

Witty-mato kuoli nopeasti

23.3.2004 11:42 — Jaakko Kuivalainen

Arviot viikonlopun Witty-madon saastuttamista tietokoneista vaihtelevat 30 000 - 50 000 välillä. Valtaosa koneista saastui ensimmäisen tunnin aikana. Matotartunnan saanut kone pysyi pystyssä keskimäärin puolituntia tuhorutiinin käynnistyttyä.

Internet Storm Centerin **Johannes Ullrich** arvioi Zdnet-uutispalvelun haastattelussa Witty-verkkomadon levinneen noin 30 000 tuhanteen tietokoneeseen. Näistä noin 20 000 sai tartunnan ensimmäisen tunnin aikana lauantaiamuna, Ullrich kertoi.

- Koska mato kaatoi lopulta tietokoneet, se kuoli todella nopeasti, Ullrich selitti Zdnetille.

SANS-instituutin Internet Storm Centerin tilastojen mukaan porttia 4000 skanaavien ip-osoitteiden määrä lähti laskuun alle tunnin nousun jälkeen ja voimakkaimman leviämisen vaihe kesti noin kaksi tuntia.

Tietoturvyhtiö iDefensen arvioi madon saastuttaneen lauantaina ainakin 50 000 tietokonetta.

Tukkoon puolessa tunnissa

Witty kävi läpi leviämisvaiheessa 20 000 satunnaisesti valittua ip-osoitetta etsien haavoittuvia BlackICE-palomuureja. Tämän jälkeen mato aloitti kovalevyn korruptoinnin. Ullrich kertoo kovalevyn kirjoitusrutiinin kaataneen saastuneen koneen noin puolessa tunnissa.

Zdnetin mukaan tietoturvyhtiö Internet Security Systems kertoi maanantaina, että noin kaksi prosenttia asiakkaistaan oli vailla päivitystä, kun Witty aloitti leviämisensä. ISS julkaisi paikkauksen alunperin tietoturvyhtiö eEye Digital Securityn löytämälle aukolle keskiviikkoiltana.

<http://www.digitoday.fi/tietoturva/2004/03/23/witty-mato-kuoli-nopeasti/20048670/66>