

Symantec: Pankkien on opastettava asiakkaitaan

20.4.2007 13:11 — Antti Kirves

Phishing-ongelmat ovat Nordealle ja muille pankeille kova pala purtavaksi. Pelkästä tekniikasta ei ole apua, kun asiakkaita huijataan.

Nordea on viime kuukausina tämän tästä ollut otsikoissa asiakkaiden tietoja kalastelevien rikollisten takia niin Ruotsissa kuin Suomessakin.

Nordean tapauksia tutkinut asiantuntija painottaa, että pankkia ei ole hakkeroitu, vaan sen asiakkaita on käytetty hyväksi ja huijattu antamaan luottamuksellisia tietoja.

- Syynä voi olla se, että Nordea on Ruotsin suurin pankki. Nordean turvaratkaisu näyttää myös antavan helpoimman tavan huijata käyttäjiä luovuttamaan tietojiaan, sanoo tietoturva-asiantuntija **Per Hellqvist** Symantecista.

Hellqvistin mielestä avain pankkitietojen kalastelun loppumiseen on käyttäjien opastamisessa.

- Pankkien pitää kertoa asiakkailleen selkeästi ja suoraan, millä tavoin ne viestivät heidän kanssaan. Asiakkaille on opetettava uudelleen ja uudelleen, etteivät pankit kysy tunnuksia sähköpostiviesteissä.

Nordeaa ennen Ruotsissa kalasteltiin Eurocardin ja Swedbankin tunnuksia.

- Sitten hyökkääjät tajusivat, että mitä isompi kohde ja mitä enemmän sillä on asiakkaita, sitä paremmat mahdollisuudet heillä on huijauksien onnistumiseen.

Brändille koituu suurin vahinko

Pankin tai muun verkossa toimivan yrityksen brändille tekee hallaa aina, kun sitä käytetään tietojen kalastelussa.

- Tämä on suurin vahinko Nordealle ja muille kalastelun syöteiksi joutuneille pankeille. Ihmiset eivät enää luota verkkopankkeihin ja -kauppoihin. Luottamuksen uudelleenrakentaminen on hyvin hidasta ja kallista, Hellqvist toteaa.

Myös tietoturva maksaa. Siksi pankit ovat taipuvaisia hyväksymään tietyn huijausriskin.

- Pankeille on halvempaa maksaa korvauksia kalastelusta - paitsi, jos mukaan lasketaan vahinko brändin tahriintumisesta. En tiedä, miten sitä voitaisiin mitata. Selvää on, että mitä enemmän brändi yhdistetään huijauksiin, sitä vähemmän siihen luotetaan.

Tekniikka auttaa, mutta ei ratkaise

Yhdeksi tekniseksi parannukseksi Hellqvist ehdottaa kuvatunnistautumista. Siinä asiakas valitsee kuvan, jonka hän lataa palveluun. Jos hän vastedes kirjautuessaan näkee valitsemansa kuvan sivulla, hän tietää olevansa oikealla sivulla.

Ruotsissa keskustellaan Hellqvistin mukaan nyt kovasti myös spf:n (Sender Policy Framework) käytöstä. Spf:ää käytetään sähköpostiviestin lähettäjän tunnistamiseen. Tässä pankit voisivat hänen mielestään auttaa asiakkaitaan.

Spf ei kuitenkaan ole aivan ongelmaton vaihtoehto, eikä tekniikasta ei yksin ole muutenkaan pankkiongelmien ratkaisuksi.

- Pankit eivät koskaan voi estää pahiksia lähettämästä kalasteluviestejä. Internetissä melkein kuka tahansa voi tehdä melkein mitä tahansa. Verkkopankkiin voi tietysti toivoa lisää tietoturvaa, mutta mitä turvallisempi järjestelmä on, sitä vaikeampi se on käyttää, Hellqvist tuumaa.

Huijausten kieli kehittyy

Ruotsalaisalastelun teho ei Hellqvistin mukaan ole perustunut ainakaan moitteettomaan kieleen. Meillä "hoono soomi" on auttanut välttämään kalasteluyrityksiä.

- Sama toistuu jokaisessa maassa, jossa kalastelua on havaittu. Ensin tulee erittäin keho paikallinen kieliversio, joka on ilmeisesti konekäännetty, Hellqvist sanoo.

Kun rikollinen saa näistä ensimmäisistä kalasteluista rahaa, hän panostaa uusiin viesteihin, jotka näyttävät jo paremmilta.

- Syntyperäisen kielenpuhujan on helppo nähdä, että kyse on roskasta. Monille, kuten maahanmuuttajille, lukihäiriöisille tai sellaisille, jotka eivät muuten ymmärrä hallinnon kieltä, tilanne on aivan toinen.

Uusimmat Ruotsissa leviävät kalasteluviestit ovat Hellqvistin mukaan jo todella hyvää ruotsia.

- Ilmeisesti kalastelijat ostavat jo käännöspalveluja syntyperäisiltä ruotsinpuhujilta. Paljon rahaa menee Baltian maihin, Venäjälle ja Valko-Venäjälle. Niissä maissa on ihmisiä, jotka puhuvat meidän kieliämme.

Työkalupakilla alkuun

Kalasteluoperaatio aloitetaan ostamalla tarkoitukseen tehty parinsadan dollarin työkalu, phishing kit.

Työkalukitissä on kalastelua varten valmiit viestipohjat, joihin lisätään netistä oikean pankin sivuillaan käyttämät kuvat.

Kittejä myymällä rikollinen saa rahaa uusien viestien kielen ja ulkoasun parantamiseen. Viidellä dollarilla saa netistä 29 000 sähköpostiosoitetta, joihin roskapostittaa kalasteluviestejä.

- Osa kalastelijoista on täysin ammattimaisia ja he tekevät paljon rahaa. Phishing on todella tehokasta ja tuottoisaa, ja riski on minimaalinen. Siksi kalastelu ei häviä mihinkään, Hellqvist arvelee.

Trojalaisistakin on kiusaa

Verkkopankkien asiakkaita kiusaavat myös haittaohjelmat, kuten [Sampo Pankki tällä viikolla varoitti](#)

Pankkitrojalaisia on laidasta laitaan. Jotkut vakoilevat tekstiä, jota käyttäjä kirjoittaa sellaisille web-sivulle, jotka sisältävät esimerkiksi sanat "bank" tai "credit card".

Hienostuneemmissa pankkitrojalaisissa on listat eri puolilla maailmaa sijaitsevien pankkien verkkotunnuksista, joiden ulospäin suuntautuvaa http-liikennettä haittaohjelmat kuuntelevat.

Pankkitrojalaiset voivat käyttää rootkit-tekniikoita piiloutuakseen ja ne usein päivittävät itsensä.

- Ne voivat käyttää myös JavaScript injection -tekniikoita saadakseen käyttäjän selaimen näyttämään oikealla pankin sivulla esimerkiksi väärän kirjautumiskentän, joka toimittaa käyttäjän tunnukset rikolliselle, Hellqvist sanoo.

Hyökkääjä voi myös peittää selaimen url-osoitekentän valeosoitteena toimivalla gif-kuvalla, jolloin käyttäjästä näyttää siltä, että hän on oikealla sivulla. Saman tempun voi tehdä salatusta yhteydestä selaimessa kertovalle riippulukkosymbolille.

<http://www.digitoday.fi/tietoturva/2007/04/20/symantec-pankkien-on-opastettava-asiakkaitaan/20079665/66>

