Veikko Mikael Markkanen

Kiristyshaittaohjelmahyökkäysten kohteiden valikoituminen

Tietotekniikan kandidaatintutkielma

22. tammikuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Veikko Mikael Markkanen

Yhteystiedot: markkvmx@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Kiristyshaittaohjelmahyökkäysten kohteiden valikoituminen

Title in English: Targeting of ransomware attacks

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 37+0

Tiivistelmä: Kiristyshaittaohjelmahyökkäysten muodostama rasite kasvaa. Hyökkäyksiä ohjaavien voimien ymmärtäminen on tullut ratkaisevan tärkeäksi tehokkaampia torjuntamekanismeja rakennettaessa. Kiristyshaittaohjelmahyökkäysten kehitystä ja luonnetta käsittelevä akateeminen tutkimus osoittaa kiristysrikollisuutta harjoittavien toimijoiden motiivit pääosin taloudellisiksi, mutta myös ideologiset motiivit ovat yleistyneet. Hyökkäykset vastaavasti kehittyvät kohdennetuimmiksi, jolloin kohteesta saatavan tiedon ja käyttäytymisen vaikutus kohdentumisriskiin kasvaa. Haittaohjelmien tekninen toteutus, liiketoimintamalli, sekä hyökkäyspinta-ala ovat siten jatkuvassa muutoksessa, korostaen kykyä ennakoida hyökkäyksiä. Haasteeksi jää kuinka aktiivisesti yritykset ja valtiolliset toimijat tähän kykenevät reagoimaan. Tämä lisää ajankohtaisen tutkimuksen tarvetta ja tekee riittävästä resursoinnista entistä tärkeämpää.

Avainsanat: digitalisaatio, hybridivaikuttaminen, kiristyshaittaohjelmat, kyberrikollisuus, kyberriski, kyberturvallisuus, verkkorikollisuus

Abstract: Ransomware attacks have become more and more frequent and severe. Investigating the forces driving these attacks has become crucial in order to create more effective preventative measures. Academic literature addressing the evolution and nature of ransomware attacks shows that majority of the threats are financially motivated but ideological motives are also becoming more common. Correspondingly, the attacks are becoming more targeted,

which implies that the role, behaviour and information footprint of an organisation contributes to the risk of becoming a target for a ransomware attack. The technical implementation of the malware, the ransomware business model, and the area of attack are constantly changing, challenging the ability of companies and government actors to anticipate attacks. This increases the need for up-to-date research and makes adequate resourcing of preventive measures all the more important.

Keywords: cyber crime, cyber risk, cyber security, ransomware, hybrid influence, digitisation

Termiluettelo

Advanced persistent threat (APT)	Suomeksi ”kehittynyt jatkuva uhka”, on tarkkaan suunniteltu, salassa toteutettu kyberhyökkäys pitkäjänteisesti maalinnettua tietoverkkoa vastaan, jossa hyökkääjä hankkii ja ylläpitää laitonta jalansijaa kohdejärjestelmässä.
Big Game Hunting (BGH)	Big game hunting operaatiossa rikolliset kohdistavat hyökkäyksen mahdollisimman suureen organisaatioon, sille mahdollisimman arvokkaaseen dataan tai omaisuuteen. Kohteet operaatiolle valikoituvat mm. kohdeorganisaation markkina-arvon ja seisonta-ajan kriittisyyden myötä.
Encryption technology	Suomeksi ”salaustekniikka”, tarkoittaa digitaalisen tiedon salaamista matemaattisin menetelmin. Salausprosessin läpikäynyttä tietoa ei saada palautettua ilman tarkkaa matemaattista avainta (koodia), jolla salaus voidaan purkaa.
Hajautetut kryptovaluutat	Virtuaalivaluuttoja, joiden vaihto tapahtuu suoraan käyttäjältä toiselle ilman välikäsiä. Hajautettujen kryptovaluuttojen käyttö on suhteellisen salattua, eikä niitä säätele mikään entiteetti.
Haittaohjelma	Tietokoneohjelma, joka tarkoituksellisesti aiheuttaa tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa.
Hybridivaikuttaminen	Poliittisesti motivoitunut suunnitelmallinen toiminta, jolla pyritään saavuttamaan omat tavoitteet erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen.
Kohdistamaton hyökkäys	Uhkatyyppi, jossa hyökkääjä haluaa saavuttaa samalla kertaa lukuisia potentiaalisia uhreja yhden valikoidun kohteen sijaan. Hyökkääjät käyttävät usein automaattisia ja yleisesti saatavilla olevia hyökkäysmetodeja. Kohdistamaton hyökkäys voi muuttua kohdistetuksi hyökkääjän toteuttaessa suoria toimenpiteitä tarkempaa kohdetta vastaan.
Kohdistettu hyökkäys	Uhkatyyppi, jossa tunnistamattomat uhkatekijät pyrkivät ak-

	tiivisesti murtamaan kohde-entiteetin infrastruktuurin. Hyökkäykset ovat usein yksilöllisesti suunniteltuja. Kohdistettuja hyökkäyksiä toteuttavat toimijat omaavat riittävästi erikoistumista sekä resursseja toteuttaa hyökkäyksiä pitkällä aikajaksolla.
Liiketoimintatiedon hallinta	Eng. business intelligence. Liiketoimintatiedon hallinta on systemaattista yrityksen suorittamaa liike-elämän tietojen hankintaa, tallennusta ja analysointia.
Ransomware-as-a-Service (RaaS)	Suomeksi ”kiristyshaittaohjelmat palveluna” on kiristyshaittaohjelmien ekosysteemissä syntynyt liiketoimintamalli, jossa valmiiksi rakennettuja kiristyshaittaohjelmahyökkäysten toteuttamiseen vaadittavia työkaluja myydään tai vuokrataan rikollisten kesken.
Toimijaprofiili	Eng. Organizational profile. Toimijaprofiili on viitekehys, jonka avulla havainnollistetaan toimintaympäristöä muokkaavia ja tehtäviin liiketoimintapäätöksiin vaikuttavia sisäisiä ja ulkoisia tekijöitä.
Verkon segmentaatio	Verkon segmentaatiolla tarkoitetaan prosessia, jossa arkaluontoista informaatiota sisältävät verkot erotetaan muista verkoista. Segmentaation kautta voidaan keskittää tietoturvatoimenpiteet niihin verkon osiin, joissa tarve on suurin.
Vertaisverkko (P2P)	Verkko, jossa ei ole kiinteitä palvelimia ja asiakkaita, vaan jokainen verkkoon kytketty taho toimii sekä palvelimena että asiakkaana verkon muille jäsenille. Salatuissa vertaisverkoissa käyttäjien tiedot salataan niin, etteivät kyseisen verkon muut asiakkaat voi nähdä kuka käyttäjä on. Myös heidän tiedostonsa salataan niin, ettei kukaan voi nähdä suoraan, mitä toisella käyttäjällä on jaettavana.

Taulukot

Sisällys

1 Johdanto

Internet on luonut ekosysteemin, joka tukee haittaohjelmien kehitystä, jakoa ja rahoitusmekanismeja ennennäkemättömällä tavalla. Tässä ekosysteemissä kiristyshaittaohjelmat ovat nousseet verkkorikollisuuden keulakuvaksi. Hyökkäystyyppi kykenee hyväksikäyttämään digitaalisen toimintaympäristön haavoittuvuuksia poikkeuksellisen tehokkaasti eikä kehityksen ennusteta laantuvan.

Kiristyshaittaohjelmien lisääntymisen myötä merkittäviä resursseja on kulutettu hyökkäystyypin analyysiin ja torjuntakeinojen määrittelyyn. Hyökkäysten rajoittaminen on kuitenkin muodostunut ongelmalliseksi. Organisaatiot eivät tunnista kiristyshaittaohjelmien muodostamaa uhkaa. Puutteellisen tilannekuvan johdosta kyberturvallisuusinvestointien toteuttaminen tapahtuu suhteuttamatta realistisiin toimijaprofiileihin, mikä johtaa turvallisuuskulttuurin tehottomuuteen ja hyökkäysten menestykseen.

Tämä tutkimus lähestyy ongelmaa tarkastelemalla todennäköistä kiristyshaittaohjelmahyökkäyksen kohdetta hyökkääjien motiivien, toimintamallien ja toimintaympäristön riskitekijöiden kautta.

Tutkimusaiheena kohteiden valikoituminen on tuore, eikä tähän keskittyvää akateemista tutkimusta juurikaan ole. Tästä johtuen työssä käsitellään kattavasti hyökkäystyypin ympärille rakennettua tutkimusmateriaalia. Erityisen merkittäviksi lähteiksi osoittautuivat Atapour-Abarghouei, Bonner ja McGough (2019), Al-rimy, Maarof ja Shaid (2018), O'Kane, Sezer ja Carlin (2018) ja Hernandez-Castro, Cartwright ja Stepanova (2017) tutkimukset kiristyshaittaohjelmien kehityksestä sekä luonteesta.

Tuloksena saavutettu konkreettinen käsitys toimintaympäristöstä ja hyökkäyksiä ohjaavista voimista täydentää aiempaa teknispohjaista ymmärrystä haittaohjelmista ja vaikuttaa täten organisaation kyberturvallisuuskulttuuriin, sekä kykyyn toimeenpanna turvallisuusyhteisön suosituksia.

Tutkielma koostuu johdannosta, kolmesta sisältöluvusta ja yhteenvedosta. Luvussa 2 rakennetaan työn tausta käsittelemällä internetin ja rikollisuuden suhdetta sekä kiristyshaittaohjel-

mia tämän ekosysteemin tuloksena. Luvussa 3 muodostetaan uhkakuva analysoimalla kiristyshaittaohjelmahyökkääjien motiiveja ja toimintamalleja. Luvussa 4 tarkastellaan varsinaista riskiä joutua hyökkäyksen kohteeksi ja selvitetään toteutuneiden hyökkäysten avulla, mikä tekee kiristyshaittaohjelmahyökkäyksen kohteesta uhrin. Lopuksi vedetään yhteen keskeiset kiristyshaittaohjelmahyökkäysten kohdentumisajurit.

2 Internet ja kiristyshaittaohjelmat

Naughton (2016) mukaan alun perin suljettuun ympäristöön tarkoitettuna järjestelmänä internettiä ei rakennettu kyberturvalliseksi. Internetin pohjimmainen rakenne perustuu edelleen tietoliikennettä tukeviin kommunikaatioprotokolliin. Nämä protokollat tarjoavat niin haitallisille, kuin legitiimeille ohjelmille tasa-arvoisen alustan levitä (O'Kane, Sezer ja Carlin 2018). Internetin luontaisen käsitteen turvallisuudesta voidaankin nähdä perustuvan luottamukseen tiedon lähettäjän ja vastaanottajan välillä.

Nykyään liki 5 miljardin aktiivisen käyttäjän ekosysteemissä, Zero Trust periaatetta seurailen (Køien 2021), tätä luottamusta ei ole olemassa. Sen sijaan valtaosan verkkopalveluiden käyttäjistä omatessa vähän tai ei lainkaan tietoa järjestelmän toiminnasta, Armstrong (2003) kirjoittaa kulutuskäytön korreloivan suoraan rikollisen toiminnan esiintymiseen.

2.1 Internetin ja rikollisuuden suhde

Havainnollistaaksemme kiristyshaittaohjelmien muodostaman uhan laajuutta, käsitellään ensin internetin ja rikollisuuden suhdetta Wall (2001) jaon mukaan kolmesta näkökulmasta.

Kommunikaatio: Internet tarjoaa ainutlaatuisen alustan tiedon välitykselle erottelematta sen laillista alkuperää. Perinteisen rikollisuuden fasilitoinnin rinnalla verkkorikollisuus kukoistaa jaettujen haavoittuvuuksien, palveluiden ja innovaation ohella (Stalans ja Finn 2016). O'Kane, Sezer ja Carlin (2018) mukaan kyberturvallisuusyhteisön työ rajoittaa rikollisuutta on osa samaa ekosysteemiä. Tieto uusista puolustusmekanismeista vuotaa tehokkaasti niin lailliseen, kuin laittomaan käyttöön, mahdollistaen verkkorikollisuuden tyypeille nopean sopeutumisen uusiin olosuhteisiin.

Rakenne: Internetin rajaton rakenne tarjoaa mahdollisuuksia rikollisille aktiviteeteille valtioiden lakien toimivallan ulkopuolelta. Viranomaistoiminnan näkökulmasta Armstrong (2003) kirjoittaa internetin esittävän 2000-luvun ensimmäisen vuosisadan kokonaisvaltaisimman haasteen lainvoimalle. Verkko on luonteeltaan rajaton, anonyymi ja tarjoaa lukemattomia työkaluja rikollisiin aktiviteetteihin. Hyökkäykset voivat tapahtua mistä, mihin ja milloin ta-

hansa. Tästä huolimatta globaali toimintaympäristö ei ole mahdollistanut internetille yhteistä hallintoa tai normistoa (Stalans ja Finn 2016). Tämä on johtanut pirstaleisiin käytäntöihin ja kerroksiin maiden välillä. Säätelyn puutteen myötä merkittävä osa verkkorikollisista toimii maista käsin, joissa viranomaiset katsovat hyökkäyksiä läpi sormien, kasvattaen poliittista jännitettä ja kiihdyttäen keskustelua internetin segmentaatiosta (G7 Summit 2021).

Toimintaympäristö: Viimeisenä Wall (2001) nostaa internetin virtuaalisen ulottuvuuden vaikutuksen rikollisuuden kehitykseen. Uusi toimintaympäristö on luonut uusia yhteiskuntaa mullistavia keksintöjä, mahdollistanut uutta teknologiaa, lukuisia uusia palveluita, haavoittuvuuksia ja tätä kautta uusia rikoksen muotoja. Yhteiskunnan pääoman siirtyminen verkkoon toi kaikki toimijat samaan ekosysteemiin (O'Kane, Sezer ja Carlin 2018; Al-rimy, Maarof ja Shaid 2018). Minchev (2016) tiivistää tilanteen ongelmallisuuden toteamalla eron verkon toimintaan perehtyneiden asiantuntijoiden ja kuluttajien välillä olevan lähtökohtaisesti liian suuri. Ekosysteemissä, jossa kuka tahansa voi olla kohde kenelle tahansa, puutteellinen tietämys laitteiden toiminnasta ja turvallisuuskäytänteistä muodostuu kriittiseksi.

2.2 Kiristyshaittaohjelmien kehitys ekosysteemin mahdollistamana

Kiristyshaittaohjelmat kuuluvat haittaohjelmakategoriaan, jossa kohdekäyttäjän tiedostot ja/tai liitännäiset resurssit tehdään käyttökelvottomiksi. Vastineeksi tilanteen palauttamisesta kategorian ohjelmat kehottavat käyttäjää maksamaan lunnaat, yleensä suhteessa menetetyn toiminnallisuuden arvoon. Kohdekäyttäjän pelko arvokkaan tiedon hallinnan menettämisestä sekä avainresurssien lukittuminen tukee lunnaiden maksamista. Toisin kuin muissa haittaohjelmissa, kiristyshaittaohjelmista juontavat seuraukset ovat liki poikkeuksetta peruuttamattomia (Cybersecurity & Infrastructure Security Agency 2020).

Internetin muodostama ekosysteemi on tarjonnut hedelmällisen kasvualustan niin kiristyshaittaohjelmille kuin haittaohjelmien yleiselle kehitykselle (O'Kane, Sezer ja Carlin 2018). Tässä ekosysteemissä nopeinta kasvua nähdään kuitenkin kiristyshaittaohjelmien osalta. Hyökkäystyyppi herätti laajan akateemisen mielenkiinnon 2015 jolloin lukuisat kiristyshaittaohjelmien toimintamallia rajoittaneet ongelmat olivat ratkenneet teknologisen kehityksen sivuvaikutuksena. Al-rimy, Maarof ja Shaid (2018) kartoittavat näistä merkittävimpiä. Heidän

mukaansa, aiemmin tietokoneiden ja internetpalveluiden huono saatavuus, kehittymätön salausteknologia (eng. encryption technology) sekä turvattomat maksumenetelmät eivät pitkään tarjonneet hyökkäystyypille mahdollisuutta kehittyä. Kun nämä fasiliteetit tulivat saataville, kiristyshaittaohjelmahyökkäysten maisemakuva muuttui radikaalisti:

- **Salausteknologia:** Salaustekniikoiden, kuten symmetrisen avaimen, epäsymmetrisen avaimen ja avaimettomien primitiivien ilmaantumisen myötä kiristyshaittaohjelmien heikko teho jäi historiaan. Uusien tekniikoiden leviäminen on muodostanut verkkorikollisille monia vaihtoehtoja toteuttaa hyökkäyksiään kehittämällä kestäviä ja rikkoutumattomia kiristyshaittaohjelmia (Symantec 2016). Salausteknologian kehityksen myötä lunnaiden maksu on usein muodostunut halvimmaksi keinoksi selviytyä hyökkäyksistä. Aiemmin helposti korjattavissa ollut ongelma, muodostui alun perin turvallisuustarkoitukseen kehitettyjen salaustekniikoiden myötä peruuttamattomaksi vahingoksi (O'Kane, Sezer ja Carlin 2018).
- **Jäljittämättömät maksumenetelmät:** Anonyymien vertaisverkkojen ja hajautettujen kryptovaluuttojen, kuten Bitcoinin ilmaantuminen mahdollisti laajojenkin kiristyshaittaohjelmahyökkäysten toteuttamisen ja lunnaiden vaatimisen ilman merkittävää huolta viranomaisten väliintulosta (Al-rimy, Maarof ja Shaid 2018). Tulos näkyy jatkuvana uutisvirtana laajoista kiristyshaittaohjelmahyökkäyksistä sekä alati kasvavista lunnasvaatimuksista (Palo Alto Networks 2021b).
- **Markkinat:** Menestyksekkään hyökkäystyypin maineen karttuessa, rikollinen kiinnostus kiristyshaittaohjelmia kohtaan on kasvanut sen rinnalla. Kehitys on johtanut markkinoiden syntyyn kiristyshaittaohjelmien ympärille. Ransomware as a Service (RaaS) malli tarjoaa vähemmän teknisille rikollisille väylän helppoon tuottoon, kun taas kiristyshaittaohjelmiin erikoistuneet toimijat ovat laskeneet operatiivista riskiään entisestään rakentamalla ja vuokraamalla työkaluja sekä palvelujaan (Paganini 2015). RaaS-malli rinnastuu suoraan kiristyshaittaohjelmien laajaan hyökkäyspinta-alaan (Meland, Bayoumy ja Sindre 2020).

Havainnollistaakseen hyökkäystyypin muodostamaa uhkaa, Cybersecurity Ventures toteutti vuonna 2015 arvion kiristyshaittaohjelmista juontuvien vahinkojen globaaleista kustannuksista. Tämä arvio ylsi 325 miljoonaan dollariin. Kuusi vuotta myöhemmin 2021 ajankohtai-

nen arvio on 20 miljardia dollaria nostaen kustannukset 57 kertaisiksi (Cybersecurity Ventures 2021). Yksittäisen organisaation näkökulmasta tilanne ei ole parempi. Kyberturvallisuusyritys Sophos arvioi keskimääräisen kiristyshaittaohjelmahyökkäyksen muodostavan kohdeorganisaatiolle 1.85 miljoonan dollarin tappiot (Sophos 2021). Hyökkäysten ilmetessä arvioidusti joka 11 sekunti sekä kybervakuutusten korvaushakemusten kasvaessa yli 100 prosentin vuositahtia (Richardson, North ja Garofalo 2021), lukemat kuvaavat kiristyshaittaohjelmien muodostumista yhdeksi 2000-luvun merkittävimmistä kyberuhista.

3 Kiristyshaittaohjelmahyökkääjät - motiivit ja toimintatavat

Organisaatioiden suojaamiseksi kiristyshaittaohjelmahyökkäyksiltä tarvitaan uusia lähestymistapoja hyökkäysten havaitsemisen lisäksi myös niiden ennakointiin ja vahingon lähtökohtaiseen estämiseen (Atapour-Abarghouei, Bonner ja McGough 2019). Kokonaisvaltaista ymmärrystä kiristyshaittaohjelmahyökkäysten luonteeseen tarvitaan puolustusratkaisujen kehittämiseksi. Täten tutkimus hyökkäysten motiiveihin on muodostunut tärkeäksi. Motiivit säteilevät rikollisten toimintamalleihin ja lopulta vaikuttavat kiristyshaittaohjelmahyökkäysten kohteiden valikoitumiseen (Al-rimy, Maarof ja Shaid 2018).

Luvussa kiristyshaittaohjelmien taloudelliseen tuottoon tähtäävän perusluonteen (O'Kane, Sezer ja Carlin 2018) sekä hyökkäystyyppiä ympäröivän poliittisen kehyksen johdosta (Sanger ja Perlroth 2020), motiivien katselmointi toteutetaan esitetyistä näkökulmista.

3.1 Taloudellinen motivaatio

Hernandez-Castro, Cartwright ja Stepanova (2017) määrittelevät kiristyshaittaohjelmahyökkääjän oletusarvoiseksi tavoitteeksi tuoton maksimoinnin haittaohjelmin tartutetuista laitteista. Richardson ja North (2017) mukaan tämä pyrkimys korkeampaan tuottoon on ohjannut kiristyshaittaohjelmien kehityskaarta aina ensimmäisestä levykkein välitetystä PC-Cyborg kiristyshaittaohjelmasta 2020-luvun menestyväksi liiketoiminnaksi. Pyrkimystä korkeampaan tuottoon käsitellään myös Al-rimy, Maarof ja Shaid (2018) koosteessa kiristyshaittaohjelmiin keskittyvästä akateemisesta tutkimusmateriaalista. Koosteessa tuoton tavoittelu jaetaan pääosin liiketoiminnan kehittämiseen ja sen ylläpitoon. Kappaleessa taloudellisia motiiveja lähestytään samasta näkökulmasta, sillä mainittujen voidaan nähdä toimivan keskeisinä vektoreina hyökkääjien yleisiin toimintamalleihin.

Kyberturvallisuusyritys Crwodstriken (2020) raportin mukaan kiristyshaittaohjelmat esiintyvät yli 80 prosentissa taloudellisesti motivoituneista hyökkäyksistä.

Tehokkaampaa liiketoimintaa

Kiristyshaittaohjelmien liiketoimintamallin perusta on vahingon ja lunnaiden suhde, Hernandez-Castro, Cartwright ja Stepanova (2017) kirjoittavat. Heidän mukaansa lunnasvaatimuksen täytyy vaikuttaa helpoimmalta tavalta palautua kiristyshaittaohjelmahyökkäyksestä tai operaatio on merkityksetön. Rikolliset kuluttavat suhteen painottamiseksi kohti suurempaa maksupotentiaalia merkittävästi resursseja. Organisaatioiden muodostuminen hyökkäysten kohteeksi yksittäisten kuluttajien sijaan on seurausta tästä kehityksestä.

Merkittävä kohde resursseille on haittaohjelmien teho. Kiristyshaittaohjelmat ovat muodostuneet sukupolvesta toiseen kyvykkäämmiksi nopeampaan ja laajempaan järjestelmien murtamiseen sekä tiedostojen salaamiseen. O'Kane, Sezer ja Carlin (2018) mukaan yli 60 kiristyshaittaohjelmaperheen läsnä ollessa turvallisuusinvestointien kiertäminen haittaohjelmien eri variantein mahdollistaa kasvavan yhteiskunnallisen rasitteen. 2021 ensimmäisessä neljänneksessä aktiivisia perheitä havaittiin Palo Alto Networks (2021a) mukaan 114. O'Kanen ym. johtopäätöstä sivuten, havaitaan varianttien kehityksen ja ylläpidon olevan edelleen aktiivista toimintaa, ennakoiden hyökkäysten yhä laajempaa tuhovaikutusta.

Kehitystä havaitaan myös kiristyshaittaohjelmien psykologisesta näkökulmasta. Tehokkaan hyökkäyksen täytyy vakuuttaa uhri haittaohjelman muodostamasta rasitteesta ja lunnaista luotettavana keinona palautua tilanteesta (Krebs 2016). Merkittäviksi tekijöiksi psykologisen vaikutuksen kasvattamiselle ovat muodostuneet kiristyksen kerrokset. Arvokasta tietoa ei enää pelkästään lukita, vaan se pyritään varastamaan ja mahdollisesti myymään riskeeraten kohteen toimintakyvyn niin teknisestä, kuin sosiaalisesta näkökulmasta (Cybersecurity & Infrastructure Security Agency 2020). Vastapainoksi kiristyshaittaohjelmien muodostamalle rasitteelle hyökkääjät ovat kehittäneet kommunikaatiota kohteiden kanssa ja ovat usein valmiita neuvottelemaan tilanteesta ja jopa lunnaiden hinnasta (Hernandez-Castro, Cartwright ja Stepanova 2017).

Vahinko-lunnas -suhteen rinnalla Al-rimy, Maarof ja Shaid (2018) käsittelevät tarkemmin kohteiden hakua. Heidän mukaansa riittävän tarjonnan mahdollistama kohteiden testaaminen suhteessa piilevään tuottoon on muodostunut merkittäväksi elementiksi kiristyshaittaohjelmien ekosysteemissä. Näkyvät trendit, kuten hyökkäysten kohdistaminen palveluntarjoa-

jiin ja elintarvikealalle, ovat seurausta rikollisten työstä löytää uusia ja tuottavia kohteita. Ryan (2021) lähestyy aihetta eri näkökulmasta. Hän kirjoittaa viranomais- ja turvallisuusyhteisön pyrkimyksen vastata haasteeseen asettavan rikolliset paineistettuun tilanteeseen säilyä päivitysprosessin edellä. Molempien näkökulmien voidaan nähdä pitävän paikkansa, joten kohteiden haku liitetään niin liiketoiminnan kehittämiseen kuin sen ylläpitoon.

Meland, Bayoumy ja Sindre (2020) puolestaan kirjoittavat suhteellisen viimeaikaisen RaaS-palveluiden yleistymisen tuoneen kiristyshaittaohjelmat huomattavasti laajemmille markkinoille. Sama havaitaan kasvaneen kiristyshaittaohjelmatyökalujen tarjonnan myötä (Al-rimy, Maarof ja Shaid 2018). Ryan (2021) rinnastaa ilmiön tarkemmin rikollisten motiiveihin. Hän kirjoittaa hyökkäystyypin kaupallistumisen mahdollistaneen teknisesti kyvykkäille rikollisille tehokkaampaa liiketoimintaa vuokraamalla ja rakentamalla haittaohjelmia myyntiin kohtuullisen pienellä riskillä. Kiristyshaittaohjelmista kiinnostuneille rikollisille sen sijaan palvelut tarjoavat väylän muuten saavuttamattomiin tuottoihin. Hyökkäysteknologian käyttökynnyksen laskiessa, kasvavan määrän ennestään tuntemattomia hyökkääjiä voidaan havaita heikentävän hyökkäysten ennakoitavuutta.

Kaupallistuminen ja laajan hyökkäyspinta-alan ylläpito juontavat O'Kane, Sezer ja Carlin (2018) mukaan pitkälti hyökkäystyypin automatisaatiosta. Kiristyshaittaohjelmien automatisointi mahdollistaa käyttäjän roolin vähentämisen hyökkäysprosessissa. Manuaalisen työn poistaminen hyökkäyksistä pienentää kiinnijäämisen riskiä sekä mahdollistaa hyökkäysten kustannustehokkaamman toteutuksen. Automatisaation myötä riski generoidulle kiristyshaittaohjelmahyökkäykselle kasvaa jokaisessa verkkoon liittyneessä organisaatiossa.

Kiristyshaittaohjelmia laukaisevien ja erityisesti palveluja hyödyntävien toimijoiden motivaatiot rinnastetaan pääosin suoraan taloudelliseen tuottoon, mutta työkalujen potentiaalia on sivuttu myös mm. aktivismin, markkinoiden manipulaation, sabotaasin ja terrorismin näkökulmista (Greenberg 2018; Ransomware Task Force 2021; Ryan 2021). Kyseiset esimerkit ovat hyökkäystyypin näkökulmasta harvinaisia eikä kirjallisuuskatsauksen kannalta tutkimusmateriaalia ole riittävästi. Epäsuoraan tuottoon tai aatteelliseen vaikutukseen tähtäävien hyökkäysten mahdollisesti yleistyessä, aihetta on syytä käsitellä lähitulevaisuudessa tarkemmin.

Toiminnan jatkuvuus

Kiristyshaittaohjelmien olemassaolo perustuu vaihtokauppaan. Rikollisille toiminnan jatkuvuus edellyttää hyökkäystyypin yleisen maineen ja erityisesti oman organisaation neuvotteluvalttien priorisointia kaikessa toiminnassa Hernandez-Castro, Cartwright ja Stepanova (2017) kirjoittavat. Tarve säilyä varteenotettavana toimijana johtaa rikollisten itse määrittelemien rajojen ja kohteiden kunnioittamiseen. Cartwright (2019) mukaan kiristyshaittaohjelmahyökkääjien on pakko nähdä vaivaa maineensa yksilöimiseen, sillä toimialan kasvottomuus johtaa tilanteeseen, jossa yksi näkyvä huijaus (tiedostojen palauttamatta jättäminen lunnasta vastaan) vaikuttaa luottamukseen kaikkialla. Esimerkki tästä nähtiin vuonna 2016, kun Kansas Heart sairaalaa kiristänyt rikollisjengi vaati uusia lunnaita ensimmäisten jälkeen toimintakyvyn palauttamiseksi (Trend Micro 2016). Uusia lunnaita ei maksettu ja esimerkillä oli vaikutusta lunnasvaatimusten suosioon kriisinhallinnassa (Cartwright ja Cartwright 2019).

Uutena kehityksenä viranomaistoiminnan vaikutus kiristyshaittaohjelmien ekosysteemiin on kasvanut merkittävästi 20-luvulla. Elektronisten valuuttojen jäljitys on kehittynyt, samoin rikollisten tunnistaminen. Viranomaisten resurssien ollessa rajalliset, valtaosa huomiosta kohdistuu luonnollisesti laajoja seurannaisvaikutuksia omanneisiin hyökkäyksiin. Richardson, North ja Garofalo (2021) kirjoittavat erityisesti jengien tarpeesta muuttaa toimintatapojaan. Tuotot kattavat yhä harvemmin korkean profiilin muodostamaa riskiä rikolliselle toiminnalle. Tällä on merkitystä kohteiden valikoitumiselle, sillä näyttävien hyökkäysten houkuttavuuden laskiessa, matalan profiilin organisaatioiden riski vastaavasti nousee. Kehityksen on osaltaan ennustettu korostavan automatisoitujen hyökkäysten ja RaaS-mallin roolia kiristyshaittaohjelmien evoluutiossa (O'Kane, Sezer ja Carlin 2018).

Jatkuva kilpailu viranomaisten ja turvallisuusyhteisön kanssa nostaa hyökkäysten hintaa. Uusien menetelmien rakentaminen ja testaaminen vaatii merkittävästi resursseja ja aikaa, joita rikollisorganisaatiot omaavat rajallisesti. Toimivia metodeja halutaan käyttää mahdollisimman tehokkaasti (Maigida ym. 2019). Voidaan todeta, ettei trendien merkitystä kohteille tule aliarvioida. Samantyyppiset menetelmät altistavat samantyyppisiä organisaatioita, kunnes merkittävä enemmistö kykenee puolustautumaan uhkaa vastaan.

3.2 Poliittinen motivaatio

Valtioiden tiedetään käyttäneen rikollista kapasiteettia likaisiin töihinsä kautta aikojen Broadhurst (2014) kirjoittaa. Kyberulottuvuuden merkityksen kasvun myötä, verkossa tapahtuva hybridivaikuttaminen on muodostunut yhdeksi tämän kapasiteetin tehokkaimmista ilmenemismuodoista (Giannopoulos, Smith ja Theocharidou 2020). Luonnollisesti kiristyshaittaohjelmat eivät voi välttyä tältä keskustelulta (G7 Summit 2021). Jokainen hyökkäys omaa poliittisen aspektin, sillä jokaisella hyökkäyksellä on isäntämaa sekä kohde. Kiristyshaittaohjelmien muodostaman yhteiskunnallisen rasitteen myötä poliittinen motivaatio ylläpitää hyökkäävän kapasiteetin luomaa painetta kasvaa (Cyberwatch Finland 2021).

Poliittisen vaikuttamisen tasot

Poliittinen motivaatio kiristyshaittaohjelmien taustalla jakautuu Broadhurst ym. (2014) mukaan kolmeen tasoon: hyökkäysten toteuttamiseen, -sponsorointiin ja -laiminlyöntiin. Kybertoimintaympäristön epäselvyyden vuoksi tarkennusta teoreettista havainnointia pidemmälle on hankala saavuttaa (Giannopoulos, Smith ja Theocharidou 2020). Tästä huolimatta kohteiden painopiste lännessä sekä isäntämaat valtaosalle hyökkäyksistä ovat tiedossa (G7 Summit 2021). Gunnerriuksen (2021) määritelmän mukaan hybridivaikuttamisen ydin on vaikuttaa kilpailevan valtion poliittiseen päätöksentekoon oman valtion etujen mukaisesti. Erityisesti kriittiseen infrastruktuuriin kohdistuneiden hyökkäysten yleistyessä kiristyshaittaohjelmien toteutuksen voidaan nähdä toimivan väitteen mukaan (Hayes 2021).

Organisaatioiden kannalta olennaista kehityksessä on ymmärtää kiristyshaittaohjelmien merkitys politiikan työkaluna. Isäntämaiden strateginen välinpitämättömyys hyökkäyksiä kohtaan on niiden elinehto. Tämä tarkoittaa valtioiden potentiaalia vaikuttaa hyökkäysten kohdentamiseen tarpeidensa mukaan (Ransomware Task Force 2021; The White House 2021).

Hybridivaikuttaminen kyberulottuvuuden kautta on laajalti todettu ongelmalliseksi. Tilannekuva poliittisesta ilmapiiristä on merkittävä tekijä hyökkäyksiin varautuessa. Greenberg (2018) mukaan konkreettisena esimerkkinä voidaan pitää Venäjän ja Ukrainan konfliktin hybridiulottuvuutta, jossa Venäjän tiedustelupalveluun linkitetyt NotPetya kiristyshaittaohjelmahyökkäykset laukaistiin Ukrainan kriittisiin järjestelmiin. Operaatio on nähtävissä vaikut-

tamisen keinona heikentää Ukrainan asemaa vallitsevassa tilanteessa.

Sama kapasiteetti omaa potentiaalia ilmetä esimerkiksi Euroopan energiakriisin yhteydessä. Hyökkäysten kohdistaminen energiasektorille voisi tukea NordStream2 hankkeen edistystä, joten motiiveja toiminnalle on havaittavissa. Tarve näille toimille määrittää toteutuvatko ne.

Yhteiskunnallinen rasite

Kiristyshaittaohjelmien taloudellisia ja yhteiskunnallisia vaikutuksia ei ole myöskään syytä aliarvioida. Nykyisellään ransomware-ilmiö on pakottanut valtiot, Yhdysvallat kärjessä, kuluttamaan merkittävästi resursseja kyberturvaan. Nämä resurssit ovat pois muualta, kuten asevarustelusta ja globaalin vaikutusvallan ylläpidosta. Tämän lisäksi lainvastuun puute hyökkäystyypin ympärillä muodostaa merkittävän psykologisen rasitteen. Tyytymättömyys viranomaisia ja poliittisia päättäjiä kohtaan lisää sisäistä epävakautta, joka kuluttaa uskottavuutta politiikan kentällä (Renz 2016). Kohteiden kannalta tätä on syytä peilata oman organisaation yhteiskunnalliseen merkitykseen.

Tiedustelutarpeet

Merkittävä ulottuvuus poliittisesti motivoituneiden kiristyshaittaohjelmahyökkäysten osalta liittyy valtioiden tiedustelutarpeisiin. Nykyisessä toimintaympäristössä tiedustelutavoitteiden toteuttamiseen vaadittava tieto on suurelta osin siirtynyt tietoverkkoihin kirjoittaa Johansson (2021). Kyberhyökkäykset täydentävät valtioiden aktiivista tiedustelua paljastaen merkittävästi uutta tietoa järjestelmien turvallisuudesta, organisaation sisäisistä toimintamalleista, kriisinhallinnasta ja poliittisista reaktioista (Rid ja Buchanan 2015). Kiristyshaittaohjelmien hyödyntäminen tiedustelutarkoituksiin on loogista, sillä rikolliset suorittavat tiedustelun isäntävaltion puolesta ja kustannukset korvaa kohde. Tästä syystä valtioiden passiivisuus hyökkäysten rajoittamisessa on hankalaa, koska tämä itsessään ei näyttäydy aktiivisena sodankäyntinä, mutta seuraukset vastaavat vihamielisiä toimia. Vaikkei todisteita suorasta vaikutuksesta ole, useat valtioihin linkitetyt APT-ryhmät käyttävät kiristyshaittaohjelmia yhtenä hyökkäysmetodeistaan (MITRE ATT&CK® 2021).

Kohteiden kannalta tiedusteluvaikutuksen määrittely on kuitenkin hankalaa. Johansson (2021)

mukaan tiedustelua toteutetaan, jotta konfliktitilanteisiin tullaan parhaista mahdollisista asemista. Kiristyshaittaohjelmahyökkäykset toteuttavat tätä tarkoitusta automaattisesti etsiessään lakkaamatta heikkoja lenkkejä yhteiskunnasta. Hyökkäykset kohdistetaan laajasti ja ne, joista merkittävää tietoa on tarjolla, huomioidaan valtioiden toimesta.

Harmaa alue

Viimekädessä kiristyshaittaohjelmahyökkäyksin testataan rajoja (Renz 2016). Kiristyshaittaohjelmat paljastavat kuinka paljon haittaa kybertilassa voidaan aiheuttaa, ennen rauhan käsitteen murtumista. Tämä pätee riippumatta motiiveista hyökkäyksen taustalla.

4 Kohteeksi joutumisen riski

Kiristyshaittaohjelmahyökkäyksen uhka voi realisoitua monella tapaa, joista toiset ovat muita todennäköisempiä. Tässä luvussa katselmoidaan merkittävimpiä hyökkäykseen johtavia riskejä, joita organisaatiot kohtaavat omassa toimintaympäristössään. Riskien käsittely motiivien ja toimintamallien pohjalta mahdollistaa organisaatioille tilaisuuden verrata toimijaprofiiliaan työn tuloksiin ja näin ollen harkita turvallisuusinvestointeja suhteessa konkreettiseen uhkaan.

Esitetty materiaali on koottu merkittävistä akateemisista tutkimuksista, ajankohtaisista turvallisuusyhteisön tuottamista raporteista, sekä analyyseistä.

4.1 Organisaatiokohtainen riski

Alun perin kiristyshaittaohjelmahyökkäykset vaikuttavat toteutuneen spray-and-prey muodossa, yksittäisen kohteen omatessa vähän merkitystä. Atapour-Abarghouei, Bonner ja McGough (2019) kuitenkin toteavat viime aikoina rikollisten alkaneen käyttää resursseja enemmän kohdistettujen tartuntavektoreiden tunnistamiseen. Erityisesti jengien osalta uusissa hyökkäysmetodeissa on havaittu yhtäläisyyksiä aiemmin vain valtiollisissa tiedusteluoperaatioissa tavattuun Advanced persistent threat-malliin (APT). APT-malli, jota rikollisjengit yhä useammin seuraavat, hyödyntää informaatiota yhtenä pääasiallisena resurssina kohteiden valitsemisessa ja hyökkäysten menestyksekkäässä toteuttamisessa. Kohdistettujen hyökkäysten riskin konkretisoituessa Big Game Hunting – trendin myötä, turvallisuusyhteisön on täytynyt kehittää ja ylläpitää kykyä vastata uhkaan. Tässä kappaleessa aihetta lähestytään käsittelemällä informaatiota, joka vaikuttaa yksittäisen organisaation prioriteettiin kohteena.

4.1.1 Vahingon arvo

Kiristyshaittaohjelmahyökkääjien motiiveja katselmoidessa, havaittiin yhdeksi merkittävimmistä rikollisten työ kehittää mahdollisimman tuhoisia hyökkäyksiä. Hernandez-Castro, Cartwright ja Stepanova (2017) mukaan mitä merkittävämpi ero toiminnan palauttamisen ja lunnasvaatimuksen väliin saatiin, sen kannattavammaksi investoinniksi hyökkäykset rikollisille

muodostuivat. Väitteeseen pohjaten rikollisille houkuttelevan kohteen määrittäminen voidaan aloittaa vastaamalla kahteen perustavanlaatuiseen kysymykseen:

- Mikä on riskin arvo, jonka hyökkäys muodostaa yrityksen liiketoiminnalle
- Mikä on riskin arvo, jonka hyökkäys muodostaa toimitusketjulle

Julkisten profiilien, tietovuotojen, sekä rikollisen tiedustelun myötä vastaukset näihin kysymyksiin ovat usein saatavilla avoimesti. O'Kane, Sezer ja Carlin (2018), Richardson, North ja Garofalo (2021), Symantec (2016), sekä Atapour-Abarghouei, Bonner ja McGough (2019) tutkimusten pohjalta olennainen informaatio voidaankin kiteyttää kolmeen ehtoon, joiden nähdään toistuvan toteutuneissa kiristyshaittaohjelmahyökkäyksissä:

Organisaatiot ovat vahvasti riippuvaisia informaatiojärjestelmistä, joten toiminnan katkeamisen rahallinen arvo on merkittävä. Usein tämän lisäksi, organisaation oman liiketoiminnan ohella lukuisat asiakkaat kokevat merkittäviä vaikutuksia hyökkäyksestä esitettyihin kohteisiin. Ja lopulta data, jota organisaatiot säilövät on kriittistä niin organisaation omalle, kuin asiakkaiden toiminnalle. Jokainen ehto voidaan muuttaa myös poliittiseen kontekstiin.

Palo Alto Networksin (2021b) raportissa esitetään ydinkohdat 2020 suosituimmista kiristyshaittaohjelmien varianteista. Raportin avulla voidaan tarkastella kohdistettujen hyökkäysten toimintamallia seuranneita variantteja ja verrata näiden suosimia kohteita edellä esitettyihin ehtoihin. Hallituksen, terveydenhuollon, energian, huipputeknologian ja logistiikan alojen ilmetessä suosittuina kohteina, havaitaan ehtojen pätevän.

4.1.2 Todennäköisyys onnistua hyökkäyksessä

O'Kane, Sezer ja Carlin (2018) mukaan jokaisen hyökkäyksen myötä rikolliset ottavat riskin paljastaa itsensä ja työkalunsa. Tämän lisäksi kohdistetun hyökkäyksen toteuttamiseen kulutetaan runsaasti aikaa ja resursseja (vrt. luku 3 - Toiminnan ylläpito). Idean taustalta, yhdeksi merkittävimmistä kiristyshaittaohjelmahyökkäyksiä käsittelevistä tutkimuksen haaroista onkin muodostunut hyökkäysten kustannusten ja hyökkääjän riskin kasvattaminen (Al-rimy, Maarof ja Shaid 2018).

Akateeminen tutkimus on nostanut varautumisen tason merkittävimpänä indikaattorina kiris-

tyshaittaohjelmahyökkäysten menestykselle. Aihetta lähestytään lukuisista eri näkökulmista, merkittävimpinä kuitenkin heikko valmistautuminen riskinä organisaatiolle (Hathaway 2012), tai korkea valmistautuminen kyberturvallisuuden perustana (Atapour-Abarghouei, Bonner ja McGough 2019). Suositusten ja hyvien käytänteiden runsaasta määrästä johtuen tässä tutkimuksessa yleisimmistä elementeistä toteutettiin seuraava kooste taulukossa 1.

Taulukko 1. Kooste suosituksista hyviksi käytännöiksi (Al-rimy, Maarof ja Shaid 2018; Atapour-Abarghouei, Bonner ja McGough 2019; Ransomware Task Force 2021; Brewer 2016; Cybersecurity & Infrastructure Security Agency 2020)

Suositukset organisaatiolle
Laadi kattava varakopiosuunnitelma
Hanki nykyaikaiset virus- ja haittaohjelmientorjuntatyökalut
Toteuta verkon segmentointi arvokkaan datan rajaamiseksi
Monitoroi toimitusketjua haavoittuvuuksien varalta
Valmistele kriisinhallintasuunnitelma kyberhyökkäysten varalle
Aseta rajat työntekijöiden henkilökohtaiselle verkkotoiminnalle työaikana
Huolehdi järjestelmien ajantasaisuudesta
Käytä välipalvelimia sekä mainoksenestoa
Implementoi tehokkaat käytännöt järjestelmien hallintaan, sovellusten käyttöön sekä ohjelmistojen rajoittamiseksi

Suositukset loppukäyttäjälle
Perehdy sosiaalisen manipulaation muodostamaan uhkaan
Hanki koulutusta tietojen kalastelusta ja sen torjunnasta
Seuraa hyviä salasanakäytänteitä ja ylläpidä vahvaa tunnistautumista

Merkittävää tietoa organisaation kyberturvallisuuspolitiikasta, investoinneista, sekä yleisestä työkulttuurista on enemmän tai vähemmän avoimesti saatavilla. Tästä johtuen oman toimijaprofiilin tunnistaminen muodostuu alati kriittisemmäksi (Atapour-Abarghouei, Bonner ja McGough 2019). Kaikki turvallisuutta heikentävä toiminta, josta organisaatioissa ei olla

tietoisia, mutta rikollisten on mahdollista selvittää, muodostuu riskiksi ja näin ollen siirtää painoarvoa kohden kannattavaa investointia hyökkääjän näkökulmasta (Hathaway 2012).

Poliittisesti motivoituneiden toimijoiden lisäksi, myös perinteisten rikollisten onkin havaittu suorittavan tiedustelua organisaatioiden tietoverkoissa ja järjestelmissä, johtaen useampiin tarkasti suunniteltuihin ja menestyviin hyökkäyksiin (Bhatt, Yano ja Gustavsson 2014). Tärkeäksi muodostuu siis tieto vuodetusta ja avoimesti tarjotusta informaatiosta turvallisuuspäätöksenteon tukena. Mukaanlukien omalle organisaatiolle kriittisen tiedon vuotaminen toimitusketjun varrella.

4.1.3 Tuotto-odotus

Akateemisen tutkimuksen priorisoidessa hyökkäysten mitigaatio (Herrera Silva ym. 2019), vähemmän tutkimuksia on syntynyt lunnaiden maksun ympärille. Tästä huolimatta, kohdistettujen hyökkäysten näkökulmasta selkeää korrelaatiota havaitaan tiettyjen organisaation toimintatapojen ja lunnaiden maksupotentiaalin välillä (Hernandez-Castro, Cartwright ja Stepanova 2017). Pääasiallisesti nämä tutkimukset argumentoivat lunnaiden maksun vastustamisen johtavan organisaatioiden profiloitumiseen huonona kohteena (Huang ym. 2018).

Richardson ja North (2017) mukaan viranomaisyhteistyöllä on yhteys kohdennettujen hyökkäysten todennäköisyyteen. Väitettä perustellaan kahdesta näkökulmasta. Teoriassa, valtion virastojen suosituksia noudattavat organisaatiot harvoin maksavat lunnaita (Federal Bureau of Investigation 2021). Samalla viranomaisyhteistyö itsessään muodostaa hyökkääjille riskin, aktiivisten seuraustoimenpiteiden myötä. Viranomaiset ovat osoittaneet kyvykkyyttä tuottaa rikollisorganisaatiolle lamauttavia seurauksia, sekä jäädyttää hyökkäyksessä hankittuja tuottoja (Department of Justice 2021). Näin ollen useiden hyökkääjien näkökulmasta valtaosa vastaavista kohteista muodostuu riskialttiiksi suhteessa maksupotentiaaliin. Jos hyökkäys toteutetaan viranomaisyhteistyöstä huolimatta, motiivi täytyy poiketa suorasta taloudellisesta. Vastaavia toimijoita, kuten luvussa kolme käsiteltiin, on vähemmän.

Maksupotentiaalin kasvattajana puolestaan, Hernandez-Castro, Cartwright ja Stepanova (2017) nostavat tutkimuskirjallisuudessa kiristyshaittaohjelmien kannalta harvemmin käsitellyt kybervakuutukset. Aiemmin hyvänä liiketoimintana ilmenneet kybervakuutukset paransivat or-

ganisaatioiden kykyä palautua kyberhyökkäyksistä, mutta erityisesti kiristyshaittaohjelmien yleistymisen ja kasvavien kustannusten myötä moni vakuuttaja on joutunut nostamaan hintoja, vaatimuksia tai yksinkertaisesti rajoittamaan tarjontaa (Shetty ym. 2018). Tutkiessaan kybervakuutusten merkitystä kyberriskienhallinnalle Dudley (2019) toteaa vakuutusten perusidean olevan halvimman ratkaisun korvaaminen. Tällöin lunnaiden maksu ilmenee usein ensimmäisenä vaihtoehtona priorisoiden vakuutuksen hankkineet organisaatiot kohteena.

Kolmas merkittävä korrelaatio esiintyy Everett (2016) avattaessa riskienhallinnan historiaa. Everett kirjoittaa aiempien tietoturvaonnettomuuksien ja kiristyshaittaohjelmien vaikuttavan merkittävästi organisaation maalautumiseen kohteena. Jos toimijan tiedetään maksaneen lunnaat tietyn hyökkäyksen yhteydessä, rikollisten voidaan nähdä päätelleen tämän olevan todennäköisesti valmis maksamaan uudelleen. Näin ollen rikollisten investointi hyökkäykseen kannattaa suuremmalla todennäköisyydellä (Symantec 2016). Cybereason (2021) raportti tukee päätelmää. Sen mukaan 80 % organisaatioista, jotka maksoivat lunnaat, joutuivat hyökkäyksen kohteeksi uudelleen.

4.2 Yleinen riski

Yleinen riski kiristyshaittaohjelmahyökkäykselle on huomattavasti kohdistettua hyökkäystä käsitellympi aihe. Perinteisesti kiristyshaittaohjelmahyökkäykset ovat seuranneet kohdistamattoman hyökkäyksen mallia, hyödyntäen internetin tarjoamaa hyökkäyspinta-alaa. Yleinen riski ei muutu samoja järjestelmiä ja alustoja hyödyntävien toimijoiden välillä. Täten menetelmät, jotka hyödyntävät yleisimpiä tartuntavektoreita ovat aina olleet kiristyshaittaohjelmien suosiossa. Korkean käsittelyasteen johdosta kappaleessa katselmoidaan näistä yleisimpiä.

Sähköposti

Sähköposti on selkeästi suosituin tartuntavektori niin kiristyshaittaohjelmille kuin haittaohjelmille yleisesti. Syy tähän löytyy käyttöasteesta. Liki jokaisella internetin käyttäjällä on pääsy työ-, koulu- tai henkilökohtaiselle sähköpostitilille. Sähköpostein leviävien haittaohjelmien pääasiallinen hyökkäysmetodi on sosiaalinen manipulaatio. Sosiaalinen manipulaa-

tio hyväksikäyttää käyttäjän vaistoa reagoida nopeaa toimintaa vaativalta tilanteelta vaikuttavaan viestiin. Mitä lähemmäs omaa toimintaympäristöä huijausviestin aihe osuu, sen helpompi siihen on samaistua ja langeta. Jos käyttäjä erehtyy kommunikoimaan viestin kanssa, avaamalla sen linkit tai tiedostot, tietomurto käynnistyy. Suurin riski alun perin kohdistamattomissa hyökkäyksissä muodostuu siis ihmisvirheestä. (Atapour-Abarghouei, Bonner ja McGough 2019; Zimba ja Wang 2017).

Exploit kit

Järjestelmäpuolella merkittävimmän uhan muodostaa Exploit Kittien, eli haittaohjelmien jalkauttamisalustojen olemassaolo (Symantec 2016). Nämä rikollisten jatkuvasti päivittämät työkalut toimivat pohjautuen tunnettuihin haavoittuvuuksiin yleisimmissä alustoissa ja järjestelmissä. Kuten sähköposti, yleisimmät tuotteet joita Exploit Kitit hyödyntävät ovat miljoonien asiakkaiden käytössä täten tarjoten lukemattomasti kohteita. Kittien varsinaisen menestyksen taustalla on kuitenkin luontainen viive päivitysprosessissa. O'Kane, Sezer ja Carlin (2018) mukaan missä tahansa ajankohdassa järjestelmät sisältävät eri vakavuustasojen haavoittuvuuksia. Rikolliset pyrkivät hyödyntämään näitä haavoittuvuuksia mahdollisimman pienellä viiveellä, kun taas organisaatiolta kuluu haavoittuvuuden löytämiseen, korjauksen kehitykseen, testaukseen ja jalkauttamiseen keskimäärin 30 vuorokautta. Ottaen huomioon aikavälin merkittävät vaihtelut organisaatioiden kesken voidaan todeta päivittämättömien järjestelmien ja liitännäisen viiveen muodostavan sähköpostin jälkeen kriittisimmän riskin kohdistamattomien hyökkäysten suhteen. (O'Kane, Sezer ja Carlin 2018).

Käyttöjärjestelmät

Windows pohjaisia alustoja vastaan rakennetut kiristyshaittaohjelmat dominoivat hyökkäystyypin uhkakuvaa. Kohdistamattomien hyökkäysten tähdätessä mahdollisimman laajaan hyökkäyspinta-alaan Windows käyttäjät ovat luonnollinen kohde Al-rimy, Maarof ja Shaid (2018) toteavat. Korkea käyttöaste säteilee myös mobiiliin. F-Secure State of Cyber Security (2017) raportin mukaan erityisesti Android pohjaiset laitteet ovat yleistyneet kiristyshaittaohjelmahyökkäysten kohteena. Käyttöasteen lisäksi syynä kehitykseen on havaittu avoimet sovellustenjakokäytänteet, sekä hidas tempo käyttöjärjestelmäpäivityksissä (ks. Exploit Kit). Kehi-

tyksen huomioiden Al-rimy, Maarof ja Shaid (2018) nostavat Windowsin ja mobiilin lisäksi myös IoT-laitteiden myötä syntyvän riskin. Tietoisuuden perinteisistä kohteista lisääntyessä, IoT:n potentiaalia kohteena testataan enenvässä määrin. IoT-laitteiden rooli toimintaympäristössä omaa potentiaalia merkittäviin häiriöihin linkitetyissä järjestelmissä.

Kirjautumistunnukset

Kirjautumista vaativien palveluiden merkittävän kasvun myötä, automaattisten skriptien rakentaminen tunnusten murtamiseksi on kehittynyt nopeasti. Tunnusten määrän lisääntyessä ja laskentatehon kasvaessa tehokkaiden skriptien ohjelmointi on tullut helpoksi. Vanhanaikaiset tunnistetiedot ovat muodostuneet kriittiseksi haavoittuvuudeksi järjestelmissä. Usein rikolliset hyödyntävät murrettuja tunnuksia Remote desktop protocol (RDP) -palvelimilla, jotka mahdollistavat tiedostojensalausprosessin aloittamisen, johtaen lunnasvaatimuksiin (Zimba ja Wang 2017).

Muut tartuntavektorit: Vaikka akateeminen kirjallisuus on laajalti samaa mieltä edellä mainittujen tartuntavektoreiden tärkeydestä, useat muut vaikuttavat uhkakuvaan. Syvempää tutkimusta aihepiiriin ovat toteuttaneet mm. Symantec (2016), O'Kane, Sezer ja Carlin (2018), sekä Zimba ja Wang (2017).

4.3 Toimialakohtainen riski

Raportit kiristyshaittaohjelmahyökkäysten kohteista trendeinä ovat perinteisesti olleet yksityisen sektorin vastuulla. Kuitenkin hyökkäysten yleistyessä ja näin ollen tutkimusmateriaalin lisääntyessä myös akateeminen yhteisö on alkanut siirtyä kohti konkreettisempaa lähestymistapaa. Katselmoidaksemme toimialakohtaisen riskin nykyistä tilannekuvaa, tässä kappaleessa käsitellään Atapour-Abarghouei, Bonner ja McGough (2019) ja Symantec (2016) tutkimuksia kiristyshaittaohjelmien kohteista ja esitetään hyökkäyksiä eniten kokeneet sektorit. Ajankohtaisuuden varmistamiseksi, mainittuja tutkimuksia verrataan Sophosin (2021), sekä Palo Alto networksin (2021b) raportteihin.

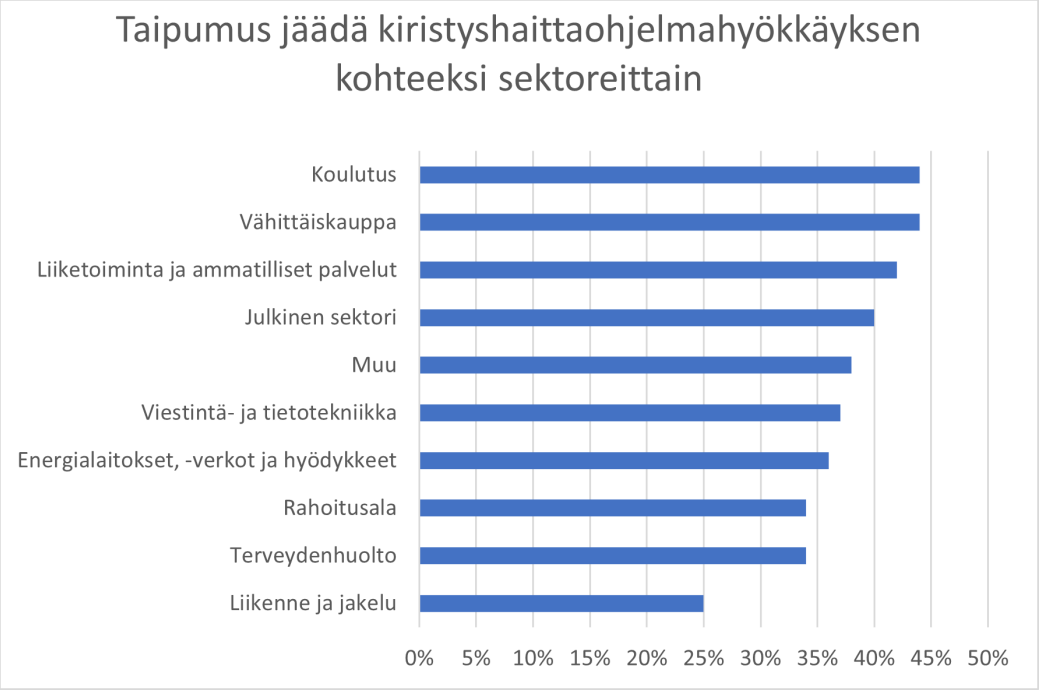
Koulutus: Koulutus on muodostunut yhdeksi kiristyshaittaohjelmahyökkäysten yleisimmistä kohteista. Atapour-Abarghouei, Bonner ja McGough (2019) mukaan koulutus oli hyökä-

tyin kohde vuonna 2017. Tilanne on säilynyt samana vuoteen 2021 saakka (Sophos 2021). Atapour-Abarghouei ym. esittävät tutkimuksessaan sektorin suosion johtuvan yleisestä budjettivajeesta, tietoturva-ammattilaisten puutteesta, sekä pienistä ja ylikuormitetuista IT-osastoista. Näiden rajoitteiden lisäksi korkeatempoinen tiedostojen jakaminen ja keskitetyt järjestelmät luovat houkuttelevan kohteen rikollisille.

Terveydenhuolto: Terveydenhuollon fasiliteetit ovat yksi kiristyshaittaohjelmahyökkäysten näkyvimmistä kohteista, organisaatioiden ollessa vastuussa tuoda turvallisuusongelmat nopeasti julki. Huolimatta joidenkin rikollisten julistuksista jättää hyökkäämättä sektorille, äärimmäisen arkaluontoinen data, korkea verkkointegraatio, sekä kriittiset ja vaikeasti päivitettävät järjestelmät tekevät sektorista tuottavan kohteen hyökkäyksille (Sophos 2021; Office of Information Security 2021).

Alueellinen hallinto: Atapour-Abarghouei, Bonner ja McGough (2019) mukaan valtion virastoihin kohdistuneet hyökkäykset kolminkertaistuivat vuosien 2015 ja 2016 välillä. Tästä saakka hyökkäykset ovat yleistyneet tasaisesti ja sektori on edelleen yksi kohdistetuimmista. Syy suosioon johtuu sektorin yleisesti hyvistä resursseista, sekä järjestelmien kriittisestä luonteesta. Samalla Yhdysvaltojen senaatin ja kotimaanturvallisuusviraston komitean raportin (2021) mukaan virastot epäonnistuvat toistuvasti jopa perustavanlaatuisen kyberturvan ylläpidossa.

Vähittäismyynti: Monien vähittäiskaupan organisaatioiden toiminnan pohjautuessa yhä enemmän tehokkaisiin, matalan latenssin järjestelmiin, riippuvuus tekniikasta kasvaa. Järjestelmähäiriöistä johtuvien, jopa hyvin lyhyiden seisokkien hinta on kasvanut merkittäväksi. Sophos (2021) raportin mukaan, valtaosan organisaatioista kuuluessa yksityiselle sektorille kohteen houkuttavuutta nostaa myös viranomaistoiminnan puute, sekä matala profiili valtaosan hyökkäyksistä kohdalla. Atapour-Abarghouei, Bonner ja McGough (2019) kirjoittavat hyökkäysten usein kohdistuvan henkilöstöosastoihin, näiden omatessa laajat valtuudet organisaatioiden sisällä. Vähittäiskauppa kokee koulutuksen rinnalla eniten kiristyshaittaohjelmahyökkäyksiä.



Kaavio 1 Sophosin (2021) ja Symantecin (2016) pohjalta

5 Yhteenveto

Tutkimustiedon pohjalta kohteen prioriteetin määrittäminen on mahdollista. Runsaan hyökkäysdatan myötä syntyneestä toisteisuudesta johtuen motiivit, toimintatavat sekä riskitekijät kyetään mallintamaan yleisiin kaavoihin, jotka ohjaavat hyökkäysten kohdistumista. Tehokkaan reagoinnin muodostama haaste kuitenkin kasvaa. Viranomaisten ja turvallisuusyhteisön pyrkiessä ratkaisemaan kiristyshaittaohjelmahyökkäysten muodostamaa ongelmaa, rikolliset ovat motivoituneet ylläpitämään ja näin ollen kehittämään toimintaansa. Osin pakon ja osin verkkorikollisuutta suosivan ekosysteemin tuloksena, kehitys liiketoimintatiedon hallinnassa on johtanut alati tehokkaamman vahinko-lunnas -suhteen muodostumiseen niin hyökkäysten teknisen toteutuksen, yhteiskunnallisen rasitteen, kuin kohteiden haun osalta. Tästä syystä ennakoinnin merkitys kasvaa ja tutkimushaaran edistämiseen tarvitaan enemmän resursseja.

Yksinkertaisempi lopputulos on todeta, että generoitua hyökkäystä voidaan odottaa joka tapauksessa. Vallitsevassa tilanteessa automatisaatio ja kiristyshaittaohjelmien kaupallistuminen ohjaavat laajalti hyökkäystyypin kehitystä. Tämä voidaan kuitenkin nähdä hyvänä päätelmänä, sillä generoitujen hyökkäysten estäminen tapahtuu pääosin perustavanlaatuisesta kyberturvallisuudesta huolehtimalla (Traficom 2020). Suhteuttaen nykyiseen kehitykseen, perustason kyberturvan ylläpito tapaa kuitenkin epäonnistua.

Priorisoinnin merkitys ei tästä huolimatta tule laskemaan. Kohdistetut, käsin räätälöidyt hyökkäykset ovat edelleen merkittävin uhka korkean profiilin organisaatioille. Kohdistetussa hyökkäyksessä uhkatoimija määrittelee kohteen arvon riskin, tuoton ja toteutukseen vaadittavien resurssien kautta. Organisaatiosta saatava tieto siis ratkaisee resurssit, joita kohteen murtamiseen tullaan kuluttamaan. Ilman perustavanlaatuisia muutoksia kiristyshaittaohjelmien mahdollistajiin (ks. alaluvut 2.1 ja 2.2), erityisesti suurten organisaatioiden täytyy tunnistaa APT-mallia seuraavan kiristyshaittaohjelmahyökkäyksen riski omassa toimintaympäristössään.

Kohdistettujen hyökkäysten yläkäsitteenä, poliittinen motivaatio ohjaa hyökkäysten suuria mittakaavoja. Hyökkäysten painopisteeseen myötävaikutetaan eri tasoilla (rajoitetaan, sponsoroidaan, toteutetaan) tavoitteena tuottaa kilpailevalle valtiolle painetta siellä missä poliit-

tinen tarve on olemassa. Tämä voi olla hyvinkin laaja, vain yleinen etu, kuten pakottaa valtion resurssit pois asevarustelusta ja globaalin vaikutusvallan edistämisestä, kotimaan kriittisen infrastruktuurin kyberturvallisuuden kehittämiseen. Konfliktin syttyessä, organisaatioiden rooli yhteiskunnassa muodostuu kriittiseksi riskiksi. Tällöin on liki varmaa, että puolustus pettää, joten kriisinhallinnan merkitys korostuu.

Kiristyshaittaohjelmahyökkäyksen realisoituessa, tarjolla ei enää ole hyviä vaihtoehtoja. Omatoimisesti toiminnan palauttaminen voi aiheuttaa organisaatiolle ja sen asiakkaille kriittisiä seurauksia, kun taas lunnaiden maksaminen takaa pelkästään todennäköiseksi kohteeksi muodostumisen. Nämä riskit täytyy kuitenkin ymmärtää, jotta mahdolliseen uhkaan osataan reagoida ajoissa. Oman toimijaprofiilin tunnistaminen ja tätä myötä kiristyshaittaohjelmahyökkäyksen riskiin varautuminen säilyvät parhaana suojana hyökkäysten muodostamalta uhkalta.

Lähteet

Armstrong, Helen L, ja Patrick J Forde. 2003. “Internet anonymity practices in computer crime”. *Information management & computer security,* https://doi.org/10.1108/09685220310500117.

Atapour-Abarghouei, Amir, Stephen Bonner ja Andrew Stephen McGough. 2019. “Volenti non fit injuria: Ransomware and its Victims”. Teoksessa *2019 IEEE International Conference on Big Data (Big Data),* 4701–4707. https://doi.org/10.1109/BigData47090.2019.9006298.

Bhatt, Parth, Edgar Toshiro Yano ja Per Gustavsson. 2014. “Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks”. Teoksessa *2014 IEEE 8th International Symposium on Service Oriented System Engineering,* 390–395. https://doi.org/10.1109/SOSE.2014.53.

Brewer, Ross. 2016. “Ransomware attacks: detection, prevention and cure”. *Network Security* 2016 (9): 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours ja Steve Chon. 2014. “An analysis of the nature of groups engaged in cyber crime”. *An analysis of the nature of groups engaged in cyber crime, International Journal of Cyber Criminology* 8 (1): 1–20. https://ssrn.com/abstract=2461983.

Cartwright, Anna, ja Edward Cartwright. 2019. “Ransomware and reputation”. *Games* 10 (2): 26. https://doi.org/10.3390/g10020026.

Crowdstrike. 2020. *Crowdstrike Services Cyber Front Lines Report.* Viitattu 20. lokakuuta 2021. https://www.crowdstrike.com/resources/reports/crowdstrike-services-cyber-front-lines-2020/.

Cybereason. 2021. *Ransomware: The True cost to Business.* Viitattu 15. lokakuuta 2021. https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business.

Cybersecurity & Infrastructure Security Agency. 2020. “Ransomware Guide”, viitattu 20. syyskuuta 2021. https://www.cisa.gov/stopransomware/ransomware-guide.

Cybersecurity Ventures. 2021. “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031”, viitattu 5. lokakuuta 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Cyberwatch Finland. 2021. *Cyberwatch Finland Kuukausikatsaus Kesäkuu.* https://www.cyberwatchfinland.fi/.

Department of Justice. 2021. *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside.* Viitattu 28. lokakuuta 2021. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

Dudley, Renee. 2019. “The extortion economy: How insurance companies are fueling a rise in ransomware attacks”. *Pro Publica,* http://www.businessforum.com/ProPublica_08-27-2019.pdf.

Everett, Cath. 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.

F-Secure. 2017. https://www.f-secure.com/content/dam/f-secure/en/investors/governance/annual-general-meeting/2018/f-secure-annual-report-2017.pdf.

Federal Bureau of Investigation. 2021. *Federal Bureau of Investigation - Ransomware.* Viitattu 1. marraskuuta 2021. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

G7 Summit. 2021. “CARBIS BAY G7 SUMMIT COMMUNIQUÉ” (kesäkuu). Viitattu 29. syyskuuta 2021. https://www.consilium.europa.eu/media/50361/carbis-bay-g7-summit-communique.pdf.

Giannopoulos, Georgios, Hanna Smith ja Marianthi Theocharidou. 2020. “The Landscape of Hybrid Threats: A Conceptual Model”. *European Commission, Ispra,* https://publications.jrc.ec.europa.eu/repository/handle/JRC123305.

Greenberg, Andy. 2018. “The untold story of NotPetya, the most devastating cyberattack in history”. *Wired, August* 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Gunneriusson, Håkan. 2021. “Hybrid warfare: Development, historical context, challenges and interpretations”. *ICONO 14, Revista de comunicación y tecnologıas emergentes* 19 (1): 15–37. https://doi.org/10.7195/RI14.V19I1.1608.

Hathaway, Melissa E. 2012. “Leadership and responsibility for cybersecurity”. *Georgetown Journal of International Affairs,* 71–80. http://www.jstor.org/stable/43134340..

Hayes, Kingsley. 2021. “Ransomware: a growing geopolitical threat”. *Network Security* 2021 (8): 11–13. https://doi.org/10.1016/S1353-4858(21)00089-1.

Hernandez-Castro, Julio, Edward Cartwright ja Anna Stepanova. 2017. “Economic analysis of ransomware”. *Available at SSRN 2937641,* http://dx.doi.org/10.2139/ssrn.2937641.

Herrera Silva, Juan A, Lorena Isabel Barona López, Ángel Leonardo Valdivieso Caraguay ja Myriam Hernández-Álvarez. 2019. “A survey on situational awareness of ransomware attacks—detection and prevention parameters”. *Remote Sensing* 11 (10): 1168. https://doi.org/10.3390/rs11101168.

Huang, Danny Yuxing, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren ja Damon McCoy. 2018. “Tracking ransomware end-to-end”. Teoksessa *2018 IEEE Symposium on Security and Privacy (SP),* 618–631. IEEE. https://doi.org/10.1109/SP.2018.00047.

Johansson, Mirva. 2021. “Venäjän ja Kiinan sotilastiedusteluorganisaatioiden kybermenetelmien kehitys vuosina 2004–2021”. MSc thesis, Jyväskylän yliopisto. http://www.urn.fi/URN:NBN:fi:jyu-202105243182.

Krebs, Brian. 2016. “Before You Pay that Ransomware Demand. . . ”, https://krebsonsecurity.com/2016/12/before-you-pay-that-ransomware-demand/.

Køien, Geir M. 2021. “Zero-Trust Principles for Legacy Components”. *Wireless Personal Communications,* 1–18. https://doi.org/10.1007/s11277-021-09055-1.

Maigida, Abdullahi Mohammed, Morufu Olalere, John K Alhassan, Haruna Chiroma, Emmanuel Gbenga Dada ym. 2019. “Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms”. *Journal of Reliable Intelligent Environments* 5 (2): 67–89. https://doi.org/10.1007/s40860-019-00080-3.

Meland, Per Håkon, Yara Fareed Fahmy Bayoumy ja Guttorm Sindre. 2020. “The Ransomware-as-a-Service economy within the darknet”. *Computers & Security* 92:101762. https://doi.org/10.1016/j.cose.2020.101762.

Minchev, Zlatogor. 2016. “Cyber Threats Identification in the Evolving Digital Reality”. *Proceedings of the National Conference on "Education and Research in the Information Society"* (Plovdiv), 011p–022p. http://hdl.handle.net/10525/2471.

MITRE ATT&CK®. 2021. Viitattu 22. lokakuuta 2021. https://attack.mitre.org/groups/.

Naughton, John. 2016. “The evolution of the Internet: from military experiment to General Purpose Technology”. *Journal of Cyber Policy* 1 (1): 5–28. https://doi.org/10.1080/23738871.2016.1157619.

O’Kane, Philip, Sakir Sezer ja Domhnall Carlin. 2018. “Evolution of ransomware”. *IET Networks* 7 (5): 321–327. https://doi.org/10.1049/iet-net.2017.0207.

Office of Information Security. 2021. *Ransomware Trends 2021.* Viitattu 4. lokakuuta 2021. https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html.

Paganini, P. 2015. *Tox, how to create your ransomware in 3 steps.* https://securityaffairs.co/wordpress/37180/cyber-crime/tox-ransomware-builder.html.

Palo Alto Networks. 2021a. *Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report.* Viitattu 20. lokakuuta 2021. https://unit42.paloaltonetworks.com/ransomware-families/.

———. 2021b. *Ransomware Threat Report.* Viitattu 20. lokakuuta 2021. https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.

Ransomware Task Force. 2021. “Combating Ransomware”, viitattu 25. lokakuuta 2021. https://securityandtechnology.org/ransomwaretaskforce/report/.

Renz, Bettina. 2016. “Russia and ‘hybrid warfare’”. *Contemporary Politics* 22 (3): 283–300. https://doi.org/10.1080/13569775.2016.1201316.

Richardson, Ronny, ja Max M North. 2017. “Ransomware: Evolution, mitigation and prevention”. *International Management Review* 13 (1): 10. https://digitalcommons.kennesaw.edu/facpubs/4276.

Richardson, Ronny, Max M North ja David Garofalo. 2021. “Ransomware: The Landscape Is Shifting–A Concise Report”. *International Management Review* 17 (1): 5–86. https://www.proquest.com/scholarly-journals/ransomware-landscape-is-shifting-concise-report/docview/2509693987/se-2.

Rid, Thomas, ja Ben Buchanan. 2015. “Attributing cyber attacks”. *Journal of Strategic Studies* 38 (1-2): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Al-rimy, Bander Ali Saleh, Mohd Aizaini Maarof ja Syed Zainudeen Mohd Shaid. 2018. “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions”. *Computers & Security* 74:144–166. https://doi.org/10.1016/j.cose.2018.01.001.

Ryan, Matthew. 2021. “The Sociology of Ransomware”. Teoksessa *Ransomware Revolution: The Rise of a Prodigious Cyber Threat,* 143–152. Springer. https://doi.org/10.1007/978-3-030-66583-8_9.

Sanger, David E, ja Nicole Perlroth. 2020. “Russian criminal group finds new target: Americans working at home”. *New York Times,* https://nyti.ms/2CAaL98.

Shetty, Sachin, Michael McShane, Linfeng Zhang, Jay P Kesan, Charles A Kamhoua, Kevin Kwiat ja Laurent L Njilla. 2018. “Reducing informational disadvantages to improve cyber risk management”. *The Geneva Papers on Risk and Insurance-Issues and Practice* 43 (2): 224–238. https://doi.org/10.1057/s41288-018-0078-3.

Sophos. 2021. “The State of Ransomware”, viitattu 20. lokakuuta 2021. https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx.

Stalans, Loretta J, ja Mary A Finn. 2016. “Understanding how the internet facilitates crime and deviance”. *Victims & Offenders* 11 (4): 501–508. https://doi.org/10.1080/15564886.2016.1211404.

Symantec. 2016. “Special Report: Ransomware and Businesses 2016”. *Symantec Corp,* 1–30. https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/5c_ISTR2016_Ransomware_and_Businesses.pdf.

Traficom. 2020. “Kyberturvallisuus ja yrityksen hallituksen vastuu”, viitattu 20. lokakuuta 2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf.

Trend Micro. 2016. *Kansas Hospital Hit by Ransomware, Extorted Twice.* Viitattu 12. marraskuuta 2021. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kansas-hospital-hit-by-ransomware-extorted-twice.

US Senate. 2021. “Federal Cybersecurity: America’s Data Still At Risk”, https://www.hsdl.org/?view&did=857006.

Wall, David. 2001. “Cybercrimes and the Internet”. Teoksessa *Crime and the Internet,* 1–17. Routledge London. https://doi.org/10.4324/9780203299180.

Zimba, Aaron, ja Zhaoshun Wang. 2017. “Malware-free intrusions: Exploitation of built-in pre-authentication services for APT attack vectors”. *International Journal of Computer Network and Information Security* 9 (7): 1. https://doi.org/10.5815/ijcnis.2017.07.01.