DoS: Odmítnutí síťových služeb

Vložil/a cm3l1k1 [1], 14 Říjen, 2004 - 18:22

- Hacking [2]
- Security [3]

Útoky na internetové servery jsou vděčným tématem novinových článků i diskusních příspěvků na webu. Když se ale něco takového přihodí vám, zřejmě uvidíte celý problém ze zcela jiné perspektivy.

Autorem tohoto článku, který vyšel v Computerworldu 6/2003 je Deborah Radcliffová.

Útoky na internetové servery jsou vděčným tématem novinových článků i diskusních příspěvků na webu. Když se ale něco takového přihodí vám, zřejmě uvidíte celý problém ze zcela jiné perspektivy. Jedním z typů útoků, kterým je věnována značná pozornost uživatelů i médií, je DoS (Denial of Service). DoS (Denial of Service) je forma útoku, při níž je síťový server zahlcen tisíci falešných požadavků na poskytnutí nějakých služeb nebo dat. Tyto požadavky jsou vysílány programy umístěnými na jednom nebo několika vnějších počítačích. Vzhledem k zahlcení serveru falešnými požadavky není možno uspokojovat potřeby skutečných uživatelů.

Například společnost Terra Lycos, respektive její velmi navštěvované internetové produkty, jako Lycos Mail, Tripod nebo Angelfire, odolávají útokům typu DoS nejméně jedenkrát měsíčně. Firma přitom zajišťuje provoz více než 300 různých webů, které navštěvuje 40,3 milionu uživatelů. Množství lidí postižených nedostupností služeb, kterou útoky DoS mohou (v případě svého úspěchu) způsobit, je tak značné. „Společnosti, které působí na internetovém mediálním trhu nebo poskytují hostingové služby, jsou obvyklým cílem útoků typu DoS," říká Tim Wright, CTO (Chief Technology Officer) a CIO (Chief Information Officer) společnosti Terra Lycos. V případě jeho společnosti však nejde o smrtící útoky typu DDoS (Distributed Denial of Service), které k zahlcení serverů využívají množství předem napadených serverů, ale o starší typ DoS. (Útoky DDoS byly značně medializovány před třemi lety v souvislosti se zahlcením serverů Amazon, Yahoo, eBay a dalších.) Ani při odrážení útoku typu DoS však není situace jednoduchá.

Staré, ale silné

Útoky typu DoS, se kterými se Wright setkává, se na počítačové scéně vyskytují podstatně déle než útoky typu DDoS. Zatímco v případě distribuovaného útoku DoS se využívá především efektu síly -- ohromného množství předem podrobených serverů, které k nebohé oběti posílají své žádosti -- útoky typu DoS si vystačí se zahlcením žádostmi o spojení z jednoho nebo několika málo počítačů. Jde o tzv. útoky syn flood, které jsou snad tak staré jako samotný protokol TCP.

Útoky typu syn flood posílají falešné požadavky na synchronizaci při zahájení spojení (connection synchronization -- syn). Cílový server vyšle odpověď ack (acknowledgement), na kterou však již neobdrží žádnou reakci. Cílový server drží session otevřenou po předem definovaný úsek času a poté ji zavře. Pokud takových požadavků přijde velké množství, server má otevřené velké množství spojení a není schopen obsloužit další uživatele. V případě množství falešných požadavků pak vlastně jen čeká na odpovědi -- a neobsluhuje nikoho, protože není schopen otevřít další spojení. Proti útokům typu syn flood neexistuje v podstatě žádná ochrana, protože využívají způsobu definovaného pro zahájení TCP session. „Nejhorší útoky jsou takové, při kterých se protokoly tváří, že je všechno v pořádku," komentuje tuto skuztečnost Wright.

Dokonalejší útoky

Útočníci jsou vynalézaví, a tak se i útoky typu syn flood zdokonalují -- a stávají se daleko nepříjemnějšími. Nová forma syn flood, nazývaná DRDoS (Distributed Reflection Denial of Service), byla přibližně před rokem použita proti serverům společnosti Gibson Research. Útok trval čtyři hodiny a přidělal vedení firmy nemálo starostí. Útok typu DRDoS je podle Steva Gibsona, prezidenta společnosti GRC, do jisté míry opakem útoku typu syn flood. Gibson sám razí tento nový název právě od doby, kdy loni v lednu takový útok zažil na vlastní kůži. Tenkrát útočníci zahlcovali množství počítačů na internetu pakety, které měly tyto stroje přesvědčit, že se GRC.com snaží iniciovat spojení. A tato zařízení, jako hodné a poslušné přístroje, masově odeslala na GRC.com odpověď ack.

Server GRC.com věděl, že neodeslal žádnou žádost o inicializaci spojení, a tak příchozí zprávy ack prostě zahodil. Odesílací zařízení se však domnívala, že se jejich zprávy ztratily kdesi v kybernetickém prostoru, a tak poslala zprávy znovu tak, až se intenzita útoku zečtyřnásobila. Gibson tvrdí, že ví o řadě dalších firem, které byly napadeny útokem typu DRDoS. „Webhostingové společnosti a velké webové servery jsou těmi největšími a nejsnáze zaměřitelnými cíli," říká. „To prostě naštvete někoho, kdo je schopen pomocí stažené utility zahájit útok, a on ani chvíli neváhá, aby vás potrestal," dodává.

Filtrování příchozích paketů podle Wrighta i Gibsona nepomáhá, protože zpomaluje veškerý provoz. V případě útoku typu DRDoS navíc pakety přicházejí odevšad, takže není možné odfiltrovat jen jednu nebo několik adres. Jedinou možností, jak se s takovými útoky vypořádat, je podle Gibsona odpojit cílový stroj od webu a vyčkávat, až se situace uklidní. Je také možné požádat svého poskytovatele internetových služeb, aby zrušil spojení s vaším serverem, tj. aby zahazoval příchozí pakety syn i ack směřující k cílovému stroji. „Tak útočníci nemohou blokovat provoz dalším strojům připojeným do stejného síťového segmentu," vysvětluje. „Ale když se nad tím zamyslíte, tak zjistíte, že útočníci stejně vyhráli. Váš server je nefunkční. Ale co se s tím dá dělat," zakončuje Gibson.

Léky na útoky typu syn flood

* Zkraťte dobu, po kterou server čeká na pokračování session vyvolané příkazem syn po odpovědi ack.
* Blokujte provoz, který přichází z útočících falešných IP adres.
* Použijte filtrování paketů tekoucích z vaší sítě, abyste zabránili zneužití vlastních serverů pro roli útočníků na další servery.

Léky na útoky typu DRDoS

* V době útoku požádejte svého poskytovatele infternetových služeb, aby zrušil cestu paketům jdoucím na napadenou IP adresu. To ovšem bohužel znamená ztrátu možnosti komunikovat z této adresy, a tedy vyřazení služby z provozu.
* Požijte nástroje pro analýzu vzorků síťového provozu a síťové čmuchaly (sniffers), abyste byli schopni rychleji rozpoznat přicházející útok.

URL článku:
https://www.security-portal.cz/clanky/dos-odm%C3%ADtnut%C3%AD-s%C3%AD%C5%A5ov%C3%BDch-slu%C5%BEeb

Odkazy:
[1] https://www.security-portal.cz/users/cm3l1k1
[2] https://www.security-portal.cz/category/tagy/hacking
[3] https://www.security-portal.cz/category/tagy/security