Tampereen yliopisto

Antti Välipakka

RANSOMWAREN TOIMINTAPERIAATE JA SILTÄ SUOJAUTUMINEN

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
05/2019

TIIVISTELMÄ

Antti Välipakka: Ransomwaren toimintaperiaate ja siltä suojautuminen
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikka, TkK
05/2019

Tässä kandidaatintyössä käsitellään ransomware-haittaohjelmien toimintaperiaatteita ja suojautumiskeinoja ransomwareilta. Suojautumiskeinoista käsitellään erityisesti kahta uutta kehitettyä suojautumiskeinoa, avainvarmuuskopiontimenetelmää ja hunajatiedostomenetelmää. Työssä avataan myös hieman ransomwarejen historiaa. Lähteinä työssä on käytetty pääsääntöisesti erilaisia tieteellisiä artikkeleita. Työn tuloksena voidaan todeta, että ransomwaret, niin kuin muutkin haittaohjelmat kehittyvät jatkuvasti. Tämä tarkoittaa sitä, että myös ransomwareilta suojautumiskeinojen tulee kehittyä jatkuvasti. Tulevaisuudessa tulee myös ottaa huomioon mobiililaitteilla toimivat ransomwaret.

Avainsanat: ransomware, tietoturva

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

malware	haittaohjelma
makro	mahdollistaa jonkin toiminnon automatisoinnin
JavaScript	pääasiassa web –ympäristössä toimiva ohjelmointikieli
RSA	Rivest–Shamir–Adleman, julkiseen avaimeen perustuva salausmenetelmä
kryptolompakko	kryptovaluuttojen käyttämä virtuaalinen lompakko rahojen säilytykselle
Master File Table	tietokanta, joka sisältää tiedon jokaisesta järjestelmän tiedostosta ja hakemistosta [1]
USB	Universal Serial Bus, tapa yhdistää oheislaitteita tietokoneeseen
Master Boot Record	järjestelmän käynnistykseen liittyvä sijainti järjestelmässä [2]

1. JOHDANTO

Microsoftin Windows –käyttöjärjestelmällä toimivia haittaohjelmia on lukuisia. Ransomware on yksi näistä. Ransomware on haittaohjelma, joka yleensä lukitsee käyttäjän tiedostoja. Lukitsemisen jälkeen ransomware vaatii uhriltaan lunnaita tiedostojen avaamiseksi. Edistyneimmät ransomwaret salakirjoittavat tiedostot niin, että niitä on mahdoton avata ilman lunnaiden maksusta saatavaa purkuavainta. Jotkut ransomwaret uhkaavat levittää uhrinsa henkilökohtaisia tiedostoja internettiin, jos uhri ei maksa kiristäjälle.

Tässä työssä käsitellään ransomwarejen toimintaa ja sitä, miten niiltä voi suojautua. Erityisesti otetaan huomioon avainvarmuuskopiontitekniikka ja hunajatiedostomenetelmä. Avainvarmuuskopiointitekniikkaa käyttämällä voidaan poimia talteen ransomwaren salakirjoituksen yhteydessä ulos syötetty salakirjoitusavain. Tällä salakirjoitusavaimella voidaan purkaa ransomwaren lukitsemien tiedostojen salakirjoitus. Hunajatiedostomenetelmän perusidea on huomata ransomwaren toiminta järjestelmässä ja estää sen toiminta huomaamisen jälkeen. Tutkimuskysymykseni on: Miten ransomwarelta voidaan suojautua nykyisessä tietoyhteiskunnassa? Työssä käsitellään ransomwaren määritelmää ja toimintaa sekä yleisiä suojautumiskeinoja.

Luvussa 2 käydään läpi ransomwaren historiaa. Luvussa 3 käsitellään ransomwaren toimintaperiaatetta ja syitä ransomwaren käyttöön. Luvussa 4 käsitellään ransomwarelta suojatumista. Lopuksi esitetään yhteenveto.

2. RANSOMWAREN HISTORIAA

Ransomwaren nimi on yhdistelmä englanninkielisistä sanoista ”ransom” eli lunnas tai lunnaat ja ”malware” eli haittaohjelma. Ransomwarea voidaan pitää eräänlaisena troijalaishaittaohjelmana. Ransomwaren tärkein tehtävä on kerätä rahaa. Rikolliset ovat käyttäneet aikojen saatossa useita tapoja huijatakseen rahaa uhreiltaan, mutta ransomwaren tapauksessa uhrilla on kaksi vaihtoehtoa: olla maksamatta lunnaita ja menettää lukitut tiedostot tai maksaa lunnaat ja saada tiedostonsa takaisin. [3]

Ransomwaren juuret ulottuvat vuoteen 1989, jolloin Joseph Popp loi ensimmäisen ransomwaren. Hänen luomansa ohjelman nimi oli ’AIDS’. Popp levitti haittaohjelmaansa postittamalla fyysisiä levykkeitä, jotka sisälsivät haittaohjelman. Hän postitti levykkeitä yli 20 000 yli 90 eri maahan. Kun tämän haittaohjelman sisältämä levyke asetettiin tietokoneeseen, AIDS lukitsi kiintolevyllä sijaitsevat tiedostot salakirjoittamalla ne. Tämän jälkeen haittaohjelma vaati uhriltaan $189 lähetettynä postitse Panamaan. Tämä ransomware ei kuitenkaan ollut erityisen menestyksekäs, koska tavoitettavia uhreja oli vähän, käytetty salakirjoitusmenetelmä oli huono, lunnasmaksun lähetys oli vaikeaa, ja tuohon aikaan tietokoneilla säilytetty data ei ollut arvokasta. [4] Ransomwaret ovat kehittyneet huomattavasti ensimmäisestä AIDS-ransomwaresta. Yksi tunnetuimmista ja pahamaineisimmista ransomwareista on WannaCry. Se aiheutti laajasti kaaosta vuonna 2017 [5].

2.1 WannaCry

Toukokuussa 2017 WannaCry-niminen ransomware tuli julkisuuteen. Vaikka WannaCry ei toimintaperiaatteeltaan eroa muista ransomwareista, erityisen siitä tekee sen infektoimien tietokoneiden määrä [5]. Se tartutti yli 200 000 tietokonetta 150 eri maassa. WannaCryn tuhojen aiheuttamat kustannukset ovat arviolta 4–8 miljardia dollaria [6]. WannaCry käytti tartuttamisessa hyväkseen Windowsin tietoturva-aukkoa, joka paikattiin vain Windows Vistassa ja sitä uudemmissa Windows-versioissa. Tämä tarkoitti sitä, että Windows Vistaa vanhemmat Windows-versiot jäivät kokonaan paikkaamatta. Koska Vistaa vanhempia Windows-versioita käytettiin vielä 2017 runsaasti, joutui Microsoft kuitenkin tarjoamaan tietoturvapaikkauksen myös vanhemmille Windows-versioille. Moni Windowsin käyttäjä oli myös ottanut Windowsin automaattiset päivitykset pois päältä, mikä taas auttoi WannaCrytä leviämään tehokkaammin. WannaCryn leviämistä esti brittiläisen tutkijan tekemä löydös WannaCryn lähdekoodista. Hän löysi koodista niin sanotun ”kill switchin” eli tappokytkimen, jolla haittaohjelman leviäminen saatiin loppumaan. Syytä sille, miksi WannaCryn tekijä oli tällaisen koodinpätkän laittanut haittaohjelmaansa, ei ole löydetty. [5]

Kuva 1 WannaCry-ransomwaren ilmoitus käyttäjälle [5]

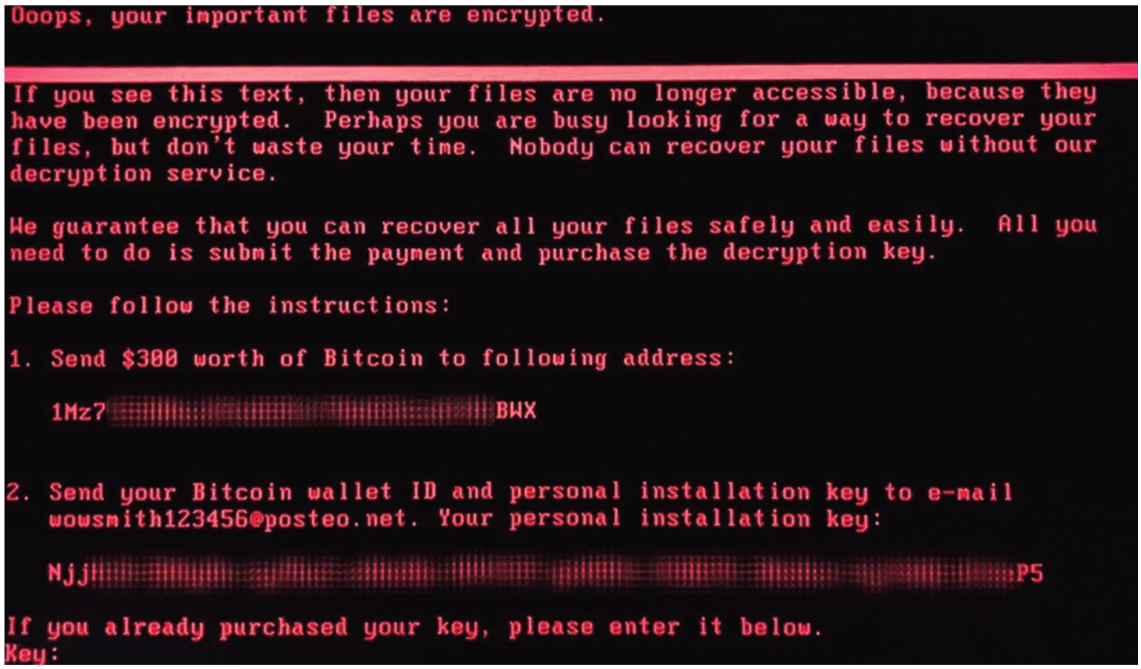
Kuvassa 1 on näkymä WannaCryn uhrilleen näyttämästä ilmoituksesta. Ilmoituksessa uhria uhkaillaan kertomalla, että hänen tiedostonsa on lukittu ja näitä lukittuja tiedostoja ei pysty avaamaan kukaan muu kuin haittaohjelman tekijä. Lukittujen tiedostojen avaamista varten tulee maksaa lunnaat. Uhrille esitetään myös kaksi eri aikarajaa. Ylemmän aikarajan ylittymisen jälkeen lunnassumma kasvaa. Alemman aikarajan umpeutuessa uhrin tiedostot lukkiutuvat ikuisesti. Ilmoituksessa on kerrottu myös ohjeet, joissa kerrotaan, miten uhri voi hankkia Bitcoineja, joita tarvitaan 300 dollarin edestä lunnaita varten.

2.2 NotPetya

Vuoden 2017 heinäkuussa huomattiin uusi ransomware. Tämä uusi ransomware kulkee monella nimellä: NotPetya, ExPetr, Petya ja Petrwrap. Näistä tunnetuin on NotPetya. NotPetyan tuhojen kustannusten arvioidaan olleen yli kymmenen miljardia dollaria [6]. Tämä ransomware otti kohteekseen pääasiassa yrityksiä, jotka sijaitsivat Venäjällä, Ukrainassa ja muualla Euroopassa. Kohteeksi joutui arviolta 2000 yritystä. WannaCryn tapaan NotPetya käytti hyväkseen EternalBlue- ja EternalRomance-nimisiä Windowsin tietoturva-aukkoja. NotPetya levisi naamioituneena suositun ukrainalaisen kirjanpito-ohjelman, MeDocin, päivityksenä. Kohdejärjestelmään sisään päästyään NotPetya varasti kirjautumistunnukset järjestelmästä ja pääsi näin leviämään yrityksen verkossa. [5]

Vaikka NotPetya vaati lunnaita (noin 300 puntaa Bitcoineina) muiden ransomwarejen tapaan, se erosi muista ransomwareista siten, että se salakirjoitti niin sanotun Master File Table:n muiden tiedostojen lisäksi. NotPetyaa tutkittaessa huomattiin, että se ei olisi pystynyt purkamaan salakirjoittamiensa tiedostojen salakirjoitusta, vaikka uhri olisi maksanut lunnaat. NotPetya on siis uudenlainen ransomware, koska sen tarkoitus ei ollut vain saada lunnaita uhrilta, vaan myös pysyvästi lukita uhrin tiedostot. [5]

NotPetya nimi on peräisin toisesta ransomwaresta, joka käytti nimeä Petya. Sekä Petyan että NotPetyan toiminta perustuu EternalBlue-tietoturva-aukkoon. Englanninkielinen sana ”not” eli suomeksi ”ei” NotPetyan nimen alussa viittaa siihen, että NotPetyan tarkoituksena ei ole avata lukittuja tiedostoja. [6]



Kuva 2 NotPetyan ilmoitus uhrille **[5]**

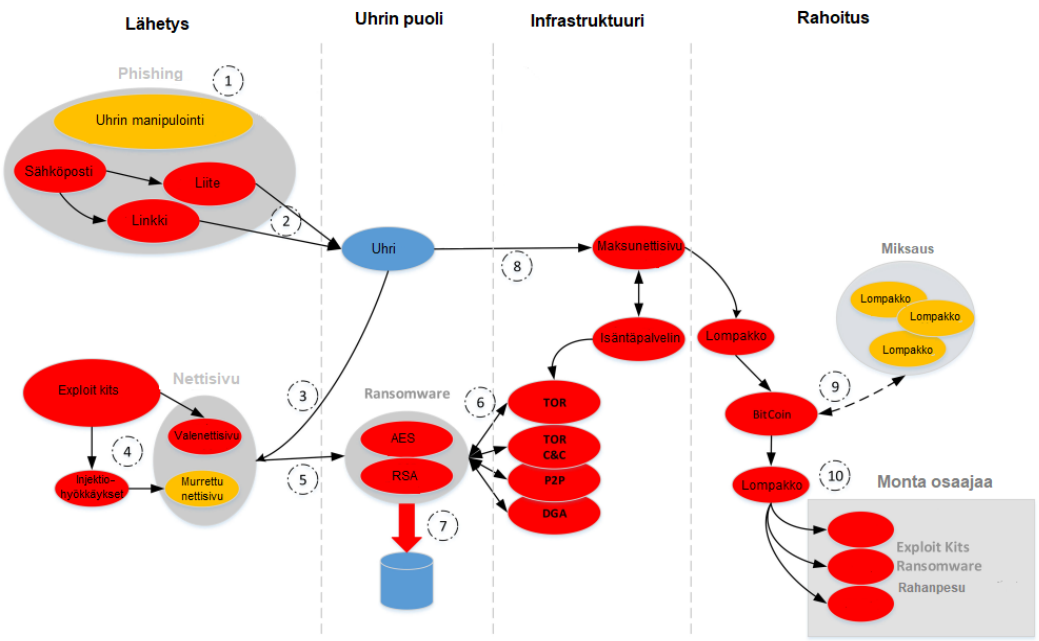
Kuvassa 2 on NotPetyan antama ilmoitus uhrille. Ilmoituksessa kerrotaan uhrin tiedostojen olevan lukittuja. Viestissä kerrotaan, että lukitut tiedostot ovat avattavissa ainoastaan maksamalla lunnaita 300 dollaria Bitcoineina. Kuten aikaisemmin todettiin, lunnaat maksamalla lukittuja tiedostoja ei saa avattua.

3. TOIMINTAPERIAATE

Ransomwaren toiminta perustuu viiteen askeleeseen. Ensimmäinen on uhrin etsiminen. Tämä tapahtuu esimerkiksi roskapostilla. Seuraava askel on saada uhri suorittamaan haittaohjelma. Tämä voidaan tehdä esimerkiksi siten, että haittaohjelman ikoni on vaihdettu suoritettavan tiedoston ikonista PDF-tiedoston ikoniksi, jolloin tämän tiedoston avaaminen ei tunnu niin vaaralliselta. Kolmannessa vaiheessa, haittaohjelman avaamisen jälkeen, luodaan salakirjoitusavain, jolla salataan tiedostot. Tämä salakirjoitusavain lähetetään automaattisesti haittaohjelman hallitsijan tietokoneelle tai palvelimelle. Neljännessä kohdassa tapahtuu itse tiedostojen salaaminen. Viimeisessä vaiheessa haittaohjelman uhri saa lunnasvaatimuksen. [3]

Tässä luvussa käsitellään aluksi ransomwaren toimintaperiaatetta yksityiskohtaisesti. Seuraavaksi käsitellään ransomwarejen yleisesti käyttämää tiedostojen salakirjoitusmenetelmää AES:ia. AES:n jälkeen käsitellään tiedostojen salaamiseen liittyvää julkisen avaimen salausalgoritmia RSA:ta. Lopuksi käydään vielä läpi syitä ransomwarejen käyttöön.

3.1 Toimintaperiaate



***Kuva 3 Ransomwaren toimintaperiaate* lähteeseen [4] perustuen**

Kuvassa 3 on esitetty useimpien ransomwarejen toimintaperiaate askel askeleelta. Kaikki ransomwaret eivät käyttäydy kuvan mukaisesti, mutta suurin osa käyttäytyy. [4]

1. Ensimmäisessä kohdassa uhria manipuloidaan avaamaan esimerkiksi sähköpostin haitallinen liitetiedosto tai uhria houkutellaan nettisivulla painamaan jotakin mainosta tai linkkiä.

2. Sähköpostit ovat ransomwarejen yksi yleisimmistä leviämistavoista. Nykyään sähköpostia käyttää iso osa maailman väestöstä, mutta valitettavasti kaikilla näistä käyttäjistä ei ole tietoturva niin hyvin hallussa, että he osaisivat tunnistaa haitalliset sähköpostit.

3. Hyökkäyksen alkuvaiheessa uhri ohjataan infektoituneelle nettisivulle tai joissakin tapauksissa ransomware latautuu suoraan uhrin tietokoneelle.

4. Infektoitunut nettisivu sisältää ohjelman, joka skannaa uhrin tietokonetta tietoturvaaukkojen ja muiden heikkouksien osalta, ja yrittää asentaa uhrin tietokoneelle ransomwaren.

5. Ransomware kuljetetaan uhrin tietokoneelle.

6. Ransomware on yhteydessä palvelimeensa ja lähettää sinne salauksenpurkuavaimen. Yhteytenä käytetään esimerkiksi TOR-verkkoa ja muita anonyymejä verkkoja.

7. Tässä vaiheessa käyttäjän data lukitaan salakirjoituksella. Myös uhrin tietokoneeseen kytketyt ulkoiset laitteet lukitaan salakirjoituksella.

8. Tässä vaiheessa käyttäjä huomaa joutuneensa ransomwaren uhriksi ja huomaa siis tiedostojensa lukittuneen. Uhri saa myös ransomwarelta ilmoituksen siitä, että uhrin tiedostot on lukittu, ja ransomware vaatii lunnaita lukituksen poistamisesta. Useat ransomwaret myös aiheuttavat uhrille lisäpaineita ilmoittamalla aikaikkunasta, jossa uhrin tulee maksaa lunnaat, tai haittaohjelma syyttää uhria jostakin rikoksesta.

9. Bitcoin ja muut kryptovaluutat ovat yleisin maksutapa, jolla ransomwaren vaatimat lunnaat voi maksaa. Lunnasrahat usein ”pestään” kierrättämällä maksu usean eri kryptolompakon kautta, jotta hyökkääjän identiteetti ei paljastuisi.

10. Ransomware ei ole nykyään enää yhdenmiehenoperaatio, vaan se vaatii monen eri osaajan työpanosta.

Ransomwarea on kahta erilaista tyyppiä: kryptograafiset ja ei-kryptograafiset. Ei-kryptograafisten ransomwarejen toiminta perustuu käyttäjän ja tietokoneen välisen yhteyden estämiseen esimerkiksi lukitsemalla tietokoneen näytön tai muokkaamalla kiintolevyn käynnistysosiota, jolloin tieto-

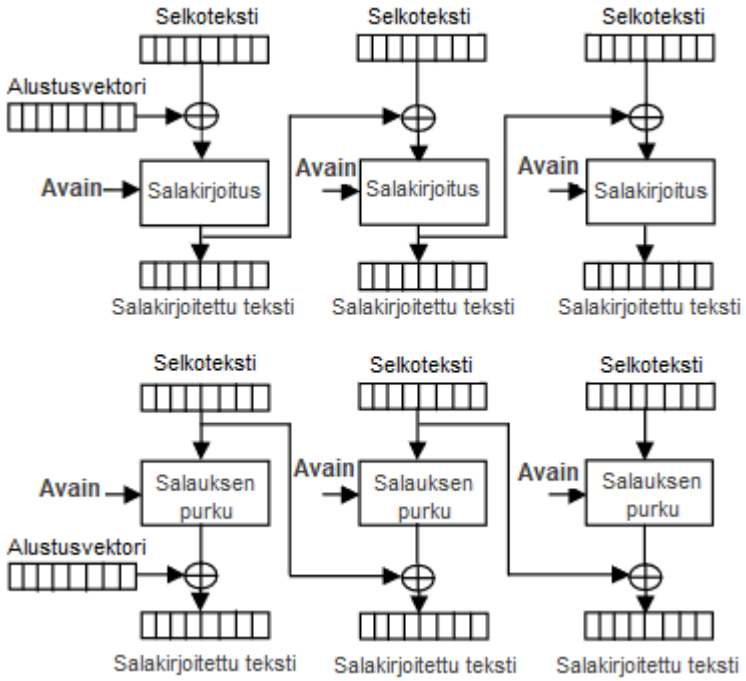
konetta ei pysty enää käynnistämään. Kryptograafiset ransomwaret eivät sinänsä estä tietokoneen käyttämistä muuten kuin lukitsemalla joitakin tiedostoja. Tiedostojen lukitseminen tapahtuu käyttämällä erittäin vahvoja kryptograafisia algoritmeja. [3] Hyvä esimerkki tällaisesta vahvasta kryptograafisesta algoritmista on AES (Advanced Encryption Standard). AES on vahva salausalgoritmi, jota USA:n hallitus käyttää huippusalaisten materiaalien salaamiseen [7].

3.1.1 AES

AES on yksi lukuisista eri salausmenetelmistä. Sen kehitti kaksi kryptograafikkoa, Vincent Rijmen ja Joan Daemen. AES kehitettiin vanhentuneen salausmenetelmän, DES:in (Data Encryption Standard), tilalle. AES on salausmenetelmä, joka hyödyntää lohkosalausmenetelmää. Lohkosalausmenetelmässä salakirjoitettava, vielä selväkielisessä muodossa oleva teksti eli selkoteksti jaetaan lohkoihin. Jokainen näistä lohkoista salataan käyttämällä samaa avainta. AES:n käyttämä lohkopituus on 128 bittiä. AES käyttää kolmea eri avainkokoa: 128, 192 ja 256 bittiä. AES on myös symmetrisen avaimen käyttöön perustuva, eli AES käyttää samaa avainta salakirjoittamaan selkotekstin ja purkamaan salakirjoitetun tekstin. [8]

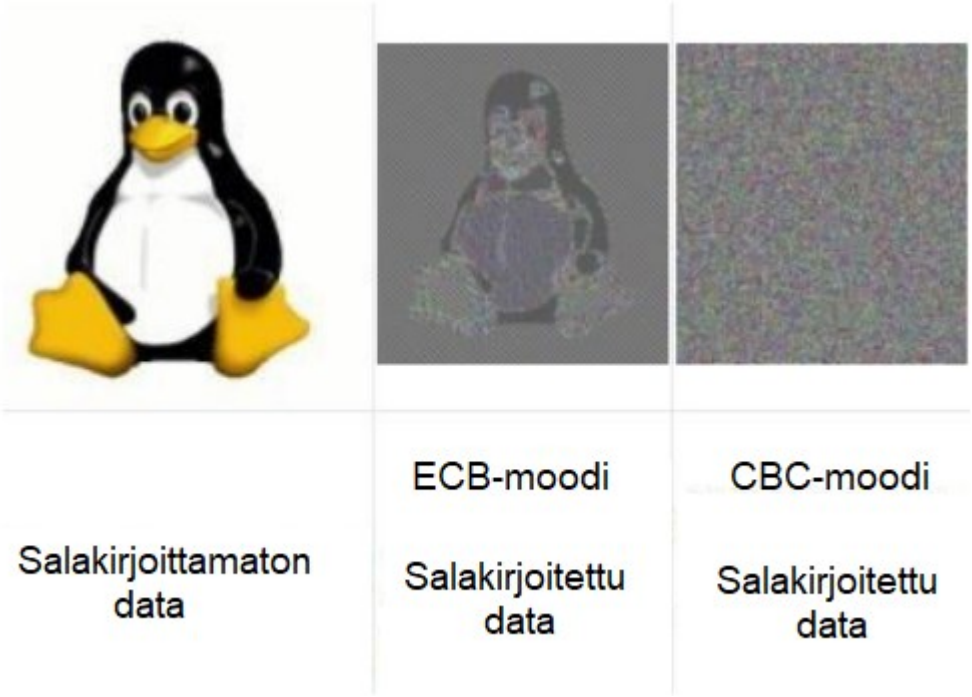
AES on iteroiva algoritmi ja jokaista sen suorittavaa iterointia kutsutaan kierrokseksi. Kierroksien lukumäärä on 10, 12 tai 14 riippuen valitusta avainkoosta. Jokainen AES:n kierroksista, viimeistä kierrosta lukuun ottamatta, koostuu maksimissaan neljästä muunnoksesta. Nämä muunnokset ovat nimeltään Sub Bytes, ShiftRows, MixColumns ja AddRoundKey. MixColumns-muutosta ei tapahdu viimeisellä kierroksella. Salakirjoituksen purku tapahtuu tekemällä salakirjoitusvaiheet käänteisjärjestyksessä. [9]

AES:in turvallisuutta tehostetaan käyttämällä sen yhteydessä jotakin moodia. Näitä moodeja on useita. Näistä moodeista yksinkertaisin on ECB (Electronic Codebook). ECB:tä edistyneempi ja turvallisempi moodi on CBC (Cipher Blocker Chaining). CBC toimii siten, että jokainen AES:lla salakirjoitettu lohko riippuu kaikista selkokielisistä tekstilohkoista, jotka on prosessoitu siihen mennessä. [9]



***Kuva 4 CBC:n toiminta perustuen lähteeseen* [10]**

Kuvassa 4 on esitetty CBC:n toiminta. Aluksi selkokielinen teksti eli selkoteksti XOR-operoidaan yhdessä alustusvektorin kanssa. Alustusvektori on jokin satunnaisesti valittu luku. XOR on looginen operaattori, jonka ulostulona on 1 vain, jos jompikumpi sen saamasta kahdesta syötteestä on arvoltaan 1. Lopuksi XOR-operoitu tulos salakirjoitetaan salakirjoitusavaimella ja tuloksena saadaan salakirjoitettu teksti. Tätä toistetaan vielä kaksi kierrosta. Niin kuin kuvasta 4 huomataan, salakirjoituksen purku tapahtuu tekemällä salakirjoituksen vaiheet käänteisessä järjestyksessä. [10]



Kuva 5 AES-ECB ja AES-CBC ero perustuen lähteeseen **[9]**

Kuvassa 5 havainnollistuu hyvin AES-ECB:n ja AES-CBC:n ero. Kuvan esimerkkiin on otettu salakirjoitettavaksi kohteeksi kuva. Vaikka ECB-moodia käytettäessä kuva salakirjoitetaan, salakirjoitettu lopputulos muistuttaa silti hyvin paljon alkuperäistä kuvaa. Käytettäessä CBC-moodia, lopputuloksesta ei voi päätellä tai nähdä, millainen alkuperäinen kuva oli.

3.1.2 RSA

RSA (Rivest–Shamir–Adleman) on tekijöidensä mukaan nimetty julkisen avaimen salausalgoritmi, eli toisin kuin AES, RSA on epäsymmetriseen salaukseen perustuva salausmenetelmä. RSA:n toiminta perustuu kahteen eri avaimeen: julkiseen ja yksityiseen avaimeen. Käyttämällä julkista avainta voidaan salakirjoittaa teksti siten, että nämä salakirjoitetut tekstit voidaan lukea ainoastaan toisella mainitulla avaimella, salaisella avaimella.

Ransomwaret hyödyntävät RSA:ta siten, että ne salakirjoittavat tiedostojen salakirjoitukseen käytetyn AES:in salakirjoitusavaimen [4]. Koska ransomwaren tekijällä eli ransomwaren isännällä on hallussaan RSA:n avainparin yksityinen avain, voi ransomware turvallisesti lähettää RSA:lla salakirjoitetun avaimen takaisin isännälleen.

3.2 Syitä ransomwaren käyttöön

Nyky-yhteiskunta on kehittymässä kovaa vauhtia tietoyhteiskunnaksi. Etäkäyttöisten tiedostojensäilytyspaikkojen, esimerkiksi pilvipalveluiden, käyttö on lisääntynyt valtavasti viime vuosina. Nämä tiedostojen säilytyspaikat sisältävät valtavia määriä dataa, mikä tekee niistä houkuttelevia

kohteita verkkorikollisille. Näitä tietoja rahastetaan käyttämällä ransomwareja pelkän varastamisen sijaan. Yksi pahimmista ransomwarehyökkäyksistä tapahtui helmikuussa vuonna 2016, kun eräässä sairaalassa ransomware lukitsi potilastietoja, eikä näihin tietoihin päästy enää käsiksi. Sairaala joutui lopulta maksamaan lunnaita 3,6 miljoonaa dollaria. [3] Tällaisia hyökkäyksiä varten tarvitaan tehokkaita suojautumiskeinoja.

NotPetyan tapauksessa hyökkääjien motiivit ovat hieman erilaiset. Vaikka hyökkääjät vaativat ransomwarensa uhriksi joutuneelta kohteelta lunnaita tiedostojen avaamista varten, ei lukittuja tiedostoja avata. NotPetyan epäillään olevan kybersodankäynnin väline, jonka päätarkoituksena rahankeruun sijaan on rampauttaa yrityksiä [6].

4. SUOJAUTUMINEN RANSOMWARELTA

Tässä luvussa käsitellään aluksi varmuuskopiointia. Sen jälkeen käsitellään tietoturvavalppautta. Voidaan ajatella, että paras tapaus suojautua ransomwarelta on yrittää välttyä saastumiselta kokonaan eli tietoturvavalppaus. Tietoturvavalppauden jälkeen käsitellään kahta tekniikka, joilla voidaan suojautua ransomwareilta. Ensimmäinen näistä tekniikoista on avainvarmuuskopiointitekniikka ja toinen on hunajatiedostomenetelmä. Lopuksi tässä luvussa käsitellään vielä suojautumista organisaation näkökulmasta.

4.1 Varmuuskopiointi

Ransomwarelta suojautumisen avain on omien tärkeiden tiedostojen varmuuskopiointi. Täytyy kuitenkin muistaa sijoittaa nämä varmuuskopioidut tiedostot sellaiseen paikkaan, joka ei mielellään ole yhteydessä internettiin ja on ainakin muussa paikassa, kuin alkuperäiset tiedostot. Tämä varmuuskopiointi koskee sekä tavallisia kotikäyttäjiä että yrityksiä. Ransomwaren saastutettua tietokoneen tai palvelimen se lukitsee siellä sijaitsevia tiedostoja.

Lukittaviksi tiedostoiksi kohdistuvat ransomwaren tekijän määrittelemät tiedostotyypit. Yleisemmät lukittavat tiedostotyypit ovat Microsoft Wordin tekstitiedostot .doc ja .docx, yleisimmät kuvatiedostot .jpg, .jpeg ja .png ja .txt sekä .pdf. Joskus ransomware ohjelmoidaan lukitsemaan suoraan koko Omat tiedostot –kansio (engl. ”My Documents”) riippumatta kansion sisällöstä. [4] Omat tiedostot –kansio on yleensä oletustallennuskansio eri tiedostoille, joten sen koko lukitseminen voi olla erittäin kohtalokasta. Ransomwaren luoja voi myös vapaasti määritellä, mitä tiedostotyyppejä ja missä sijainneissa ne lukitaan.

4.2 Tietoturvavalppaus

Tapoja, joilla ransomware ja muutkin haittaohjelmat saastuttavat uhrinsa tietokoneen, on monia. Helpoin tapa saastuttaa tietokoneensa on ladata ransomwaren sisältävä tiedosto ja avata se. Ransomwaren voi myös saada esimerkiksi sähköpostin liitetiedostona tai avaamalla saastunut nettisivu. Saastunut nettisivu on kaikista ongelmallisin tapaus, koska sivulla vieraileva ei välttämättä edes tiedä joutuneensa hyökkäyksen kohteeksi, koska sivu saattaa toimia täysin normaalisti ja niin kuin ennenkin. Sivuston koodiin ujutettu haittaohjelma, tässä tapauksessa ransomware, latautuu sivustolla vierailevan tietokoneelle automaattisesti sivuston avaamisen jälkeen, ja sitten se suorittaa itsensä. [3] Tällaisesta nettisivun saastuttamisesta haitallisella sisällöllä, yleensä JavaScript-koodinpätkällä, käytetään englannin kielessä nimitystä ”waterhole attack” [4].

Haittaohjelman sisältäviä tiedostoja vastaan voi suojautua parhaiten käyttämällä tietokoneellaan päivitettyä antivirusohjelmaa. Kuitenkaan paraskaan antivirusohjelma ei estä saastumista, jos käyttäjä väkisin suorittaa tiedoston antivirusohjelman varoituksista huolimatta. Antivirusohjelma voi olla myös liian tehoton havaitakseen haittaohjelman avattavan tiedoston sisällä. Saastunut tiedosto voi olla myös salakirjoitettu niin vahvasti, että antivirusohjelma ei tunnista sen olevan haitallinen. Tämän takia käyttäjältä vaaditaan tietoturvavalppautta.

Tiedostojen avaamisessa tarvitaan käyttäjältä valppautta eli käyttäjän tulee olla tietoinen eri tiedostotyypeistä. Yleinen rikollisten käyttämä keino saada uhri avaamaan haittaohjelmalla saastutettu tiedosto on nimetä tiedosto siten, että tiedostonimeen on laitettu esimerkiksi tavallisen tekstitiedoston pääte .txt, mutta itse varsinainen tiedostopääte onkin jotain ihan muuta. Esimerkki tällaisesta tilanteesta on tiedosto ”dokumentti.txt.exe”. Tässä esimerkissä käyttäjä saattaa huolimattomasti lukea, että tiedosto on tekstitiedosto, vaikka oikeasti tiedosto on .exe-päätteinen eli se on suoritettava sovellus.

Microsoft Wordin tekstitiedostoja käytettäessä pitää olla todella tarkkana, koska Wordin tekstitiedostoon on saatettu tehdä makro. Tällaiset makrot eivät ole suoraan haitallisia, mutta niiden sisältämät komennot voivat olla haitallisia ja ne voivat suorittaa haitallisen käskyn. Tällaisella haitallisella käskyllä voidaan esimerkiksi ladata internetistä tiedosto ja suorittaa se suoraan ilman käyttäjän suostumusta.

Myös .pdf –tiedostot voivat sisältää makroja. Nämäkin makrot voivat olla haitallisia. Pdf-tiedoston sisältämät haitalliset makrot toimivat hieman eri tavalla kuin Wordin makrot. Pdf-tiedoston haitallinen makro voi sisältää JavaScriptillä tehdyn makron. Tämä makro voi esimerkiksi avata Word-tiedoston, joka sekin sisältää uuden haitallisen makron. Haitallisten Word-tiedostojen makrot käsiteltiin jo aikaisemmin.

Tietoturvavalppauskaan ei aina riitä ransomwareilta suojautumiseen, vaan tarvitaan myös muita keinoja. Yksi näistä keinoista on avainvarmuuskopiointitekniikka.

4.3 Avainvarmuuskopiotekniikka

Jung Taek Seo *et al.* esittävät artikkelissaan [3] erään uudenlaisen tavan suojautua ransomwareilta: heidän kehittelemänsä avainvarmuuskopiointitekniikka. Ransomwaren salakirjoitettua uhrinsa tiedostot se yleensä lähettää salakirjoituksen purkamiseen vaadittavan purkuavaimen isäntäpavelimelleen. Artikkelissa esitetään tapa, jolla tämä salausavain kaapataan ja varmuuskopioidaan turvalliseen sijaintiin.

Artikkelissa esitetty avainvarmuuskopiointitekniikka toimii seuraavanlaisesti: Kun ransomware aloittaa tiedostojen lukitsemisen, se kutsuu käyttöjärjestelmän salakirjoituskirjastoa. Tässä vaiheessa tämä kutsu siepataan ja salakirjoitusavain kopioidaan talteen. Artikkelissa kerrotaan, että

tämän avainvarmuuskopiointitekniikan tueksi tehtiin oma ransomwareohjelma. Tämä ohjelma ohjelmoitiin salakirjoittamaan ennalta määrätyt tiedostot käyttämällä samaa tekniikkaa, kuin ”oikeat” ransomwareohjelmat. Salakirjoitusavain onnistuttiin poimimaan tiedostojen salakirjoitushetkellä, ja näin ollen tiedostojen lukitus voitiin purkaa maksamatta lunnaita. [3]

Yhteenvetona artikkelissa todettiin, että vaikka nykyään on jo tehokkaita ransomwareilta suojautumistekniikoita, ne eivät välttämättä enää riitä tulevaisuudessa. Tämä uusi kehitetty tekniikka on erittäin hyvä, koska sen toiminta perustuu tilanteeseen, jossa ransomware on jo ehtinyt tehdä tuhoa lukitsemalla tiedostoja. Nämä lukitut tiedostot kuitenkin pystytään luotettavasti avaamaan tällä metodilla. [3]

4.4 Hunajatiedostomenetelmä

J.A. Gómez-Hernández *et al.* esittelevät artikkelissaan [2] uudenlaisen lähestymistavan ransomwareilta suojautumiseen. Tämä lähestymistapa ei keskity pelkästään ransomwaren kiinni saamiseen tartunnan alkuvaiheessa, vaan tarkoituksena on estää ransomwaren toiminta kokonaan. Tämän uuden tavan pääideana on kylvää tietokoneelle ”hunajatiedostoja” eli tiedostoja, jotka houkuttelevat ransomwaren salakirjoittamaan ne ja saavat näin ransomwaren ansaan. Jos ransomware yrittää salakirjoittaa näitä hunajatiedostoja, ransomwaren toiminta estetään ja lisäksi aloitetaan automaattisesti puhdistustoimet ransomwaren poistamiseksi tietokoneelta. Menetelmää varten luotiin ohjelma nimeltä R-Locker, joka hoitaisi hunajatiedostomenetelmän käytännössä. [2]

Tätä hunajatiedostomenetelmää lähdettiin kehittämään keräämällä ensiksi lista asioista, jotka viittaavat ransomwaren läsnäoloon järjestelmässä:

- Kasvava määrä tiedostoja, joiden tiedostopääte on ennalta tunnetusti ransomwareihin liittyvä
- Tiettyjen tiedostojen muokkaus
- Tiettyjen erikoiskäskyjen ajaminen, esimerkiksi *vssadmin*-käsky estää järjestelmän palauttamisen edelliseen, puhtaaseen ja ransomware-vapaaseen tilaan
- Epäilyttävät tapahtumat Master File Tablessa
- (Master Boot Recordin) muokkaaminen siten, että järjestelmä ei pysty enää käynnistymään normaalisti, vaan käyttäjälle näytetään järjestelmän käynnistyksessä ransomwaren oma ilmoitus

[2]

Tämän listan perusteella lähdettiin rakentamaan R-Lockeria. R-Lockerille asetettiin tiettyjä vaatimuksia, joiden täyttyminen varmistaa ohjelman toimimisen käytännössä:

- Tehokkuus: Ransomwaren aiheuttama haitallinen toiminta järjestelmässä on oltava mahdollisimman pieni.
- Pieni tehonkulutus: Muistin käytön ja tallennustilan käyttö tulee olla pientä.
- Selkeys: Ohjelman ei tule vaatia erityisiä käyttöoikeuksia asennus- tai käyttövaiheessa. Muuten käyttäjät eivät tule käyttämään tätä ohjelmaa.
- Läpinäkyvyys: Ohjelman ei tule vaikuttaa muiden järjestelmän ohjelmien toimivuuteen. Muutoin saattaa ilmetä ongelmatilanteita.
- Yksinkertaisuus: Ohjelman tulee olla helppokäyttöinen. Tämä vaatimus ei ole kuitenkaan pakollinen, mutta se on silti toivottu ominaisuus.

[2]

R-Locker toimii siten, että se luo aluksi ansatiedostot eli hunajatiedostot. Näihin tiedostoihin kirjoitetaan satunnaista sisältöä. Jos jokin ohjelma alkaa lukea tällaista hunajatiedostoa, tämän ohjelman tiedot otetaan ylös. Lopuksi järjestelmän käyttäjälle annetaan ilmoitus havainnosta, ja käyttäjä voi joko todeta tiedoston luvun olleen sallittua tai sitten käyttäjä voi käskeä R-Lockeria poistamaan ransomwaren. [2]

4.5 Suojautuminen organisaation näkökulmasta

Tietoturvayhtiö McAfeen huomasi vuonna 2016, että ransomwarejen kohteina on yhä useammin yritys kotikäyttäjien sijaan. Tämä siksi, että yritykset ovat maksukykyisempiä maksamaan isompia lunnaita. Kyberrikolliset ottavat kohteekseen rahakkaita kohteita eli isoja organisaatioita, jotka käsittelevät arvokasta dataa, kuten talous-, henkilöstöhallinto- (engl. ”HR”) ja terveystietoja. [11]

Erityisesti sairaaloita varten kehitetyssä ohjeistuksessa Dean F. Sittig ja Hardeep Singh esittävät neliportaisen ohjeistuksen [12] ransomwareja vastaan. Tämän ohjeistuksen avulla organisaatiot pystyvät paremmin suojelemaan terveystietojaan. Ensimmäisessä vaiheessa organisaation IT-henkilöstön tulee varmistaa tietokoneiden ja verkkojen suojaukset. Seuraavaksi tulee huolehtia henkilökunnan tietoturvaosaamisesta ja kouluttamisesta. Kolmannessa vaiheessa organisaation tulee valvoa tietokoneiden käyttöä epäilyttävän käytöksen varalta ja tarvittaessa toimia ripeästi tietoturvaongelmia kohdatessaan. Viimeisessä vaiheessa organisaation tulee palautua ripeästi mahdollisista ransomwarehyökkäyksistä ja tehdä tarvittavat muutokset, jotta näitä hyökkäyksiä ei jatkossa tulisi. [12]

Tietoturvaratkaisuja yrityksille tarjoavan Duo Securityn mukaan ransomwaret ovat erityisen vaarallisia yrityksille, koska ne voivat rampauttaa kokonaan niiden toiminnan. Duo Security kertoo myös, että he saavat usein ilmoituksia organisaatioilta ransomwarehyökkäyksistä, mutta yritysten varmuuskopiointi on huonoa tai jopa olematonta. Varmuuskopiointien puuttuessa yritykset joutuvat pakon edessä maksamaan lunnaat saadakseen tiedostonsa takaisin. [11]

Kuten yksityishenkilöidenkin kohdalla, paras tapa suojautua ransomwarelta on pitää ohjelmistot, varsinkin antivirus-ohjelmistot, ja käyttöjärjestelmät päivitettyinä. Seuraavaksi kannattaa huolehtia varmuuskopioinnista. Varmuuskopiointi on hankalampaa organisaatioille kuin yksityishenkilöille, koska varmuuskopioitavaa dataa on mahdollisesti erittäin paljon ja se vie paljon tilaa. Myös datan arvo on varmasti organisaatioille kalliimpaa kuin yksityishenkilöille. Organisaatioiden varmuuskopiot tulee myös sijoittaa sellaiseen paikkaan, joka ei ole yhteydessä organisaation verkkoon, koska ransomwareilla on yleensä tapana levitä nopeasti saastuneen tietokoneen verkkoon. Esimerkiksi ulkoinen (USB:n) välityksellä tietokoneeseen kytketty kovalevy on huono vaihtoehto varmuuskopioinnille, jos tätä ulkoista kiintolevyä pidetään koko ajan kiinnitettynä tietokoneeseen. Organisaation yksittäisiä työntekijöitä koskevat samat tietoturvaneuvot kuin yksityishenkilöitäkin. Työntekijöitä tulee siis kouluttaa tietoturvariskeistä. [11]

Tietoturvaratkaisuja yrityksille tarjoavan Unisys:n varapuheenjohtajan Tom Pattersonin mukaan tehokkain tapa organisaatiolle ransomwareilta suojautumiseen on organisaation verkon segmentointi pieniin osiin eli mikrosegmentointi. Sisäverkon mikrosegmentoinnissa jokainen sisäverkossa lähetetty paketti allekirjoitetaan. Tietyssä mikrosegmenttiverkossa sallitaan vain tämän tietyn mikrosegmenttiverkon paketit. Näin estetään tehokkaasti ransomwaren leviämistä organisaation sisäverkon sisällä tietokoneesta toiseen. [11]

Etäyhteysohjelmia tarjoavan Bomgarin varapuheenjohtajan Stuart Faceyn mukaan organisaatioon kohdistuvista haasteista isoin on ymmärrys siitä, kenellä on pääsyoikeus tietoon ja millä tasoilla organisaation verkossa. Organisaation tulee olla selvillä siitä, että työntekijän hakiessa pääsyä laitteelle tai verkkoon kyseessä on oikeasti oikea henkilö. Ei ole kuitenkaan takeita siitä, etteikö verkkorikollinen olisi tunkeutunut organisaation verkkoon ja ole saamassa samalla lisää pääsyä organisaation verkkoon tai laitteisiin työntekijän tekemän haun mukana. Verkkorikollisille organisaation ylläpitäjän pääsyoikeuksien saaminen organisaation verkkoon on erittäin tavoiteltua. Tämän takia verkkorikolliset ottavatkin usein kohteekseen organisaatioiden verkkojen sellaisia laitteita, joista on pääsy muihin laitteisiin ja verkkoihin. Tällaisten hyökkäyksien takia organisaation tulee olla perillä siitä, että keillä työntekijöillä on pääsy mihinkin paikkoihin ja voisiko näitä pääsyoikeuksia rajoittaa ja kuinka paljon. [11] Optimaalisessa tilanteessa työntekijöillä on pääsy vain sellaisiin verkkoihin, joita he oikeasti tarvitsevat työntekoonsa.

5. YHTEENVETO

Nykyisessä tietoyhteiskunnassa ransomwaret ovat erittäin iso uhka muiden haittaohjelmien lisäksi. Ransomwarejen kohteena ovat sekä yksityiset käyttäjät, että organisaatiot. Varsinkin organisaatioiden tulee olla varuillaan ransomwarejen osalta. Organisaatiot ovat houkuttelevampia kohteita, kuin yksityiset käyttäjät, koska organisaatiot pitävät hallussaan enemmän ja todennäköisesti arvokkaampaa dataa. Ransomwareilta voi suojautua parhaiten pitämällä järjestelmien suojaukset ajan tasalla. Tämän lisäksi tarvitaan tietoturvavalppautta.

Tässä työssä käytiin läpi kaksi uutta ransomwareilta suojautumiskeinoa, avainvarmuuskopiointimenetelmä ja hunajatiedostomenetelmä. Nämä molemmat suojautumiskeinot ovat vielä kehitysasteilla, mutta jatkokehityksen jälkeen niistä saadaan varmasti kaksi hyvää suojautumiskeinoa ransomwareja vastaan. Nämä kaksi suojautumiskeinoa voisi myös mahdollisesti yhdistää yhdeksi kokonaisuudeksi.

Koska ransomwaret kehittyvät koko ajan, tulee suojautumiskeinojenkin kehittyä. Ransomwareja vastaan taistellaan tällä hetkellä kehittelemällä uudenlaisia suojautumiskeinoja, kuten avainvarmuuskopiointitekniikka ja hunajatiedostomenetelmä. Tulevaisuudessa tarvitaan kuitenkin uusia keinoja ransomwarejen kehittyessä. Europolin laatiman raportin mukaan [13] tulevaisuudessa uhkaksi muodostuu mobiililaitteilla toimivat ransomwaret.

LÄHTEET

[1] Master File Table (MFT) Saatavissa (viitattu 28.2.2019): https://docs.microsoft.com/en-us/windows/desktop/devnotes/master-file-table

[2] J.A Gómez-Hernández, L. Álvarez-González & P. García-Teodoro, R-Locker: Thwarting ransomware action through a honeyfile-based approach, Computers & Security, Vol. 73, Mar 2018, pp. 389–398. Saatavissa (viitattu 11.3.2019): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0167404817302560

[3] J. T. Seo, Y. Kangbin, L. Kyungroul, Ransomware prevention technique using key backup, Concurrency and Computation: Practice and Experience, Vol. 30(3), Oct 2017, pp. e4337–n/a. Saatavissa (viitattu 17.1.2019): https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.4337

[4] P. O'Kane, S. Sezer, D. Carlin, Evolution of ransomware, IET Networks, Vol. 7, No. 5, 23 Aug 2018, pp. 321–327. Saatavissa (viitattu 17.1.2019): https://ieeexplore.ieee.org/document/8444566

[5] D. Emm, S. Furnell, The ABC of ransomware protection, Computer Fraud & Security, Vol. 2017(10), Oct 2017, pp. 5–11. Saatavissa (viitattu 17.1.2019): https://www.sciencedirect.com/science/article/pii/S1361372317300891

[6] A. Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History Saatavissa (viitattu 28.2.2019): https://www.wired.com/story/notpetya-cyberattack-ukraine-rsia-code-crashed-the-world/

[7] L. Hathaway, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, Jun 2003. Saatavissa (viitattu 9.3.2019): https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

[8] Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, Nov 2001, Saatavissa (viitattu 11.3.2019): https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[9] A. Pillai, R. Kadikar, M.S. Vasanthi & B. Amutha, Analysis of AES-CBC Encryption for Interpreting Crypto-Wall Ransomware, IEEE, Apr 2018, pp. 0599. Saatavissa (viitattu 11.3.2019): https://ieeexplore-ieee-org.libproxy.tuni.fi/stamp/stamp.jsp?tp=&arnumber=8524494

[10] M. Vaidehi & B.J. Rabi, Design and analysis of AES-CBC mode for high security applications, IEEE, Jul 2014, pp. 499. Saatavissa (viitattu 28.3.2019): https://ieeexplore-ieee-org.libproxy.tuni.fi/document/6966347

[11] S. Mansfield-Devine, Ransomware: taking businesses hostage, Network Security, Vol. 2016, No. 10, Oct 2016, pp. 8–17. Saatavissa (viitattu 24.1.2019): https://www.sciencedirect.com/science/article/pii/S1353485816300964

[12] D. F. Sittig & H. Singh, A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks, Applied clinical informatics 7.02: 624-632, Jun 2016. Saatavissa (viitattu 18.4.2019): https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4941865/

[13] Internet Organised Crime Threat Assessment (IOCTA) raportti 2018 Saatavissa (viitattu 28.3.2019): https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf