digitoday

Maailman pahin haittaohjelma paljastui

29.5.2012 07:00 — Digitoday *toimitus@digitoday.fi*

Tietoturvayritykset ovat saaneet käsiinsä vakoiluohjelman, joka erään asiantuntijan mukaan on ehkä kaikkien aikojen pahin hyökkäysohjelma. Flame tai Skywiper -nimillä tunnettu sovellus on ilmeisesti länsimaisen vakoilujärjestön käsialaa.

F-Securen blogissa tietoturva-asiantuntija **Mikko Hyppönen** kirjoittaa, että massiivinen, monimutkainen haittaohjelma kerää informaatiota ja vakoilee.

Haittaohjelman kehitti todennäköisesti länsimainen tiedustelu- tai sotilasorganisaatio.

Hyppösen mukaan Flamen pahin puoli se, että se on levinnyt jo vuosia.

- Stuxnet, Duqu ja Flame ovat kaikki esimerkkejä tapauksista joissa me - virustorjuntateollisuus - olemme epäonnistuneet. Kaikki nämä levisivät salassa pitkiä aikoja.

Flame on erittäin monipuolinen vakoiluohjelma. Se kerää tietoa saastuneen tietokoneen näppäimistöltä, näytöltä, mikrofonista, kiintolevyltä, verkkoyhteyksistä, langattomasta lähiverkosta, bluetooth-yhteyksistä, usb-liikenteestä ja järjestelmäprosesseista. Se voi siis esimerkiksi kuunnella tietokoneen ympäristön keskusteluja ja tarkkailla lähistöllä olevia bluetooth-laitteita.

- Skywiper on varmasti hienostunein haittaohjelma, jonka olemme tavanneet, sitä voi hyvällä syyllä väittää monimutkaisimmaksi koskaan löydetyksi haittaohjelmaksi, Crysys Lab kirjoittaa raportissaan, johon *Wall Street Journal* viittaa.

Venäläinen Kaspersky Labs ja unkarilainen Crysys Lab pitävät Flamea valtion tukemana tuotteena.

Flamen tartuttamia tietokoneita on löydetty erityisesti Lähi-idästä. Haittaohjelma on suunnattu tarkasti rajattuun vakoiluun. Sitä levitetään ilmeisesti usb-muistitikulla, josta ohjelman ensimmäinen kuuden megatavun kokoinen moduuli latautuu tietokoneelle.

Ohjelma ottaa internetin kautta yhteyttä useisiin komentopalvelimiin ja tarvittaessa lataa niistä uusia ohjelmamoduuleja. Ohjelman koko paketti on 60 megatavua. Tavallisesti haittaohjelmat on kooltaan korkeintaan muutamia satoja kilotavuja.

Symantecin turvaoperaatioiden johtaja **Orla Cox** huomauttaa, että Flame kerää valtavan määrän tietoa:

- Tavallisesti tyypillinen hyökkäysohjelma kirjoitetaan keräämään tarkasti rajoitettuja tietoja, koska muuten datamassasta on vaikea löytää haluttuja tietoja. Tämä on kuin vanhanaikaista vakoilua. Kerää kaikki mihin pääset käsiksi ja sitten siivilöi se. Tämä osoittaa, että ohjelman takana on tiedusteluorganisaatio, jolla on resursseja käsitellä tietomassoja.

Kaspersky Labsin **Vitaly Kamluk** nosti esiin sen kuinka rajattu hyökkäys on. Haittaohjelmasta on tavattu vain 382 tartuntaa, joista 189 Iranissa. Lisäksi ohjelman kohteena ovat yksilöt, eivät organisaatiot.

Crysys Lab arvioi, että se on voinut törmätä viitteisiin tästä haittaohjelmasta Euroopassa jo vuonna 2007 ja tartuntaan Yhdistyneissä Arabiemiirikunnissa 2008. Kaspersky ja Symantec arvelevat vakoiluohjelman käynnistyneen vuonna 2010.

Kamlukin mukaan ohjelman tekstiosat on kirjoitettu erittäin hyvällä englannin kielellä, mutta se ei välttämättä todista mitään ohjelman alkuperästä.

Symantecin Cox arveli, että ohjelma pystyy myös poistamaan itsensä koneelta. Silloin hyökkäyksen kohde ei koskaan edes tiedä, että häntä on vakoiltu.

http://www.digitoday.fi/tietoturva/2012/05/29/maailman-pahin-haittaohjelma-paljastui/201230308/66