

## Suomalainen www-palvelin levitti toistuvasti haittaohjelmia

14.10.2008 12:38 — Kalevi Nikulainen

Viestintäviraston tietoturvaüksikkö CERT-FI kertoo, että sen tietoon on tullut suomalainen www-palvelin, jota käytettiin toistuvasti haittaohjelmien jakamiseen.

Yksikkö selvittää, että palvelimella olleiden haavoittuvuuksien vuoksi palvelimelle saatiin jatkuvasti lisättyä uusia haitallisia ohjelmistoja, vaikka niitä aika ajoin myös poistettiin.

CERT-FI:n mukaan tutkimukset palvelimen ylläpitäjän roolista tapauksessa ovat kesken.

Viestintäviraston tietoturvaüksikkö huomauttaa uudessa [tietoturvakatsauksessaan](#), että internet-verkossa esiintyvät haitalliset ilmiöt, kuten haittaohjelmien levitys, tietoa keräävien haittaohjelmien tiedontallennuspalvelimet ja botnet-verkkojen komentopalvelimet tarvitsevat palvelinresursseja toimiakseen tehokkaasti.

Yksikkö kertoo Hosting-palveluntarjoajien joukossa on yrittäjiä, joiden käytössä olevista verkko-osoitteista tavataan keskimääräistä enemmän haitalliseksi luettavaa sisältöä tai liikennettä.

Syy haitallisen sisällön keskittymiseen voi olla yrityksen välinpitämätön linja asiakkaitensa tarjoamien palvelujen laatuun. Joillekin tämä saattaa olla myös tarkoituksellisesti ylläpidetty kilpailuetu, CERT-FI arvioi.

### Tietyt verkkolohkot usein esillä

Yksi usein esiin tullut palveluntarjoaja oli San Franciscossa toiminut Intercage, jonka hallitsemat verkkolohkot ovat tulleet usein esiin haittaohjelmatapausten yhteydessä. Sen asiakkaana on ollut Estdomains-niminen verkkotunnusten tarjoaja, joka liittyy moneen haitallisessa käytössä olleeseen verkkotunnukseen. Tietoturva yhteisön painostuksen vuoksi Intercagelle verkkoyhteyksiä tarjonneet operaattorit katkaisivat sen yhteydet syyskuun lopussa. Estdomains jatkaa toimintaansa käyttäen muiden palveluntarjoajien

---

yhteyksiä. Osa Intercagen käyttämistä verkko-osoitteista on siirtynyt toisille palveluntarjoajille.

Aikaisemmin on ollut esillä myös pietarilaisen Russian Business Network -palveluntarjoajan toiminta. RBN poistui verkosta marraskuussa 2007. CERT-FI:n mukaan Intercagen ja RBN:n tyyppisiä palveluntarjoajia on kuitenkin tälläkin hetkellä toiminnassa useita.

<http://www.digitoday.fi/tietoturva/2008/10/14/suomalainen-www-palvelin-levitti-toistuvasti-haittaohjelmia/200826754/66>