

Virolainen palveluntarjoaja hääti superspammarin palvelimiltaan

28.11.2008 09:28 — Marko Mannila

Pieni virolainen Starline Web Services katkaisi valtavan Srizbi-bottiverkon yhteydet. Suuren osan maailman roskapostista lähettävä Srizbi on häädetty jo Yhdysvalloistakin.

Starlinen palvelimet ylläpitivät neljää verkkotunnusta, jotka turvayhtiö ControlEye havaitsi Srizbin kontrollipisteiksi. Srizbi on vaikeasti poistettava rootkit-tyyppinen haittaohjelma, jonka arvioidaan muodostavan yhden maailman suurimmista bottiverkoista. Srizbin verkossa arvioidaan olevan 450 000 tietokonetta, joista lähtee valtava määrä roskapostia.

Srizbi häädettiin aiemmin tässä kuussa kalifornialaisen McColon palvelimilta. Srizbissä on kuitenkin varamekanismi, jolla bottiverkon haltijat pystyvät ottamaan katkon jälkeen uudelleen yhteyden verkkoon.

Srizbissä on algoritmi, joka tietysin väliajoin luo uusia verkkotunnuksia. Srizbi tunnustelee, ovatko kyseiset verkkotunnukset käytössä ja alkaa ottaa vastaan verkkotunnuksista tulevia käskyjä.

Roskapostittajien, joilla on hallussaan sama algoritmi, rekisteröivät kyseiset verkkotunnukset ja voivat siten jatkaa toimintaansa. He tarvitsevat kuitenkin palveluntarjoajan ylläpitämään palvelimiaan.

Starlinen yhteyksiä ylläpitää virolainen Compic. Viron CERT on useasti valittanut Compicin suosivan haittaohjelmia ylläpitäviä sivuja, PC World kertoo.

<http://www.digitoday.fi/tietoturva/2008/11/28/virolainen-palveluntarjoaja-haati-superspammarin-palvelimiltaan/200830803/66>