telenor | common operation

DDoS támadások, detektálás, védekezés

Galajda József - Core Transport Network Planning Expert

(D)DoS - áttekintés

- (D)DoS – (Distributed) Denial of Service
  - Szolgáltatás megtagadással járó támadás
  - Célja egy adott informatikai szolgáltatás ellehetetlenítése, megbénítása. A szolgáltatás felhasználóit megakadályozza annak igénybevételében.
  - Amennyiben nem egy helyről indul a támadás, elosztott támadásról beszélhetünk.
  - Gyakran teljesen szabványos eszközök „okos” használatával érik el a céljukat a támadók

Célpontok, motiváció

- WEB szolgáltatások pl. bankok, online fizetési szolgáltatások, kormányzati oldalak, online áruházak, stb.
- Politikai motiváció, anyagi haszonszerzés (pl. zsarolás), szándékos károkozás (bevétel kiesés, presztízs veszteség)
- Más tevékenységek elfedése

Kezdetek

- Nehéz megmondani, mikor volt az első támadás
- „trin00” az első szélesebb körben is ismert DDoS támadás, 1999 augusztusában, a Minesota Egyetem szerverei ellen irányult.
- Két napon keresztül, UDP flood
- A Solaris 2.x rendszereken futtatták a rossz indulatú kódot
- RPC távolról kihasználható puffer-túlírási hiba kihasználásával (exploiting) került a rendszerekre (CERT IN-99-04)
- A forrás címek nem voltak meghamisítva
- Tehát nem új keletű a probléma, viszont az utóbbi pár évben jelentős mennyiségi ugrás történt a támadások gyakoriságában és a támadás során generált forgalom mennyiségében

Támadás típusok

- Sok támadási fajta létezik
- Alapvetően két fő kategóriába lehet a támadásokat sorolni:
  - Mennyiségi (volumetric)
  - Applikáció ellen irányuló

Hálózati rétegek és támadások - Network

- SYN flood
- ICMP/PING flood
  - Egyszerű PING csomagok nagy számban
  - PoD – Ping of Death. Hibás formátumú/túlméretes ICMP csomagok küldésén alapul
  - Smurf attack – aszimmetrikus támadás

Hálózati rétegek és támadások - Network

- Teardrop támadás
  - Átlapolódó IP szeletek
  - Win 3.1, Win 95, NT, Linux kernel < 2.0.32, 2.1.63
- PUSH/ACK flood
  - Szerver oldalról nagyobb erőforrásigény ezeknek a feldolgozása

Hálózati rétegek és támadások - Session

- DNS amplification támadás
  - DNS lekérdezések hamis forrás címmel
  - Nem a DNS szolgáltatás ellen irányul
- DNS NXDOMAIN (non-existent domain) flood
  - Magának a DNS szolgáltatásnak az ellehetetlenítése

Hálózati rétegek és támadások - Session

- NTP amplification
  - Hamis forrás cím
  - Kis kérésre nagy mennyiségű válasz (1 csomag -> 300 válasz csomag)
- SSL flood, SSL renegotiaion
  - Szerver oldalról nagyobb erőforrás igény

Hálózati rétegek és támadások – Alkalmazás réteg

- OWASP top 10 alkalmazás biztonsági kockázat
  - https://www.owasp.org/index.php/Top_10_2017-Top_10
- Slow POST/READ
  - Kiépített kapcsolatban nagyon lassan küldi a kliens az üzenet törzsét (akár 1 byte/2 perc)
  - A szervernek be kell minden részt várni
- Slowloris
  - Kis sávszélesség igény
  - Minél több kapcsolatot minél hosszabb ideig próbál fenntartani
- HTTP GET/POST flood
  - Volumetric

Honnan jön a támadás?

- BOT net
  - Rosszindulatú kód futtatása sok host-on
- A rosszindulatú kód hogy kerül a gépemre?
  - Nem legális szoftverek telepítése
  - Felhasználói figyelmetlenség/nemtörődömség
  - Szoftverhibákat/sebezhetőségeket kihasználva

DDoS rekord

- KrebsOnSecurity.com IT bizonsággal foglalkozó oldal 2016 szeptemberében elszenvedett egy rekord nagyságú DDoS támadást
- 620 Gbps
- Ezt megelőzően a legnagyobb volumenű támadás 336 Gbps volt, amplification jellegű támadásból (aszimetrikus, a küldött adat mennyisége többszörös választ generál)
- A KrebsOnSecurity.com ellen irányuló támadás nem amplification jellegű volt. A támadás web kérések és GRE csomagoknak álcázott szemét formájában jelentkezett, amihez legitim forrás kell
- Ezek egy eddig nem látott méretű és képességű botnet meglétére utalnak

DDoS rekord

- A forgalom nagy számú kompromittált IoT eszközről érkezett
- Routerek, IP kamerák, egyéb okos eszközök, amelyek rossz, vagy alapértelmezett biztonsági beállításokkal kapcsolódnak a publikus Internetre
- A támadás után egy héttel az „Anna-Senpai” nevet használó szerző nyilvánosságra hozta a Mirai forráskódját, ezzel szélesre tárva a kaput a hasonló támadások előtt (pl. https://github.com/jgamblin/Mirai-Source-Code)

Mirai botnet

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Mirai botnet

- Jó pár hónapos nyomozás után KerbsOnSecurity publikált egy cikket, amiben felfedte a Mirai botnet mögött álló személyeket
- https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author
- 3 évre visszamenőleg talált nyomokat hasonló IoT eszközöket felhasználó botnet támadásokra
- Minecraft szerverek ellen irányuló támadások vizsgálatából származik sok nyom. Ezeket a szervereket anyagi károkozás céljával támadják
- Több cég is szakosodott ezen szerverek DDoS elleni védelmére
- Az egyik ilyen cég tulajdonosára terelődött a gyanú…

Detektálás

- A szokásos hálózati forgalomnál lényegesen több a beérkező adatmennyiség/kérés
- A szolgáltatások lassúak, vagy nem elérhetőek
- IDS rendszerből érkező riasztások (titkosítás nehezíti)
- Netflow analízis

Védekezés

- Sok támadási forma miatt nincs egyszerű és egységes védelem
- Teljesen más védelmet kell használni mennyiségi és alkalmazás-specifikus támadások esetén
- Hogy történjen a beavatkozás? Automatikusan? Kézzel indítva?
- Költséges a védekezés
- Kimutatások szerint annak valószívűsége, hogy ha egyszer már célponttá váltunk, és újra megtörténik a támadás, több, mint 80%.

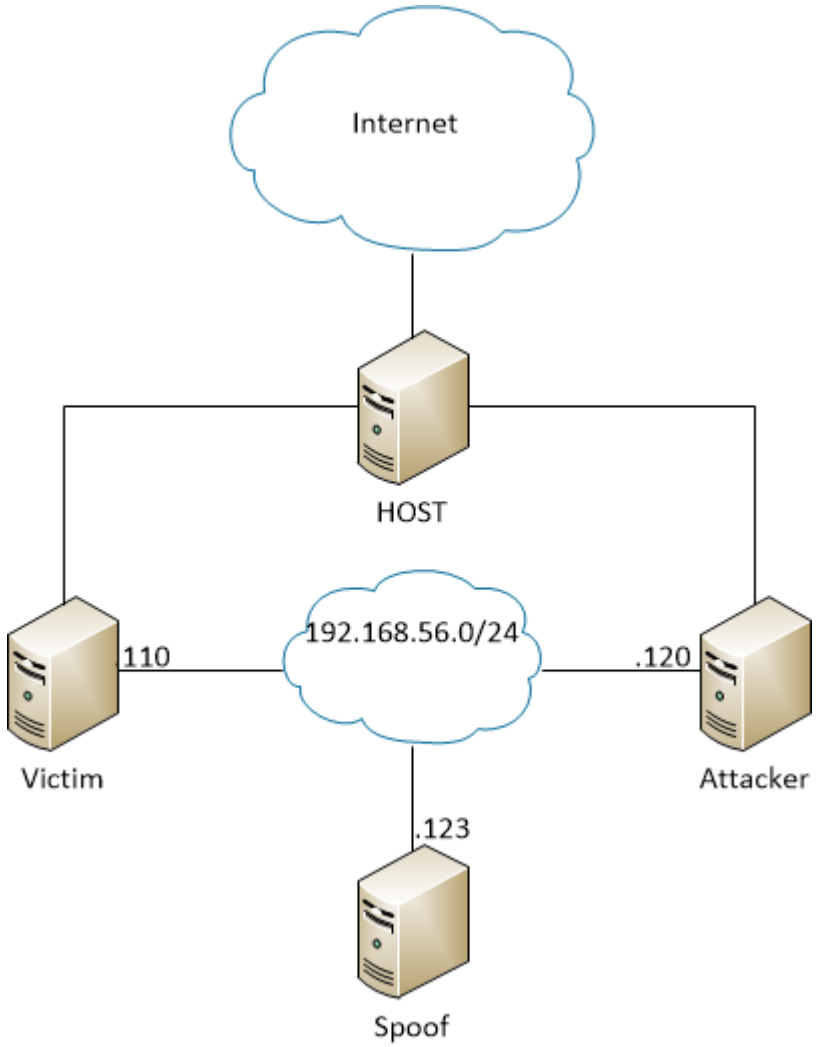
Védekezés - volumetric támadások

- Blackholing/sinkholing
  - ISP támogatás kell hozzá
  - Routing alapú
  - DNS alapú
- Cloud jellegű megoldások
  - Nagy kapacitású privát
  - Specifikus szoftverekkel, sok támadási vektor kezelése
  - Szolgáltatásként vásároljuk meg a DDoS védelmet.

Védekezés – Alkalmazás specifikus támadások

- A hagyományos L3/L4 tűzfal megoldások nem elegendőek
- WAF – Web Application Firewall
- Full proxy megoldások
  - SSL off-loading
  - DNS off-loading
- Hibrid megoldások (cloud + on-premise)

Demo topológia



Volumetric attack

- hping3 – SYN flood, spoofed source

```
hping3 -S -p 80  -c 5000 --spoof
192.168.56.123 192.168.56.120 –flood
```

- Hping3 – SYN flood, spoofed random source

```
hping3 -S -p 80  -c 5000 --rand-source
192.168.56.120
```

- Hping3 – UDP flood

```
hping3 --udp --data 1400 192.168.56.120
--flood
```

Slow HTTP POST/GET

- slowhttptest
  - Test mode:
  - -H: slow headers, a.k.a SlowLoris
  - -B: slow body, a.k.a R-U-Dead-Yet
  - -R: Range attack, a.k.a Apache killer
  - -X: Slow read

```
slowhttptest -H -u http://192.168.56.120 -i 10 -c 500
slowhttptest -B -u http://192.168.56.120 -i 10 -c 500
```

Kvíz

1. A „volumetric” támadást jellemzi, hogy
   a) Nagy mennyiségű forgalmat generál
   b) Nem generál forgalmat
   c) Csak ICMP protokollt használ
2. A mirai botnet által generált forgalom a KerbsOnSecurity ellen
   a) 10 Mbps
   b) 14 Tbps
   c) 620 Gbps
3. Az SSL forgalom DDoS detektálás szempontjából
   a) Jó dolog, megkönnyíti a detektálást
   b) A titkosítás miatt megnehezíti a detektálást
   c) Nem releváns