

Palvelunestohyökkäyksen uusi muoto havaittu Suomessa

21.1.2009 07:57 — Kalevi Nikulainen

Viestintäviraston tietoturveyskikkö CERT-FI kertoo, että sen tietoon on tullut tapauksia, joissa internetin suuntaan avoimiin nimipalvelimiin on kohdistunut runsaasti kyselyitä nimipalvelun juuren NS-tietueelle. Samoja kyselyitä on havaittu myös suomalaisissa verkoissa sijaitseviin nimipalvelimiin.

CERT-Fi selvittää, että kyselyiden määrä yksittäistä nimipalvelinta kohti ei ole merkillepantavan korkea, joten tarkoituksena ei ilmeisesti ole hyökätä kyseltäviä nimipalvelimia vastaan. Tietoturveyskikön mukaan kyseessä vaikuttaisi pikemminkin olevan rekursiivisia nimipalvelimia hyödyntävän palvelunestohyökkäyksen uudempi muoto.

Väärentämällä nimipalvelukyselyiden lähde-ip-osoite, saadaan aikaan vahvistusvaikutus, jos nimipalvelimien tuottamat vastaussanommat ovat kyselyviestiä suurempia.

Esimerkiksi kysymällä nimipalvelun juuren NS-tietueita, vastauksena tähän lyhyeen kyselyyn saadaan pitkä lista juurinimipalvelimista. Näin saadaan aikaan väärennettyyn osoitteeseen huomattava määrä ei-toivottua vastaussanomaliikennettä. Tyypillisesti tämäntyyppisiä hyökkäyksiä on toteutettu käyttämällä hyväksi nimipalvelimia, jotka sallivat rekursiiviset kyselyt kaikkialta internetistä. Tällä hyökkäysmenetelmällä ei kuitenkaan kyetä hyödyntämään sellaisia nimipalvelimia, joissa rekursiiviset kyselyt tuntemattomista verkoista on kielletty.

Hyväksikäyttäminen mahdollistuu

Eräät nimipalvelintoteutukset vastaavat kuitenkin tuntemattomista verkoista peräisin oleviin, nimipalvelimen välimuistista löytyviä tai muuten ilman iteratiivisia kyselyitä saatavilla olevia tietueita koskeviin kyselyihin, vaikka rekursiiviset kyselyt näistä tuntemattomista verkoista olisi estetty. CERT-FI:n mukaan se mahdollistaa tällä tavalla toimivan nimipalvelimen hyväksikäyttämisen palvelunestohyökkäyksessä myös silloin, kun rekursiiviset

kyselyt ulkoverkosta on kielletty.

Tällöin myös DNS-palvelimen välimuistissa olevien tietojen selvittäminen voi olla mahdollista tutkimalla mitä tietueita koskeviin kyselyihin saadaan vastaus. Nimipalvelintoteuksissa vastaaminen välimuistista löytyviä tietueita koskeviin kyselyihin on tyypillisesti poistettava käytöstä erikseen, jolloin nimipalvelimen hyväksikäyttö estyy.

CERT-FI toteaa, että nimipalvelimen hyväksikäyttöyrityksiä voi pyrkiä havaitsemaan esimerkiksi etsimällä nimipalvelimen lokeista merkkejä suurista määristä tietyllä lähde-ip-osoitteella tehdyistä kyselyistä, jotka ovat peräisin omien luotettujen verkkojen ulkopuolelta.

<http://www.digitoday.fi/tietoturva/2009/01/21/palvelunestohyokkayksen-uusi-muoto-havaittu-suomessa/20091680/66>