

## Selainvoro nappaa tiedot verkkopankkikohtaisesti

21.11.2007 15:50 — Timo Poropudas  
[timo.poropudas@sanoma.fi](mailto:timo.poropudas@sanoma.fi)

F-Secure varoittaa uudesta tavasta viedä käyttäjiltä verkkopankkitunnuksia. Hyökkäyksiin käytetään "Man in the Browser" -tekniikkaa, joka nappaa tunnukset selainistunnosta ja välittää ne rikollisten palvelimiin.

"Man in the Browser" perustuu tietokoneessa olevaan haittaohjelmaan, joka aktivoituu vasta käyttäjän mennessä verkkopankkiin. Haittaohjelma pystyy tallentamaan verkkopankin sivustossa syötettävät tiedot (käyttäjänimi ja salasana) kaappaamalla html-koodia käyttäjän internet-selaimesta. Nämä tiedot lähetetään ja tallennetaan verkkorikollisen ftp-sivustoon, josta ne myydään muille verkkorikollisille.

**Verkkorikolliset ovat** aina etsineet keinoja varastaa ihmisten henkilökohtaisia tietoja ja pankkitunnuksia. Rikollisten käyttämät tekniikat ovat kehittyneet pystyäkseen vastaamaan tietoturvaratkaisujen jatkuvaan kehitykseen.

Aluksi tietoja pyrittiin varastamaan näppäinpainallukset tallentavien keylogger-ohjelmien avulla, ja ajan myötä ilmaantui monimutkaisempia keinoja, kuten phishing- ja pharming-tyyppiset verkkohuijaukset.

**Phishingissä** eli tietojen kalastelussa käytetään sähköpostiviestejä, jotka on naamioitu näyttämään rahalaitoksen lähettämiltä viesteiltä. Kun käyttäjä klikkaa viestissä olevaa linkkiä, hänet ohjataan aidolta verkkopankkisivustolta näyttävään huijaussivustoon, joka varastaa käyttäjän sisäänkirjautumistiedot. **Pharming-hyökkäyksissä** käyttäjä ohjataan automaattisesti väärennettyyn sivustoon (joka näyttää hänen oman pankkinsa sivustolta), kun hän yrittää käydä verkkopankissa. Näissä tapauksissa käyttäjän ei tarvitse klikata mitään, sillä verkko-osoitteen väärentäminen tapahtuu internet-tasolla. "Man in the Middle" -huijauksissa verkkorikollinen esiintyy pankin sivustona, kaappaa käyttäjän syöttämät tiedot, ja käyttää niitä päästäkseen käsiksi uhrin pankkitiliin.

F-Securen mukaan uuden haittakäyttäytymisen tarkkailuun perustuvat tietoturvaohjelmat ovat paras vastine tällaisille hyökkäyksille, sillä haittakoodit suunnitellaan nimenomaan

---

tietyille verkkopankeille. Toisin kuin esimerkiksi phishing-viestejä, haittakoodoja ei levitetä massoittain. Tällainen rajoitettu levitys tekee viruskuvausten ja virustunnisteiden laatimisesta hyvin haasteellista.

- **Tietojen kalastelu** on menettämässä tehoaan, koska pankit ovat tehostaneet sivustojensa sisäänkirjautumisen suojausta. Samasta syystä "Man in the Browser" -tyyppisten hyökkäysten määrä on kasvussa, sanoo F-Securen tutkimusjohtaja **Mikko Hyppönen**.

<http://www.digitoday.fi/tietoturva/2007/11/21/selainvoro-nappaa-tiedot-verkkopankkikohtaisesti/200729544/66>