

Roskapostittaja siirtyi Venäjälle TeliaSoneran avulla

19.11.2008 16:40 — Perttu Pitkänen
perttu.pitkanen@sanoma.fi

Puolet maailman roskapostista lähettänyt McColo-yhtiö on ilmeisesti siirtänyt työkalunsa venäläisille palvelimille, kun yrityksen verkkoyhteydet katkaistiin viime viikolla. Välytyskanavan tarjosi TeliaSonera.

Viime viikolla [roskapostin määrä putosi noin 70 prosenttia](#) kalifornialaisen McColo -yhtiön palvelimet irrotettiin verkosta.

Viikonloppuna yhtiö heräsi taas henkiin välittääkseen roskapostia suoltavan bottiverkkonsa hallinnan Kaliforniasta Venäjällä sijaitseville palvelimille [Kertoo The Register -verkkolehti](#).

McColo siirsi viikonloppuna dataa Venäjälle noin 12 tuntia tiedonvarmistussopimuksen ansiosta, jonka yhtiö oli tehnyt TeliaSoneran kanssa.

The Registerin haastattelema Trend Micron asiantuntija **Paul Ferguson** arvioi, että tietojen siirtäminen viikonloppuna oli varmasti tarkkaan harkittua. Todennäköisesti roskapostittajat arvelivat, että töissä olisi vähemmän väkeä, ja heidän huomattaisiin vasta maanantaina.

Ferguson on tehnyt tapahtumasta [raportin \(pdf\)](#) yhdessä toisen tutkijan Jet Arminin kanssa. Tutkijat eivät syytä TeliaSoneraa.

Sopimuksen TeliaSoneran ja McColon välillä väliin [Gigamon](#), kalifornialainen verkkokaistan tukkukauppaan erikoistunut yritys. McColon sijasta asiakkaaksi sopimukseen oli merkitty CWIE Holding Company. TeliaSonera katkaisi yhteyden, kun tutkijat havaitsivat, että tiedon siirtäjä oli McColo.

Tietoturvayhtiö FireEyen mukaan tiedonsiirrossa päivitettiin muun muassa venäläisen Rustock-botnetin tartuttamia tietokoneita siten, että nämä odottavat ohjeita uudelta palvelimelta.

Tauko roskapostissa tuskin kestää kovin kauaa, asiantuntijat arvioivat. Tietoturvayhtiö Sophosin mukaan Rustock-

verkosto voi lähettää 30 miljoonaa roskapostia päivässä.

<http://www.digitoday.fi/tietoturva/2008/11/19/roskapostittaja-siirtyi-venajalle-teliasoneran-avulla/200829976/66>