Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Mitä ovat haittaohjelmat

Yleiskatsaus

Olet varmasti kuullut termeistä viirus, trojalainen tai rootkit kun ihmiset puhuvat kyberturvallisuudesta. Kaikki nämä termit kuvaavat samaa asiaa, eli erityyppisiä ohjelmia joita rikolliset käyttävät saastuttaakseen tietokoneita tai muita laitteita. Yleinen termi näille kaikille on haittaohjelma (malware). Tässä uutiskirjeessä kerromme mitä haittaohjelmat ovat, kuka niitä luo ja tärkeimpänä; miten voit suojautua niitä vastaan.

Vierastoimittaja

Lenny Zeltser suojaa työkseen asiakkaidensa IT-toimintoja NCR Corp:lla ja opettaa haittaohjelmilta suojautumista SANS instituutilla. Lenny on aktiivinen Twitterissä **@lennyzeltser** ja kirjoittaa turvallisuusaiheista blogia osoitteessa **zeltser.com**.

Mikä on haittaohjelma?

Yksinkertaistettuna, haittaohjelma on sovellus joka tekee haittallisia toimia kohteellensa. Englanninkielinen sana ”malware” tulee yhdistelmistä ”malicious” eli haitallinen ja ”software”, eli sovellus. Kyberrikolliset asentavat haittaohjelmia tietokoneisiin tai muihin laitteisiin saadakseen pääsyn kyseiseen laitteeseen tai sen sisältöön. Kun haittaohjelma on asentunut, rikolliset pystyvät vakoilemaan verkkoliikennettä, varastamaan salasanojan tai tiedostoja tai käyttää saastunutta järjestelmää muihin järjestelmiin hyökkäämiseen. Haittaohjelmat voivat myös estää sinua pääsemästä käsiksi omiin tiedostoihin ja vaatia sinulta maksua tiedostojen palauttamiseksi.

Yleinen harhaluulo on se, että haittaohjelmat koskevat vain Windows-koneita. Vaikka Windows on yleisyytensä vuoksi edelleen hyökkääjien suosituin kohde, haittaohjelmat voivat tarttua myös muihin järjestelmiin ml. Applen järjestelmät, matkapuhelimet tai tabletit. Tämän vuoksi kaikki ovat alttiina niille, myös sinä.

Kuka luo haittaohjelmia?

Nykyisin haittaohjelmia eivät enää luo vain uteliaat harrastelija tai amatöörihakkerit, vaan myös ammattirikolliset. Heidän päämääränään on ansaita rahaa saastuneella järjestelmällä, esimerkiksi myymällä hankittuja tietoja, lähettämällä roskapostia, kiristämällä tai käyttämällä saastuneita järjestelmiä palvelunestohyökkäyksiin. Eri tahot jotka luovat tai jakelevat haittaohjelmia voivat olla yksittäisiä rikollisia, rikollisryhmiä tai valtiollisia toimijoita. Henkilöt jotka luovat tämän päivän pitkälle kehittyneitä haittaohjelmia saattavat olla hyvin keskittyneitä tarkoituksiinsa ja tehdä haittaohjelmia pääasiallisena

Mitä ovat haittaohjelmat

työnään. Lisäksi, kun haittaohjelma on kehitetty, he usein myyvät sen eteenpäin muille ja joissakin tapauksissa tarjoavat laadukasta asiakaspalvelua päivittämällä ohjelmia ja tarjoamalla ostajille tukea.

Itsesi suojaaminen

Yleisin tapa suojautua on asentaa tunnetun toimittajan haittaohjelmilta suojaava sovellus, kuten anti-virus ohjelma. Tällaiset sovellukset ovat suunniteltu huomaamaan ja pysäyttämään haittaohjelmat. Kyberrikolliset kuitenkin innovoivat ja kehittävät kehittyneempiä haittaohjelmia, jotka osaavat ohittaa suojaavat sovellukset. Anti-virus toimittajat vuorostaan kehittävät omia sovelluksia huomaamaan haittaohjelmat paremmin. Tästä on tullut kilpavarustelua, jossa kumpikin osapuoli yrittää olla jatkuvasti toista edellä. Valitettavasti, haittaohjelmien tekijät ovat yleensä yhden askeleen edellä. Koska et pysty täysin luottamaan suojaaviin sovelluksiin, seuraavana on lueteltu muutamia asioita mitä voit tehdä suojataksesi itseäsi paremmin:

Suojaa itsesi haittaohjelmilta olemalla tarkkana sähköpostin käytön kanssa, varmistamalla laitteidesi päivitykset ja käyttämällä anti-virus sovellusta.

- Kyberrikolliset käyttävät haittaohjelmissaan usein hyväkseen eri järjestelmien tai sovellusten haavoittuvuuksia. Mitä ajantasaisempia sovelluksia tai käyttöjärjestelmiä käytät, sen vähemmän hyväksikäytettäviä haavoittuvuuksia niissä on ja sen vaikeampi haittaohjelman on tarttua. Tämän vuoksi, varmista että käytössäsi on aina uusimmat versiot ja käytä hyväksesi automaattisia päivityksiä aina kun mahdollista.
- Yleisin tapa hyökätä mobiililaitteita vastaan on luoda väärennetty sovellus ja saada käyttäjä asentamaan se omalle koneelleen. Tämän vuoksi asenna sovelluksia vain luotetuista lähteistä, kuten valmistajan sovelluskaupasta. Lisäksi voit varmistaa, että sovellus ei ole aivan uusi, sillä on paljon latauksia ja hyviä arvosteluja.
- Käytä tietokoneella aina vain rajoitettuja käyttöoikeuksia pääkäyttäjän oikeuksia sijaan. Suhtaudu epäilevästi, jos järjestelmä pyytää sinua syöttämään pääkäyttäjän salasanan. Tällä tavalla estät monien haittaohjelmien asentumisen koneelle.
- Kyberrikolliset yleensä huijaavat käyttäjiä asentamaan haittaohjelman laitteelle itse. He voivat lähettää sinulle sähköpostia jossa on liitetiedosto tai linkki. Nämä saattavat olla erittäin laadukkaasti tehtyjä ja tulla luotettavan näköisestä lähteestä kuten pankiltasi tai tuttavalta. Kun avaat linkin tai liitetiedoston, haittaohjelma asentuu laitteellesi. Suhtaudu epäilevästi, jos lähetetyssä viestissä pyydetään nopeita toimia, se on jotenkin hämmentävä tai viestissä luvataan liian hyviä asioita. Terve järki on yleensä paras keino suojautua.

Mitä ovat haittaohjelmat

- Varmista laitteidesi sisältö säännöllisesti joko paikallisesti ulkoiselle muistilaitteelle tai pilvipalveluun. Tällä tavalla pääset käsiksi tietoihisi, jos niille joskus käy jotain tai haittaohjelma salakirjoittaa niiden sisällön. Varmistukset ovat usein ainoa tapa palauttaa tiedot haittaohjelman jälkeen.

Parhaat keinot suojautua haittaohjelmilta ovat siis järjestelmien ja sovellusten päivittäminen, anti-virus sovellusten käyttäminen ja terve järki sähköpostin käytössä.

LUE LISÄÄ

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

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

Kalastelu:	https://securingthehuman.sans.org/ouch/2015#december2015
Sosiaalinen hakkerointi:	https://securingthehuman.sans.org/ouch/2014#november2014
Mobiililaitteiden suojaaminen:	https://securingthehuman.sans.org/ouch/2015#january2015
Tablettisi suojaaminen:	https://securingthehuman.sans.org/ouch/2016#january2016
Varmistukset :	https://securingthehuman.sans.org/ouch/2015#august2015

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy