Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Toimitusjohtajahuijaus

Mikä on toimitusjohtajahuijaus?

Verkkorikolliset ovat ovelia ja keksivät jatkuvasti uusia tapoja saada tarvitsemansa. Yleisimpiä keinoja tähän on kohdistaa hyökkäykset tavallisiin henkilöihin, kuten sinuun. Kyberrikolliset ovat kehittäneet uuden hyökkäystavan nimeltä "Toimitusjohtajahuijaus (CEO Fraud tai Business Email Compromise (BEC)). Tämän tyyppisissä hyökkäyksissä, kyberrikolliset esittävät yrityksesi toimitusjohtajaa tai muuta johtohenkilöä. Hyökkääjä lähettää sähköpostin työtekijälle johtajan nimissä yrittäen kalastella tietoja tai pyytää henkilöä tekemään jotain.

Vierastoimittaja

Angela Pappas toimii tietoturvakoulutuksen ja –tietoisuuden johtajana Thomson Reautersilla. Työssään Angela vastaa lähettiläsohjelmasta (Ambassador program), verkkokoulutuksista ja työntekijöiden tietoturvatietoisuudesta.

Tälläiset hyökkäykset ovat poikkeuksellisen tehokkaita, koska rikolliset tekevät yleensä paljon etukäteistutkimusta ennen hyökkäyksen suorittamista. Rikolliset tutkivat yrityksesi tiedot etukäteen ja tunnistavat avainhenkilöt, toimistojen sijainnit ja yrityksessä työskentelevät henkilöt, mm. sosiaalisesta mediasta. Kun rikolliset tietävät kaiken tarpeellisen, he kohdistavat hyökkäykset tiettyihin henkilöihin riippuen heidän tavoitteistaan. Jos rikolliset haluavat rahaa, he saattavat kohdistaa hyökkäyksen taloushallintoon, jos he haluavat pääsyn tietylle palvelimelle, he kohdistavat hyökkäyksen IT-henkilöstöön.

Kun kohde on tunnistettu, rikolliset laativat hyökkäyksensä ja yleisimmin käytetään kohdistettua kalastelua. Normaalissa kalasteluhyökkäyksessä rikolliset lähettävät mahdollisimman monta sähköpostia yritykseen tarkoituksenaan saada muutama henkilö tekemään haluamansa toimet, esim. klikkaamaan linkkiä tai avaamaan haittaohjelmaliite. Kohdistettu kalastelu on saman tyyppinen, mutta hyökkäys kohdistetaan tiettyihin henkilöihin ja lähetetyt viestit ovat räätälöityjä ja yleensä paljon paremmin ja laadukkaammin laadittu kuin geneverisessä hyökkäyksessä. Hyvin tehtyä kohdistettua hylkäystä voi olla erittäin hankala tunnistaa. Viesti saattaa olla laadittu erittäin laadukkaasti, ja näyttää tulevan joltakin jonka tunnet tai muulta

Toimitusjohtajahuijaus

luotettavalta lähettäjältä, esim. toimitusjohtajalta. Viestit saattavat sisältää yrityksesi luottamuksellista tietoa, virallisia logoja tai jopa toimitusjohtajan virallisen allekirjoituksen. Viesteissä vaaditaan yleensä kiireellisiä toimia ja usein pyydetään luottamuksellisuutta, että tieto viestistä ei leviäisi. Kyberrikollisten tarkoituksena on saada sinut kiirehtimään ja tämän myötä tekemään jotain mitä et ehkä ajateltuasi tekisi. Alla on kuvattu muutamia erilaisia tilanteita:

Toimitusjohtajahuijaukset ovat tehokkaita hyökkäyksiä, joiden avulla voidaan ohittaa monia turvamekanismeja. Sinä olet itse yrityksesi paras puolustuskeino.

- **Rahansiirto**: Kyberrikolliset jahtaavat rahaa ja ovat selvittäneet ketkä yrityksessä hoitavat rahaliikennettä. Rikolliset laativat viestin jossa he esittävät olevansa kirjanpitäjän esimies tai vastaava ja pyytävät siirtämään mahdollisimman nopeasti rahaa tietylle tilille, koska jossakin on joku hätätilanne.

- **Veropeto**s: Kyberrikolliset haluavat hankkia henkilötietoja veropetosta varten ja he kohdistavat hyökkäyksen HR-henkilöön. He laativat viestin jonka on lähettänyt yrityksen johtaja, jossa pyydetään mahdollisimman pian yrityksen työntekijätietoja johonkin kiireelliseen käyttöön.

- **Juristihuijaus**: Kaikki toimitusjohtajahuijaukset eivät välttämättä edellytä sähköpostia, vaan rikolliset saattavat käyttää esim. puhelinta. Tässä esimerkissä esimiehesi tai joku johtaja lähettää sinulle viestin, että yrityksen juristi soittaa sinulle pian ja pyytää tiettyjä tietoja. Tämän jälkeen saat puhelun juristilta joka kyselee sinulta asioita mitä rikolliset haluavat tietää. Tässäkin tapauksessa sinulta pyydetään nopeasti jotakin tietoja ja puhelimessa voi olla hankalaa miettiä asioita tarpeeksi nopeasti.

Itsesi suojaaminen

Mitä voit tehdä itsesi tai yrityksesi suojaamiseksi? Terve järki on yleensä kaikkein tehokkain puolustuskeino. Jos saat esimieheltäsi tai johtajalta viestin tai pyynnön joka ei vaikuta täysin asianmukaiselta, saatat olla hyökkäyksen uhri. Hyviä

Toimitusjohtajahuijaus

vinkkejä huijauksen huomaamiseen sähköpostissa ovat kiireellisyyden tunne, epäselvyydet nimikirjoituksessa tai logossa ja viestin outo tai erilainen sävy. Lisäksi kannattaa tarkistaa viestin lähettäjän osoite ja puhelinnumero, ne saattavat joskus paljastaa huijauksen. Sähköpostiosoite saattaa olla samankaltainen, mutta muutaman kirjaimen erolla. Jos et ole täysin varma viestin aitoudesta, soita tai mene tapaamaan henkilöä ja varmista että he ovat lähettäneet kyseisen viestin. Älä koskaan vastaa suoraan vastaanotettuun viestiin tai tee kiireessä mitään mitä et tekisi muutenkin. Yrityksellesi on todennäköisesti politiikkoja ja periaatteita joissa määritellään toimintatapoja tai –ohjeita ja pyynnöt joissa pyydetään toimimaan näiden vastaisesti pitäisi aina herättää epäilyksiä riippumatta mistä pyyntö on tullut. Jos et ole varma mitä sinun pitää tehdä, ole välittömästi yhteydessä esimieheesi, tietoturvastaavaan tai yrityksesi IT-tukeen.

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/2014#november2014
Kalastelu:	https://securingthehuman.sans.org//ouch/2015#december2015
Mitä ovat haittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#march2016
Kaksivaiheinen tunnistautuminenn:	https://securingthehuman.sans.org/ouch/2015#september2015
Päivän vinkki:	https://www.sans.org/tip-of-the-day

Lisenssi

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