

## Sony BMG:n DRM:n poistaja avaa takaoven

15.11.2005 10:26 — Jaakko Kuivalainen

**Alex Halderman** ja **Ed Felten** kertovat todistaneensa oikeiksi Matti Nikin löydöt Sony BMG:n rootkit-DRM:n poistossa käytetyn ActiveX-komponentin tietoturva-aukoista. Sony BMG:n ActiveX:llä hyökkääjä voi pahimmillaan saada tietokoneen hallintaansa.

Sony BMG tarjoaa sivuillaan kohutun rootkitin poistoon päivityksen, joka jättää itse DRM:n komponentit tietokoneeseen. Kaikkien lisäosien poistoa mielivän pitää pyytää poisto-ohjelmaa erikseen levy-yhtiön asiakaspalvelusta. Tässä yhteydessä tietokoneelle asennetaan ActiveX-komponentti, jolla varmistetaan, ettei myöhemmin saatavaa poistolinkkiä käytetä eri koneessa.

Kotimaisen version rootkit-suojauksesta tehnyt Matti Nikki kertoi viikonloppuna [digitodayn Tekijänoikeuslaki-blogissa](#) löytäneensä todennäköisesti vakavan tietoturva-aukon Sony BMG:n ActiveX:stä. Aukko liittyy komponentin tarjoamiin metodeihin, joita ovat muun muassa "ExecuteCode" ja "InstallUpdate".

Princetonin yliopiston jatko-opiskelija Alex Halderman ja hänen ohjaajansa professori Edward Felten kertoivat myöhään maanantaina tutkineensa ActiveX:n toimintaa Nikin vihjeestä. He sanovat laatineensa toimivan esimerkkihyväksikäytön, joka osoittaa, että komponenttia voi käyttää ylimääräisten ohjelmien asentamiseen. Hyödyntäminen onnistuu pelkällä muokatulla www-sivulla.

Nikki esitteli jo viikonloppuna [omilla sivuillaan](#), kuinka Sony BMG:n ActiveX:llä tietokoneen saa käynnistymään uudestaan.

Toistaiseksi ei ole tiedossa, jääkö Sony BMG:n ActiveX tietokoneeseen myös sen jälkeen, kun itse DRM on poistettu.

Felten ja Halderman kertovat [Freedom to Tinker -blogissa](#) julkaisevansa tietonsa piakkoin.

Microsoftin ActiveX-tekniikka toimii vain Internet Explorer -selaimissa, eikä Sony BMG:n rootkit-kopiosuojauksen asennuskaan onnistu kuin Windows-järjestelmissä, joissa

---

käyttäjä on kirjautunut ylläpitäjänä koneeseen.

*Sony BMG:n ActiveX:n tietoturvariskeistä keskusteluun voi osallistua [digitodayn Tekijänoikeuslaki-blogissa](#)*

<http://www.digitoday.fi/tietoturva/2005/11/15/sony-bmgn-drmn-poistaja-avaa-takaoven/200517304/66>