

Nettiselaimen lisäosa on tietoturvariski

16.1.2008 13:52 — Aleksis Moisio aleksi.moisio@sanoma.fi

Nettiselaimiin ladattavista laajennuksista on tullut viime kuukausina tietomurtautujien kannalta houkuttelevia kohteita. Itse selainten tietoturvaongelmiin on puututtu, mutta moni selainlaajennuksen tekijä laiminlyö tietoturvan ajattelemisen ohjelmointivaiheessa.

Selainten toiminnallisuutta parantavien laajennuspalikoiden ohjelmointivirheet tarjoavat yhä useammin tietomurtautujille eli kräkkerille oikopolun surffaajan koneelle. Näin arvioivat suomalaiset tietoturva-asiantuntijat.

- Kyllä kräkkerit tutkivat näitä suosituimpia laajennuksia, sanoo tietoturva-asiantuntija **Pekka Sillanpää** Nixusta.

Selainlaajennukset ovat nykyisin suosittuja, sillä nettisurffaajat arvostavat nopeutta ja tehokkuutta. Siksi verkkoselaimista suunnitellaan kevyitä. Ajatuskulku on seuraava: massoille jaettavaan selaimen liitetään vain välttämättömät osat ja lisäominaisuuksia kaipaavat voivat muokata selaintaan lisäämällä siihen laajennuksia.

Esimerkiksi Mozilla Firefox -selaimen voi asentaa vaikkapa Delicious Bookmarks -laajennuksen, joka integroi selaimen Delicious-linkinjakopalveluun. Internet Explorer -selaimen käyttäjä voi puolestaan asentaa esimerkiksi Google Desktop- tai QuickTime-laajennuksen.

Samalla kun laajennus parantaa selaimen toiminnallisuutta, se hajauttaa vastuun tietoturva-arkkitehtuurista.

- Hyökkäykset selainlaajennuksia kohtaan ovat varmasti yleistymässä, sillä suositut laajennuspalikat muuttuvat houkutteleviksi kräkkerin silmissä, Sillanpää sanoo.

Aluksi kräkkerit tunkeutuivat kotikoneelle Windowsin tietoturva-aukkojen kautta. Sitten kräkkerit siirtyivät hyväksikäyttämään selainten ongelmia. Lopulta kiinnostus kohdistui nettiselainten laajennuksiin eli extension-, plugin- ja add-on-palikoihin, selittää tutkimusjohtaja **Mikko Hyppönen** F-Securelta.

- Selainlaajennuksien aukkoja käyttävät hyökkäykset ovat yleistyneet aivan viime kuukausina, Hyppönen sanoo.

Kräkkerin kannalta selainlaajennus on kiinnostava kohde, koska se ei yleensä päivity yhtä säännöllisesti ja tiheästi kuin itse selain tai käyttöjärjestelmä. Säännöllisten tietoturvapäivitysten avulla esimerkiksi Mozilla Foundation ja Microsoft pystyvät hillitsemään selaimiensa tietoturvaongelmia.

- Koska itse olet viimeksi päivittänyt selaimesi laajennukset? Hyppönen kysyy.

Laajennukset tarjoavat yleensä paljon avonaisemman väylän käyttäjän koneelle kuin itse selain. Siinä missä Mozilla Firefox suorittaa verkkosivuilla olevia skriptejä sivuston tasolla, laajennukset asettuvat matalammalle tasolle osaksi Firefoxia käyttäen hyväkseen chrome-protokollaa. Tämä tekee esimerkiksi näppäimistön lyönnejä nauhoittavan keylogger-kuuntelijan tekemisestä helpompaa.

Ongelmalliseksi tilanteen tekee myös se, että monet ohjelmat ja laitteet, kuten kännykät tai digitaalikamerat, asentavat selainlaajennuksia käyttäjän huomaamatta. Esimerkiksi Applen QuickTime-videolaajennuksesta on paljastunut useita tietoturva-aukkoja viimeisen vuoden aikana. Moni käyttäjä on ollut kuitenkin autuaan tietämätön koko QuickTime olemassaolosta koneellaan.

Hyppönen ennustaa tilanteen laukeavan perinteisen kaavan mukaisesti: aluksi hyökkäysten määrä lisääntyy, sitten ongelmaan reagoidaan ja kehitetään ratkaisu. Hän ennustaa, että selainvalmistajat ottavat tulevaisuudessa vastaan tietoja kolmansien osapuolien tekemien laajennusten tietoturvaongelmista ja varoittavat laajennusten käyttäjiä selaimen kautta.

<http://www.digitoday.fi/tietoturva/2008/01/16/nettiselaimen-lisaosa-on-tietoturvariski/20081430/66>