Arttu Ylä-Sahra

Kiristyshaittaohjelmien toiminta ja ehkäisy

Tietotekniikan kandidaatintutkielma

28. huhtikuuta 2017

Jyväskylän yliopisto

Tietotekniikka

Tekijä: Arttu Ylä-Sahra

Yhteystiedot: eearyla@student.jyu.fi

Ohjaaja: Sanna Mönkölä

Työn nimi: Kiristyshaittaohjelmien toiminta ja ehkäisy

Title in English: Operation and mitigation of ransomware

Työ: Kandidaatintutkielma

Sivumäärä: 21+0

Tiivistelmä: Kiristyishaittaohjelmat ovat nykyään huomattavan yleisiä, ja ne aiheuttavat iskiessään sekä taloudellisesti että toiminnallisesti vakavia vahinkoja. Tutkielmassa tutkittiin teoreettis-kvalitatiivisella kirjallisuusanalyysillä, millaisia piirteitä nykyaikaiset kiristyshaittaohjelmat sisältävät. Löydösten pohjalta pyrittiin muodostamaan luettelo hyvistä käytänteistä. Tärkeimpinä löydöksinä havaittiin selvä riippuvuus loppukäyttäjien puutteellisen ymmärryksen ja haittaohjelmien tartuntariskin välillä; sama yhteys havaittiin myös löysästi suojattujen ja päivittämättömien järjestelmien osalta. Nykyaikaiset kiristyshaittaohjelmat ovat löydösten perusteella kryptografisilta menetelmiltään hyvin tehokkaita, joten ajantasaisten varmuuskopioiden ylläpidon tärkeys korostui. Lisäksi suunnitelmallisuuden tärkeys korostui: haittaohjelmat toimivat hyvin nopeasti, joten toimivan hätätilasuunniteman olemassaolo on ensiarvoista. Tietoverkkojen suurin roolin vuoksi korostui tarve suunnitella turvajärjestelmät siten, että haittaohjelmat eivät pääse vapaasti muodostamaan yhteyksiä keskuspalvelimiin tai leviämään tietoverkkojen kautta.

Avainsanat: kiristyshaittaohjelmat, toiminta, torjunta, ehkäisy

Abstract: Ransomware programs are very common today, and are a cause of significant economical and operational damages upon striking. In this thesis, qualitative and theoretic literature analysis was used to find out common traits of modern ransomware programs - these traits were then used to build a list of good practices for dealing with ransomware threats. Core findings include a noticeable correlation between user awareness and the risk of infection; similar correlation was found for out-of-date, poorly secured systems and risk of infection. It

was also found that modern ransomware programs tend to use highly effective cryptography, making up-to-date backups vital. The importance of preparedness is emphasized by the fact that a proper IRP (incident response plan) is highly important due to the time-sensitiveness of attacks; also, there are clear benefits for designing systems to hinder C&C (command and control) traffic and propagation of ransomware programs through computer networks.

Keywords: ransomware, operation, mitigation, prevention

Sisältö

1 JOHDANTO 1

2 KIRISTYSHAITTAOHJELMA 3

3 KIRISTYSHAITTAOHJELMIEN TOIMINTA 5
3.1 Kohteiden valikoituminen 5
3.2 Psykologinen tartuttamisstrategia 5
3.3 Kryptografia ja tiedostosalauksen tekninen toteutus 6
3.4 Maksutavat 8

4 TARTUNTOJEN EHKÄISY JA NIISTÄ PALAUTUMINEN 9
4.1 Lunnaiden maksamisen 9
4.2 Hallinto- ja suunnittelunäkökulma 9
4.3 Ihmislähtöinen näkökulma 10
4.4 Tietoverkkonäkökulma 11
4.5 Riskinhallinnallinen näkökulma 12

5 YHTEENVETO 14

LÄHTEET 16

1 Johdanto

Kiristyshaittaohjelmat (engl. *ransomware*) ovat ohjelmia, jotka arkisen määritelmän mukaisesti salaavat kovalevyltä tiedostoja ja sen jälkeen esittävät lunnasvaatimuksen tiedostojen vapauttamisesta (Mansfield-Devine 2016, sivu 9). Tämänkaltaisia haittaohjelmia on ollut jo olemassa kauan: Young ja Yung (May 1996, sivu 131) mainitsevat jo vuonna 1996 kirjoitetussa artikkelissaan useita vapaasti leviäviä ja kryptografiaa hyödyntäviä haittaohjelmia. Kryptografialla tarkoitetaan salatun viestinnän menetelmien tutkimusta ja käyttöä, mutta tässä tutkielmassa keskitytään pääasiassa erilaisten menetelmien ominaisuuksiin haittaohjelmien kannalta.

Kiristyshaittaohjelmien toiminta vaikuttaa kaikkiin keskiverroista tietokoneiden käyttäjistä suuryrityksiin. Kuten verkkorikollisuudesta yleensä, myös kiristyshaittaohjelmista on muodostunut merkittävä taloudellinen vaikutustekijä, jonka yhteydessä epäilemättä liikkuu merkittäviä rahavirtoja eri suuntiin. Mansfield-Devinen raportoiman, IBM:n tekemän tutkimuksen mukaan 2016 haittaohjelmien uhrit maksoivat yhteensä jopa lähemmäs 1 miljardin dollarin verran vaatimusrahoja (“Ransomware becomes most popular form of attack as payouts approach $1bn a year” 2017, sivu 2).

Kiristyshaittaohjelmien suosio rikollisuudessa on kasvanut hurjalla tahdilla: Intel Security havaitsi vuonna 2016 jopa 127 % kasvun kiristyshaittaohjelmahavainnoissa edelliseen vuoteen verrattuna. Trend Micro puolestaan raportoi 79 uudesta haittaohjelmaperheestä vuoden 2016 ensimmäisellä puoliskolla, verraten 29 eri perheeseen koko vuodelle 2015 (Mansfield-Devine 2016, sivu 8-9). Nykyään on saatavilla jopa ns. valmispalveluita (engl. *RaaS/Ransomware as a Service*), joiden avulla kyberrikollinen ei tarvitse merkittävää teknistä osaamista voidakseen levittää uniikkia, kustomoitua haittaohjelmaa (Cabaj ja Mazurczyk 2016, sivu 15).

Tämä tutkielma perustuu teoreettiseen, kvalitatiiviseen kirjallisuusanalyysiin pohjautuen kiristyshaittaohjelmia käsitteleviin teksteihin. Tutkimuksen pyrkimyksenä on tiivistää mielenkiintoisimmat havainnot yhteinäiseksi kokonaisuudeksi. Luvussa 2 tarkastellaan miten kiristyshaittaohjelma käsitteenä yleisesti määritellään kirjallisuudessa ja hieman niiden varhaishistoriaa. Kiristyshaittaohjelmien toimintatapoja ja teknisiä piirteitä tarkastellaan luvussa 3.

Luvussa 4 kootaan yhteen erilaisia ehdotuksia tartuntojen ehkäisemiseen ja niiltä suojautumiseen, ja pohditaan niiden toimivuutta. Erityisenä tavoitteena on yrittää kehittää jonkinlainen hyvien käytänteiden luettelo, jota seuraamalla kiristyshaittaohjelmien aiheuttama riski on tehokkaasti hallittavissa.

2 Kiristyshaittaohjelma

Kuten johdannossa mainittiin, kiristyshaittaohjelmat eivät ole uusi keksintö. Gazet (2010, sivu 78) esittelee kiristyshaittaohjelmaksi kutsuttavissa olevan ohjelma, joka on vuodelta 1989. Tämä ohjelma, ns. ”AIDS-troijalainen”, levisi postin välityksellä, ja vaikutti pintapuolisesti täysin harmittomalta AIDS-sairaudesta kertovalta opetusohjelmalta. Kuitenkin tietyn ajan kuluttua ohjelma lukitsi koneen tiedostot, ja vaati kirjallisiin lisenssiehtoihin perustuen käyttäjää lähettämään shekin Panamaan vapauttaakseen tiedostot. Tälläinen ohjelma täyttää johdannossa esitetyn määritelmän: tiedostojen salaaminen, ja lunnasvaatimus vaatimus tietojen vapauttamiseksi.

Kiristyshaittaohjelmat toimivat useimmissa tapauksissa troijalaisten tavoin, eivätkä ne tartuta tiedostoja missään vaiheessa. On kuitenkin löydetty poikkeuksia tähän sääntöön: Mansfield-Devine (2016, sivu 12) mainitsee Netskope-yhtiön tutkijoiden havainnon Virlock-haittaohjelmaperheen päivityksestä, joka toi haittaohjelmiin virusmaisia käytöspiirteitä. Havaitut ohjelmat saastuttivat puhtaat tiedostot siten että niiden avaaminen voi aiheuttaa tartunnan. Lisäksi havaittiin polymorfisuutta, ts. viruksen muoto muuttui joka kopioinnin yhteydessä, eikä niille siten voinut määrittää helposti yksittäistä hahmoa.

Ensimmäiset ns. modernit kryptografiaan perustuvat kiristyshaittaohjelmat ilmestyivät vuonna 2005, mutta niiden kryptografian taso oli varsin heikkolaatuista ja helposti purettavaa. Tyypillisesti kryptografia oli myös symmetristä, eli sama avain sekä salasi että purki tiedoston. Myös joitakin assymmetriseen (julkinen ja yksityinen avain) kryptografiaan perustuvia ohjelmia julkaistiin jo tuolloin, mutta niissä oli puutteita - esimerkiksi monella käyttäjällä jaettu, sama julkinen avain Gazet (2010, sivu 86).

Vahvempia, uniikkeja avaimia luova ja huomattavasti haastavemmin purettavia ohjelmia ilmestyi vasta myöhemmin: esim.yksi ensimmäisistä edellä mainittuja assymmetrisiä ja uniikkeja avaimia käyttävä CryptoWall 3.0 julkaistiin vuonna 2015. (Cabaj ja Mazurczyk 2016, sivu 15). Vuoden 2012 jälkeen ilmestyivät myös ensimmäiset Android-pohjaiset kiristyshaittaohjelmat, jotka esim. salaavat käyttäjän valokuvia, ja voivat vaihtaa laitteen suojakoodin painottaakseen lunnasvaatimuksiaan. (Zavarsky ja Lindskog 2016, sivu 471).

Kuten johdannossa on mainittu, arkiseen määritelmään kuuluu tiedostojen salaaminen ja niiden vapauttaminen lunnaita vastaan. Tämä määritelmä kuitenkin esim. käsittelee vain tiedostoja, joten sitä on syytä yleistää kattamaan erilaisempia haittaohjelmia.

Onkin olemassa useita hyviä tapausesimerkkejä sellaisista hyökkäyksistä, joita ei voi sovittaa arkimääritelmään helposti. Otetaan esimerkkinä tietokantahyökkäykset: MongoDB-tietokantajärjestelmät ovat viime aikoina valikoituneet haittaohjelmien uhreiksi huonosti suunniteltujen oletusasetusten takia. Joissakin MongoDB:n versioissa tietokanta on oletusarvoisesti auki mistä tahansa saapuville yhteyspyynnöille, ilman salasanasuojausta. Näin hyökkääjän on ollut helppo tunkeutua tietokantaan, turmella sen sisältö ja jättää lunnasvaatimus tilalle. (Cimpanu 2017).

Erityisen dramaattinen tapausesimerkki MongoDB-hyökkäyksestä on CloudPets-älylelujen käyttämään tietokantaan tehty hyökkäys, jota Hunt (2017) esittelee artikkelissaan. Murron yhteydessä vuoti julkiseksi suuri määrä nuorten lasten ääninauhoitteita, profiilikuvia ja tarkkoja sijaintitietoja, koska tietokantaa ei oltu suojattu oikein.

Toinen mielenkiintoinen esimerkki toiminnallisuuden lukitsemisesta löytyy Itävalloista, jossa huipputason hotellin tietojärjestelmiin tehtiin kohdistettu hyökkäys. Tämä hyökkäys lamautti täydellisesti hotellin varaus- ja korttiavainjärjestelmät, lukiten vieraat pois huoneistaan. Hotelli ei onnistunut palauttamaan järjestelmiään kuntoon omin avuin, joten hallinnon oli pakko maksaa lunnaat. Tämän jälkeen hallinto myös teki päätöksen siirtyä takaisin mekaaniseen lukitusjärjestelmään vastaavan estämiseksi. (Berghuis 2017).

Havaintojen perusteella yleistettynä käsitteenä voitaneen pitää minkä tahansa tiedon tai joskus myös toiminnallisuuden lukitsemista vastoin käyttäjän tahtoa, ja lunnaiden vaatimista sen vapauttamiseksi.

3 Kiristyshaittaohjelmien toiminta

Tässä luvussa eritellään erilaisia kiristyshaittaohjelmien toiminnallisia piirteitä. Toiminallisia piirteitä ovat kaikki kiristyishaittaohjelmien tekniset ominaisuudet joilla kiristys toteutetaan, sekä myös muut kiristyshaittaohjelmien toimintaan liittyvät käytännön ominaisuudet (esim. miten kiristäjä motivoi maksamaan lunnaat)

3.1 Kohteiden valikoituminen

Kuka tahansa voi joutua kiristyshaittaohjelman uhriksi. On kuitenkin havaittavissa tiettyjä suuntauksia siinä, ketkä ovat erityisen alttiitta kohteeksi joutumiselle.

Mansfield-Devinen raportoiman McAfeen tutkimuksen mukaan viime vuosina on voitu havaita selvä kohteenmutos yksityishenkilöistä yrityksiin, motivaationa paremppi tuottavuus hyökkääjälle. Uudet uhat kohdistuivat erityisesti pienyrityksiin, joilla on ns. laaja hyökkäyspinta (esim. paljon haavoittuvaisia, vanhentuneita ja/tai hauraita järjestelmiä), mutta vain vähän resursseja hyökkäysten torjumiseen. (Mansfield-Devine 2016, sivu 9).

Toinen rajautuvuutensa vuoksi mielenkiintoinen havaittu trendi on terveydenhuollon järjestelmien valikoituminen hyökkäyskohteiksi. Terveydenhuollon järjestelmät ovat Mansfield-Devinen mukaan valikoituneet kohteeksi seuraavista syistä: järjestelmiä ei monin paikoin ole päivitetty joko sen vaikeuden tai yksinkertaisesti investointien puutteen vuoksi, ja lisäksi järjestelmien kaatumisen aiheuttamat, potentiaalisesti hengenvaaralliset seuraamukset ovat tehokas motivaattori esimerkiksi sairaaloille. FireEye-turvallisuusyhtiö raportoi syksyllä 2016 havainneensa massiivisen hyökkäysaallon erityisesti Yhdysvalloissa, Japanissa, Koreassa ja Thaimaassa sijaitseviin terveydenhuoltoorganisaatioihin. (Mansfield-Devine 2016, sivu 9-10).

3.2 Psykologinen tartuttamisstrategia

Jotta kiristyshaittaohjelmakampanja olisi tekijöilleen tuottoisa, tekijöiden tulee saada haittaohjelmat leviämään tehokkaasti kohderyhmänsä keskuudessa. Lisäksi lunnaiden maksami-

sesta on tehtävä kaikkein houkuttelevin ja pinnallisesti järkevin vaihtoehto. Käyttäjälle on jäätävä sellainen vaikutelma, että lunnasrahojen maksaminen on ylivoimaisesti helpoin ja kivuttomin vaihtoehto.

Psykologiset menetelmät ovat yksi avain tähän: Krebs (2016) toteaa, että tehokkaan kiristysvaatimuksen on iskostettava uhriin tietty pelko arvokkaiden tietojensa menetyksestä, ja siten vakuutettava että nopealla (monesti näkyvän ajastimen tahdittamalla) lunnasrahojen maksamisella kaikki on taas ennallaan.

Krebsin ja Sullivanin mukaan jotkut toimijat suostuvat neuvottelemaan ehdoista, ja tarjoavat jopa ympäri vuorokauden verkossa toimivan teknisen tuen. Sullivan (2017) mainitsee muutamia Spora-kiristyshaittaohjelman teknisen tuen keskustelulokista löytyviä esimerkkejä, missä aikataulusta on suostuttu poikkeamaan Bitcoinien haastavan saatavuuden vuoksi. Lisäksi Sporan tekijät tarjoavat halvempia hintoja, mikäli käyttäjä haluaa purkaa salauksen vain muutamasta yksittäisestä tiedostosta. On melko selvää miksi neuvottelualttiutta on: pienempikin summa hitaammin on parempi kuin ei mitään, ja jos uhrin ”ahdistaa nurkkaan” ilman pakotietä, lunnaiden maksu voi jäädä huonoimmaksi vaihtoehdoksi.

Myös kiristyshaittaohjelmat hyödyntävät kyberrikollisuudessa muutenkin olennaista luontaista uteliaisuutta. Naamioimalla haittaohjelma joksikin kiinnostavaksi, esim. urheilutapahtumien katseluohjelmaksi tai jostakin julkisuuden henkilöstä kertovaksi vuodoksi voidaan käyttäjä houkutella lataamaan muuten kyseenalaisen oloinen ohjelma. Erinomainen esimerkki tästä on forensiikka-asiantuntija Lawrence Abramsin löytämä, sopivasti Yhdysvaltojen presidentinvaalien vaaliväittelyiden aikaan julkaistu Donald Trump -teemainen kiristyshaittaohjelma. (Mansfield-Devine 2016, sivu 11).

3.3 Kryptografia ja tiedostosalauksen tekninen toteutus

Tehokkaan kiristyshaittaohjelman piirteisiin kuuluu (assymmetrinen) julkiseen ja yksityiseen avaimeen perustuva kryptografia: kuten Cabaj ja Mazurczyk (2016, sivu 15) toteavat tutkimuksessaan CryptoWall-haittaohjelmaan liittyen, voidaan yksityinen avain jättää vain keskuspalvelimen tietoon ja välittää ainoastaan julkinen avain ennen lunnaiden maksamista. Julkiseen ja yksityiseen avaimeen nojaavissa kryptografiamenetelmissä julkista avainta

käytetään salaamisen ja yksityistä purkamiseen. Yksityistä avainta ei myöskään ole helppo päätella julkisesta avaimesta, joka tekee assymmetrisestä kryptografiasta hyvin toimivan menetelmän kiristykseen.

Assymmetriset menetelmät eivät kuitenkaan sovellu sellaisenaan isojen viestien salaamiseen, joten ns. hybridimenetelmän (useita menetelmiä päällekkäin) käyttäminen on tekijälle hyödyllistä (Young ja Yung, May 1996, sivu 133). Zavarsky ja Lindskog (2016, sivu 469) vahvistaa hybridimenetelmien todellisen hyödyllisyyden toteamalla että tutkimuksensa haittaohjelmaperheistä kaikki viimeaikaisimmat variantit käyttävät edellä mainittuja hybridimenetelmiä.

On käytännön esimerkkejä siitä, miten heikko salaus sallii salausmenetelmän toiminnan päättelyn vertaamalla salattuja tiedostoja ja niiden salaamattomia versioita keskenään. Lisäksi on löydetty tapaus, jossa heikon salausmenetelmän salausavain oli sisäänrakennettu muuttumattomaksi haittaohjelmaan, tehden purkamisesta erittäin helppoa. (Mansfield-Devine 2016, sivu 14). Lisäksi Young ja Yung (May 1996, sivu 133) ovat teoreettisesti osoittaneet, että mikäli kiristyshaittaohjelma käyttää puhtaasti symmetristä salausmenetelmää (sama avain sekä salaukseen että purkamiseen) ilman avaimen välittämistä ulkopuoliselle taholle, siitä on mahdotonta tehdä tehokasta ja pitävää.

Tyypillisesti kiristyshaittaohjelmat toimivat käyttöjärjestelmässä tiedostotasolla. Tästä yleisestä toimintamallista poikkeavat esim. Petya- ja Mamba-haittaohjelmat. Petya salaa tiedostojen sijaan suoraan NTFS-tiedostojärjestelmän päätiedostotaulukon (engl. *Master File Table*): tiedostot eivät itsessään muutu, mutta käyttöjärjestelmä ei osaa paikallistaa niitä tiedostotaulukon puuttuessa. Sophoksen havaitsema Mamba puolestaan käyttää kokolevysalausta, ja käytännössä estää kaiken muun toiminnan paitsi lunnasvaatimuksen esittämisen. (Mansfield-Devine 2016, sivu 12).

Brewer (2016, sivu 7) mainitsee kiristyshaittaohjelmien erityispiirteenä taipumuksen tarkkaan varmuuskopioiden hävittämiseen. Hänen mukaansa esim. CryptoLocker-ohjelma hävittää Windowsin integroidun varmuuskopiojärjestelmän sisällön, ja jotkut variantit myös muuten tutkivat levyn hakemistorakennetta varmuuskopioiden löytämiseksi. Näin menetellään epäilemättä siksi että käyttäjän olisi vaikeampi palauttaa järjestelmää toimintakuntoi-

seksi varmuuskopioiden avulla.

3.4 Maksutavat

Bitcoin on varsin yleinen maksutapa. Se on virtuaalinen, hajautettu kryptovaluutta (engl. *cryptocurrency*), joka perustuu julkiseen lohkoketjuun (Betancourt 2013). Bitcoinin perusominaisuuksiin kuuluvat sekä täysi jäljitettävyys että anonyymisyys: kaikki valuuttasiirrot ovat julkisesti nähtävissä ja kenen tahansa varmennettavissa, mutta ns. Bitcoin-lompakoilla ei välttämättä ole minkäänlaisia tunnistetietoja, eikä siten myöskään selkeää omistajaa (Kharraz ym. 2015, sivu 14-15).

Kharraz ym. (2015, sivu 16) ovat havainneet tutkimuksessaan, että Bitcoin-lompakoiden vaihtuvuus kiristyshaittaohjelmien käytössä on suurta. Tutkimuksen mukaan otoksen lompakoista 84.46 %:ssa oli enintään kuusi niitä koskevaa siirtoa; lisäksi 68.93 % lompakoista oli käytössä enintään 10 päivää. Tutkimuksen mukaan näihin lompakkoihin siirretyt rahat välitettiin eteenpäin kymmenien välitilien kautta, tai pilkottiin pienemmiksi osiksi ja hajautettiin. Näiden toimenpiteiden tarkoitus on hankaloittaa rahojen jäljittämistä kiristyshaittaohjelmalähtöiseksi, joka voisi johtaa tekijöiden paljastumiseen rahoja käytettäessä.

Bitcoin ei kuitenkaan ole ainoa maksutapa mitä haittaohjelmien käytössä on havaittu: lunnasvaatimuksista on havaittu esim. vaatimuksia lähettää prepaid-liittymän latauskoodi tietylle käteisarvolle tai soittaa tiettyyn (väärään) teknisen tuen numeroon Windows 10-lisenssin uusimiseksi (Mansfield-Devine 2016, sivu 9). Harva maksutapa lienee kuitenkaan yhtä anonyymi ja tunnettu kuin Bitcoin - ja se selittänee miksi nimenomaisesti Bitcoin on yleistynyt kiristyshaittaohjelmien maksuvälineenä.

4 Tartuntojen ehkäisy ja niistä palautuminen

Ehkäisy- ja palautumismenetelmät on hyvä jakaa niiden kontekstin mukaisesti: osa menetelmistä on pääosin teknisiä ja tietojärjestelmien toimintaan perustuvia, osa taas enemmän ihmislähtöisiä ja sellaisia, joita on hyvin hankalaa korvata teknologiaan perustuvilla ratkaisuilla.

4.1 Lunnaiden maksamisen

Yksi tapa palautua vahingoista nopeasti voi olla niinkin yksinkertainen kuin lunnaiden maksaminen. Kuten alaluvussa 3.2 todetaan, ehdotkaan eivät välttämättä ole kiveen hakattuja. Mansfield-Devinen raportoiman F-Securen tutkimuksen mukaan kolme neljästä ryhmästä suostui neuvottelemaan, antaen keskimäärin noin 29 % alennusta lunnaista (Mansfield-Devine 2016, sivu 16). Voi siis olla hyödyllistä yrittää neuvotella itselleen parempaa kauppaa, jolloin vahingot jäävät vähäisemmiksi ja lähinnä taloudellisiksi - olettaen että tartunnan syy kyetään selvittämään ja korjaamaan.

Edellä mainittu toimintamalli on kovasti kiistanalainen, ja sitä ei suosittele esim. Yhdysvaltojen keskusrikospoliisi FBI. FBI muistuttaa tiedotteessaan, että vaikka lunnaat maksettaisiinkin, mitään todellista takuuta tietojen takaisinsaannista ei välttämättä ole; lisäksi lunnaiden maksamisella lähettää viestiä että tälläinen rikollinen toiminta on kannattavaa. Samalla FBI kuitenkin myöntää sen, että toiminnalliset vaatimukset voivat puoltaa lunnaiden maksamista, jos vaihtoehtona on jokin sidosryhmien (esim. yrityksen osakkeenomistajat, työntekijät, asiakkaat) kannalta selvästi huonompi lopputulos. (Mansfield-Devine 2016, sivu 16).

4.2 Hallinto- ja suunnittelunäkökulma

Haittaohjelmien tartuntariskiä on syytä käyttää yhtenä systemaattisena tarkastelukriteerinä, kun suunnitellaan teknisiä järjestelmiä ja organisaation käytänteitä. Brewer (2016, sivu 7-8) toteaa, että yksi parhaista tavoista huolehtia suojauksen pitävyydestä on järjestelmien aktiivinen päivittäminen ja korjaaminen. Näin ehkäistään se riski, että järjestelmiin jäisi pitkik-

si ajoiksi korjaamattomia haavoittuvuuksia joita haittaohjelma voisi hyväksikäyttää. Brewer myös suosittelee vahvasti suojattujen varmuuskopioiden luontia ja ylläpitoa: varmuuskopioiden pitäisi mielellään olla kokonaan verkosta irrotettuja, ettei esim. pilvipalvelua tai verkkolevyä hyödyntävä haittaohjelma pysty niitä turmelemaan. Lisäksi Brewer suosittelee että järjestelmät asennetaan tartunnan jälkeen mahdollisuuksien mukaan kokonaan uusiksi, jotta järjestelmään ei jäisi toimintakykyisiä osia haittaohjelmista: hänen mukaansa haittaohjelmien jälkien täydellinen puhdistaminen voi olla varsin hankalaa. Uudelleenasennus on paljon helpompi toteutttaa ajantasaisten varmuuskopioiden avulla, joten myös siitä syystä niiden ylläpito on ensiarvoisen tärkeää.

Lisäksi Brewer (2016, sivu 8) suosittelee erityisen hätätilannesuunnitelman (engl. *IRP/incident response plan*) tekoa. Tähän suunnitelmaan kirjattaisiin täsmälliset toimenpiteet mitä hyökkäyksen sattuessa tulisi toteuttaa, jotta hyökkäys saataisiin nopeasti pysäytettyä - koska haittaohjelmat toimivat nopeasti, mikä tahansa viivästys voi pahentaa tilannetta merkittävästi.

4.3 Ihmislähtöinen näkökulma

Yhtenä hyvin yleisenä ja toistuvana teemana hyökkäyksissä näyttäisi olevan yksinkertaisesti ymmärryksen puute tietoturvallisuudesta. Mansfield-Devine (2016, sivu 14) toteaa, että merkittävä osa hyökkäyksistä hyödyntää sosiaalista manipulointia (engl. *social engineering*), toisinsanoen käyttäjien ymmärtämättömyyttä ja/tai välinpitämättömyyttä turvallisuusvaatimuksista ja toimiensa seurauksista. Hänen mukaansa tämä ymmärryksen puute on erittäin merkittävää yleisesti koko käyttäjäkunnassa että erityisesti myös liikemaailman keskuudessa. Myös Wright toteaa samaa ymmärryksen puutteesta, ja lisää että myös löysä BYOD-politiikka (*Bring Your Own Device*, omien laitteiden tuonti organisaatioon) aiheuttaa turvallisuusongelmia (Mansfield-Devine 2016, sivu 9).

On ilmeisen tärkeää huolehtia, että käyttäjät ymmärtävät millaisilla toimilla voi olla vaarallisia vaikutuksia. Käyttäjä ei esimerkiksi välttämättä aavista, että yllättävän monet sähköpostien liitetiedostot voivat olla haitallisia; alaluvussa 3.1 mainittu haittaohjelmahyökkäys toteutettiin sähköpostitse välitetyillä Word-asiakirjoilla, joihin oli sisällytetty haittaohjelma-

koodia sisältäviä makroja. Varsinkaan vanhemmat käyttäjät eivät välttämättä tule edes ajatelleeksi että harmittoman oloinen tekstiasiakirja voisi sisältää haittaohjelmakoodia. Brewer (2016, sivu 8) toteaa että erityisen koulutuksen järjestäminen käyttäjille olisi tärkeää: näin käyttäjät tietäisivät, millaisissa toimissa todennäköisemmin piilee vaara.

Ymmärryksen puute korostuu erityisesti tiukemmin suojatuissa järjestelmissä. Esimerkiksi Android-puhelimissa sovelluksille myönnetään vain tietyt oikeudet, jotka kysytään käyttäjältä ennen asennusta tai operaatioiden suoritusta; tämän tulisi teoriassa estää suuremmat vahingot, mikäli käyttäjä osaa suhteuttaa oikeudet sovelluksen käyttötarkoitukseen. Zavarsky ja Lindskog (2016, sivu 466) toteavat että kaikki tutkimuksen Android-kiristyshaittaohjelmat ensimmäisenä järjestävät itselleen suuret oikeudet, joko pyytämällä niitä suoraan tai harhautuksen kautta. Tutkimuksen Android-haittaohjelmaperheiden suuri määrä vihjaa siitä että valveutuneisuudessa on ilmeisesti myös tältä osin puutteita.

4.4 Tietoverkkonäkökulma

Nykyisistä kiristyshaittaohjelmista suurin osa leviää tietoverkkojen välityksellä. On siis aiheellista miettiä ja suunnitella, millaisia varotoimenpiteitä verkkoinfrastruktuuriin on mahdollista lisätä jotta haittaohjelmien leviäminen olisi hankalampaa.

Unisys-yhtiön turvallisuusjohtaja Tom Patterson ehdottaa mikrosegmentaatiota yhtenä verkkosuojaratkaisuna; mikrosegmentaatiossa jokaiseen IP-tason pakettiin lisätään kryptografinen allekirjoitus, jonka avulla paketin alkuperä voidaan varmentaa ja paketti välittää eteenpäin vain jos se on reitityssäännöissä sallittu. Mikrosegmentaation avulla verkkoliikennettä voidaan säädellä hyvin tarkasti, ja kiristyshaittaohjelmahyökkäykset eristää tehokkaasti vain pieneen osaan koko verkosta. (Mansfield-Devine 2016, sivu 15). Tämä epäilemättä rajoittaa hyökkäyksen vahinkoja, mutta voi vastaavasti mm. lisätä resurssivaatimuksia tehokkaan ja toimivan ratkaisun toteuttamiseen.

Cabaj ja Mazurczyk (2016, sivu 18-20) tarjoavat puolestaan ratkaisuna ohjelmamääritteisiin verkkoihin (*software-defined networking*) perustuvaa suodatusratkaisua. Toisin kuin perinteisessä tiedostosuodatuksessa, edellä mainittu menetelmä puuttuu suoraan haittaohjelman toimintaan: CryptoWall tarvitsee julkisen avaimen noutamiseen yhteyden keskuspalvelimeen.

Tämän yhteyden se muodostaa välityspalvelinten kautta. Tutkimuksen mukaan reaktiivinen DNS-suodatus on osoittautunut tehokkaaksi tätä toimintamallia vastaan: reaktiivisessa DNS-suodatuksessa jokainen ohjelman lähettämä DNS-pyyntö kopioidaan ja analysoidaan, ja mikäli taustalta paljastuu tunnettu haittaohjelmapalvelin, liikenne kohteeseen voidaan katkaista ja samalla estää julkisen avaimen vastaanottaminen.

Vaihtoehtoisesti pyynnöt voidaan myös pakottaa kulkemaan tarkistuspalvelimen kautta; jälkimmäinen vaihtoehto tosin luo pullonkaulan, jolla voi olla merkittävää vaikutusta verkon toimintanopeuteen. Ensimmäisessä ratkaisussa tätä ongelmaa ei ole, mutta toisaalta tarkistusnopeuden merkitys korosttu: mikäli palvelin on liian hidas, se ei ehdi reagoimaan ennen kuin haittaohjelma on saanut ladattua julkisen avaimen.

Cabaj ja Mazurczyk (2016, sivu 20) suosittelevat tutkimuksessaan, että tehokkaimman lopputuloksen kannalta olisi parasta suoraan puuttua välityspalvelinten toimintaan. He kuitenkin myös toteavat että DNS-pohjainen suodatus on tutkimuksessa osoittautunut riittävän tehokkaaksi salauksen estämiseksi.

4.5 Riskinhallinnallinen näkökulma

Myös riskinhallinnallinen näkökulma on tarkastelemisen arvoinen: on mahdollista että kaikki varotoimenpiteet pettävät joko puhtaan sattuman tai sitten kohdistetun hyökkäyksen kautta, ja tällöin on hyvä olla jonkinlainen keino suhteettomien vahinkojen estämiseen.

Carter (2016, sivu 33) kertoo että on kehitetty ns. kyberkiristysvakuutuksia, joiden tehtävä on kattaa kyberhyökkäyksistä koituvat kulut; näin taataan se, että vaikka hyökkäys sattuisikin niin organisaation resurssit eivät kärsi hyökkäyksestä yli kantokyvyn.

Vaikka vakuutusehdot vaihtelevatkin uutuuden vuoksi vielä suuresti, on kyberkiristysvakuutuksille yleistettävissä muutama yhteinen tekijä. Yleensä vakuutus määritellään koskevan niitä uhkatilanteita, joissa joko uhataan kyberhyökkäyksellä tai salaisen tiedon julkaisulla; joissakin tilanteissa vakuutus rajataan vain niihin tapauksiin joissa vaaditaan rahalunnaita. (Carter 2016, sivu 34).

Lisäksi kyberkiristysvakuutukset tyypillisesti sisältävät ilmoitus- ja lupavaatimuksia: vakuu-

tuksenottajan pitää ehdoissa määritellyssä ajassa ilmoittaa ainakin vakuutuksen antajalle (joskus myös viranomaisille) uhasta, ja ehdottomasti saatava lupa vakuutuksenantajalta ennen kuin mitään kuluja tuottavia toimenpiteitä tehdään. Vakuutukset ovat tyypillisesti myös jälkikorvausperiaatteella toimivia: vakuutuksenottajan on ensin itse maksettava esim. tutkimuksista ja lunnaista koituvat kulut, ja haettava vakuutuksenantajalta korvausta menoihin. Lisäksi jotkin vakuutukset maksavat korvauksia vain jos lunnasvaatimukseen on päätetty suostua, eväten korvaukset pelkkään tutkimustyöhön. (Carter 2016, sivu 34-35).

Carter lopuksi toteaakin että vaikka kyberkiristysvakuutus voikin olla hyvin arvokas apuväline tappioiden ehkäisemiseen, on yllämainituin perustein myös erittäin tärkeää ymmärtää tarkkaan mitä vakuutusehdot korvaavat ja sallivat.

5 Yhteenveto

Kiristyshaittaohjelmat ovat selvästikin nykyään hyvin monimuotoisia ja teknisesti varsin edistyneitä työkaluja. Niitä on mahdollista käyttää vaikka teknistä osaamista ei merkittävästi olisi, ja niitä käytetään myös kohdistettuihin hyökkäyksiin.

Kirjallisuuskatsauksen tulosten perusteella seuraavia hyviä käytänteitä olisi hyvä noudattaa tartunariskin vähentämiseksi, sekä torjunnan ja palautumisen tehokkuuden takaamiseksi:

- Loppukäyttäjien on ymmärrettävä vaaranpaikat käyttämiensä ohjelmien ja laitteiden kanssa. On ymmärrettävä, millaiset toimenpiteet ovat vaarallisia, ja joihin on syytä perehtyä tarkemmin jos on vähänkään epävarma. Tätä varten on syytä järjestää esim. organisaatiokohtaista koulutusta, joissa selitetään mitkä ovat oikeat käytänteet eri tilanteissa ja mitä saa/ei saa tehdä. Tämän koulutuksen pitää koskea myös esim. matkapuhelimia ja tabletteja, koska haittaohjelmia on myös niille saatavilla.
- On huolehdittava siitä, että järjestelmät ovat tärkeytensä mukaan varmuuskopioituja; lisäksi nämä varmuuskopiot on suojattava siten, ettei niiden turmeltuminen voi tapahtua vahingossa tai kiristyshaittaohjelman toimesta. Nämä varmuuskopiot voivat olla elintärkeitä hyökkäyksen sattuessa: koska nykyaikaiset haittaohjelmat tyypillisesti käyttävät vahvaa kryptografiaa ja ovat vaikeasti murrettavissa, ei voida luottaa siihen että toiminnallisuutta voitaisiin palauttaa helposti jotain muuta reittiä käyttäen.
- Tietoverkot ovat olennainen kulkukanava ja leviämisreitti kiristyshaittaohjelmille, joten niiden suojaamiseen on syytä perehtyä tarkasti. Verkkosuunnittelijan on rajoitettava verkon sisäistä liikennöintiä tarpeiden mukaiseksi, ja lisäksi rakennettava dynaamisesti reagoivia suojautumismenetelmiä. On todettu, että näillä toimenpiteillä on mahdollista hidastaa tai jopa parhaimmillaan pysäyttää alkuunsa potentiaalinen haittaohjelmahyökkäys. Myös perinteiset menetelmät puoltavat paikkaansa: esim. sähköpostisuodatus joka estää makroja sisältävien Word-dokumenttien tai suoritettavien tiedostojen vastaanottamisen estäisi yhden ison ihmislähtöisen hyökkäyskanavan
- Järjestelmällinen murtotestaus (engl. *penetration testing*) olisi esim. MongoDB:n kohdalla voinut paljastaa ammottavan tietoturvareiän. Mikään ei estä murtautujia tekemästä samaa, joten järjestelmän ylläpitäjien on syytä tehdä testausta säännöllisesti ja

varsinkin ohjelmamuutosten jälkeen.

- BYOD-politiikan on edellisten sääntöjen perusteella oltava suht tiukkaa; näin taataan että kaikki aiemmin mainitut edellytykset voivat täyttyä, ja että yhtenäistä politiikkaa noudatetaan kaikkialla eikä ns. heikkoja lenkkejä pääse syntymään. Käytännössä tämä voi edellyttää sitä että laitteisiin ohjelmisto asennetaan kokonaan uusiksi, joten mielekkyys on hyvin tilannekohtaista.
- Hyökkäykset ovat tyypillisesti varsin aikakriittisiä, joten sellaisen sattuessa on kyettävä toimimaan nopeasti ja johdonmukaisesti isompien ongelmien välttämiseksi. Kaikilla eri osapuolilla, joita hyökkäys voi koskea, on oltava ns. tarkistuslista toimenpiteistä jotka tulee tehdä hätätilanteessa. Loppukäyttäjälle tämä voi esim. tarkoittaa käskyä soittaa tiettyyn puhelinnumeroon ja informoida IT-tukea, IT-tuelle tämä voi olla esim. ohjemuistio järjestelmien riippuvaisuuksista, varmuuskopiojärjestelmän toiminnasta ja palveluista jotka on suljettava hyökkäyksen hidastamiseksi.
- Organisaation on syytä harkita kyberturvallisuusvakuutuksen hankkimista, varsinkin jos toiminalliset edellytykset ovat hyvin Internet-sidonnaisia. Sopivia vakuutuksia on tarjolla, mutta ehtojen suuren vaihtuvuuden vuoksi on tärkeää ymmärtää niiden täsmällinen soveltuvuus organisaation toimintaan.

Käytänneluettelo on muodostettu kokonaisuutena, joten sitä on myös syytä pyrkiä noudattamaan kokonaisuutena. Jos osia käytänteistä jätetään harkitsemattomasti noudattamatta, voi käydä että seuraavat ongelmat kumpuavat juuri niistä sivuutetuista käytänteistä. Esimerkiksi koulutuksen unohtaminen voi johtaa siihen että hienoinkin tietoturvajärjestelmä on hyödytön, koska käyttäjät eivät ymmärrä sen merkitystä ja toimintatapaa.

Lähteet

Berghuis, Koen. 2017. “Hotel ransomed by hackers as guests locked out of rooms”. http://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms.

Betancourt, Michael. 2013. “Bitcoin” [kielellä en]. *CTheory* (): 18/2013. https://journals.uvic.ca/index.php/ctheory/article/view/14792.

Brewer, Ross. 2016. “Ransomware attacks: detection, prevention and cure”. *Network Security* 2016, numero 9 (): 5–9. doi:10.1016/S1353-4858(16)30086-1. https://www.sciencedirect.com/science/article/pii/S1353485816300861.

Cabaj, K., ja W. Mazurczyk. 2016. “Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall”. *IEEE Network* 30, numero 6 (): 14–20. doi:10.1109/MNET.2016.1600110NM.

Carter, James S. 2016. “The Ins and Outs of Cyber Extortion Insurance Coverage” [kielellä English]. *Risk Management; New York* 63, numero 10 (): 32–35. http://search.proquest.com/docview/1854174581/abstract/CF43B13B8F16404EPQ/1.

Cimpanu, Catalin. 2017. *MongoDB Databases Held for Ransom by Mysterious Attacker.* https://www.bleepingcomputer.com/news/security/mongodb-databases-held-for-ransom-by-mysterious-attacker/.

Gazet, Alexandre. 2010. “Comparative analysis of various ransomware virii” [kielellä en]. *Journal in Computer Virology* 6, numero 1 (): 77–90. doi:10.1007/s11416-008-0092-2. http://link.springer.com/article/10.1007/s11416-008-0092-2.

Hunt, Troy. 2017. *Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages.* https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/.

Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge ja Engin Kirda. 2015. “Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks”, 3–24. New York, NY, USA: Springer-Verlag New York, Inc. doi:10.1007/978-3-319-20550-2_1. http://dx.doi.org/10.1007/978-3-319-20550-2_1.

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

Mansfield-Devine, Steve. 2016. “Ransomware: taking businesses hostage”. *Network Security* 2016, numero 10 (): 8–17. doi:10.1016/S1353-4858(16)30096-4. https://www.sciencedirect.com/science/article/pii/S1353485816300964.

“Ransomware becomes most popular form of attack as payouts approach $1bn a year”. 2017. *Network Security* 2017, numero 1 (): 1–2. doi:10.1016/S1353-4858(17)30001-6. https://www.sciencedirect.com/science/article/pii/S1353485817300016.

Sullivan, Sean. 2017. *Bitcoin Friction Is Ransomware’s Only Constraint.* https://labsblog.f-secure.com/2017/02/22/bitcoin-friction-is-ransomwares-only-constraint/.

Young, A., ja Moti Yung. May 1996. “Cryptovirology: extortion-based security threats and countermeasures”, 129–140. ISBN: 1081-6011. doi:10.1109/SECPRI.1996.502676.

Zavarsky, Pavol, ja Dale Lindskog. 2016. “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization”. *Procedia Computer Science* 94:465–472. doi:10.1016/j.procs.2016.08.072. http://www.sciencedirect.com/science/article/pii/S1877050916318221.