

Sql-pistos nousee kohti haittaohjelmien kärkeä

25.4.2008 16:25 — Timo Poropudas
timo.poropudas@sanoma.fi

Suomessakin joitakin sivustoja saastuttanut Nihaorr1.com-hyökkäys on kiertänyt maailmalla. Ohjelma käyttää verkkopalvelujen tietokantoja tartuttamispesäkkeinä.

Nihaorr1.com-hyökkäys on kaksivaiheinen. Ensimmäisessä vaiheessa pyritään saastuttamaan julkinen verkkosivu haittakoodilla sql-pistos-tekniikalla (sql injection), sanoo tietoturvalato Nixun asiantuntija **Pekka Sillanpää**.

Tämäntyyppiset injektiohyökkäykset ovat toisella sijalla [OWASP Top 10](#):n listassa tyypillisimmistä web-sovellusten haavoittuvuuksista.

Toisessa vaiheessa käyttäjät, jotka selaavat saastunutta sivustoa, joutuvat hyökkäyssarjan kohteeksi, joilla pyritään muun muassa ottamaan haltuun käyttäjän kone.

- Mikäli käyttäjän koneen päivitykset eivät ole ajan tasalla, näillä hyökkäyksillä on suuri mahdollisuus onnistua, Sillanpää sanoo.

Vastaavat hyökkäykset ovat yleistyneet maailmalla. F-Secure kertoi eilen tietoturvablogissaan, että tähän mennessä on tavattu kolme domainia, joista hyökkäystä on levitetty: nmidahena.com, aspder.com ja nihaorr1.com.

F-Securen mukaan tämän tyyppisten hyökkäysten leviäminen johtuu siitä, että yhä useammat nettipalvelut käyttävät tietokantapohjaisia järjestelmiä nopeuttaakseen toimintaa. Monet niistä sallivat käyttäjien ladata sisältöä tietokantoihinsa.

- Ellei dataa sanitoida ennen kuin se tallennetaan, on mahdotonta kontrolloida mitä palvelu tarjoaa sivuston käyttäjille, F-Securen blogissa kirjoitetaan.

<http://www.digitoday.fi/tietoturva/2008/04/25/sql-pistos-nousee-kohti-haittaohjelmien-karkea/200811672/66>