

Windowsin verkkomatoon vaikea tarttua

7.1.2009 08:48 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Suomessa liikkuva verkkomato on vahvistunut Microsoftin laajalti uutisoituun Windows-aukkoon iskeväksi. Madosta on havaittu eri muunnelmia, eikä siitä pääse helposti eroon.

Cert-Fi päättelee saamiensa analyysitulosten perusteella, että [Suomessakin esiintyneestä verkkomadosta](#) on olemassa useita eri variantteja.

Yksi varianteista kulkee nimellä [Worm:Win32/Conficker.B](#) (tunnettu myös nimellä [Worm:W32/Downadup.AL](#)). Tämä osaltaan vahvistaa epäilyn siitä, että mato käyttää lähiverkossa leviämiseen hyväksyttävää [Microsoftin korjaamaa MS08-067-haavoittuvuutta](#).

Madon teknisistä kuvauksista käy Cert-Fi:n mukaan ilmi, että mato myös levittää itseään arvaamalla pääkäyttäjän tunnussanoja lähiverkkojen levyjaoille. Tämä selittää osaltaan Windows-toimialueen hallintapalvelimelle kasvaneen liikenteen sekä sen, että toimialueen tunnuksia voi mennä lukkoon.

Verkkomato myös käyttää hyväkseen esimerkiksi tiedostoattribuutteihin liittyviä keinoja itsensä piilottamiseen. Näiden keinojen takia verkkomadon poistaminen voi olla työlästä, ja matojen saastuttamien tietokoneiden siivoamiseen käsin tulee suhtautua suurella varauksella, Cert-Fi huomauttaa.

Cert-Fi on aikaisemmin julkaissut [erillisen ohjeen](#) haittaohjelman saastuttamaksi epäilyn Windows-järjestelmän tutkimista varten.

<http://www.digitoday.fi/tietoturva/2009/01/07/windowsin-verkkomatoon-vaikea-tarttua/2009285/66>