Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Minut hakkeroitiin, mitä nyt?

Yleiskatsaus

Me tiedämme, että sinä välität tietokoneestasi ja mobiililaitteistasi ja teet tarvittavia toimia niiden suojaamiseksi. Riippumatta kuinka turvallisesti laitteitasi käytät, on kuitenkin mahdollista, että jossakin vaiheessa joudut hakkereiden uhriksi. Tässä uutiskirjeessä kerromme miten pystyt päättelemään jos näin on käynyt ja miten voit toimia tämän jälkeen. Mitä nopeammin huomaat että jotain on vialla ja reagoit, sen vähemmän vahinkoa mahdollinen hyökkääjä saa aikaiseksi.

Vierastoimittaja

Samantha Davison (**@sam_e_davison**) toimii turvallisuustietoisuuden ja –koulutuksen vastaavana päällikkönä Uberillä ja kouluttaa työntekijöitä ympäri maailmaa yli 350:ssä kaupungissa.

Mistä voit päätellä että sinut on hakkeroitu

Voi olla hankalaa huomata joutuneensa hakkerin uhriksi, koska ei ole olemassa yhtä tiettyä asiaa, joka sen osoittaisi. Hakkereiden jäljiltä jää sen sijaan usein monia pienempiä vihjeitä, indikaattoreita. Mitä useamman alla olevista tunnistat, sen todennäköisempää on että olet joutunut uhriksi.

- Laitteesi tietoturvaohjelmisto (anti-virus) on hälyttänyt järjestelmässä olevasta haittaohjeista, varsinkin jos sitä ei ole pystytty poistamaan tai laittamaan karanteeniin
- Selaimesi kotisivu on yllättäen vaihtunut tai selaimesi ohjaa sinut sivuille, joille sinun ei ollut tarkoitus mennä
- Laitteeltasi löytyy uusia käyttäjätilejä tai sovelluksia, joita et ole itse asentanut
- Laitteesi tai sovelluksesi kaatuilevat, laitteillasi on outoja ikoneita tai avautuvia ikkunoita
- Sovellus pyytää sinua auktorisoimaan muutoksia järjestelmääsi, vaikka et ole asentanut tai päivittänyt itse mitään
- Salasanasi ei yllättäen toimi, kun yrität kirjautua laitteellesi tai verkkopalveluun, vaikka olet varma, että salasana on oikein
- Ystäväsi kyselevät sinulta tulevasta roskapostista tai oudoista viesteistä joita et ole itse lähettänyt
- Matkapuhelinlaskullasi on tunnistamattomia veloituksia maksullisiin numeroihin

Minut hakkeroitiin, mitä nyt?

- Mobiililaitteesi käyttää poikkeuksellisen paljon mobiilidataa tai akkua

Miten voit toimia

Jos uskot että laitteesi on hakkeroitu, kannattaa toimia mahdollisimman pian. Mikäli käytät työnantajasi toimittamaa laitetta tai käytät laitetta työtehtäviin, älä yritä korjata vikaa itse. Sen lisäksi, että voit tehdä lisää vahinkoa, voit myös tuhota laitteelta arvokasta todistusaineistoa, jota tarvitaan mahdollisen rikoksen tutkimisessa. Kannattaa ilmoittaa epäilyksesi yrityksesi kontaktointitapojen mukaisesti, eli yleensä ilmoittamalla IT-tuelle, turvallisuusyksikölle tai esimiehellesi. Jos et jostakin syystä saa yhteyttä yritykseesi tai sinua huolestuttaa reagointiaika, irrota laitteesi verkosta ja laita se nukkumismoodiin tai lentotilaan. Vaikket ole täysin varma onko laite altistunut, ilmoittaminen kannattaa aina varmuuden vuoksi. Jos käyttämäsi laite on omasi tai käytät sitä henkilökohtaisiin tarkoituksiin, voit tehdä seuraavat toimenpiteet:

Ennemmin tai myöhemmin saatat joutua hakkerin uhriksi. Mitä nopeammin huomaat tämän ja reagoit, sen parempi.

- **Vaihda salasanasi**: Ei vain laitteesi salasanat, vaan myös kaikkien verkkopalveluiden salasanat. Varmista, ettet käytä salasanojen vaihtamiseen hakkeroitua laitetta, sen sijaan käytä eri laitetta jonka tiedät olevan turvallinen.
- **Anti-virus**: Jos tietoturvaohjelmistosi ilmoittaa infektoituneesta tiedostosta, voit seurata sovelluksen suosituksia. Tämä merkitsee yleensä tiedoston laittoa karanteeniin, puhdistamista tai poistamista. Useimmat sovellukset tarjoavat lisäksi linkkiä josta löytyy lisätietoja kyseisestä tartunnasta. Jos et ole varma mitä tehdä, kannattaa tiedosto laittaa vähintään karanteeniin ja jos se ei ole mahdollista, niin poistaa se.
- **Uudelleenasennus**: Jos et pysty korjaamaan haittaohjelmatartuntaa tai haluat varmistua täysin laitteesi turvallisuudesta, paras vaihtoehto on laitteen uudelleenasennus. Tietokoneiden osalta seuraa käyttöjärjestelmän tai laitevalmistajan suosituksia. Useimmiten tämä tarkoittaa käyttöjärjestelmän uudelleenasennusta toimittajan työkaluilla. Jos nämä työkalut puuttuvat tai ovat jotenkin viallisia, ota yhteyttä toimittajaan tai vieraile heidän verkkosivuilla. Älä uudelleenasenna käyttöjärjestelmää suoraan varmuuskopiolta, koska tällöin järjestelmään saattaa palautua samat haavoittuvuudet joista yrität päästä eroon. Varmistuksia kannattaa käyttää vain tietojen palauttamiseen. Mobiililaitteiden palauttamisessa kannattaa seurata laitevalmistajan ohjeita, nämä löytyvät yleensä

Minut hakkeroitiin, mitä nyt?

mm. heidän verkkosivuiltaan. Useimmissa tapauksissa laite vain palautetaan tehdasasetuksiin ja tiedot palautetaan varmistuksista. Jos et koe pystyväsi edellä mainittuihin toimenpiteisiin, kannattaa pyytää apua ammattilaiselta. Jos laitteesi on suhteellisen vanha, voi olla yksinkertaisempaa ja jopa halvempaa ostaa uusi. Kun olet saanut uudelleenasennetun tai uuden laitteen käyttöösi, muista asentaa siihen viimeisimmät tietoturvapäivitykset ja jos vain laite sen mahdollistaa, varmista että laite päivittää itsensä automaattisesti.

- **Varmistukset**: Tärkein vaihe itsensä suojaamisessa on varmistaa laitteidesi säännöllisten varmistusten toimivuus. Mitä useammin varmistat, sen parempi. Tietyt varmistuspalvelut hoitavat varmistukset automaattisesti niin, että uudet tai muuttuneet tiedostot varmuuskopioidaan joka tunti. Riippumatta siitä mitä palvelua käytät, varmista säännöllisesti että saat myös palautettua tietoja. Hakkeroinnin uhriksi joutumisen jälkeen varmistukset ovat usein ainoa tapa palauttaa tietosi.
- **Viranomaiset**: Jos koet jonkun asian uhkaavaksi tai laittomaksi, ilmoita asiasta viranomaisille.

LUE LISÄÄ

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

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

Varmistukset:	https://securingthehuman.sans.org/ouch/2015#august2015
Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2015#april2015
Mitä ovat haittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#march2016
Uuden tablettilaiteesi suojaaminen:	https://securingthehuman.sans.org/ouch/2016#january2016

Lisenssi