Kiristysohjelmien toimintatavat ja haittavaikutukset

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tieto- ja viestintätekniikka
Joulukuu 2025
Joonas Hovinen

TURUN YLIOPISTO
Tietotekniikan laitos

Joonas Hovinen: Kiristysohjelmien toimintatavat ja haittavaikutukset

TkK-tutkielma, 22 s.
Tieto- ja viestintätekniikka
Joulukuu 2025

Viime vuosikymmeninä haittaohjelmat ovat kehittyneet yksinkertaisista vitsiohjelmista sivistyneiksi hyökkäyksiksi kiristysohjelmien muodossa. Kiristysohjelmat (engl. ransomware) ovat merkittävä uhka yksityishenkilöille, yrityksille ja julkisille organisaatioille maailmanlaajuisesti. Ransomware-as-a-service (RaaS) -malli on madaltanut kynnystä kiristysohjelmahyökkäysten toteuttamiseen ja mahdollistanut haittaohjelmien leviämisen myös kokemattomien toimijoiden toimesta. Lisäksi kryptovaluuttojen käyttö on helpottanut lunnasmaksujen vastaanottamista jäljittämättömällä tavalla.

Kiristysohjelmat ovat taloudellisesti kannattavia, jonka takia niiden kehitys on jatkuvaa. Jotta vastatoimia voidaan kehittää, on ymmärrettävä kiristysohjelmien toimintatavat. Tässä kirjallisuuskatsauksessa tarkastellaan kiristysohjelmien toimintaperiaatteita, leviämistapoja, hyökkäysvektoreita sekä tunnetuimpia maailmanlaajuisia kiristysohjelmia, kuten WannaCry, NotPetya ja LockBit. Lisäksi tarkastellaan kiristysohjelmien käyttämiä salaus- ja naamioitumistekniikoita, sekä keinoja havaita ja torjuta kiristysohjelmien toimintaa. Kirjallisuuskatsauksessa käsitellään myös kiristysohjelmien kehitystä sekä tunnettujen kiristysohjelmien aiheuttamia haittavaikutuksia.

Asiasanat: kiristysohjelmat, haittaohjelmat, tietoturva

Sisällys

1 Johdanto

Nykypäivänä lähes kaikilla on esteetön pääsy internetiin jollain laitteella, eikä se vaadi käyttäjältä minkäänlaista tietämystä tietoturvasta. Tämän seurauksena kyberrikollisuus on noussut suureen suosioon - tietämätöntä käyttäjää on helppo huijata ja vaikka virustorjuntaohjelmat ovat usein esiasennettuja, haittaohjelmille altistuminen eri laitteilla on yleistä.

Haittaohjelma on yleinen käsite sellaisille tietokoneohjelmille, jotka jollain tavalla varastavat tai tuhoavat tietoja, tai häiritsevät tietoliikennettä tietokoneessa tai tietojärjestelmässä. Haittaohjelmat luokitellaan niiden toimintaperiaatteiden, käytöksen ja leviämistaktiikoiden perusteella eri kategorioihin, kuten virukset, madot, troijalaiset, vakoiluohjelmat ja kiristysohjelmat.

Erityisesti viime vuosikymmenenä kiristysohjelmat ovat nousseet suosioon. Kiristysohjelmilla tarkoitetaan haittaohjelmia, jotka jollain tavalla estävät pääsyn uhrin tiedostoihin tai lukitsevat tämän laitteen kokonaan, ja jotka tyypillisesti tarjoavat pääsyn takaisin maksua vastaan. Niiden yleistymisen ohella kiristysohjelmat ovat osoittautuneet vakavaksi uhaksi monien yritysten järjestelmille ja tietokannoille, kuten myös kriittiselle infrastruktuurille.

1.1 Tutkielman tarkoitus ja tutkimuskysymykset

Kiristysohjelmia on useita erilaisia ja niistä jokaisella on omat toimintaperiaatteet. Tämän tutkielman tarkoituksena on analysoida kiristysohjelmien käyttämiä keino-

ja levitä ja naamioitua, sekä tutkia niiden haittavaikutuksia ja niiden aiheuttamia vahinkoja. Tämä suoritetaan käymällä läpi aiheen kirjallisuutta, sekä ottamalla aiemmin hyvin tunnettuja kiristysohjelmia tarkasteltavaksi. Näistä kiristysohjelmista tutkitaan niiden toimintatapoja liittyen leviämiseen, tiedostojen salaamiseen ja yleiseen käytökseen. Tutkielma pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

1. Kuinka kiristysohjelmat toimivat?

2. Mitkä ovat kiristysohjelmien haittavaikutukset?

1.2 Tutkielman rakenne ja tutkimusmenetelmät

Tutkielman toisessa kappaleessa käsittellään kiristysohjelmia yleisesti ja käydään läpi niiden historiaa ja kehitystä. Kolmannessa kappaleessa käsitellään tarkemmin kiristysohjelmien hyökkäysmenetelmiä ja toimintaperiaatteita. Neljännessä kappaleessa käydään läpi tunnettujen kiristysohjelmien käyttämiä toimintatapoja ja niiden aiheuttamia haittavaikutuksia. Viides kappale sisältää yhteenvedon läpikäydyistä asioista.

Tutkielma on suoritettu kirjallisuuskatsauksena. Aineistoa on haettu eri tietokannoista tarkkaan määritellyillä hakulauseilla ja pelkästään englanninkielisiä aineistoja on käytetty. Tiedonhakua on suoritettu IEEE-, ACM-, Web of Science- ja Science Direct-tietokannoista. Käytettyjen hakulausekkeiden tarkoituksena on löytää aineistoa haittaohjelmien ja kiristysohjelmien toiminnasta yleisesti, sekä tiettyjen kiristysohjelmien toimintatavoista. Suurimmaksi osaksi haku on toteutettu käyttämällä hakulauseketta "(Ransomware OR "Crypto-ransomware") AND (Obfuscat* OR Attack OR Spread*) AND method*"hieman muunneltuna tietokannasta riippuen. Tämä mahdollistaa aineiston löytämisen liittyen kiristysohjelmien naamioitumis-, hyökkäys-, sekä leviämismenetelmiin. Lausekkeen alkuosaa (Ransomware OR "Crypto-ransomware") on käytetty, koska hakua suorittaessa huoma-

sin joidenkin aineistojen käyttävän kiristysohjelmalle nimenomaan termiä "Crypto-ransomware" pelkän "Ransomware" sijaan. Lisäksi aineistoina on käytetty CISA:n (Cybersecurity and Infrastructure Security Agency) eli Yhdysvaltojen kyberturvallisuus- ja infrastruktuuriturvallisuusviraston julkaisuja, sekä Kasperskyn ja VirusTotalin tilastoja.

2 Kiristysohjelmat

Haittaohjelmia tunnetaan jo 1970-luvulta. Haittaohjelmilla tarkoitetaan haitallista koodia sisältäviä ohjelmia, jotka tarkoituksellisesti aiheuttavat ei-toivottuja tapahtumia laitteessa. Tyypillisesti haittaohjelmat keräävät laitteen käyttäjältä henkilökohtaisia tietoja ja pyrkivät toimimaan huomaamattomasti, jotta niiden läsnäolo ei paljastuisi. Kiristysohjelmilla on toisenlainen toimintatapa; tarkoituksena on saada käyttäjän huomio ja saada tämä maksamaan lunnaita pitäen laitetta ja tiedostoja panttina.

Ensimmäinen kiristysohjelma, joka tunnetaan AIDS-troijalaisena, ilmaantui vuonna 1989. Troijalaisen pääperiaate oli sama kuin nykyajan kiristysohjelmilla, eli tiedostoihin pääsy evättiin lunnaita vastaan. [1] Tämä ohjelma levisi fyysisesti tartunnan saaneita levykkeitä jakamalla. Levykkeissä oli harjaanjohtava kansikuva ja ohjelma määritellään troijalaiseksi, koska sen annettiin olettaa olevan tavallinen ohjelma.

Kiristysohjelmahyökkäykset ovat yleistyneet suurelta osaa myös siitä syystä, että kiristysohjelmien luominen ja levittäminen käyttäen nykyään saatavilla olevia työkaluja on helpottunut huomattavasti. Ransomware-as-a-service (RaaS)-malli on yleisimmin hyödynnetty tapa levittää kiristysohjelmia, sillä se mahdollistaa myös kokemattomien toimijoiden toteuttaa teknisesti kehittyneitä hyökkäyksiä [2]. RaaS-malli perustuu siihen, että joku yksilö tai ryhmä kirjoittaa kiristysohjelman ja myy tämän sitten eteenpäin räätälöitynä asiakkaalle. Asiakas on tässä tapauksessa se,

joka käynnistää hyökkäyksen kohteeseen. Tilastojen mukaan yli 4000 kiristysohjelmahyökkäystä toteutetaan päivittäin [2], mutta ne kohdistuvat lähes yksinomaisesti Microsoft Windows-alustoihin, vaikka esimerkiksi Linux OS:lle ja Androidille niitä on havaittu. Tutkimusten mukaan noin 95 % kaikista kiristysohjelmaan viittaavista havainnoista kohdistuvat Windows-laitteille [3].

Ennen kryptovaluuttojen yleistymistä kiristysohjelmilla oli hankaluuksia saada maksu luotettavalla tavalla. Kiristysohjelmien kehittäjille ei ollut saatavilla maksutapaa, jota on mahdoton jäljittää ja joka toimii sijainnista riippumatta. Oli yleistä, että maksutapana toimi esimerkiksi Paysafecard, MoneyPak tai jokin vastaava, mutta nämäkään eivät ole saatavilla kaikille maasta riippuen. [4] Kun kryptovaluutat kuten Bitcoin alkoivat nousta suosioon vuonna 2009, kiristysohjelmat alkoivat käyttää niitä maksujen suorittamiseen, sillä ne ratkaisivat kaikki maksuun liittyvät ongelmat.

2.1 Lukitsevat kiristysohjelmat

Kiristysohjelmat luokitellaan tyypillisesti kahteen pääkategoriaan: lukitseviin kiristysohjelmiin ja salaaviin kiristysohjelmiin. Lukitsevat kiristysohjelmat rajoittavat uhrin laitteen toimintaa ja esittävät viestin, jossa ohjeistetaan maksamaan rahasumma laitteen normaalin käytön palauttamiseksi [5]. Käytännössä rajoittaminen toteutetaan esimerkiksi lukitsemalla näyttö tai poistamalla näppäimistön ja hiiren toiminnallisuus. Usein kiristysohjelma estää myös pääsyn tehtävienhallintaan tai virustentorjuntaohjelmiin, ja se määritetään suorittumaan automaattisesti käyttöjärjestelmän käynnistyksen yhteydessä.

Tämän kategorian tuhoisimpia muotoja ovat pääkäynnistystietueen (engl. Master Boot Record, MBR) ylikirjoittavat kiristysohjelmat. Pääkäynnistystietue sijaitsee massamuistilaitteen, kuten kiintolevyn, ensimmäisessä lohkossa ja sisältää tiedot levyn partitioista sekä koodin, joka käynnistää käyttöjärjestelmän. Pääkäynnistys-

tietuekiristysohjelmat ylikirjoittavat tai salaavat tämän alueen, mikä tekee käyttöjärjestelmän käynnistämisen mahdottomaksi. Tällöin lunnasviesti voidaan näyttää välittömästi käynnistyksen yhteydessä, eikä laitetta voi käyttää muuhun. Lukitseviin kiristysohjelmiin ei kuitenkaan sisälly varsinaista tiedostojen vahingoittamista tai tuhoamista, minkä vuoksi tiedot voidaan useimmissa tapauksissa palauttaa ilman lunnasrahojen maksamista. Jos pääkäynnistystietue on ylikirjoitettu, se on kuitenkin rakennettava uudelleen ennen kuin tietoihin voidaan jälleen päästä.

2.2 Salaavat kiristysohjelmat

Salaavat kiristysohjelmat salakirjoittavat uhrin tiedostot, mikä tekee niistä käyttökelvottomia. Tämän jälkeen ne vaativat lunnaita salauksen purkamiseen tarvittavan avaimen saamiseksi. Tämä tarkoittaa, että vaikka haittaohjelma saataisiin poistettua järjestelmästä, salatut tiedostot pysyvät ilman salausavainta pysyvästi lukukelvottomina.

Ensimmäisenä salaavana kiristysohjelmana pidetään AIDS-troijalaista. Se hyödynsi yksinkertaista symmetrisen salauksen ja alustavektorin yhdistelmää järjestelmässä havaittujen tiedostojen salaamiseen [5]. Kyseinen salausmenetelmä on kuitenkin nykyaikaisiin tekniikoihin verrattuna helposti murrettavissa.

Ensimmäinen RSA-salausalgoritmia hyödyntävä kiristysohjelma, Gpcode, havaittiin Venäjällä vuonna 2004. Kiristysohjelman ensimmäiset variantit käyttivät vielä heikkoja salausmenetelmiä, mutta vuonna 2006 ohjelman kehittäjä julkaisi useita uusia variantteja, joissa hyödynnettiin eripituisia RSA-avaimia salaamiseen. Tämä kehitys oli merkittävä, sillä nykyisistä tunnetuista kiristysohjelmista noin kolmasosa käyttää RSA-salausta [6].

Salaavat kiristysohjelmat ovat huomattavasti yleisempiä kuin lukitsevat kiristysohjelmat, ja niiden arvioidaan muodostaneen noin 90 % kaikista kiristysohjelmahyökkäyksistä vuonna 2019 [7]. Lisäksi ne voidaan jaotella käytetyn salausmene-

telmän perusteella symmetristä, epäsymmetristä tai hybridisalausta hyödyntäviin kiristysohjelmiin.

2.2.1 Symmetrinen salaus

Symmetrinen salaus perustuu siihen, että viestin lähettäjä ja vastaanottaja käyttävät viestin salauksessa ja salauksen purkamisessa samaa avainta [8]. Tunnettuja symmetrisiä salausalgoritmeja ovat esimerkiksi Data Encryption Standard (DES) ja Advanced Encryption Standard (AES). Symmetristä salausta hyödyntävät kiristysohjelmat käyttävät yhtä ja samaa avainta tiedostojen salaukseen ja purkuun, ja salausalgoritmi on tyypillisesti upotettu suoraan haittaohjelman koodiin.

Symmetrisen salauksen etuna on sen nopeus. Sitä hyödyntäen tiedostot voidaan salata hyvin lyhyessä ajassa. Tämän vuoksi, vaikka virustorjuntaohjelma tunnistaisi kiristysohjelman toiminnan ja siirtäisi sen karanteeniin, suuri osa uhrin tiedostoista saattaa jo olla salattu. Tässä vaiheessa voi syntyä ongelma, jossa kiristysohjelma on poistettu tai eristetty ja tiedostot pysyvät salattuna, sillä salauksen purkuavain tai purkutoiminnallisuus oli ainoastaan kyseisen ohjelman sisällä.

2.2.2 Epäsymmetrinen salaus

Epäsymmetrinen salaus on salausmenetelmä, jossa salaukseen ja salauksen purkuun käytetään eri avaimia. Sitä käytetään usein synonyyminä julkisen avaimen salaukselle, koska yleisesti käytetyt julkisen avaimen salauksen algoritmit kuten RSA ja ECC edustavat epäsymmetristä salausmallia. Verrattuna symmetriseen salaukseen epäsymmetrinen salaus on laskennallisesti raskaampaa ja siten hitaampaa [8], mutta turvallisempaa, koska salauksen purkamiseen ei riitä yksi avain. Tämä tarkoittaa, että kiristysohjelman käyttämä epäsymmetrinen salaus voi antaa virustorjuntaohjelmalle tai käyttäjälle enemmän aikaa havaita haitallinen toiminta ja pysäyttää se ennen laajamittaisen vahingon syntymistä.

2.2.3 Hybridisalaus

Hybridisalaus yhdistää symmetrisen ja epäsymmetrisen salauksen edut. Hybridisalausta hyödyntävät kiristysohjelmat salaavat ensin uhrin tiedostot symmetrisellä salauksella ja tämän jälkeen salaus- ja purkuavaimet epäsymmetrisellä salauksella. Tällöin salausprosessi säilyttää symmetrisen salauksen nopeuden ja epäsymmetrisen salauksen tarjoaman turvallisuuden. [8]

2.3 Leviäminen

Troijalaisella tarkoitetaan haittaohjelmaa, joka on naamioitu tavalliseksi ja luotettavaksi ohjelmaksi tai on muutoin toiminnan kannalta normaali sovellus, mutta sisältää siihen upotettua haitallista koodia. Ohjelma voi näyttäytyä käyttäjälle täysin normaalina, mutta taustalla se voi avata takaovia, joiden kautta ulkopuolinen toimija saa luvattoman pääsyn järjestelmän tietoihin. Tätä leviämistaktiikkaa käytti CryptoLocker-niminen kiristysohjelma [9], jota käsitellään tarkemmin erillisessä luvussa.

Mato on haittaohjelmatyyppi, joka leviää automaattisesti järjestelmästä toiselle ilman käyttäjän toimenpiteitä. Madot voivat levitä esimerkiksi paikallisissa verkoissa, internetissä TCP:n (Transmission Control Protocol) välityksellä, vertaisverkoissa, sekä sähköpostin tai pikaviestisovelluksien kautta [10].

Haavoittuvuus on tietojärjestelmässä tai verkossa oleva heikko kohta, jota hyökkääjät voivat hyödyntää saadakseen luvattoman pääsyn järjestelmään [11]. Haavoittuvuuksien hyödyntäminen mahdollistaa haittaohjelmien, erityisesti matojen, erittäin nopean leviämisen ilman käyttäjän toimenpiteitä. Tunnetuimpia esimerkkejä on Mydoom-mato vuodelta 2004, joka levisi sähköpostin välityksellä poikkeuksellisen nopeasti, tartuttaen arviolta 50 miljoonaa tietokonetta maailmanlaajuisesti ja aiheuttaen noin 38 miljardin dollarin vahingot yrityksille ja yksityishenkilöille [12].

Haavoittuvuuksien avulla voidaan ohittaa tärkeitä turvallisuusominaisuuksia ja avata takaovia tartunnan mahdollistamiseksi.

Kiristysohjelmat muodostavat merkittävän uhan varsinkin yrityksille. Yritysympäristössä yksittäisissä työasemissa säilytetään usein vain käyttöjärjestelmä ja välttämättömät sovellustiedostot, kun taas liiketoiminnan kannalta tärkeät tiedostot tallennetaan keskitetysti jaetuille verkkolevyille. Tämä helpottaa tiedostojen jakamista ja varmuuskopiointia, mutta samalla altistaa järjestelmän kiristysohjelmille. Mikä tahansa verkkoon liitetty laite voi toimia tartuntapintana. Jos yksi työasema saa kiristysohjelmatartunnan, voi se salata kaikki jaetut resurssit, joihin sillä on käyttöoikeus, vaikka itse työasemalla ei olisi mitään arvokasta tietoa. [13]

2.4 Naamioitumisen menetelmät

Kiristysohjelmien keskeisimpiä ominaisuuksia hyökkääjän näkökulmasta on niiden kyky pysyä huomaamattomana siihen saakka, kunnes kohdejärjestelmän tiedostot on ehditty salata. Kiristysohjelmien havaitsemiseen kätetyt työkalut toimivat perinteisten virustorjuntaohjelmien tavoin ja hyödyntävät samankaltaisia tekniikoita, kuten ohjelmabinäärien staattista analyysia ennen ohjelman suorittamista. Vaikka nämä menetelmät tarjoavat perustason suojaa, ne voivat tuottaa vääriä negatiivisia tuloksia erityisesti uusien tai naamioitumistekniikoita hyödyntävien haittaohjelmien kohdalla. [13] Kiristysohjelmat käyttävät naamioitumiseen useita eri tekniikoita, kuten roskakoodin upottamista ohjelmaan, ohjelman muuttujien uudelleennimeämistä, polymorfismia ja erilaisten pakkausmenetelmien käyttöä [14].

Roskakoodin upottaminen tarkoittaa tarpeettoman koodin lisäämistä ohjelmaan siten, että ohjelman toiminnallisuus ei muutu. Sen tarkoituksena on tehdä ohjelmasta monimutkaisempi ja suurempi kooltaan, joka vaikeuttaa erityisesti staattista analyysia. Muuttujien uudelleennimeäminen puolestaan estää ohjelman toimintaan perustuvien nimeämiskäytäntöjen välittymistä käännettyyn binääriin. Polymorfisel-

la haittaohjelmalla tarkoitetaan sellaista haittaohjelmaa, joka hyödyntää salausalgoritmeja muuttaakseen binääristä muotoaan jokaisella suoritus- tai leviämiskerralla havaintojen välttämiseksi. Tämänkaltaista naamioitumistaktiikkaa käyttää esimerkiksi LockBit 3.0-kiristysohjelma [15]. Lisäksi haittaohjelmat voivat hyödyntää erilaisia pakkausmenetelmiä, joiden avulla ohjelma puretaan vasta suorituksen aikana, mikä vaikeuttaa virustorjuntaohjelmien tekemää analyysia ja tunnistusta.

3 Hyökkäysmenetelmät

3.1 Hyökkäysvektorit

Kiristysohjelmien leviämisessä käytetään useita eri menetelmiä, joita kutsutaan hyökkäysvektoreiksi. Tyypillisiä kiristysohjelmien käyttämiä hyökkäysvektoreita ovat muun muassa sähköpostit, SMS-viestit, kolmannen osapuolen sovelluskaupat, itsestään leviävät haittaohjelmat sekä sosiaalisen manipuloinnin taktiikat.

Sähköposti on yleisimmin käytetty hyökkäysvektori kiristysohjelmien levittämisessä [4]. Hyökkääjät lähettävät uhreille sähköposteja, jotka sisältävät harhaanjohtavan linkin tai liitetiedoston, jonka avaaminen johtaa haittaohjelman asentumiseen laitteelle. Arviolta 63,3 % kiristysohjelmatartunnoista välittyy sähköpostin kautta, joista 35,7 % liitetiedostojen ja 28,6 % sähköpostissa olevien linkkien kautta [16]. Haitalliset sähköpostit perustuvat usein verkkourkintaan (engl. phishing), jossa viestit naamioidaan näyttämään luotettavalta taholta, kuten pankilta tai tuttavalta.

Laajamittainen sähköpostien levittäminen toteutetaan usein bottiverkkojen avulla [4]. Bottiverkot muodostuvat kaapatuista tietokoneista tai muista verkkoon liitetyistä laitteista, joita hyökkääjä voi käyttää huomaamattomasti erilaisten haitallisten toimintojen, kuten palvelunestohyökkäysten toteuttamiseen tai roskapostin lähettämiseen.

Etätyöpöytäyhteys (engl. Remote Desktop Protocol) (RDP) on kiristysohjelmien toiseksi yleisimmin hyödyntämä hyökkäysvektori [4]. RDP on Microsoftin kehittä-

mä protokolla, jonka avulla voidaan luoda etäyhteys tietokoneeseen ja hallita sitä etäkäyttöisesti. Protokollasta on vuosien varrella löydetty haavoittuvuuksia, joita hyökkääjät ovat hyödyntäneet kiristysohjelmien levittämisessä ja haitallisen koodin suorittamisessa etänä [4].

Haittaohjelma-alustat (engl. exploit kit) ovat työkaluja, jotka automatisoivat haavoittuvuuksien hyväksikäyttöä. Laitteelle asennetuista ohjelmistoista saattaa löytyä haavoittuvuuksia, jotka mahdollistavat tartunnan saamisen. Haavoittuvuuksien hyödyntäminen voi olla tavalliselle käyttäjälle vaikeaa, mutta haittaohjelma-alustat tekevät siitä hyökkääjälle helppoa. Niitä myydään sekä palveluina että tuotteina. Aiemmin haittaohjelma-alustat olivat hyvin suosittuja kiristysohjelmahyökkäysten yhteydessä. Esimerkiksi Adobe Flash - kehitysympäristössä havaitut haavoittuvuudet ovat mahdollistaneet useiden kiristysohjelmien levittämisen. Näihin kuuluvat esimerkiksi CryptoWall, TeslaCrypt, Crilock ja Waltrix [17].

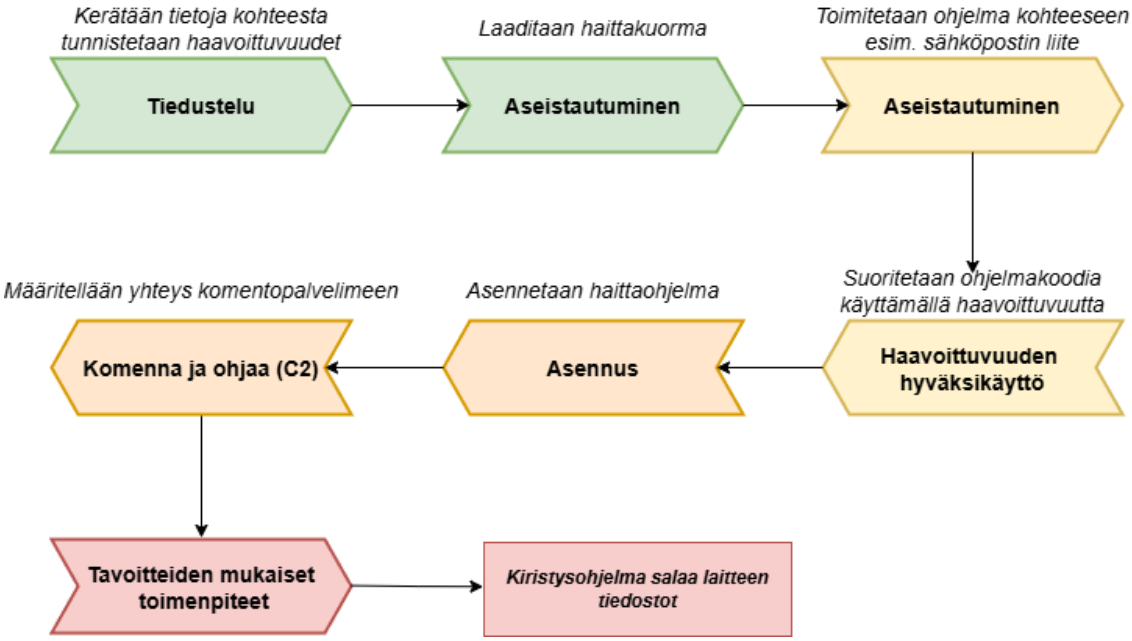
Sosiaalinen manipulointi viittaa taktiikoihin, joiden avulla hyökkääjä pyrkii hyödyntämään kohteen luottamusta saadakseen tämän suorittamaan toiminnon, joka vaarantaa laitteen. Tavoitteena on yleensä houkutella uhri asentamaan haittaohjelma itse. Luottamusta voidaan rakentaa esimerkiksi valheellisella ystävyyssuhteella, uskottavalta vaikuttavalta sähköpostilla tai harjaanjohtavalla puhelinsoitolla [17].

3.2 Hyökkäyksen vaiheet

Hyökkäyksen eri vaiheiden tutkiminen on keskeistä, sillä sen avulla voidaan ymmärtää kiristysohjelmien toimintatapoja ja kehittää tehokkaampia torjunta- ja ennaltaehkäisykeinoja. Haittaohjelmien tyypillisestä elinkaaresta on olemassa malleja, jotka pyrkivät havainnollistamaan hyökkäyksen vaiheet kohta kohdalta. Tunnetuimpia tällaisia malleja ovat Lockheed Martinin MITRE ATT & CK ja Cyber Kill Chain.

Lockheed Martin esitti vuonna 2011 mallin kyberhyökkäyksistä, joka pyrkii mal-

lintamaan hyökkäyksen eri vaiheet hyökkääjän näkökulmasta. Tämä malli on laajasti hyväksytty ja osoittautunut toimivaksi vastakeinojen parantamiseksi. Malli tunnetaan nimellä Cyber Kill Chain (CKC) ja se koostuu seitsemästä vaiheesta: tiedustelu, aseistautuminen, toimitus, haavoittuvaisuuden hyväksikäyttö, asennus, komenna ja ohjaa (C2) (engl. Command and Control) ja tavoitteiden mukaiset toimenpiteet. [17] Vaiheet ovat havainnollistettu kuvassa 3.1.



Kuva 3.1: Cyber kill chain:in eri vaiheet.

Tiedusteluvaiheessa hyökkääjä pyrkii keräämään mahdollisimman paljon tietoa kohteista, jotta mahdollisimman kattava hyökkäys saadaan aikaan. Hyökkääjä saattaa esimerkiksi kerätä tietoja kohteen sosiaalisen median profiileista tai muista verkkopalveluista. Hyökkääjä saattaa myös avata portteja mahdollisien haavoittuvaisuuksien ansiosta kohteen käyttämiin sovelluksiin tai verkkopalveluihin.

Aseistautumisvaiheessa hyökkääjä rakentaa haittakuorman (engl. payload) sekä valitsee taktiikat, joilla voidaan piiloutua järjestelmän turvallisuusominaisuuksilta ja avata tarvittavia takaovia. Yleisimmät menetelmät perustuvat muun muassa PDF-tiedostojen tai Microsoft Office -sovellusten haavoittuvuuksiin, joiden avulla voidaan

poistaa kriittisiä suojausominaisuuksia käytöstä ja suorittaa haitallista koodia etänä [18]. Vuonna 2022 Microsoft Office -tuotteiden haavoittuvuudet muodostivat noin 82 % kaikista havaituista haavoittuvuuksia hyödyntävistä hyökkäyksistä Kasperskyn neljännesvuosiraportin mukaan [19].

Toimitusvaiheessa haittakuorma siirretään kohdejärjestelmään hyödyntämällä jotakin aiemmin tunnistettua leviämistaktiikkaa. Haavoittuvaisuuden hyväksikäyttövaiheessa hyökkääjä käyttää valitsemiaan teknisiä keinoja kohdejärjestelmän vaarantamiseksi ja haittakuorman suorittamiseksi. Seuraavaksi asennusvaiheessa pyritään luomaan pysyvä pääsy järjestelmään esimerkiksi asentamalla etäkäyttöön tarkoitettu troijalainen (engl. remote access trojan) (RAT) tai avaamalla uusia takaovia myöhempiä toimenpiteitä varten.

Kun järjestelmään on saatu pysyvä yhteys, siirrytään C2-vaiheeseen. Tällöin haittaohjelma ottaa yhteyden hyökkääjän hallinnoimaan C2-palvelimeen, jonka kautta voidaan ohjata tartunnan saaneita järjestelmiä, päivittää haittaohjelman komponentteja ja hallita salausprosessia. Kaikki kiristysohjelmat eivät kuitenkaan edellytä C2-palvelinta tiedostojen salaamiseen. Lopuksi suoritetaan hyökkääjän tavoitteen mukaiset toimenpiteet. Kiristysohjelmien tapauksessa tämä tarkoittaa kohdistettujen tiedostotyyppien salakirjoittamista ja lunnasviestin esittämistä, jossa uhri ohjataan maksutoimenpiteisiin. [17]

4 Laajalle levinneitä kiristysohjelmia haittavaikutuksineen

Kiristysohjelmat, kuten WannaCry, NotPetya ja LockBit ovat levinneet laajasti eri puolilla maailmaa ja aiheuttaneet merkittäviä taloudellisia vahinkoja. Ne ovat häirinneet sekä yritysten että yksityishenkilöiden toimintaa ja vaikuttaneet myös kriittisen infrastruktuurin palveluihin. Erityisesti WannaCry- ja NotPetya-kiristysohjelmien tarkoituksena oli levitä mahdollisimman laajalle mahdollisimman nopeasti käyttäen vakavia haavoittuvuuksia. Vastatoimet alkavat kehittyä hyvin nopeasti hyökkäyksen havaitsemisen jälkeen ja tästä syystä itsestään leviäminen on kiristysohjelmille erittäin hyödyllinen mekanismi. On hyvä mainita, että osa näiden kiristysohjelmien käyttämistä hyökkäysmenetelmistä ja haavoittuvuuksista on nykyisin korjattu. Järjestelmät, jotka eivät ole saaneet tarvittavia turvallisuuspäivityksiä kuitenkin pysyvät haavoittuvina. Tästä syystä vanhatkin kiristysohjelmat voivat jatkaa tänä päivänä leviämistä tietyissä ympäristöissä.

4.1 WannaCry

WannaCry on yksi historian laajimmalle levinneistä kiristysohjelmista, ja se havaittiin ensimmäisen kerran helmikuussa vuonna 2017. Tämä ohjelma käytti AES-128-salausalgoritmia tiedostojen salaamiseen, eikä sillä alun perin ollut itsestään leviämiseen tarkoitettuja ominaisuuksia. Saman vuoden toukokuussa tästä ohjelmasta

havaittiin uusi variantti, joka sisälsi madon kaltaisia leviämisominaisuuksia ja hyödynsi haavoittuvuuksia, jotka olivat vuotaneet Yhdysvaltain turvallisuusviranomaisilta. [20], [21] Tämän ohjelman taustalla oli maailmanlaajuisesti levinnyt hyökkäys, joka samana vuonna kohdistui yli 150:een eri maahan ja tartutti yli 300 000 laitetta. Hyökkäyksellä oli haitallisia seurauksia monille yrityksille ja organisaatioille kuten hallituksille, terveydenhuollolle, telekommunikaatiolle ja öljy- ja kaasutuotannolle. [21] Erityisen vakavasti WannaCry vaikutti Yhdistyneen kuningaskunnan terveydenhuoltojärjestelmään (NHS), jossa järjestelmiin pääsyn estyminen keskeytti sairaaloiden toimintoja ja johti yli 19 000 potilasajanvarauksen peruuntumiseen. Hyökkäys kustansi NHS:lle arviolta noin 92 miljoonaa puntaa. [22]

WannaCry:n tunnetuin variantti on itsestään leviävä madon kaltainen ohjelma, joka koostuu kahdesta pääkomponentista. Niistä toinen tarjoaa kiristysohjelman toiminnallisuuden ja toinen, madon kaltainen komponentti, mahdollistaa haavoittuvuuden hyödyntämisen leviämiseen. WannaCry käytti hyökkäyksessä kahta vuonna 2017 löydettyä haavoittuvutta hyödyntävää menetelmää. Niistä toinen on nimeltä EternalBlue, joka perustui Windows-käyttöjärjestelmässä olevan Server Message Block (SMB) -protokollan haavoittuvuuteen. Tämä haavoittuvuus salli pääsyn verkossa kiinni olevalle tietokoneelle ja koodin suorittamisen etänä [23]. Toista menetelmää kutsutaan nimellä DoublePulsar, joka on pysyvä takaovi, jota voidaan käyttää pääsyyn ja koodin suorittamiseen aiemmin vaarannetussa laitteessa. Tämä antaa hyökkääjän asentaa laitteelle lisää haittaohjelmia [21]. Näitä kahta menetelmää käyttäen WannaCry pystyy ensin leviämään usealle laitteelle (EternalBlue), jonka jälkeen laitteeseen voidaan istuttaa haittaohjelmien asentamiseen mahdollistava takaovi (DoublePulsar).

Suorittaessaan madon kaltaista komponenttiaan WannaCry pyrkii ensin muodostamaan yhteyden verkkotunnukseen www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Tämä toimii eräänlaisena tappokytkimenä ohjelmalle ja jos yhteyttä osoit-

teeseen ei saada luotua, ohjelman madon kaltainen komponentti jatkaa toimintaansa. Ohjelma yrittää luoda prosessin nimeltä "Microsoft Security Center (2.0) Service"mssecvs 2.0 [20], jonka tarkoituksena on erehdyttää käyttäjä luulemaan prosessia Windowsin omaan tietoturvajärjestelmään kuuluvaksi. Tämä on tyypillinen keino haittaohjelmille naamioitua käyttäjältä.

Tämän jälkeen ohjelma yrittää purkaa kiristysohjelman sisältävän komponentin Windows-kansioon ja suorittaa sen. Lisäksi WannaCry luo Windowsin rekisteriin avaimen, joka mahdollistaa ohjelman käynnistyksen aina käyttöjärjestelmän käynnistyksen yhteydessä. Prosessin aikana ohjelma luo myös varmuuskopioita eri hakemistoihin, lisää itsensä Windowsin AutoRun-toiminnallisuuteen ja pyrkii lopettamaan SQL- ja MS Exchange-prosesseja varmistaakseen psysyvyyden laitteella. Pysyvyyden varmistettua ohjelma poistaa luomansa varmuuskopiot. [21]

Madon kaltainen komponentti purkaa ja suorittaa lopuksi kiristysohjelman sisältävän komponentin, jonka jälkeen salausprosessi alkaa. Tämä tapahtuu ensin luomalla jokaiselle kohdistetulle tiedostolle 16 tavun kokoinen AES-avain käyttämällä ohjelman tarjoamaa funktiota. Tämän jälkeen jokainen luotu AES-avain salataan julkisella RSA-avaimella. Salatut tiedostot nimetään uudelleen ja ne saavat tiedostopäätteen WANACRY!. [20] Tässä vaiheessa tiedostojen salausta ei voida purkaa ilman purkuavainta, jonka hyökkääjä tarjoaa ainoastaa Bitcoinilla maksettavaa rahasummaa vastaan.

4.2 NotPetya

Noin kuukausi WannaCry-ohjelman julkaisun jälkeen kesäkuussa 2017, uuden kiristysohjelman nimeltä NotPetya havaittiin leviävän nopeasti Ukrainassa. Ohjelma levisi alusta alkaen hyvin nopeasti yritysmaailmassa, sillä usean suuren ukrainalaisen yrityksen käyttämä M.E.Doc-kirjanpitojärjestelmä sisälsi takaoven, joka mahdollisti ohjelman leviämisen itsestään [9].

NotPetya perustuu aiempaan, vuoden 2016 maaliskuussa havaittuun Petya-nimiseen kiristysohjelmaan, joka levisi sähköposteihin kiinnitetyn tiedoston kautta. NotPetya-variantti toimii WannaCry:n tapaan ja käyttää hyväkseen EternalBlue-haavoittuvuutta, mutta lisäksi se hyödyntää EternalRomance- ja Mimikatz - nimisiä haavoittuvuuksia hyödyntäviä menetelmiä. Mimikatz perustuu Windowsissa olevaan haavoittuvuuteen, jonka avulla laitteen käyttäjien salasanat voidaan poimia muistista. EternalRomance on myös SMB-protokollan haavoittuvuutta hyödyntävä menetelmä, jonka avulla voidaan upottaa haitallista koodia järjestelmään. Nämä kolme haavoittuvuutta saivat NotPetyan leviämään ennennäkemättömän nopeasti [24].

Edeltäjäänsä verrattuna NotPetyan toiminnassa on yksi hyvin merkittävä ero. Kun alkuperäinen Petya toimii kiristysohjelmien tyypilliseen tapaan tarjoten tietojen salauksen jälkeen salauksen purkamismahdollisuuden rahasummaa vastaan, NotPetyalla huomattiin nopeasti puuttuvan tämä mahdollisuus. Vaikka ohjelma pyytää salauksen jälkeen kryptovaluuttamaksua, ei purkuavainta todellisuudessa edes ole olemassa [24].

NotPetya käyttää hybridisalausta, joka hyödyntää AES-128 ja RSA - algoritmeja salatakseen kovalevyn pääkäynnistystietueen (engl. Master Boot Record). Kun salaus on suoritettu, käyttöjärjestelmän käynnistäminen estetään ja näytölle ilmestyy viesti, jossa ohjeistetaan lunnaan maksamiseen. Tässä vaiheessa kaikki kovalevyllä olevat tiedostot ovat käyttökelvottomia käytännössä pysyvästi, sillä salauksen purkaminen ilman avainta on mahdotonta.

NotPetya aiheutti maailmanlaajuisesti merkittäviä vahinkoja jo ensimmäisen tartuntapäivän aikana. Tunnettuja kohteita olivat muun muassa yritykset Maersk, Merck ja TNT Express. Vaikka tarkkojen taloudellisten vahinkojen arviointi on vaikeaa, Valkoisen talon arvioiden mukaan NotPetya aiheutti vuonna 2018 yli 10 miljardin dollarin vahingot maailmanlaajuisesti. [25]

4.3 LockBit

Syyskuussa vuonna 2019 havaittiin uusi kiristysohjelma nimeltä ABCD. Tästä ohjelmasta havaittiin uusi variantti nimeltään LockBit venäjänkielisillä kyberrikollisuusfoorumeilla vuoden 2020 tammikuussa. LockBit on esimerkki RaaS-hyökkäyksestä, jonka takana on samanniminen kyberrikollisryhmä. LockBit on aiheuttanut vahinkoa useille erikokoisille organisaatioille ja vuonna 2022 LockBit oli aktiivisin maailmanlaajuinen kiristysohjelmaryhmä ja RaaS-palveluntarjoaja uhrien lukumäärällä mitattuna. [15] LockBit toimii RaaS (Ransomware as a Service) - mallin mukaisesti, eli rikollisryhmä myy kiristysohjelman niille, jotka haluavat tehdä hyökkäyksen, ottaen osan lunnasrahoista maksuna.

LockBit-hyökkäykset kohdistuvat usein teollisuusyrityksiin ja sen seurauksena haittavaikutukset ovat joissain tapauksissa hyvinkin suuret [26]. Hyökkäykset suoritetaan usein yhteen kohteeseen kerrallaan, eli päätavoitteena ei aina ole saastuttaa laitteita laajalti ympäri maailmaa, vaan saada tietyn yrityksen tai organisaation tiedostot salattua. Tämän takia LockBit-hyökkäyksille on myös tyypillistä kiristää uhria tietojen salaamisen lisäksi sillä, että tiedot julkistetaan, jollei lunnaita makseta. Tämä kannustaa usein uhria maksamaan lunnaat, mutta joissain tapauksissa uhrien tietoja on julkistettu esimerkiksi TOR-sivustoilla.

LockBit on kehittynyt vuosien varrella paljon ja ohjelman variantti LockBit 3.0 (tunnetaan myös nimellä LockBit Black) on näistä tunnetuin. LockBit 3.0 on suunniteltu toimimaan mahdollisimman nopeasti ja se on vaikeampi havaita kuin edeltäjänsä. Riippuen suoritusympäristöstä, LockBit voidaan konfiguroida toimimaan eri tavoin ohjelmaa rakentaessa ja ohjelman toimintaa voidaan mukauttaa antamalla sille käynnistyksen yhteydessä eri argumentteja komentoriviltä [27]. Argumenteilla voidaan esimerkiksi määrittää, kuinka ohjelma leviää ja mitä tiedostoja salataan. Suorittaessa ohjelmaa on myös pakollista antaa salasana, jonka ohjelman myyjä tarjoaa. Tämä estää ohjelman suorittamisen yksilöiltä, jotka eivät ole siihen lupaa saaneet.

Lisäksi salasana toimii suojana virustorjuntaohjelmilta, sillä suoritettava ohjelma pysyy salattuna ennen oikean salasanan syöttämistä. Ennen tiedostojen salaamista LockBit 3.0 käyttää useita julkisesti saatavilla olevia työkaluja, sekä aiempienkin varianttien käyttämää Stealbit-työkalua tiedostojen siirtämiseen eri pilvipalveluihin, jotta uhria voidaan kiristää arkaluontoisten tietojen levittämisellä julkisuuteen [27].

LockBit 3.0 kykenee ohittamaan käyttäjätilien valvonnan (engl. User Account Control), jonka tarkoituksena on varmistaa, että ohjelmat eivät voi toimia korkeammilla oikeuksilla ilman käyttäjän suostumusta. Tämän seurauksena LockBit pystyy suorittamaan koodia korkeammilla oikeuksilla kuin mitä sillä pitäisi olla, mikä mahdollistaa ohjelman leviämisen uhrin verkossa oleviin muihin laitteisiin. Lisäksi suorituksen edetessä LockBit lisää useita avaimia Windowsin rekisteriin, tekee muutoksia ryhmäkäytäntöihin ja lopettaa lukuisia palveluja ja prosesseja. [27]

LockBitin joustavuus tekee siitä hyvin tuhoisan, sillä se mahdollistaa tietylle kohteelle juuri oikeanlaisen hyökkäyksen muodostamisen. Pelkästään Yhdysvalloissa kiristysohjelmahyökkäyksistä noin 1 700 on tunnistettu LockBit-hyökkäyksiksi vuodesta 2020 vuoteen 2023 ja tänä aikana lunnaita on maksettu noin 91 miljoonaa dollaria. Hyökkäykset ovat kohdistuneet muun muassa kuntien ja maakuntien hallintoihin, kouluihin sekä hätäpalveluihin. Ranskassa samalta aikaväliltä hyökkäyksiä on tunnistettu 69 ja Australiassa, Kanadassa ja Uudessa Seelannissa tapauksia on myös tunnistettu kymmeniä. [15]

5 Yhteenveto

Nykyisin kiristysohjelmat muodostavat merkittävän uhan yksityishenkilöille, yrityksille ja julkisille organisaatioille maailmanlaajuisesti. Kiristysohjelmien taloudellinen kannattavuus mahdollistaa jatkuvan kehityksen, jonka takia niistä on vaikea päästä kokonaan eroon. Ransomware-as-a-service -malli on tehnyt kiristysohjelmahyökkäysten tekemisestä helppoa. Se mahdollistaa suuren hyökkäyksen tekemisen kenelle tahansa. Kryptovaluutat ovat mahdollistaneet kiristysohjelmien vaatimien lunnasmaksujen saamisen rikollisille tavalla, jota ei voi jäljittää.

Tämän kirjallisuuskatsauksen tavoitteena oli vastata kahteen tutkimuskysymykseen. Ensimmäinen tutkimuskysymys oli "Kuinka kiristysohjelmat toimivat?" Kiristysohjelmat voivat tartuttaa kohdejärjestelmän hyödyntämällä haavoittuvuuksia, sosiaalista manipulointia tai muita leviämistapoja, kuten sähköpostiliitteitä. Kiristysohjelmat voivat käyttää useita eri salausmenetelmiä tiedostojen salaamiseen, ja osa ohjelmista levittää itseään automaattisesti verkossa. Useimmat kiristysohjelmat pyrkivät pysymään huomaamattomina siihen asti, että salaus on suoritettu.

Toinen tutkimuskysymys oli "Mitkä ovat kiristysohjelmien haittavaikutukset?" Laajalle levinneet kiristysohjelmahyökkäykset ovat todistaneet, että niillä voidaan aikaansaada suurta taloudellista tuhoa maailmanlaajuisesti ja niitä voidaan käyttää joko taloudellisen hyödyn takia, tai jopa aseena kokonaista maata tai hallitusta vastaan. Tutkimalla aiempien hyökkäysten toimintatapoja voidaan kehittää vastakeinoja tulevaisuutta varten ja ennaltaehkäistä uusia hyökkäyksiä.

Tietoturvan perussääntöjen noudattaminen, kuten laitteiden ajan tasalla pitäminen ja epäilyttävien tiedostojen suorittamatta jättäminen, laskee uhriksi joutumisen riskiä huomattavasti. Toisaalta uusia haavoittuvuuksia löydetään käyttöjärjestelmistä ja laajasti käytetyistä ohjelmista usein, ja tämä saattaa mahdollistaa haittaohjelman leviämisen ilman käyttäjän virhettä. Yksilötasolla uhriksi joutuminen voi tarkoittaa kaikkien henkilökohtaisten tiedostojen menettämistä, mikäli varmuuskopioita ei ole tehty. Suuremmilla yrityksillä ja organisaatioilla uhriksi joutuminen voi olla hyvinkin tuhoisaa, jos toiminnan kannalta tärkeitä tai salaisia tiedostoja on salattu tai uhattu julkistaa. Tästä huolimatta useat viranomaiset ja organisaatiot eivät kannata lunnaiden maksamista, sillä ensinnäkin maksaminen ei takaa tiedostojen salauksen purkamista, ja toiseksi se kannustaa ja edistää kiristysohjelmien kehitystä jatkossa. [15]

Lähdeluettelo

[1] M. Cen, X. Deng, F. Jiang ja R. Doss, ”Zero-Ran Sniff: A zero-day ransomware early detection method based on zero-shot learning”, *Computers & Security*, vol. 142, id: 103849, 2024. DOI: https://doi.org/10.1016/j.cose.2024.103849.

[2] A. Dib, G. Sabri ja M. S. M. Mendjel, ”Ransomware Attack Detection based on Pertinent System Calls Using Machine Learning Techniques”, *International Journal of Computer Networks and Communications*, vol. 15, s. 124–145, heinäkuu 2023. DOI: 10.5121/ijcnc.2023.15408.

[3] VirusTotal, ”Ransomware in a global context”, https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf (Vierailtu 2025-04-20).

[4] H. Oz, A. Aris, A. Levi ja A. S. Uluagac, ”A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions”, *ACM Computing Surveys (CSUR)*, vol. 54, s. 1–37, syyskuu 2022. DOI: 10.1145/3514229.

[5] A. Patel ja J. Tailor, ”A malicious activity monitoring mechanism to detect and prevent ransomware”, *Computer Fraud & Security*, vol. 2020, nro 1, s. 14–19, 2020. DOI: https://doi.org/10.1016/S1361-3723(20)30009-9.

[6] K. Begovic, A. Al-Ali ja Q. Malluhi, ”Cryptographic ransomware encryption detection: Survey”, *Computers & Security*, vol. 132, id: 103349, 2023. DOI: https://doi.org/10.1016/j.cose.2023.103349.

[7] T. McIntosh, A. S. M. Kayes, Y.-P. P. Chen, A. Ng ja P. Watters, "Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions", *ACM Computing Surveys (CSUR)*, vol. 54, nro 9, s. 1–36, lokakuu 2021. DOI: 10.1145/3479393.

[8] P. Bajpai, A. K. Sood ja R. Enbody, "A key-management-based taxonomy for ransomware", teoksessa *2018 APWG Symposium on Electronic Crime Research (eCrime)*, San Diego, CA, USA, 2018, s. 1–12. DOI: 10.1109/ECRIME.2018.8376213.

[9] M. A. Mos ja M. M. Chowdhury, "The Growing Influence of Ransomware", teoksessa *2020 IEEE International Conference on Electro Information Technology (EIT)*, Chicago, IL, USA, 2020, s. 643–647. DOI: 10.1109/EIT48999.2020.9208254.

[10] C. Obimbo, A. Speller, K. Myers, A. Burke ja M. Blatz, "Internet Worms and the Weakest Link: Human Error", teoksessa *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2018, s. 120–123. DOI: 10.1109/CSCI46756.2018.00030.

[11] A. Dalvi, P. Kulkarni, A. Kore ja S. G. Bhirud, "Dark Web Crawling for Cybersecurity: Insights into Vulnerabilities and Ransomware Discussions", teoksessa *2023 2nd International Conference for Innovation in Technology (INOCON)*, Bangalore, India, 2023, s. 1–6. DOI: 10.1109/INOCON57975.2023.10101162.

[12] N. Khadam, N. Anjum, A. Alam, Q. Ali Mirza, M. Assam, E. A. Ismail ja M. R. Abonazel, "How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan", *Heliyon*, vol. 9, nro 12, id: e22823, 2023. DOI: https://doi.org/10.1016/j.heliyon.2023.e22823.

[13] E. Berrueta, D. Morato, E. Magaña ja M. Izal, "Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic", *Expert Systems with Applications*, vol. 209, id: 118299, 2022. DOI: https://doi.org/10.1016/j.eswa.2022.118299.

[14] U. Urooj, M. A. B. Maarof ja B. A. S. Al-rimy, "A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model", teoksessa *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi, Malesia, 2021, s. 1–6. DOI: 10.1109/CRC50527.2021.9392548.

[15] CISA, "Understanding Ransomware Threat Actors: LockBit", https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (Vierailtu 2025-04-20).

[16] S. Kok, A. Abdullah ja N. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm", *Journal of King Saud University - Computer and Information Sciences*, vol. 34, nro 5, s. 1984–1999, 2022. DOI: https://doi.org/10.1016/j.jksuci.2020.06.012.

[17] T. Dargahi, A. Dehghantanha, P. Nikkhah Bahrami, M. Conti, G. Bianchi ja L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features", *Journal of Computer Virology and Hacking Techniques*, vol. 15, s. 277–305, 2019. DOI: 10.1007/s11416-019-00338-7.

[18] R. Dubin, "Content Disarm and Reconstruction of Microsoft Office OLE files", *Computers & Security*, vol. 137, id: 103647, 2024. DOI: https://doi.org/10.1016/j.cose.2023.103647.

[19] Kaspersky, *Eight times more users attacked via an old Microsoft Office vulnerability in Q2*, https://www.kaspersky.com/about/press-releases/eight-times-more-users-attacked-via-an-old-microsoft-office-vulnerability-in-q2 (Vierailtu 2025-04-20), 2022.

[20] M. Akbanov, V. G. Vassilakis ja M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry", *Computers & Electrical Engineering*, vol. 76, s. 111–121, 2019. DOI: https://doi.org/10.1016/j.compeleceng.2019.03.012.

[21] M. Akbanov, V. G. Vassilakis ja M. D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms", *Journal of Telecommunications and Information Technology*, vol. 75, s. 113–124, maaliskuu 2019. DOI: 10.26636/jtit.2019.130218.

[22] Cyber Security Policy, "Securing cyber resilience in health and care: Progress update October 2018", Department of Health & Social Care, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf (Vierailtu 2025-04-20).

[23] M. Satheesh Kumar, J. Ben-Othman ja K. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection", teoksessa *2018 IEEE Symposium on Computers and Communications (ISCC)*, Natal, Brasilia, 2018, s. 1–6. DOI: 10.1109/ISCC.2018.8538354.

[24] R. A. Lika, D. Murugiah, S. N. Brohi ja D. Ramasamy, "NotPetya: Cyber Attack Prevention through Awareness via Gamification", teoksessa *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Shah Alam, Malesia, 2018, s. 1–6. DOI: 10.1109/ICSCEE.2018.8538431.

[25] CISA, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Vierailtu 2025-04-20).

[26] N. Suk-On, N. Thiratitsakun ja K. Chimmanee, "Digital Forensic Analysis of Lockbit Ransomware Attack on Operational Technology", teoksessa *2024*

8th International Conference on Information Technology (InCIT), Chonburi, Thaimaa, 2024, s. 624–629. DOI: 10.1109/InCIT63192.2024.10810564.

[27] CISA, "#StopRansomware: LockBit 3.0", https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a (Vierailtu 2025-04-20).