Amplification DDoS attacks with game servers
class Alejandronolla(Mandalorian):

    def __init__(self):
        self.name = 'Alejandro Nolla Blanco'
        self.nickname = 'z0mbiehunt3r'
        self.role = 'Threat Intelligence Analyst'
        self.interests = ['networking', 'python', 'offensive security']
        self.member_of = 'mlw.re'
What is an Amplification Attack?

The “bad guy” sends spoofed requests.

Intermediate servers “amplify” answers.

Victim gets flooded.

UDP as transport protocol.

Upper layers must properly control communication.
The “hacker without time” solution
“Gameserver status query libraries” for the win!

---

protocol: source
stimulus:
- `\xFF\xFF\xFF\xFF\xFF\xF56\x00\x00\x00\x00`
- `\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF` Source Engine Query\x00
Let's frag...
HAIL TO THE KING(s), BABY

<table>
<thead>
<tr>
<th>Game</th>
<th>Protocol</th>
<th>Amplification factor (max.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS Condition Zero</td>
<td>half-life</td>
<td>x109.8</td>
</tr>
<tr>
<td>f.e.a.r</td>
<td>gamespy</td>
<td>x107</td>
</tr>
<tr>
<td>quake-4</td>
<td>doom3</td>
<td>x88</td>
</tr>
<tr>
<td>CS Source</td>
<td>half-life</td>
<td>x83</td>
</tr>
</tbody>
</table>

Tested about 75 games, 67 vulnerable
Perceived really high amplification factors
THE ROOT OF ALL EVIL

Quake Engine

id Tech 2

id Tech 3

id Tech 4

GoldSrc

IW engine

ioquake3

Source Engine

Already vulnerable!

CVE-1999-1066

AMPLIFICATION DDOS WITH GAME SERVERS
AMPLIFICATION DDOS WITH GAME SERVERS

THE ROOT OF ALL EVIL

Quake Engine

id Tech 2

id Tech 3

id Tech 4

Quake

GoldSrc

IW engine

Source

Engine

ioquake3

Already vulnerable!
CVE-1999-1066

CALL OF DUTY

DOOM 3

ioquake3

GreHack
UNINTENDED SELF-FLOOD

# capinfos undisclosed_game.pcap

Number of packets: 817
Capture duration: 200 seconds
Data byte rate: 244 bytes/s
Data bit rate: 1958 bits/s
Average packet size: 59.99 bytes
Average packet rate: 4 packets/sec
UNINTENDED SELF-FLOOD

# capinfos undisclosed_game.pcap

Number of packets: 817
Capture duration: 200 seconds
Data byte rate: 244 bytes/s
Data bit rate: 1958 bits/s
Average packet size: 59,99 bytes
Average packet rate: 4 packets/sec

With just one request
CLOAKING A DDOS ATTACK

- Responses triggered to any payload, even to one byte
- "disconnect" flood
- Token flood

Be a genuine Predator
Collateral damage #01

if data_to_send > MTU:
    ip.flags = 0x01 # More Fragments
    ip.frag_offset = XX

Needs (exhaustive) reassembling!
if data_to_send > MTU:
    ip.flags = 0x01 # More Fragments
    ip.frag_offset = XX

Needs (exhaustive) reassembling!

Collateral damage #01

Collateral damage #02

“backscatter” effect

ICMP “port unreachable” responses

Adds more traffic...
Amplification DDOS with Game Servers

Amplification factor of x33,34
You bring the spoofed queries, Valve brings the servers

https://developer.valvesoftware.com/wiki/Master_Server_Query_Protocol
## FINDING SERVERS (THE EASY WAY)

<table>
<thead>
<tr>
<th>Game</th>
<th>Servers</th>
<th>Vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counter Strike 1.6</td>
<td>24,100</td>
<td>YES</td>
</tr>
<tr>
<td>Minecraft</td>
<td>9,692</td>
<td>YES</td>
</tr>
<tr>
<td>CS Global Offensive</td>
<td>9,079</td>
<td>YES</td>
</tr>
<tr>
<td>Team Fortress 2</td>
<td>8,136</td>
<td>YES</td>
</tr>
<tr>
<td>CS Source</td>
<td>7,531</td>
<td>YES</td>
</tr>
<tr>
<td>Call Of Duty 4</td>
<td>5,219</td>
<td>YES</td>
</tr>
<tr>
<td>Battlefield 3</td>
<td>4,241</td>
<td>NO</td>
</tr>
<tr>
<td>DayZ</td>
<td>4,216</td>
<td>YES</td>
</tr>
</tbody>
</table>

www.gametracker.com, games with most servers
FINDING SERVERS (THE RUDE WAY)

- One request per IP address to source protocol default port 27015 (in few hours...)
- 81,000 answers, 55,460 “looked like” source protocol
AMPLIFICATION DDOS WITH GAME SERVERS

MUTLIGATION NETWORK LAYER

MUST be mitigated at edge/upstream level

RTBH, uRPF, ACL, fw rules...

VICTIM

UPSTREAM #1

UPSTREAM #2
Easily detected by IDS/IPS/DPI rules

content: "\xff \xff \xff \xff \xff 73 74 61 74 75 73 52 65 73 70 6f 6e 73 73 65"; nocase; offset: 0; depth: 18;
MITIGATION NETWORK LAYER

Easily detected by IDS/IPS/DPI rules

c content: "\x00\x00\x00\x00\x00\x0073 74 61 74 75 73 52 65 73 70 6f 6e 73 74 65\n
statusResponse
AMPLIFICATION DDOS WITH GAME SERVERS

MITIGATION APP. LAYER

**IP requests throttling**
Less concurrent requests, more servers

**Limit source IP to actual gamers**
Can be still used against players

**Use challenge/response tokens**
Implemented in the proper way
CONCLUSIONS

- There are a lot of vulnerable servers

- Huge online gaming infrastructures also vulnerable

- Amplification attacks transition to game servers based?

- BCP 38, BCP84, uRPF, filtering, filtering and more filtering....
SOME LAST WORDS...

Valve didn’t worry too much (hey Valve, giving feedback doesn’t hurt...)

Spanish cert INTECO handled almost everything (thanks guys, you rock!)

Dozens vulnerabilities notified through US-CERT (thanks again, INTECO)
QUESTIONS?

Alejandro Nolla Blanco

twitter.com/z0mbiehunt3r

blog.alejandronolla.com

@ alejandro.nolla@gmail.com