

## Suomessa yli 20 internet-vakoilutapausta

12.6.2008 14:12 — Kalevi Nikulainen

Suomen valtionhallintoon ja puolustusteollisuuteen iskeneet internet-vakoilijat ovat vastuussa myös samanlaisista hankkeista muualla maailmassa, kuten Yhdysvalloissa, Britanniassa, Italiassa ja Ruotsissa, kertoo tietoturvayhtiö F-Securen tutkimusjohtaja Mikko Hyppönen.

Suomessa näitä tarkoin suunnattuja tapauksia on Supon toimintakertomukseen kirjattu vuoden 2004 jälkeen yli 20. F-Secure on tietoinen 4-5 tapauksesta. Yhdysvalloissa U.S. Homeland Securities laski lähes 13 000 vakoiluiskua viime vuoden aikana.

- Kohdistettuja iskuja tulee todella vähän, kun F-Securen viruslaboratorioon tulee päivittäin 40 000 hyökkäysilmoitusta.

Hyppösen mukaan iskuissa noudatetaan samaa kaavaa. Kohteina ovat huippujohtajat puolustusvälineteollisuudessa ja tärkeät henkilöt valtionhallinnoissa, joille lähetetään oikealta näyttävä henkilökohtainen viesti, jossa voi olla liitteenä pdf-tiedosto, Excel-tiedosto, Word-dokumentti, PowerPoint-esitys tai Access-tietokanta.

- Access-tietokantoja (MDB) on nähty hyökkäyksissä mutta todella vähän, sen sijaan XLS-tiedostoja näkyy enemmän.

### Mitä tapahtuu kohdistetussa hyökkäyksessä?

Hyppönen näyttää F-Securen viruslaboratoriossa mitä tapahtuu, kun kohdistetun hyökkäyksen pdf-liitettä klikataan. Ensin näyttää siltä kuin esiin tuleva Acrobat kaatuu ja virkoaa hetken päästä näyttäen liitetiedoston.

- Samalla kun katsomme esiin tullutta liitetiedostoa, Poison Ivy -takaporttiohjelma on jo ottanut koneen haltuunsa.

Poison Ivy antaa vakoilijalle lähes täyden kontrollin saastuneeseen tietokoneeseen. Sen tiedostoja voi ladata, muuttaa ja lisätä. Lisäksi prosesseja voidaan lopettaa ja muokata Windowsin rekisteriä.

---

Hyppönen korostaa, että normaalit ihmiset ja yritykset voivat olla rauhassa. Iskut kohdistuvat vain harvoihin paikkoihin. Niissä se voi sitten olla todellinen ongelma. Englannissa saastunut tietokone suolsi tietoa 18 kuukautta ennen kuin se huomattiin.

- Vain osa tapauksista raportoidaan. Huomaamatta jää suuri osa niistä. Hälytyskellojen pitäisi soida käyttäjällä, jos liitteen avaamisen jälkeen Word, Acrobat, PowerPoint tai Access välähtää hetkeksi näkyviin ja poistuu ruudulta palatakseen hetken kuluttua uudelleen.

## Jäljitys Kiinaan

Hyökkäykset on pystytty Hyppösen mukaan jäljittämään Kiinaan, jossa ne ovat uponneet 3322.org-, 8800.org-, 9966.org- ja 8866.org-palvelusivustojen vaihtuviin ip-numeroihin.

Näiden kiinalaisten paikkojen omistaja **Peng Young** kertoo Business Weekille, että 3322.orgiin on rekisteröitynyt yli miljoona internet-osoitetta. Vuosimaksu .org-, .net- tai.com-päätteen käytöstä on kohtuulliset 14 dollaria vuodessa.

- Kuka tahansa voi perustaa sivuston 3322.org-palveluun, mutta ongelmana on, että kaikki on kiinan kielellä. Se edesauttaa ajatusta, että hyökkääjät ovat kiinalaisia, Hyppönen kertoo.

Tutkimusjohtaja näyttää tietokoneelta, millainen kiinalainen sivusto on. Siitä ei todellakaan saa mitään selvää läntisen kirjainmaailman perusteella.

## Todiste yhteydestä ihmisoikeussivuihin

F-Securen tutkimusjohtaja mukaan nyt on päästy todistamaan, että samat henkilöt ovat taustalla hyökkäyksissä Kiinan ihmisoikeussivustoihin ja läntisiin koviin kohteisiin, kuten valtionhallintoon ja aseteollisuuteen.

- Samaa koodia on käytetty tietojen kalasteluun floridalaisessa ihmisoikeusjärjestössä, joka työllistää vain muutamia ihmisiä, kuin suuressa englantilaisessa puolustusvälinevalmistajassa. Missään muualla ei ole nähty samanlaista haittaohjelmakokonaisuutta.

Kohteina ovat ihmisoikeusjärjestöt taistelevat muun muassa Tiibetin, uiguurien ja Kiinan ihmisoikeuksien puolesta. Sinne vakoojat lähettävät takaporttiohjelmiä naamioiden viestintä aidon näköisiksi ja etsivät yksityisiltä tietokoneilta pgp-avaimia kryptattujen keskusteluviestien avaamiseksi.

- Samasta lähteestä haittaohjelma on tullut, mutta onko

---

kyseessä virallinen Kiina, siihen ei voida vastata.

Hyppösen mukaan yhtenä mahdollisuutena on kiinalainen rikollisryhmä, joka sitten myisi tietonsa eteenpäin parhaalle maksajalle.

### **Useita kieliversioita**

Vakoojat ovat tietävästi lähettäneet takaporttiohjelmalla kuorutettuja haittaohjelmiaan ainakin viidellä kielellä, jotka ovat englanti, saksa, italia, ruotsi ja suomi.

Hyppösen mukaan tietojen saaminen suomalaisista tärkeistä henkilöistä hallinnossa ja puolustusteollisuudessa on saatu joko tietomurron tai perinteisen vakoilun keinoin.

- Hyökkääjillä on voinut hyvin olla paikallisia avustajia, ja silloin mennään helposti valtioiden väliseen vakoiluun.

Eri tiedustelulaitoksilla on lonkerot kaikissa länsimaissa, ja voi olla, että jokin sellainen yrittää saada kiinalaiset näyttämään syyllisiltä.

Hyppönen kertoo, että vaikka jäljet vievät Kiinaan, ne voivat vielä jatkua johonkin toiseen valtioon.

<http://www.digitoday.fi/tietoturva/2008/06/12/suomessa-yli-20-internet-vakoilutapausta/200815954/66>