

Windowsin kuvakeaukkoon hyökätty ehkä Suomessakin

24.7.2010 09:40 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Windowsin pikakuvakeaukkoon iskevä Stuxnet-haittaohjelma on voinut levitä Suomeen. Lisäksi aukkoon tunkee jo muitakin haittaohjelmia maailmalla.

Viestintäviraston tietoturveyskeskus [Cert-fi kertoi](#) perjantaina tutkivansa suomalaista Stuxnet-tartuntaepäilyä. Kysymys on haittaohjelmasta, joka tähtää Windows-käyttöjärjestelmän avonaiseen pikakuvakehaavoittuvuuteen.

Cert-fi:n mukaan Stuxnet-haittaohjelmasta on kymmeniä tuhansia havaintoja ympäri maailmaa, ja valtaosa havainnosta on Iranista, Indonesiasta ja Intiasta.

Lisäksi haavoittuvuutta pyritään käyttämään muissakin haittaohjelmissa. Eräs uusi haittaohjelmaperhe esimerkiksi tallentaa näppäimistön painallukset saastuneessa tietokoneessa.

Tuoreet haittaohjelmahavainnot korostavat pelkoa, että Windows-aukko voi saada aikaan [uuden helposti leviävän verkkomadon](#). Uudet uhat eivät ole kuitenkaan [arviolta](#) niin hienostuneita kuin Stuxnet, jonka tiedetään levinneen Siemensin teollisuusjärjestelmiin.

Apujatarjolla

Microsoft ja Siemens ovat julkaisseet automatisoituja työkaluja Stuxnet-haittaohjelman rajoittamiseksi. Microsoftin Fix It -linkki lataa asennuspaketin, joka poistaa kaikki kuvakkeet käytöstä ja muuttaa ne valkoisen paperiarkin näköisiksi.

Siemens tarjoaa kahta työkalua. Trend Micron tekemä työkalu tarkistaa, onko tietokone Stuxnet-haittaohjelman saastuttama. Simatic-päivitys taas tekee samat rekisterimuutokset kuin Microsoftin työkalu. Siemens kuitenkin varoittaa, että viruksen poistaminen saattaa vaikuttaa tehtaiden toimintaan ennalta arvaamattomalla tavalla.

Ensimmäinenlaatuun

[Siemens tietä](#)istaiseksi vain yhdestä tapauksesta, jossa erään järjestelmäintegraattorin Simatic WinCC -tietokone saastui. Yksikään tuotantolaitos ei ole tiettävästi vielä saanut tartuntaa.

Stuxnet on Siemensin tietojen mukaan ensimmäinen troijalainen, joka hyökkää yhtiön niin sanottuja scada-tehdasjärjestelmiä (supervisory control and data acquisition) vastaan.

Ennen kuin Microsoftin korjauspäivitys on saatavilla, tietoturvaohjelmien pitäminen ajan tasalla vähentää merkittävästi tartunnan todennäköisyyttä, Cert-fi muistuttaa.

<http://www.digitoday.fi/tietoturva/2010/07/24/windowsin-kuvakeaukkoon-hyokatty-ehka-suomessakin/201010244/66>