Lauri Pellikka

KIRISTYSHAITTAOHJELMIIN LIITTYVÄT UHAT SEKÄ NIIHIN VARAUTUMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Pellikka, Lauri
Kiristyshaittaohjelmiin liittyvät uhat sekä niihin varautuminen
Jyväskylä: Jyväskylän yliopisto, 2024, 26 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Mehtälä, Saana

Pitkään jatkunut yhteiskuntien digitalisaatio on tehnyt organisaatioista sekä yksityishenkilöistä yhä riippuvaisempia eri teknologioiden sekä tietojärjestelmien mahdollistamista hyödyistä. Kehityksen kääntöpuolena rikollisuus sekä muut haitalliset ja vaaralliset ilmiöt digitaalisissa ympäristöissä ovat myös lisääntyneet. Tämän kandidaatintutkielman tarkoituksena oli selvittää etenkin 2010-luvulla valtavasti yleistyneiden kiristyshaittaohjelmien aiheuttamia uhkia niin organisaatioille kuin yksityishenkilöille sekä sitä, kuinka näihin uhkiin voitaisiin varautua. Tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena, jossa analysoitiin laajasti kiristyshaittaohjelmia, niiden kehitystä, havaitsemista ja torjumista käsitteleviä vertaisarvioituja tieteellisiä artikkeleita sekä muuta aiheen kannalta relevanttia kirjallisuutta. Tutkielman tuloksena havaittiin, että kiristyshaittaohjelmat aiheuttavat pahimmillaan erittäin mittavia vahinkoja niin liiketoiminnalle kuin yksityishenkilöllekin. Haittaohjelmien tekijät usein hyödyntävät tekniikkaa, joiden havaitsemiseen ja torjumiseen ei ole olemassa yhtä kehittyneitä ratkaisuja. Lisäksi inhimillisten virheiden havaittiin olevan yksi merkittävimmistä uhkatekijöistä. Uhkiin varautumiseen liittyviä tekijöitä tutkittaessa havaittiin tehokkaimmiksi yleisesti tieto- ja kyberturvallisuutta edistävät toimet, joskin tietoturvaorganisaatioilla on myös täysin omia tekniikoita kiristyshaittaohjelmien havaitsemiseen sekä torjumiseen. Torjuntatekniikoiden kehittämisen sekä ihmisten tietoisuuden lisäämisen tueksi aiheen lisätutkimukselle on tarvetta tulevaisuudessa.

Asiasanat: kiristyshaittaohjelma, uhka, ennaltaehkäisy, tartunta, havaitseminen

ABSTRACT

Pellikka, Lauri
The threats of ransomware and how to be prepared for them
Jyväskylä: University of Jyväskylä, 2024, 26 pp.
Information systems, Bachelor's Thesis
Supervisor: Mehtälä, Saana

The long-standing digitization of societies has made organizations and individuals increasingly dependent on the benefits enabled by various technologies and information systems. However, the flip side of this development is the rise of criminal activities and other harmful phenomena in digital environments. This bachelor's thesis aimed to explore the threats posed by ransomware, a type of malicious software that became widespread, particularly in the 2010s, to both organizations and individuals, and how these threats could be prevented. The thesis was conducted as a descriptive literature review, analyzing peer-reviewed scientific studies and articles that addressed ransomware, its development, detection, and prevention. The findings revealed that ransomware can cause extensive damage to both businesses and individuals. Criminals often exploit techniques for which there are no equally advanced solutions. Additionally, human errors were identified as one of the most significant threat factors. Beyond mitigation techniques and human awareness, there is a need for further research in this field. Among the factors related to preparedness, measures promoting general information and cybersecurity were found to be the most effective, although security organizations also employ unique techniques for detecting and mitigating ransomware.

Keywords: ransomware, thread, prevention, infection, detection

TAULUKOT

SISÄLLYS

1 JOHDANTO

Pitkään jatkunut yhteiskuntien digitalisaatio on tehnyt organisaatioista sekä yksityishenkilöistä yhä riippuvaisempia eri teknologioiden sekä tietojärjestelmien mahdollistamista hyödyistä. Tämän kehityksen kääntöpuolena voidaan pitää rikollisuuden, terrorismin ja jopa sodankäynnin siirtymistä yhä enenevissä määrin digitaalisiin ympäristöihin. Kyberrikollisuus voikin aiheuttaa merkittävää rahallista, henkistä tai sosiaalista haittaa niin yksityishenkilöille, organisaatioille kuin yhteiskunnillekin. Niin kyberrikollisuuden kuin siihen liittyvän tieteellisen tutkimuksen ollessa aihealueina tuoreita, ovat usein rikollisten hyökkäyskeinot edistyneempiä, kuin olemassa olevat puolustusmekanismit (O'Kane ym., 2018). Koko ala elää myös jatkuvassa muutoksessa, minkä takia aiheen tutkimus koetaan tärkeänä, jotta kyberrikollisuudelta puolustautuminen voisi kehittyä hyökkääjien tasolle.

Tuottavuutensa vuoksi erääksi yleisimmistä kyberrikollisuuden muodoista ovat nousseet kiristyshaittaohjelmat (Kara ym., 2022). Kiristyshaittaohjelmista aiheutuneet kustannukset ovat nousseet viime aikoina valtavasti. Esimerkiksi vuonna 2018 arvioitiin kiristyshaittaohjelmiin suoraan tai välillisesti liittyvien kulujen nousseen 8 miljardiin Yhdysvaltain dollariin siitä huolimatta, että 94 % hyökkäyksen kohteeksi joutuneista yrityksistä ei maksanut vaadittuja lunnaita hyökkääjälle (Or-Meir ym., 2019). Vuonna 2020 kumuloituneiden tappioiden arvioidaan ylittäneen 74 miljardin dollarin rajan (August ym., 2022).

Tämä kandidaatintutkielma käsittelee kiristyshaittaohjelmiin liittyviä uhkia sekä miten niihin voidaan pyrkiä varautumaan niin yksilön kuin olemassa olevien puolustusmekanismien taholta. Tavoitteena on tuoda esiin kiristyshaittaohjelmien historiaa, toimintamalliin liittyviä ominaisuuksia suhteessa muihin haittaohjelmiin, niiden vaikutuksia sekä hyökkäyksen seurauksia yksilöille ja organisaatioille. Tarkoituksena on myös pohtia keinoja ja mekanismeja, joilla kiristyshaittaohjelmahyökkäyksiin voitaisiin ennaltaehkäisevästi vaikuttaa ja varautua. Näiden tavoitteiden tueksi asetettiin tälle tutkimukselle seuraavat tutkimuskysymykset:

- *"Mitä uhkia kiristyshaittaohjelmiin liittyy?"*

- *"Miten kiristyshaittaohjelmiin liittyviin uhkiin voidaan varautua?"*

Tutkimus toteutettiin kuvailevana kirjallisuuskatsauksena, jonka lähdemateriaalit ovat vertaisarvioituja tieteellisiä artikkeleita, konferenssiesityksiä sekä aiheen kannalta hyödyllisiä verkkosivustoja. Lähteiden etsintään hyödynnettiin tietokantoja, joita ovat Jyväskylän yliopiston tietokanta JYKDOK, Scopus, IEEE Xplore sekä Google Scholar -hakukone. Tietokannat ovat tutkimuksen kannalta relevantteja, sillä niistä löytyy runsaasti aiheeseen liittyviä tutkimuksia. Hakutermeinä käytettiin esimerkiksi *ransomware, thread, prevention, infection* ja *detection* sekä niiden yhdistelmiä. Lähdekirjallisuutta valittaessa huomioidaan kyseisen lähteen viittausten lukumäärä, julkaisun/julkaisijan vaikutusvalta alalla sekä aiheen sopivuus suhteessa tutkittavaan aiheeseen sekä tutkimuskysymyksiin. Tietokannoista noudettujen lähteiden julkaisijat täyttävät myös vähintään Julkaisufoorumin tason 1. Nämä tekijät ja rajaukset huomioon ottaen aiheeseen sopivia hakutuloksia tuli noin 100 artikkelia. Kaikki nämä aineistot käytiin läpi, jonka tuloksena tutkielman kannalta epärelevanteiksi katsotut lähteet rajattiin pois. Epärelevanteiksi katsottiin sellaiset lähteet, joiden tutkimusaiheena oli jokin muu kuin kiristyshaittaohjelmiin liittyvät uhat tai niiden vastatoimet. Näihin sisältyi esimerkiksi merkittävä määrä tutkimuksia IoT- ja Android-ympäristöjen suhteesta kiristyshaittaohjelmiin. Lisäksi epärelevanteiksi katsottiin lähteet, jotka sisällöltään olivat suurelta osin vastaavia jo lähteeksi valikoituneiden artikkeleiden kanssa. Karsinnan jälkeen lähdeaineistoksi valikoitui 38 lähdettä.

Tutkielman tuloksena havaittiin, että kiristyshaittaohjelmat aiheuttavat pahimmillaan erittäin mittavia vahinkoja niin liiketoiminnalle kuin yksityishenkilöllekin (Zimba & Chishimba, 2019; Kshetri & Voas, 2022; Corbet & Goodell, 2022). Matthijssen ym. (2023) sekä O'Kane ym. (2018) mukaan haittaohjelmien tekijät usein hyödyntävät tekniikkaa, joiden torjumiseen ei ole olemassa yhtä kehittyneitä ratkaisuja, mikä tekee niihin varautumisen ja niitä vastaan puolustautumisen hankalaksi. Lisäksi inhimillisten virheiden havaittiin olevan yksi merkittävimmistä uhkatekijöistä (Matthijsse ym., 2023; O'Kane ym., 2018). Torjuntatekniikoiden kehittymisen sekä ihmisten tietoisuuden lisäämisen mahdollistamiseksi aiheen tutkimukselle on tarvetta. Tutkielmaa tehdessä havaittiin, että torjuntatekniikoihin liittyviä teknisiä tutkimuksia oli huomattavasti enemmän, aihealueen inhimillisen osuuden tutkimusaineistossa jäädessä kovin pieneksi. Uhkiin varautumiseen liittyviä tekijöitä tutkittaessa havaittiin tehokkaimmiksi yleisesti tieto- ja kyberturvallisuutta edistävät toimet, joskin tietoturvaorganisaatioilla sekä aiheen tutkijoilla on myös täysin omia tekniikoita kiristyshaittaohjelmien havaitsemiseen sekä torjumiseen.

Tutkielma koostuu neljästä erillisestä, toisiaan tukevasta osasta. Johdannon jälkeen toisessa luvussa käsitellään kiristyshaittaohjelman määritelmää sekä tehdään katsaus niiden historiaan. Luvussa tarkastellaan lisäksi myös

kiristyshaittaohjelmien toimintamalleja ja niiden vaikutuksia uhreihinsa niin organisaatioiden kuin yksityishenkilöidenkin kannalta. Kolmannessa luvussa käsitellään puolestaan organisaatioiden ja yksityishenkilöiden varautumismahdollisuuksia kiristyshaittaohjelman tartunnan välttämiseksi sekä tuodaan ilmi toimintatapoja tartunnan saamisen jälkeen. Lisäksi luodaan katsaus olemassa oleviin puolustusmekanismeihin, joita tietoturvaorganisaatiot hyödyntävät kiristyshaittaohjelmia havaitsevissa ja torjuvissa ratkaisuissaan. Viimeisenä yhteenvetoluvussa pyritään havaittujen löydösten perusteella luomaan synteesi sekä keskustelemaan siitä suhteessa tutkimuskysymyksiin. Yhteenvedossa esitellään myös tutkielmaan ja sen aiheeseen liittyviä rajoitteita sekä mahdollisia jatkotutkimusaiheita.

2 KIRISTYSHAITTAOHJELMAT

Tässä luvussa pyritään aiempaan tietoon ja tutkimukseen pohjautuen määrittelemään kiristyshaittaohjelman käsite sekä sen olennaisimmat erot muihin haittaohjelmiin nähden. Lisäksi luvussa tarkastellaan kiristyshaittaohjelman toimintamallia hyökkäyksen eri vaiheissa ja pyritään tuomaan ilmi niiden vaikutuksia yksityishenkilöille sekä organisaatioille.

2.1 Kiristyshaittaohjelman määritelmä

Kiristyshaittaohjelma (ransomware) on rikollis- tai häirintätarkoituksiin käytetty haittaohjelman muoto. Asennettaessa tietokoneelle se estää käyttäjän pääsyn joihinkin tiedostoihin tai mahdollisesti koko järjestelmään, kunnes vaaditut lunnaat on maksettu hyökkääjälle. Hyökkääjä ei lähtökohtaisesti hyödy varastetun tiedon jälleenmyynnistä, vaan uhrin maksamista lunnaista (Paquet-Clouston ym., 2019). Kiristyshaittaohjelma salaa uhrin tiedostoja, kuten esimerkiksi valokuvia tai muita dokumentteja. Jos uhrin tiedostoja ei ole varmuuskopioitu, jää hänelle vaihtoehdoiksi joko lunnaiden maksaminen tai tiedostoista totaalisesti luopuminen. Tästä syystä hyökkääjät ottavatkin kohteeksi useammin joko pieniä yrityksiä tai yksityishenkilöitä, sillä heidän tiedostonsa ovat harvemmin varmuuskopioitu kuin suurempien organisaatioiden (Or-Meir ym., 2019).

Useimmissa lähteissä kiristyshaittaohjelmat jaetaan kahteen alalajiin. Kara & Aydos (2022) sekä Zhang-Kennedy ym. (2018) esittävät jaon krypto-kiristyshaittaohjelmiin ja lukitsija-kiristyshaittaohjelmiin. Karan ja Aydosin (2022) mukaan krypto-kiristyshaittaohjelma salaa uhrin koneella olevat tiedostot. Tämän jälkeen uhrin näytölle ilmestyy ilmoitus, jossa kerrotaan tiedostojen salauksen purkautuvan ainoastaan salausavaimella. Vaaditun salausavaimen saamiseksi täytyy uhrin maksaa hyökkääjän vaatimat lunnaat (Kara & Aydos, 2022). Zhang-Kennedyn ym. (2018) mukaan lukitsija-kiristyshaittaohjelma puolestaan evää uhrin pääsyn koko järjestelmään. Tässäkin tapauksessa näytölle ilmestyy hyökkääjän vaatimukset lunnaista, jotka maksamalla järjestelmään on mahdollista

päästä käsiksi (Zhang-Kennedy ym., 2018). Tätä vaatimusviestiä voidaan pitää kiristyshaittaohjelmien merkittävimpänä erona muihin haittaohjelmiin nähden. Siinä missä muut haittaohjelmat pyrkivät salaamaan olemassaolonsa tietokoneelta sekä sen käyttäjältä, pyrkii kiristyshaittaohjelma tämän lunnasvaatimusviestin muodossa tekemään olemassaolonsa mahdollisimman nopeasti selväksi uhrille (Hull ym., 2019). Näiden kahden alalajin lisäksi Beaman ym., (2021) mainitsee kolmanneksi variaatioksi pelotteluohjelmaa, joka voi kiristyshaittaohjelmien tapaan lähettää uhrille popup-ikkunoita, jossa uskotellaan tälle tietokoneensa olevan vaarassa, ellei hän lataa tiettyä tiedostoa. Vaikkakin tällainen ohjelma on uhrille näkyvyyden sekä ilmoitusviestien suhteen luonteeltaan kiristyshaittaohjelmaa vastaava, ei se kuitenkaan vaadi lunnaita maksettavaksi. Tällaisen ohjelman tarkoituksena onkin ainoastaan pelotella uhriaan, joten sen voidaan nähdä olevan enemmänkin tavanomaisen haittaohjelman muoto. Tätä tukee esimerkiksi Or-Meir ym. (2019) artikkelissaan jakamalla kiristyshaittaohjelmat ja pelotteluohjelmat omiksi tyyppikategorioikseen haittaohjelmien kontekstissa.

Vaikkakin kiristyshaittaohjelmien ensimmäiset hyökkäykset ajoittuvat 1980-luvulle, ovat ne yleistyneet räjähdysmäisesti 2010-luvun aikana. Pelkästään Yhdysvalloissa kiristyshaittaohjelmahyökkäyksien määrä kolminkertaistui vuosien 2019 ja 2021 välillä (Leo ym., 2022). Yilmazin ym. (2021) tutkimuksen mukaan merkittävimpänä tekijänä suosion kasvun taustalla voidaan nähdä olevan 2010-luvulla kehittyneiden, hyökkääjän anonyymiyden mahdollistavien maksutapojen yleistyminen. Näin ollen hyökkääjät pystyivät siirtymään fyysisestä rahan liikuttelusta hienostuneempiin rahastusmenetelmiin. Keinoja ovat esimerkiksi tekstiviestit korkeahintaisiin numeroihin, koodilla lunastettavat lahjakortit, maksupalvelut (esim. YandexMoney, Qiwi), prepaid-palvelut (esim. Ukash, Paysafecard) sekä kryptovaluutat. Suosituimpana maksutapana pidetäänkin kryptovaluuttoja (esim. Bitcoin, Ethereum, Monero, Zcash), sillä niiden ansiosta kiristyshaittaohjelmien tekijöiden jäljittämisestä on tullut huomattavasti haastavampaa (Yilmaz, ym., 2021).

Eräs eniten mielipiteitä jakavia ilmiöitä kiristyshaittaohjelmiin liittyen on, tulisiko uhrin maksaa hyökkääjän vaatimat lunnaat vai ei. Leon ym. (2022) mukaan maksamalla lunnaat uhri hyväksyy asemansa, ja on valmis tukemaan rikollista toimintaa. Esimerkiksi Yhdysvalloissa tällainen toiminta voidaan nähdä rikollisena, jolloin uhrikin saattaa joutua teostaan rikosoikeudelliseen vastuuseen (Leo, ym., 2022). Lunnaat maksamallakaan ei voida saada täyttä varmuutta tiedostojen palauttamisesta. Cartwrightin ym. (2023) mukaan hyökkääjä voi vaatia uutta maksua, palauttaa tiedostot edelleen osittain tai kokonaan salattuina tai saastuneina, tai jättää uhrin täysin omilleen ja kadota. Lunnaiden maksamatta jättäminen taas voi johtaa vaikeaan taisteluun salatuista tiedostoista, jotka pahimmassa tapauksessa voidaan menettää kokonaan (Cartwright, ym., 2023). Zimban ym. (2019) mukaan esimerkiksi FBI on yleisesti ohjeistanut olemaan maksamatta hyökkääjien vaatimia lunnaita. Everettin (2016) mukaan kiristyshaittaohjelman kohteeksi joutuneista yksityishenkilöistä arviolta noin 25–50 % maksoi hyökkääjän vaatimat lunnaat, kun taas yrityksistä näin teki alle 10 %. Selkeän eron taustalla voidaan nähdä olevan kaksi syytä. Ensinnäkin yrityksiltä

vaadittavien lunnaiden summa on lähtökohtaisesti huomattavasti yksityishenkilöltä vaadittavaa summaa suurempi. Suurempi lunnasvaatimus motivoi yrityksiä löytämään vaihtoehtoisen keinon selviytyä tilanteesta. Yksityishenkilöiltä vaadittavat summat ovat usein maltillisia, jolloin uhrista voi tuntua houkuttelevalta vaihtoehdolta vain maksaa itsensä ulos tilanteesta. Toisena syynä voidaan pitää yrityksien parempaa yleistä valmiustasoa tällaisten tilanteiden varalle (Everett, 2016). Etenkin suuremmissa yrityksissä tietoturva ja tärkeiden tiedostojen varmuuskopiointi on usein hoidettu asiallisesti (Or-Meir ym., 2019). Yrityksillä voi olla myös omia IT-henkilöitä tai pääomaa ulkoistamaan asian selvittelyn tarkemmin. Yksityishenkilöillä ei välttämättä ole mahdollisuutta ryhtyä asiaa selvittämään sen tarkemmin, jolloin vaihtoehdoiksi jäävät lunnaiden maksaminen tai tiedostoista/tietokoneesta täysin luopuminen. Yksityishenkilön halukkuuteen maksaa lunnaat vaikuttavat myös lunnasmaksun suuruus suhteessa yksilön kokemaan arvoon omista tiedostoistaan, henkilön arvio hyökkääjän luotettavuudesta tiedostojen palauttamisen suhteen sekä henkilön tiedostoihin liittyvän tietovuodon mahdollisuus (Cartwright ym., 2023).

2.2 Historia

Kiristyshaittaohjelmien historiaa voidaan pitää verrattain lyhyenä, sillä vasta internetin ja erilaisten tietojärjestelmien tullessa yhä yleisempään arkikäyttöön on niistä ollut relevanttia uhkaa ihmisille ja organisaatioille. Razaullan ym. (2023) mukaan kiristyshaittaohjelmien aikakausi alkoi 2000-luvun alkupuolella, mutta niiden pioneerityö on tehty jo vuonna 1989. Eräässä kansainvälisessä AIDS-konferenssissa biologian tohtori Joseph Popp jakoi 20 000 kiristyshaittaohjelmalla saastutettua levykettä. Asettamalla levykkeen tietokoneeseen, kiristyshaittaohjelma asentui käyttäjän tietokoneelle ja salasi kaikki C-aseman tiedostot. Tämän jälkeen loppukäyttäjälle näytettiin viesti, jossa kerrottiin tiedostojen takaisin saamiseksi vaadittavasta maksusta panamalaiseen postilokeroon. Tämän takia kiristyshaittaohjelma sai nimekseen AIDS-troijalainen (Razaulla ym., 2023). Ensimmäinen, nykyaikaisia kiristyshaittaohjelmia muistuttava hyökkäysaalto tapahtuikin yli 15 vuotta tohtori Poppin ohjelman jälkeen. Vuonna 2005 GPCode-nimistä kiristyshaittaohjelmaa levitettiin kalastelusähköpostien sekä peukaloitujen internet-linkkien avulla (O'Kane, ym., 2018). Tämän jälkeen kiristyshaittaohjelmia levittäviä hyökkäysaaltoja on ollut lukuisia, joista tehokkaimmiksi ovat osoittautuneet WannaCry- ja NotPetya-kiristyshaittaohjelmat vuonna 2017 sekä TeslaCrypt vuonna 2015 (Palatty, 2023).

Aiheen historiaan pohjaten voidaan nähdä, että kiristyshaittaohjelmia havainnoivat virustorjuntasovellukset ovat kehittyneet usein vastaamaan johonkin jo tapahtuneeseen iskuun. Kiristyshaittaohjelmien koodaajat ovat siis taitavia kehittämään aina uusia tapoja päihittää olemassa olevat puolustuskeinot. Näin ollen voidaan olettaa, että tulevaisuudessakin uudentyyppiset kiristyshaittaohjelmat tulevat olemaan varteenotettava uhka yhä kasvavassa internetin ja siihen liittyvien tietojärjestelmien sekä digitaalisten tekniikoiden käyttäjäkunnassa.

2.3 Toimintamalli

Lemmoun ym. (2021) mukaan kiristyshaittaohjelmien toiminnan voidaan nähdä perustuvan neljään eri toimintavaiheeseen. Ensimmäinen vaihe on tartuntavaihe, jossa uhriksi joutuneeseen tietokoneeseen asentuu kiristyshaittaohjelma. Luon ja Liaon (2007) mukaan tartuntatapoja on monia, mutta troijalaisten tapaan suurin osa kiristyshaittaohjelmien tartunnoista johtuu tietokoneen käyttäjän huolimattomuudesta joko sähköpostin liitteiden tai verkosta ladattujen tiedostojen kanssa. Ohjelma voi asentua myös kopeloitujen verkkosivustojen linkeistä tai turvattomien verkkoyhteyksien kautta (Luo & Liao, 2007). Kiristyshaittaohjelmien tartuntatekniikat ovat siis monipuoliset, suurimpana uhkana ollessa loppukäyttäjän huolimattomuus tai tietämättömyys mahdollisista vaaroista.

Tartunnan jälkeen kiristyshaittaohjelman toiminta riippuu sen suvusta, joita on olemassa kymmeniä erilaisia (O'Kane ym., 2018). Krypto-kiristyshaittaohjelmat pyrkivät salaamaan uhrin tietokoneen tiedostot, kun taas lukitsija-kiristyshaittaohjelmien tavoitteena on lukita käyttäjä ulos ja estää tätä käyttämästä tietokonettaan. Krypto-kiristyshaittaohjelmat hyödyntävät salauksessaan kolmea erilaista salauskeinoa, jotka on esitelty taulukossa (taulukko 1).

Salauskeino	**Toimintatapa**	**Käyttötarkoitus**
Symmetrinen salausavain	Luo ainoastaan yhden avaimen joko kohdesysteemissä tai upotettuna kiristyshaittaohjelman binääriin	Tehokas salaamaan suuria määriä tiedostoja nopeasti
Epäsymmetrinen salausavain	Hyödyntää salauspareja tiedostojen salaamisen ja purkamiseen	Pystyy myös luomaan jokaiselle uhrille tapauskohtaiset avaimet, jolloin yhden uhrin salausavain ei toimi toisen uhrin kohdalla
Hybridisalaus	Hyödyntää molempia, symmetristä sekä epäsymmetristä salausta	Ensin uhrin tiedostot salataan mahdollisimman nopeasti hyödyntäen symmetristä salausavainta, jonka jälkeen avain salataan epäsymmetristä salausta hyödyntämällä

TAULUKKO 1 Krypto-kiristyshaittaohjelmien hyödyntämät salaustekniikat (mukaillen Oz ym. 2022).

Lukitsija-kiristyshaittaohjelma puolestaan pyrkii lukitsemaan käyttäjän järjestelmän ulkopuolelle. Esimerkiksi Android-ympäristöissä ohjelma luo kelluvan, koko näytön kokoisen ikkunan, jota käyttäjä ei pysty ohittamaan eikä sulkemaan. Tällä välin ohjelma vaihtaa puhelimen PIN-koodin, mikä lukitsee käyttäjän järjestelmän ulkopuolelle (Su ym., 2018). Windows-ympäristössä haittaohjelma lukitsee käyttäjän ulos järjestelmästä luomalla uuden työpöydän (CreateDesktop) rajoitetuin ominaisuuksin, jonka jälkeen ohjelma vaihtaa (SwitchDesktop) uuden työpöydän käyttäjälle aktiiviseksi ja estää tätä vaihtamasta takaisin alkuperäiseen työpöytään esimerkiksi poistamalla pikakomennot käytöstä (Kharraz ym., 2015).

Yilmazin ym., (2021) mukaan salauksen tai lukituksen jälkeen seuraavana vaiheena kiristyshaittaohjelmat esittävät vaatimuksensa lunnasrahojen maksusta loppukäyttäjälle. Vaatimus voidaan esittää joko graafiseen käyttöliittymään ilmestyvänä ikkunana, tai vaihtoehtoisesti resurssienhallintaan syntyvänä tekstitiedostona. Maksuvaatimus voi sisältää myös esimerkiksi aikamääreen tai laskurin, joka ilmaisee, koska tiedostoja aletaan poistamaan lopullisesti. Vaikka tällaisen aikapaineen luomisen voitaisiin nähdä lisäävän uhrin epätoivoa ja tätä myöden halukkuutta maksaa lunnaat, ei tälle löydetty tieteellistä näyttöä (Yilmaz, ym., 2021). Kokemus mahdollisesti menetettävien tiedostojen arvosta suhteessa vaadittuihin lunnaisiin on yksilöllinen, joten erityyppisillä viestintätavoilla voidaan nähdä harvoin olevan vaikutusta uhrin lopulliseen maksuhalukkuuteen (Ali, 2017).

Viimeisenä vaiheena kiristyshaittaohjelmien toiminnassa on tiedostojen tai käyttäjän pääsyoikeuden palautuminen (Luo & Liao, 2007). Tämä voi tapahtua maksamalla hyökkääjän vaatimat lunnaat, jolloin tämä luovuttaa uhrille salausavaimen, tai vaihtoehtoisesti salausavaimen selvittäminen muilla keinoin. Keinoja ovat esimerkiksi tunnettujen ja jonkin aikaa jo vaikuttaneiden kiristyshaittaohjelmahyökkäyksien salausavaimien löytyminen internetistä (Palatty, 2023) tai salausavaimien ratkaisevien salauksen purkuohjelmien hyödyntäminen (Filiz, ym., 2021). Vaikkakin näitä purkuohjelmia on markkinoille ilmestynyt kiristyshaittaohjelmien lisääntyessä, ovat ne edelleen jäljessä rikollisten saavuttamasta kehityksestä. Tämän takia purkuohjelmat kykenevät purkamaan vain joidenkin kiristyshaittaohjelmasukujen salauksia, eivätkä niitäkään välttämättä kokonaan (Akbanov ym., 2019). Aiheen tutkimusta on julkaistu erittäin rajallisesti, joskin valtaosa niistä viimeisien vuosien varrelta. Tutkimuksen edistyessä mahdollinen purkuohjelmien kehitys mahdollistaisi uhrillekin turvallisemman ratkaisun tilanteen selvittämiseksi joutumatta kuitenkaan maksamaan hyökkääjän vaatimia lunnaita ja täten tukemaan rikollista toimintaa.

Tässä luvussa esitelty kiristyshaittaohjelmien toimintamalli kaikkine osineen on yleiskuvaus, joka sopii lähes kaikkien eri versioiden malliksi. Tällainen malli on pitkälle hioutunut hyökkääjien toimesta. Siitä osoituksena voidaan pitää liiketoimintamallia, jota rikolliset myyvät tahoille, joiden intressinä on tällainen hyökkäys toteuttaa. Melandin ym. (2020) mukaan onkin lähes kenen tahansa pientä ohjelmointiosaamista omaavan mahdollista tilata esimerkiksi TOR-verkosta kiristyshaittaohjelmahyökkäys ja toteuttaa tämä haluamallaan tavalla.

Tällaista palvelua kutsutaan termillä Ransomware-as-a-Service (RaaS) (Hull ym., 2019). Hullin ym. (2019) mukaan palvelun avulla mahdollisten hyökkäävien tahojen määrä on lähes loputon, mikä on omiaan lisäämään uhkaa joutua hyökkäyksen kohteeksi. Tällainen franchise-tyylinen palvelu ja sen helppokäyttöisyys ovat osasyy kiristyshaittaohjelmien lisääntymisen taustalla (Hull, ym., 2019). Tämänkaltaisen toiminnan tavoin haittaohjelman tarjoaja voi vähentää riskiään joutua toiminnastaan vastuuseen, joskin rikollisuuden kontekstissa liikutaan kyllä vähintäänkin harmaalla alueella.

2.4 Vaikutukset

Kuten mistä tahansa rikollisesta toiminnasta, seuraa kiristyshaittaohjelmalla toteutetusta hyökkäyksestä monenlaisia vaikutuksia uhrilleen, olipa sitten kyseessä yksityishenkilö tai yritys. Vaikutusten luonne ja mahdolliset seuraamukset kuitenkin joiltain osin eroavat toisistaan. Tässä alaluvussa käsitelläänkin hyökkäyksestä koituvia vaikutuksia molempien tapausten kannalta.

Kattavan tietoturvan sekä asiaan perehdytetyn henkilökunnan omaava yritys pienentää sekä riskiään joutua hyökkäyksen kohteeksi, että mahdollisia ponnisteluja hyökkäyksestä toipumiseen (Yuryna Connolly ym., 2020). Riskit ovat kuitenkin koko ajan olemassa. Kiristyshaittaohjelman kohteeksi joutumisella on huomattavia vaikutuksia yrityksen talouteen, maineeseen ja asiakas- sekä yhteistyösuhteisiin. Zimban ja Chishimban (2019) mukaan yrityksille koituvat kustannukset kiristyshaittaohjelmista tulevat kahdessa muodossa:

1. Yrityksien hyökkääjille maksamat lunnaat. Summa voi vaihdella satojen ja tuhansien dollarien välillä.

2. Tuotannon tai liiketoiminnan keskeytymisestä sekä hyökkäyksestä palautumiseen aiheutuvat kustannukset. Summat vaihtelevat tuhansista miljooniin dollareihin riippuen liiketoiminnan koosta sekä keskeytyksen ja palautumiseen tarvittavan ajan pituudesta.

Myös Kshetri ja Voas (2022) nostavat edellä mainitut yrityksien suurimmiksi kuluiksi kiristyshaittaohjelmahyökkäyksessä, kuitenkin lisäten vielä esimerkiksi mahdollisista oikeustoimista aiheutuvat kulut. Tutkimuksessaan he tuovat esiin myös muita yrityksien kokemia vaikutuksia, kuten vaikeuksia palkata tai pitää töissä kyberturvallisuuden osaajia (Kshetri & Voas, 2022). Lisäksi esimerkiksi Corbet ja Goodell (2022) tuovat esiin hyökkäyksen kohteeksi joutuneiden yritysten kärsivän merkittävästä mainehaitasta niin asiakkaiden, yhteistyökumppaneiden kuin muidenkin alalla toimivien tekijöiden silmissä. Uhkana yrityksille pahimmassa tapauksessa voi siis olla miljoonien tappiot keskeytyneestä tuotannosta, työntekijöiden menetys tai vaikeus palkata uusia tekijöitä, pisimmillään kuukausien palautuminen hyökkäyksestä sekä mainehaitan kärsiminen niin

asiakkaiden kuin muidenkin sidosryhmien silmissä. Tällaiset vaikutukset tekisivät liiketoiminnalle isoa tuhoa missä tahansa yrityksessä.

Yksityishenkilön kokemat vaikutukset kiristyshaittaohjelman iskiessä ovat suppeammat, mutta myös yksilöllisemmät yrityksien kokemiin vaikutuksiin verrattuna. Alin (2017) mukaan yksilön taloudelliset menetykset rajoittuvat saastuneen koneen sisältämien tiedostojen ja järjestelmien koettuun yhteisarvoon. Toisaalta tähän lisäyksenä joissain tapauksissa voidaan joutua lisäämään myös itse koneen rahallinen arvo, sillä niissä tapauksissa, kun lunnaita ei makseta hyökkääjälle, voi kone jäädä mahdollisesti käyttökelvottomaksi. Vaihtoehtona on myös lunnaiden maksaminen, jolloin menetys on lunnaiden summa. Toisena mahdollisena yksityishenkilön uhkana voidaan pitää maineeseen ja henkilökohtaiseen informaatioon liittyviä uhkia. Vaikka lähtökohtaisesti suurin osa kiristyshaittaohjelmista ei hyödy uhrin tiedostojen jälleenmyynnistä (Paquet-Clouston ym., 2019), on se silti mahdollinen skenaario. Tässäkin tapauksessa mahdollisesti vuodettavien tietojen arvo on yksilöllinen, mutta silti haitallista kenelle tahansa. Vuodetut tiedot voivat aiheuttaa merkittävää vahinkoa uhrille, ja asian korjaaminen voi olla erittäin pitkä ja raskas prosessi, joka ei välttämättä onnistu koskaan.

Yksityishenkilön kokemat vaikutukset siis rajoittuvat taloudellisiin vaikutuksiin joko lunnaiden tai menetettyjen tiedostojen ja laitteiden muodossa tai mahdollisesti koettuihin sosiaalisiin menetyksiin henkilökohtaisten tietojen vuotoina. Isossa kuvassa yksityishenkilöihin kohdistuvat uhat ovat huomattavasti pienempiä kuin yritysten kokemat, mutta saattaa niiden vaikutus uhriin olla kuitenkin mittava. Tutkielmaa tehdessä ei yksikään lähde käsitellyt esimerkiksi uhrien kokemia psyykkisiä haasteita, jotka henkilöstä riippuen voivat olla suuriakin.

3 KIRISTYSHAITTAOHJELMIIN VARAUTUMINEN

Ennakkoon varautumista voidaan pitää asianmukaisena ja kustannustehokkaana keinona suojautua nykyaikaiselta kyberrikollisuudelta. Kiristyshaittaohjelmilta suojautuminen ei tee tästä poikkeusta. Tässä luvussa käsitellään organisaation ja yksityishenkilön mahdollisuuksia varautua kiristyshaittaohjelman hyökkäykseen sekä tuodaan ilmi jo olemassa olevia tietoturvayritysten hyödyntämiä ja alan tieteentekijöiden kehittelemiä teknisiä ratkaisuja, joilla kiristyshaittaohjelmia voidaan mahdollisesti havaita sekä purkaa.

3.1 Yksilön ja organisaation varautumiskeinot

Siinä missä yritystoimintaan liittyvä tietoturva ja kyberrikollisuudelta varautuminen suojelee taloudellisesti arvokasta sisältöä ja on usein jossain määrin laissa säädeltyä, voidaan yritysten käyttämiä varautumiskeinoja hyödyntää myös yksityishenkilöiden kohdalla. Varautumiskeinoja ollessa useita, lähtee kuitenkin sekä Leo ym. (2022) että Luo ja Liao (2007) herättelemään hyökkäykseltä suojautujaa ajattelemaan itse omaa toimintaansa sekä pohtimaan olisiko henkilö tai yritys valmis kohtaamaan kiristyshaittaohjelmahyökkäyksestä koituvat vahingot. Pessimistinen lähtökohta aiheen tutkiskelulle on tarpeen, sillä parhaimmatkin varautumiskeinot voivat olla ohitettavissa esimerkiksi inhimillisen virheen tai hyökkääjän edistyneen teknologian takia. Useat kirjallisuuden ehdottamista varautumiskeinoista kiristyshaittaohjelmia vastaan ovat jo tunnettuja, hyvän tietoturvan mahdollistamisen ja ylläpitämisen keinoja. Keinot kuitenkin esitellään, jotta niiden merkitys juuri kiristyshaittaohjelmien vastaisessa toiminnassa kävisivät ilmi.

Ensimmäinen konkreettinen varautumiskeino Ektan ja Bansalin (2021) sekä Aidan ym. (2017) mukaan on kattavan ja ajantasaisen virustorjunnan ylläpitäminen. Virustorjunnan tehtäviin kuuluukin tiedostojen tarkistaminen ja epäilyttävien tiedostojen poistaminen tai vähintään niistä ilmoittaminen käyttäjälle. Toisaalta Adamovin ym. (2019) mukaan kehittyneimmät kiristyshaittaohjelmat

osaavat ohittaa virustorjunnan luomalla oikealta näyttävän digitaalisen allekirjoituksen. Näin kävi esimerkiksi vuonna 2019, kun LockerGoga-nimisen kiristyshaittaohjelman kerrottiin iskeneen suureen norjalaiseen teollisuusyritykseen sekä kahteen yhdysvaltalaiseen kemiallisia tuotteita valmistavaan yritykseen (Adamov ym. 2019). Virustorjunta ei siis ole täydellinen keino estää kiristyshaittaohjelman asentumista tietokoneelle, mutta se on kuitenkin oleellinen osa varautumista. Vaikka nykypäivän virustorjuntaohjelmat eivät onnistukaan havaitsemaan kaikkia kiristyshaittaohjelmia, voidaan aiheen tutkimuksella edistää niiden kehittymistä hyökkääjien hyödyntämien tekniikoiden tasolle.

Seuraava olennainen keino kiristyshaittaohjelmilta varautumiseen on Luon ja Liaon (2007) sekä Furnellin ja Emmin (2017) mukaan tietokoneen käytön kannalta oleellisten järjestelmien, kuten käyttöjärjestelmän sekä verkkoselainten pitäminen turvallisuuspäivitysten suhteen ajantasaisina. Tällä tarkoitetaan esimerkiksi Windowsille ilmestyvien päivitysten lataamista mahdollisimman pian päivityksen julkaisemisen jälkeen (Luo & Liao, 2007; Furnell & Emm, 2017). Akbanovin ym. (2019) mukaan tällaista vanhan Windows-version haavoittuvuutta hyödynsi esimerkiksi yksi tuhoisimmista kiristyshaittaohjelmista, WannaCry vuonna 2017. Tuolloin kaikille Windows-käyttöjärjestelmille oli julkaistu uusi turvallisuuspäivitys, jonka asentamatta jättäminen teki laitteesta haavoittuvaisen. Lopulta yli 300 000 tietokonetta maailmanlaajuisesti saastui WannaCry-ohjelmalla (Akbanov ym. 2019).

Kolmantena merkittävänä varautumiskeinona kirjallisuudessa esiintyy tärkeiden tiedostojen sekä järjestelmien varmuuskopiointi (Kara & Aydos, 2022; Yuryna Connolly ym., 2020). Ajantasaisella varmuuskopioinnilla voidaan välttyä tiedostojen tuhoutumisesta tai saastumisesta aiheutuvasta haitasta tilanteessa, jossa kiristyshaittaohjelma on päässyt saastuttamaan uhrin tietokoneen. Yuruna Connollyn ym. (2020) mukaan onkin todettu, että uhrit, jotka eivät ole varmuuskopioineet tiedostojaan, joutuvat suuremmalla todennäköisyydellä maksamaan hyökkääjän vaatimat lunnaat. Voidaan nähdä, että virustorjunnan tavoin varmuuskopiointi on lähtökohtaisesti yrityksillä hallussa, mutta yksityishenkilöiden keskuudessa näissä käytännöissä on huomattavasti suurempaa hajontaa.

Muita mainittuja varautumiskeinoja ovat esimerkiksi Furnellin ja Emmin (2017) mainitsema hyvä verkonhallinta. Tällä tarkoitetaan organisaatioiden yritysverkkojen sekä yksityishenkilöiden kotiverkkojen hyvää ja tarpeeksi rajoitettua järjestelmänvalvojanoikeuksien hallintaa sekä käytetyn verkon riittävää hajauttamista (Furnell & Emm, 2017). Tällä tavoin mahdollisen hyökkäyksen leviämistä yritys- tai kotiverkkoa pitkin voidaan rajoittaa hallitusti.

Näistä edellä mainituista keinoista huolimatta tärkeimpänä varautumiskeinona kiristyshaittaohjelman hyökkäykselle pidetään kuitenkin ihmisten tietoisuuden lisäämistä aiheen ympärillä. Esimerkiksi Matthijsse ym. (2023) sekä O'Kane ym. (2018) painottavat loppukäyttäjän roolin olevan erittäin kriittinen tartuntatapauksissa. Sähköpostien liitetiedostot ja linkit sekä epäilyttävillä verkkosivuilla vierailu tai niiden linkkien avaaminen ovatkin käyttäjän itsensä kompastuskiviä mahdolliseen tartuntaan. Toisaalta tällaisten ansojen välttäminen on nykypäivänä yhä haastavampaa, sillä kiristyshaittaohjelmia sisältävät

sähköpostit, kuin myös nettisivujen linkit, ovat entistä taidokkaammin räätälöity kohteidensa mukaan. O'Kanen ym. (2018) mukaan tällaista räätälöityä huijausyritystä kutsutaan sosiaaliseksi manipuloinniksi (social engineering). Huolestuttavaa on, että hyökkääjien tekniikat niin itse kiristyshaittaohjelmissa kuin sosiaalisessa manipuloinnissakin ovat kehittyneet valtavasti, mutta aiheen tutkimus keskittyy lähes ainoastaan kiristyshaittaohjelmien teknisiin toteutuksiin. Matthijssen ym. (2023) mukaan ei ainuttakaan empiiristä, ihmisen käytöksen huomioon ottavaa tutkimusta ole tehty rikosprosessista kiristyshaittaohjelman hyökkäyksen toteuttajan ja uhrin välillä. Myöskään hyökkäyksen aikaista uhrin päätöksentekoa ei ole juurikaan tutkittu. Aihealueen tutkimus kyllä painottaa, miten tärkeä rooli ihmisten tietoisuudella on, mutta juuri kukaan ei ole tutkinut, miten ja mihin perustuen tätä tietoisuutta tavallisen loppukäyttäjän tapauksessa voitaisiin lisätä (Matthijsse, ym., 2023).

3.2 Puolustusmekanismit

Siinä missä loppukäyttäjän suojautumistavoista on verrattain vähän tutkimustietoa, ovat aihealueen suosituimpia tutkimuskohteita olleet erilaiset mekanismit, joita hyödyntämällä voitaisiin kiristyshaittaohjelma havaita uhrin koneesta tai mahdollisesti jo ennen saastumista. Lemmoun ym. (2021) mukaan nykyiset, haittaohjelmia havaitsevat virustorjuntateknologiat toimivat pääasiassa kolmella eri mekanismilla, jotka on esitelty taulukossa (taulukko 2).

Havaitsemistekniikka	**Esimerkkisovellus**	**Toimintatapa**
Käytökseen perustuva havaitseminen	CryptoDrop	Havaitsee kiristyshaittaohjelmille ominaisia käyttäytymismalleja, kuten salattujen tiedostojen nimeämiskäytänteitä tai taustakuvan vaihtamista
Digitaaliseen allekirjoitukseen perustuva havaitseminen	-	Tarkistaa tiedostojen digitaalisen allekirjoituksen, ja vertaa sitä jo tuntemiinsa allekirjoituksiin. Tuntematon allekirjoitus aktivoi virustorjunnan
Syöttitiedosto (Decoy file)	Padvish, AntiRansomV3	Johonkin normaaliin kansiorakenteeseen asennettava tiedosto, jonka muutos- tai salausyritykset viruksentorjunta havaitsee

TAULUKKO 2 Virustorjuntaohjelmien havaintatekniikat (mukaillen Lemmou ym., 2019)

Uusia, eri menetelmillä haittaohjelmia havaitsevia mekanismeja tarvitaan, sillä Prachin ja Kumarin (2022) mukaan digitaaliseen allekirjoitukseen tai kohdetiedoston käyttäytymismalleihin perustuvat tietoturvaohjelmat alkavat käydä vanhanaikaisiksi. Tulevaisuudessa tekniikat ovatkin varmasti kehittymässä, sillä esimerkiksi tekoälyä (Alvee ym., 2021) sekä koneoppimista (Almousa ym., 2021) apunaan käyttäviä havaintatekniikoita on pystytty jo tieteellisissä testiolosuhteissa hyödyntämään tehokkaasti. Lisäksi hyökkäyksien jälkeen erilaisia kiristyshaittaohjelmia voidaan jäljittää esimerkiksi Bitcoin liikenteen, Google-hakujen tai VirusTotal-ohjelmasta löytyvien binäärien kautta, mikäli se on esimerkiksi rikostutkinnan tai tiedonsaannin kannalta oleellista (Huang ym., 2018).

4 YHTEENVETO

Tämän tutkielman tarkoituksena oli kirjallisuuskatsauksen keinoin tuoda esiin kiristyshaittaohjelmiin liittyviä uhkakuvia sekä seurauksia organisaatioille ja yksityishenkilöille. Lisäksi tutkielma pyrki luomaan yleiskuvan mahdollisista ehkäisykeinoista niin potentiaalisen uhrin kuin olemassa olevien puolustusmekanismienkin osalta. Tutkielman lähdemateriaalit koostuivat vertaisarvioiduista tieteellisistä artikkeleista, konferenssiesityksistä sekä aiheen kannalta relevanteista verkkosivuista.

Tutkielman toisessa luvussa määriteltiin kiristyshaittaohjelman käsite sekä kuvattiin kiristyshaittaohjelmien historiaa ja toimintamallia. Lisäksi toisessa luvussa käsiteltiin kiristyshaittaohjelman hyökkäyksen vaikutuksia niin organisaation kuin yksityishenkilönkin kontekstissa. Kolmannessa luvussa puolestaan tuotiin esiin organisaatioiden ja yksityishenkilöiden varautumismahdollisuuksia ehkäistäkseen kiristyshaittaohjelman tartunnan. Lisäksi kolmannessa luvussa käsiteltiin lyhyesti olemassa olevien havainta- ja puolustusmekanismien toimintaa ja tulevaisuuden mahdollisuuksia.

Tälle kirjallisuuskatsaukselle määriteltiin aluksi kaksi tutkimusta ohjaavaa tutkimuskysymystä, joihin pyrittiin vastaamaan. Nämä kysymykset olivat:

- *"Mitä uhkia kiristyshaittaohjelmiin liittyy?"*
- *"Miten kiristyshaittaohjelmiin liittyviin uhkiin voidaan varautua?"*

Tutkielman perusteella voidaankin havaita, että kiristyshaittaohjelmien muodostama turvallisuusuhka on noussut merkittäväksi haasteeksi 2010-luvulla. Kiristyshaittaohjelmien suosio rikollisten keskuudessa johtuu pitkälti houkuttelevista taloudellisista tuotto-odotuksista, tekijän anonymiteetin mahdollistavien maksutapojen yleistymisestä sekä kiristyshaittaohjelmien pitkälle hioutuneesta toimintamallista.

Organisaatioiden osalta kirjallisuuskatsaus tuo esiin kiristyshaittaohjelmien hyökkäyksien aiheuttavan merkittäviä taloudellisia vaikutuksia. Näitä vaikutuksia tarkasteltaessa erottuvat selkeästi kahdet pääasialliset tekijät: lunnaiden maksaminen hyökkääjille ja liiketoiminnan keskeytymisestä johtuvat

kustannukset. Lähdemateriaalien pohjalta havaittiin, että liiketoiminnan keskeytymisen katsotaan olevan taloudellisesti merkittävämpi tekijä kuin lunnaiden maksaminen. Lisäksi organisaatiot kohtaavat maineellisia haittoja, jotka heikentävät esimerkiksi työntekijöiden rekrytointia ja yhteistyösopimusten muodostamista ja ylläpitoa.

Yksityishenkilöiden osalta kiristyshaittaohjelmien vaikutukset rajoittuvat taloudellisiin menetyksiin ja tietoturvariskeihin. Taloudelliset menetykset liittyvät usein lunnaiden maksamiseen tai menetettyjen tiedostojen arvon menetykseen. Vaikka yksityishenkilöt kokevat usein henkilökohtaisempia vaikutuksia, kuten tiedostojen menetyksen tai tietovuodon mahdollisuuden, organisaatioille koituvat taloudelliset ja maineelliset haitat ovat laajempia ja monimutkaisempia.

Lisäksi havaittiin, että varautuminen kiristyshaittaohjelmiin vaatii monipuolista lähestymistapaa. Perinteiset tietoturvamenetelmät, kuten laadukas virustorjunta, ovat välttämättömiä kiristyshaittaohjelmien havaitsemiseksi ja torjumiseksi. Kuitenkin tutkielma tuo esiin, että pelkät virustorjunnat eivät välttämättä pysty tunnistamaan kaikkia uhkia. Turvallisuuspäivitysten ajantasaisuus sekä säännöllinen tiedostojen varmuuskopiointi ovat myös oleellisia varautumiskeinoja. Näiden keinojen lisäksi havaittiin inhimillisten tekijöiden olevan kriittinen tekijä kiristyshaittaohjelmien torjunnassa. Loppukäyttäjien tietoisuuden lisääminen ja koulutus ovat tärkeitä toimenpiteitä, sillä inhimilliset virheet, kuten sähköpostiliitteiden avaaminen, ovat merkittäviä tartuntareittejä. Tämä korostaa, että teknologiset ratkaisut eivät yksin riitä, vaan käyttäjien osallistuminen ja tietämys ovat avainasemassa.

Tutkielman onnistuneisuutta arvioidessa on ensin otettava huomioon tutkielman tekoon vaikuttaneet haasteet ja rajoitteet. Merkittävimpinä haasteina ja rajoitteina voidaan tämän tutkielman osalta pitää saatavilla olevan lähdemateriaalin rajallisuutta. Etenkin inhimillisten tekijöiden osallisuutta kiristyshaittaohjelmiin oli saatavilla olevissa lähdemateriaalissa käsitelty erittäin vähän suhteutettuna siihen, kuinka tärkeäksi osaksi tietoturvaa valikoitu lähdemateriaali sen painotti. Lisäksi on tarpeen huomioida mahdollisen kiristyshaittaohjelmahyökkäyksen kohteeksi joutuneiden organisaatioiden ja yksityishenkilöiden haluttomuus jakaa informaatiota kokemuksistaan, mikä rajoittaa alan tutkimuksen tietämystä aiheesta.

Toisaalta kiristyshaittaohjelmien ollessa verrattain tuore uhkatekijä kybermaailmassa, on aiheen tutkimuskin vielä kehittyvää. Tästä esimerkkinä tämän tutkielman lähdeaineistot, joista ainoastaan kolme kappaletta on julkaistu ennen vuotta 2017. Aihealueen ympärille liittyy vahvasti jatkuva muutos ja ajankohtaisuus, joiden vuoksi aiheen jatkotutkimukselle on tulevaisuudessa tarvetta. Havaitsemis- ja puolustautumismekanismien tutkimus on myös alalla tarpeen, jotta rikollisten hyödyntämien tekniikoiden etumatka suhteessa virustorjuntajärjestelmiin saadaan kurottua kiinni.

Mainitut haasteet ja rajoitteet huomioon ottaen voidaan tutkielmaa kokonaisuudessaan pitää kuitenkin kohtalaisen onnistuneena, sillä se tarjoaa katsauksen kiristyshaittaohjelmien uhkiin sekä niihin varautumiseen yksilöiden ja organisaatioiden näkökulmasta. Asetettuihin tutkimuskysymyksiin pystyttiin

lähdeaineiston perusteella vastaamaan sekä havaittuja löydöksiä tarkastelemaan kokoavasti ja kriittisesti. Tämän tutkielman pohjalta mielenkiintoinen jatkotutkimusaihe olisikin esimerkiksi empiirinen tutkimus loppukäyttäjän toimista ja käytöksestä simuloidussa kiristyshaittaohjelman hyökkäyksessä.

LÄHTEET

Adamov, A., Carlsson, A., & Surmacz, T. (2019). An analysis of lockergoga ransomware. *In 2019 IEEE East-West Design & Test Symposium (EWDTS)*, 1-5. https://doi.org/10.1109/EWDTS.2019.8884472

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive survey on petya ransomware attack. *In 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, 122-125. https://doi.org/10.1109/ICNGCIS.2017.30

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology*, (1), 113-124. https://doi.org/10.26636/jtit.2019.130218

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Issues in Informing Science and Information Technology*, 14, 1-13. http://www.informingscience.org/Publications/3707

Almousa, M., Basavaraju, S., & Anwar, M. (2021). Api-based ransomware detection using machine learning-based threat detection models. *In 2021 18th International Conference on Privacy, Security and Trust (PST)* 1-7. https://doi.org/10.1109/PST52912.2021.9647816

Alvee, S. R., Ahn, B., Kim, T., Su, Y., Youn, Y. W., & Ryu, M. H. (2021). Ransomware attack modeling and artificial intelligence-based ransomware detection for digital substations. *In 2021 6th IEEE Workshop on the Electronic Grid (eGRID)* 1-5. https://doi.org/10.1109/eGRID52793.2021.9662158

August, T., Dao, D., & Niculescu, M. F. (2022). Economics of ransomware: Risk interdependence and large-scale attacks. *Management Science*, 68(12), 8979-9002. https://doi.org/10.1287/mnsc.2022.4300

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 1-22. https://doi.org/10.1016/j.cose.2021.102490

Cartwright, A., Cartwright, E., Xue, L., & Hernandez-Castro, J. (2023). An investigation of individual willingness to pay ransomware. *Journal of Financial Crime*, 30(3), 728-741. https://doi.org/10.1108/JFC-02-2022-0055

Corbet, S., & Goodell, J. W. (2022). The reputational contagion effects of ransomware attacks. *Finance Research Letters*, 47, 1-8. https://doi.org/10.1016/j.frl.2022.102715

Ekta, Bansal, U. (2021). A review of ransomware attack. *In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, 221-226. https://doi.org/10.1109/ICSCCC51823.2021.9478148

Everett, C. (2016). Ransomware: to pay or not to pay?. *Computer Fraud & Security*, 2016(4), 8-12. https://doi.org/10.1016/S1361-3723(16)30036-7

Filiz, B., Arief, B., Cetin, O., & Hernandez-Castro, J. (2021). On the effectiveness of ransomware decryption tools. *Computers & Security*, 111, 1-12. https://doi.org/10.1016/j.cose.2021.102469

Furnell, S., & Emm, D. (2017). The ABC of ransomware protection. *Computer Fraud & Security*, 2017(10), 5-11. https://doi.org/10.1016/S1361-3723(17)30089-1

Hull, G., John, H., Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, 2019(8), 1-22. https://doi.org/10.1186/s40163-019-0097-9

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K. & McCoy, D. (2018). Tracking ransomware end-to-end. *In 2018 IEEE Symposium on Security and Privacy (SP)*, 618-631. https://doi.org/10.1109/SP.2018.00047

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications*, 190, 1-14. https://doi.org/10.1016/j.eswa.2021.116198

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. *In Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015*, 3-24. Springer International Publishing. https://doi.org/10.1007/978-3-319-20550-2_1

Kshetri, N., & Voas, J. (2022). Ransomware as a business (RaaB). *IT Professional*, 24(02), 83-87. https://doi.org/10.1109/MITP.2022.3157208

Kumar, S., Prachi (2022). An effective ransomware detection approach in a cloud environment using volatile memory features. *Journal of Computer Virology and Hacking Techniques*, 18(4), 407–424. https://doi.org/10.1007/s11416-022-00425-2

Leo, P., Isik, Ö., & Muhly, F. (2022). The ransomware dilemma. *MIT Sloan Management Review*, 63(4), 13-15. https://www.proquest.com/scholarly-journals/ransomware-dilemma/docview/2678515108/se-2

Lemmou, Y., Lanet, J. L., & Souidi, E. M. (2021). A behavioural in‐depth analysis of ransomware infection. *IET Information Security*, 15(1), 38-58. https://doi.org/10.1049/ise2.12004

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security*, 16(4), 195-202. https://doi.org/10.1080/10658980701576412

Matthisse, S.R., van 't Hoff-de Goede, M.S., Leukfeldt, E.R. (2023). Your files have been encrypted: a crime script analysis of ransomware attacks. *Trends in Organized Crime*, 1-27. https://doi.org/10.1007/s12117-023-09496-z

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, 92, 1-9. https://doi.org/10.1016/j.cose.2020.101762

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *The Institution of Engineering and Technology*, 7(5), 321-327. https://doi.org/10.1049/iet-net.2017.0207

Or-Meir, O., Nissim, N., Elovici, Y., Rokach, L. (2019). Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM Computing Surveys*, 52(5), 1-48. https://doi.org/10.1145/3329786

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 54, 1-37. https://doi.org/10.1145/3514229

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, 5(1), 1-11. https://doi.org/10.1093/cybsec/tyz003

Palatty, N. J. (2023). 10 of the Biggest Ransomware Attacks in History, noudettu 10. marraskuuta 2023, osoitteesta https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/

Prachi, Kumar, S. (2022). An effective ransomware detection approach in a cloud environment using volatile memory features. *Journal of Computer Virology and Hacking Techniques*, 18(4), 407–424. https://doi.org/10.1007/s11416-022-00425-2

Razaulla, S., Fachkha, C., Markarian, M., Gawanmeh, A., Mansoor, W., Fung, B. C. M., Assi, C. (2023). The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access*, 11, 40698-40723. https://doi.org/10.1109/ACCESS.2023.3268535

Su, D., Liu, J., Wang, X., & Wang, W. (2018). Detecting Android locker-ransomware on Chinese social networks. *IEEE Access*, 7, 20381-20393. https://doi.org/10.1109/ACCESS.2018.2888568

Yilmaz, Y., Cetin, O., Arief, B., Hernandez-Castro, J. (2021). Investigating the impact of ransomware splash screens. *Journal of Information Security and Applications*, 61, 1-13. https://doi.org/10.1016/j.jisa.2021.102934

Yuryna Connolly, L., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, 6(1), 1-18. https://doi.org/10.1093/cybsec/tyaa023

Zimba, A., & Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research*, 4(1), 3-31. https://doi.org/10.1007/s41125-019-00039-8

Zimba, A., Wang, Z., & Chishimba, M. (2019). Addressing crypto-ransomware attacks: before you decide whether to-pay or not-to. *Journal of Computer Information Systems*. 61, 53-63. https://doi.org/10.1080/08874417.2018.1564633

Zhang-Kennedy, L., Assal, H., Rocheleau, J., Mohamed, R., Baig, K., & Chiasson, S. (2018). The aftermath of a crypto-ransomware attack at a large academic institution. *In 27th USENIX Security Symposium (USENIX Security 18)* 1061-1078. https://www.usenix.org/conference/usenixsecurity18/presentation/zhang-kennedy