

FBI käytti ensimmäisen kerran vakoiluohjelmaa

20.7. 13:47 (päivitetty 13:58) — *Matias Mäki*
matias.maki@sanoma.fi

Yhdysvaltojen liittovaltion poliisi FBI sai oikeuden määräyksellä hyödyntää cipav-nimistä vakoiluohjelmaa lukiolle pommiuhkauksien lähettämistä epäillyn Myspace-tunnukseen.

FBI-agentit saivat oikeudelta luvan käyttää ensimmäisen kerran cipav-nimistä vakoiluohjelmaa pommiuhkausten lähettäjäksi epäiltyä kohtaan.

Cipav on ilmeisesti Windows-haittaohjelma, jonka FBI laukaisee sähköpostin tai pikaviestinten avulla. Ohjelma saastuttaa kohdekoneen sähköpostin, Gmail- tai Myspace-tunnusten kautta. Jälkimmäisissä tapauksissa haittaohjelma leviää verkkopalvelusta käyttäjän koneelle.

Koneelle soluttautumisen jälkeen cipav penkoo kohdekoneen kovalevyn ja sen jälkeen lähettää FBI:lle kaikkien ajossa olevien ohjelmien nimet, selaintiedot, käyttöjärjestelmän tyypin sarjanumeroineen ja loput käyttäjätiedot Windowsin rekisteristä.

Haittaohjelma kirjaa myös ylös kaikki käyttäjän vierailemat nettiosoitteet, muttei käyttäjän sähköisten keskustelujen sisältöjä.

Aiemmin FBI on voinut ainoastaan käyttää näppäinpainallusten nauhoittajia. Organisaatio on tosin tehnyt useita vakoiluohjelmakokeita vuosien varrella. Näistä tunnetuimpia ovat Omnivore ja Magic Lantern.

Washingtonissa sijaitsevaa Timberlinen lukiota pommiuhkauksilla kiusannut koulun entinen oppilas onnistuttiin jäljittämään ohjelmalla. Koulun kiusaaja käytti useita Gmail-tunnuksia ja Myspace-tunnusta uhkausten lähettämiseen.

Lukio tyhjennettiin pilaviestien pommiuhkausten vuoksi useana päivänä. Räjäheteitä ei koskaan löydetty.

Lisäksi uhkailija hyödynsi kolmea Italiassa sijaitsevaa tietokonetta, joihin hän oli murtautunut. Italialaisharhautuksen vuoksi FBI:n piti ottaa cipav käyttöön,

sillä Googlen ja Myspacen toimittamat ip-osoitteet johtivat ainoastaan Italiaan saakka.

Uhkailija pidätettiin tällä viikolla ja hänet tuomittiin häirinnästä ja identiteettivarkaudesta 90 päiväksi nuorisovankilaan.

<http://www.digitoday.fi/tietoturva/2007/07/20/fbi-kaytti-ensimmaisen-kerran-vakoiluohjelmaa/200717564/66>