

BIOS:iin pesiytyvää haittaohjelmaa on mahdoton poistaa

24.3.2009 06:34 — Olli Sulopuisto

CanSecWest-tapahtumassa esiteltiin tekniikka, jota käyttämällä haittaohjelma voi saastuttaa BIOS:in lopullisesti.

Haittaohjelmat voivat tartuttaa PC-koneen [BIOS:in niin, että uudelleenkäynnistys tai BIOS:in uudelleenohjelmointi eivät auta](#). [Core Security Technologiesin Anibal Sacco](#) ja [Alfredo Ortega](#) esittelivät tekniikan CanSecWest-konferenssissa. He tartuttivat mallin vuoksi Windows-koneen, OpenBSD:tä ajavan pc:n ja VMware-virtuaalikoneen.

Päästäkseen käsiksi BIOS:iin ohjelman pitää ensin saada pääkäyttäjän oikeudet, mutta sen jälkeen siitä eroon pääseminen on käytännössä mahdotonta. Mikään ei estä kehittämästä toista haittaohjelmaa, joka hankkii BIOS-syöpäläiselle tarvittavat oikeudet asentamista varten.

<http://www.digitoday.fi/tietoturva/2009/03/24/biosiin-pesiytyvaa-haittaohjelmaa-on-mahdoton-poistaa/20097728/66>