

## domainabc.hu a domainHírforrás

Ügyfélszolgálat: 30/6161616 vagy 30/6 DOMAIN ( azaz 30/6-366-246 )

Weboldala címe: <http://www.domainabc.hu/>

---

## Biztonsági rés a hazai DNS-ek kétharmadán

2008.08.14. 17:21

**A BME Híradástechnikai tanszékének kritpografiával és biztonsággal foglalkozó laboratóriuma által közzétett tanulmány szerint a Dan Kaminsky által publikált biztonsági részt a hazai szolgáltatók kétharmada figyelmen kívül hagyta.**



A biztonság kulcsa.

A BME Híradástechnikai tanszékének kritpografiával és biztonsággal foglalkozó laboratóriuma egy napokban közzétett tanulmánya szerint a hazai domainipar nagyobbik része nem vette komolyan az Internet eddigi egyik legjelentősebb hibáját feltáró jelentést és a biztonsági részt "befoltozására" nem tett intézkedéseket.

"A Dan Kaminsky nevével jegyzett internetes DNS támadás lehetőségéről a nagyközönség 2008. július 8-án szerzett tudomást, amikor számos gyártó és fejlesztő előre egyeztetett módon egyszerre jelentett be egy korábban ismeretlen hiba ellen védekezést nyújtó javítócsomagot. A hiba súlyossága miatt egyedülálló összefogás született, és ennek eredménye volt az, hogy a hiba kijavítása napvilágra került, de a hiba nem. Az eredeti tervek szerint Dan Kaminsky 2008. augusztus 7-én ismerteti a hiba és a támadás pontos módszerét a Black Hat 2008 konferencia keretében. Így 30 napja volt a rendszergazdáknak és üzemeltetőknek, hogy a rendelkezésre álló javításokat teszteljék és telepítsék." - áll a

tanulmányban.

A hiba egy cache "mérgezés" tesz lehetővé, amely azt eredményezi, hogy illetéktelenül a domain nevekre irányuló kéréseket át lehet irányítani egy "idegen" tartalomra.

"Összesen 5861 darab ismert magyar DNS kiszolgálót vizsgáltunk meg. A kiszolgálók számbavétele során 2015 olyan kiszolgálót találtunk, amelyek gyakorta intéznek kéréseket más szerverek felé és Magyarországon üzemelnek (helymeghatározás forrása: geoip), 4509 olyan szerver IP címet találtunk, amelyek a 400 000 fölötti bejegyzett magyar .hu domain kiszolgálásáért felelős. Ezek átlapolt eredménye az összesen 5861 darab ismert kiszolgáló."

2107 darab DNS szerver hajtott végre lekérdezést kéréseinkre az 5861 darab ismert címből. Ezek közül 670 darab IP címen elérhető szerver alkalmazta a port-randomizációs védelmet, a többi 1437 nem. Vélhetőleg sebezhető, nem javított tehát a válaszoló szerverek 68%-a. Az összes, kérést nem végző szervereket is beleértve ez természetesen csak 24%" - derül ki a Bencsáth Boldizsár és Buttyán Levente szerzők kutatási publikációjából.

A kutatók megvizsgálták a hazai internetes közösséget kiszolgáló internet szolgáltatók által biztosított DNS szervereket is. A vizsgálat szerint a 15 potenciális támadási forrásból 13 jól védettnek bizonyult.

### Nem cél, csak eszköz

A Dan Kaminsky által felvázolt hiba egy eszköz lehet az internetes visszaélésekre szakosodott bűnbandák számára. A feltárt hiba kihasználásával egyszerűbbé válhat az adathalászat. A biztonsági rés használatával egyszerűen átirányítható pl. egy-egy bank honlapjára irányuló kérés és a bank eredeti honlapjának megjelenik segítségével a látogatót megtevesztve megszerezhetőek a felhasználó jelszavai és felhasználó nevei.

Forrás: <http://www.crysys.hu/publications/files/BencsathB08DNS.pdf>

Fodor Ákos