Praktické zkušenosti s (D)DoS útoky

Ing. Tomáš Hála
ACTIVE 24, s.r.o.
www.active24.cz

Proč si o tom povídáme?

Dva příklady z poslední doby

- DoS útoky v ČR z března 2013
  - internetová média
  - portál Seznam.cz
  - banky
  - telekomunikační operátoři

- DoS útok na Spamhaus (CloudFlare)

Co s tím má společného ACTIVE 24?

Co s tím má společného ACTIVE 24?

- provozujeme portál iHNed.cz (vč. Respekt.cz, Ekonom.cz aj.)

- provozujeme projekty pro mobilní operátory

- provozujeme stránky bank

- obdobným útokům čelíme dlouhodobě
  (např. eshopy s RC modely, exekutoři, DC HUB aj.)

Co se v březnu vlastně stalo?

Co se v březnu vlastně stalo?

- DoS útoky typu SYN flood a odražené SYN-ACK
- spoofované adresy
- datový tok zanedbatelný (desítky až stovky Mbps), ale několik Mpps
- přicházel přes NIX.CZ (ze sítě RETN limited)
- spíše DoS než DDoS
- mediální DoS
- ale jaký byl motiv?

Cyber Europe 2012

Cyber Europe 2012

- předcházet zahlcení pracovníků

- dělit samotné řešení problému od komunikace

- problematika sdílení informací

- cvičení mají smysl – důležité je širší zastoupení

ACTIVE24-CSIRT

- http://www.active24.cz/csirt/

- první a dosud jediný registrovaný CSIRT tým z komerční sféry v ČR

- u Trusted Introducer registrován 9.2.2012 – status Listed

- navázal přímou spolupráci s ostatními týmy v ČR i po celém světě

- úzce spolupracuje s národním týmem CSIRT.CZ

Simulace DoS ve spolupráci s CZ.NIC

Simulace DoS ve spolupráci s CZ.NIC

- v rámci výběrového řízení na nové FW

- firewall má vždy své limity (max pps, sessions rate, sessions count aj.)

- syn cookies – nemusí stačit, ale měly by být zapnuté by default

- překvapivě nižší naměřený strop max pps než udávaná hodnota

Simulace DoS ve spolupráci s CZ.NIC

- výkonný firewall určitě pomůže, ale jen do svých limitů

- extrémní levnost a snadnost vygenerování podobného útoku

- 1M pps lze vygenerovat z běžného serveru s Broadcom kartami

- cena útoku vs. cena protiopatření

- bylo by toho hodně na testování, ale je to zejména otázka času

Aktuality

- náš ACTIVE24-CSIRT tým začal cíleně pracovat na aktivním vyhledáváni a blokováni zneužitých služeb v naší síti, tzn. už neřešíme jen přijatá oznámení, ale aktivně vyhledáváme a neutralizujeme nalezený malware. Blokujeme spoofované adresy, limitujeme množství odeslané pošty, poskytujeme zákazníkům informace a varování aj.

- v rámci NIX.CZ se chystá "čistá" VLAN pro "odpovědné" členy

- BCP-38, omezení rekurzivních i autoritativních DNS aj.- samoregulace

- IPv6 může pomoci zmírnit dopady resp. ztížit provedení útoku

Prostor pro Vaše dotazy