Jan Boček, Miloslav Janda

Jméno je moc

Představte si, že máte takřka neomezené množství zdrojů a královskou moc. Vaši autoritu ve fiktivní zemi ale začíná podrývat internet. Zkuste jej zničit, rozbít, ochromit, rozpustit. V novém seriálu postupně vyzkoušíme všechny známé i neznámé možnosti, jak toho dosáhnout

Říká se, že ochromit internet je primitivní úkol. Stačí, když pomocí vyhledávače Google zkusíte najít výraz „Google". Zkusili jsme, nefunguje to.

Jmenuji se 192.203.230.10

Mnohem schůdnější se zdá být cesta, využívající takzvaný DNS (Domain name server neboli Server, který se stará o doménová jména). Tyto servery slouží k překladu názvu domén na IP adresy, například ns.nasa.gov na 192.203.230.10. Díky tomu si nemusíte pamatovat ono nepraktické čtyřčíslí, stačí znát název domény. Doménový server totiž ve své paměti uchovává záznamy, jednoznačně propojující číslo i název dané domény.

Doménový server provozuje každý poskytovatel internetu nebo webhostingu. Jakmile si u něj zaregistrujete doménu, musí poskytovatel přidat záznam právě do tabulky svého DNS serveru. Zároveň má každý poskytovatel svůj nadřazený server. Ten zase ví, který poskytovatel má k dispozici jaké domény. To stejné se opakuje na dalších úrovních.

Hierarchie serverů zaručuje rychlost a robustnost internetu. Důvod je jednoduchý: tabulka, obsahující všechna propojení mezi IP adresou a jménem domény, by byla nesmyslně dlouhá. Decentralizovaný systém je efektivnější. Pokud zadáte do adresního okna svého prohlížeče třeba stránku www.nasa.gov, budete potřebovat dvě úrovně DNS. První vás odkáže na servery, které spravují doménu nejvyššího řádu (.gov), některý z nich vás pošle na server druhé úrovně, který se stará o doménu nasa.gov. Ten teprve dovede přeložit celou adresu www.nasa.gov na jednoznačnou IP adresu, kterou potřebuje váš prohlížeč pro zobrazení stránky.

Vyvrátit z kořenů

To byla nutná teorie. Skutečná práce na zničení internetu začíná až teď.

Zaměřme se na nejvyšší úroveň DNS serverů. Z jejich pyramidové organizace vyplývá, že musí existovat server nebo servery, které celý systém zastřešují. Skutečně je tomu tak; nejvyšší úroveň se nazývá Root DNS (kořenový DNS) a po celém světě jich najdeme třináct. Konečně jsme se dostali k tomu, co hledáme od začátku: rozumnému počtu zranitelných míst.

Kdyby se totiž podařilo vyřadit všech třináct kořenových DNS najednou, výsledkem bude kýžený chaos. Bez znalosti překladu domén prvního řádu (.gov, .com, .cz) byste se nedostali ani do své emailové schránky, natož k méně používaným službám. Mnoho služeb by kvůli dalším komplikacím nefungovalo ani pak.

Takhle jednoduchý náš úkol bohužel není. Za prvé, je potřeba odstavit všechny servery najednou a na dostatečně dlouhou dobu (než „vyhnijí" záznamy na DNS serverech nižší úrovně). Každý server totiž uchovává identické údaje, takže je zastupitelný kterýmkoliv jiným. Za druhé, je třeba počítat i se zálohami, které tyto servery mají neznámo kde. Obě tyto komplikace zřejmě lze překonat, třetí námitka je ale závažnější.

Ne vždy jde totiž o jednotlivé stroje ukryté kdesi ve sklepě. Tak je tomu u šesti DNS serverů, které se všechny nacházejí na území Spojených států. Skupina zbylých sedmi serverů se sice při odkazu ze sítě tváří jako samostatné počítače, fyzicky jsou ale rozesetě po celém světě. Server, označovaný písmenem F, se skládá z 46 počítačů rozmístěných od Kalifornie po HongKong a od Johannesburgu po Oslo. Server J má dokonce 51 uzlů. Součástí obou těchto sítí je také server v Praze. Celkem po světě najdete 167 fyzických serverů.

I váš počítač může být teroristá

Takové množství cílů z hlediska fyzického odstranění vypadá jako neřešitelný problém. Je proto potřeba bojovat jejich zbraněmi – přistupovat k nim po síti. Zevnitř sítě totiž naštěstí stojíme proti pouhým třinácti (byť velmi silným) protivníkům. Jaká je jejich fyzická struktura, nás teď nemusí zajímat.

V historii internetu se do dnešního dne uskutečnily dva masivní útoky na kořenové DNS. První z nich začal 21. října 2002 a trval něco přes hodinu. Útočníci zaplavili servery obrovským množstvím nesmyslných dat (datových paketů), takže počítače nebyly schopné reagovat na skutečné požadavky na síti. Tímto způsobem se podařilo odstavit devět ze třinácti serverů. Architektura internetu, postavená na sdílení stejných dat všemi servery, ovšem útoku odolala bez závažnějších problémů. Po dobu útoku provoz po síti fungoval, byl jen pomalejší.

Konkrétní útočníky se nikdy nepodařilo odhalit. K zaplavení sítě falešnými pakety totiž použili rozsáhlý botnet (síť destrukčních počítačů), rozprostřený po celém světě.

Architektura sice odolala, ale pořádně se pod náporem prohnula. Útok ovšem alarmoval provozovatele kořenových DNS serverů. Ti se shodli na vývoji nové technologie, sloužící k další decentralizaci serverů. Při hypotetickém útoku na server se pak měl útok rozpustit v množství mirrorů (menších serverů, kopírujících obsah kořenového DNS serveru). Při zaplavení jednoho konkrétního serveru se měl nápor rozptýlit mezi desítkami jeho kopií – každý požadavek v novém systému míří k nejbližšímu lokálnímu serveru. Nový systém dostal jméno Anycast.

Bomby proti hackerům

Rozdíl mezi starým a novým systémem se naplno projevil 6. února 2007. Tentokrát byl útok veden na šest ze třinácti serverů. Čtyři z nich stačily Anycast aplikovat, zbylé dva ne. Útok byl oproti předchozímu ještě masivnější, delší i lépe promyšlený. První kolo útoku trvalo dvě a půl hodiny, druhé pět hodin.

Ze šesti serverů se dva podařilo téměř totálně odstavit. Šlo o servery, umístěné ve Spojených státech a nevyužívající technologii Anycast. Zbylé servery útok přestály víceméně bez problémů. Zajímavé je, že se tentokrát podařilo vystopovat původce útoků. Sice nebyla objevena konkrétní organizace, ale podařilo se lokalizovat umístění botnetu. Téměř všechny nakažené počítače útočily z asijsko-pacifické oblasti. V reakci na útok se zástupci Spojených států vyjádřili v tom smyslu, že pokud bude znovu napadena jejich komunikační infrastruktura, odpoví nejdříve kybernetickým protiútokem. Jestliže ani tehdy útok neustane, přenesou problém z virtuálního světa do reality a zaútočí na původce bombami.

Obálka bulvárního deníku Weekly World News slibuje 11. ledna 2003 teroristický útok na internet. Katastrofický scénář se naštěstí nekonal

Návrh řešení

Fyzický útok na kořenové DNS servery je vzhledem ke kombinaci mnoha problémů nereálný. Druhá varianta, virtuální útok pomocí zaplavení serverů datovými pakety, by byla reálná pouze v případě shromáždění opravdu obrovského množství destrukčních počítačů k odstavení všech 167 serverů na dostatečně dlouhou dobu. K tomu se musí přidat dokonalá decentralizace botnetu a perfektní utajení místa, ze kterého je nakažená síť ovládána, neboť hrozí jeho fyzická likvidace. Nezbytnou podmínkou útoku je také znemožnění komunikace mezi správci kořenových DNS serverů a jejich zrcadel (mirrorů).

V některých domorodých kulturách znamená znalost pravého jména moc nad jeho nositelem. Podobné je to i se strukturou internetu