Selviytymisopas kiristys-haittaohjelmia vastaan

Kokemuksia kiristyshaittaohjelmista Suomessa
ja neuvoja niistä selviytymiseen

Viestintäviraston julkaisu 005/2016 J

Viestintävirasto

Sisältö

1 Kiristyshaittaohjelmat ovat kasvava kiusa

Varo kiristäjää! Kiristyshaittaohjelma ujuttautuu koneellesi salaa kuin varas yöllä, ottaa tiedostosi panttivangiksi ja vaatii lunnaita. Paras apu varovaisuuden lisäksi on huolehtia varmuuskopioista ja pitää tietoturva ajan tasalla. Ohjekoosteessa kerromme myös kansalaisten, yritysten ja organisaatioiden kokemuksista ja kohtaamisista kiristyshaittaohjelmien kanssa.

1.1 Tiedostosi on kaapattu, maksa lunnaat!

Kiristyshaittaohjelma lukitsee tiedostoja tai koko laitteen ja vaatii rahaa lukkojen avaamiseksi. "Maksa, tai ohjelma tuhoaa tiedostosi yksitellen!" Näin uhkaili Jigsaw-haittaohjelma keväällä 2016. Ohjelma vaatii lunnaita ja lupaa avata vahvalla salauksella lukitsemansa tiedostot maksamisen jälkeen. Tai muuten!

Kannattaako maksaa? Pääsääntöisesti ei. Kiristyshaittaohjelmat ovat rikollisten levittämiä, ja lunnailla rahoitetaan rikollisten toimintaa. Sekä asiantuntijat että viranomaiset suosittelevat olemaan maksamatta. Vaikka uhri päättäisikin maksaa lunnaat, ei ole mitään takeita siitä, että lunnaiden vaatija pitäisi sanansa ja vapauttaisi tiedostot. Joissakin tapauksissa rahat kelpaavat kyllä, mutta panttivankeja ei alunperinkään aiottu vapauttaa ja uhri menettää tiedostonsa.

1.2 Mistä haittaohjelma tulee koneelle?

Haittaohjelmat tarttuvat tietokoneisiin, mobiililaitteisiin ja muihin verkkoon kytkettyihin järjestelmiin. Syyllinen saattaa olla sähköpostin mukana tullut liitetiedosto, joka lataa koneelle vahingollista sisältöä. Tai ilkeä tihulainen tulee epämääräiseltä sivustolta ajattelematttomasti klikatun linkin takaa. Joskus syypää voi olla tutussakin sivustossa, jonka käyttämä julkaisualusta on vanhentunut ja murtautuja on ujuttanut sinne ikävyyksiä. Tapoja on monia, mutta niitä vastaan voi suojautua.

1.3 Varmuuskopiot ja päivitykset ajan tasalle

Tärkeintä on pitää järjestelmän ohjelmistopäivitykset ja tietoturvaohjelmisto ajan tasalla. Myös sähköpostiliikenteestä kannattaa suodattaa haitallinen sisältö. Office-liitetiedostoista kannattaa kytketä makrokomentojen suorittaminen pois päältä. Erityisesti kiristyshaittaohjelmia vastaan on syytä suojautua huolehtimalla tiedostojen ja järjestelmän säännöllisestä varmuuskopioinnista.

Esimerkiksi Windows-järjestelmän automaattiset tietoturvapäivitykset auttavat pitämään tietoturvariskit kurissa. Kaikista ohjelmistoista ja järjestelmistä paljastuu säännöllisesti haavoittuvuuksia, joita haittaohjelmat käyttävät hyväkseen. Päivityksillä korjataan tietoturva-aukkoja ja parannetaan turvallisuutta myös kiristyshaittaohjelmia vastaan.

1.4 Kuka näitä inhotuksia levittää ja miksi?

Haittaohjelmien levittäminen on rikollista ja sillä tavoitellaan taloudellista hyötyä. Rikos ei kannata, jos siitä jää kiinni eikä lunnaita makseta. Silti Suomessakin moni maksaa rikollisten vaatimia summia saadakseen tiedostonsa takaisin, vaikka lopputulos onkin epävarma. Aina vaihtoehtoja ei ole, jos ongelmiin ei ole varauduttu varmuuskopioilla.

Maailmalla kiristyshaittaohjelmien tekeminen on merkittävää rikollista liiketoimintaa. Viime vuonna lunnasmäärät nousivat satoihin miljooniin euroihin ja tänä vuonna uskotaan miljardin euron rajan rikkoutuvan. Haittaohjelmabuumi ei näytä olevan ainakaan vähentymässä, joten valistusta ja suojautumista tarvitaan niin kodeissa kuin organisaatioissakin.

1.5 Haittaohjelmilla on monet kasvot

Ilmiö tunnetaan kaikkialla maailmassa. Kiristyshaittaohjelmat aiheuttavat mer-

kittävää vahinkoa kaikkialla, missä on verkkoon kytkettyjä laitteita. Erilaisia kiristäjiä on aktiivisesti liikkeellä satoja erilaisia ja ne käyttäytyvät eri tavoin. Tekijät muuntelevat ohjelmiaan säännöllisesti välttääkseen virustorjuntaohjelmien tutkat ja muut turvasuodattimet.

Useimmat nykyaikaiset kiristyshaittaohjelmat vaativat lunnaat Bitcoin-valuutassa, koska se on helppoa verkossa ja anonyymisti. Bitcoin-rahasiirtoja ei voi seurata eikä jäljittää, joten tekijät saavat rahat pidettyä piilossa. Jotkut haittaohjelmat osaavat jopa tunnistaa laitteeseen tallennetun Bitcoin-lompakon ja varastaa sinne tallennetut rahat.

1.6 Miten kiristyksestä voi selvitä?

Jos kaikesta varovaisuudesta huolimatta kiristyshaittaohjelma kaappaa tietosi ja vaatii lunnaita, toivottavasti varmuuskopiot ovat ajan tasalla. Joissakin tapauksissa kiristäjiä vastaan on olemassa purkutyökaluja, jolla kiristyshaittaohjelman salaamat tiedostot voidaan palauttaa ja salaus purkaa. Jos salaus on tehty huolimattomasti tai jos haittaohjelmaan itseensä on lipsahtanut haavoittuvuuksia, uhrin voi saada vapaaksi maksamatta lunnaita.

Viestintävirasto julkaisi heinäkuussa sarjan Tietoturva nyt! -artikkeleita, joissa kerrottiin kiristyshaittaohjelmatapauksista, niistä selviytymisestä ja niihin varautumisesta. Pyysimme lukijoita kertomaan meille omista kokemuksistaan.

1.7 Lisätietoja

Iskikö kiristyshaittaohjelma? Varaudu ja iske takaisin! (Tietoturva nyt! 26.5.2016)

Locky-kiristyshaittaohjelma on palannut lyhyeltä tauolta (Tietoturva nyt! 28.6.2016)

Kiristyshaittaohjelmat rantautuivat Android-puhelimiin (Tietoturva nyt! 1.12.2015)

Haittaohjelma tarttuu, vaikka et klikkaisi mitään - osa 1 (Tietoturva nyt! 17.9.2015)

TeslaCrypt-kiristyshaittaohjelmasta löytyneet viat voivat helpottaa tietojen palauttamista (Tietoturva nyt! 27.1.2016)

Web-palvelimia uhkaavan kiristyshaittaohjelman salaus voidaan purkaa lunnaita maksamatta (Tietoturva nyt! 10.11.2015)

[Teema] Älä panikoi, näin pääset eroon haittaohjelmasta (Tietoturva nyt! 13.10.2014)

Got ransomware? These tools may help (InfoWorld 29.4.2016)

Ransomware is now the biggest cybersecurity threat (ZD Net 6.5.2016)

Ransom Aware: Kaspersky Lab Detected a 14% Increase in New Ransomware Modifications in Q1 2016 (Kaspersky lab 5.5.2016)

Ransomware Overview (Google docs) – luettelo kiristyshaittaohjelmista ja niiden vaikutuksista.

Ransomware-katsaus (15.5.2014, huomaa päiväys!)

2 Vieraskynä: Kyber-rikollisuus ei kannata

Varhaiset kiristyshaittaohjelmat esittivät poliisia, mutta olivat oikeasti rosvoja. Uhkailu oli perätöntä. Nykyään lunnastroijalaiset kertovat suoraan ottaneensa panttivankeja ja vaativat niistä rahaa. Rikollinen bisnes tekee rumaa jälkeä myös tietoverkoissa.

2.1 Haittaohjelmaan ei voi luottaa

Suurin osa tietokoneita kiusaavista haittaohjelmista on kyberrikollisten tekemää. Rikollisilla on taloudelliset motiivit, ja lunnaiden vaatiminen on tehokas ja yksinkertainen tapa saada rahaa. Kiristyshaittaohjelmat tai lunnastroijalaiset (ransomware) ovat ehkä tuottavin liiketoimintamalli kyberrikollisten maailmassa juuri nyt. Niiden liikevaihto lasketaan sadoissa miljoonissa euroissa.

Tämä malli ei ole uusi. Varhaisimmat kiristyshaittaohjelmat ilmestyivät jo 2000-luvun alussa. Varsinainen kultaaika alkoi 2013 kun mm. Browlockniminen haittaohjelma levisi maailmanlaajuisesti. Kyseessä oli ns. poliisikiristyshaittaohjelma (police ransomware). Se yritti pelotella uhria väittämällä, että hän on jäänyt kiinni rikoksesta. Väitetty rikos oli usein ikävästi leimaava, kuten lapsipornon hallussapito. Uhria peloteltiin viranomaisten logolla sekä pitkällä vankeustuomiolla. Uskottavuutta lisäsi vielä uhrille näytetty hänen oma IP-osoitteensa ja maantieteellinen sijaintinsa.

Säikäytetylle uhrille tarjottiin onneksi vankilatuomiota kätevämpi keino päästä pälkähästä. Tapauksen sai sovittaa muutaman sadan euron tai dollarin suuruisella "sakolla". Maksu tapahtuu käyttämällä esimerkiksi Paysafecard-, MoneyPak-, MoneyGram-, UKash- tai Western Unionin rahasiirtopalveluita. Nämä Suomessa melko tuntemattomat palvelut toimivat ostamalla koodi tarvittavalle summalle. Koodi voidaan lähettää verkossa ja rahat sai nostaa missä päin maailmaa tahansa jopa ilman henkilöllisyyden tarkistusta. Tällaista rahasiirtoa ei voi peruuttaa jälkikäteen, mikä tietenkin sopii mainiosti rikollisille.

2.2 Panokset kovenevat

Harvinaisempi muunnelma poliisikiristyshaittaohjelmasta toi mukanaan oikeita lapsipornokuvia ja tallensi niitä uhrin tietokoneen levylle. Syytös hallussapidosta piti siis teknisesti paikkansa, vaikka vika ei ollut käyttäjän. Voisi olla vaikeata puolustautua, jos tällainen kone joutuisi viranomaisten tutkittavaksi.

Vuonna 2014 sattui kaksi erittäin ikävää kiristyshaittaohjelmiin liittyvää kuolemantapausta. 17-vuotias autistinen opiskelija hirttäytyi Britanniassa saatuaan kiristyshaittaohjelman. Romanialainen mies hirtti itsensä ja 4-vuotiaan poikansa samasta syystä. Hän kertoi teon motiivista itsemurhaviestissä. Mies tiesi olevansa syytön, mutta pelkäsi viranomaisten todella syyttävän häntä perusteettomasti. Lunnaisiin ei ollut rahaa eikä hän halunnut, että poika joutuu elämän häpeällisesti tuomitun pedofiilin lapsena.

2.3 Vahva salaus ei jätä vaihtoehtoja

Vuonna 2015 kiristyshaittaohjelmamarkkinat mullistuivat. Poliisi-aiheiset huijaukset väistyivät ja tilalle tulivat salakirjoittavat kiristyshaittaohjelmat (crypto ransomware). Näiden toimintaperiaate on täysin erilainen. Haittaohjelma salakirjoittaa käyttäjän tiedostot ja lupaa purkaa salauksen maksua vastaan. Uhrille ei jää muita vaihtoehtoja kuin palauttaa varmuuskopiot, menettää tiedostonsa tai maksaa vaadittu summa. Joissakin haittaohjelmistoissa salakirjoitus toimi huonosti ja sen sai purettua tarkoitukseen tehdyllä työkalulla.

Rikollisten liiketoimintamalli muistuttaa hämmästyttävän paljon tavallista laillista liiketoimintaa. Asiakkaalle myydään palvelua jota hän todella tarvitsee. Salatut tiedostot voivat olla hyvinkin arvokkaita. Tarjottu salauksen purkupalvelu toimii, ja asiakas saa siis sen palvelun

mistä hän maksaa. Palvelun ostoprosessi on tehty mahdollisimman helpoksi. Jotkut haittaohjelmat tarjoavat palveluita eri kielillä. Monella ohjelmalla on jopa tukipalvelu, johon voi ottaa yhteyttä ongelmatilanteissa. Erityinen haaste on Bitcoin-maksu, joka on tekninen ja monelle tuntematon. Tärkein ero lailliseen liiketoimintaan on, että kiristyshaittaohjelmien tekijät ovat itse aiheuttaneet ongelman, johon he myyvät ratkaisua.

Näiden tekijöiden yhteisvaikutuksesta syntyy maine. Haittaohjelman uhri kääntyy usein Googlen puoleen selvittämään onko kyseessä huijaus, vai saako todella tiedostot takaisin maksamalla? Netistä löytyy runsaasti tarinoita onnistuneista palautuksista. Tämä on elintärkeätä kyberrikollisten liiketoiminnan jatkuvuuden kannalta.

2.4 Kyberkaapattu auto, hissi tai lentokone?

Salakirjoittavien kiristyshaittaohjelmien yksi heikko kohta on kiinteä hinnoittelu. Hinta on yleensä parinsadan ja tuhannen euron välissä, mutta datan määrä tai arvo ei siihen vaikuta. Yksikin saastunut työasema yritysverkossa voi salakirjoittaa useita teratavuja verkkolevyillä, mutta troijalainen saattaa silti pyytää vain yhden bitcoinin purkutyökalusta. Lähitulevaisuudessa voidaan odottaa kehitystä lunnashinnoittelussa. Dynaaminen hinnoittelu voi ottaa huomioon salakirjoitettujen tiedostojen määrän ja laadun varmistaakseen, että purkupalveluista saadaan optimaalinen tuotto.

Pidemmällä tähtäimellä saatamme nähdä IoT-kiristystroijalaisia. Esineiden internet on kuuma puheenaihe ja halpojen laitteiden turvataso on usein huono. Monissa laitteissa on haavoittuvuuksia, joiden kautta laitteen saa haltuun tai sen voi saastuttaa haittaohjelmilla. Motiiveista hyökätä IoT-laitteisiin puhutaan vähemmän. Hyökkäykset jäävät harvinaiseksi ilmiöksi, ellei niihin keksitä ansaintamalleja. Laitteen lukitseminen ja lunnaiden vaatiminen voisi olla yksi tällainen malli.

Kuvittele, että auto ei käynnisty ja sen näytölle ilmestyy kiristysviesti. Pitää käydä netissä ja maksaa parisataa euroa ennen kuin auton saa takaisin käyttöönsä. Kiireinen saattaa mieluummin maksaa lunnaat kuin hinauttaa auton korjaamolle.

2.5 Lisätietoja

A Short History & Evolution of Ransomware (KnowBe4 2016/5)

Ransomware: Past, Present, and Future (Cisco Talos Intel 11.4.2016)

Ransomware's history and evolution in facts and figures (Kaspersky 22.6.2016)

The Rapid Evolution of Ransomware in the Enterprise (Security Week 2.5.2016)

Links Found Between Different Ransomware Families (Security Week 12.4.2016)

Kirjoittaja Mikael Albrecht työskentelee tietoturva-asiantuntijana F-Secure Oyj:ssa

3 Vieraskynä: Kiristyshaittaohjelmia HUS:n työasemissa

Kiristyshaittatapaukset ovat vuonna 2016 yleistyneet sairaaloissa ympäri maailmaa eikä Suomikaan ole tässä asiassa poikkeus. Mediassa on uutisoitu kevään aikana lunnastroijalaisten hyökkäyksistä mm. Helsingin ja Uudenmaan sairaanhoitopiirin tietoverkossa.

Keväällä 2016 muutama kiristyshaittaohjelma läpäisi HUS:n virustorjunnan ja sähköpostisuodatuksen. Kevään aikana työasemia on saastunut yhteensä neljä. Haittaohjelmat tulivat normaalin nettiselailun tai sähköpostin liitetiedoston mukana. Haittaohjelma saattoi piileksiä esimerkiksi sähköpostiviestiin liitettynä tekaistuna lähetyslistana.

Levyjä salakirjoittava kiristyshaittaohjelma havaitaan yleensä hyvin nopeasti. Käyttäjät ottavat herkästi yhteyttä palvelupisteeseen ja tapauksen selvitys alkaa usein jo ennen valvontajärjestelmän hälytystä.

3.1 Haittaohjelmaan reagoidaan nopeasti

Kevään haittaohjelmatapauksissa kiristyshaittaohjelma salasi käyttäjän oikeuksilla työaseman hakemistot sekä käyttäjälle luovitetut levyjaot. Kun tapaus tulee esille, ensimmäisenä tehtävänä on selvittää, mikä työasema on saastunut ja minkä käyttäjän tunnuksilla levyt on salakirjoitettu. Kun nämä on selvitetty, voidaan käyttäjän työasema asentaa uudelleen ja tehdä luettelo varmuuskopioilta palautettavista levyalueista. Jos palautettavaa tietoa ei ole paljon, toimet ovat ohi vielä samana päivänä. Jos käyttäjällä on laajoja oikeuksia, voi tiedostojen palautus kestää useita päiviä. Kaikkein tärkeintä on pitää varmuuskopiot ajan tasalla.

3.2 Lunnaita ei pidä maksaa

Potilastietoja ja henkilöstötietoja säilyttävät tietojärjestelmät ovat HUS:ssa erillään käyttäjien työasemista ja levyjaoista, joten tyypillinen kiristyshaittaohjelma ei niihin pääse käsiksi. Tavallisilla levyillä säilytetään tyypillisesti erilaista normaaliin toiminnan järjestämiseen liittyvää materiaalia, joten kiristyshaittaohjelmat voivat hetkellisesti haitata sairaalan tehokasta toimintaa. HUS:n kohtaamissa kiristyshaittaohjelmatapauksissa potilasturvallisuus ei ole ollut vaarassa eikä lunnaita ole maksettu.

Kevään kiristyshaittaohjelmatapausten jälkeen HUS on kiristänyt sisään tulevan sähköpostin tarkastuksia haittaohjelmien varalta. Sähköpostisuodatuksen tiukentamisen jälkeen haitalliset lunnastroijalaiset eivät ole päässeet tärvelemään tiedostoja. Haittaohjelmasuodatus raportoi silti edelleen säännöllisesti tunkeutumisyrityksistä.

3.3 Lisätietoja

Verkkorikolliset tunkeutuvat sairaalan verkkoon, lukitsevat tiedostoja ja vaativat rahaa – Ovatko tietoni turvassa? (Yle 29.5.2016)

Vieraskynä-artikkelin on tuottanut HUS:n tietohallinto

4 Suomi kertoo: Kiristystä, kiusaa ja ylimääräistä työtä

Viestintävirasto kysyi kokemuksia kiristyshaittaohjelmista. Puolet vastaajista kertoi törmänneensä kiristyshaittaohjelmiin, onneksi harvempi oli päätynyt kiristyksen uhriksi. Tilanteista selviää varmuuskopioinnin, virustorjunnan ja sähköpostin suodatuksen avulla. Myös käyttäjäoikeuksien järkeistäminen ja koulutus osoittautuivat tehokkaiksi suojautumiskeinoiksi.

Viestintävirasto kyseli kesä-heinäkuussa 2016 suomalaisten kokemuksia kiristyshaittaohjelmista. Kyselyyn tuli 111 vastausta, joista 71 % yrityksiltä ja organisaatioilta. Noin puolet vastaajista kertoi kohdanneensa itse kiristyshaittaohjelmia ja 36 % jääneensä kiristyksen uhriksi. Onneksi suurin osa kiristyksen uhreista oli selvinnyt tilanteesta varmuuskopioilla tai muilla keinoilla ja vain kolme kertoi maksaneensa haittaohjelman vaatimat lunnaat. Lunnaita maksettiin virtuaalivaluutalla ja summa vaihteli 500 ja 1000 euron välillä.

Haittaohjelmien uhrien kokemuksia:

- *Haittaohjelma pääsi yrityksen verkkoon ja salasi verkkolevyiltä tuotekehitysmateriaalia. Onni onnettomuudessa, että vain muutamaa tiedostoa oli muokattu edellisen yön varmuuskopioinnin jälkeen. Kaikki muu saatiin palautettua varmuuskopioilta.*
- *Yksittäisiä tartuntoja, ei onneksi päässyt laajentumaan työasemaverkkoon. Nopean hälytyksen avulla saastuneet koneet saatiin eristettyä ja siivottua.*
- *Käyttäjämme klikkasi huijauslinkkiä älypuhelimella ja kiristyshaittaohjelma lähti latautumaan! Onneksi silloinen ohjelma ei toiminut iPhonessa.*

"Virus oli niin tuore, että virustutkamme ei aamupäivällä tunnistanut sitä. Testasimme uudelleen iltapäivällä, jolloin virus jo jäi kiinni."

Virustorjunta pysäyttää haitakkeen — useimmiten

Usein virustorjunnasta on apua, mutta sekään ei aina yksin riitä. Kiristyshaittaohjelmia tehtaillaan ja muunnellaan päivittäin useita erilaisia, jotta virustorjuntatietokannat eivät pysyisi niiden perässä.

- *Palomuuriohjelmisto on hälyttänyt joka kerta eikä kiristyshaittaohjelma ole päässyt läpi.*
- *Ensimmäiset kryptologger-tartunnat pääsivät ajantasaisen virustorjunnan läpi. Myöhemminkään virustietopäivitykset eivät ole saaneet kaikkea kiinni.*
- *"Poliisi"-kiristysohjelma tarttui kotona ja lukitsi koneen. Käyttämäni virustorjunta ei pystynyt poistamaan haittaohjelmaa, mutta verkosta löytyi vinkki toiseen tuotteeseen, jonka ilmaisversio korjasi tilanteen.*
- *Useita tapauksia: TeslaCryptiä, Lockyä, Cerberiä, jne. Onneksi virustorjunta on keskeyttänyt kaikki haittaprosessit ennen kuin tiedostoja on tuhottu.*
- *Virus oli niin tuore, että virustutkamme ei aamupäivällä tunnistanut sitä. Testasimme uudelleen iltapäivällä, jolloin virus jo jäi kiinni.*
- *Suojausohjelma pysäytti kiristäjän eikä vahinkoa päässyt syntymään.*

"Jos maksaa lunnaat, saa entistä hanakammin lisää ja kalliimpia ransomware-hyökkäyksiä.

Yritysverkon riskit moninkertaiset

Eniten vahinkoa kiristyshaittaohjelmat saavat aikaan yritysverkoissa. Kun lunnastroijalainen pääsee valloilleen käyttäjän koneella, sillä on kaikki käyttäjän oikeudet ja pääsyvaltuudet yrityksen verkossa. Siksi tietohallinnossa kannattaakin pitää huoli verkon segmentoinnista ja käyttövaltuuksien riittävästä rajaamisesta. Liian suurilla oikeuksilla haittaohjelmakin pääsee tekemään tuhojaan tarpeettoman laajalle. Huonolla tuurilla menetetään samalla yhteisen verkkolevyn jaetut aineistot ja vielä varmuuskopiotkin.

- *Kiristyshaittaohjelma iski sairaalan tietojärjestelmään. Korjaus saattaa viedä jopa päiviä ja haitata suoraan erikoissairaanhoitoa. Kun kaikkia tietojärjestelmiä ei voida käyttää, sairaala toimii pienemmällä teholla. Myös tietohallinnolla olisi muutakin tekemistä kuin siivota jonkun ilkimyksen tihutöitä.*
- *ICT-palveluntoimittajalle kiristyshaittaohjelmatapaukset ovat jokapäiväisiä. Niistä aiheutuu kustannuksia ja pahimmillaan myös ongelmia, jos varmuuskopioita ei ole. Lunnaiden maksajiakin on – jopa toistuvasti! Liiketoiminnalle koituu silti merkittäviä kustannuksia, maksoi lunnaat tai ei. Jos maksaa lunnaat, saa entistä hanakammin lisää ja kalliimpia ransomware-hyökkäyksiä.*

"Aiheutti aivan hirveästi ylimääräistä työtä!"

Kiusaa, vaivaa ja ylimääräistä työtä

Vaikka lunnaita ei tarvitsisi maksaa, haittaohjelman siivoaminen aiheuttaa aina ylimääristä työtä, vaivaa ja kustannuksia. Yrityksen verkossa jyllääväl haitake saattaa katkaista monien työntekijöiden päivätyöt, kun tarvittavat sovellusohjelmat eivät toimi. Arvokasta työaikaa kuluu kaikilta, kun tietohallinto selvittää ja korjaa asiaa.

- *Tartunta tuli viattoman oloiselta blogisivustolta murretun Wordpressin kautta päivittämättömän flash playerin avulla. Salauskiristyksen vangiksi jäi yksi työasema, yksi verkkohakemisto ja osa jaetusta verkkolevystä, johon oli rajoittamattomat kirjoitusoikeudet. Illalla iskenyt tuholainen huomattiin aamulla, kun verkkosovellukset eivät toimineet. Selvittelyyn ja korjauksiin meni usean henkilön työpäivä.*
- *Otettiin saastunut kone pois verkosta ja palautettiin tiedostot varmuuskopioista. Aiheutti aivan hirveästi ylimääräistä työtä!*
- *Vaikka varmuuskopiot saa palautettua, siinä menettää puolen päivän työt.*

"Varmuuskopion ongelma pakotti maksamaan lunnaat. Toivottavasti tämä ongelma ei tule toistumaan."

Varmista varmuuskopioiden toiminta!

Tepsivin suoja jo iskenyttä lunnastroijalaista vastaan on toimiva varmuuskopiokäytäntö. Ajantasaisilta varmuuskopioilta palautetut tiedot minimoivat haittaohjelmien aiheuttamat vahingot. Parhaassa tapauksessa menetetään vain aivan viimeisimmät muutokset tiedostoihin. Varmuuskopioista on apua vain, jos ne toimivat oikein eikä niiden päälle voi normaalisti kirjoittaa. Varmuuskopiokäytäntöä on hyvä testata säännöllisin väliajoin.

- *Sama asiakas sai vuoden aikana neljä kertaa tartunnan saman sarjan haittaohjelmasta. Onneksi varmuuskopiot ovat aina toimineet ja maksimissaan on menetetty vain tuntien työ.*

- *Ajantasaiset varmuuskopiot antavat suojaa kiristyksiä vastaan. Täytyy vain muistaa varmistaa myös mobiililaitteet sekä mobiiliverkon että WLAN-verkon ylitse.*
- *Tartunnan saatuamme noudatimme palveluntarjoajan ohjeita. Ajantasaiset varmistukset pelastivat tietojen menetykseltä. Olemme lisänneet tiedotusta ja koulutusta entisestään.*
- *Varmuuskopion ongelma pakotti maksamaan lunnaat. Toivottavasti tämä ongelma ei tule toistumaan.*
- *Suojaus oli puutteellinen, joten yksi kone saastui. Windows-koneen toimialueella ei ollut virustorjuntaa, joten kaikki jaetut tiedostot menivät myös. Varmuuskopiot olivat pilvessä suoraan kirjoitettavissa, joten nekin menivät! Onneksi tiedot sai vielä palautettua pilven varjosta (shadow copy).*

"Haittaohjelma tapauksesta ei selvitty. Kone oli muutenkin jo vanha."

Suodata ohjelmat ja makrot sähköpostista

Tavallisimmin kiristyshaittaohjelma yrittää päästä koneelle sähköpostien liitteiden avulla. Liitetiedostoja kannattaa lähestyä varoen ja useissa yritysverkoissa suoritettavat liitteet pysäytetään sähköpostisuodattimiin. Myös Office-dokumenttien makrokoodit kannattaa kytkeä pois päältä kaikista verkon kautta ladatuista tiedostoista.

- *Roskapostisuodatus poistaa sähköpostiliikenteestä kaiken suoritettavan ohjelmakoodin sekä makroja sisältävät dokumentit. Vain salasanasuojatut zip-tiedostot päästetään läpi. Turvatoimet ovat pitäneet, mutta suurin ansio on hyvin valistetuissa käyttäjissä.*
- *Pahimman hyökkäyskampanjan aikana olemme myös estäneet web-mail-palvelujen käytön, jotta liitetiedostot eivät pääse valvomattoman sähköpostipalvelimen läpi.*
- *Yhteiskäyttöisille sähköpostitunnuksille tulee paljon roskapostia ja muuta, joiden osalta ei osata olla niin tarkkoja.*

Vain tarpeelliset oikeudet ja levyjaot

Yritysverkkoon saattaa unohtua kaikenlaisia vanhojakin levyjakoja, joiden tarkoitusta kukaan ei oikein enää muista. Kaikista levyjaoista ja niiden käyttäjistä ja oikeuksista on hyvä pitää kirjaa, jotta niitä voidaan tarvittaessa poistaa ja lisätä hallitusti. Oikeuksia ei kannata jakaa tarpeettomasti vain "varmuuden vuoksi".

- *Tartunnan saaneiden koneiden käyttäjillä oli liian laajat oikeudet yhteiselle verkkolevylle.*
- *Lopputuloksena koneen normaalin käyttäjätunnuksen oikeuksia rajattiin.*
- *Ensimmäinen versio osasi kryptata vain käyttäjälle mapattuja verkkolevyjä, mutta seuraava versio osasi jo etsiä kaikkia avoimia jakoja. Todella veemäisiä viruksia!*

"Ei yhtään kiristyshaittaohjelmatartuntaa. Jotakin on selvästi tehty oikein."

Kouluta, tiedota, panosta verkonvalvontaan

Niin yritysverkoissa kuin kotonakin asianmukaisesti koulutettu käyttäjäkunta on paras turva kiristyshaittahyökkäyksiä vastaan. Myös nykyaikaiset torjuntatekniikat auttavat selviytymään ongelmista jo ennen niiden syntymistä.

- *Henkilöstön koulutukset, sisäinen tiedotus, parantuneet prosessit ja uudet teknologiat auttavat pitämään kiristyshaittaohjelmat kurissa. Perin-*

teinen virustorjunta on auttamatta jäljessä, joten otimme käyttöön sandboxingin ja uuden sukupolven palomuurit (NGFW).

- *Lähes 500 työntekijän organisaatiomme on selvinnyt hienosti, kun ainuttakaan kiristystapausta ei ole raportoitu. Ilmeisesti HAVARO-valvontapalvelu ja VY-verkon haitta-ohjelmien suodatuspalvelu IRHS ovat auttaneet pitämään tuholaiset kurissa.*
- *Järjestelmässämme on tuhansia työasemia eikä yhtään kiristyshaittaohjelmatartuntaa. Jotakin on selvästi tehty oikein.*

Uhri ei ole syyllinen

Aina ei uhri ole yhtä onnekas, tietoja ei saa takaisin eikä välttämättä edes lunnaiden maksu auta. Varhaisilla kiristysohjelmilla oli tapana syyllistää uhriaan väittämällä käyttäjän tehneen jotakin väärää.

- *Erityisesti 2014–2015 puhdistimme paljon haittaohjelmia asiakkaidemme koneista. Monet asiakkaat olivat häpeissään tapahtuneesta, uskottiinhan tartuntojen tulevan "arveluttavilta" sivustoilta. Varmasti moni oli jättänyt hakematta apua sen vuoksi.*
- *Käytännössä hyökkääjän infra oli niin kelvotonta, ettei luvattu tiedostojen palautus olisi mitenkään toiminut vaikka lunnaat maksaisi.*
- *Haittaohjelmatapauksesta ei selvitty. Kone oli muutenkin jo vanha, joten hankimme ja asensimme uuden, mistä aiheutui ylimääräistä työtä. Tietojen palautus ei ollut vaivan arvoista, joten ne menetettiin.*

5 Vieraskynä: Poliisin matkassa Revetonin perässä

"Maksoin sen halvatun sakon, poistakaa lukitus ennen kuin muija tulee kotiin!" Näillä sanoilla alkaneesta puhelusta käynnistyi poliisina esiintyneen Reveton-kiristyshaittaohjelman tutkinta Suomessa neljä vuotta sitten. Vieraskynä-artikkelissa poliisi jäljittää haittaohjelmaa.

5.1 Reveton tulee kylään

Oli keskiviikko ja kello lähestyi neljää iltapäivällä Itä-Uudenmaan poliisilaitoksella. Vapaapäivät odottivat ja olin jo lähdössä, kun puhelin soi. Tunnekuohussa oleva mieshenkilö kiroili ankarasti ja vaati koneensa lukituksen avaamista: "Maksoin sen halvatun sakon, poistakaa lukitus ennen kuin muija tulee kotiin!"

Soittajan tietokone oli lukittu ja ruudulla vaadittiin sadan euron sakkomaksua poliisin nimissä. Kuulimme tästä haittaohjelmasta ensimmäistä kertaa. Puhelun jälkeen soitin nykyiseen Kyberturvallisuuskeskukseen, KRP:lle ja F-Securelle. Kukaan ei tuntenut menossa olevaa ransomware-kampanjaa. Oltiin "etupellossa". Vapaapäivät saivat odottaa.

5.2 Ongelman laajuus alkoi paljastua

Tietokone tutkittiin. Koneesta löytyi myöhemmin Revetoniksi nimetty haittaohjelma. Vaikka haittaohjelma oli koneen haltijalle vähintäänkin kiusallinen, se ei lukitsemisen lisäksi tehnyt muuta vahinkoa tietosisältöön. Ohjelmaan oli rakennettu toiminne lukituksen avaamiseksi, mutta se oli kytketty pois päältä. Rikolliset eivät edes halutessaan voineet poistaa lukitusta, vaikka uhri maksaisi lunnaat.

Poliisi, Viestintävirasto ja F-Secure tiedottivat asiasta yhtä aikaa, jotta tieto haittaohjelmasta tavoittaisi mahdollisimman monen. Tiedotuksella pyrittiin myös avustamaan rikoksen uhriksi joutuneita ja minimoimaan rikosvahinko. Euroopasta saamamme tiedon mukaan samanlaisen haittaohjelman uhrien määrä oli nopeassa kasvussa.

5.3 Vanhat keinot oli korvattava uusilla

Tutkinnassa kaikki jäljet johtivat ulkomaille. Aluksi rikollisryhmiä näytti olevan yksi. Palvelin toimi sellaisessa maassa, jota ei tunnettu nopeasta toiminnasta kyberrikosten selvityksissä. Rikolliset tietävät nämä maat ja niiden palveluntarjoajat vähintään yhtä hyvin kuin viranomaiset.

Kiristyksen uhrin piti ostaa "sakkomaksua" varten prepaid-maksukortti, kuten R-kioskin myymä PaySafe. Uhrin piti kioskilla tallettaa kortille lunnassumma ja lähettää sitä vastaava siirtokoodi rikolliselle. Rikolliset myivät saamansa PaySafe-koodit rikollisilla foorumeilla. Rahoja nostettiin ympäri maailmaa pienissä erissä. Maksukoodin käyttäjä ei välttämättä tiennyt mitään niiden alkuperästä.

Kansainvälinen esitutkintayhteistyö ei ehtinyt kunnolla käynnistyä, kun tuottoisa toimintamalli oli jo monistunut useamman rikollisryhmän käyttöön. Ransomware-ilmiötä oli enää mahdotonta pysäyttää. Haittaohjelman toiminta muuttui ja tiuhaan tahtiin syntyneet uudet versiot hämäsivät virustorjuntaa. Lukituksen avaamiseen apua pyytävien kansalaisten puhelut alkoivat tukkia poliisin ja Viestintäviraston asiakaspalveluja.

Vaikka perinteisesti poliisin tehtävä ei ole avustaa rikoksilla aiheutettujen vahinkojen korjaamisessa, kansalaisille tarvittiin ajantasainen neuvontapalvelu. Tarvittiin ratkaisu, joka pitäisi rikosvahingon pienenä ja helpottaisi viranomaisten puhelinvaihteiden painetta. Poliisi julkaisi yhteistyössä Viestintäviraston ja F-Securen kanssa www.ransomware.fi-sivuston.

5.4 Pahin vältettiin – toistaiseksi

Onneksi lunnaiden maksuun käytetyistä kansainvälisistä maksuväylistä Suomessa tunnettiin vain yksi, PaySafeCard. Ja onneksi sitä myytiin vain R-kioskeissa. Yhteistyö molempien kanssa saatiin nopeasti käyntiin. Maksukuittiin lisättiin asiaa koskeva varoitus ja asiakkaita tiedotettiin. Rikoksen uhreista suurimmalle osalle rahat saatiin palautettua.

Poliisille tehtiin reilut tuhat ilmoitusta. Kaikista yhteydenotoista ei kirjattu rikosilmoitusta. Muuta emme voineet tehdä lainsäädännön puitteissa. Kansainvälinen yhteistyö ei aina ole menestystarina. Tässä tapauksessa lupaavasta alusta huolimatta tulokset jäivät lopulta Espanjan poliisin kiinniottojen lisäksi vähäisiksi. Suomesta löytyi mm. yksi Revetonin pääpalvelimista. Liikenne kiersi useiden eri maiden kautta.

F-Secure auttoi palvelimen tutkinnassa. Ohjelmisto oli osittain tuhottu ja vaati erityisosaamista parsia se toimintakuntoon. Palvelimen tutkinnassa avautui hyvä näkymä haittaohjelmalla saastuneiden koneiden määrästä ja mahdollisesti aiheutuneista vahingoista. Uhreja oli Suomessa kymmeniä tuhansia, maailmanlaajuisesti miljoonia.

Palvelin oli vuokrattu Venäjältä eikä vuokraajan henkilöllisyyttä saanut vuokratiedoista selville. Rikolliset jäivät ainakin toistaiseksi vapaalle, mutta Suomessa aiheutettu vahinko jäi pieneksi. Tähän päästiin avoimella yhteistyöllä. Kun viranomaisten toimivat yhdessä yksityisen sektorin kanssa, hyviä tuloksia on saavutettavissa myös verkkorikollisuuden torjunnassa. Tässä tapauksessa median asialle antama huomio ja siten kansalaisten lisääntynyt tietoisuus auttoivat merkittävästi.

5.5 Kyberrikollisuus on tullut jäädäkseen

Tuosta keskiviikon iltapäivästä on vuosia. Vaikka Reveton eri versioineen ei enää ole merkittävä ongelma, sen jälkeen on tullut kehittyneempiä kiristysohjelmia. Enää haittaohjelma ei lukitse ruutua, vaan etsii ja salaa uhrin kannalta arvokkaita tietoja. Pahimmillaan tiedostoja ei saa takaisin. Varmuuskopiot nousevat taas arvoonsa.

Yhtenä huolestuttavana kehityssuuntana on käyttää salaavia kiristysohjelmia myös tietomurroissa. Murtauduttuaan kohteen tietojärjestelmiin rikolliset etsivät järjestelmistä arvokkaita tietoja ja salaavat nämä tiedot käyttökelvottomiksi. Seuraavaksi uhri saa kiristysviestin. Tapauksia on myös Suomessa, vaikka poliisille näistä ei tietääkseni ole ilmoituksia tehty. Kiristysrikollisuuden kasvu on näkynyt jo vuosia yksikkömme työtehtävissä.

Yritykset kiinnostavat rikollisia enemmän kuin yksittäiset kansalaiset. Ne ovat huomattavasti maksukykyisempiä ja niistä löytyy tietoja, jotka ovat sen toiminnalle elintärkeitä ja jotka tarvitaan käyttöön nopeasti. Koska tietoturvaa ei aina oteta huomioon tuotteissa ja palveluissa, rikollisille avautuu jatkuvasti uusia mahdollisuuksia ansaita kyberrikollisuudella.

Revoton oli yksi ensimmäisiä tapauksia, jossa viranomaiset ja yritykset tekivät yhteistyötä kyberrikollisuuden taltuttamiseksi. Kaikkien osapuolien osuus on tarpeen. Toimivalla yhteistyöllä nykyiset ja tulevatkin uhat pystytään torjumaan.

5.6 Lisätietoja Revetonhaittaohjelman historiasta

27.7.2012 Mainospalvelut ja vanhat Java-versiot kiristyshaittaohjelman levittäjinä (Tietoturva nyt!)

15.5.2013 Tietoturvaloukkaukset ja niiden kehitys 2012

15.5.2014 Ransomware-katsaus

Kirjoittaja Jari Javanainen työskentelee rikosylikonstaapelina Itä-Uudenmaan poliisilaitoksen tietotekniikkarikostutkintaryhmässä

Yhteystiedot
PL 313
Itämerenkatu 3A
00181 Helsinki
puh: 0295 390 100
fax: 0295 390 270
www.viestintävirasto.fi