

## Bagle piiloutuu rootkitillä

28.3.2006 14:24 — Tuomas Karvonen

Panda Softwaren viruslaboratoriossa on tunnistettu uusia Bagle-madon variantteja, joilla on rootkit-ominaisuuksia, kuten tiedostojen, toimintojen ja rekisterimerkintöjen piilottaminen. Näin ollen ne pystyvät piilottamaan olemassaolonsa ja myös tekemänsä toiminnot, Panda korostaa.

Uudet Bagle-madot yrittävät esimerkiksi lopettaa saastuttamastaan koneesta useita toimintoja ja lisäksi yrittävät ladata koneeseen tiedoston/tiedostoja, joka voi olla esimerkiksi toinen haittaohjelma.

Lopetettavat toiminnot kuuluvat esimerkiksi tietoturvaohjelmistoille, virustorjuntaohjelmille ja palomuuireille, joten kone jää haavoittuvaksi muiden haittaohjelmien hyökkäyksille.

- Rootkitien tekemisestä ja myymisestä on tullut selvä osa järjestäytynyttä rikollisuutta: koska ne pystyvät piiloutumaan perinteisiltä tietoturvaohjelmistoilta, ne mahdollistavat näkymättömän hyökkäyksen. Hyökkääjien motiivi on ennen kaikkea taloudellisen hyödyn tavoittelu. Suosittelemme perinteisen virustorjunnan täydentämistä proaktiivisella suojalla, kommentoi Pandan viruslaboratorion johtaja **Luis Corrons**.

F-Secure huomioi lisäksi, että ainakin yhdessä uudessa rootkit-Baglessa näyttäisi olevan ohjelmointivirheitä, joten kyseessä on varhainen versio. Tämä näyttäisi kuitenkin olevan vaarallinen ensiaskel, ja kehitystä kannattaa F-Securen mukaan seurata, jos Bagle-matojen tekijät ovat vakavissaan päättäneet päivittää haittaohjelmaperheensä rootkiteillä.

<http://www.digitoday.fi/tietoturva/2006/03/28/bagle-piiloutuu-rootkitilla/20066119/66>