DoS a DDoS útoky (Odmítnutí služby)

DoS útok je pokusem o vyřazení zdroje z provozu tím, že se zaplní jeho kapacita pro zpracování požadavků nebo se vyčerpá jeho síťová propustnost. Pokud útok probíhá z mnoha různých míst najednou (často z tisíců infikovaných počítačů), mluvíme o **DDoS útoku** (Distributed Denial of Service).

Jak útok funguje?

Představte si útok jako dav lidí, který se naráz pokusí projít dveřmi do malého obchodu. Skuteční zákazníci se dovnitř nedostanou, protože vstup je zcela zablokován útočníky, kteří tam ve skutečnosti nechtějí nakupovat.

Hlavní typy útoků:

- **Objemové útoky (Volumetric):** Cílem je zahltit šířku internetového pásma (linku). Útočník posílá obrovské množství dat, dokud se linka „neucpe“.
- **Protokolové útoky:** Zaměřují se na slabiny v síťových protokolech (např. TCP/IP). Příkladem je **SYN Flood**, který vyčerpá paměť serveru tím, že otevírá tisíce nedokončených spojení.
- **Aplikační útoky (Layer 7):** Nejsložitější typ. Útočník simuluje běžné chování uživatele (např. neustále načítá vyhledávání na e-shopu), což enormně zatěžuje procesor a databázi serveru.

Co je to Botnet?

U **DDoS** útoků útočník nevyužívá svůj vlastní počítač (ten by byl snadno odhalen a zablokován). Místo toho ovládá **botnet** – síť „zombie“ počítačů, chytrých televizí nebo kamer (IoT zařízení), které byly dříve infikovány virem. Na povel útočníka začnou všechna tato zařízení naráz bombardovat cíl požadavky.

Srovnání DoS a DDoS

Vlastnost	DoS	DDoS
Počet zdrojů	Jeden útočník (jedna IP adresa).	Tisíce až miliony zdrojů.
Náročnost obrany	Snadná (stačí zablokovat jednu IP).	Velmi obtížná (útok přichází odevšad).
Síla	Omezená výkonem jednoho stroje.	Obrovská (schopná vyřadit i velké korporace).

Motivy útočníků

- **Vydírání:** „Zaplaťte výkupné, jinak váš web během výprodejů shodíme.“
- **Hacktivismus:** Protest proti politickému nebo společenskému rozhodnutí.
- **Konkurenční boj:** Snaha poškodit podnikání soupeře.
- **Krytí jiného útoku:** DDoS se často používá jako „kouřová clona“, která odvede pozornost správců, zatímco útočník krade data jinou cestou.

Jak se bránit?

Obrana vyžaduje kombinaci technologií a strategií:

```
1. **Firewall a IPS:** Detekce a blokování podezřelých vzorců chování.
2. **Rate Limiting:** Omezení počtu požadavků, které může jedna IP adresa poslat za sekundu.
3. **Anycast a Scrubbing centra:** Služby (jako Cloudflare nebo Akamai), které provoz "proženou" čistícími servery, kde odfiltrují škodlivé pakety a k cíli pustí jen ty legitimní.
4. **[[rpki|RPKI]] a BGP filtrace:** Pomáhá proti útokům využívajícím [[bgp_hijacking|BGP hijacking]] k přesměrování provozu.
```

Související pojmy: BGP Hijacking, Firewall, Botnet, IP adresa, TCP/IP, DNS, RPKI.