaittaohjelma

Locky on kiristyshaittaohjelma, joka ensimmäisen kerran tavattiin vuonna 2016. Locky pyrkii käyttäjän manipuloinnin avulla pääsemään uhrin sähköpostista tämän tietokoneelle, ja tämän jälkeen suorittamaan ohjelmiston ensisijaisen tavoitteen, joka on salata käyttäjän tiedostot ja vaatia lunnaita tiedostojen avaamista vastaan. (Belcic 2019.)

Lockyn pääsääntöinen hyökkäysvektori on sähköpostin liitetiedostojen kautta latautuminen. Usein tämä tapahtuu lataamalla haittaohjelmalla saastutettu Word dokumentti tietokoneelle. Tämän jälkeen, käyttäjän manipulointitaktiikoiden avulla, dokumentti pyrkii saamaan käyttäjän käynnistämään Wordin makro-ominaisuuden. Jos makro-ominaisuuden käynnistää, tulee käynnistäneeksi haitallisen skriptin eli automaattisen käskyjonon tietokoneen toimintoja tai komentoja, joka tämän jälkeen lataa uusimman version Locky-haittaohjelmistosta tietokoneelle. (Belcic 2019.)

Lockysta tekee erittäin vaarallisen sen ominaisuus salata monenlaisia tiedostoja ja ohjelmistoja. Tiedostot voivat olla esimerkiksi Office ohjelmistojen yleisesti käyttämiä kuten Word, PowerPoint, Excel ja pdf. Videotiedostot ja vastaavat ovat myös salauksen mahdollisia kohteita. Lockyllä on myös ominaisuus minkä avulla se pyrkii sekoittamaan Windowsin system32-hakemiston tietoja, mikä takaa sen, ettei tietokonetta pysty tämän jälkeen käyttämään normaalisti. Haittaohjelma vaihtaa tiedostojen nimet, ja tiedostojen laajennuksiin esim. .doc ja .pdf tulevat uudet tiedoston päätteet. Näitä päätteitä voivat olla esimerkiksi thor ja locky. Salauksen jälkeen Locky näyttää uhriksi joutuneelle käyttäjälle sen lunnasvaatimukset ja ohjeet miten kyseiset rahat tulee toimittaa kiristäjille. Kuten monet muutkin uudemmat kiristyshaittaohjelmat, pyydetään lunnaita bitcoineina. (Belcic 2019.)

Lockyn poistaminen on lopulta melko yksinkertaista. Jokainen päivitetty virustorjuntaohjelmisto pystyy poistamaan haittaohjelman tietokoneelta. Vaikka ohjelmiston poistaa, on vahinko aiheutunut. Tiedostot, jotka Locky on jo päässyt salaamaan pysyvät salattuina. Ainoa tällä hetkellä tunnettu tapa saada tiedot avattua on lunnasrahojen maksaminen, tosin rahojen maksaminen ei takaa tiedostojen takaisinsaantia, koska hyökkääjillä ei ole mitään tarvetta olla rehellisiä ja toimittaa salauksenpurkuavainta. (Belcic 2019.)

2.2 Yhteenveto

Aikaisemman kappaleen esimerkeistä pystytään tekemään muutamia johtopäätöksiä. Ensimmäinen ja tärkein on, että kiristyshaittaohjelmistoja luodaan pääsääntöisesti, jotta hyökkääjät pystyvät hyötymään taloudellisesti. Motiivina on yleensä mahdolliset lunnasvaatimukset tai pelko salaisuuksien levittämisestä, jonka avulla hyökkääjät pyrkivät hyötymään rahallisesti.

Toisena voidaan päätellä, että kiristyshaittaohjelmistot alkoivat rajusti yleistymään 2000-luvun Internetin käytön yleistymisen johdosta. Kiristyshaittaohjelmissa alettiin myös käyttämään parempia ja monimutkaisempia salausmenetelmiä, jonka avulla pystyttiin varmistamaan, että uhriksi joutunut käyttäjä ei pysty purkamaan tiedostojen salausta ilman, että maksaa lunnasrahat.

Kolmantena kryptovaluuttojen yleistyminen, etenkin bitcoinin takaa sen, että lunnasrahoja on yksinkertaista vaatia, mutta samalla se luo hyökkääjälle anonymiteetin. Jos rahavirtoja ei voida seurata, on lähes mahdotonta selvittää hyökkäyksen alkuperä ja mahdollinen tekijä. Tämä takaa sen, että hyökkäyksien tekeminen on paljon riskittömämpää kuin olettaisi, ja vasta usean maan hallituksien ja tietoturvayhtiöiden voimat, kuten Cryptolockerin tapauksessa, voi olla edellytyksenä, että tekijät saadaan kiinni ja vastuuseen teoistaan.

Viimeisenä pystytään tekemään johtopäätös, että kiristyshaittaohjelmat voivat aiheuttaa massiivista tuhoa, jos haittaohjelma pääsee kiinni kriittiseen dataan. Lockyn tapauksessa haittaohjelma pääsi leviämään Hollywoodin sairaalaan potilastietokantaan, ja sairaalan oli lopulta maksettava yli 17 000 dollarin lunnasrahat. Haittaohjelman osuessa kriittiseen infrastruktuuriin on kynnys maksaa lunnasrahat paljon matalampi, koska mahdolliset seuraukset siitä, että ei maksa voivat olla paljon suuremmat yrityksen toiminnan kannalta. (Winston 2016.)

3 WannaCry-kiristyshaittaohjelma

WannaCry on vuonna 2017 yleiseen tietoon tullut kiristyshaittaohjelma, joka oli osana laajaa verkkohyökkäystä, jolla saastutettiin satojatuhansia Windows-pohjaisia tietokoneita yli 150 maassa. Mikä tekee WannaCryn leviämisestä merkittävän, on kuinka nopeasti ohjelmisto pääsi leviämään. Verkkohyökkäys kesti noin 4 päivää, mutta sen aiheuttamat tuhot noina neljänä päivänä olivat erittäin suuret. (Laotto 2020.)

Ohjelmiston leviämiseen vaikutti merkittävästi EternalBlue-haavoittuvuus Windows-käyttöjärjestelmissä. Kyseisen haavoittuvuuden oli kehittänyt Yhdysvaltojen Kansallinen turvallisuusvirasto eli NSA. Shadow Brokers -niminen ryhmä oli onnistunut varastamaan ja levittämään haavoittuvuuden yleiseen tietoon noin vuosi ennen varsinaisen hyökkäyksen tapahtumista, ja kyseinen haavoittuvuus oli myös korjattu uusimmassa Windowsin versiossa. Valitettavasti useat käyttäjät ja organisaatiot eivät olleet päivittäneet käyttöjärjestelmiään, minkä vuoksi useat käyttöjärjestelmät olivat yhä alttiita hyökkäykselle. (F-Secure 2017.)

3.1 EternalBlue-haavoittuvuus

EternalBlue on tietoturvahaavoittuvuus, joka antaa hyökkääjälle kyvyn suorittaa etänä haitallista koodia ja tällä tavoin saada pääsyn toisen osapuolen tietoverkkoon. Hyökkäys toimii lähettämällä erityisesti luotuja datapaketteja ja käyttäen hyväksi Microsoft Windows-käyttöjärjestelmää, jossa on käytössä ”Server Message Block” (SMB) -protokolla. Hyökkäyksen onnistuminen vaatii vanhaa SMBv1 -versioita ja siinä olevaa heikkoutta toimiakseen. (Cisecurity.org 2019.)

Server Message Block (SMB) on tiedoston jakoon liittyvä verkkoprotokolla, jonka avulla tietokoneen ohjelmistot voivat lukea, kirjoittaa sekä pyytää palveluita mahdollisesti verkossa olevilta muilta laitteilta. Käytännön esimerkkejä on monia,

mutta perinteinen tiedon tallentaminen tietokantaan tai tulostimen käyttö voi olla osa SMBtä. (Microsoft 2016.)

Mikä tekee EternalBlue-haavoittuvuudesta erittäin riskialttiin, on sen kyky mahdollisesti saattaa koko tietoverkko ja kaikki siihen liitetyt laitteet alttiiksi hyökkäykselle. Haittaohjelma, joka käyttää EternalBlue-haavoittuvuutta vaatii ainoastaan yksittäisen saastuneen laitteen, joka on kytkettynä yrityksen tietoverkkoon. Tämän jälkeen on mahdollista, että kaikki laitteeseen liitetyt ja samaan verkkoon kuuluvat laitteet ovat vaarassa joutua haittaohjelman hyökkäyksen kohteeksi. Tämä tekee myös mahdollisista tuhoista palautumisen ja korjauksen vaikeaksi. Haittaohjelman leviämisen pysäyttämiseksi, on tärkeää sulkea koko tietoverkko. Muussa tapauksessa haittaohjelma pystyy vieläkin leviämään laitteesta toiselle, joten osittainen sulkeminen ei ole toimiva tapa korjata haittaohjelman tekemiä tuhoja. (Cisecurity.org 2019.)

EternalBlue-haavoittuvuudesta tekee erittäin mielenkiintoisen se tieto, että kyseisen haavoittuvuuden oli alun perin kehittänyt NSA osana heidän tavoitettaan kerätä erilaisia tietoturvahaavoittuvuuksia. (Burdova 2020). Haavoittuvuus oli luotu tavalla, jonka avulla sitä pystyi käyttämään erittäin laajasti ja luotettavasti monissa eri Windows-ympäristöissä. Mikko Hyppönen F-Securelta kuvailee tätä termillä ”weapons grade”, koska kyseistä haavoittuvuutta oli erittäin helppoa ja tehokasta soveltaa monissa haittaohjelmissa (F-Secure 2017).

Haavoittuvuuden toi julkiseen tietoon hakkeriryhmä nimeltä ”Shadow Brokers”, joka oli onnistunut murtautumaan NSAn tietojärjestelmään ja varastamaan satojen megatavujen edestä erilaisia hyökkäystyökaluja. Murtautuminen piti sisällään myös EternalBlue-haavoittuvuuden ja siihen liittyvät työkalut (F-Secure 2017.). Microsoft korjasi haavoittuvuuden noin kuukausi sen jälkeen, kun Shadow Brokers ryhmä julkaisi haavoittuvuuden Internetiin kaikkien saataville (Microsoft 2020).

3.2 WannaCryn toiminta

3.2.1 WannaCryn Leviäminen

Alkuperäinen leviämistapa 2017 hyökkäyksessä oli skannata Internetissä olevia avoimia SMB-portteja, ja sitä kautta pyrkiä levittämään ohjelmistoa käyttäen hyväksi EternalBlue-haavoittuvuutta. EternalBlue-haavoittuvuuden ansioista hyökkääjän ei tarvitse kuin löytää muutama haavoittunut ja avonainen SMB-portti Internetistä, ja tällä tavoin ohjelmiston leviäminen on saatu aloitettua. (F-Secure 2017.)

WannaCry-haittaohjelmisto toimii verkkomatona, joka tarkoittaa sitä, että yhden laitteen saastuttamisen jälkeen ohjelma pyrkii leviämään seuraavaan aukinaiseen verkosta löytyvään laitteeseen, ja tämän jälkeen toistamaan prosessin. Tämä tapahtuu ohjelman asentamisen jälkeen, jolloin WannaCry pystyy skannaamaan verkossa olevat laitteet ja leviämään seuraavalle laitteelle käyttäen EternalBlue-heikkoutta. Tämän jälkeen ohjelma käyttää Doublepulsar-nimistä työkalua, joka aiheuttaa sen, että WannaCry pystyy asentumaan ja käynnistämään itsensä ilman, että kenenkään tarvitsee vuorovaikuttaa sen toimintaan. (Laotto 2020.)

Kyseinen toiminnallisuus takaa sen, että ohjelmisto pystyy leviämään erittäin nopeasti yrityksen verkossa ja ilman, että hyökkääjän tarvitsee tehdä mitään edesauttaakseen hyökkäyksen onnistumista.

WannaCryn leviämisellä oli myös heikkous, jonka avulla haittaohjelman leviäminen saatiin pysäytettyä. WannaCryn ohjelmistokoodiin oli luotu ominaisuus, millä ohjelmiston leviäminen pystytiin tarvittaessa pysäyttämään. Tämän niin sanotun ”kill switch” toiminnon löysi Marcus Hutchins perjantaina 12.5.2017 vain muutama tunti sen jälkeen, kun WannaCryn hyökkäys oli alkanut. WannaCryn saapuessa uhriksi valikoituneelle tietokoneelle, se pyrkii ensimmäisenä ottamaan yhteyttä tiettyyn yksittäiseen verkkosivustoon ja

saamaan sieltä vastauksen. Jos WannaCry ei saanut vastausta verkkosivustolta, ohjelmisto jatkoi normaalisti toimintaansa, mutta jos sivusto antoikin vastauksen, WannaCry lopetti yllättävästi toimintansa, eikä se pyrkinyt enää tekemään haitallisia toimintoja tietokoneella. (F-Secure 2017.)

Täyttä varmuutta ei ole, miksi WannaCrylla ylipäätänsä oli kyseinen toiminto. Tätä toiminnallisuutta epäillään tehdyksi siksi, että sillä pystyttäisiin välttämään mahdollisten tietoturvayritysten pyrkimyksiä tutkia millainen ohjelma WannaCry on. Tietoturvayritykset käyttävät erilaisia ns. ”Sandbox”-testausmenetelmiä. Näiden avulla pyritään tutkimaan haittaohjelmia, ja suorittamaan haittaohjelmille kaikki tarvittavat pyynnöt turvallisessa ympäristössä. Tästä syystä WannaCry pystyi selvittämään, oliko ohjelma mahdollisesti tietoturvayrityksen Sandboxin sisällä, jos ohjelma saikin yllättäen pyyntöön vastauksen. On myös epäilty, että hyökkääjät halusivat vain yksinkertaisen tavan, jolla pystyi tarvittaessa estämään WannaCryn leviämisen. (F-Secure 2017.)

3.2.2 Salaus ja lunnasvaatimus

WannaCryn asentuessa tietokoneelle kiristyshaittaohjelma pyrkii salaamaan tietokoneella olevat tärkeät tiedostot käyttäen RSA 2048-salausta. RSA on julkisen avaimen salausalgoritmi. Kyseistä salausta käytetään laajasti esimerkiksi turvallisen tiedon välittämiseen. RSA toimii luomalla kaksi erillistä avainta, toinen salainen ja toinen julkinen. Julkisella avaimella voidaan salata viestejä ja salaisella avaimella voidaan niitä avata. WannaCryn tapauksessa julkista avainta käytetään salaamaan tietokoneella olevat tiedostot, kun taas salaisen avaimen vievät kiristäjät omaan tietokantaansa ja näin takaavat sen, että salausta ei voi poistaa ilman, että maksaa lunnasrahat. Salaus on erittäin vahva ja tiedostojen avaaminen muulla tavoin kuin avainta käyttäen ei ole mahdollista nykytekniikalla. (Martin & al. 2017)

Sillä välin, kun tiedostoja salataan, pyrkii WannaCry luomaan tiedostoja, joiden sisälle se asentaa ohjelmistoja ja työkaluja. Ohjelmistojen ja työkalujen avulla se pystyy poistamaan uhrin tietokoneelta mahdollisia varmuuskopioita. Tämä

tehdään siitä syystä, ettei uhriksi joutunut vahingossa pystyisi palauttamaan tiedostojaan ennen kuin lunnasrahat on maksettu. Ohjelma myös pyrkii tor-verkkoa käyttäen tekemään toimintojansa anonyymina, joka takaa sen, että ohjelman toimia on hankalampi seurata. (Martin & al. 2017)

Tämän jälkeen, kun tiedostojen salaaminen on valmis, näyttää ohjelmisto lunnasvaatimusikkunan (kuva 3). Lunnasvaatimukset ovat aina bitcoineina, joka vastasi 2017 noin $ 300 dollaria. Lunnasvaatimuksen hinta nousi 3 päivän sisällä $ 600 dollariin jos lunnaita ei ollut vielä maksettu. Lopulta 7 päivän jälkeen ohjelma ilmoittaa, että tiedostot katoavat kokonaan. (Laotto 2020.)

Kuten muissakin kirityshaittaohjelmissa, haittaohjelman poistaminen itsessään jälkikäteen ei ole monimutkainen ongelma, mutta salauksen purkaminen ilman salausavainta ei ole yleensä mahdollista. Lunnaiden maksaminenkaan ei takaa, että tiedostot saa myöhemmin avattua. On myös epäilty, että WannaCryn tapauksessa hyökkääjillä ei ole ollut mitään aikomusta avata uhrien tiedostoja, kun lunnaat oli maksettu. (Laotto 2020.)

Kuva 3. WannaCryn lunnasvaatimusikkuna (Wikipedia 2017).

3.3 Media ja vaikutus

WannaCryn vaikutus oli merkittävä. WannaCryn avulla saastutettiin yli 200 000 tietokonetta ja laitetta yli 150 maassa. Neljä pahiten hyökättyä maata olivat Venäjä, Ukraina, Intia ja Taiwan. Kohteita oli monia ja näihin kuuluu muun muassa valtion toimintoja, sairaaloita ja suuria yrityksiä. (F-Secure 2017) (Laotto 2020).

Espanjalainen Telefonica oli ensimmäisiä yrityksiä, joihin WannaCry iski. WannaCry iski yritykseen niin voimakkaasti, että työntekijöitä kehotettiin lopettamaan työskentely ja sulkemaan tietokoneet, jotta haittaohjelman leviäminen saataisiin pysäytettyä. Joidenkin lähteiden mukaan jopa 85 % yrityksen tietokoneista olisi saastunut WannaCry-kiristyshaittaohjelmiston johdosta. (Toledano 2017.)

Yksi suurimpia kohteita, jossa haittaohjelman hyökkäys koettiin, oli Iso-Britanniassa. National Health Service eli NHS on Iso-Britannian julkinen terveydenhoitopalvelu. Sairaaloiden tietojärjestelmät olivat niin saastuneet WannaCryn johdosta, että se aiheutti ongelmia normaaleissa toiminnoissa. Monet sairaalat peruivat rutiinitarkastuksia ja varoittivat, että sairaaloihin ei kannata tulla, ellei kysymyksessä ole hätätapaus. Potilaita lähetettiin kotiin, koska heidän sairaskertomuksiaan ei pystytty avaamaan, ja ambulansseja ei pystytty ohjaamaan oikeisiin osoitteisiin. (ABC.net.au 2017) (BBC.com 2017.)

Renault oli myös yksi yritys, joka kärsi WannaCrysta. WannaCryn takia Renault joutui pysäyttämään viisi sen tehdasta eri puolilla maailmaa, joko osittain tai kokonaan. Pysäyttämisen syynä oli haittaohjelman leviämisen estäminen ja isompien tuhojen välttäminen. (Frost, Tajitsu & Reuters 2017.)

WannaCrylla oli myöhemmin myös paljon poliittista vaikutusta. Etenkin Isossa-Britanniassa keskusteltiin, oliko NHS mahdollisesti alirahoitettu, koska se ei ollut kyennyt päivittämään järjestelmiään vastaamaan WannaCryn tapaisiin uhkiin. NHS onkin nostanut tietoturvaansa kohdistuvaa rahoitusta merkittävästi vuoden 2017 jälkeen. (Arthur 2017) (Hughes 2019.)

3.4 WannaCrylta suojautuminen

Yleisesti suurimmaksi hyväksytyksi syyksi minkä takia WannaCry pääsi leviämään laajalle ja nopeasti on yritysten haluttomuus päivittää heidän käyttöjärjestelmiänsä ja ohjelmistojaan. Microsoft oli päivittänyt Windows 7- ja Windows 10 -käyttöjärjestelmät ennen hyökkäyksen alkamista, mutta suurin osa yrityksistä, joihin haittaohjelma iski, eivät olleet tehneet tietoturvapäivityksiä. Pahimmassa tapauksessa yritykset käyttivät yhä vanhoja käyttöjärjestelmiä kuten Windows XP;tä, jonka tuki oli loppunut jo useita vuosia sitten. Tämän vuoksi myöhemmin myös Windows XP sai tietoturvapäivityksen EternalBlue-haavoittuvuutta vastaan. (F-Secure 2017) (Microsoft 2017.)

Yleiset suositellut käytännöt WannaCryn leviämisen ja tarttumisen estämiseksi ovat siis.

1. Päivitä käyttöjärjestelmä mahdollisimman uuteen versioon ja lataa kaikki tietoturvapäivitykset, jotka ovat saatavilla.
2. Älä koskaan klikkaa, avaa tai lataa epäilyttäviä linkkejä, sähköposteja tai muita vastaavia, joiden kautta haittaohjelma pystyy latautumaan tietokoneelle.
3. Vältä tuntemattomia USB-tikkuja tai muita medialaitteita, joiden sisällöstä et ole täysin varma.
4. Asenna tietoturvaohjelmisto tai jokin vastaava, ja pidä se päivitettynä.
5. Tärkein, etenkin kiristysohjelmien kannalta on tehdä säännöllisiä varmuuskopioita tiedoista, jotta tiedostot voidaan tarvittaessa palauttaa.

(Laotto 2020) (F-Secure 2017.)

4 WannaCryn vaikutus myöhempään tietoturvaan

WannaCry-hyökkäys vuonna 2017 oli yksi suurimpia ja onnistuneimpia kiristyshaittaohjelmiston tekemiä hyökkäyksiä. Tässä luvussa selvitetään, miten yritysten käytännöt ovat muuttuneet vuosien 2018–2020 aikana. Käytetäänkö kiristysohjelmistoja vielä samalla tavalla? Ovatko hyökkäysmetodit samat kuin vuonna 2017? Onko yritysten yleinen tietoturvataso parantunut vai kenties heikentynyt?

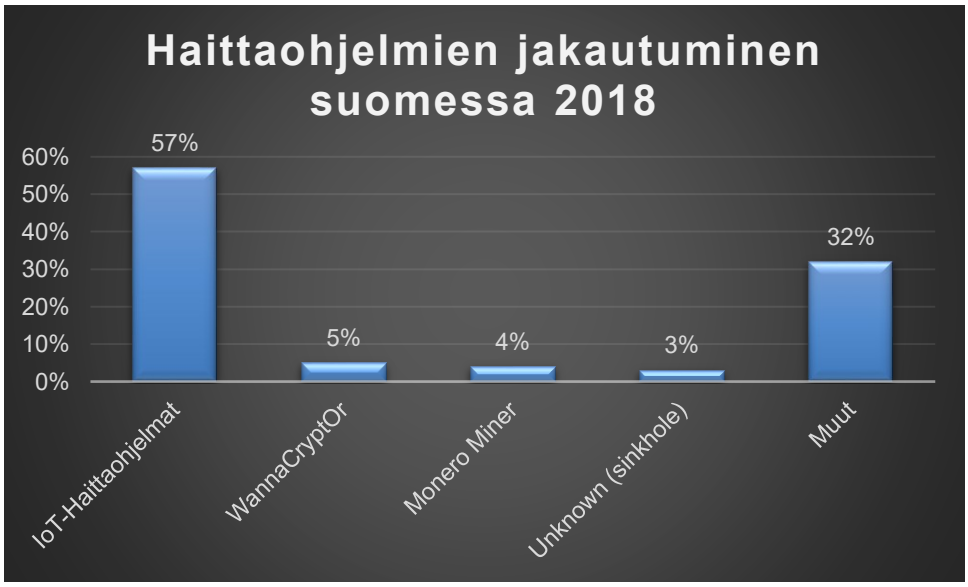
Aloitan tämän luvun vertailemalla vuosien 2018–2020 välistä dataa, ovatko kiristysohjelmistojen käyttömäärät laskussa vai nousussa. Tämän avulla pystyn selvittämään, onko kiristyshaittaohjelmien käyttö yhä järkevää. Sen jälkeen selvitän, ovatko hyökkäysmetodit samat kuin ennen. WannaCry käytti hyväkseen EternalBlue-haavoittuvuutta, joten ovatko haavoittuvuudet yhä laajassa osassa hyökkäyksiä vai ovatko metodit muuttuneet. Lopulta selvitän käyttävätkö yritykset enemmän resursseja tietoturvaan vai ovatko budjetit kenties pysyneet samalla tasolla.

4.1 Hyökkäysmetodit vuosien 2018–2020 aikana

Hyökkäysmetodien tutkimukseen käytetään yritysten tietoturvavuosiraportteja ja artikkeleita, josta käy ilmi erilaiset trendit ja millaisia hyökkäyksiä rikolliset suosivat. Valitut yritykset, joilta katson kyseisiä raportteja ovat Kyberturvallisuuskeskus, F-Secure ja Sophos. Kyberturvallisuuskeskus ja F-Secure sen takia, koska ne ovat suomalaisia, ja siksi niistä saatu data vastaan parhaiten siihen, millaisia uhkia suomalaiset yritykset kokevat. SophosLabs on valittu koska se julkistaa pääsääntöisesti uhkaraportteja, jotka keskittyvät haittaohjelmiin. Tämä sopii täydellisesti tutkittavaan ympäristöön, koska pyrin selvittämään kiristysohjelmistojen käyttöä enkä laajempia hyökkäysuhkia tässä opinnäytetyössä.

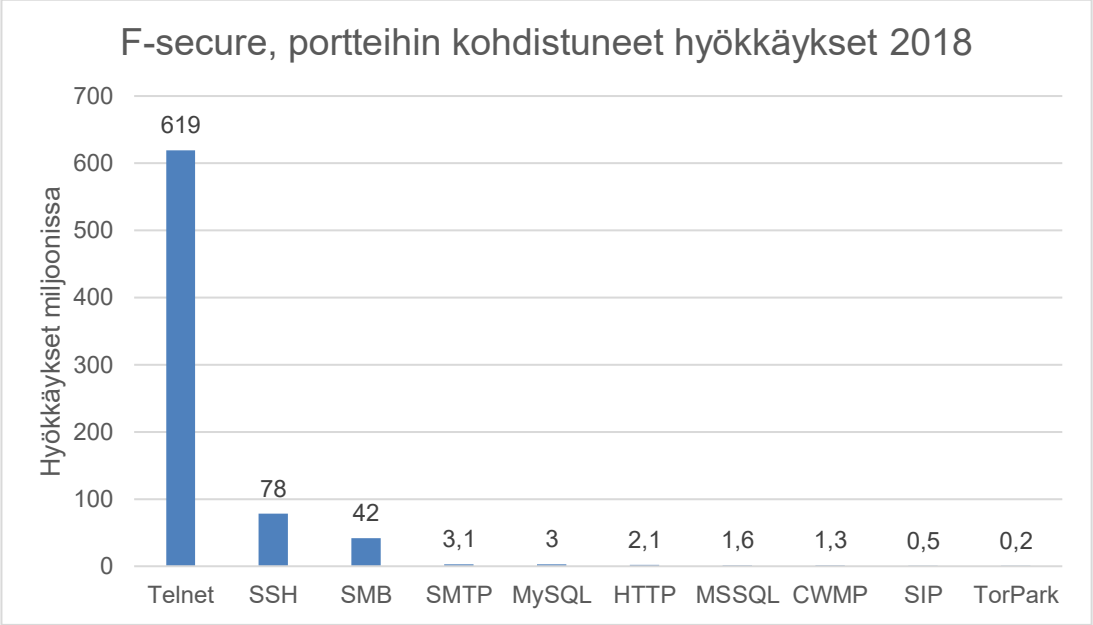
4.1.1 Vuosi 2018

Haittaohjelmien käyttö muuttui rajusti vuoden 2018 aikana. Jos vuotta 2017 voi pitää kiristysohjelmistojen vuotena oli vuosi 2018 pääsääntöisesti IoT-laitteisiin kohdistuvaa haittaohjelmien hyökkäämistä. (Kuva 4.) (Kyberturvallisuuskeskus 2018.)



Kuva 4. Haittaohjelmien jakautuminen suomessa vuonna 2018 (Kyberturvallisuuskeskus 2018).

F-Securen ja Sophoksen data tukee yllä olevaa näkymää. F-Securen kohtaamat hyökkäykset olivat suurelta osin kohdistettu Telnet ja SSH protokollaa vastaan, joista etenkin Telnet on erittäin yleisesti käytetty IoT laitteiden yhteydessä. (Kuva 5.) (F-Secure 2018b.)



Kuva 5. F-secure, portteihin kohdistuneet hyökkäykset miljoonissa. (F-Secure 2018b).

Kiristyshaittaohjelmistot olivat myös mukana vuoden 2018 hyökkäyksissä. Hyökkäysvektori oli tosin muuttunut paljon WannaCryn tapaisista EternalBlue-heikkouksiin kohdistuvista hyökkäyksistä. SMB portti 445 oli kuitenkin edelleen normaalia enemmän hyökätty verrattuna aikaisempiin vuosiin (F-Secure 2018b). Suurin vektori oli erilaiset sähköpostihuijaukset ja liitteet, jotka sisälsivät erilaisia haittaohjelmia tai dokumentteja. Liitteiden makrojen kautta latautui koneelle yleensä haittaohjelma. Yleisesti ottaen kiristyshaittaohjelmat eivät ole ensisijainen hyökkäyksen tavoite, vaan tavoitteena on ensin saada tietokoneelle mahdollinen lataus sovellus, botti tai takaportti, jonka kautta voidaan myöhemmin asentaa pankkitroijalaisia tai kiristyshaittaohjelmistoja. F-Securen dataa seuraten voi todeta, että vuonna 2018 erilaiset pankkitroijalaiset olivat paljon yleisempiä kuin kiristyshaittaohjelmistot. (F-Secure 2018c.)

Myös monet kryptolouhijat olivat paljon yleisempiä kuin mitä kiristyshaittaohjelmat. Tästä esimerkkinä on Lahdesta löytynyt WannaMine-niminen haittaohjelma, jonka avulla louhittiin Monero-nimistä virtuaalivaluuttaa.

WannaMine, kuten WannaCry, käyttää hyväkseen Eternablue-heikkoutta, mutta tämän lisäksi se käyttää myös hyväksi Mimikatz-nimistä ohjelmistoa, jonka avulla pystytään varastamaan käyttäjätunnuksia ja salasanoja, ja näin ollen leviämään myös verkoissa missä Eternablue on päivitetty. (F-Secure 2018a) (Kyberturvallisuuskeskus 2018.)

Kiristyshaittaohjelmien osalta on noussut isommaksi trendi murtautua yritysten verkkoihin manuaalisesti. Tämän jälkeen, kun suojaukset ja muut turvaohjelmistot on ajettu alas, hyökkääjät asentavat ja käynnistävät kiristyshaittaohjelmiston ja salaavat organisaation koko tietokannan ja muun mahdollisesti verkossa olevan tiedon. Tämän jälkeen kiristäjät ottavat yhteyttä sähköpostitse, ja vaativat lunnaita. Tästä on esimerkkinä SamSam-kiristysohjelmisto. Vaikka tämän tapaiset hyökkäykset eivät ole niin yleisiä, ovat ne paljon tuhoisampia koska hyökkääjät voivat varmistaa, että haittaohjelman tuho on perusteellista, ja tällä tavoin pakottaa yrityksen maksamaan lunnasrahat. WannaCryn osalta lunnaat olivat 300–600 dollarissa, mutta tämän tapaisissa hyökkäyksissä vaatimukset voivat helposti nousta 10.000–50.000 dollariin. Hyökkäyksestä tekee myös petollisen se, että hyökkääjät voivat valita täysin ajankohdan, milloin he suorittavat hyökkäyksen. Esimerkkinä on hyökkääminen perjantai-iltana tai pyhäpäivinä. Tämä takaa sen, että tietojärjestelmästä vastuussa olevat henkilöt eivät välttämättä ehdi reagoimaan hyökkäykseen tarpeeksi ajoissa. (Sophoslabs 2018.)

Vuodesta 2018 johtopäätöksinä voi tehdä seuraavat:

- Kiristyshaittaohjelmien käyttö on vähentynyt verrattuna vuoteen 2017 ja tilalle on tullut uusia versioita kuten kryptovaluutanlouhinta.
- Isoin hyökkäysvektori on roskaposti, joka on tullut haavoittuvuuksien tilalle. Roskapostin käytöllä pyritään saamaan käyttäjä avaamaan joko liitetiedosto, jossa on haittaohjelma tai menemään sivustolle, jolta latautuu haittaohjelma tietokoneelle.

- IoT on iso hyökkäyskohde helpon turvallisuuden takia. Esimerkiksi helppo käyttäjätunnus ja salasanakombinaatio.
- Kiristyshaittaohjelmistojen käyttö on edelleen mahdollista, mutta yleensä ei ole hyökkäyksen ensisijainen tavoite.
- Manuaalinen murtautuminen ja kiristyshaittaohjelmiston käynnistäminen, kun suojaukset on poistettu, on paljon suositumpaa kuin ennen. Tästä esimerkkinä SamSam.

Turvallisuustoimien osalta kaikki mainitsevat päivittämisen tärkeyden, ja sen miten tärkeätä on opettaa työntekijöille mahdollisista sähköpostiin liittyvistä uhista. Sähköpostin huolimaton käyttäminen oli vuonna 2018 heikkous, jonka myötä monet haittaohjelmat pääsivät leviämään. Salasanojen ja käyttäjänimien yksinkertaisuus on myös asia, mikä on hyvä muistaa ja korjata esimerkiksi salasanahallintaohjelmia käyttäen. Etenkin verkkolaitteiden perussalasanat tulisi muuttaa heti asennuksen yhteydessä. (Sophoslabs 2018) (Tietoturvakeskus 2018) (F-Secure 2018a.)

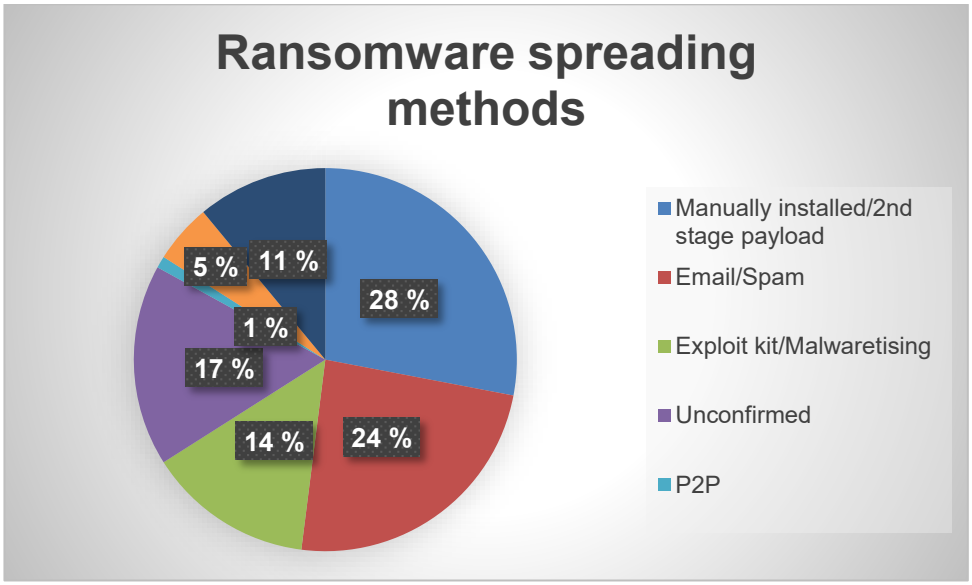
4.1.2 Vuosi 2019

Vuonna 2019 kiristyshaittaohjelmistojen käyttö muuttui paljon kohdennetummaksi niin sanotun ”big game hunting” ilmiön seurauksena, ja osittain myös paljon vaarallisemmaksi uhaksi verrattuna aikaisempiin vuosiin (Kyberturvallisuuskeskus 2019). Vaikka SamSam on esimerkkinä vuonna 2018 tapahtuneesta kohdennetusta kiristyshaittaohjelmien käytöstä, oli vuosi 2019 täynnä tapauksia, joissa useat yritykset joutuivat vastaavanlaisten hyökkäysten kohteiksi. Lunnasvaatimukset myös huomattavasti kovenivat, koska yritykset toisin kuin peruskäyttäjät pystyvät maksamaan paljon suurempia lunnassummia. Sen sijaan, että puhuttaisiin 10.000–50.000 dollarista, joita SamSam vaati aikaisempana vuonna, olivat vaatimukset nyt luokaltaan jopa 400 000 dollaria. (F-Secure 2019b.)

Hyökkäysvektorit olivat pysyneet osittain samoina. Haittaohjelmia levitettiin pääsääntöisesti yhä sähköpostin ja roskapostin kautta. F-Secure raportoi, että

43 % levityksistä tapahtuu yhä kyseistä vektoria käyttäen ja noin 24 % tulee manuaalisen asennuksen johdosta tai toisen haittaohjelman toissasijaisena hyökkäyksenä. (F-Secure 2019b.)

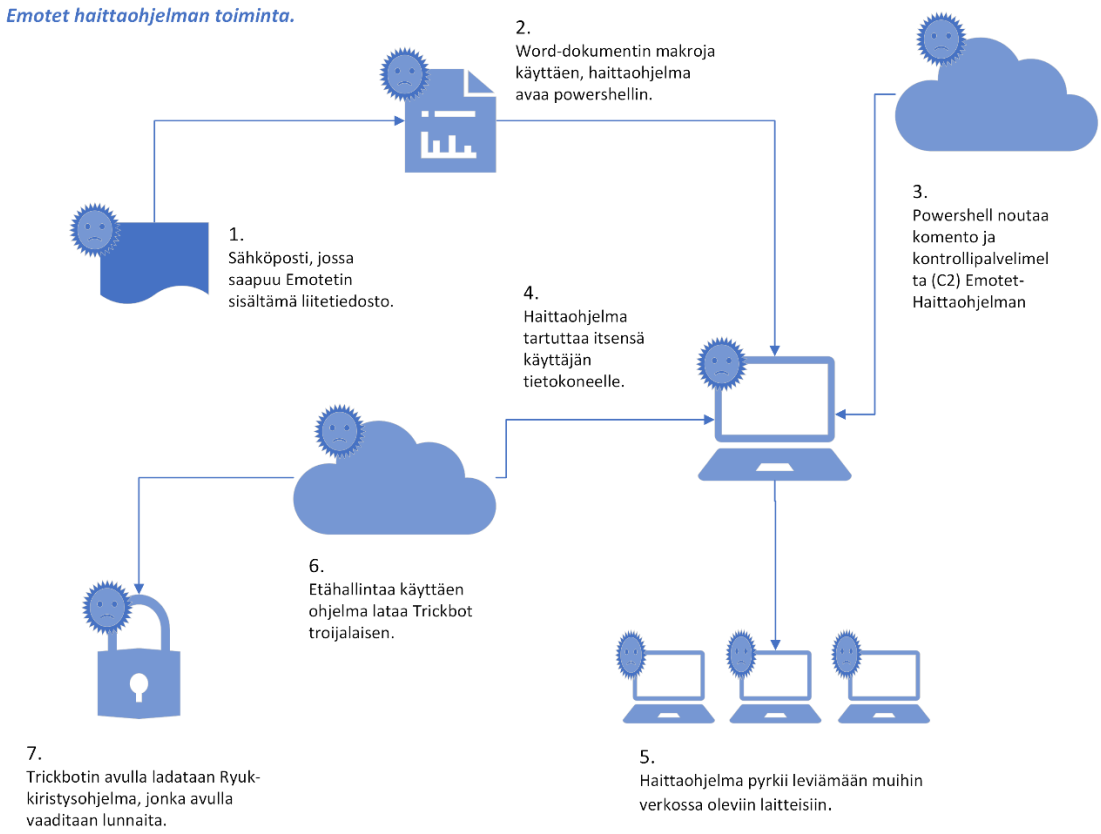
Kiristyshaittaohjelmien osalta muutosta oli kuitenkin tapahtunut. Kirityshaittaohjelmistojen vektori oli ensisijaisesti manuaalinen asennus ja vasta tämän jälkeen sähköposti ja roskapostin käyttö (Kuva 6). Tämä myös kertoo kiristyshaittaohjelmien muuttuneesta toiminnasta. Big game hunting-ilmiöstä johtuen on rikollisten paljon mielekkäämpää pyrkiä manuaalisesti hyökkäämään ja murtautumaan yritysten järjestelmiin ja näin takaamaan, että haittaohjelma suorittaa toimintonsa ilman häiriöitä. (F-Secure 2018b.)



Kuva 6. Kiristyshaittaohjelmien levittämismetodit (F-Secure 2019b).

Kiristyshaittaohjelmistojen tyyppien ja varianttien määrä oli myös laskenut. Vaikka tämä on hyvä asia, tarkoittaa se myöskin sitä, että resursseja on kohdennettu näihin muutamaan jäljelle jääneeseen ohjelmistoon, ja sitä kautta kyseiset kiristyshaittaohjelmat ovat vaarallisempia, kuin koskaan aikaisemmin. (F-Secure 2019b.)

Kiristyshaittaohjelmistojen toiminta ja ominaisuudet myös kehittyivät merkittävästi vuonna 2018. Sähköpostipohjaisissa hyökkäyksissä käytettiin paljon useammin hyväksi käyttäjän manipulointitekniikoita, joilla pyritään samaan uhri avaamaan liitetiedosto, joka ei välttämättä heti sisällä itse kiristyshaittaohjelmaa vaan ohjelmiston, jonka tehtävänä on varastaa käyttäjän sähköpostitili. Tätä kautta hyökkääjä pyrkii pääsemään käsiksi aikaisempiin sähköpostiviestiketjuihin ja käyttäjän osoitekirjaan, jota käyttämällä hyökkääjät pystyvät lähettämään paljon uskottavampia sähköpostiviestejä ja näin leviämään yrityksen verkon sisällä nopeasti. Viestit voivat olla aidosta viestikeskustelusta lainattuja, joka lisää uskottavuuden määrää ja näin lisää luottamusta viestin sisällä oleviin liitteisiin. Kun leviäminen on saavuttanut kriittisen pisteen tai paljastumis- riski on olemassa, alkaa hyökkäyksen toinen vaihe, jossa haittaohjelma lataa kiristyshaittaohjelmiston ja pyrkii salaamaan mahdollisimman suuren osan yrityksen verkkoon kiinnitetyistä laitteista. (Kyberturvallisuuskeskus 2019.)



Kuva 7. Esimerkki Emotet haittaohjelman toiminnasta. (Kyberturvallisuuskeskus 2019).

Hyökkäyksen vaarallisuus piilee juuri siinä, että haittaohjelma voi olla yrityksen verkossa pitkään ilman, että se varsinaisesti aiheuttaa tuhoja. Kun haittaohjelma viimein lataa kiristyshaittaohjelman ja salaa merkittävän osan yrityksen verkkoa, voi tuhoista olla vaikea selviytyä ilman lunnaiden maksamista. Esimerkiksi Norsk Hydro ilmoitti, että sille aiheutuneet menetykset olivat 55–65 miljoonan euron suuruiset, kun LockerGoga-kiristyshaittaohjelma pääsi yrityksen palvelimille, läppäreille ja koneille salaamaan tiedostot. Demant-yhtiö sen sijaan ilmoitti lähemmäs 100 miljoonan dollarin vahingot, kun kiristyshaittaohjelma pääsi salaamaan heidän tietokantansa. Näissä tapauksissa ei lunnaita maksettu, mutta tuhot olivat kuitenkin huomattavat, ja näistä aiheutuneet toiminnan seisokit erittäin kalliita. (F-Secure 2019a) (Kyberturvallisuuskeskus 2019.)

Vuonna 2019 pilvipalveluiden käyttö jatkoi yleistymistään, ja tuli siten myös otollisemmaksi kohteeksi hyökkääjille. Pilvipalveluita ei aina ole turvattu ja asennettu kunnolla, mikä voi pahimmassa tapauksessa antaa hyökkääjälle laajan pääsyn yrityksen verkkoon. Pilvipalvelut sisältävät myös paljon järjestelmänvalvojan työkaluja ja mahdollisia yrityksen tietokantoja, jotka ovat erittäin otollisia kohteita hyökkääjille. (Sophoslabs 2019.)

Varmuuskopiot ovat myös yhä useammin kiristyshaittaohjelmien kohteena. Hyökkääjät ovat hyvin ymmärtäneet, että tuhoutuneet tai salatut varmuuskopiot laskevat lunnaiden maksukynnystä. Tämä on huomattu tehokkaaksi tavaksi etenkin sellaisia yrityksiä vastaan, jotka luottavat varmuuskopioihin eivätkä panosta niin suuresti tietoturvaohjelmistoihin.

Tämän kaiken lisäksi hyökkääjät ovat alkaneet naamioimaan haittaohjelmien toimintoja ja alkaneet hyökkäämään tietoturvayritysten koneoppimistoimintoja vastaan. Naamiointitapoja on useita, haittaohjelmat pyrkivät esimerkiksi yhä useammin käyttämään hyväksi käyttöjärjestelmien kuten Windowsin omia työkaluja, kuten PowerShell tai cmd.exe. Hyökkääjät voivat myös digitaalisesti pyrkiä allekirjoittamaan ohjelmistonsa, jotta ne vaikuttavat luotetuilta virustorjuntaohjelmien silmissä tai ylipäätänsä pyrkiä toimimaan tavalla, joka vähemmän kiinnittää huomiota niiden toimintaan. (Sophoslabs 2019.)

WannaCry ja sen erilaiset versiot ovat yhä käytössä ja ovat yhä merkittävä osa Sophoslabsin saamista varoituksista päivittäin. Tämä trendi tuntuu kertovan siitä, että Internetissä on yhä useita miljoonia laitteita, joita ei ole päivitetty Eternablue-haavoittuvuutta vastaan. (Sophoslabs 2019.)

Johtopäätöksinä vuodesta 2019 voi tehdä seuraavat:

- Kiristyshaittaohjelmat ovat muuttaneet toimintatapojansa paremmin aikaansa sopivammiksi, ja ne ovat yhä merkittävä uhka vuonna 2019.
- Hyökkäysvektorit ovat osittain muuttuneet näiden toimintatapojen takia.
- Kiristyshaittaohjelmien tyyppien ja varianttien määrät ovat laskeneet, mutta jäljelle jääneet ovat tuhoisampia kuin ennen.
- Lunnasvaatimukset ja kiristyshaittaohjelmista aiheutuneet tuhot ovat nousseet merkittävästi.
- Pilvipalvelupohjaiset sovellukset ovat yhä useammin hyökkäysten kohteena.
- WannaCry ja sen erilaiset versiot leviävät yhä, mikä tarkoittaa, että tietokoneita on yhä laajasti päivittämättä EternaBlue-haavoittuvuutta vastaan.

Turvatoimien osalta suositukset keskittyvät ennaltaehkäisyyn ja varautumiseen. Sähköpostipohjaiset hyökkäykset ovat osa yritysten arkea, joten henkilöstön kouluttaminen sähköpostiuhkia vastaan on tärkeämpää kuin koskaan aikaisemmin. Ajantasaiset varmuuskopiot, jotka ovat erillään muista yrityksen toiminnoista ovat tärkeässä osassa big game hunting-tapaisten hyökkäysten tuhojen välttämiseksi. Tämän lisäksi päivitykset, ajantasainen virusturva ja hyvä salasanahallinta ovat tärkeitä välttyäkseen mahdollisilta murtautumisyrityksiltä. (F-Secure 2019b.)

4.1.3 Vuosi 2020

Vuosi 2020 on erittäin ainutlaatuinen verrattuna edellisiin kahteen vuoteen. Covid-taudin johdosta useat ihmiset joutuivat kosketuksiin tietokoneisiin ja

Internetiin enemmän kuin koskaan aikaisemmin, ja tämä toi mukanaan uudenlaisia uhkia. Yritykset etenkin joutuivat laajentamaan toimintojansa etätöitä varten, ja tämä on avannut uusia heikkouksia ja tapoja päästä kiinni yritysten verkkoihin.

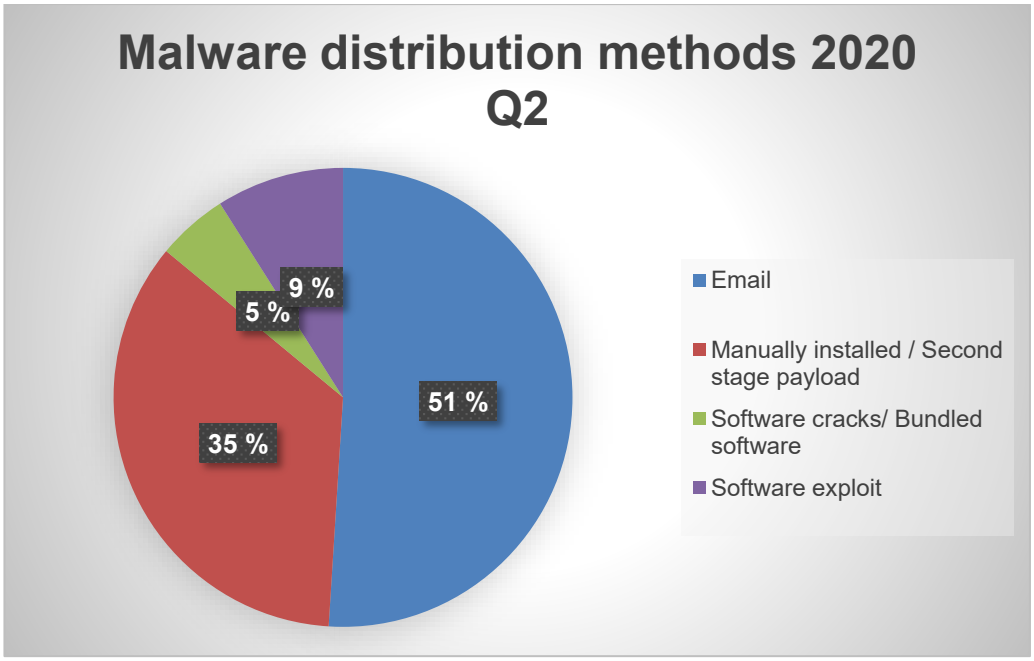
Kiristyshaittaohjelmistot jatkoivat kasvuaan vuonna 2020. Lunnaiden maksumäärät ovat nousseet (Kuva 8), ja kiristyshaittaohjelmat ovat koko ajan kehittäneet uusia torjuntamenetelmiä erilaisia puolustustoimia vastaan. Kiristyshaittaohjelmia käyttävät rikolliset ymmärtävät kuinka kallista pienikin seisokki yrityksen tietojärjestelmissä on, ja tästä syystä ovat myös lunnasvaatimusten määrät nousseet. (Sophoslabs 2020.)

Kuva 8. Vuoden 2020 keskimääräiset lunnasmaksut. (Sophoslabs 2020).

Kiristyshaittaohjelmistojen käyttö myös muuttui merkittävästi aikaisempaan vuoteen verrattuna. Uusimpana trendinä oli käyttää kiristyshaittaohjelmistoja datan vuotamiseen tai varastamiseen, ja tämän jälkeen uhkailla yritystä, että sen data vuodetaan Internetiin kaikkien nähtäville elleivät he maksa lunnasrahoja. Tämä niin kutsuttu ”Extortionware”-ilmiö yleistyi merkittävästi vuonna 2020. Toisinaan hyökkääjät varastivat datan ja tämän jälkeen vielä salasivat yrityksen tietokannat, joka lisäsi vain ennestään painetta maksaa lunnasrahat. Joissakin

tapauksissa on myös käytetty palvelinestohyökkäyksiä tehostamaan kiristyshaittaohjelmien lunnasvaatimuksia. Lunnaiden maksukaan ei välttämättä takaa, että tiedot saadaan takaisin, ja joissakin tapauksissa on vaadittu lisää lunnasrahoja, jotta varastettuja tietoja ei vuodettaisi. (F-Secure 2020b.)

Haittaohjelmien levittämistavat vastaavat 2019 vuoden lukuja. Sähköpostiliitteet ja roskaposti olivat suurin yksittäinen tapa levittää haittaohjelmia yritysten sisälle. Tämä vastasi noin 52 % kaikesta levitetyistä haittaohjelmistoista, kun taas manuaalisesti asennetut tai toissasijaiset asennukset olivat 35–41 % luokkaa riippuen ajankohdasta. (F-Secure 2020b.)



Kuva 9. Haittaohjelmien levittämistavat Q2 2020. (F-Secure 2020b).

Etätyöt ja niihin liittyvät ohjelmistot lisäsivät myös Internetiin avoimina olevien RDP-palvelujen määrää. Tämä puolestaan oli merkittävänä osana verkkohyökkäyspinta-alan kasvua, mikä tarkoittaa siis laitteita tai ohjelmistoja, jotka näkyvät Internetiin ja mihin hyökkääjän on mahdollista tunkeutua. Kodeista on tullut jatkumo yritysten verkoille, ja tätä kautta koteihin kohdistuu entistä enemmän hyökkäyksiä, jolla pyritään pääsemään yritysten järjestelmien sisälle. (Kyberturvallisuuskeskus 2020.)

RDPn käyttö hyökkäysvektorina on ollut kasvussa vuodesta toiseen, ja on yhä useammin osana onnistuneissa kiristyshaittaohjelmistojen käytöissä. Sophoslabsille RDPstä lähtöisin olevat kiristyshaittaohjelmien hyökkäykset ovat olleet yksi suurimpia syitä yritykselle tulevista tietoturvailmoituksista, ja yhä useampi RDP-palvelu on Internetiin näkyvä, vaikka suosituksiin kuuluukin pitää kyseiset toiminnot palomuurin takana ja mieluusti VPN-ohjelman avulla suojattuna. Harva yritys kuitenkaan tekee näin jokaisen RDP-palvelun osalta. (Sophoslabs 2020.)

Vuoden 2020 aikana nähtiin myös laaja kampanja, jossa käytettiin hyväksi covid-19-teemaisia sähköpostiviestejä. Kyseiset roskapostit vastasivat tyypillisesti nähtyjä huijausviestejä, mutta olivat teemaltaan covidia hyväksi käyttäviä. Näitä esimerkiksi saattoivat olla erilaiset covidiin liittyvät tiedotteet tai uutiset. Kaikkien huijausten tavoite oli kuitenkin sama, saada käyttäjä avaamaan liitetiedosto, joka sisälsi haittaohjelman tai saada käyttäjä avaamaan sivuston linkin, jonka kautta latautui haittaohjelma. (F-Secure 2020a.)

Vuodesta 2020 johtopäätöksinä voi tehdä seuraavat:

- Kiristyshaittaohjelmien käyttö on lisääntynyt, ja näiden aiheuttamat lunnasvaatimukset ja tuhot ovat nousseet.
- Yritykset maksoivat yhä useammin lunnasrahat vuoden 2020 aikana.
- Pelkkä uhka tärkeän datan levittämisestä Internetissä saattaa riittää lunnaiden maksamiseen.
- Hyökkäysvektorit ovat pysyneet samana vuoteen 2019 verrattuna.
- Covid-19 johtunut etätöiden suosio on lisännyt räjähdysmäisesti RDP protokollan käyttöä etätöiden tekemisessä.
- covid-pohjaiset huijausviestit ovat yleisin huijausviesti trendi.

Vuoden 2020 turvatoimet liittyvät pitkälti etätöiden ja niiden aiheuttamien uhkien hallintaan. Riskienhallinta ei pysy perässä muuttuvassa maailmassa ja tästä syystä yritykset ottavat yhä useammin käyttöön ratkaisuja, joiden riskejä ei osata arvioida tai niitä ei ymmärretä. Yhä useampi yrityksen toiminto näkyy Internetiin, vaikka sen ei tarvitse näkyä. VPN-palvelujen käyttö ja ylimääräisten toimintojen

poistaminen laskee hyökkäyspinta-alaa. Lopulta henkilöstön koulutus on yhä tärkeämpää kuin koskaan aikaisemmin, jotta etätyöt voidaan suorittaa turvallisesti ja sähköpostiuhat ymmärretään selvästi. Päivitykset ja ajantasainen virustorjuntaohjelmisto ovat myös tärkeämmässä osassa kuin koskaan aikaisemmin, jotta hyökkääjät eivät pääse helposti sisälle yrityksen järjestelmiin. (Sophoslabs 2020) (Kyberturvallisuuskeskus 2020)

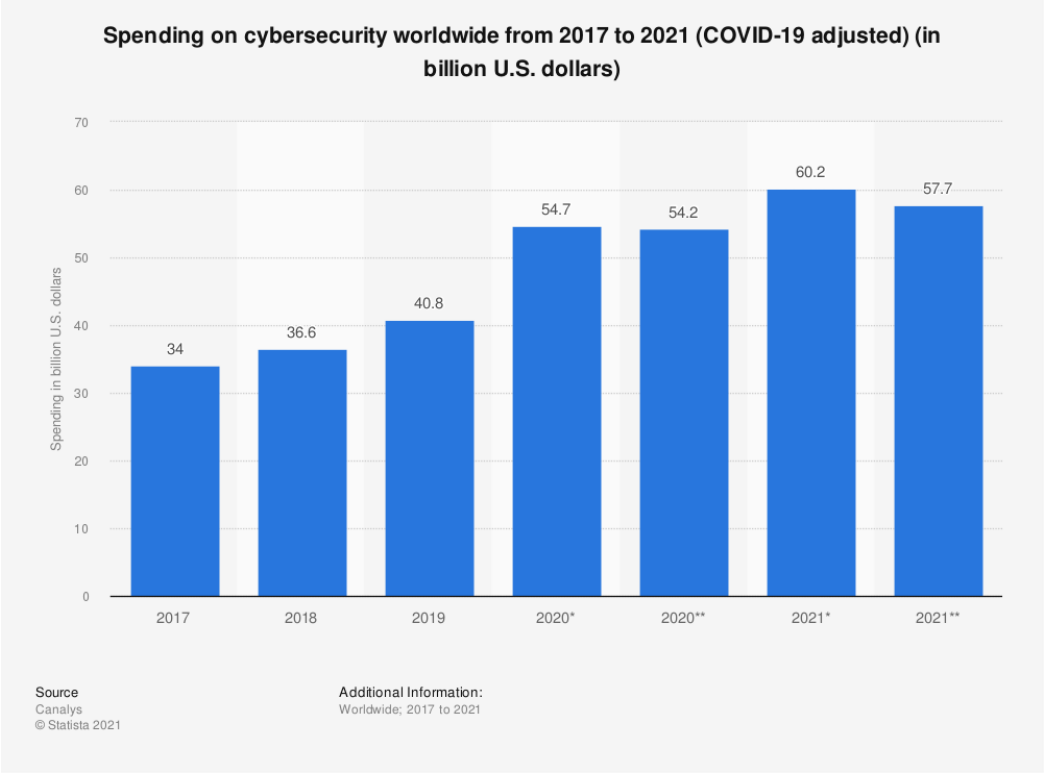
4.2 Yritysten tietoturvareagointi

Yritykset ovat sijoittaneet rajusti tietoturvaan viimeisen 3 vuoden aikana. Pelkästään vuonna 2018 kyberturvallisuuteen ja siihen liittyviin tuotteisiin panostettiin yli 36,6 miljardia dollaria (Kuva 10) mikä on merkki siitä, että erinäköiset uhat kuten kiristyshaittaohjelmistot otetaan tosissaan. Mutta on paljon myös sektoreita kuten energia-ala, joka investoi vähemmän kuin 0,2 % heidän olemassa olevista tuloistaan kyberturvaan. (Morgan 2019.)

Vuoden 2021 osalta uskotaan, että tietoturvaan panostaminen nousee yli 150 miljardiin dollariin, mikä olisi yli 12% kasvua verrattuna vuoteen 2020. Tietoturvaan panostaminen nähdään yhä useammin tärkeänä ja järkevänä investointina. Se nähdään myös tapana säästää rahaa, jos joutuu mahdollisen hyökkäyksen uhriksi. (Moore 2021.)

Vuosien 2021–2025 aikana rahankäytön oletetaan vain kasvavan johtuen IoT-laitteiden määrän ja käytön jatkuvasta kasvusta. Yrityksillä on myös kasvava tarve investoida tietoturvatuotteisiin ja ratkaisuihin, joilla pystytään paremmin vastaamaan muuttuviin tulevaisuuden uhkiin ja uusiin kehityksiin. Myös yksittäiset käyttäjät käyttävät huomattavasti enemmän aikaa ja rahaa saadakseen tietokoneet ja muut kodin laitteet turvattua. Etenkin toimiva virustorjuntaohjelmisto nähdään monessa kodissa järkevänä ostoksena. Panostukset tietoturvatuotteisiin ja palveluihin uskotaan maksavan vuosina 2021–2025 noin 1,75 biljoonaa dollaria. Hintaan sisältyy panostukset esimerkiksi pilvipalveluiden tietoturvaan, datan suojelemiseen, infrastruktuurin suojelemiseen ja tietoturva palveluihin ja ohjelmistoihin. (Braue 2021.)

Yleisesti pystytään näkemään, että yritykset ja myös peruskäyttäjät ovat alkaneet panostamaan rajusti enemmän tietoturvaan vuosien 2017 ja 2018 jälkeen (Kuva.10).



Kuva 10. Kyberturvallisuuden rahankäyttö vuosilta 2017–2021. (Canalys. 2021).

4.3 Yhteenveto

Yhteenvetona voidaan huomioida, että kiristyshaittaohjelmistojen käyttö vuosina 2018–2020 on noussut ja yleisesti ottaen kiristyshaittaohjelmat ovat huomattavasti vaarallisempia kuin koskaan aikaisemmin. Keskimääräiset lunnasvaatimukset viimeisen 4 vuoden aikana ovat yli satakertaistuneet, ja vuonna 2020 tietovuoto voi helposti aiheuttaa puolen miljoonan vahingot ja tilanteesta riippuen, jopa enemmän. Kiristyshaittaohjelmistoilla on ollut vaikutusta yritysten tietoturvakäytäntöihin. Yritykset käyttävät ja investoivat huomattavasti enemmän resursseja, jonka avulla pyritään välttämään mahdollisia tietoturvauhkia. Näihin sisältyy muun muassa ratkaisuja ja toimintoja erilaisia kiristyshaittaohjelmistoja vastaan.

Huomioitavaa on myös verrata WannaCryta sen myöhempiin variantteihin ja kilpailijoihin. WannaCryn hyökkäys onnistui käyttämällä hyväksi EternalBlue-heikkoutta. Mutta suurin osa uudemmista kiristyshaittaohjelmistoista käyttää hyväksi yhä useammin erilaisia sähköpostihuijauksia, joiden avulla pyritään murtautumaan yrityksen tietojärjestelmiin. Vasta toisessa vaiheessa alkaa varsinaisen kiristyshaittaohjelmiston levittäminen. Hyökkäystrendit ovat siis muuttuneet, ja nämä todennäköisesti tulevat muuttumaan ja modernisoitumaan tulevaisuudessakin. Toki huomioitavaa on, että WannaCry ja sen erilaiset versiot ovat yhä käytössä. Tämä kertoo mielestäni siitä, että verkossa on vieläkin käytössä mahdollisesti miljoonia tietokoneita ja muita laitteita, joita ei ole päivitetty EternalBlue-heikkoutta vastaan. Trendi on huolestuttava, koska korjaus EternalBlue-haavoittuvuuteen on ollut saatavilla jo usean vuoden ajan.

Yritykset ovat myös alkaneet investoimaan huomattavia summia tietoturvapalveluihin ja -tuotteisiin. Vaikka trendi on positiivinen, on silti monia sektoreita kuten energia-ala, joka ei ole nostanut samalla tavalla budjettiaan (Morgan 2019.). Yksilön vastuu etenkin covid-19 aikana on noussut yhä tärkeämmäksi yksittäiseksi tavaksi välttää laajat tietoturvavuodot ja hyökkäykset. Etätyöt ja monet muut uudet ongelmat ovat aiheuttaneet sen, että vaikka järjestelmät olisivat uudet ja päivitetyt, ei yrityksen riskienhallinta silti pysy perässä.

5 Korjausehdotuksia

Lopulta käyn läpi korjausehdotuksia, joita yritysten mielestäni kannattaisi harkita aikana, jolloin hyökkäykset voivat saapua mistä tahansa ja olla mahdollisesti erittäin kalliita yrityksen tuotannolle.

5.1 Päivittäminen ja sen tärkeys

WannaCryn leviämisen suurin yksittäinen syy oli yritysten haluttomuus päivittää järjestelmiään. Kuten luvussa 3.4 kävin läpi, Microsoft oli korjannut EternalBlue-haavoittuvuuden Windows 7 ja Windows 10-ympäristöihin. Jos yritykset olisivat päivittäneet tietokoneitaan useammin, olisi vahinko ollut merkittävästi pienempi.

Tästä syystä on tärkeätä pitää käyttöjärjestelmät, tietoturvaohjelmisto ja muut mahdollisesti hyökättävissä olevat ohjelmat päivitettynä ja ajan tasalla. Etenkin aikana, jolloin hyökkäykset erilaisiin löydettyihin heikkouksiin tapahtuvat nopeammin ja nopeammin on tärkeätä päivittää ja reagoida nopeasti.

5.2 Varmuuskopiot ja niiden pitäminen turvallisessa ympäristössä.

Varmuuskopiot ovat tärkeitä, ja niiden ottaminen säännöllisin väliajoin on hyvä tapa selviytyä, jos joutuu kiristysohjelmiston hyökkäämäksi. Mutta yritysten olisi myös tärkeä muistaa segmentoida mahdollinen palautuspalvelin ulos normaalista käyttöverkosta. Luvussa 4.1.2 ja kuva 7 on esimerkkinä, mitä voi tapahtua, jos haittaohjelma pääsee vapaasti leviämään verkossa missä kaikki laitteet ovat yhteydessä. Varmuuskopioista ei ole mitään hyötyä, jos niitä ei pysty hyökkäyksen jälkeen käyttämään.

Varmuuskopioiden kohdalla on myös hyvä harjoitella mahdollisia tilanteita, joissa tarvitsee käyttää kyseisiä kopioita. Harjoittelun avulla on mahdollista palautua kiristyshaittaohjelman aiheuttamista tuhoista nopeammin, etenkin jos mahdolliset tilanteet ja käytännöt on tarkkaan dokumentoitu.

5.3 Henkilöstön kouluttaminen

Henkilöstön kouluttaminen mahdollisia sähköpostihuijauksia vastaan on yksi tärkeimpiä asioita, mitä yritykset mielestäni voivat tällä hetkellä tehdä. Data myös puhuu tämän puolesta, kun yli 50% tapahtuvista haittaohjelmahyökkäyksistä on sähköpostiin kohdistuvia, ja trendi ei näytä ainakaan laskevan.

Koulutuksessa on tärkeätä mielestäni panostaa, miksi varovaisuus on tärkeää ja myös painottaa, että yksi heikko linkki voi vahingossa aiheuttaa tuhoja millä voi olla yrityksen kannalta pitkäkestoisia vaikutuksia. Koulutusta on myös tärkeä kohdentaa henkilöille, jotka ovat vastuussa yrityksen IT- palveluista, jotta he pystyvät reagoimaan tehokkaasti ja ajantasaisesti erilaisiin uhkiin.

5.4 Laitteiden ja IoT-laitteiden turvaaminen

Lopulta haluaisin mainita IoT-laitteista ja yleisesti laitteista, että jos niitä ei käytetä, ne tulisi poistaa käytöstä. Jokainen laite, joka on näkyvillä Internetiin, on mahdollinen hyökkäyskohde ja heikkous yritysverkossa.

Jos laitteita tarvitsee käyttää, on muistettava perusteet. Laitteet tulee päivittää mahdollisimman usein ja uusimpaan versioon niiden käyttämästä ohjelmasta. Laitteiden oletussalasanat ja käyttäjätunnukset on myös aina vaihdettava koska on vain ajan kysymys, milloin oletussalasanat ovat yleisessä tiedossa Internetissä ja kyseisiin laitteisiin tullaan tekemään erilaisia hyökkäyksiä käyttäen näitä salasanoja.

On myös hyvä muistaa, että kaikkien laitteiden ei tarvitse olla helposti saatavilla tai näkyvissä Internetin kautta. RDP-protokollan kautta tehdyt hyökkäykset ovat yhä useammin osa onnistuneita tietoturvamurtautumisia. On siis hyvä selvittää minkä laitteiden täytyy olla nettiin näkyvissä, ja onko niitä esimerkiksi mahdollista suojata VPN- tai jonkun muun toiminnon avulla.

6 Yhteenveto

Opinnäytetyön tavoitteena oli selvittää, mikä on WannaCry-kiristyshaittaohjelmisto ja miksi se oli niin merkittävä vuonna 2017 aiheutuneessa verkkohyökkäyksessä. Opinnäytetyön tavoitteena oli myös selvittää kiristyshaittaohjelmistojen historiaa, ja lopulta vastata kysymykseen, onko WannaCrylla ollut vaikutusta yritysten tietoturvakäytäntöihin.

Tuloksena sain selvitettyä hieman kiristyshaittaohjelmistojen historiaa, tässä tapauksessa AIDS, Cryptolocker ja Locky-ohjelmistojen avulla. Selvitettyä miten WannaCry-haittaohjelmisto toimii ja miten kyseinen haittaohjelma pääsi leviämään merkittävästi vuonna 2017. Lopuksi tuloksena on saatu hieman vuosien 2017–2020 statistiikkaa haittaohjelmistojen ja kiristyshaittaohjelmistojen käytöstä. Näiden statistiikkojen avulla olen pystynyt tekemään johtopäätöksiä ja vastaamaan kysymykseen onko WannaCryn tapaisilla kiristyshaittaohjelmistoilla ollut merkitystä yritysten tietoturvakäytäntöihin. Voin lopullisesti vastata, että kyllä mielestäni WannaCrylla on ollut vaikutusta yritysten tietoturvakäytäntöihin. Yritykset ovat varautuneet paremmin kuin koskaan aikaisemmin kiristyshaittaohjelmistojen aiheuttamiin uhkiin. Kiristyshaittaohjelmistot ovat jatkaneet kehittymistä, ja täten aiheuttavat vuosi vuodelta uusia haasteita tietoturvayrityksille, jotka pyrkivät suojaamaan yritysten laitteita.

Hankaluuksia työssä aiheutti osittain lähteiden puute tai vanhentuneet linkit lähteisiin. AIDS-haittaohjelmasta kirjoittaessani huomasin, että erittäin vanhat lähteet ovat tosi useasti vanhentuneet tai eivät enää löydettävissä helposti.

Kirjoittaessani opinnäytetyötä opin, kuinka tärkeätä on kirjata tarkasti ja aikaisin mahdolliset lähteet ja muut käytetyt dokumentit. Useasti näitä korjatessa joutui tekemään paljon ylimääräistä työtä, minkä olisi voinut välttää kirjoittamalla heti kaiken kohdilleen. Alkuperäisen alueen rajaaminen oli myös erittäin haastavaa, etenkin historiaesimerkkien kohdalla. Kiristyshaittaohjelmista on monia esimerkkejä, mutta kaikkia ei voinut mitenkään valita opinnäytetyötä varten.

Lähteet

ABC.net.au 2017. Biggest ransomware outbreak in history' hits nearly 100 countires with data held for ransom. Viitattu 9.11.2021. https://www.abc.net.au/news/2017-05-13/biggest-ransomware-outbreak-in-history-hits-nearly-100-nations/8523102

Arthur, Charles 2017. The ransomware attack is allabout the insufficient funding of the NHS. The Guardian 13.5.2017. Viitattu 9.11.2021. https://www.theguardian.com/commentisfree/2017/may/13/nhs-computer-systems-insufficient-funding

Bates, Jim 1990. TrojanHorse: Aids Information Introductory Diskette Version 2.0. VirusBulletin, Tammikuu 1990. Viitattu 31.10.2021. https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf

BBC.com 2017. NHS cyber-attack: GPs and hospitals hit by ransomware. Viitattu 9.11.2021. https://www.bbc.com/news/health-39899646

Belcic, Ivan 2019. What is Locky Ransomware. Avast Academy 28.11.2018. Viitattu 3.11.2021. https://www.avast.com/c-Locky

Belcic, Ivan 2020. What is Cryptolocker Ransomware and How to Remove it. Avast Academy 27.2.2020. Viitattu 3.11.2021. https://www.avast.com/c-Cryptolocker

Braue, David 2021. Global Cybersecurity Spending Predicted to Exceed $1.75 Trillion From 2021-2025. Cybercrime Magazine 10.9.2021. Viitattu 11.11.2021. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

Burdova, Carly 2020. What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?. Avast Academy 18.6.2020. Viitattu 9.11.2021. https://www.avast.com/c-EternalBlue#topic-2

Canalys 2021. Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted) (in billion U.S. dollars). Statista. Statista Inc.. Viitattu 11.11.2021. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

Cisecurity.org 2019. MS-ISAC Security Primer – EternalBlue. Viitattu 9.11.2021. https://www.cisecurity.org/white-papers/ms-isac-security-primer-eternal-blue/

Cybersecurity & infrastructure security agency 2014. GameOver Zeus P2P Malware. Viitattu 15.11.2021. https://us-cert.cisa.gov/ncas/alerts/TA14-150A

Daniels, Drew 2021. Combating extortionware in 2021: A rising attack method for the modern day hacker. Security Magazine 29.1.2021. Viitattu 31.10.2021. https://www.securitymagazine.com/articles/94468-combating-extortionware-in-2021-a-rising-attack-method-for-the-modern-day-hacker

Department of justice 2014. U.S. Leads multi-national action against “Gameover Zeus” Botnet and “Cryptolocker” ransomware, charges botnet administrator. Viitattu 3.11.2021. https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-Cryptolocker-ransomware

Frost, Laurence – Tajitsu, Naomi & Reuters 2017. Renault-Nissan is resuming production after a global cyberattack caused stoppage at 5 plants. Businessinsider 15.5.2017. Viitattu 9.11.2021. https://www.businessinsider.com/renault-nissan-production-halt-WannaCry-ransomeware-attack-2017-5?r=US&IR=T

F-Secure 2017: Mikko Hypponen speaks about WannaCry at SPECIES, Youtube-videopalvelu, julkaistu 19.5.2017 https://www.youtube.com/watch?v=ZqNSoHFtGM0. Viitattu 5.11.2021

F-Secure 2018a. Attack Landscape of 2018, So far. Raportti. Viitattu 10.11.2021. https://blog.F-Secure.com/attack-landscape-2018-far/

F-Secure 2018b. Attack Landscape H2 2018: Attack traffic increases fourfold. Raportti. Viitattu 10.11.2021. https://blog.F-Secure.com/attack-landscape-h2-2018/

F-Secure 2018c. Online shoppers more vulnerable to spam as the holidays inch closer. Viitattu 10.11.2021. https://www.F-Secure.com/en/press/p/online-shoppers-more-vulnerable-to-spam-as-the-holidays-inch-closer

F-Secure 2019a. Attack Landscape H1 2019. Raportti. Viitattu 11.11.2021. https://blog-assets.F-Secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

F-Secure 2019b. Attack Landscape H2 2019. Raportti. Viitattu 11.11.2021. https://blog-assets.F-Secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf

F-Secure 2020a. Attack landscape H1 2020. Raportti. Viitattu 11.11.2021. https://blog-assets.F-Secure.com/wp-content/uploads/2020/09/17142720/F-Secure-attack-landscape-h12020.pdf

F-Secure 2020b. Attack landscape update. Raportti. Viitattu 11.11.2021. https://blog-assets.F-Secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf

F-Secure 2021.Trojan Mikä on Troijalainen. Viitattu 12.11.2021. https://www.F-Secure.com/fi/home/articles/what-is-a-trojan

Grigorik, Nikolai 2017. Screenshot of a Cryptolocker Attack. Wikipedia 22.12.2017. Viitattu 3.11.2021. https://en.wikipedia.org/wiki/Cryptolocker#/media/File:Cryptolocker.jpg

Hughes, Owen 2019. NHS trust IT spend up more than £150m since WannaCry. Digitalhealth 15.8.2019. Viitattu 9.11.2021. https://www.digitalhealth.net/2019/08/nhs-trusts-it-spend-up-more-than-150m-since-WannaCry/

Kaspersky 2018. Cryptolocker Virus Definition. Viitattu 3.11.2021. https://usa.kaspersky.com/resource-center/definitions/Cryptolocker

Kyberturvallisuuskeskus 2018. Tietoturvan vuosi. Raportti. Viitattu 10.11.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf

Kyberturvallisuuskeskus 2019. Tietoturvan vuosi. Raportti. Viitattu 11.11.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_aukeamittain.pdf

Kyberturvallisuuskeskus 2020. Tietoturvan vuosi 2020. Raportti. Viitattu 11.11.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf

Laotto, Nica 2020. What is WannaCry. Avast Academy 27.2.2020. Viitattu 9.11.2021. https://www.avast.com/c-WannaCry

Lee, Martin & al. 2017. Player 3 Has Entered the Game: Say Hello to 'WannaCry'. TalosIntelligence 12.5.2017. Viitattu 9.11.2021. https://blog.talosintelligence.com/2017/05/wannacry.html

McAfee LLC, 2018. What is ransomware? Viitattu 29.10.2021. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

Microsoft 2016. Server Message Block Overview. Viitattu 9.11.2021. https://docs.Microsoft.com/en-us/previous-versions/Windows/it-pro/Windows-server-2012-r2-and-2012/hh831795(v=ws.11)

Microsoft 2017. Microsoft Security Bulletin MS17-010 – Critical. Viitattu 9.11.2021. https://docs.Microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Moore, Susan 2021. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. Gartner 17.5.2021. Viitattu 11.11.2021. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Morgan, Steve 2019. Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021. Cybercrime Magazine 10.6.2019. Viitattu 11.11.2021. https://cybersecurityventures.com/cybersecurity-market-report/

Popp, Joseph L. 1989. AIDS Information Trojan. Wikipedia 30.11.1989. Viitattu 31.10.2021. https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)#/media/File:AIDS_DOS_Trojan.png

Seals, Tara 2021. Ransomware Volumes Hit Record Highs as 2021 Wears On. Threatpost 3.8.2021. Viitattu 29.10.2021. https://threatpost.com/ransomware-volumes-record-highs-2021/168327/

Sophoslabs 2018. Sophos Threat report 2019. Raportti. Viitattu 10.11.2021. https://news.sophos.com/en-us/2018/11/14/threat-report-2019/, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

Sophoslabs 2019. Sophos 2020 Threat Report. Raportti. Viitattu 11.11.2021. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf

Sophoslabs 2020. Sophos 2021 Threat Report. Raportti. Viitattu 11.11.2021. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

Toledano, Bruno 2017. Hackean la red interna de Telefónica y de otras grandes empresas españolas. El Mundo 12.5.2017. Viitattu 9.11.2021. https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

VirusBulletin 1990. Aids Information Version 2.0. VirusBulletin Magazine January 1990. Viitattu 31.10.2021. https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf

Wikipedia 2005. Haittaohjelma. Viitattu 12.11.2021. https://fi.wikipedia.org/wiki/Haittaohjelma

Wikipedia 2014. Operation Tovar. Viitattu 3.11.2021 https://en.wikipedia.org/wiki/Operation_Tovar

Wikipedia 2017. WannaCry Ransomware attack. Viitattu 9.11.2021. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png

Wikipedia 2020 NHS. National Health service. Viitattu 9.11.2021. https://en.wikipedia.org/wiki/National_Health_Service

Winston, Richard 2016. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. Los Angeles Times 18.2.2016. Viitattu 5.11.2021. https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html