Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

WannaCry-haittaohjelmasta opittua

Yleiskatsaus

Olet varmasti törmännyt viime viikkoina uuteen “WannaCry”-nimiseen kyberhyökkäykseen. “WannaCry”-saastutti globaalisti yli 200 000 tietokonetta, lukiten lukuisten organisaatioiden, mm. Brittiläisten sairaaloiden tietoja ja tiedostoja. On monia syitä miksi juuri tämä hyökkäys saavutti niin paljon huomiota. Se levisi koneelta koneelle käyttäen tunnettua haavoittuvuutta Windows-käyttöjärjestelmissä ja haittaohjelma oli kryptaava, joka tarkoittaa sitä että saastutettuaan koneen, se lukitsi kaikki käyttäjän tärkeimmät tiedostot estäen käyttäjän pääsyn niihin. Ainoat keinot saada tiedostot takaisin on palauttaa ne varmuuskopioista tai maksaa hyökkääjälle $300 lunnaat. Tärkein huomio hyökkäyksessä on se, että sitä ei olisi pitänyt edes tapahtua. Haavoittuvuus jota ”WannaCry” käyttää oli hyvin tunnettu ja korjattu Microsoftin toimesta jo kuukausia sitten. Uhriksi joutuneet organisaatiot olivat jättäneet päivitykset asentamatta tai käyttivät vanhoja käyttöjärjestelmiä, kuten Windows XP:tä, jolle päivityksiä ei enää tarjota. Alla on listattu yksinkertaisia asioita joita voit tehdä estääksesi ”WannaCry”-tyyppiset hyökkäykset jatkossa.

Vierastoimittaja

Dr. Johannes Ullrich toimii Tutkimuksen Dekaanina (Dean of Research) SANS:n teknologiainstituutissa ja on DShield.org:n perustaja. Hän vastaa **SANS Internet Storm Center**-keskuksesta, joka monitoroi ajankohtaisia kyberturvauhkia ja opettaa SANS:n Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) and IPv6 (**SEC546**)-kursseja.

Tietoturvapäivitykset

Ensimmäisenä ja tärkeimpänä, varmista että kaikki käyttämäsi tietokoneet, mobiililaitteet sovellukset ja muut verkkoon yhteydessä olevat järjestelmät ovat päivitetty. Kyberrikolliset etsivät jatkuvasti uusia haavoittuvuuksia ja käyttävät näitä hyväkseen hyökkäyksissä. Samaan aikaan laitteiden ja sovellusten valmistajat tekevät paljon työtä korjatakseen löydettyjä haavoittuvuuksia julkaisemalla päivityksiä. Jos varmistat laitteiden ja sovellusten automaattiset päivitykset, vaikeutat kaikkien hyökkäysten ja laitteidesi hakkeroimisen todennäköisyyttä. Turhauttavinta ”WannaCry”-hyökkäyksessä on nimenomaan se kuinka helposti se olisi ollut estettävissä, päivitykset olivat olemassa jo kuukausien ajan ja toimivan haavoittuvuuksienhallinnan prosessien omaaville yrityksille ”WannaCry” ei aiheuttanut ongelmia. Pyri aina mahdollisuuksien

WannaCry-haittaohjelmasta opittua

mukaan aktivoimaan automaattiset päivitykset ja varmista päivitysasetukset kaikissa laitteissa ja sovelluksissa jotka ovat yhteydessä Internettiin, mukaan lukien tietokoneet, mobiililaitteet, älytelevisiot, verkkolaitteet, pelikonsolit ja jopa autot. Jos käyttöjärjestelmäsi tai laitteesi ei enää tue tai tarjoa päivityksiä, kuten Windows XP, vaihda ne uudempiin.

Tärkein keino itsesi suojaamiseen "WannaCry:n" kaltaisilta hyökkäyksiltä on pitää laitteesi päivitettyinä, varoa kalastelua ja huolehtia varmuuskopioinnista.

Varmistukset

Joissakin tapauksissa kiristyshaittaohjelmien kaltaiset kyberhyökkäykset saattavat saastuttaa myös päivitetyt laitteet. Tässä tapauksessa ainoa keino suojautua on varmistaa laitteidesi sisältämät tiedot. Oikeaoppisessa varmuuskopioinnissa laitteidesi tiedot tallennetaan myös muualle kuin itse laitteeseen ja jos alkuperäisille tiedoille käy jotain, niin saat palautettua tietosi. Valitettavasti liian monet eivät huolehdi asianmukaisesta varmuuskopioinnista, vaikka se on nykyisin erittäin helppoa ja kustannustehokasta. Voit varmistaa tietosi kahdella tavalla, fyysiselle laitteelle tai pilvipalveluun. Kummassakin tavassa on hyvät ja huonot puolesta ja voit myös käyttää molempia rinnakkain saadaksesi molempien hyvät puolet.

Fyysisillä laitteilla tarkoitetaan hallitsemiasi laitteita, kuten ulkoisia muistitikkuja tai kovalevyjä. Näiden suurimpana hyötynä on suuret tallennusmäärät ja nopeat datasiirtonopeudet. Toisaalta mahdolliset haittaohjelmat saattavat siirtyä myös ulkoisille muistilaitteille jos ne ovat kiinni saastuneessa laitteessa. Jos varmuuskopioita ulkoisille muistilaitteelle, muista irrottaa ne laitteestasi aina käytön jälkeen ja säilyttää niitä turvallisessa paikassa. Pilvipalveluissa tallennat tietosi johonkin verkossa sijaitsevaan palveluun, yleensä asentamalla laitteellesi sovelluksen joka hoitaa varmuuskopioinnin ja tietojen siirtämisen automaattisesti. Paras puoli tässä lähestymistavassa on yksinkertaisiin ja jos saat haittaohjelmatartunnat, niin infektio ei yleensä pääse leviämään verkossa sijaitseviin tietoihisi. Huonona puolena on rajoittuneempi tallennuskapasiteetti ja hitaammat siirtonopeudet. Muista aina tutustua tarkasti pilvipalvelun tarjoajan tietoturvaan ja varmistaa esim. tarjoavatko he tietojen salaamista ja vahvaa tunnistautumista.

WannaCry-haittaohjelmasta opittua

Kalastelu

Viimeisenä, hyökkääjät muuttavat ja päivittävät jatkuvasti hyökkäystapojaan, mutta he yleensä tarvitsevat aina jonkun keinon päästä kohteensa laitteelle ja tämä tapahtuu usein kalastelun avulla. Kalastelulla tarkoitetaan sitä kun käyttäjä huijataan avaamaan haitallinen sähköposti tai verkkosivu naamioimalla pyyntö. Hyökkääjät lähettävät esim. sähköpostin, jonka avaamalla tai linkkiä klikkaamalla käyttäjä saa koneellensa haittaohjelmatartunnan. Vaikka ”WannaCry” ei tarttunut tällä tavalla, niin suurin osa kiristyshaittaohjelmista ja monista muista haittaohjelmista tarttuu juuri kalasteluviestien kautta. Lisäksi, kyberrikolliset jotka kehittivät ”WannaCry”-haittaohjelman tulevat varmasti päivittämään sitä ja käyttämään mm. kalastelua levittääkseen ohjelmaa entistä laajemmalle. Tärkein suojauskeino kalastelulta suojautumiseen on terveen järjen käyttö, jos viesti vaikuttaa mitenkään oudolta tai liian hyvältä ollakseen totta, se saattaa olla hyökkäys.

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, kokenut IT-ammattilainen. Kirill turvaa tällä hetkellä Nebula Oy:n asiakkaiden liiketoimintaa konsultoimalla ja kehittämällä asiakkaiden tietoturvaviitekehyksiä ja toimintamalleja.

Lähteet

Mitä ovat haittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#march2016
Kiristyshaittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#august2016
Varmuuskopiointi:	https://securingthehuman.sans.org/ouch/2015#august2015
Kalastelu:	https://securingthehuman.sans.org/ouch/2015#december2015
Pilvipalveluiden turvallinen käyttö:	https://securingthehuman.sans.org/ouch/2016#november2016

Lisenssi