Ransomware-hyökkäysten torjunta organisaatiossa: Ehkäisy, ennakointi ja havaitseminen

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Kesäkuu 2025
Lasse Haapiainen

TURUN YLIOPISTO
Tietotekniikan laitos

Lasse Haapiainen: Ransomware-hyökkäysten torjunta organisaatiossa: Ehkäisy, ennakointi ja havaitseminen

TkK-tutkielma, 24 s.
Tietotekniikka
Kesäkuu 2025

Ransomware-hyökkäykset ovat kasvava uhka organisaatioille eri toimialoilla. Tämä tutkielma on kirjallisuuskatsaus, joka kokoaa ajankohtaista tutkimustietoa ransomware-hyökkäysten torjunnan keskeisistä osa-alueista: ehkäisystä, ennakoinnista ja havaitsemisesta. Työssä esitellään ransomware-uhkien kehityshistoriaa, yleisimpiä tartuntavektoreita sekä torjuntaan käytettäviä teknisiä ja organisatorisia toimenpiteitä. Lisäksi kuvataan erilaisia havaitsemismenetelmiä, kuten koneoppimiseen perustuvia ratkaisuja ja nykyisiä havaitsemistyökaluja. Tutkielma osoittaa, että tehokas ransomware-torjunta edellyttää moniulotteista ja jatkuvasti päivitettävää lähestymistapaa, jossa yhdistyvät teknologiset keinot, ennakoiva varautuminen ja henkilöstön koulutus.

Asiasanat: ransomware, kyberturvallisuus, haittaohjelmat, ehkäisy, havaitseminen, tietoturva

UNIVERSITY OF TURKU
Department of Computing

Lasse Haapiainen: Ransomware-hyökkäysten torjunta organisaatiossa: Ehkäisy, ennakointi ja havaitseminen

Bachelor's Thesis, 24 p.
Laboratory Name
June 2025

Ransomware attacks pose an increasing threat to organizations across various sectors. This thesis is a literature review that compiles current research on the key aspects of defending against ransomware: prevention, preparation, and detection. It presents the historical development of ransomware threats, the most common infection vectors, and both technical and organizational countermeasures. Furthermore, it outlines various detection methods, including machine learning-based solutions and modern detection tools. The study emphasizes that effective ransomware defense requires a multifaceted and continuously evolving approach that combines technological measures, proactive planning, and user education.

Keywords: ransomware, cybersecurity, malware, prevention, detection, information security

Sisällys

1 Johdanto

Ransomware-hyökkäyksistä on viime vuosina muodostunut merkittävä uhka eri alojen organisaatioille [1]. Ransomware on haittaohjelma, joka salaa uhrin datan ja vaatii lunnaita salauksen purkamiseksi [2]. Se aiheuttaa huomattavia taloudellisia tappioita yrityksille ja organisaatioille, ja sen esiintyvyys on kasvanut merkittävästi. Vuoden 2021 arvioiden mukaan hyökkäyksiä tapahtui keskimäärin 11 sekunnin välein [3]. Samana vuonna ransomwaren aiheuttamien taloudellisten vahinkojen arvioitiin olevan noin 20 miljardia Yhdysvaltain dollaria [2].

Tämä tutkielma on kirjallisuuskatsaus, joka kokoaa yhteen ajankohtaista tutkimustietoa ransomware-hyökkäysten torjunnan eri osa-alueista. Tutkielma tarkastelee erityisesti kolmea näkökulmaa: ehkäisy, ennakointi ja havaitseminen. Työssä esitellään yleisiä tartuntavektoreita, hyökkäysten teknologista kehitystä sekä nykyisiä torjuntatekniikoita ja -työkaluja. Tavoitteena on jäsentää kattavasti, millaisia teknisiä ja organisatorisia toimenpiteitä ransomware-uhkiin voidaan kohdistaa, ja miten organisaatiot voivat parantaa valmiuttaan tällaisia hyökkäyksiä vastaan.

Tutkielman tutkimuskysymykset ovat:

TK1: Millaisia ennakoivia ja ehkäiseviä toimenpiteitä organisaatiot voivat toteuttaa suojautuakseen ransomware-hyökkäyksiltä?

TK2: Millaisia menetelmiä ja työkaluja on käytettävissä ransomware-hyökkäysten havaitsemiseen ja analysointiin, ja mitä haasteita niihin liittyy?

Tutkielmassa käytettiin tiedonhakuun IEEE Xplore, Web of Science ja ACM

Digital Library tietokantoja. Tiedonhaussa käytettiin hakusanoja: ransomware, prevention, detection ja mitigation. Hakulausekkeet olivat aina muotoa “ransomware AND hakusana”. Jokaisessa haussa käytettiin kahta rajausta: ransomware on mainittu dokumentin otsikossa ja tulokset on julkaistu 2021—2024.

Tällä menetelmällä saatiin IEEE Xplore -tietokannasta yhteensä 244 hakutulosta, joista valittiin 11. Web of Science -tietokannasta löytyi vastaavasti 225 tulosta, joista suuri osa oli päällekkäisiä IEEE:n hakutulosten kanssa; näistä valittiin 2. ACM Digital Library -tietokannasta löytyi 142 tulosta, joista valittiin 5 samalla hakumenetelmällä.

2 Ransomware

Ransomware on haittaohjelman alalaji, joka salaa uhrin datan ja vaatii lunnaita salauksen purkamista vastaan [2]. Onnistunut ransomware-hyökkäys voi estää organisaation kyvyn tarjota kriittisiä palveluja, ja johtaa joissain tapauksissa merkittävään toiminnalliseen häiriöön tai kokonaisvaltaiseen toimintakyvyttömyyteen [4]. Ransomware on kehittynyt yksinkertaisesta haittaohjelmasta edistyneeksi ja vaaralliseksi uhaksi, joka kohdistuu niin yksilöihin, organisaatioihin kuin valtioihin. Jatkuvasti kehittyvät hyökkäystekniikat, kryptovaluuttojen tarjoama anonymiteetti sekä uhrien haluttomuus ilmoittaa hyökkäyksistä mainehaitan pelossa ovat vaikeuttaneet taistelua ransomware-hyökkäyksiä vastaan [5].

Ransomware-hyökkäyksillä on vakavat ja laajat seuraukset, jotka ulottuvat lunnaiden maksamisen ohi. Hyökkäykset voivat häiritä organisaation toimintaa, mikä puolestaan johtaa viivästyksiin, taloudellisiin tappioihin ja vahinkoon organisaation maineelle. Toiminnan häiriintymisestä aiheutuu myös tuottavuuden menetystä, järjestelmien palautuskustannuksia, investointeja kyberturvallisuuteen, mahdollisia sakkoja sekä oikeudenkäyntikustannuksia. Äärimmäisissä tapauksissa ransomware-hyökkäyksen aiheuttamat seuraukset voivat jopa uhata organisaation olemassaoloa [5].

2.1 Ransomware-hyökkäysten luokittelu

Ransomware on kehittynyt monimuotoiseksi uhkaksi, joka voi ilmetä erilaisina muotoina ja hyödyntää monenlaisia hyökkäystapoja. Näiden haittaohjelmien ymmärtäminen ja luokittelu on keskeistä niin teknisten puolustusratkaisujen kuin riskien arvioinnin ja puolustusstrategioiden kehittämisessä. Tässä alaluvussa tarkastellaan ransomwaren luokittelua, joka tarjoaa selkeän kokonaiskuvan sen eri muodoista ja toimintaperiaatteista.

Crypto-ransomware

Crypto-ransomware on ransomware-tyypeistä yleisin [6]. Se on myös haitallisin, sillä se salaa käyttäjän tiedostot edistyneillä salausmenetelmillä, kuten AES- tai RSA-algoritmeilla. Salaus estää tiedostojen palauttamisen ilman lunnaita. Kryptoransomwaren laaja levinneisyys ja vakavat vaikutukset tekevät siitä keskeisen tutkimuskohteen [7].

Locker-Ransomware

Locker-Ransomware estää tiedostojen salauksen sijaan kokonaan käyttäjän pääsyn järjestelmään. Nämä hyökkäykset muuttavat yleensä järjestelmän asetuksia tai näyttävät kokoruudun viestin estäen käyttäjää pääsemästä omiin järjestelmiinsä. Tällaiset hyökkäykset ovat usein selkeämpiä ja vaativat uhrilta välitöntä huomiota. Tunnettuja locker-tyyppisiä ransomware-hyökkäyksiä ovat muun muassa Reveton ja Police-ransomware [6].

Ransomware-as-a-Service (RaaS)

RaaS on liiketoimintamalli, jossa kyberrikolliset vuokraavat tai ostavat ransomware-ohjelmia kehittäjiltä ja jakavat lunnaat kehittäjien kanssa. Tämä malli on tehnyt

ransomware-hyökkäysten toteuttamisesta helpompaa, antaen vähemmän teknisesti taitaville hyökkääjille mahdollisuuden aloittaa hyökkäyksiä vaivattomasti [8].

Scareware

Scareware ei käytä todellista tiedonsalausta, vaan hyödyntää psykologista manipulointia huijatakseen käyttäjän uskomaan, että heidän järjestelmänsä on tartutettu. Uhria painostetaan maksamaan väärennetystä virustorjuntaohjelmasta, joka väitetään ratkaisevan tämän olemattoman ongelman [6].

Doxware

Doxware käyttää erilaista lähestymistapaa uhkaamalla julkaista arkaluonteisia tai luottamuksellisia tietoja, ellei lunnaita makseta. Tällainen ransomware on erityisen tuhoisaa henkilöille tai organisaatioille, jotka käsittelevät arkaluontoista tietoa, sillä tietovuodon mahdolliset maineen ja oikeudelliset seuraukset voivat olla vakavia [6].

2.2 Ransomware-uhkien historia ja kehittyminen

Ransomware-hyökkäysten alkuperä voidaan jäljittää vuoteen 1989, jolloin julkaistiin ensimmäinen tunnettu ransomware-haittaohjelma, AIDS-troijalainen (PC Cyborg). Haittaohjelma levitettiin fyysisillä levykkeillä, jotka sisälsivät ohjelman, joka salasi uhrin tiedostojen nimet ja vaati lunnaat salauksen purkamiseksi. Tämä varhainen tapaus edusti vielä teknisesti rajoittunutta toteutusta, mutta loi perustan ransomware-ohjelmien myöhemmille toimintamalleille [2].

Vuonna 1996 tapahtui merkittävä akateeminen läpimurto, kun tutkijat analysoivat kyseisen haittaohjelman haavoittuvuuksia ja esittelivät kryptovirologian käsitteen. He esittivät toimivan konseptin haittaohjelmasta, joka käytti asymmetristä julkisen avaimen salausta. Tämä kehitys oli keskeinen siirtymävaihe, jossa yhdistyivät kryptografinen osaaminen ja haittaohjelmien kehitys [2].

2000-luvun alussa alkoi uusi aikakausi ransomwaren leviämisessä, kun internetin laajentuva käyttö mahdollisti haittaohjelmien tehokkaamman jakelun. Vuonna 2004 ilmestynyt GPCode oli yksi ensimmäisistä, joka käytti sähköpostin liitetiedostoja sekä haitallisia verkkosivulinkkejä tartuntavektoreina. Vuonna 2006 julkaistu Archievus oli ensimmäinen ransomware, joka hyödynsi RSA-salausta, mikä teki siitä teknologisesti kehittyneemmän verrattuna aiempiin. Kummassakin tapauksessa hyökkääjät suosivat matalia lunnassummia ja suurta kohdeyleisöä, mikä erosi myöhempien vuosien kohdennetuista hyökkäyksistä. Vuonna 2007 julkaistu WinLock merkitsi siirtymää niin sanottuihin locker-tyyppisiin haittaohjelmiin, jotka eivät salanneet tiedostoja, vaan estivät käyttäjän pääsyn järjestelmään esimerkiksi näyttämällä ruudulla häiritsevää sisältöä. Lunnaat pyydettiin maksullisen SMS-viestin kautta [9].

Vuonna 2008 ransomware-kehitys jatkui teknisen monimutkaisuuden suuntaan. Ransom.C käytti uskottavuutta hyväkseen esiintyen Windowsin suojauskeskuksena ja vaati uhrilta soittoa premium-puhelinnumeroon lisenssin aktivoimiseksi. Samaan aikaan julkaistu Seftad-ransomware edusti uutta tasoa haitallisuudessa, muokkaamalla tietokoneen Master Boot Recordia (MBR) ja estäen järjestelmän normaalin käynnistymisen. Tämä lähestymistapa osoitti, että hyökkääjät olivat siirtyneet pelkästään tiedostojen salaamisesta järjestelmän kriittisten osioiden, kuten käynnistysrekisterin (MBR), hallintaan [2].

Yksi merkittävimmistä teknologisista muutoksista ransomware-kehityksessä oli kryptovaluuttojen, erityisesti Bitcoinin, käyttöönotto vuodesta 2009 lähtien. Kryptovaluutat ratkaisivat kaksi aiempaa ongelmaa: maksujen alueelliset rajoitukset ja rikollisten anonymiteetin puutteen. Vuonna 2011 havaittiin jo yli 60 000 uutta ransomware-perhettä, mikä kuvastaa ilmiön nopeaa laajenemista. Vuonna 2012 ilmestynyt Reveton yhdisti locker-tyyppisen ransomwaren tietovarkauksiin, mikä laajensi haittaohjelman vaikutuksia entisestään. CryptoLocker vuonna 2013 käytti kehittynyttä 2048-bittistä RSA-salausta sekä Bitcoinia lunnasvaluuttana. Vuonna 2014 julkaistu

CTB Locker hyödynsi elliptistä käyräkryptografiaa (ECC) ja TOR-verkkoa nimettömyyden varmistamiseen sekä Bitcoinia maksuvälineenä. Samana vuonna esiin nousi myös Cryptowall, joka poisti varmuuskopiot tiedostojen palauttamisen estämiseksi ja tartutti yli 600 000 järjestelmää. Vuodesta 2014 alkaen ransomware-hyökkäykset alkoivat kohdistua myös muihin käyttöjärjestelmiin. Vuoden 2014 lopulla ilmestyi ensimmäinen locker-tyyppinen mobiili-ransomware Android Defender, joka naamioi itsensä oikeaksi antivirus-ohjelmaksi. Seuraavana vuonna ilmestyi uusi versio samalla nimellä, joka käytti edistynyttä AES-salausta tiettyjen tiedostojen salaamiseen SD-kortilla, mutta ohjelman binäärikoodissa oleva salausavain teki salauksen purkamisesta triviaalin. Vuonna 2015 ilmestyi ensimmäinen Linux-käyttöjärjestelmiin kohdistuva ransomware Linux.Encoder. Se salasi käyttäjän kotihakemiston sekä verkkosivujen hallintaan liittyvät hakemistot. Vuotta myöhemmin havaittiin ensimmäinen macOS-käyttöjärjestelmiin kohdistuva ransomware KeRanger. Ohjelma oli allekirjoitettu voimassa olevalla Mac-sovelluskehittäjän sertifikaatilla, mikä mahdollisti Applen suojauksien ohittamisen. Linux.Encoder ja KeRanger käyttivät molemmat hybridisalausta, eli kryptografista menetelmää, jossa hyödynnetään sekä symmetristä että epäsymmetristä salausta [2].

Ransomware-hyökkäysten kehitys sai uuden käänteen vuonna 2015, kun Ransomware-as-a-Service (RaaS) tuli osaksi kyberrikollisuuden liiketoimintamallia. RaaS mahdollisti ransomware-ohjelmien käytön laajemmalle joukolle hyökkääjiä, sillä se tarjosi helposti käytettäviä ja räätälöitävissä olevia ransomware-paketteja pimeiltä markkinoilta. Tämä kehitys oli merkittävä, sillä ransomware pystyi nyt tartuttamaan minkä tahansa alustan, tehden niistä riippumattomia ja helpommin mukautettavia. RaaS:n myötä ransomware-hyökkäysten määrä kasvoi merkittävästi maailmanlaajuisesti. Tämä muutti ransomware-hyökkäysten luonteen ja teki niistä yhä helpommin saavutettavissa olevia kyberrikollisille, jotka halusivat käyttää niitä omissa hyökkäyksissään [2].

Vuoden 2017 WannaCry-hyökkäys on yksi tunnetuimmista esimerkeistä kryptografisesta ransomwaresta. Hyökkäys hyödynsi EternalBlue-haavoittuvuutta Windows-järjestelmissä ja levisi nopeasti globaalisti. Sen vaikutukset olivat merkittäviä erityisesti julkisessa terveydenhuollossa. Vuonna 2019 julkaistu Maze-ransomware käynnisti uudenlaisen kiristyksen muodon, niin sanotun kaksoiskiristyksen (double extortion). Tässä mallissa uhka ei rajoitu pelkkään tiedostojen salaamiseen, vaan uhreilta varastetaan tietoa, jonka julkaisemisella heitä uhataan, mikäli lunnaat jäävät maksamatta. Tämä kasvatti merkittävästi hyökkäysten painostusarvoa [9].

Vuonna 2020 julkaistu Egregor käytti monia analyysin vastaisia tekniikoita, kuten hyötykuorman salausta ja koodin obfuskointia, vaikeuttamaan haittaohjelman havaitsemista ja tutkimista. Conti-ransomware erottui kyvyllään levitä nopeasti järjestelmästä toiseen. Usein hyökkäys alkoi phishing-viesteillä, joiden kautta ladattiin TrickBot- tai BazarLoader-troijalaisia, jotka mahdollistivat etäyhteyden [9]. Vuonna 2021 esiin noussut DarkSide kohdisti hyökkäyksensä maksukykyisiin organisaatioihin, ja sen vastuulla oli yksi kaikkien aikojen vakavimmista hyökkäyksistä – Colonial Pipeline -tapaus. Ryhmä noudatti niin sanottua “eettistä linjaa” jättäen julkiset ja humanitääriset kohteet rauhaan [9].

Vuonna 2022 havaittiin merkittävä trendi uusien haittaohjelmavariaatioiden esiintymisessä. Monet näistä käyttivät edelleen kaksoiskiristystaktiikkaa, mutta ne levitettiin yhä useammin Ransomware-as-a-Service (RaaS) -mallin mukaisesti. Erityisesti Lockbit-ransomware osoitti huomattavaa sopeutumiskykyä: sen kehittäjät kykenivät säännöllisesti päivittämään hyökkäystaktiikoita ja tarjoamaan palvelujaan muille rikollisille. Tämä mallimuutos on tehnyt torjunnasta ja ennaltaehkäisystä entistä haasteellisempaa [9].

2.3 Tartuntavektorit

Kuten muut haittaohjelmat, ransomware voi päästä organisaation järjestelmiin monin eri tavoin. Ransomwaren yleisin tartuntavektori on edelleen sähköposti [9], [10], [11], mutta ransomware-hyökkäysten leviämistavat ovat laajentuneet perinteisten sähköpostitse tapahtuvien phishing-hyökkäysten ulkopuolelle [6]. Seuraavaksi tarkastellaan ransomwaren yleisimpiä tartuntavektoreita.

Verkkourkinta (phishing) on edelleen yleisin ransomware-hyökkäyksissä käytetty tartuntavektori. Hyökkäykset alkavat usein, kun käyttäjät saavat haitallisia linkkejä tai liitteitä sisältävän sähköpostin, jotka näyttävät tulevan tutulta yhteyshenkilöltä. Hyökkääjät huijaavat käyttäjiä avaamaan liitteet tai klikkaamaan linkkejä, jotka johtavat haittaohjelmien asentamiseen, käyttäen yleisiä tiedostomuotoja kuten .pdf, .doc ja .jpg [9].

Remote Desktop Protocol (RDP) on toiseksi yleisin tartuntavektori, ja sen suosio johtuu siitä, että RDP:stä löydetään jatkuvasti uusia haavoittuvuuksia. Erityisesti vuonna 2020 havaittiin useita uusia haavoittuvuuksia RDP-asiakasohjelmista, jotka tekevät siitä houkuttelevan kohteen hyökkääjille [9].

Ohjelmistojen haavoittuvuudet sijoittuvat kolmanneksi yleisimpien tartuntavektoreiden joukkoon. Kun ohjelmistoja ei päivitetä riittävästi, hyökkääjät voivat päästä järjestelmiin ilman käyttäjätunnusten kalastelua [9].

Verkkosivustot voivat toimia myös tartuntavektoreina, kun ransomware on piilotettu haitallisille sivustoille, jotka näyttävät luotettavilta. Käyttäjät voivat ladata haittaohjelman tietämättään, kun he vierailevat näillä sivuilla [9].

Ponnahdusikkunat ovat toinen yleinen verkkopohjainen tartuntavektori. Käyttäjät huijataan klikkaamaan ponnahdusikkunoita, jotka näyttävät aidoilta ja luotettavilta. Tämän seurauksena ransomware ladataan joko automaattisesti tai ohjataan käyttäjä haitallisille linkeille [9].

3 Ransomware-hyökkäysten torjunta

Tässä luvussa tarkastellaan ransomware-hyökkäysten torjunnan keskeisiä näkökulmia, erityisesti hyökkäysten ehkäisyä, ennakointia sekä tehokkaita havaitsemis- ja analyysimenetelmiä. Ransomware-hyökkäykset ovat kehittyneet monivaiheisemmiksi ja tuhoisammiksi, ja niiden torjunta edellyttää jatkuvasti mukautuvaa ja moniulotteista lähestymistapaa. Luvussa käsitellään toimenpiteitä ja tekniikoita, joiden avulla organisaatiot voivat valmistautua ransomware-hyökkäyksiin, tunnistaa ne nopeasti ja minimoida niiden aiheuttamat vahingot. Keskeisiä aiheita ovat muun muassa ennaltaehkäisevät toimenpiteet, tapahtumavasteen suunnittelu, nykyaikaiset havaitsemistyökalut ja analyysimenetelmät, jotka muodostavat olennaisen osan organisaatioiden kyberturvallisuusstrategiaa ransomware-hyökkäysten varalta.

3.1 Ehkäiseminen ja ennakointi

Ransomware-hyökkäysten ehkäisy ja ennakointi muodostavat perustan tehokkaalle puolustukselle. Tässä alaluvussa keskitytään käytännön toimenpiteisiin, joiden avulla organisaatiot voivat suojautua ennen hyökkäysten tapahtumista. Tällaisia toimenpiteitä ovat muun muassa riskiarvioinnit, haavoittuvuuksien hallinta, henkilöstön koulutus sekä tapahtumavasteen suunnittelu. Koska hyökkäykset kohdistuvat usein liiketoimintakriittisiin kohteisiin ja voivat aiheuttaa merkittäviä vahinkoja, ajoissa toteutetut ennakoivat toimet ovat keskeinen osa kyberturvallisuusstrategiaa.

3.1.1 Tapahtumavaste-suunnitelma

Bajpai [12] mukaan yleiseen tapahtumavaste-suunnitelmaan kuuluu viisi vaihetta: valmistelu, tunnistus, sisäänpääsyn rajoittaminen, puhdistus ja palautus. Valmisteluvaiheessa kartoitetaan käytettävissä olevat tietotekniset resurssit ja niiden suojaamiseen liittyvät turvatoimet. Tässä vaiheessa arvioidaan myös mahdolliset turvatoimien aukot, jotka voivat altistaa järjestelmät hyökkäyksille. Tunnistusvaiheessa etsitään merkkejä haitallisesta toiminnasta suojatuissa ympäristöissä. Varhainen tunnistus, kuten ransomwaren estäminen tartunnan alkuvaiheessa, on tehokasta, mutta sen onnistuminen riippuu organisaation tietoturvan tasosta. Sisäänpääsyn rajoittamisessa pyritään estämään ransomwaren leviäminen. Tavoitteena on eristää saastuneet järjestelmät nopeasti ja estää tartunnan leviämistä laajemmalle alueelle. Puhdistusvaiheessa pyritään poistamaan kaikki ransomware jäänteet ja tutkimaan tartunnan lähde. Tämä vaihe sisältää digitaalisen rikostutkinnan ja järjestelmän täydellisen puhdistamisen. Viimeisessä vaiheessa, palautuksessa, palautetaan järjestelmät normaalitilaan mahdollisimman nopeasti ja suoritetaan jälkikäteinen arviointi siitä, mitä opittiin hyökkäyksestä ja kuinka turvallisuushenkilöstö voi estää tulevat hyökkäykset.

Ransomware eroaa monin tavoin muista haittaohjelmista, minkä vuoksi yleinen tapahtumavaste-suunnitelma ei välttämättä riitä torjumaan nykyaikaisia hyökkäyksiä. Tämän vuoksi Bajpai [12] ehdottaa erityisesti ransomware-kohtaista tapahtumavaste-suunnitelmaa, jossa tulisi huomioida seuraavat seikat.

Ransomware-hyökkäysten torjunta vaatii syvällistä kryptografian ymmärrystä. On tärkeää selvittää, millaista salausta hyökkäyksessä on käytetty, mikä on avaimen koko ja onko olemassa haavoittuvuuksia, jotka voisivat paljastaa salausavaimen tai mahdollistaa sen palauttamisen ilman, että lunnaita tarvitsee maksaa. Tällainen tekninen analyysi voi olla ratkaisevaa tietojen palauttamisen kannalta.

Toisin kuin monet muut haittaohjelmat, ransomwarea levittävät toimijat — erityisesti Ransomware-as-a-Service (RaaS) -mallissa — pyrkivät julkisesti nimeämään

ja häpäisemään uhrejaan kyberrikollisten foorumeilla ja blogeissa. Tämän vuoksi organisaatioiden on varauduttava siihen, että hyökkäys ei ole pelkästään tekninen, vaan myös maineeseen vaikuttava kriisi, jonka hallintaan tarvitaan huolellisesti suunniteltu ulkoinen viestintästrategia.

Koska ransomware-hyökkäykset kohdistuvat tarkoituksella liiketoiminnan kannalta kriittisiin toimintoihin saadakseen aikaan mahdollisimman suuren painostuksen, on olennaista, että organisaatiot tunnistavat ennakolta ne toiminnot ja resurssit, joiden häiriintyminen aiheuttaisi vakavimmat seuraukset. Tämä ennakkotunnistus on keskeinen osa tehokasta riskienhallintaa ja kyberturvallisuusvalmiutta.

Ransomware-hyökkäysten mittakaavan ja vaikutusten vuoksi monet organisaatiot ovat ryhtyneet ottamaan kybervakuutuksia. Tämän vuoksi ransomwareen varautumisen tulisi sisältää myös vakuutukseen liittyviä strategioita, jotta hyökkäyksen taloudellisia vaikutuksia voidaan hallita ennakoivasti.

Koska ransomware-hyökkäykset ovat usein erittäin kehittyneitä ja vaikeasti torjuttavia — erityisesti RaaS-mallin kasvun myötä — organisaation omat tietoturvatiimit eivät välttämättä kykene reagoimaan riittävästi yksin. Usein tarvitaan ulkopuolisia asiantuntijoita, joilla on osaamista esimerkiksi digitaaliseen forensiikkaan, haittaohjelmien eristämiseen ja hyökkääjien kanssa neuvottelemiseen. Tämä erottaa ransomware-hyökkäykset muista yleisistä kyberuhista, kuten DDoS-hyökkäyksistä, jotka voidaan usein torjua sisäisin toimin.

3.1.2 Ehkäisytekniikoita

Tietoturvapäivitykset

Hyökkääjät hyödyntävät usein käyttöjärjestelmien haavoittuvuuksia ransomwaren levittämiseen. Käyttäjien on tärkeää varmistaa, että kaikki liitetyt laitteet ovat ajantasaisia ja niissä on uusimmat tietoturvapäivitykset asennettuna. Haavoittuvuuksien hyödyntäminen mahdollistaa luvattoman pääsyn järjestelmiin, ransomwaren leviä-

misen ja muiden haitallisten toimintojen toteuttamisen. Tämä korostaa vahvojen tietoturvatoimenpiteiden toteuttamisen, haavoittuvuuksien nopean paikkaamisen ja ajantasaisen tietoturvakäytännön ylläpitämisen tärkeyttä tällaisten hyökkäysten aiheuttamien riskien estämiseksi [13].

Nollaluottamusarkkitehtuuri

Nollaluottamusarkkitehtuuri (Zero Trust Architecture, ZTA) on verkkosuojauksen malli, joka ei luota mihinkään verkkoon, vaikka se olisi sisäinen. Sen perusperiaate on, että käyttäjien ja järjestelmien on aina todistettava henkilöllisyytensä ja käyttöoikeutensa ennen pääsyä järjestelmän resursseihin. Tämä lähestymistapa voi estää ransomware-hyökkäysten leviämisen verkossa tarjoamalla vahvan suojan sivuttaiselle liikkeelle [6].

Sähköpostin tietoturvatoimet

Sähköpostin tietoturvaa voidaan parantaa kouluttamalla työntekijöitä tunnistamaan kalasteluviestejä sekä hyödyntämällä teknisiä ratkaisuja, jotka suodattavat haitallisia liitteitä ja viestejä [14].

Etäyhteyksien poistaminen

Etäyhteyksien poistaminen käytöstä on suositeltavaa, koska nämä protokollat voivat sisältää haavoittuvuuksia, jotka uhkaavat organisaatioiden turvallisuutta. Hallintaliittymien tulisi olla eristettyjä ensisijaisesta verkkoympäristöstä ja niillä tulisi olla omat yhteytensä, jotta organisaatio voi suojautua mahdollisilta hyökkäyksiltä. Mikäli hallintaliittymät joutuvat ransomware-hyökkäyksen kohteeksi, organisaatio voi kärsiä merkittävästä ajanhukasta ja suurista palautuskustannuksista. Jos etäyhteydet ovat tarpeellisia, niiden käyttöä tulisi rajoittaa ja järjestelmänvalvojan pääsyä hallita tiukasti samalla, kun järjestelmät päivitetään säännöllisesti [15].

Työntekijöiden koulutus ja tietoisuuden lisääminen

Verkon käyttäjillä on keskeinen rooli yrityksen suojaamisessa ransomware-hyökkäyksiltä, ja heidän on hallittava ransomware-uhkien tunnistaminen ja torjunta [13]. Työntekijöiden kouluttaminen lisää kyberturvallisuustietoisuutta ja auttaa tunnistamaan mahdollisia uhkia, kuten epäilyttäviä viestejä ja liitteitä, mutta inhimillisten virheiden riskiä ei voida täysin poistaa [14].

Vanhan palomuurin käyttö

Verkon turvallisuutta vahvistamalla voidaan estää luvaton pääsy ja ransomware-hyökkäykset, jotka leviävät muun muassa phishing-hyökkäyksillä. Tämä saavutetaan käyttämällä vahvaa palomuuria, sulkemalla tarpeettomat portit ja prosessit, noudattamalla tiukkoja salasanakäytäntöjä sekä estämällä uusien laitteiden ja tallennusvälineiden automaattinen liittäminen [13].

Pääsynhallinta ja vähimmän oikeuden periaate

Ransomwaren aiheuttamia vahinkoja voidaan pienentää noudattamalla vähimmän oikeuden periaatetta, jossa käyttäjille myönnetään vain heidän työtehtäviensä kannalta välttämättömät oikeudet. Tehokas toteutus edellyttää jatkuvaa pääsynvalvontaa ja uhkien havaitsemista [14].

Verkon segmentointi

Verkon segmentointi estää hyökkäyksen leviämisen organisaation alueelta toiselle. Se on tärkeä osa verkon suunnittelua, sillä se voi pelastaa koko organisaation hyökkäyksen aikana. Lisäksi IT-verkon ja operaatioverkon eriyttäminen voi estää yrityksen toiminnan keskeytymisen hyökkäyksen aikana [15].

Varmuuskopiointi

Tärkeiden tietojen varmuuskopiointi turvalliseen etäpaikkaan ja varmuuskopioiden säännöllinen testaus varmistavat luotettavan palautuksen ilman lunnaiden maksamista [14]. On tärkeää, että varmuuskopion sijainti ei ole yhteydessä pääverkkoon, koska on olemassa ransomwaren muotoja, jotka pystyvät löytämään ja tuhoamaan varmuuskopioidut tiedot [15].

Päätelaitteen tietoturvaratkaisut

Kehittyneet päätelaitteen tietoturvaratkaisut, jotka hyödyntävät koneoppimista ransomwaren torjunnassa, tarjoavat ennakoivaa suojaa, mutta edellyttävät jatkuvia päivityksiä ja voivat aiheuttaa vääriä hälytyksiä [14].

Sallittujen sovellusten lista (Whitelist)

Sallittujen sovellusten listan käyttö estää luvattoman ohjelmiston suorittamisen ja vähentää ransomware-riskin, mutta se voi olla vaikeasti toteutettavissa suurissa ympäristöissä hallinnan monimutkaisuuden vuoksi [14].

3.2 Havaitseminen ja analyysi

Ransomware-hyökkäysten havaitseminen ja analysointi ovat keskeisessä roolissa organisaatioiden kyvyssä reagoida nopeasti ja tehokkaasti. Tässä alaluvussa tarkastellaan, kuinka ransomware-hyökkäyksiä voidaan havaita ja analysoida tehokkaasti, jotta hyökkäykset voidaan estää ennen niiden aiheuttavan merkittävää vahinkoa. Erilaiset havaitsemismenetelmät ja -työkalut ovat tärkeitä, sillä nopea tunnistaminen mahdollistaa ripeän reagoinnin ja hyökkäyksen leviämisen estämisen. Analyysimenetelmien avulla voidaan paitsi arvioida hyökkäyksen luonteen ja vaikutusten laajuutta, myös tunnistaa hyökkäyksen toteutustavat, mikä auttaa organisaatiota kehittämään

puolustusta ja ennaltaehkäisemään vastaavia hyökkäyksiä tulevaisuudessa.

3.2.1 Haittaohjelma-analyysi

Haittaohjelmien havaitsemiseen käytetään useita erilaisia tekniikoita, kuten tiedostojen analysointia erityisillä työkaluilla sekä ohjelmien ominaisuuksien luokittelua haitallisten ja hyvänlaatuisten ohjelmien erottamiseksi. Haittaohjelman analyysi voidaan jakaa kolmeen pääluokkaan: staattiseen, dynaamiseen ja hybridianalyysiin. Staattisessa analyysissä tarkastellaan haittaohjelman rakennetta ilman, että koodia suoritetaan, ja siihen kuuluu muun muassa tiedostojen merkkijonojen ja funktioiden tarkastelua. Dynaaminen analyysi puolestaan seuraa haittaohjelman toimintaa eristetyssä ympäristössä, kuten virtuaalikoneessa, ja tarkastelee sen käyttäytymistä, kuten muistimuutoksia ja verkkoaktiviteetteja. Hybridianalyysi yhdistää sekä staattisen että dynaamisen analyysin, hyödyntäen molempien menetelmien etuja [16].

Staattinen analyysi on nopeampaa, mutta ei sovellu hyvin obfuskoiduille tai polymorfisille haittaohjelmille. Dynaaminen analyysi on tehokkaampaa tuntemattomien uhkien havaitsemisessa, mutta haittaohjelmat voivat joskus piilottaa todellisen käyttäytymisensä analyysitilanteessa, erityisesti suljetuissa ympäristöissä [16].

3.2.2 Havaitseminen koneoppimisella

Perinteiset koneoppimistekniikat

Perinteiset koneoppimistekniikat ovat yleisimmin käytettyjä ransomware-havaitsemisessa niiden toteutuksen helppouden ja tarkkuuden vuoksi. Yleisimmät algoritmit ovat tukivektorikoneet (SVM), päätöspuut ja Naive Bayes. Vähemmän käytettyjä ovat muun muassa logistinen regressio. Perinteinen koneoppiminen edellyttää asiantuntijoiden panosta ominaisuuksien luomisessa ja tietojen huolellisessa merkitsemisessä ennen niiden syöttämistä malliin. Perinteisissä koneoppimismalleissa haasteena on se, että ransomwaren kehittyessä malli vaatii jatkuvia päivityksiä, mikä voi lisätä

hyökkäysriskiä. Lisäksi perinteiset mallit päivitetään usein alusta alkaen, ja niiden on vaikea käsitellä monimutkaisia tietorakenteita ja sekvenssejä [17].

Syväoppimistekniikat

Syväoppimismenetelmät pystyvät käsittelemään raakadataa ja poimimaan tärkeitä piirteitä ilman asiantuntijoiden apua. Tämä koneoppimisen osa-alue on saanut paljon huomiota ja osoittanut hyviä tuloksia erityisesti sekventiaalisten tietojen ja visuaalisen objektitunnistuksen alueilla. Menetelmä perustuu tiedon käsittelyyn useiden kerrosten läpi ja yleiskäyttöisten algoritmien hyödyntämiseen, joiden avulla saadaan abstraktioita edellisten kerrosten tuloksista. Näin syväoppimismallit voivat paljastaa uusia näkemyksiä, joita perinteisillä menetelmillä ei välttämättä huomattaisi. Yleisiä syväoppimisalgoritmeja, kuten pitkän ja lyhyen aikavälin muistiin perustuvia verkkoja (Long Short-Term Memory, LSTM), konvoluutiohermoverkkoja (Convolutional Neural Networks, CNN) sekä autoenkoodereita (Autoencoders), käytetään muun muassa ransomwaren havaitsemiseen. LSTM-verkot ovat erityisen hyödyllisiä, koska ne pystyvät säilyttämään aiemmin hankittua tietoa, mikä on tärkeää ransomwareohjelmien tunnistamisessa. Ne soveltuvat erityisesti sekventiaalisen datan, kuten aikarivien, analysointiin, joita esiintyy usein ransomwaren havaitsemisessa käytetyissä lokitiedostoissa. Haasteena syväoppimistekniikoissa on niiden usein korkea resurssiintensiivisyys ja aikavaativuus. Tämä voi aiheuttaa erityisiä haasteita, erityisesti pyrittäessä reaaliaikaiseen ransomwaren havaitsemiseen [17].

Ensemble-oppimistekniikat

Ensemble-oppimismallit yhdistävät useita heikkoja perusmalleja parantaakseen ennustetarkkuutta. Tämä lähestymistapa vähentää yksittäisten mallien virheitä hyödyntämällä muiden vahvuuksia, mikä johtaa parantuneeseen kokonaispätevyysasteeseen. Ensemble-mallit käsittelevät koneoppimisen yleisiä haasteita, kuten luokkien epäta-

sapainoa, käsitteen siirtymistä ja ylisovittamista. Satunnaismetsä (Random Forest) on yksi laajimmin käytetyistä algoritmeista ransomwaren havaitsemisessa sen toteutuksen yksinkertaisuuden ja korkean tarkkuuden vuoksi. Boosting on toinen usein sovellettu tekniikka, johon kuuluvat algoritmit kuten AdaBoost, Gradient Boosting ja XGBoost. [17].

3.2.3 Havaitsemistyökalut ja tekniikat

Davies ym. [18] tarkastelevat nykyisiä ransomware-hyökkäysten havaitsemistekniikoita, jotka jakautuvat statisiin ja dynaamisiin lähestymistapoihin. Tässä alaluvussa käsitellään näitä tekniikoita ja niiden käyttöä ransomware-hyökkäysten tunnistuksessa. Suurin osa seuraavista työkaluista ja tekniikoista hyödyntää hybridianalyysiä.

2entFox

2entFox on Bayesilaisen uskomusarkkitehtuurin pohjalta kehitetty ransomware-havaitsemistyökalu, joka on suunniteltu erityisesti havaitsemaan sitkeästi selviytyvät ransomware-hyökkäykset Windows-ympäristössä. Työkalun testauksessa on kuitenkin ilmennyt matala havaitsemistarkkuus ja korkea väärien positiivisten osuus.

CryptoDrop

CryptoDrop käyttää Shannonin entropiaa havaitakseen crypto-ransomware-aktiviteettia. Työkalu keskittyy käyttäjädatan muutoksiin ja hyödyntää entropian analysointia tiedostojärjestelmässä. Vaikka se on tehokas tietyissä tilanteissa, se vaatii keskimäärin kymmenen tiedoston muutoksen ennen kuin se tunnistaa haitallisen toiminnan.

EldeRan

EldeRan on kaksivaiheinen järjestelmä, joka valitsee tärkeimmät ominaisuudet ransomware-perheiden tunnistamiseksi. Vaikka sen käyttö on nopeaa, järjestel-

män validointia on kritisoitu, sillä se suoritettiin puhtaasti asennetussa Windows-ympäristössä, jossa ei ollut muita kolmannen osapuolen sovelluksia, mikä teki testauksesta helppoa.

HoneyPot

HoneyPot on tekniikka, jossa houkuttelevat resurssit sijoitetaan kriittisiin paikkoihin tiedostojärjestelmässä, ja niiden muutoksia seurataan haitallisen toiminnan havaitsemiseksi. Koska nämä tiedostot ovat harhautustiedostoja, niitä ei normaalisti käytetä, joten niiden päivitys voi viitata haitalliseen toimintaan. Kuitenkin haittaohjelmat eivät aina reagoi niihin, mikä voi ohittaa puolustuksen. Tekniikka on kuitenkin hyödyllinen erityisesti nollapäivähyökkäysten havaitsemisessa ja on yhdistetty muihin havaitsemistyökaluihin, kuten R-Lockeriin.

PayBreak

PayBreak on työkalu, joka keskeyttää API-kutsut kryptografisiin kirjastoihin ja tunnistaa staattisesti linkitetyt kryptografiset kirjastot. Se kerää salauskohtaisia tietoja ja tallentaa ne turvallisesti "Key Escrow-menetelmällä, mikä mahdollistaa tiedostojen palauttamisen ransomware-hyökkäyksen jälkeen. Työkalu keskittyy vain symmetriseen salaukseen, ja sen toiminta voi estyä obfuskaatiotekniikoilla. PayBreakin suorituskyky on parempi kuin monilla muilla reaaliaikaisilla suojausjärjestelmillä, mutta se vaatii etukäteistietoa käytetyistä kirjastoista ja hookeista, ja kryptografisten tietojen keskitetty tallentaminen voi olla riskialtista.

RAPPER

RAPPER on työkalu, joka käyttää laitteiston suorituskykylaskureita (HPCs) ransomware-hyökkäysten havaitsemiseen. Työkalu tunnistaa poikkeavan järjestelmäkäyttäytymisen analysoimalla järjestelmän ja API-kutsuja. RAPPERin havaitsemistekniikka

perustuu kaksivaiheiseen prosessiin, jossa ensin hyödynnetään tekoälyverkkoa ja sen jälkeen nopeaa Fourier-muunnosta. Tämä lähestymistapa tarjoaa tarkan, nopean ja luotettavan ratkaisun vähäisellä seurantapisteiden määrällä.

Redemption

Redemption on työkalu, joka arvioi prosessien haitallisuutta laskemalla niiden suorittamien toimien perusteella kertynyttä "pahantahtoisuuden pistemäärää". Jos pistemäärä ylittää tietyn rajan, prosessi keskeytetään. Tärkeimpiä tekijöitä pistemäärän nousussa ovat tiedostojen yliviivaaminen, hakemiston kulkeminen ja entropian ero tiedostojen kirjoittamisessa. Työkalu tarjoaa myös edistyksellisen palautustoiminnon.

R-Killer

R-Killer on tunnistustyökalu, joka keskittyy sähköpostiin, sillä se on yleisin ransomware-hyökkäysten tartuntavektori. Työkalu käyttää toistuvaa neuroverkkoa (recurrent neural network) liitteen luokittelemiseksi mahdolliseksi ransomwareksi. Liite analysoidaan staattisesti haitallisten ominaisuuksien tunnistamiseksi, sen dynaamista käyttäytymistä tarkastellaan eristetyssä ympäristössä, ja lisäksi tutkitaan kaikki URL-osoitteet, joihin liitteen binääriohjelma pääsee suoritettaessa.

R-Locker

R-Locker on honeypot-pohjainen järjestelmä, jossa käytetään "honeyfile-käsitettä. Tämä tiedosto houkuttelee ransomware-hyökkäyksiä ja estää niitä hyökkäämästä oikeisiin tiedostoihin. R-Locker on helppo toteuttaa ja on osoittautunut tarkaksi ja vähän resursseja kuluttavaksi, mutta se on testattu vain UNIX-järjestelmissä.

RWGuard

RWGuard hyödyntää kirjoitetun tiedoston entropiaa mahdollisen ransomware-hyökkäyksen havaitsemiseksi. Työkalu yhdistää entropian tarkastelun muihin havaitsemistekijöihin, kuten Random Forest -koneoppimisalgoritmiin, parantaakseen havaitsemistarkkuutta ja vähentääkseen väärien positiivisten osumia.

ShieldFS

ShieldFS käyttää myös entropian mittaamista tiedostojärjestelmässä ja hyödyntää sitä koneoppimisessa ransomware-hyökkäysten havaitsemiseksi. Työkalu tarjoaa mahdollisuuden tiedostojen palauttamiseen, mikäli niitä on muutettu. ShieldFS käyttää Random Forest -algoritmia erottaakseen haitallisen ja hyvänlaisen käyttäytymisen ja voi palauttaa salausavainmateriaalia prosessin muistista.

UShallNotPass

UShallNotPass on työkalu, joka käyttää kryptografisten kirjastojen API-kutsujen väliintuloa estääkseen ransomwarea hyödyntämästä salausominaisuuksia. Sen havaitsemisjärjestelmä koostuu kahdesta osasta: väliintuloprosessista, joka tunnistaa kutsut kryptografisesti turvallisiin pseudosatunnaislukugeneraattoreihin (CSPRNG-API), sekä ohjausprosessista, joka tekee valtuutuspäätöksiä prosesseille. Työkalu hyödyntää dynaamista valkoinen lista -lähestymistapaa valtuutuksen toteuttamiseen ja aiheuttaa vain vähäistä suorituskyvyn heikkenemistä, mikä tekee sen käytöstä käytännöllistä. Myöhemmin tutkijat paransivat työkalun suorituskykyä ja julkaisivat sen päivitetyn version nimeltä NoCry. Lisäksi tekniikkaa kehitettiin edelleen korvaamalla CSPRNG-funktio käyttöjärjestelmässä omalla deterministisellä satunnaislukugeneraattorilla.

UNVEIL

UNVEIL on dynaaminen analyysijärjestelmä, joka mahdollistaa ransomwareen liittyvän käyttäytymisen tutkimisen luomalla keinotekoisen työpöytäympäristön, jossa epäillyt haitalliset binäärit suoritetaan. Järjestelmä seuraa tiedostojärjestelmän muutoksia suorituksen aikana ja hyödyntää muun muassa Shannonin entropian laskentaa ransomware-ohjelmien havaitsemiseksi vertaamalla saman prosessin levyltä lukeman ja levylle kirjoittaman datan määrää.

4 Yhteenveto

Tässä tutkielmassa tarkasteltiin ransomware-hyökkäysten torjuntaa organisaatioissa kolmen keskeisen näkökulman kautta: ehkäisy, ennakointi ja havaitseminen. Kirjallisuuskatsaukseen perustuva tutkimus pyrki vastaamaan kahteen tutkimuskysymykseen, jotka käsittelivät organisaatioiden keinoja suojautua ja reagoida ransomware-uhkiin.

TK1: Millaisia ennakoivia ja ehkäiseviä toimenpiteitä organisaatiot voivat toteuttaa suojautuakseen ransomware-hyökkäyksiltä? Ensimmäisen tutkimuskysymyksen osalta havaittiin, että tehokas suojautuminen edellyttää sekä teknisiä että organisatorisia toimenpiteitä. Ennakoivina keinoina korostuvat tapahtumavasteen laatiminen, kriittisten resurssien tunnistaminen sekä ulkoisen viestinnän suunnittelu mahdollisten mainehaittojen varalta. Teknisistä ehkäisevistä toimenpiteistä keskeisiä ovat säännölliset tietoturvapäivitykset, nollaluottamusarkkitehtuuri, sähköpostiliikenteen suojaus, pääsynhallinta, etäyhteyksien rajoittaminen ja verkon segmentointi. Myös huolellisesti toteutettu, eristetty varmuuskopiointi sekä henkilöstön koulutus ja tietoisuuden lisääminen ovat olennaisia keinoja estää hyökkäysten etenemistä ja vähentää inhimillisten virheiden riskiä.

TK2: Millaisia menetelmiä ja työkaluja on käytettävissä ransomware-hyökkäysten havaitsemiseen ja analysointiin, ja mitä haasteita niihin liittyy? Toiseen tutkimuskysymykseen vastattiin tarkastelemalla erilaisia analyysi- ja tunnistusmenetelmiä. Haittaohjelma-analyysi voidaan toteuttaa staattisesti, dynaamisesti tai näitä yhdistelevällä hybridimallilla, mikä mahdollistaa uhkien tarkastelun eri näkökulmista.

Koneoppimispohjaiset lähestymistavat, kuten luokittelualgoritmit, syväoppimismallit ja ensemble-tekniikat, osoittautuvat lupaaviksi, mutta ne vaativat merkittäviä resursseja ja huolellista suunnittelua esimerkiksi mallien ajantasaisuuden ja väärien hälytysten hallinnan osalta. Työkaluista esiin nousevat muun muassa CryptoDrop, ShieldFS ja R-Locker, jotka hyödyntävät entropia-analyysiä, honeypot-tekniikoita tai API-kutsujen tarkkailua haitallisen toiminnan tunnistamiseksi. Näihin menetelmiin liittyy kuitenkin haasteita, kuten korkea laskentatehon tarve, väärien positiivisten esiintyvyys sekä vaikeus havaita uusia ja muuntautuvia uhkia erityisesti reaaliaikaisessa ympäristössä.

Yhteenvetona voidaan todeta, että ransomware-hyökkäysten torjunta edellyttää monitasoista ja jatkuvasti päivitettävää lähestymistapaa, jossa yhdistyvät teknologiset ratkaisut, strateginen ennakointi ja henkilöstön osaaminen. Organisaatioiden on tärkeää rakentaa resilienssiä paitsi estääkseen hyökkäykset, myös tunnistaakseen ja hallitakseen ne mahdollisimman nopeasti ja tehokkaasti.

Lähdeluettelo

[1] A. Lawall ja P. Beenken, ”A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem”, teoksessa *ACM International Conference Proceeding Series*, Association for Computing Machinery, 5. kesäkuuta 2024, s. 210–216, ISBN: 979-8-4007-1651-5. DOI: 10.1145/3655693.3661321.

[2] H. Oz, A. Aris, A. Levi ja A. S. Uluagac, ”A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions”, *ACM Computing Surveys*, vol. 54, nro 11, 31. tammikuuta 2022, Publisher: Association for Computing Machinery, ISSN: 15577341. DOI: 10.1145/3514229. arXiv: 2102.06249.

[3] S. Mujeye, ”Ransomware: To Pay or Not to Pay? The results of what IT professionals recommend”, teoksessa *ACM International Conference Proceeding Series*, Association for Computing Machinery, 21. tammikuuta 2022, s. 76–81, ISBN: 978-1-4503-9551-9. DOI: 10.1145/3520084.3520096.

[4] N. A. Malik, A. M. Delshadi, M. Ibrar et al., ”Behavior and Characteristics of Ransomware - A Survey”, teoksessa *2nd International Conference on Cyber Resilience, ICCR 2024*, Institute of Electrical ja Electronics Engineers Inc., 2024, ISBN: 979-8-3503-9496-2. DOI: 10.1109/ICCR61006.2024.10532983.

[5] S. Duraibi, C. Kaur ja A. B. Pawar, ”Cyber Extortion Unveiled: The Evolution, Tactics, Challenges, and Future of Ransomware”, teoksessa *Proceedings - 2023 International Conference on Computational Science and Computational Intelli-*

gence, CSCI 2023, Institute of Electrical ja Electronics Engineers Inc., 2023, s. 861–867, ISBN: 979-8-3503-6151-3. DOI: 10.1109/CSCI62032.2023.00144.

[6] C. B. Basha, N. Misra, J. Jayashankari et al., "Understanding and Mitigating Ransomware Threats: Trends, Techniques, and Countermeasures in the Digital Age", teoksessa *International Conference for Technological Engineering and its Applications in Sustainable Development, ICTEASD 2023*, Institute of Electrical ja Electronics Engineers Inc., 2023, s. 383–387, ISBN: 979-8-3503-3647-4. DOI: 10.1109/ICTEASD57136.2023.10585140.

[7] C. Omar, K. Nabil ja M. Benabdellah, "A Systematic Review and Taxonomy of Ransomware Detection Based on Artificial Intelligence Algorithms", teoksessa *2024 3rd International Conference on Embedded Systems and Artificial Intelligence (ESAI)*, IEEE, 19. joulukuuta 2024, s. 1–11, ISBN: 979-8-3315-2205-6. DOI: 10.1109/ESAI62891.2024.10913856. url: https://ieeexplore.ieee.org/document/10913856/.

[8] A. A. M. Ali Alwashali, N. A. A. Rahman ja N. Ismail, "A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack", teoksessa *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, ISSN: 21611343, vol. 2021-December, Institute of Electrical ja Electronics Engineers Inc., 2021, s. 92–96, ISBN: 978-1-6654-0888-2. DOI: 10.1109/DESE54285.2021.9719456.

[9] S. Razaulla, C. Fachkha, C. Markarian et al., "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions", *IEEE Access*, vol. 11, s. 40 698–40 723, 2023, Publisher: Institute of Electrical and Electronics Engineers Inc., ISSN: 21693536. DOI: 10.1109/ACCESS.2023.3268535.

[10] N. Sharma ja R. Shanker, "Analysis of Ransomware Attack and Their Countermeasures: A Review", teoksessa *Proceedings of the International Conference on*

Electronics and Renewable Systems, ICEARS 2022, Institute of Electrical ja Electronics Engineers Inc., 2022, s. 1877–1883, ISBN: 978-1-6654-8425-1. DOI: 10.1109/ICEARS53579.2022.9751949.

[11] R. Moussaileb, N. Cuppens, J. L. Lanet ja H. L. Bouder, "A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms: Case Closed?", *ACM Computing Surveys*, vol. 54, nro 6, 31. tammikuuta 2021, Publisher: Association for Computing Machinery, ISSN: 15577341. DOI: 10.1145/3453153.

[12] P. Bajpai ja R. Enbody, "Know Thy Ransomware Response: A Detailed Framework for Devising Effective Ransomware Response Strategies", *Digital Threats: Research and Practice*, vol. 4, nro 4, 20. lokakuuta 2023, Publisher: Association for Computing Machinery, ISSN: 25765337. DOI: 10.1145/3606022.

[13] G. F. M. Karo-Karo, M. S. A. Harumnanda ja C. Lim, "Investigating Multiple Malware as a Service (MaaS): Analysis and Prevention Techniques", teoksessa *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, Institute of Electrical ja Electronics Engineers Inc., 2023, s. 270–274, ISBN: 979-8-3503-3943-7. DOI: 10.1109/ICoCICs58778.2023.10277515.

[14] A. K. Upadhyay, P. Dubey, S. Gandhi ja S. Jain, "Ransomware Detection And Data Recovery", teoksessa *2024 International Conference on Electrical, Electronics and Computing Technologies, ICEECT 2024*, Institute of Electrical ja Electronics Engineers Inc., 2024, ISBN: 979-8-3503-7809-2. DOI: 10.1109/ICEECT61758.2024.10738908.

[15] Y. K. Bin Mohamed Yunus ja S. Bin Ngah, "Ransomware: Stages, detection and evasion", teoksessa *Proceedings - 2021 International Conference on Software Engineering and Computer Systems and 4th International Conference on Com-*

putational Science and Information Management, ICSECS-ICOCSIM 2021, Institute of Electrical ja Electronics Engineers Inc., 1. elokuuta 2021, s. 227–231, ISBN: 978-1-6654-1407-4. DOI: 10.1109/ICSECS52883.2021.00048.

[16] F. Aldauiji, O. Batarfi ja M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art", *IEEE Access*, vol. 10, s. 61 695–61 706, 2022, Publisher: Institute of Electrical and Electronics Engineers Inc., ISSN: 21693536. DOI: 10.1109/ACCESS.2022.3181278.

[17] J. Ispahany, M. R. Islam, M. Z. Islam ja M. A. Khan, "Ransomware Detection Using Machine Learning: A Review, Research Limitations and Future Directions", *IEEE Access*, vol. 12, s. 68 785–68 813, 2024, Publisher: Institute of Electrical and Electronics Engineers Inc., ISSN: 21693536. DOI: 10.1109/ACCESS.2024.3397921.

[18] S. R. Davies, R. Macfarlane ja W. J. Buchanan, "Review of Current Ransomware Detection Techniques", teoksessa *7th International Conference on Engineering and Emerging Technologies, ICEET 2021*, Institute of Electrical ja Electronics Engineers Inc., 2021, ISBN: 978-1-6654-2714-2. DOI: 10.1109/ICEET53442.2021.9659643.