

Hyökkääjälle selaimet käyvät avoimesta välityspalvelimesta

3.8. 10:17 (päivitetty 10:28) — Matias Mäki
matias.maki@sanoma.fi

Sony-rootkin leviämisen jäljittämisestä tunnettu Dan Kaminsky esitteli työkalun, jonka avulla hyökkääjä voi luoda kohteensa selaimen avulla näennäisverkon, jonka avulla pääsee esimerkiksi kohteen sisäverkkoon. Työkalu ei hyödynnä varsinaisia tietoturvaavoittuvuuksia vaan selainten yleisiä toimintaperiaatetta.

[Dan Kaminskyn](#) slirpie-työkalun avulla hyökkääjä voi tunneloida verkkoliikennettä kohteensa selaimen avulla. Työkalu hyödyntää selainten perustoimintatapaa.

Selainten ongelmallisen toiminnallisuuden avulla hyökkääjä voi esimerkiksi selata käyttäjän palomuurin ja nat-reitittimen takana olevia palvelimia käyttäjän selaimen avulla. Hyökkääjän tarvitsee ainoastaan houkutelaa käyttäjä haittakoodia sisältävälle sivustolle.

Toimii kaikilla valtaselaimilla

Hyödynnetyr"[anti-dns pinning](#)"- ja "[dns-rebinding](#)"-nimillä tunnetun keinoon on todettu toimivan ainakin Internet Explorerin 6- ja 7-, Firefoxin 1-2- sekä Operan 9.0.2-versioilla.

Ainoastaan KHTML/Webkit-pohjaiset selaimet, kuten Safari ja Konqueror, puuttuvat listasta. Tämä ei kuitenkaan tarkoita sitä, että nämä selaimet olisivat haavoittumattomia.

Hyökkäykseen tarvitaan palvelin ja nimitunnus

Perustason dns-rebinding -hyökkäyksessä hyökkääjä rekisteröi nimitunnuksen, johon pahaa aavistamaton käyttäjä houkutelaa. Nimitunnusta tarjoillaan nimipalvelimelta lyhyellä ttl (time to live)-päivitysaikatiedolla.

Ensimmäisellä sivustolle suunnatulla kyselyllä käyttäjä käynnistää haitallisen javascript-koodin, jolloin koodi antaa nimitunnukselle uuden ip-osoitteen. Tämä osoite voi osoittaa esimerkiksi käyttäjän sisäverkon palvelimille tai vaihtoehtoisesti

jollekin internet-palvelimelle, johon hyökkääjä haluaa päästä ilman oman osoitteensa paljastamista.

Ongelma selainten yleisessä turvakäytännössä

Varsinainen ongelma johtuu selainten "same origin policy"-käytännöstä, eli jos kaksi palvelinta kuuluu samaan nimitunnukseen, selaimet käsittelevät niitä yhtä turvallisina ja sallivat palvelinten välisen liikenteen. Jos siis hyökkääjän palvelin ja kohdepalvelin sijaitsevat selaimen mielestä samassa domainissa, niiden välillä voidaan lähettää tietoja.

Hyökkäyksen avulla voidaan ottaa kohdepalvelimelle yhteys muuhunkin tcp-porttiin kuin web-palvelinten yleisesti hyödyntämään 80-porttiin.

Hyökkäyksen perustoteutuksen demonstraatioon voi tutustua esimerkiksi [täällä](#). Demoon voi syöttää nat-sisäverkon sisäisen ip-osoitteen, esimerkiksi 127.0.0.1, 10.0.0.1 tai 192.168.0.1. Jotkin välityspalvelimet voivat kuitenkin torpata dns-rebindingin.

Vanha tuttu, heikko suojaus

Dns-rebinding -hyökkäystä varten hyökkääjän ei tarvitse viritellä dns-palvelimia vaan ip-osoitteen vaihto tapahtuu selaimessa javascriptin, Flashin tai Javan avulla.

Keinona dns-rebinding on vanha ja tunnettu ongelma jo viime vuosikymmenen puolesta välistä. Kaminsky pitääkin ongelmaa niin vanhana, ettei sitä vastaan muisteta enää puolustautua.

Nykyisissä selaimissa hyödynnetään "dns pinning" -suojausta. Kun selain selvittää nimitunnukselle ip-osoitteen, selaimen välimuisti antaa saman ip-osoitteen selaimen kiinteästi ohjelmoidun ajan, joka ei riipu dns-palvelimen ttl-ajasta.

Ongelmaksi muodostuvatkin selainten lisälaajennukset, kuten Flash ja Java, jotka pitävät kirjaa omista ip-nimi -pareista. Hyödyntämällä esimerkiksi kahta samanaikaisesti ip-nimi -parisäilöä, voidaan ip-osoite vaihtaa.

Selaimen avulla voi luoda vpn-tunnelin sisäverkkoihin

Vaikka dns-rebinding -ongelma on tunnettu aiemmin, Kaminskyn Slirpie-työkalu demonstroi, kuinka paha ongelma oikeastaan on. Slirpie sisältää tcp-toteutuksen javascriptillä ja hyödyntää lisäksi pptp-protokollaa ja vanhaa liikenteen tunnelointiin tarkoitettua slip-ohjelmaa.

Näiden työkalujen avulla hyökkääjä voi käytännössä luoda vpn-yhteyden kohteen sisäverkkoon.

Ainakaan tällä hetkellä Kaminsky ei tarjoa työkalua ladattavaksi, mutta kertoo [luentokalvoissaan \(ppt\)](#) todennäköisesti asiasta ymmärtäville kaiken tarpeellisen.

<http://www.digitoday.fi/tietoturva/2007/08/03/hyokkaaajalle-selaimet-kayvat-avoimesta-valityspalvelimesta/200718532/66>