

Kaspersky löysi ensimmäisen Sony-rootkit-trojialaisen

10.11.2005 14:57 — Jaakko Kuivalainen

Virustorjuntayhtiö Kaspersky Lab kertoo löytäneensä torstaina ensimmäisen haittaohjelman, joka piiloutuu Sony BMG:n kopiosuojauksen rootkitin avulla. Ohjelma avaa hyökkääjälle takaoven tietokoneeseen.

Kaspersky kertoi lyhyesti asiasta torstaina iltapäivällä. Yhtiön mukaan kyseessä on takaoviohjelma, joka käyttää kopiosuojauksen rootkit-ominaisuutta piiloutumiseen. Vihulainen on saanut nimen "Backdoor.Win32.Breplibot.b". Tarkempia tietoja ohjelman toiminnasta Kaspersky lupaa vielä torstain aikana.

Virustorjuntayhtiö Sophoksen mukaan Breplibotin a-versio on troijalainen, joka avaa tietokoneeseen takaoven ja jonka avulla hyökkääjä voi ladata lisää haitallisia tiedostoja koneelle. Ohjelma ei leviä itsestään.

F-Securen tutkimusjohtaja **Mikko Hyppönen** kertoi torstaina digitodaylle, että ohjelmaa on levitetty noin kymmeneen tuhanteen sähköpostiosoitteeseen aamupäivän aikana. Hyppönen vahvistaa, että ohjelma ei leviä itsekseen. Saastuneita koneita voidaan käyttää esimerkiksi roskapostien lähettämiseen.

Sony BMG:n käyttämä XCP-kopiosuojaus asentaa käyttäjän tietokoneelle ylimääräisiä komponentteja, jotka se piilottaa käyttöjärjestelmältä. Samalla suojaus tulee piilottaneeksi kaikki tiedostot, joiden nimessä on "\$sys\$". F-Securen mukaan virustorjuntaohjelmat eivät välttämättä löydä kopiosuojauksen piilottamia haittaohjelmia.

F-Securen arvion mukaan kyseisen rootkitin sisältäviä levyjä on myyty Yhdysvalloissa useita miljoonia. Sony on kertonut suojauksen olevan käytössä 20 nimikkeessä. XCP-suojauksella varustettuja levyjä on myös myyty muutamia kappaleita Suomessa liikkeissä, jotka tuovat levynsä itse maahan. Amazon.comin kautta levyjä on voinut ostaa käytännössä mistä tahansa.

Sonyn on julkaissut verkossa "päivityksen", joka poistaa

rootkit-ominaisuuden.

Päivitys klo 15.47: Lisätty työmatkalta tavoitetun Mikko Hyppösen kommentti.

<http://www.digitoday.fi/tietoturva/2005/11/10/kaspersky-loysi-ensimmaisen-sony-rootkit-trojikalaisen/200517190/66>