Laboratory of Cryptography and Systems Security
Budapest University of Technology and Economics
Department of Telecommunications

Egy hónapja ismert a Kaminsky-DNS probléma

Hol tart ma a hazai védekezés? – A nagyok léptek, a kicsik lassúak

Bencsáth Boldizsár, Dr. Buttyán Levente
{bencsath,buttyan}@crysys.hu
BME Híradástechnikai Tanszék, CrySyS Laboratórium
http://www.crysys.hu/

Összegzés: Sokakat érint és sokakat érdekel, hogyan halad a Kaminsky-féle DNS támadás elleni védekezés implementálása hazánkban. A hiba létezése 2008. július 8-a óta ismert, és azóta elérhetőek azok a friss szoftververziók is, amelyek védelmet nyújtanak a hiba ellen. Vizsgálatunk során leellenőriztük, hogy a hazai DNS szerverek gazdái telepítették-e a védekezéshez ma elengedhetetlen szoftvereket.
Az eredmények azt mutatják, hogy a szerverek mintegy kétharmada jelenleg nem védett a támadás ellen. A nagy szolgáltatók többsége már implementálta a javasolt védelmet, de ez még nem elég az ügyfelek védelmére.

Bevezető

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.
Fontos megjegyezni ezen a ponton, hogy ipari környezetben egy szoftver frissítése még ilyen súlyos esetben sem egyszerű feladat. A magas rendelkezésreállás garantálása érdekében a szoftvereket tesztelni kell, a cégspecifikus szoftvermódosításokat pedig átdolgozni az újabb, javított változatba. Az otthoni felhasználóknak és kis cégeknek pár nap is elég lehetne a szoftverek frissítésére, de a teljes Internet frissítése időigényes feladat.
Az eredeti terveket, a 30 napos „haladékot” módosította az, hogy az idők során kb. 2 héttel a javítások bejelentése után az Interneten körvonalazódott a biztonsági probléma mibenléte, és most, a hiba publikálásának időpontjában, kis részletek kivételével már mindenki tudja, mi is a hiba és rendelkezésre állnak a támadásokra készített programok is.
Letelt tehát a 30 nap, ami alatt mindenki frissíthette szoftvereit, hogy azok védettek legyenek. Sokakban felmerül a kérdés, hogy Magyarországon mennyire készültünk fel ez alatt a súlyos probléma kezelésére és nyugodtan tölthetjük-e be kedvenc bankunk elektronikus banki

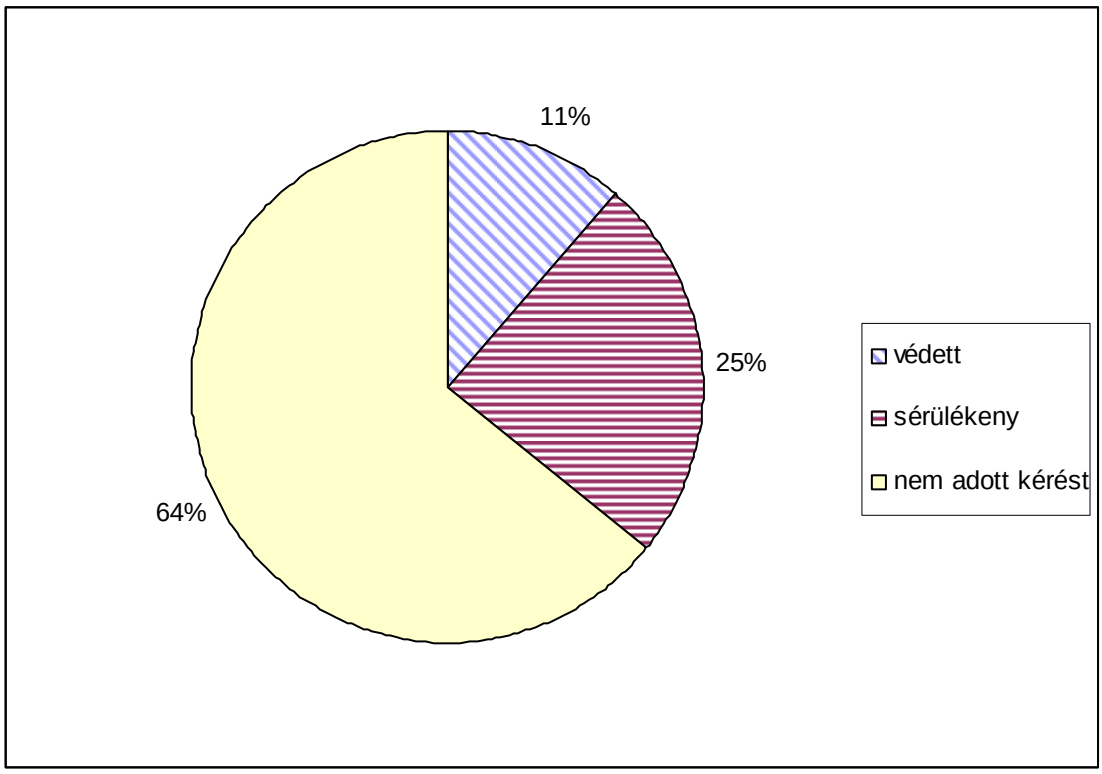
felületét az Interneten keresztül. Ezt vizsgáltuk meg Műegyetem Híradástechnikai Tanszékének CrySyS Laboratóriumában (www.crysys.hu) 2008. augusztus 6-án.

Vizsgálatunk tárgyai a hazai DNS kiszolgálók voltak. Azt kívántuk felderíteni, hogy a Magyarországon üzemelő DNS kiszolgálók milyen arányban sebezhetőek a támadás szempontjából, és mennyi a biztonságos szerver. Fontos azonban tudni, hogy egy ilyen vizsgálat komplikált és nem mindig nyújt egyértelmű eredményt, mert nincsen olyan adatbázis, ahonnan kiolvasható lenne az összes szerver címe, vagy ismerhető lenne az összes hálózat egyedi beállítása. Vizsgálatunk tehát nem feltétlenül reprezentatív, de a hozzáértőknek fontos információkkal szolgál a hazai biztonsági kultúra helyzetéről.

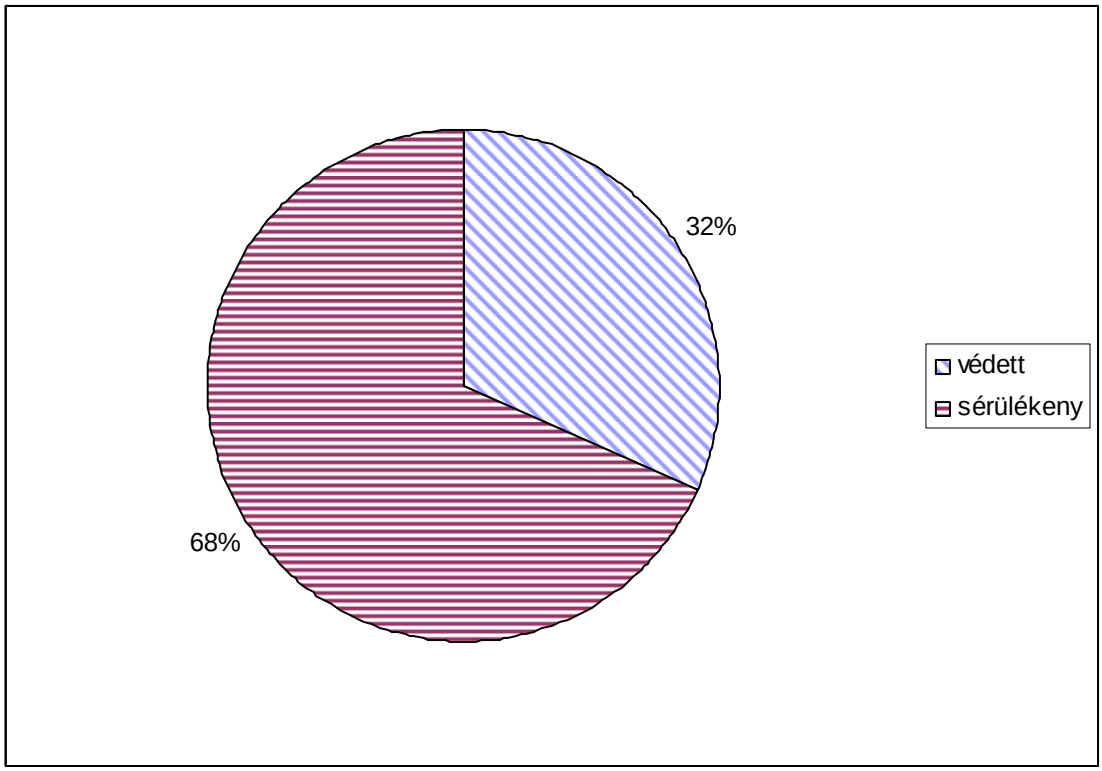
Vizsgálati eredmények

Vizsgálataink során 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, amelyik a négyszázezer fölötti (vizsgálataink szerinti adat) bejegyzett magyar .hu domain DNS 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%.)



1. ábra. Sérülékeny és védett szerverek az összes arányában



2. ábra. Sérülékeny és védett szerverek aránya a nem válaszoló szerverek nélkül

Külön megvizsgáltuk azt a 2015 darab szervert, amelyet nem a .hu domainek felelőseiként ismertünk meg, hanem tapasztalati úton figyeltük meg mint olyan szervereket, amelyek Magyarországon üzemelnek, és gyakorta hajtanak végre DNS lekéréseket.

A 2015 ilyen „gyakorlati szempontból fontosabb" szerver közül 203 kérdezett védett módon, véletlenszerű portot választva, 464 volt támadható. Együtt 667 darab szerver végzett lekérdezést a kéréseinkre válaszul, a többi nem. Ebben a részkategóriában, a kifelé is kéréseket gyakran intéző szerverek esetében 30% volt védett és 70% sérülékeny.

Megvizsgáltuk a felhasználók többségét ellátó legnagyobb internet szolgáltatók ügyfelei által elérhető főbb DNS szervereket is. Ennek eredménye számszerűség nélkül az volt, hogy a legnagyobb cégek (kb. 15) közül a többség védekezik a hiba ellen, csak két olyan céget találtunk, amelyik sebezhető DNS szerverrel is rendelkezett.

Vizsgálati módszer

Vizsgálataink során egy semleges IP tartományból intéztünk kéréseket a vizsgált DNS szerverek irányában. Ezt oly módon tettük meg, hogy a DNS szerverek a kérést a mi általunk meghatározott szerver irányában továbbították. Az általunk kezelt szervernél pedig hálózati lehallgatásos módszerrel vizsgáltuk meg, hogy a kéréseket az adott szerver (több lekérdezés alapján) véletlenszerű, vagy azonos, illetve egyszerűen kikövetkeztethető módon használta-e.

Jelentős eltérés figyelhető meg a vizsgált, és a válaszoló szerverek száma között. Ennek számos oka lehet. Egyes szerverek előtt tűzfalak szűrhetik a kéréseket, és nem engedik, hogy a hálózaton, cégen, vagy ügyfélkörön kívül külső lekérdezők is használhassák a szervert. Ugyanez érhető el azzal is, ha a szerver van úgy konfigurálva, hogy a külső felhasználók ún. rekurzív kéréseket ne hajthassanak végre. Vizsgálati szempontból viszont azt jelenti, hogy ezeket a szervereket nem tudjuk vizsgálni, lehetnek jók vagy rosszak, de a vizsgálat során használt tartományból kérésekre nem válaszolnak. Az is előfordulhat, hogy a vizsgálat azért nem megoldható, mert a szerver nem végez ún. rekurzív kiszolgálást, hanem egy másik szervernek adja tovább a kéréseket (ún. forwarder). Ilyen esetben maga a kiszolgáló védettnek tekinthető, de a forwarder útján még támadható maradhat. Ezt jelen esetben tovább nem vizsgáltuk. Az 5861 címből 637 IP szabályos „REFUSED” elutasítást adott, 2386 esetben pedig nem adott rekurzív választ a célszerver és a .hu felelős DNS szerverek felé irányított.

Nagyon fontos megjegyzés, hogy ha egy szerver nem válaszolt a vizsgálatunknál használt hagyományos, külső kérésre, az nem jelent védettséget! Nagyon könnyen elérhető az, hogy a védettnek tűnő szerver a támadó által igényelt DNS lekérdezést végezze el, tucatnyi példát mutat erre Kaminsky is előadásában. Ezért a bezárt, csak belső hálózatból elérhető szerverek elleni külső támadás igencsak elképzelhető, tűzfalas technikával, szoftverfrissítés nélkül nem lehet biztonságos helyzetet teremteni.

A fentiekből látható: csak azokra a szerverekre mondhatunk biztosat, amelyek kérést intéztek az általunk létrehozott teszt szerver felé, amelyek nem küldtek kérést, vagy nem válaszoltak, azokról nem tudunk biztosat mondani. Azt viszont egyértelműen állíthatjuk, hogy a rekurzív kérésekre is válaszoló, ismert szerverek közül kb. 67-70% jelenleg sérülékenynek mondható.

A .hu domainért felelős DNS szerverek száma tapasztalataink szerint mintegy 8820 darab, de a vizsgálataink során csak a Magyarországon működő szervereket vizsgáltuk, ez pedig vélhetően csak 4509 darab (geoip adatok alapján).

A veszélyek súlyossága

Nem célunk a támadás bemutatása, ez jelenleg számos helyen elérhető. Egyértelmű, hogy a Dan Kaminsky által felfedezett sérülékenység igen súlyos. Nem olyan könnyen megítélhető azonban, hogy ez mekkora gondot fog okozni. A http://www.sec-consult.com/files/Whitepaper-DNS-node-redelegation.pdf címen található publikáció számítási példákat is ad a sérülékenységre, de még ez is tartalmaz pontatlanságokat, a többségnek pedig értelmezhetetlen. Röviden ezért megpróbáljuk körvonalazni a probléma súlyát, a végső következtetést pedig a következő hónapok eseményei tudják megadni.

Egy sérülékeny szerveren tetszőleges támadó módosíthat DNS bejegyzéseket. Pontosítva ezt az egyszerű mondatot, csak akkor módosíthat a támadó bejegyzéseket, ha a DNS szerver irányában kéréseket tud intézni. Külső támadó tehát olyan szerver irányában nem tud támadást intézni, amely tűzfal- vagy szerverszabályok által nem engedi külső lekérdezők hozzáférését. A másik oldalról, belső támadó még ekkor is kihasználhatja a sérülékenységet, és belső támadó akár egy cégen belül megfertőzött számítógép is lehet.

A „módosíthat" szó is pontosításra szorul. A Kaminsky-támadás sok különböző kérésre épít, azaz a támadó ezer és ezer próbálkozást intéz, de egyszer sikerrel jár, és sikerül neki módosítania egy adott bejegyzést. Többségében a sok sikertelen kísérlet nem okoz riasztást, vagy más eseményt, így észrevétlen marad, de nem elképzelhetetlen a támadás detekciója sem.

Ráadásul a módosításra - implementációtól függően - nincs mindig lehetőség. Fontos tényező, hogy az adott (hamisítandó) domain adatai a támadott szerverben éppen milyen állapotban vannak, az adott domainnek hány szervere van, illetve milyen paraméterei (TTL érték). A TTL értékének kérdése egyébként jelenleg igen vitatott, mert segíthet megakadályozni a támadást, ugyanakkor a TTL érték nem biztonsági célokat szolgál, így jelenleg nem lehet erre építeni a védelmet. Ehhez járul még hozzá az is, hogy a TTL értékkel szorosan összefügg, hogy az adott támadott szerverben milyen sűrűn kérdezik le a támadás célpontjaként támadott DNS címet, zónát. Ha ritkán, akkor könnyebb a támadás, de „kevesebb" a támadott célpont, míg ha sűrűn, akkor nehéz a támadás, de a sikeres támadással több kliens is félrevezethető.

A fentieket tovább árnyalja az is, hogy milyen szolgáltatások tekintetében tudunk támadásról beszélni. A legtöbb hír főként a webes phishing támadásokat említi, pedig ez csak része a problémáknak. Érdemes áttanulmányozni Dan Kaminsky friss előadását a http://www.doxpara.com/DMK_BO2K8.ppt címen.

A phishing mellett elképzelhető a levelező rendszer támadása, pl. egy általunk intézett kérdésre a válasz nem hozzánk fog érkezni, hanem egy támadóhoz, aki kedve szerint akár módosítva továbbíthatja azt hozzánk. Ilyen esetben ráadásul a támadás nem attól függ, hogy a saját internet-szolgáltatónk védett-e, hanem attól, hogy az, aki válaszol, védett szolgáltatókon küldi-e tovább a válaszlevelet. Elég egy védtelen állomás, és a levél lehallgatható, vagy módosítható lehet.

Hasonlóan súlyos gond, ha egyes felhasználók számára automatikus frissítési szolgáltatásokat hamisítanak (pl. szoftverfrissítés, vagy vírusadatbázis, stb.) Elképzelhető, hogy egy támadó a saját (támadó) programját tudja telepíteni egy jól konstruált támadással számítógépünkre, noha gépünkön a legkorszerűbb védelmi rendszerek, vírusirtó stb. futnak. Egy ügyes támadás

a DNS segítségével ezt még akkor is megteheti, ha a letöltés SSL/TLS-en védett, rejtjelezett csatornán zajlik, hiszen többnyire ez is a DNS rendszer használata mellett történik.

Nem elképzelhetetlen a támadás kéretlen reklámlevélküldők (spammerek) által történő kihasználása sem, sőt az is előfordulhat, hogy később ez lesz a leggyakoribb támadás, ami a most közzétett hibára épül.

Azért fontos ilyen hosszan bemutatni a hiba súlyosságát, mert sokan védettnek gondolhatják magukat. Frissítették, tesztelték hálózatukat és úgy vélik, ők biztonságban vannak. Egy tipikus vállalati infrastruktúra esetén viszont számos DNS szerver van használatban, tartalékként külső szerverek is bejegyzésre kerülnek, ha a vállalat saját szerverei nem működnének stb. Ilyen esetben nagyon könnyen előfordulhat, hogy egy-egy szolgáltatás, bizonyos esetekben még mindig támadható.

A hiba kihasználása nem triviális, de nem is lehetetlen, viszont mindaddig, amíg a szerverek nincsenek frissítve, komoly a kockázat. A támadás nemcsak a rossz szerver ügyfeleit, hanem másokat is érinthet. Nehéz megmondani, hogy milyen szolgáltatásoknál okozhat gondot a támadás, szinte könnyebb lenne megmondani, hogy hol nem. Indokoltnak látszik az, hogy sokan megrémültek, és mindenképpen indokolt telepíteni, a védettséget jelentősen javító (nem teljesen megszüntető) szoftveres javításokat.

Aki kételkedik a saját böngészője mögött álló DNS sebezhetetlenségében, használja a Kaminsky saját oldalán, a http://www.doxpara.com/ oldalon megtalálható ellenőrző programot.