

F-Secure: Kaupallisten ohjelmistojen ei pitäisi käyttää rootkit-teknikoita

1.11.2005 15:03 — Jaakko Kuivalainen

F-Secure on julkaissut teknisen kuvauksen Sony BMG:n rootkit-kopiosuojauksen toiminnasta. Tutkimusjohtaja **Mikko Hyppönen** sanoo ymmärtävänsä, miksi suojaus halutaan piilottaa, mutta lisää, ettei hän asentaisi moista ohjelmaa ainakaan omalle tietokoneelleen.

Hyppönen kertoo digitodaylle, että yhtiö löysi rootkit-ominaisuuden Sony BMG:n kopiosuojauksesta kolme viikkoa sitten. Hänen tietojensa mukaan suojausta käytetään toistaiseksi vain USA:ssa myytävissä levyissä.

Hyppönen sanoo ymmärtävänsä, miksi kuluttajat eivät pidä kyseisen kopiosuojauksen toiminnasta, mutta myös sen, miksi kopiosuojaustekniikka halutaan piilottaa ja sen poistaminen estää. Omalle koneelleen hän ei moista asentaisi, hän lisää.

- Meidän tietojemme mukaan järjestelmä on ollut käytössä maaliskuusta 2005 asti. Ostimme testiä varten muutamia Sony BMG:n levyjä Amazon.comista ja voimme vahvistaa niiden sisältäneen kyseisen tekniikan, Hyppönen kirjoittaa yhtiön blogissa.

F-Securen viruskuvauksessa huomautetaan, että rootkit-teknikoiden käyttäminen kaupallisissa ohjelmistoissa on "erittäin sopimatonta".

- Järjestelmä on toteutettu niin, että sen avulla myös virukset (ja muut haitalliset ohjelmat) voisivat käyttää rootkittiä piilottamaan itsensä. Tämä voi johtaa tilanteeseen, jossa virus jää havaitsematta, vaikka käyttäjällä on päivitetty virustorjuntaohjelmisto asennettuna, jatkaa Hyppönen.

F-Secure Internet Security 2006 tunnistaa Sonyn rootkitin ja myös haittaohjelmat, jotka saattavat piilotella sen suojissa.

Yhtiö suosittelee kääntymään poisto-ohjeissa Sony BMG:n asiakaspalvelun puoleen, koska tietoturvaohjelmistojen poisto-ominaisuuden käyttö saattaa estää cd-rom-aseman

toiminnan.

F-Securen viruskuvauksessa korostetaan, että tietoturvaohjelmistojen hälytykset ovat vääriä, koska ohjelma ei ole haitallinen.

Digitodayn tekijänoikeuslaki-blogissa [vokeskustella](#) Sony BMG:n toiminnasta.

<http://www.digitoday.fi/tietoturva/2005/11/01/f-secure-kaupallisten-ohjelmistojen-ei-pitaisi-kayttaa-rootkit-tekniikoita/200516822/66>