

Ryhmätyö kasvattaa rootkit-kiusaa

8.5.2006 16:28 — *Tuomas Karvonen*

Haittaohjelmia ja muita vahingollisia ohjelmia piilottavien stealth-tekniikoiden käyttö yleistyy, McAfee kertoo. Pelkästään viimeisten kolmen vuoden aikana stealth-tekniikkaa käyttävien tapausten määrä on kasvanut yli kuudellasadalla prosentilla.

McAfee uskoo stealth-tekniikoiden nopean yleistymisen johtuvan internetissä tapahtuvista ryhmatöistä, joiden sivustoilla käytetään rootkit-ohjelmien lisäksi satoja rivejä rootkit-koodia, jota voi muokata, parantaa ja kääntää uudelleen.

Rootkit-koodien ja stealth-kehityskittien avulla haittaohjelmien tekijät voivat helpommin piilottaa prosesseja, tiedostoja ja rekisteritietoja ilman syvällistä käyttöjärjestelmän tuntemusta, yhtiö hahmottaa.

Stealth-tekniikoiden tehokkuus ja monipuolisuus ovat levittäneet ne lähes kaiken tyyppiin haittaohjelmiin. Niiden suosio on kasvanut haittaohjelmista jopa kaupallisiin ohjelmistoihin, McAfee muistuttaa.

McAfee Avert Labsin tutkimuksen mukaan vuonna 2001 Linux-pohjaisten tekniikoiden osuus kaikista stealth-haivattatekniikoista oli 71 prosenttia. Osuus on laskenut vuoteen 2005 mennessä lähes merkityksettömäksi, kun taas Windows-pohjaiset stealth-tekniikat lisääntyivät 2300 prosenttia.

<http://www.digitoday.fi/tietoturva/2006/05/08/ryhmatyo-kasvattaa-rootkit-kiusaa/20067237/66>