DDoS – sofistikovaný útok

nebo služba na objednávku?

Zuzana Duračinská, Pavel Bašta

Základem kybernetické bezpečnosti je zabezpečení dostupnosti, integrity a důvěryhodnosti informací. Intenzívní DoS a DDoS útoky vedené v roce 2013 v několika vlnách proti známým webovým serverům a službám v České republice výrazným způsobem poznamenaly první zásadu kybernetické bezpečnosti - dostupnost služeb a s tím spojených informací. Po samotném útoku se však objevily další, vedlejší efekty útoku – od zvýšení všeobecného povědomí o možných kybernetických útocích u širší veřejnosti až po zvýšení informovanosti o potřebě lepšího zabezpečení v IT infrastruktuře u techniků a bezpečnostních manažerů.

Smyslem DoS i DDoS útoku je jednoduchý: omezit dostupnost služby. To je možné udělat alespoň na jedné součásti samotného systému: výpočetní kapacitě, operační paměti či síťovému pásmu.

Pro začátek je dobré pochopit, zdali se jedná o útok typu DoS (Denial of Service) nebo DDoS (Distributed Denial of Service). I když je výsledek útoku v obou případech stejný, zásadně se liší zdroj, resp. počet zdrojů, které útok generují. Jak již z názvu „distributed“ vyplývá, packety můžou přicházet na cíl z různých zdrojů, k čemuž se nejčastěji využívají botnety. Detekce se tak stává poměrně náročná, protože není možné snadno definovat zdroj DDoSu a zamezit tak útoku. Například s využitím blokace IP rozsahů, které zahlcující systém oběti. Při DoS útoku přicházejí pakety z jednoho zdroje, což však nemusí být vždy na první pohled patrné. Generování útoku jedním nebo druhým způsobem je lehčí, než se může na první pohled zdát. Pro vytvoření DDoS útoku si můžeme pronajmout například nějaký botnet nebo využít amplifikaci. Při realizaci útoku z jednoho centra potřebujeme jenom silnou přípojku do Internetu (v řádech jednotek Gbps a vyšších).

Kde zasáhnout?

DoS resp. DDoS útok je obvykle směrován na jednu ze síťových vrstev. Přes každou síťovou vrstvu je možné nějakým způsobem službu vyřadit z provozu, avšak zabezpečení jedné vrstvy často nezabrání útoku na jinou. Proto je nezbytné věnovat pozornost každé vrstvě zvlášť. Podle toho, na kterou z OSI vrstev se útočník zaměří, se odlišuje také samotný způsob útoku (viz. tabulka).

Jak můžeme vidět, v IT infrastruktuře je hned několik cílů, na které je možné se zaměřit. I když se nám podaří jednotlivé vrstvy odpovídajícím způsobem dostatečně zabezpečit, je nutné přicházející útok rychle detekovat.

Monitorování provozu

Abychom mohli útok resp. sérii útoků v síti detekovat, je potřeba vědět, co se v síti odehrává.

Vrstva OSI	Využívaný protokol a služby	Příklad techniky útoku	Mitigace uvedeného příkladu
Aplikační vrstva	FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP	HTTP get/post - přihlašování do aplikace, upload videa, zasílání komentářů	monitorováni aplikace, CAPTCHA. Vzhledem k tomu, že na této vrstvě útoky „napodobují“ lidské konání, obrana je náročnější
Prezentační vrstva	komprimace, šifrování, konvertování	útok pomocí upravených SSL dotazů	přesměrování SSL dotazů z původní infrastruktury přes nějaký jiný zdroj
Relační vrstva	zahájení a ukončení relačního spojení	omezení služeb jinak přístupných přes Telnet	útok je možný v důsledku zranitelnosti, která může byt updatem odstraněná
Transportní vrstva	TCP, UDP	SYN flood, Smurf attack. Omezuje počet síťových připojení na zařízeních	informování o blackholingu u svého poskytovatele připojení
Síťová vrstva	směrování a síťové adresování	ICMP flooding	stanovení limitu na ICMP
Linkova vrstva	switche a přepínače	MAC flooding	omezení počtu MAC adres které mohou porty přijmout
Fyzická vrstva	síťové kabely	fyzická manipulace s vedením	omezení fyzického přístupu

K tomu slouží pasivní monitorovaní sítě. Provozovatelé větších i menších síti by měli pasivně monitorovat provoz na svých směrovačích optimálně exportem NetFlow/sFlow. Tyto exporty jim umožňují zaznamenávat informace o provozu, a to na úrovní zdrojové a cílové adresy, zdrojového a cílového portu, využitého protokolu či časových údajů. Data slouží na případnou zpětnou identifikaci útoku. Všechny tyto informace by pak v případě útoku měly provozovatelé síti být schopni vygenerovat v podobě například pcapu, a proto je vhodné daná data nějaký čas uchovávat (zpravidla až několik měsíců nazpět). Mimo pasivní ochranu je vhodné využívat také ochranu aktivní. K aktivní ochraně přistupujeme, pokud chceme podezřelý resp. škodlivý tok dat odfiltrovat. Aby tak provozovatelé sítí učinili, je nezbytné mít k dispozici alespoň zdrojovou a cílovou IP adresu a TCP/UDP porty. Provozovatelé páteřní infrastruktury mají na zastavení útoku jiné možnosti.

Jednou z možností, jak zastavit pakety ještě před tím, než dorazí do sítě, je technika známa jako Remotely-Triggered Black Hole. Ta využívá možností BGP protokolu k tomu, aby omezila pakety odesílané na rozsah oběti ze směru, který daná relace obsluhuje. Tato technika filtrace škodlivého provozu je možná mezi sítěmi, které se předem na tento stav připravily, nebo přes peeringový uzel, který tuto techniku podporuje.

Po již zmíněných (D)DoS útocích v roce 2013 byla tato technika přidána i do pravidel projektu FENIX, který je zastřešen peeringovým uzlem NIX.CZ. Cílem projektu je omezit nebo zkomplikovat realizaci útoků a tím zvýšit dostupnost internetových služeb v rámci subjektů zapojených do této aktivity. Projekt funguje na principu virtuální sítě, skrz kterou si členové v případě útoku mohou vyměňovat data. Nemělo by tedy dojít k přerušení provozu služeb. Pro vstup sítě do tohoto projektu je potřeba splnit poměrně náročné bezpečnostní, technické a organizační podmínky. Což mimo jiné zajistí, že sítě si budou navzájem důvěřovat. A v případě potřeby budou ochotné spolupracovat při řešení útoku. Takováto spolupráce boje proti (D)DoS útokům je ve světě jedinečná a sítím otevírá nové možnosti obrany.

Amplification útoky

Pro zvýšení síly útoku může útočník využívat amplifikaci (nebo-li zesílení). Pro amplification útoky se zneužívají síťové služby umožňující zesílení dopadu útoku. Samotná amplifikace spočívá ve využití možnosti získaní několikanásobně delší odpovědi na dotaz, u něhož je odpověď zaslána na podvrženou adresu (adresu oběti). Pro toto zesílení se zneužívají veřejně dostupné UDP služby, jako jsou DNS, NTP nebo SNMP. Za pomoci zneužití těchto služeb tak může i útočník s pomalejší linkou vygenerovat dostatečně silný útok. Důvod, proč se pro amplifikaci zneužívá UDP protokol, je že na rozdíl od TCP protokolu je tento protokol nespojovaný a neprobíhá v něm trojcestný handshake. Data jsou tak zasílána cílovému serveru bez vzájemného ověření. Právě díky neexistujícímu mechanismu navazování komunikace v protokolu UDP pak může útočník podvrhnout zdrojovou IP adresu a server bude považovat obdržený požadavek za skutečně odeslaný z podvržené IP.

V roce 2014 jsme byli svědky několika amplification útoků. Tyto útoky dosahovaly síly i přes 400 Gbps (případ zneužití NTP), což by již řadu systémů dokázalo vyřadit z provozu. Pro zaslání dotazů na cílový server je potřebné podvrhnout z IP adresu v hlavičce paketu a tudíž se jedná o IP spoofing. Tomu je možné zabránit přes implementaci standardu BCP38, který zabrání tomu, aby bylo možné využít síť třetí strany jako reflektor pro amplifikaci. Odchozí provoz z takovéto sítě může obsahovat jenom zdrojovou IP adresu z jejího přiděleného rozsahu. Jako reflektory jsou pro amplifikaci využívány nejčastěji otevřené resolvery. Problém rekurzívních DNS serverů spočívá v tom, že odpovídají i na dotazy z vnějšku. Útočník toho pak může jednoduše využít tak, že na DNS server zašle dotaz se zdrojovou IP adresou oběti. Server vygeneruje a odešle za útočníka několikanásobně větší odpověď přímo na adresu oběti. Při velkém (D)DoS na Spamhaus v roce 2013, se právě ve s využitím otevřených resolverů vygeneroval provoz o síle až 300 Gbps. I když jsme od té doby byli svědky i silnějších útoků, právě útok na Spamhaus rozpoutal debatu o potřebě dodržování pravidel bezpečného síťového provozu.

Jak můžeme vidět, poměr potřebné síly vynaložené na útok a obranu není vyvážen. Dostatečně silný útok vygenerujeme i pomocí pronájmu botnetu či zneužitím resolverů, kterých je stále poměrně dost. S případnou obranou je pak potřeba počítat hned na několika místech infrastruktury. V dnešní době by mělo být pasívní monitorování síti spolu s aktivní obranou neodmyslitelnou součástí každé sítě. Každý rok jsme svědky nových rekordů v generované síle útoku. Kolik Gbps bude zapotřebí na odstavení služeb v roce 2015, můžeme zatím jen tipovat. ■

Pavel Bašta

Autor článku pracuje v týmu CZ.NIC-CSIRT.CZ jako bezpečnostní analytik. Dříve pracoval ve společnosti Telefónica v dohledovém centru datových okruhů a zastával pozici administrátora informačních systémů. Je držitelem certifikace MCSE a MCTS.

Zuzana Duračinská

Autorka článku také působí v týmu CSIRT.CZ K její hlavním činnostem patří provoz služby Skener webu, příprava a realizace kybernetických cvičení, příprava odborných článků a reprezentace týmů. Pracuje také na rozvíjení spolupráce s členy bezpečnostní komunity.