

Tietojenkalastelu vähenee, haittaohjelmat tilalle

19.4.2007 08:31 — Kalevi Nikulainen

Sähköposteilla pankkitietojen kalastelu on vähenemässä, ja tilalle ovat tulossa troijalaisvirukset ja haittakoodit, jotka voivat huomaamattomasti varastaa kuluttajan pankki- ja luottokorttitiedot, kertoo EMC:n tietoturvadivisioonan RSA:n Euroopan finanssitoimialaryhmän johtaja Andrew Moloney.

Moloneyn mukaan phishing eli tietojen kalastelu ei poistu kokonaan, vaan se siirtyy pienempiin pankkeihin ja esimerkiksi hyväntekeväisyystapahtumiin, joista kärkytään luottokorttitietoja.

RSA:n Anti-Fraud Command Center on ollut suojaamassa yli 200 pankkia tai muuta rahaa organisaatiota hyökkäyksiltä. Keskus on ollut torppaamassa yli 32 000 tiedonkalasteluhyökkäystä.

Moloney selvittää, että RSA:lla on maanalaisessa toiminnassa vajaat 70 etsivää, jotka myös soluttautuvat internetin rikollispiireihin.

RSA-johtajan mukaan internetiin on muodostunut tuhansien rikollisten rakentama varjotalous, jossa voidaan käynnistää esimerkiksi neljä samanaikaista hyökkäystä pankkeja vastaan eri puolella maailmaa.

-Suurin osa hyökkäyksistä on paikallistettu Itä-Eurooppaan ja Afrikkaan, mutta kyse on todella maailmanlaajuisesta toiminnasta.

Nettirikollisuuden kasvaessa rahalaitokset ovat Moloneyn mukaan kehittäneet voimakkaasti toimintojaan suojataksaan nettiasioinnin.

Hyökkäysten vuoksi pankit ovat ryhtyneet käyttämään todentamis- ja hyökkäysentorjuntaohjelmia. Moloney toteaa, että myös suomalaispankit ovat tehneet niin.

Asevarustelukilpa osapuolten välillä

Moloneyn mukaan rikolliset testaavat pankkeja erilaisilla

hyökkäyksillä löytääkseen niistä heikkoja kohtia.

-Vastapuolella nettihuijarit kehittävät myös hyökkäystyökalujaan. Käynnissä on koko ajan asevarustelukilpailu hyvien ja pahojen välillä. Tyypilliset hyökkäykset ovat internet-tapahtumien kaappauksia ja salasanojen varastamista, joilla päästään käsiksi finanssi- ja henkilökohtaisiin tietoihin.

Nettihuijarien maailma on Moloneyn mukaan hierarkkinen ja erikoistunut. RSA on löytänyt viisi erilaista ryhmää.

-Yksi niistä keskittyy sähköpostiosoitteiden keräämiseen, toinen isojen bottiverkkojen vuokraamiseen ja kolmas kehittämään ohjelmistotyökaluja. Nämä ryhmät toimivat lain rajamailla, ja niitä on vaikea saada kiinni.

RSA-johtaja kertoo, että selvästi rikollisuuden puolella ovat kahden ryhmän edustajat, varsinaiset huijauksien tekijät ja paikalliset rikollisjoukkiot.

-Kaikkien viiden ryhmän taitoja tarvitaan pankkihyökkäyksissä. Niihin on vaikea päästä käsiksi, kun toiminta ylittää valtiolliset rajat.

Moloney korostaa, että tällaisessa tilanteessa pitää keskittyä hyökkäysten torjuntaan ja kansalaisten valistamiseen, jotta huijareiden saama rahallinen hyöty vähenisi.

<http://www.digitoday.fi/tietoturva/2007/04/19/tietojenkalaste-lu-vahenee-haittaohjelmat-tilalle/20079466/66>