

## Sony BMG:n kopiosuojaus käyttää rootkit-tekniikkaa

1.11.2005 10:32 — Jaakko Kuivalainen

Sony BMG:n cd-levyjen uusi kopiosuojaus asentaa omia ohjelmiaan käyttäjän tietokoneelle, vaarantaa tietoturvan ja yrittää estää asennettujen komponenttien poistamisen rootkit-tekniikan avulla, kertoo rootkittien poisto-ohjelman kehittäjä.

Rootkit-tekniikat ovat tapoja, jolla tavallisesti haittaohjelmat tai tietomurroissa käytetyt työkalut piilotetaan käyttäjän ja tietoturvaohjelmien näkyvistä.

Ilmaisohjelmistoja kehittävän Sysinternalsin piiloteknikoiden asiantuntija **Mark Russinovich** kertoo blogissaan löytäneensä kehittämällään Rootkit Revealer -skannausohjelmalla eräästä tietokoneestaan piilotettuja tiedostoja.

### Toisen sukupolven kopiosuojaus

Tarkemman selvityksen jälkeen hänelle selvisi, että tihutyön takana oli Sony BMG:n julkaisema kopiosuojattu levy. Kopiosuojauksen on kehittänyt brittiläinen First 4 Internet. Suojaus on levy-yhtiöiden markkinointikielessä ristitty toisen sukupolven kopiosuojauksiksi, ja se antaa käyttäjän tehdä kolme kopiota levystä.

Suojaus toteutetaan asentamalla ylimääräisiä ohjelmia tietokoneelle. Russinovichin mukaan rootkit-tekniikan vuoksi tavallinen käyttäjä ei havaitse kaikkia muutoksia järjestelmässä.

Muutokset myös vaarantavat järjestelmän tietoturvan. Russinovichin mukaan tietokoneeseen olisi mahdollista jatkossa piilottaa muitakin ohjelmia, koska rootkit piilottaa kaikki exe-tiedostot, jotka alkavat merkkijonolla "\$sys\$".

### "Turhauttavaa ja ärsyttävää"

Hän kertoo, että piilo-ohjelman poistaminen oli äärimmäisen vaikeaa.

- Koko kokemus oli äärimmäisen turhauttava ja ärsyttävä. Sony ei ainoastaan asentanut järjestelmäni ohjelmistoja, jotka käyttävät haittaohjelmien tavallisesti käyttämiä tekniikoita piilottamaan olemassaolonsa, mutta ohjelma on myös huonosti

---

kirjoitettu, eikä se anna poistaa itseään.

- Ja mikä vielä pahempaa useimmat RootkitRevealer -ohjelman käyttäjät, jotka huomaavat piilotetut tiedostot, lamauttavat tietokoneensa yrittäessään poistaa tavallisin toimenpitein piilotettuja tiedostoja, Russinovich kirjoittaa.

Russinovichin mukaan [käyttäjälisenssit](#) ei ole mainintaa asennettavista ohjelmista, joita ei voi poistaa.

## F-Secure tutkinut jo tovin

F-Secure tutkimusjohtaja **Mikko Hyppönen** kertoo kyseisen kopiosuojauksen käyttämien tekniikoiden olleen jo tovin tutkittavana. Yhtiöltä on luvassa lisätietoja jo tänään.

F-Secure esitteli alkuvuonna kehittämänsä BlackLight-tekniikan rootkit-ohjelmien tunnistamiseen. Tekniikka on lisätty yhtiön virustorjuntaohjelmien 2006-versioihin.

Helsinkiläinen **Matti Nikki** ja Hurjat Hipit -yhtye ruotivat noin viikko sitten uutta tekijänoikeuslakia testaamalla yhdessä kappaleessa niin ikään rootkit-tekniikkaa hyödyntävää suojausta. Suojaus estää kappaleen kuuntelun lopettamisen.

*Aiheesta tulossa lisää tietoa digitoday [Tekijänoikeuslaki-blogiin](#), jossa Sonyn tempauksesta voi myös vaihtaa ajatuksia.*

Uutta aiheesta: [F-Secure: Kaupallisten ohjelmistojen ei pitäisi käyttää rootkit-tekniikkaa](#) [Sony BMG: Suomeen valittavasta kopiosuojatekniikasta ei ole tietoa](#)

<http://www.digitoday.fi/tietoturva/2005/11/01/sony-bmgn-kopiosuojaus-kayttaa-rootkit-tekniikkaa/200516791/66>