

Cert-fi: Pankkirosvon piilon voi löytää tietokoneelta

4.12.2009 08:46 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Kansallinen tietoturvaviranomainen Cert-fi antaa ohjeita, miten viime aikoina suomalaisia kiusanneen Zlob-haittaohjelman voi saada pois tietokoneelta. Mutta käyttäjän pitää olla varovainen.

Tuhansia suomalaiskoneita sotkenut Zlob (tunnetaan myös nimillä Alureon tai DNSChanger) on yleensä käyttäjän löydettävissä ja poistettavissa, vaikka se yrittääkin kätkeytyä niin sanotun rootkitin avulla.

Käyttäjän tulee etsiä ja tuhota haittaohjelman käyttämä binääritiedosto ja rekisteriavaimet. Cert-fi antaa tähän tarkemmat ohjeet [tiedotteessaan](#). Lisäksi nimipalvelinasetukset tulee palauttaa suositusten mukaisiksi. Muuten tietokone yrittää jälleen ottaa yhteyttä verkon vaarallisiin paikkoihin.

Poistomenetelmä ei kuitenkaan välttämättä päde kaikkiin haittaohjelman versioihin eikä se poista koneessa mahdollisesti olevia muita haittaohjelmia. Lisäksi väärän tiedoston tai rekisteriavaimen poistaminen voi tehdä käyttöjärjestelmästä käyttökelvottoman. Siksi Cert-fi ehdottaakin varmimpana keinona käyttöjärjestelmän asentamista uudelleen.

Älä asennakoodekkia

Tietokoneen verkkoliikenteen uudelleen ohjaava Zlob-haittaohjelma on syy, miksi suomalaiset operaattorit ovat ryhtyneet poikkeuksellisiin estotoimenpiteisiin pimentäen lukuisia nettiyhteyksiä käyttäjiltä.

Cert-fi kertoo haittaohjelmaa levitetyn uskottelemalla käyttäjälle, että www-sivuilla on tarjolla multimedialakodekki, joka käyttäjän tulisi itse asentaa sisällön näkemiseksi. Zlobin avulla on yritetty huijata suomalaisilta verkkopankkitietoja. Haittaohjelmatyyppejä on kuitenkin ollut Cert-fi:lle tuttu jo vuosia.

Torjumista on vaikeuttanut ohjelman jatkuva muuntautuminen. Zlob käyttää myös monimutkaista pakkausta, mikä vaikeuttaa ohjelman havaitsemista ja toiminnan

tutkimista.

Muutetutnimipalvelinasetukset

Zlob muuttaa työaseman nimipalveluasetuksia niin, että nimenselvitys tapahtuu epäluotettavilta nimipalvelimilta, joiden antamat vastaukset ohjaavat käyttäjän www-yhteydet mahdollisesti haitallisille sivustoille.

Nimipalvelumuutokset näkyvät Windows-käyttöjärjestelmän rekisterissä seuraavan kaltaisina avaimina:

```
HKLMSYSTEMCurrentControlSetServicesTcpipParameters, nameserver=85.255.115.46,85.255.112.124  
HKLMSYSTEMCurrentControlSetServicesTcpipParametersInterfaces{interfaceGUID}, nameserver=85.255.115.46,85.255.112.124
```

Tutkitun haittaohjelman käyttämien nimipalvelinten ip-osoitteet voivat vaihdella välillä 85.255.112.0 - 85.255.127.255.

Nimipalvelinasetukset voi tarkistaa myös käyttöjärjestelmän komennolla IPCONFIG /ALL.

<http://www.digitoday.fi/tietoturva/2009/12/04/cert-fi-pankkivosvon-piilon-voi-loytaa-tietokoneelta/200925009/66>