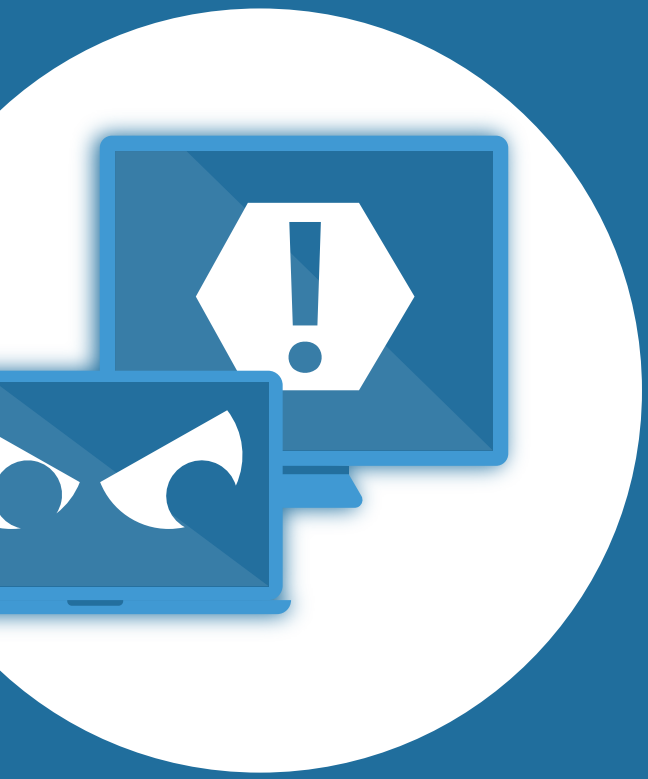
CLOUDFLARE
PARTNER NETWORK



Zkrocení stále se vyvíjející obludy jménem DDoS

ZEBRA SYSTEMS

První útok odepření služby (denial of service – DoS) byl pozorován v roce 1974, když zvědavý mladistvý středoškolský student spustil softwarový experiment, který měl zabránit přístupu k přihlášení do počítačů v místnosti plné uživatelů. Od té doby se malý experimentální DoS vyvinul do současné kybernetické obludy – a tato obluda se dramaticky vyvíjí. Například v poslední dekádě jsme pozorovali vytvoření webových stránek „DDoS k pronájmu“, které nabízejí funkci DDoS jako služba pro technicky zdatné i nekvalifikované uživatele.

3 odporné hlavy DDoS Monstra: Rozsah, Využití více vektorů a Všudypřítomnost

1. ROZSAH

V roce 2016 přitáhl pozornost světa DDoS útok z botnetu Mirai: masivní cílený objemový DDoS útok vyřadil z provozu OVH, jednoho z největších evropských poskytovatelů hostingu. Podle telemetrie OVH zahrnoval útok ve špičce 1 Tb/s, a byl proveden pomocí 145 tisíc IoT zařízení.

O pár let později, v roce 2018, prodělal jeden z největších zaznamenaných objemových DDoS útoků GitHub: šlo o 1,35 Tb/s a využíval obskurního zesilujícího vektoru: protokolu memcached, který používá UDP port 11211.

Velké útoky jsou působivé; ovšem generování velkého objemu provozu kvůli vyčerpání prostředků oběti je nákladné. Kvůli tomu se trend v útocích přesouvá ke shlukovým útokům. Ty jsou významně velké co do objemu, ale mají kratší trvání, což zaplaví cílovou webovou stránku, ale potenciálně může zůstat nezachyceno automatickými systémy kvůli svému krátkému trvání.

2. VYUŽITÍ VÍCE VEKTORŮ

Taktika DDoS útoků, tak jako taktiky jiných útoků na bezpečnost, často využívá slabin v procesech komunikačních protokolů.

Když si jako příklad vezmeme TCP protokol, tam DDoS útok může vyčerpat prostředky serveru prostřednictvím záplavy SYN paketů nebo ACK paketů. Existence slabin jako jsou tyto napříč mnohými protokoly včetně UDP a ICMP poskytuje zlomyslným aktérům arzenál různých taktik útoků, které mohou při provádění DDoS útoku využít.

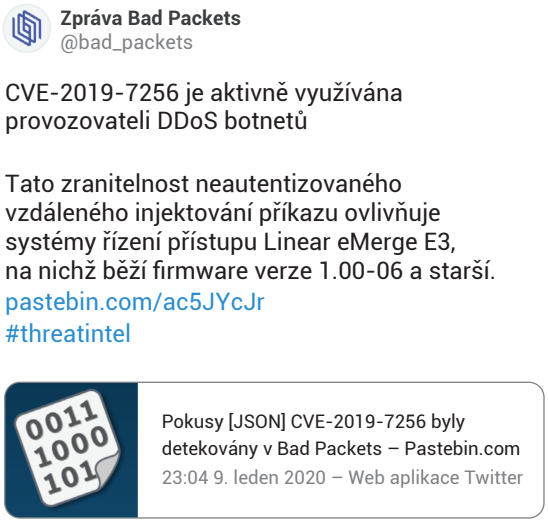
Například Wikipedia detekovala velké globální narušení přístupu uživatelů na jejich stránky v září 2019 po dobu přibližně 9 hodin. Zatímco dostupnost a výkonnost webové aplikace byla negativně ovlivněna na vrstvě HTTP serverů, DDoS útok cílil přímo na datové centra Wikipedie na síťové vrstvě. Pozorovaný objem útoku činil přes 250 Gb/s a byl kombinací záplavy ACK and UDP paketů.

3. VŠUDYPŘÍTOMNOST

Útoky DDoS jsou smutnou skutečností pro dnešní organizace a podniky. Zatímco společnosti ve větších ekonomikách, jako jsou Spojené státy, jsou lukrativním cílem pro útočníky se škodlivými úmysly, sofistikovaným DDoS útokům čelí podniky po celém světě bez ohledu na to, do které odvětvové vertikály se řadí. V roce 2019 zakusily jihoafrické banky vytrvalé DDoS útoky, které byly doprovázeny zprávami požadujícími výkupné, zatímco jihoafrické telekomunikační společnosti jako Liquid Telecom odrážely masivní DDoS útoky, jejichž objem překračoval 100 Gb/s.

„Zlomyslní aktéři neustávají ve zkoumání nových cest a taktik, jak provádět pokročilé DDoS útoky."

Rostoucí apetit DDoS příšery



Začátek roku 2020 se vyznačoval masivními DDoS útoky. EVE Online, společnost dodávající online hry pro velké množství současných hráčů (massively multiplayer online – MMO), zakusila kvůli DDoS útoku několikadenní výpadek služeb. Online fóra pro hru byla zaplavena znechucenými hráči, kteří chtěli zrušit své účty nebo požadovali odškodnění, protože se nemohli po 4 dny přihlásit. U MMO her je pro zákazníky nesmírně frustrující i malý nárůst doby odezvy, natož pak několikadenní výpadek.

Zlomyslní aktéři neustávají ve zkoumání nových cest a taktik, jak provádět pokročilé DDoS útoky. Příkladem může být fakt, že hackeři se v současné době pokoušejí skenovat Internet a vyhledat vystavená zařízení NSC Linear eMerge E3 s cílem zneužít zranitelnosti CVE-2019-7256, která by jim dovolila ovládnout zařízení, stáhnout tam a instalovat malware, a potom spustit DDoS útoky na další cíle. Tato zařízení jsou instalována obecně v budovách podniků, výrobních závodech a podobné infrastruktuře a slouží jako řídící přístupový systém pro zaměstnance a návštěvníky.

Zničte obludu DDoS v cloudu

Tradiční přístupy ochrany před DDoS spočívající v používání hardwarových apliancí umístěných v lokalitě uživatele jsou zastaralé, protože dnešní DDoS útoky jsou větší, sofistikovanější a globální, a lokální řešení ochrany před DDoS nejsou schopná čelit takovému rozsahu, rychlosti a distribuované povaze útoků.

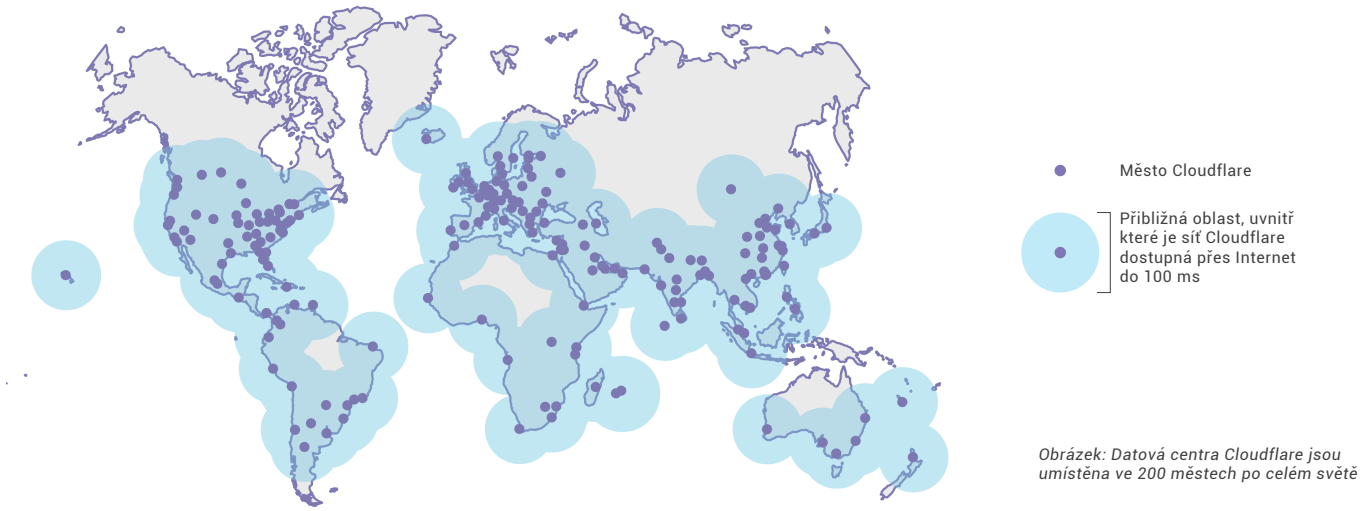
Avšak distribuovaná architektura cloudových řešení pro ochranu před DDoS poskytuje trvale pohotové obranné postavení pro eliminaci DDoS útoků v celosvětovém měřítku. Při výběru cloudového řešení ochrany před DDoS je zásadně důležité vzít v úvahu následující aspekty:

DISTRIBUOVANÁ ARCHITEKTURA

Globální povaha DDoS útoků vyžaduje, aby řešení ochrany před DDoS útoky mělo celosvětově distribuovanou architekturu, aby tak mohlo omezovat útoky co nejblíže jejich zdroje. S tím, jak se objem jednotlivých DDoS útoků zvětšuje, tradiční přístup „čistících" center se pro cloudová řešení DDoS brzy stane zastaralým. Je to důsledkem povahy čistících center tvořících ‚škrtící klapku'. Poskytovatelé tradičních řešení ochrany před DDoS investovali do malého počtu čistících center, do kterých musely být velké DDoS útoky odkloněny, protože neměli skutečně distribuovanou architekturu.

O nedostatcích přístupu založeného na čistících center se můžete dovědět více v tomto vynikajícím blogu - 'Už žádné čištění (No scrubs).'

Moderní řešení ochrany před DDoS od Cloudflare běží jako služba na každém serveru napříč všemi datovými centry Cloudflare, které jsou ve 200 městech po celém světě, a díky tomu tvoří skutečně distribuované DDoS řešení. Ať vychází DDoS útok z jakéhokoli kout světa, je eliminován v nejbližším datovém centru Cloudflare, což umožňuje rychlejší eliminaci útoku a prodloužení doby dostupnosti infrastruktury zákazníků.



Obrázek: Datová centra Cloudflare jsou umístěna ve 200 městech po celém světě

ZEBRA SYSTEMS

KAPACITA SÍTĚ

Chcete-li umlčet rozsah a velikost DDoS útoku, hraje klíčovou roli síťová kapacita řešení pro ochranu přes DDoS útoky, zejména při DDoS útocích majícím rozsah v řádu Tb/s.

Celosvětová síť Cloudflare Anycast má síťovou kapacitu přes 30 Tb/s, což jí umožňuje eliminovat dokonce i největší DDoS útoky. Navíc je Cloudflare připojen k více internetovým propojovacím bodům (IXP) než jiní poskytovatelé na celém světě. Síť Cloudflare je propojena s více než 8 tisíci sítí po celém světě včetně velkých ISP, cloudových služeb a podniků.

KOMPLEXNÍ POKRYTÍ

Existuje celý arzenál taktik útoků, které mohou zlomyslní aktéři využít pro spuštění DDoS útoku jak na aplikační, tak na síťové vrstvě. Cloudová řešení pro DDoS by měla mít schopnost eliminovat DDoS útoky komplexním způsobem na více vrstvách.

Pokročilá ochrana před DDoS Cloudflare poskytuje komplexní pokrytí ochranou proti útokům na 7. vrstvě, zatímco Cloudflare Spectrum a Magic Transit eliminují DDoS útoky na vrstvách 3 a 4. Blog ThousandEyes o analýze DDoS útoku proti Wikipedii vyzdvihuje, jak Cloudflare dovedl rychle a komplexně eliminovat velký multivektorový DDoS útok.

ROZVĚDKA V REÁLNÉM ČASE

Namísto aby byla ochrana před DDoS v reaktivním režimu, měla by nová řešení být zesílena pomocí rozvědky zaměřené na hrozby pracující v reálném čase, a tak vyvíjet proaktivní obranný val pro eliminaci DDoS útoků.

Řešení ochrany před DDoS Cloudflare je založeno na rozvědce hrozeb, která shromažďuje informace díky své stále se učící síti, která chrání přes 20 miliónů internetových sídel a prověřuje každodenně přes 1 miliardu jedinečných IP adres. Ochrana před DDoS Cloudflare vyzbrojená touto rozvědkou hrozeb, modely založenými na strojovém učení a technickými znalostmi týmu otestovanými řadou bitev, poskytuje robustní řešení schopné čelit nejpromyšlenějším DDoS útokům.

ZEBRA SYSTEMS

AUTOMATIZOVANÁ ELIMINACE

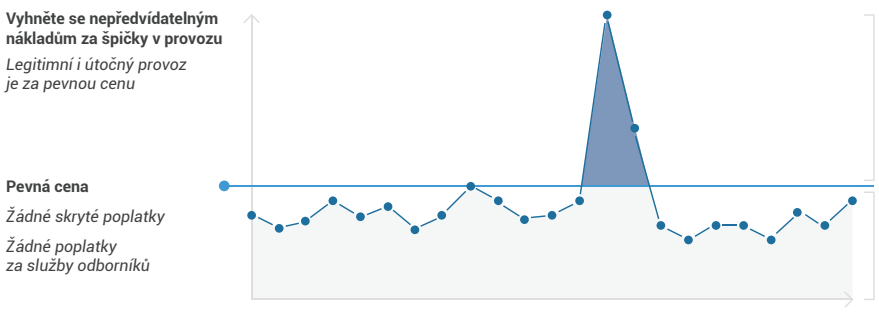
Chcete-li umlčet rozsah a velikost DDoS útoku, hraje klíčovou roli síťová kapacita řešení pro ochranu přes DDoS útoky, zejména při DDoS útocích majícím rozsah v řádu Tb/s.

Celosvětová síť Cloudflare Anycast má síťovou kapacitu přes 30 Tb/s, což jí umožňuje eliminovat dokonce i největší DDoS útoky. Navíc je Cloudflare připojen k více internetovým propojovacím bodům (IXP) než jiní poskytovatelé na celém světě. Síť Cloudflare je propojena s více než 8 tisíci sítí po celém světě včetně velkých ISP, cloudových služeb a podniků.

EKONOMICKÁ EFEKTIVITA

S tím, jak narůstá velikost a rozsah DDoS útoků, musí každý podnik a organizace zvažovat náklady na ochranu před DDoS tak, aby byly udržitelné. Poskytovatelé cloudových řešení ochrany před DDoS útoky často používají počítanou ochranu před DDoS. Zatímco cloudová řešení poskytují vynikající ochranu v porovnání s lokálními řešeními tím, že se pružně přizpůsobují tak, aby vhodně chránila před DDoS útoky, může mít počítaná eliminace často za následek obrovské špičky v účtovaných částkách. A tak místo aby podniky ztrácely peníze za neobsloužené zákazníky, mohou být potenciálně ochromeny počítanými náklady na eliminaci DDoS útoků.

Cloudflare nabízí neomezenou a nepočítanou eliminaci DDoS útoků. Tím se odstraňuje zastaralá koncepce ‘určování ceny podle náporu,’ který je zvlášť bolestivý, když je podnik pod tlakem a zakouší DDoS útok. Tím se můžete vyhnout nepředvídatelným nákladům kvůli provozním špičkám.



Staňte se hrdinou zničte obludu DDoS ještě dnes!

ZEBRA SYSTEMS