

Verkkoyhteyksien katkaisu USA:ssa vähensi roskapostia Suomessa

14.11.2008 08:34

Tietoturvayhteisön tiiviin yhteistyön seurauksena yhdysvaltalaiselta palveluntarjoajalta katkaistiin alkuviikosta verkkoyhteydet, mikä vaikutti pudottavasti roskapostin määrään, arvioi Viestintäviraston tietoturveysyksikkö CERT-FI.

CERT-FI:n mukaan McColo-niminen palveluntarjoaja on jo pidemmän aikaa ollut merkittävä roskapostia ja muuta haitallista sisältöä levittäneiden botnet-verkkojen komentopalvelimen palvelukeskus. Vasta alkuviikon toimenpiteet osoittivat, miten suuresta haittavaikutuksesta oikeasti on ollut kyse.

Viikon aikana tehdyt toisistaan riippumattomat mittaukset vahvistavat CERT-FI:n mukaan roskapostin määrän vähentyneen merkittävästi.

Tietoturveysyksikön mukaan suomalaisilta postipalveluntarjoajilta saadut ensitiedot vahvistavat tämän havainnon. Optimistisimmat mittatulokset osoittavat, että roskapostin määrä viikon aikana on tippunut kahteen kolmasosaan normaalista. Mittaustuloksia on nähtävillä esimerkiksi SpamCop.net:n [verkkosivuilla](#).

Amerikkalainen McColo ei ole ainoa operaattori, jonka toiminta on ajettu ahtaalle jatkuvien tietoturvaongelmien tai suoranaisten tietoverkkorikosepäilyjen vuoksi, kertoo CERT-FI.

Edistysaskeleita otettu selvästi

CERT-FI:n mukaan vaikuttaisi siltä, että McColon tietoliikenneyhteyksien katkaiseminen on vaikuttanut huomattavan positiivisesti internetissä lähetetyn roskapostin määrään. Vaikka useat raportit tähän viittaisivatkin, on syytä todeta, että CERT-FI:llä ei ole täysin varmaa tietoa siitä, onko havaittu notkahdus kytköksissä juuri tämän operaattorin verkkojen irtikytkemiseen.

Viime aikoina on otettu muitakin vastaavia tietoturvaa potentiaalisesti parantavia edistysaskeleita, toteaa CERT-FI.

Internetin verkkotunnuksia ja osoiteavaruuksia hallinnoiva ICANN-järjestö (Internet Corporation for Assigned Names and Numbers) on pyrkinyt perumaan EstDomains-nimisen verkkotunnusrekisteröijän toimiluvan.

- Vuosien saatossa saamiemme lukuisten raporttien perusteella näyttäisi siltä, että huomattava osa erilaisten tietoturvaloukkausten toteuttamiseen käytetyistä verkkotunnuksista on rekisteröity EstDomainsin kautta. ICANN:in puuttumisperuste tosin liittyy yrityksen johtajien Virossa saamiin valituskelpoisiin tuomioihin. Tämän hetken tiedon mukaan EstDomainsin RAA-status (Registrar Accreditation Agreement) perutaan 24.11. Sen nykyiset asiakkaat pyritään siirtämään toisten verkkotunnusrekisteröijien asiakkaiksi, toteaa CERT-FI [Tietoturvaa Nyt -osiossaan](#).

CERT-FI:n mukaan aikaisemmin Atrivona tunnettu Intercage-niminen yhdysvaltalaisoperaattori menetti tietoliikenneyhteytensä syyskuussa vastaavanlaisessa operaatiossa kuin nyt McColo. Kyseisen yrityksen hallinnoimissa verkkoalueista on CERT-FI:nkin käsittelemien tapauksen valossa jaettu toistuvasti haittaohjelmia sekä operoitu väärennettyjä vastauksia tarjoavia DNS-palvelimia.

- Sekä EstDomains että Intercage tulivat toistuvasti vastaan muun muassa vuodenvaihteen 2005/2006 Windows Metafile (WMF) -haavoittuvuutta hyödyntävien haittaohjelmien yhteydessä. Intercagen nimi on julkisuudessa liitetty EstDomainsin lisäksi myös seuraaviin yrityksiin: Esthost, UkrTeleGroup, Inhoster, Hostfresh ja Cernel. Myös osalta näistä yrityksistä on rajoitettu internet-yhteyksiä operaattoreiden vapaaehtoisin toimin. Myös Intercagen irtikytämisen aikaan uutisoitiin roskapostin määrän vähentymisestä. Tuolloin kuitenkin suomalaiset operaattorit eivät voineet vahvistaa havaintoa, CERT-FI kertoo.

Tarina ajojohdista

Varsin tarkkaan vuosi sitten huipentui myös venäläiseksi luonnehditun Russian Business Networks -nimisen ryhmittymän ajojahti. Myös näiden verkkojen kannalta on esitetty väitteitä toistuvasta ja tahalliseksi luonnehditusta tietoturvaloukkausten tehtailusta. CERT-FI:n tietojen mukaan RBN hylkäsi verkkonsa ja ajoi ainakin osan toiminnoistaan alas.

CERT-FI mainitsi asiasta 9.11.2007 päivätyssä Tietoturva nyt! -artikkelissa ja tietoturvan vuosikatsauksessa 2007. Sittemmin on ollut aika ajoin ollut nähtävissä viitteitä siitä, että RBN-ryhmittymä pyrki palauttamaan toimintojaan

verkkoon. Verkkojen irtikytkemisen vaikutuksista on yleiseen tietoturvatilanteeseen on esitetty spekulatioita, mutta tällä viikolla nähdyn roskapostin dramaattisen vähenemisen kaltaista vaikutusta ei ole pystytty osoittamaan.

Yhteistä näille tapauksille on se, että aloite yhteyksien alasajoon on tullut tietoliikennepalvelujen tarjoajilta, jotka ovat perustaneet tietonsa vapaaehtoisten tietoturvatutkijoiden laatimiin raportteihin. Mahdollisten rikosepäilyjen selvittämistä haittaa toiminnan globaali luonne ja tapauksista kärsineiden asianomistajien passiivisuus. Positiivinen poikkeus on esimerkiksi Microsoft, joka on syyskuussa haastanut lukuisia tietoturvaohjelmistoiksi naamioituneiden haittaohjelmien levittäjiä oikeuteen.

Kirjoittaja: Kalevi Nikulainen

<http://www.itviikko.fi/tietoturva/2008/11/14/verkkoyhteyksien-katkaisu-usassa-vahensi-roskapostia-suomessa/200829543/7>