

## Tutkija: SonyBMG:n rootkit on levinnyt piraattilevyissä

17.1.2006 09:57 — Jaakko Kuivalainen

Tietoturvatutkija **Dan Kaminskyn** mukaan SonyBMG:n rootkit-kopiosuojaus löytyy yhä sadoista tuhansista tietokoneista ympäri maailmaa. Hän arvioi, että levinneisyys johtuu piraattilevyistä. Kopiosuojausta käytettiin pääasiassa Pohjois-Amerikassa myydyissä levyissä.

SecurityFocus kertoo Kaminskyn selvittäneen SonyBMG-rootkitin eli XCP-kopiosuojausohjelman levinneisyyttä joulukuun puolen välin aikaan. Hän kertoi tuloksistaan ShmooCon-tietoturvatapahtumassa viime viikonloppuna.

Kaminskyn selvitys perustuu dns-palvelimien välimuistitietojen kyselyyn. Menetelmä kertoo, kuinka moni nimipalvelin on välittänyt kopiosuojausohjelmasta lähtöisin olevaa liikennettä.

### Armeijoiden verkoissa

Joulukuun selvityksestä käy ilmi, että eri puolilla maailmaa on noin 350 000 verkkoa, joiden dns-palvelimilla on välimuistissa tieto osoitteesta, jota vain kopiosuojausohjelma käyttää. Joukossa on myös paljon eri maiden valtionhallinnon ja armeijoiden verkkoja, SecurityFocus kertoo.

XCP:llä suojattuja levyjä myytiin SonyBMG:n mukaan hieman yli kaksi miljoonaa kappaletta, pääasiassa Yhdysvalloissa.

Rootkit piilottaa kopiosuojausohjelman käyttäjältä. Asiasta nousi kohu lokakuun lopulla, kun Windows-asiantuntija **Mark Russinovich** kertoi löytäneensä SonyBMG:n julkaisemasta cd-levystä peräisin olevan rootkitin koneeltaan.

### Kopiosuojattu piraattilevy?

Kaminskyn mukaan maailmanlaajuinen leviäminen osoittaa myös, kuinka suuri ongelma piratismi on.

- On todennäköistä, että iso osa levyistä on ollut piraattiversioita,

---

hän selittää.

Piraattilevyjen valmistajat voivat kopioida suojattuja levyjä helposti tekemällä niistä iso-imagen eli levykuvatiedoston . Näin piraattiversioon tulee myös itse kopiosuojaus.

Osa Yhdysvaltojen ulkopuolelle päätyneistä kopiosuojatuista levyistä on peräisin verkkokaupoista. Muun muassa Amazon.comin listoilla oli useita XCP:llä suojattuja levyjä. Myös Suomessa myytiin virallisten kanavien ohi Yhdysvalloista tuotuja levyjä ainakin muutamia kymmeniä kappaleita.

<http://www.digitoday.fi/tietoturva/2006/01/17/tutkija-sonybmgn-rootkit-on-levinnyt-piraattilevyissa/20063634/66>