Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Kiristyshaittaohjelmat

Mikä on kiristyshaittaohjelma

Kiristyshaittaohjelmasta puhuttaessa tarkoitetaan viime vuosina erittäin laajoille levinneistä tietyn tyyppisistä haittaohjelmista, jotka uhkaavat tuhota uhrinsa tiedostot. Haittaohjelma on tietokoneohjelma, jonka tarkoituksena on tehdä laitteelle jotain haitallista. Kiristyshaittaohjelmat ovat toki vain yksi osa kaikista mailman haittaohjelmista, mutta niistä on tullut erityisen suosittuja rikollisten keskuudessa niiden luomien ansaintamahdollisuuksien vuoksi. Kun kiristyshaittaohjelma asentuu koneelle, se kryptaa tietyt tai jopa kaikki koneen tiedostot. Käyttäjältä estetään pääsy näihin tiedostoihin tai joissakin tapauksessa ylipäätään koko laitteeseen, eikä käyttäjä pysty enää käyttämään tai näkemään valokuviaan tai muita tiedostojaan. Tämän jälkeen haittaohjelma ilmoittaa, että ainoa tapa palauttaa pääsy koneelle tai tiedostoihin on maksaa rikolliselle tietty rahamäärä lunnaina. Useimmiten lunnaat pitää maksaa digitaalivaluutalla, kuten Bitcoineilla jäljitettävyyden vaikeuttamiseksi. Kiristyshaittaohjelmat leviävät normaalien haittaohjelmien tavoin ja yleisin levityskeino on sähköposti jonka liitetiedoston avattuaan tai linkin avatessaan käyttäjä mahdollistaa haittaohjelman asentumisen laitteelle.

Vierastoimittaja

Lenny Zeltser keskittyy asiakkaiden IT-toimintojen suojaamiseen ”NCR Corp”-nimisessä yrityksessä ja kouluttaa haittaohjelmilta suojaamista SANS-instituutissa. Lenny on aktiivinen Twitterissä **@lennyzeltser** ja kirjoittaa turvallisuusblogia osoitteessa **zeltser.com**.

Pitäisikö lunnaita maksaa

Kysymys on hankala, eikä siihen ole yksiselitteistä vastausta. Periaatteessa mitä useampi henkilö maksaa lunnaat, sen motivoituneempia rikolliset ovat levittämään haittaohjelmia. Toisaalta, joissakin tapauksissa käyttäjällä ei ole tietojen palauttamiseksi muuta keinoa kuin maksaa. Aina kannattaa ottaa tosin huomioon, että lunnaiden maksaminen ei aina tapaa tietojen palauttamista. Koska asioit rikollisten kanssa, saatat olla saamassa kryptausavaimia tai vaikka saisit, jokin saattaa mennä salauksen purkamisessa pieleen tai koneellasi saattaa olla muita haittaohjelmia.

Kiristyshaittaohjelmat

Varmuuskopiointi

Paras yksittäinen keino palautua kiristyshaittaohjelmatartunnasta maksamatta lunnaita on pitää huoli omien tietojen varmuuskopioinnista. Tällä tavalla, tartunnasta huolimatta saat palautettua tietosi laitteen siivouksen tai uudelleenasennuksen jälkeen. Ota kuitenkin huomioon, että jos laitteeltasi pääsee käsiksi varmuuskopioihin, saattaa haittaohjelma ulottua ja salata myös kopiot. Tämän vuoksi voit käyttää esim. luotettavaa verkkopalvelua tietojen kopiointiin tai erillistä, ulkoista muistilaitetta, kuten irrotettavaa kovalevyä. Testaa varmistusten toimivuus palauttamalla tiedostoja säännöllisesti jotta varmistut siitä, että kaikki toimii jos pahin käy. Varmistukset auttavat toki muissakin tapauksissa kuin haittaohjelmien yhteydessä, jos esim. poistat tiedostoja itse vahingossa tai laitteesi hajoaa.

Kiristyshaittaohjelmat ovat haittaohjelmia, jotka saastuttaessaan laitteesi, salakirjoittavat tiedostosi ja estävät pääsyn niihin.

Muita suojaavia toimenpiteitä

Edellä mainittujen lisäksi voit suojata itseäsi kiristyshaittaohjelmilta samalla tavalla kuin suojaudut muiltakin haittaohjelmista, parhaana tapana on olla saamatta tartuntaa. Varmista, että anti-virus-sovelluksesi tunnisteet päivittyvät automaattisesti ja käytät luotettavan toimittajan sovellusta. Huomaa kuitenkin, että nämä sovellukset eivät tunnista ja reagoi kaikkiin haittaohjelmiin. Kyberrikolliset innovoivat jatkuvasti ja luovat uusia ja kehittyneempiä haittaohjelmia jotka saattavat jäädä huomaamatta anti-virus-sovelluksilta. Luonnollisesti myös anti-virus-sovellusten toimittajat päivittävät sovelluksia ja lisäävät niihin uusia ominaisuuksia, jotka auttavat suojautumisessa, mutta valitettavasti rikolliset ovat usein edellä, minkä vuoksi käyttäjän kannattaa varmistua varmuuskopioinnista ja lisäksi harkita seuraavia toimenpiteitä:

- Kyberrikolliset saavat useimmiten tartutettua laitteesi haittaohjelmalla käyttämällä hyväkseen laitteidesi ja käyttämiesi sovellusten haavoittuvuuksia ja heikkouksia. Tämän vuoksia varmista, että käyttöjärjestelmäsi ja sovelluksesi käyttävät aina uusinta versiota ja jos mahdollista, päivityttävät automaattisesti.
- Tietokoneilla kannattaa käyttää tavallista käyttäjätyyppiä, eikä pääkäyttäjäoikeudellista, kuten ”Administrator” tai

Kiristyshaittaohjelmat

”root”. Monet haittaohjelmat eivät pysty asentumaan ilman pääkäyttäjäoikeuksia ja jos sinulla ei ole niitä, ei yleensä haittaohjelmakaan niitä saa.

- Usein kyberrikolliset huijaavat käyttäjiä asentamaan haittaohjelmat itse. He saattavat lähettää sähköpostin, joka näyttää asianmukaiselta ja tulleen ystävältäsi tai pankilta. Kuitenkin jos avaat liitetiedoston tai seuraat linkkiä, saattaa haittaohjelma asentua laitteellesi. Jos vastaanotettu viesti hoputtaa tekemään jotain, vaikuttaa liian hyvältä ollakseen totta tai on kirjoitettu huonolla kielellä, se saattaa sisältää haittaohjelman. Kannattaa noudattaa tervettä järkeä avatessasi sähköposteja ja vierailtaessa internetsivuilla.

Suojaa itsesi kiristyshaittaohjelmilta olemalla valppaana käyttäessäsi sähköpostia. Varmista, että anti-virus-sovelluksesi on ajan tasalla ja huolehdi tietojesi varmuuskopioinnista.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa securingthehuman.sans.org/ouch/archives.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava IT-johtaja. Kirill turvaa tällä hetkellä Elisa Appelsiinin liiketoimintaa vastaamalla niin yrityksen omasta kuin asiakkaiden tietoturvasta.

Lähteet

Sosiaalinen hakkerointi: https://securingthehuman.sans.org//ouch/2015#december2015

Mikä on haittaohjelma: https://securingthehuman.sans.org/ouch/2016#march2016

Kryptaus: https://securingthehuman.sans.org/ouch/2016#june2016

Varmuuskopiointi: https://securingthehuman.sans.org/ouch/2015#august2015

Microsoftin artikkeli aiheesta: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

SANS FOR610 Course - Reverse Engineering Malware: https://sans.org/for610

Lisenssi