

Rock Phish -ryhmä iskee uudella tekniikalla pankkeihin

25.4.2008 10:22 — Kalevi Nikulainen

EMC:n tietoturvadivisioona RSA on paljastanut uuden kalasteluhankkeen. Siinä hyödynnetään samanaikaisesti tietojen kalastelua ja troijalaisia.

Hyökkäysten kohteena näyttävät RSA:n mukaan olevan erityisesti pankkialan yhteisöt. Rikolliset pyrkivät hankkimaan esimerkiksi verkkopankkitunnuksia sähköpostiviestien ja aidolta näyttävien haittaohjelmien avulla. Hyökkäyksistä kertoi ensimmäisenä RSA:n tietoturvakeskus AFCC.

- Pohjoismaissa uudentyypisiä iskuja ei ole tietojemme mukaan toistaiseksi havaittu. On kuitenkin todennäköistä, että hyökkäyksiä yritetään jossain vaiheessa myös Suomessa. Tarkoituksemme on paljastaa ja estää hyökkäykset jo ennalta, sanoo RSA:n myyntijohtaja **Petri Vilander**.

Hyökkäysten takana on RSA:n mukaan Rock Phish -ryhmä, joka on tehnyt maailmanlaajuisia iskuja verkkopankkeihin ja muihin verkkomaksua hyödyntäviin järjestelmiin vuodesta 2004 lähtien. Ryhmän uskotaan sijaitsevan Euroopassa.

Rock Phishin hyökkäysten määrä on merkittävä. Ryhmä on toteuttanut arviolta yli 50 prosenttia kaikista verkkourkintatapauksista maailmassa. Taloudelliset menetykset ovat kohonneet kymmeneen miljooniin euroihin. Tähän asti ryhmän ei ole tiedetty hyödyntäneen hyökkäyksissään aidolta näyttäviä haittaohjelmia.

Uudet verkkohyökkäykset yhdistävät tietojen kalastelun ja haittaohjelmat. Rikolliset pyrkivät hyökkäyksen aikana hankkimaan luottamuksellisia tietoja ja välittämään niitä edelleen. Samanaikaisesti koneelle tarttuu harmittoman näköinen ohjelma, troijalainen.

Zeus-nimisen troijalaisen avulla verkkorikolliset voivat varastaa kaikkea henkilökohtaista tietoa aina, kun käyttäjä liikkuu millä tahansa verkkosivuilla. Troijanhevonen voi määritelmän mukaan olla naamioitu hyödylliseksi esimerkiksi käyttämällä sopivaa nimeä tai sisällyttämällä ohjelmaan myös hyödyllisiä

ominaisuuksia. RSA ilmoittaa, että sen tietoturvapalvelu on perehtynyt Zeus-nimiseen troijalaiseen, sen leviämistapaan ja muunnoksiin. Zeuksesta on tähän mennessä löytynyt yli 150 varianttia, jotka yrittävät hyökätä finanssiryhteisiin ja muihin maailmanlaajuisiin organisaatioihin

<http://www.digitoday.fi/tietoturva/2008/04/25/rock-phish--ryhma-iskee-uudella-tekniikalla-pankkeihin/200811592/66>