

## F-Secure ja Mark Russinovich varoittivat Symantecia Nortonin rootkit-ominaisuudesta

12.1.2006 09:57 — Jaakko Kuivalainen

Symantec on korjannut Norton SystemWorks-ohjelmistostaan ominaisuuden, joka piilottaa tiedostoja virustorjunnalta ja Windowsin tiedostonhallinnalta. SonyBMG:n rootkit-jupakassa kunnostautuneet F-Secure ja Windows-guru Mark Russinovich saavat Symantecin varoituksessa kiitosta ongelman osoittamisesta.

Symantecin [varoituksen](#) mukaan Norton Protected Recycle Bin -ominaisuus on periaatteessa mahdollistanut haittaohjelmien piilottamisen käyttäjältä ja myös virustorjuntaohjelmien ajastetuilta ja manuaalisilta skannauksilta. Ominaisuuden tarkoitus on pitää yllä varmuuskopiota käyttäjän poistamista tiedostoista.

Yhtiö julkaisi päivityksen saatuaan ensin varoituksen ominaisuuteen liittyvistä ongelmista sekä F-Securelta että Sysinternalsin RootkitRevealer-ohjelman kehittäjältä Mark Russinovicilta. Päivitys tekee Nprotect-nimisestä kansioista normaalisti näkyvän.

Symantecin mukaan kansion piilotuksella pyrittiin estämään käyttäjää poistamasta vahingossa varmuuskopioita, joiden avulla järjestelmästä poistettuja tiedostoja voidaan palauttaa.

F-Securen tutkijat ja Russinovich löysivät lähes samanaikaisesti syksyllä myös SonyBMG:n XCP-kopiosuojauksen kohutun rootkit-ominaisuuden. Russinovich ennätti raportoidaan niistä ensimmäisenä julkisuudessa.

Russinovich sanoo eWeekille pitävänsä huolestuttavana, että kaupallisista ohjelmistoista löytyy rootkitin tapaisia ominaisuuksia. Hän huomauttaa, että toisin kuin Sony BMG:n tapauksessa Nortonin piilotoiminnolla on yritetty auttaa käyttäjää.

F-Securen tutkimusjohtajan **Mikko Hyppösen** mukaan Symantecin tapauksessa ongelma ei ollut vakavimmasta päästä, mutta hän pitää silti hyvänä asiana, että yhtiö päätti korjata sen.

---

Eweekin mukaan F-Secure sai keväällä vihiä Nortonin piilokansiosta BlackLight-ohjelman käyttäjiltä ja ryhtyi selvittämään asiaa tarkemmin.

Norton SystemWorks ja SystemWorks Premierin käyttäjät saavat päivityksen automaattisesti tuotteiden LiveUpdate-päivityksenä.

<http://www.digitoday.fi/tietoturva/2006/01/12/f-secure-ja-mark-russinovich-varoittivat-symantecia-nortonin-rootkit-ominaisuudesta/20063497/66>