Alejandro Nolla

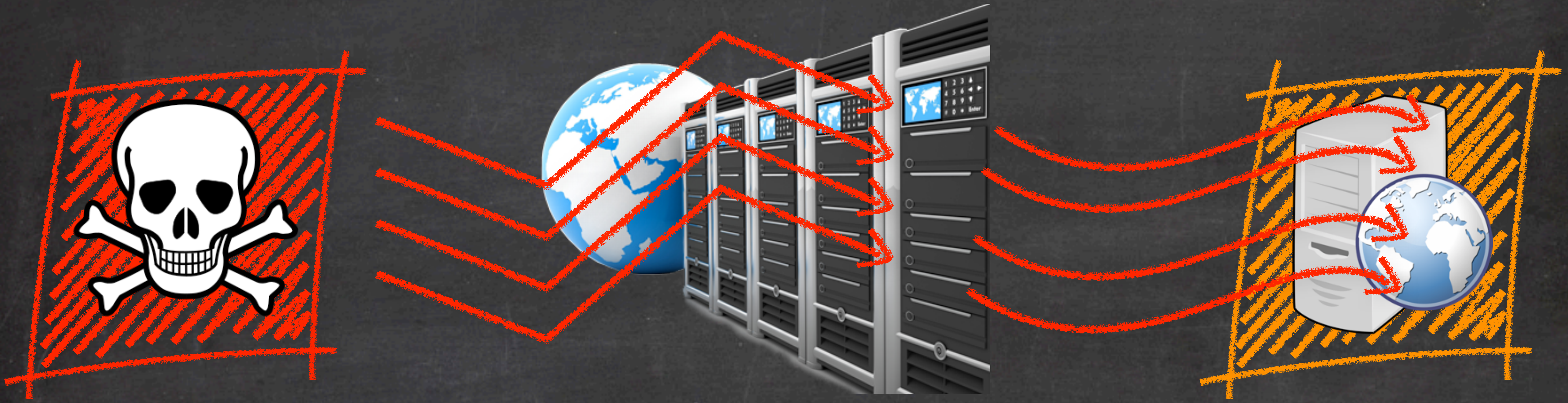
Amplification DDoS attacks with game servers

GreHack
2nd panick

```
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'
```

Hunting Malware
mlw.re Like a Sir

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

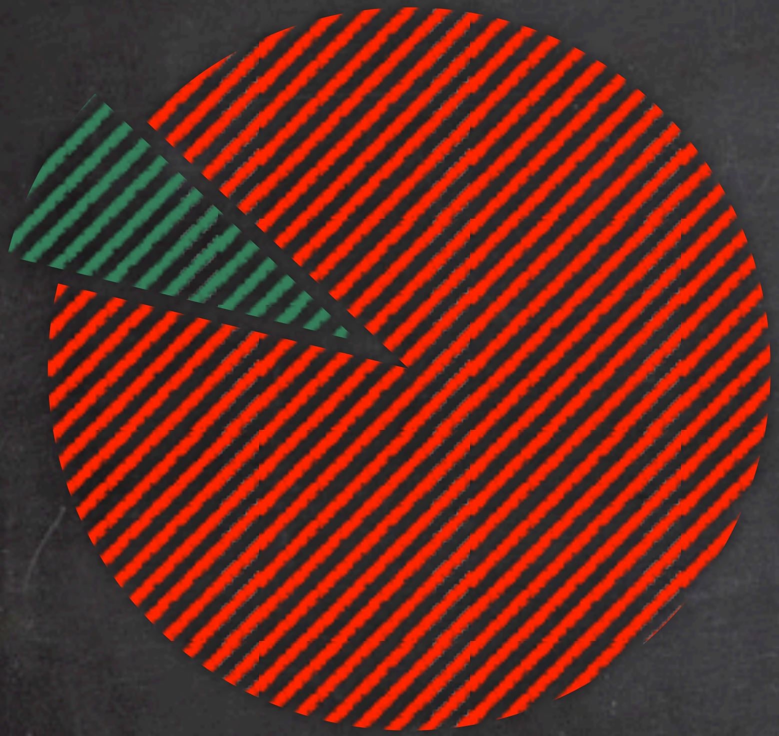
FUZZING THROUGH STIMULUS

- The "hacker without time" solution
- "Gameserver status query libraries" for the win!

```
---
protocol: source
stimulus:
  - \xFF\xFF\xFF\xFF\x56\x00\x00\x00\x00
  - \xFF\xFF\xFF\xFFTSource Engine Query\x00
```

Let's frag...

HAIL TO THE KING(s), BABY

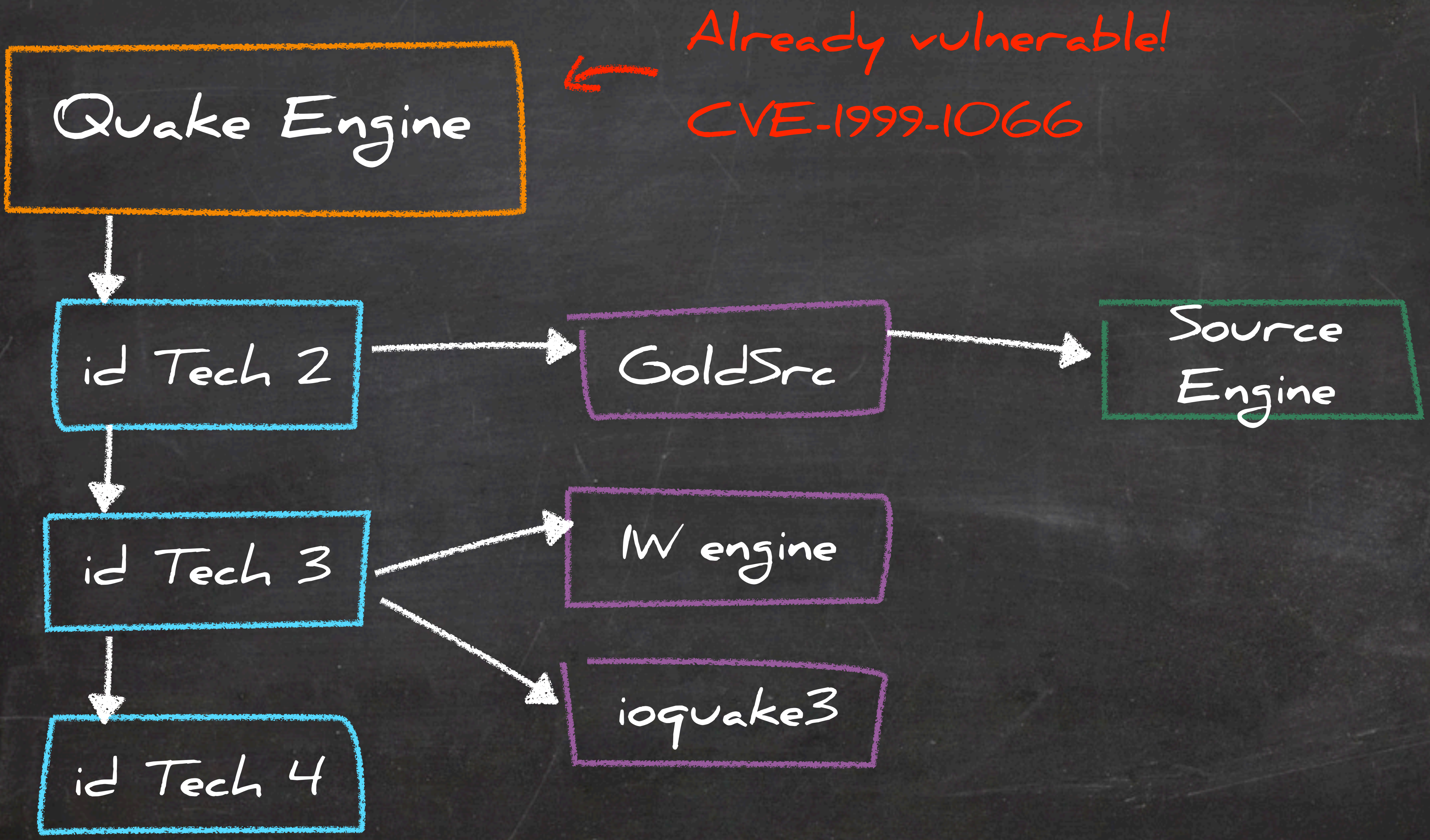


Game	Protocol	Amplification factor (max.)
CS Condition Zero	half-life	x109.8
f.e.a.r	gamespy	x107
quake-4	doom3	x88
CS Source	half-life	x83

Tested about 75 games, 67 vulnerable

Perceived really high amplification factors

THE ROOT OF ALL EVIL



Quake Engine

Already vulnerable!

CVE-1999-1066

id Tech 2

GoldSrc

Source Engine

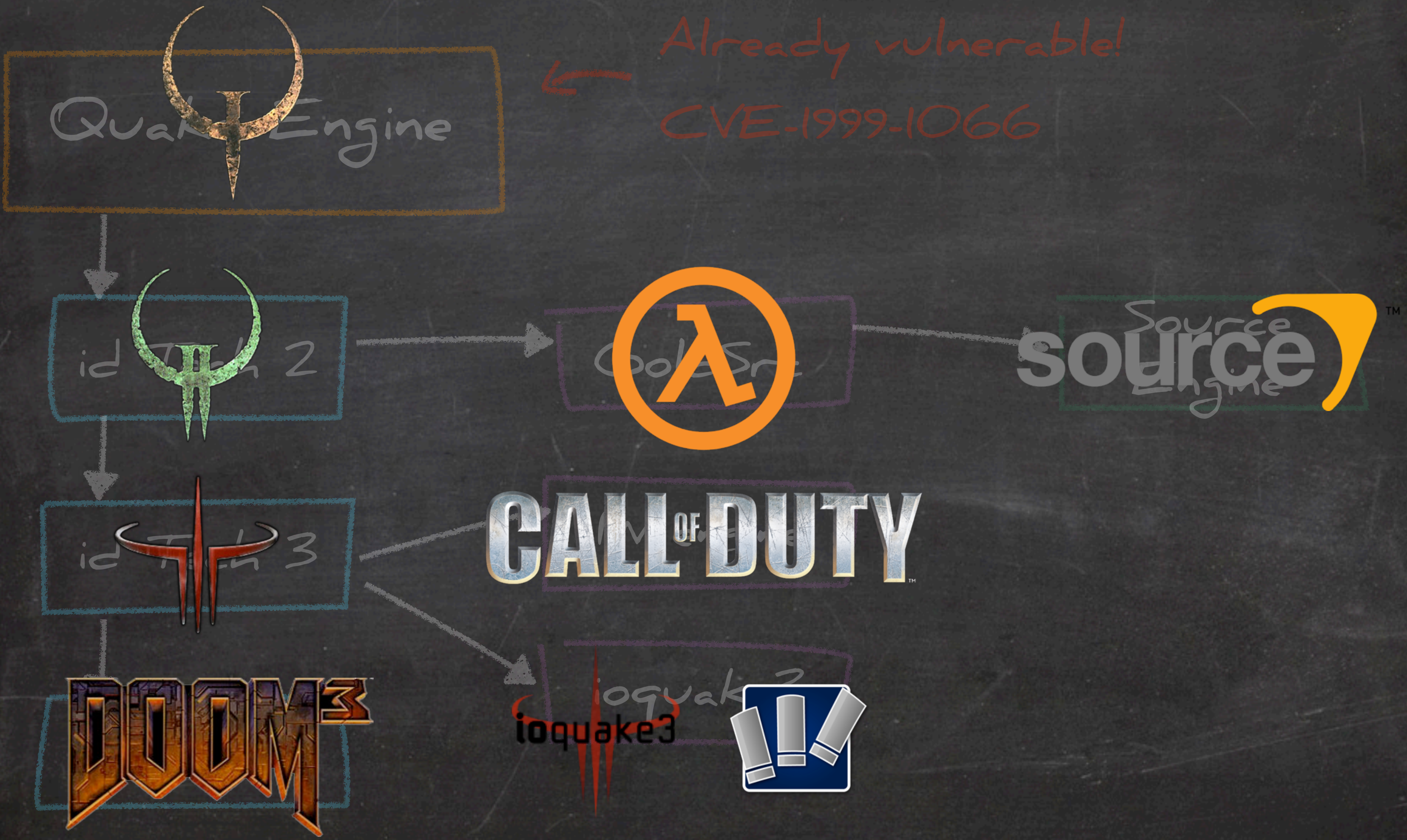
id Tech 3

IW engine

ioquake3

id Tech 4

THE ROOT OF ALL EVIL



Quake Engine

Already vulnerable!

CVE-1999-1066

id Tech 2

GoldSrc

Source Engine

id Tech 3

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

Be a genuine Predator

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

Collateral damage #01

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

Needs (exhaustive) reassembling!

Collateral damage #01

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

Needs (exhaustive) reassembling!

Collateral damage #02

"backscatter" effect

ICMP "port unreachable" responses

Adds more traffic...

ABUSING MASTER SERVER QUERY PROTOCOL

```
>>> r = sr1(IP(dst='hl1master.steampowered.com')/
        UDP(dport=27011)/Raw('\x31'))
>>> r.display()
###[ IP ]###
  [...]
###[ UDP ]###
     len= 1400
###[ Raw ]###
        load= '\xff\xff\xff\xff [...]'
```

https://developer.valvesoftware.com/wiki/Master_Server_Query_Protocol

ABUSING MASTER SERVER QUERY PROTOCOL

```
>>> r = sr1(IP(dst='hl1master.steampowered.com')/
        UDP(dport=27011)/Raw('\x31'))
>>> r.display()
###[ IP ]###
  [...]
###[ UDP ]###
  len= 1400
###[ Raw ]###
  load= '\xff\xff\xff\xff [...]'
```

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)

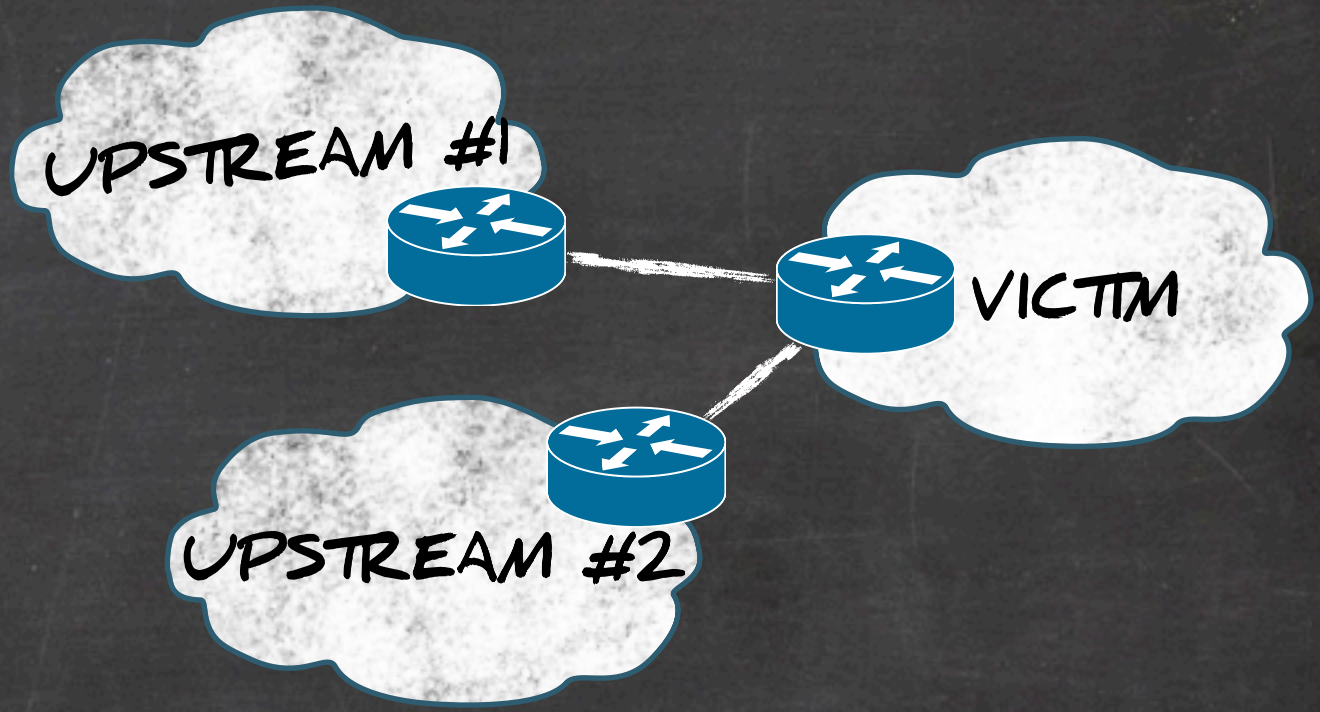
Game	Servers	Vulnerable
Counter Strike 1.6	24,100	YES
Minecraft	9,692	YES
CS Global Offensive	9,079	YES
Team Fortress 2	8,136	YES
CS Source	7,531	YES
Call Of Duty 4	5,219	YES
Battlefield 3	4,241	NO
DayZ	4,216	YES

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

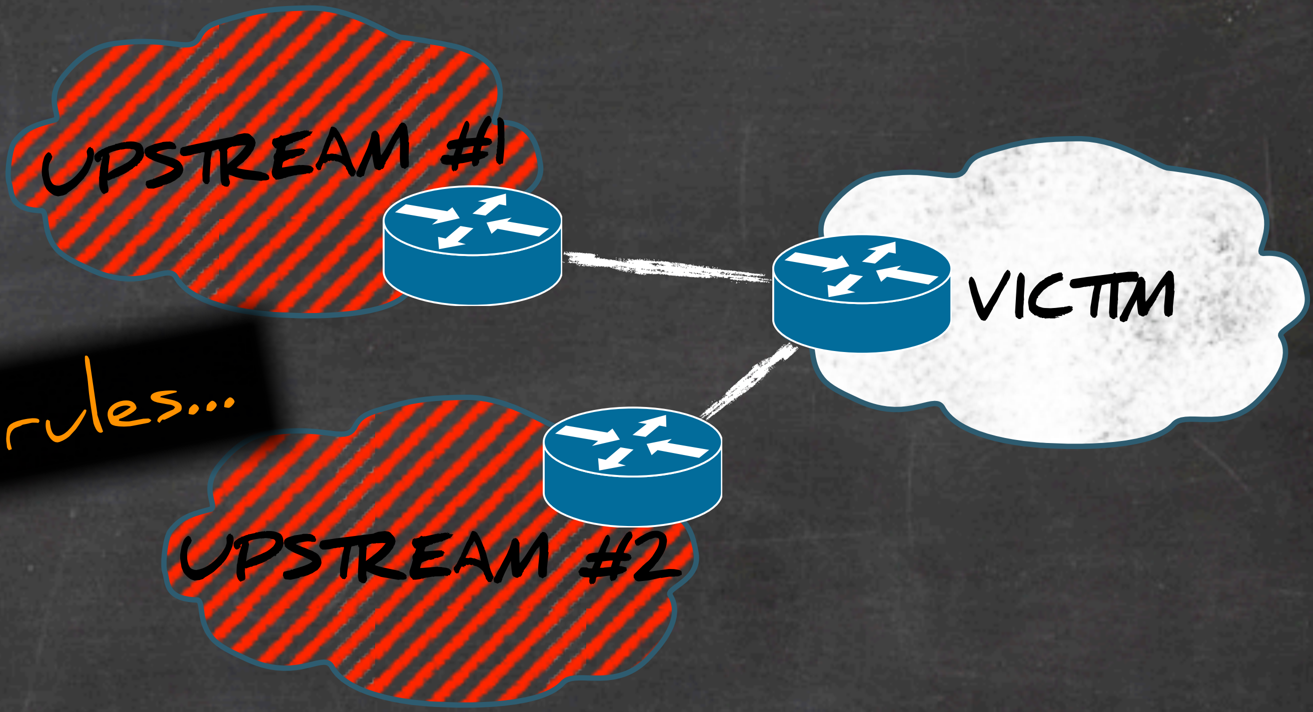
MITIGATION NETWORK LAYER



MITIGATION NETWORK LAYER

MUST be mitigated at edge/ upstream level

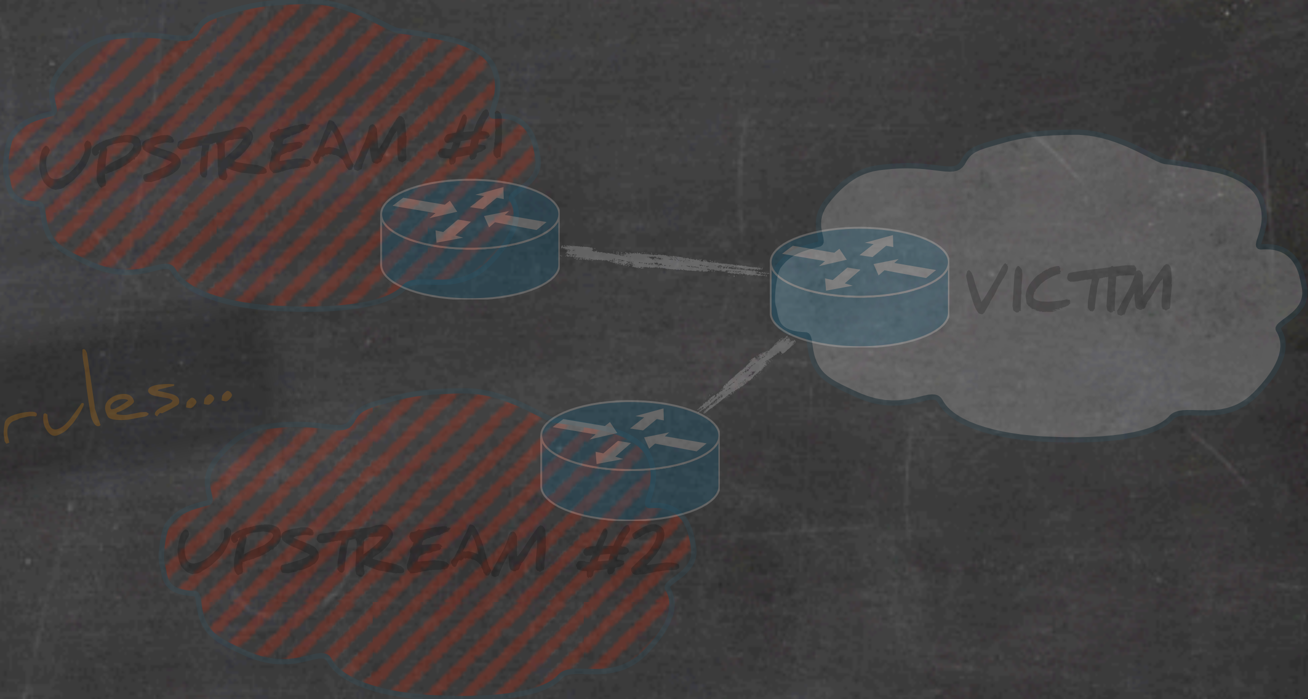
RTBH, uRPF, ACL, fw rules...



MITIGATION NETWORK LAYER

MUST be mitigated at edge/upstream level

RTBH, uRPF, ACL, fw rules...



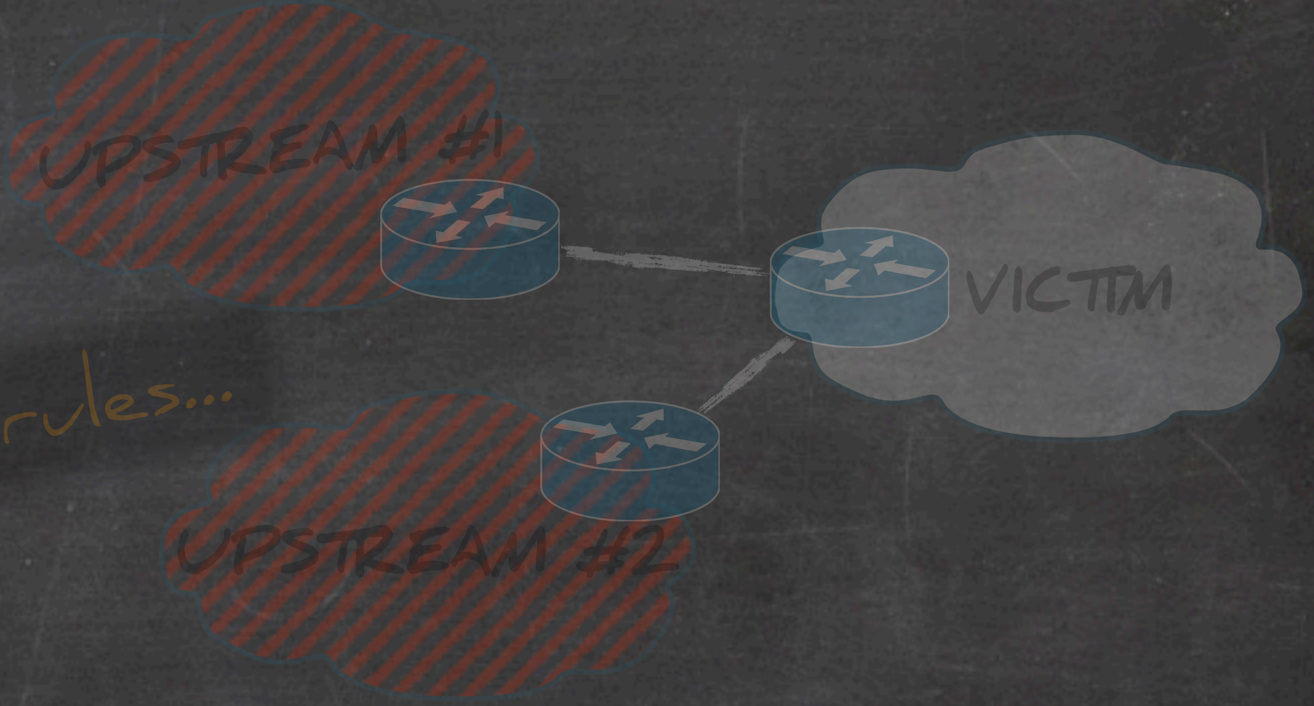
Easily detected by IDS/IPS/DPI rules

```
content:"|ff ff ff ff 73 74 61 74 75 73 52
65 73 70 6f 6e 73 65|"; nocase; offset:0;
depth:18;
```

MITIGATION NETWORK LAYER

MUST be mitigated at edge/upstream level

RTBH, uRPF, ACL, fw rules...



Easily detected by IDS/IPS/DPI rules

```
content:"|ff ff ff ff 73 74 61 74 75 73 52 65 73 70 6f 6e 73 65|"; nocase; offset:0; depth:18;
```

statusResponse

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/zØmbiehunt3r

blog.alejandronolla.com

@ alejandro.nolla@gmail.com