

FBI:n vakoiluohjelman saloja tuli julkisuuteen

20.4.2009 08:46 — Marko Mannila

FBI:n salainen vakoiluohjelma Cipav latautuu huomaamatta epäilyllin koneelle ja seuraa verkkoliikennettä.

Julkisuuteen tulleiden tietojen mukaan FBI käyttänyt Cipav-ohjelmaa terroristeja ja krakkereita vastaan jopa seitsemän vuotta.

Cipav latautuu huomaamatta kohteen tietokoneelle, kerää tietoja ja lähettää ne FBI:n palvelimelle Virginiaan [Wired](#) [kertoo](#).

Julkisuuslain perusteella esille tulleiden tietojen mukaan Cipav kerää koneen ip-osoitteen, Mac-osoitteen, avoimet portit, listan käytössä olevista ohjelmista, käyttöjärjestelmän tyypin, version ja sarjanumeron sekä oletusselaimen ja version.

Lisäksi Cipav listaa myös koneen rekisteröidyn käyttäjän ja yrityksen nimen, sisään kirjautuneen käyttäjän nimen ja url:n, jossa on viimeksi käyty.

Cipav lähettää kyseiset tiedot FBI:lle ja alkaa sen jälkeen kerätä tietoja koneen verkkokäytöstä. Ohjelma listaa esimerkiksi kaikkien palvelinten ip-osoitteet, joihin kohdekone on yhteydessä.

Paljastuneiden asiakirjojen mukaan FBI ujuttaa Cipavin kohdekoneelle käyttäen todennäköisesti selainten haavoittuvuuksia hyväkseen. Monessa tapauksessa agentit houkuttelivat kohteen käymään verkkosivulla, joka oli sisällytetty Cipav.

Cipav on ollut tärkeässä roolissa monessa tapauksessa. Ohjelmalla [jäljitettiin](#) esimerkiksi vuonna 2005 Ciscoa ja Nasaa kiusannut krakkeri.

Cipavilla paljastui myös sabotööri, joka häiritsi Bostonin alueen verkko- ja kaapelitv-palveluja vuonna 2004. Sabotööri oli yrittänyt salata henkilöllisyytensä välipalvelimilla.

FBI joutuu hakemaan oikeudelta luvan Cipavin käyttöön jokaisessa tapauksessa erikseen.

Wired-julkaisun hankkimat [Cipav-dokumentit](#) (pdf)

<http://www.digitoday.fi/tietoturva/2009/04/20/fbin-vakoiluohjelman-saloja-tuli-julkisuuteen/20099978/66>