

## Suomen vakoilussa käytetty Poison Ivy- haittaohjelmaa

11.6.2008 09:42 — Kalevi Nikulainen

Tietoja keräävän troijalaisen ujuttaminen Suomen aseteollisuuden ja valtion järjestelmiin kertoo uuden sukupolven vakoilusta ja kilpailijatiedon keräämisestä. Takaporttitoiminnot näissä iskuissa on hoitanut Poison Ivy –haittaohjelmaperheen jäsen, kertoo F-Securen tutkimusjohtaja Mikko Hyppönen.

Poison Ivy tulee osana troijalaishyökkäystä, joka voi olla naamioitu sähköpostin liitetiedostoksi.

Takaporttiohjelma antaa vakoilijalle lähes täyden kontrollin saastuneeseen tietokoneeseen. Sen tiedostoja voi ladata, muuttaa ja lisätä. Esimerkiksi huppusalaiset asiakirjat voivat nopeasti vaihtaa omistajaa tai niitä voidaan muokata hajaannuksen aiheuttamiseksi.

Haltuun otetun tietokoneen prosesseja voidaan lopettaa, mikä esimerkiksi merkitsee, että tietoturvaohjelmat keskeytetään hyökkäyksen ajaksi. Myös verkkoyhteyksiä voidaan lopettaa.

Poison Ivy antaa myös mahdollisuuden poistaa tietokoneen asennettuja ohjelmia. Myös Windowsin rekisterit ovat täysin editointivalmiina asiansa tietävälle vakoilijalle. F-Securen mukaan haittaohjelman varianteilla voidaan muuttaa ja kohdistaa sen toiminnallisuutta.

<http://www.digitoday.fi/tietoturva/2008/06/11/suomen-vakoilussa-kaytetty-poison-ivy--haittaohjelmaa/200815788/66>