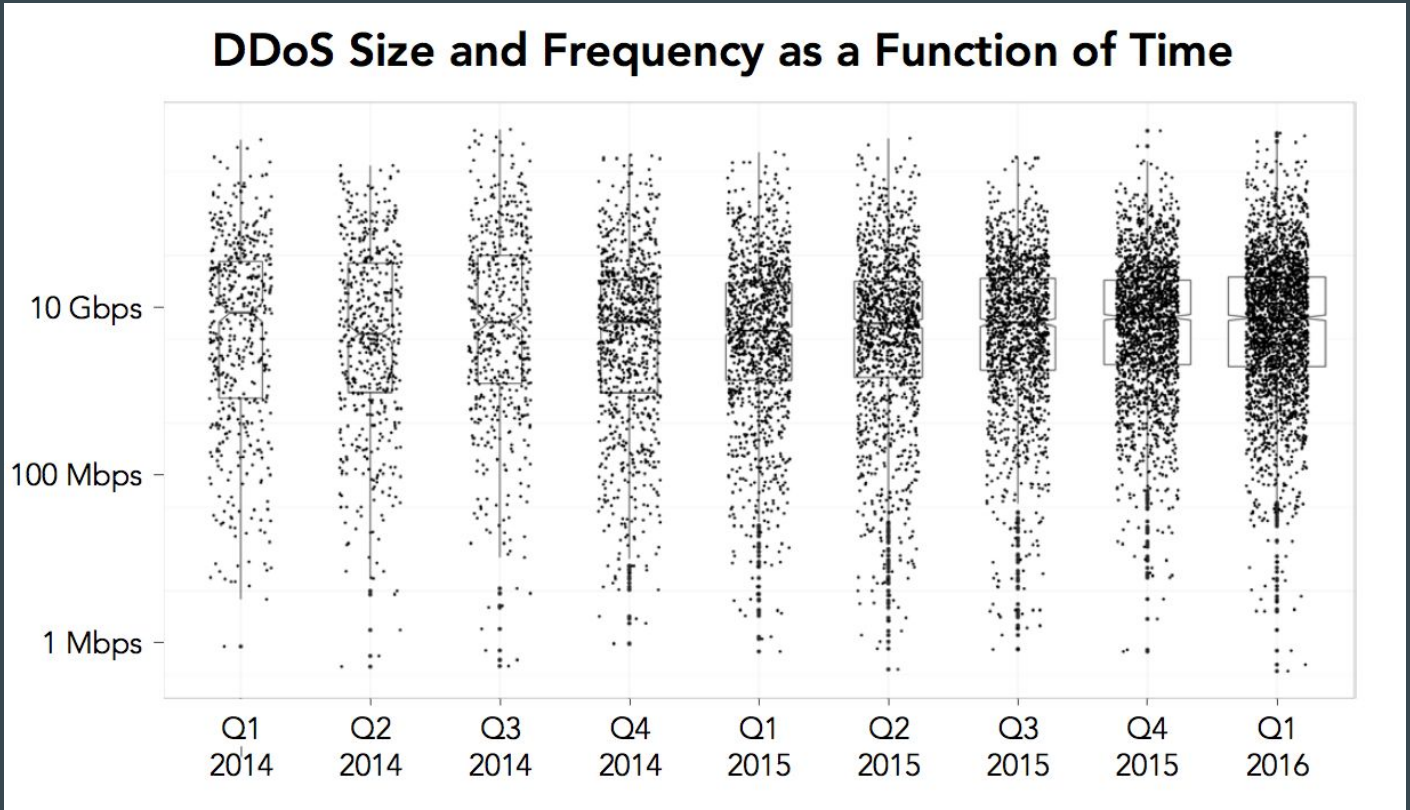
DDoS Attack Landscapes

Introduction

- ➔ General opinion AKA DDoS skeptics
- ➔ Denial of Service attacks are a fact of life on the Internet
- ➔ Service disruption
- ➔ Sometimes employed as a “smoke screen”
- ➔ What this talk is and what it is not
- ➔ Vendor independant

Trends visualization



Source: **Akamai's State of the Internet Report**

History

<1999 - SYN floods, Smurf Attack, Ping of death, first distributed attack tools ('fapi')
2000 - bundled with rootkits, first botnets controlled via ÍRC
2001 - First major attack involving DNS servers as reflectors
2002 - Attacks disrupted service at 9 of the 13 DNS root servers (also 2007 & 2015).
2003 - First DDoS mitigation services arise
2005 - 8 Gbps largest attack size
2009 - Iranian election protests
2012 - Operation Ababil
2014 - 400+ Gbps largest attack size
2015 - DD4BC emerge & The Great Canon of China
2016 - 600Gbps attack against BBC
2016 - MIT DDoS

Motivation

- Motives:
  - Revenge
  - Blackmail
  - Extortion
  - Hacktivism
  - business feud
  - leveling up
- Groups
  - Anonymous
  - Lizard Squad
  - DD4BC
  - Armada Collective
  - New World Hacking
  - ...

Hello,

To introduce ourselves first:
http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks
http://bitcoinbountyhunter.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-ex-coin-theft-owner-accuses-ccedk-of-withholding-info
Or just google "DD4BC" and you will find more info.

So, it's your turn! All servers of [REDACTED] group (internationally) are going under DDoS attack unless you pay 40 Bitcoin. Pay to 16HH1Se5zhXgqe4EBAKZxdyMump5Mi-YgrQ Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps. Right now we are running small demonstrative attack on one of your IPs: [REDACTED]. Don't worry, it will not be hard (we will try not to crash it at the moment) and will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 40 BTC at the moment, so we are giving you 24 hours to get it and pay us. Find the best exchanger for you on howtobuybitcoins.info or localbitcoins.com You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet. Current price of 1 BTC is about 250 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 40 BTC to 16HH1Se5zhXgqe4EBAKZxdyMump5MiYgrQ — we will know it's you and you will never hear from us again.
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated.

If you need to contact us, use Bitmessage: BM NC1jRewNdHxX3jHrufjxDsRWXGdNisY5 But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 100 BTC and will keep increasing for every hour of attack. Many of our "clients" believe that if they pay us once, we will be back. That's not how we work - we never attack the same target after we are paid. If you are thinking about reporting this to authorities, feel free to try. But it won't help. We are not amateurs.

REMEMBER THIS: It's a one-time payment. Pay and you will not hear from us ever again!
We do bad things, but we keep our word.
Thank you

Mechanisms

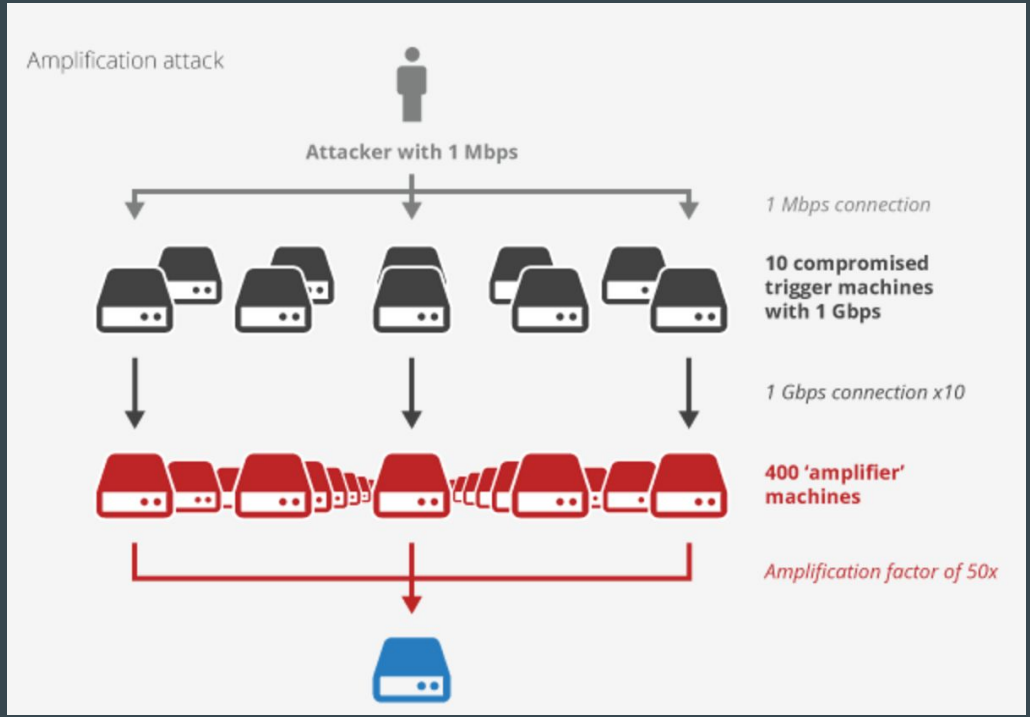
- ➔ why are DDoS attacks possible?
- ➔ volumetric attacks vs resource starvation
- ➔ infrastructure vs application attacks
- ➔ attacker bandwidth > victim bandwidth
- ➔ bps vs pps, packet storms
- ➔ stealth/creeper
- ➔ scouting & recruitment
- ➔ botnet spawned by malware

Infrastructure DDoS

- ➔ ACK, RST, FIN , PSH, URG (Out-of-state floods)
- ➔ XMAS, TCP anomaly
- ➔ SYN
- ➔ CHARGEN
- ➔ DNS
- ➔ ICMP
- ➔ RIP
- ➔ SSDP
- ➔ NTP
- ➔ UDP (FRAGMENTS)

UDP-based Amplification

- ip address spoofing
- Fire & Forget
- DNS Reflection is so 2014
- NTP amplification
  as easy as (UDP port) 123
- UDP Fragments
- Vulnerable services
  - MON_GETLIST
  - Open resolvers



Source: **blog.cloudflare.com**

Amplification factor

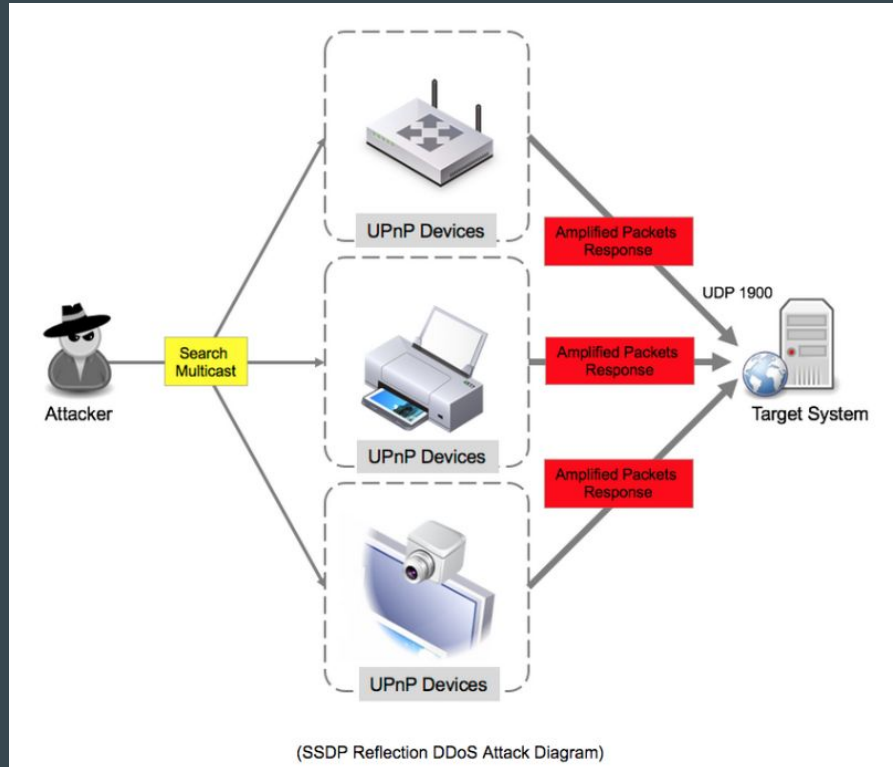
- ➔ DNS - 28 to 54x
- ➔ NTP - 556.9x
- ➔ SSDP - 30.8x
- ➔ CharGen - 358.8x
- ➔ RIPv1 - 131.24x

```
freya:ntp tuna$ ntpdc -c monlist 10.1.10.128
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
10.1.10.30           59986 10.1.10.128           18 7 2      0    128       0
nist1-sj.ustiming.org  123 10.1.10.128           18 4 4      0     76      24
nist1-la.ustiming.org  123 10.1.10.128           18 4 4      0     80      27
time-b.timefreq.bldrdo 123 10.1.10.128           19 4 4      0     65      36
198.60.73.8            123 10.1.10.128           20 4 4      0     64      37
time-a.timefreq.bldrdo 123 10.1.10.128           20 4 4      0     64      38
nist.netservicesgroup. 123 10.1.10.128           20 4 4      0     64      41
time-d.nist.gov        123 10.1.10.128           19 4 4      0     65      41
207_223_123_18.colo.te 123 10.1.10.128           20 4 4      0     64      44
india.colorado.edu     123 10.1.10.128           20 4 4      0     63      45
nist1-lnk.binary.net   123 10.1.10.128           20 4 4      0     64      47
nist01.ntp.aol.com     123 10.1.10.128           20 4 4      0     64      47
nist.time.stabletransi 123 10.1.10.128           20 4 4      0     64      48
64.250.177.145         123 10.1.10.128           20 4 4      0     64      48
time-b.nist.gov        123 10.1.10.128           20 4 4      0     64      48
nist-time-server.eoni. 123 10.1.10.128
64.90.182.55           123 10.1.10.128
ntp.sunflower.com      123 10.1.10.128
nist1-nj2.ustiming.org 123 10.1.10.128
barricade.rack911.com  123 10.1.10.128
nist-nj.ustiming.org   123 10.1.10.128
time-a.nist.gov        123 10.1.10.128
tds-solutions.net      123 10.1.10.128
nist1.symmetricom.com  123 10.1.10.128
131.107.13.100         123 10.1.10.128
utcnist2.colorado.edu  123 10.1.10.128
206.246.122.250.tdm.nn 123 10.1.10.128
time-c.timefreq.bldrdo 123 10.1.10.128
nist1-lv.ustiming.org  123 10.1.10.128
nisttime.carsoncity.k1 123 10.1.10.128
50-77-217-185-static.h 123 10.1.10.128
host-24-56-178-140.bey 123 10.1.10.128
```

```
5  import socket
6  # Set up a UDP socket
7  s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
8  # send
9  #17 00 03 2a
10 MSG = str('\x17\x00\x03\x2a') + str('\x00')*4
11 HOSTNAME = '10.1.10.128'
12 PORTNO = 123
13 s.connect((HOSTNAME, PORTNO))
14 if len(MSG) != s.send(MSG):
15     # where to get error message "$!".
16     print "cannot send to %s(%d):" % (HOSTNAME,PORTNO)
17     raise SystemExit(1)
18 MAXLEN = 4098
19 (data,addr) = s.recvfrom(MAXLEN)
20 s.close()
21 print '%s(%d) said "%s"' % (addr[0],addr[1], data)
```

SSDP Flood

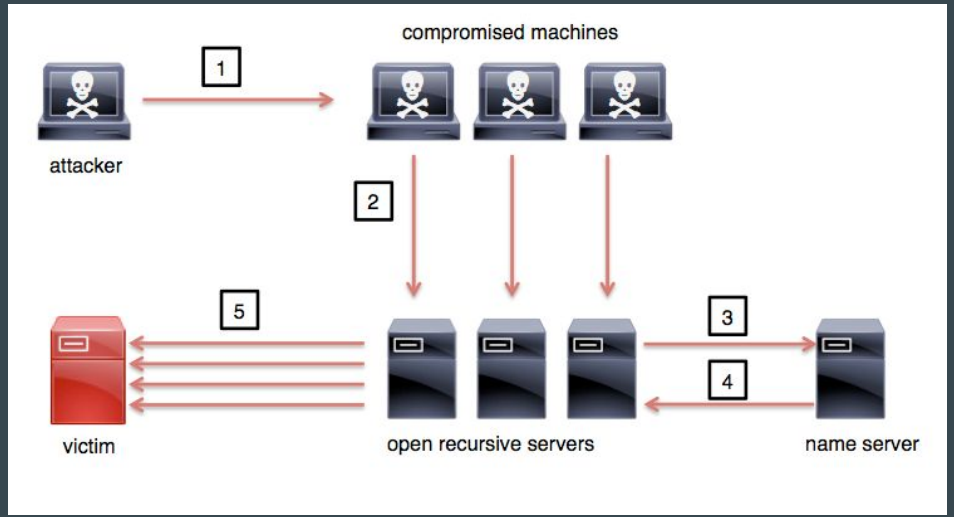
```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age = 120
LOCATION: http://192.168.1.1:80/UPnP/IGD.xml
ST: urn:schemas-upnp-org:service:WANIPConnection:1
SERVER: System/1.0 UPnP/1.0 IGD/1.0
USN: uuid:WANConnection{9679d566-230a-49d3-92e5-421e9223eaef}
000000000000::urn:schemas-upnp-org:service:WANIPConnection:1

HTTP/1.1 200 OK
Cache-Control: max-age=120
Location: http://192.168.0.1:65535/rootDesc.xml
Server: Linux/2.4.22-1.2115.nptl UPnP/1.0 miniupnpd/1.0
ST: urn:schemas-upnp-org:device:InternetGatewayDevice:
USN: uuid:b1c5d60c-1dd1-11b2-8687-a0bc8f76d644:
:urn:schemas-upnp-org:device:InternetGatewayDevice:
```



(SSDP Reflection DDoS Attack Diagram)

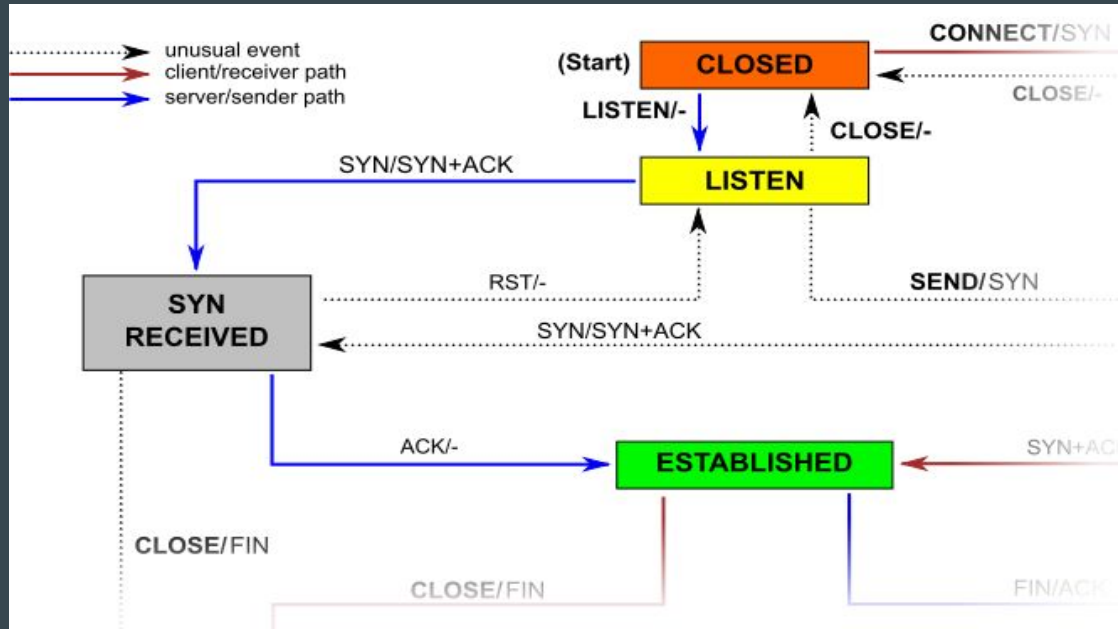
DNS reflection flood

```
04:17:11.736254 IP x.x.x.x.53 > x.x.x.x6007: 45488| 22/0/0 DNSKEY, AAAA 2600:803:240::2, A 63.74.109.2, TXT "v=spf1
ip4:63.74.109.6 ip4:x.x.x.x ip4:x.x.x.x mx a:HIDDEN
04:17:11.736257 IP x.x.x.x.53 > x.x.x.x.30267: 4354 2/2/0 NS HIDDEN . (105)
04:17:11.736276 IP x.x.x.x.53 > x.x.x.x7519: 45488| 22/0/0 Type51, RRSIG, DNSKEY, DNSKEY, DNSKEY, DNSKEY[|domain]
04:17:11.736287 IP x.x.x.x.53 > x.x.x.x.44609: 4354| 22/0/0 RRSIG, A 63.74.109.2, TXT "v=spf1
04:20:08.919421 IP x.x.x.x.53 > x.x.x.x.51286: 52156
  13/4/2 SPF, DNSKEY, DNSKEY, NAPTR, TXT "v=spf1 a mx
  ip4:x.x.x.x/21
  ip4:x.x.x.x/16 ip6:2001:04F8::0/32
  ip6:xxx:xxx:xx::xx/128 ~all", HIDDEN
```



TCP-based attacks

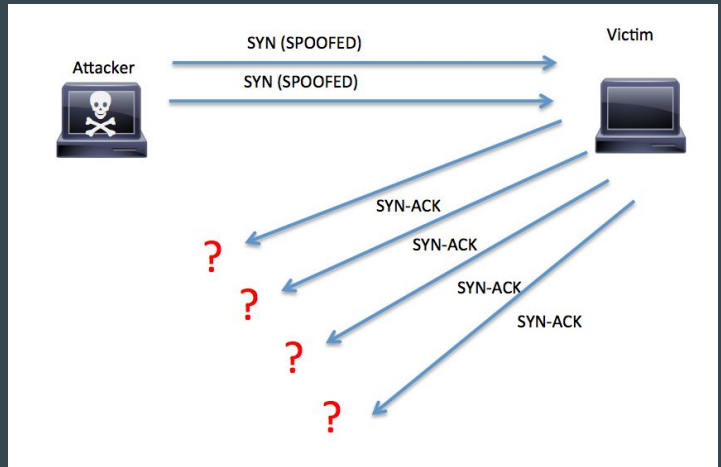
- ➔ SYN Floods
- ➔ Out-Of-State Floods
- ➔ Rainbow/Xmas Floods
- ➔ TCP Anomaly
- ➔ TCB



SYN / Rainbow floods

SYN Flood

```
21:59:49.851423 IP X.X.X.X.33465 > Y.Y.Y.Y.80: Flags [S],
seq 72209530
, win 14600,options [mss 1460,sackOK,TS val 1428345032
ecr 0,nop,wscale 3], len
gth 0
21:59:49.854397 IP184.25.56.134.44560 >
178.132.241.16.80: Flags [S], seq 19937
82773, win 14600, options [mss1460,sackOK,TS val
1530530357 ecr 0,nop,wscale 3]
, length 0
```



Rainbow flood

```
01:49:36.107817 IP X.X.X.X.45240 >
Y.Y.Y.Y.80:Flags [SRP.UW], seq
2733393585, ack 0, win 28679, urg 0, length 0
```

TCP Header

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number (if ACK set)																															
96	Data offset				Reserved				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer (if URG set)															
160 …	Options (if Data Offset > 5) …																													padding		

Application layer attacks

- ➔ Basic HTTP Floods
- ➔ Randomized HTTP Floods
- ➔ Cache-bypass HTTP Floods
- ➔ GET Floods
- ➔ POST Floods
- ➔ Slow Post
- ➔ HTTPS floods
- ➔ SSL handshake / renegotiation attacks

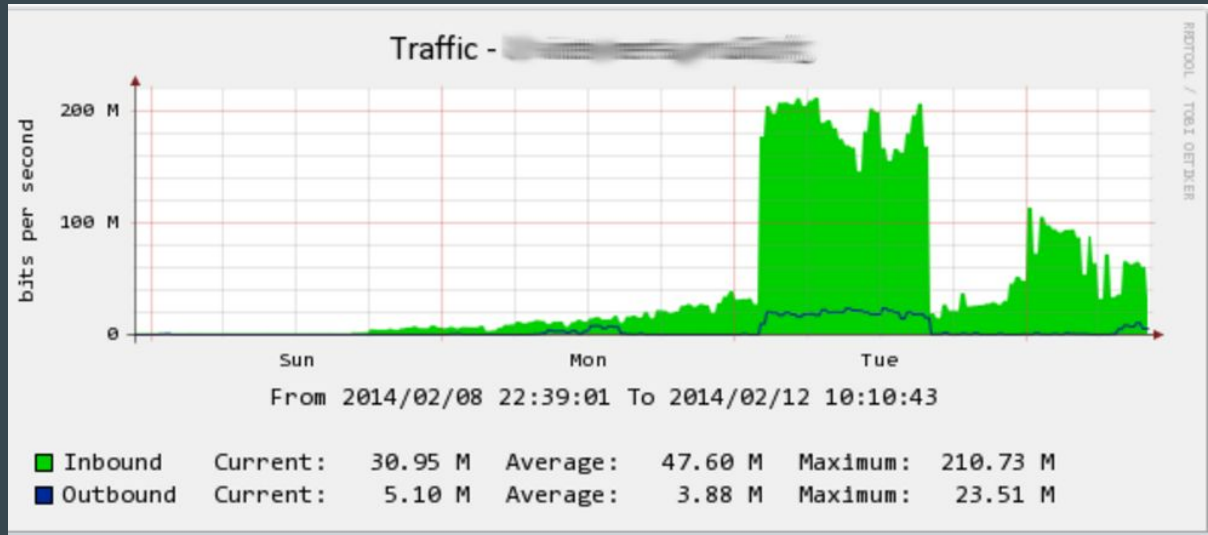
HTTP GET/POST Floods

GET Flood

```
10:49:23.674001 IP X.X.X.X.58126 > Y.Y.Y.Y.80: Flags [P.], seq 0:28
0, ack 1, win14600, length 280
....E..@..@.6..l@...r.I....P*.8..q+.P.9.....GET / HTTP/1.1
Accept:*/*
Referer: http://www.victim.com/
Accept-Language: zh-cn
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)
Host:www.victim.com
Pragma: no-cache
cache-control: private, max-age=0, no-cache
Connection:keep-alive
```

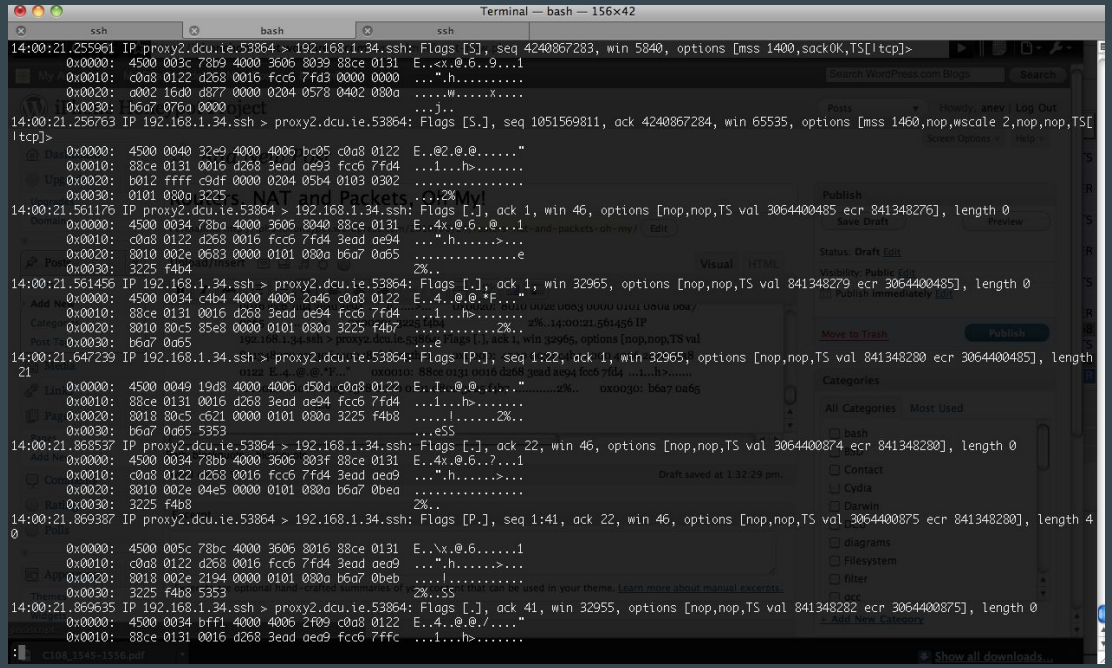
Detection

- ➔ Know your RFCs
- ➔ False positives vs. False negatives
- ➔ Anomaly detection (delta calculation)
- ➔ Appliances
- ➔ Graphs/Flow
- ➔ Into the hex
- ➔ Keen eye



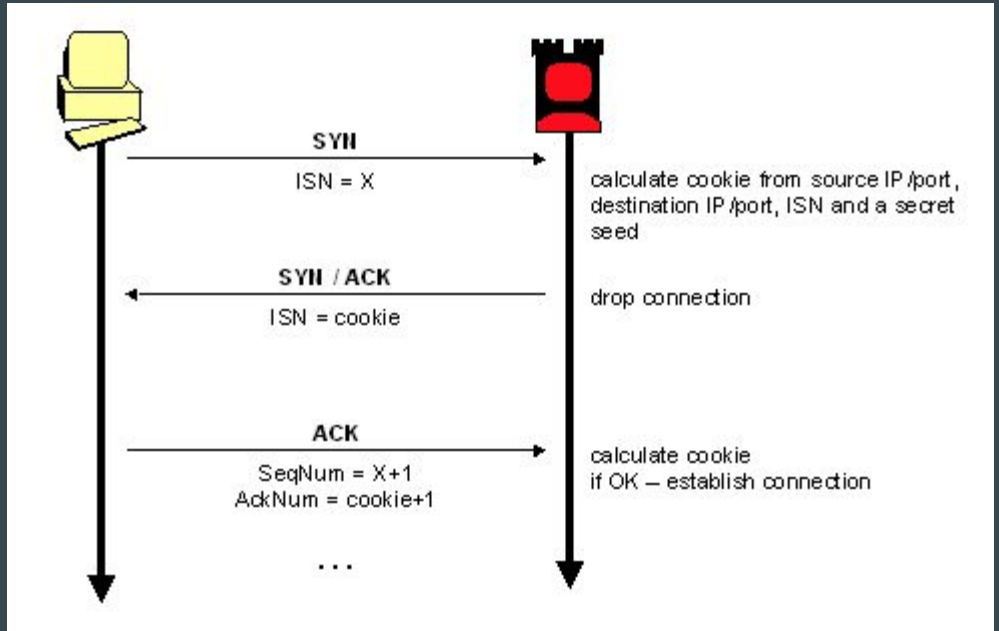
Packet forensics

```
21:28:09.101512 IP X.X.X.X.3478 >
Y.Y.Y.Y.80: Flags [S], seq 8420, win
21012, options [mss 729,nop,wscale
8,nop,nop,sackOK], length 0

21:28:09.101517 IP X.X.X.X.4041 >
Y.Y.Y.Y.80: Flags [S], seq
1612447744:1612447752, win 59258,
options [mss 19970,nop,eol], length 8
```



Mitigation Techniques

- ➔ Rate limiting
- ➔ ACLs (deny tcp any any match-all +rst)
- ➔ Blackholing
- ➔ Source Based NULL routing
- ➔ Stateful inspection devices
- ➔ SYN Cookies
- ➔ Signature Matching
- ➔ WAF
- ➔ Header Order
- ➔ DNS Truncated bit
- ➔ Network Ingress Filtering

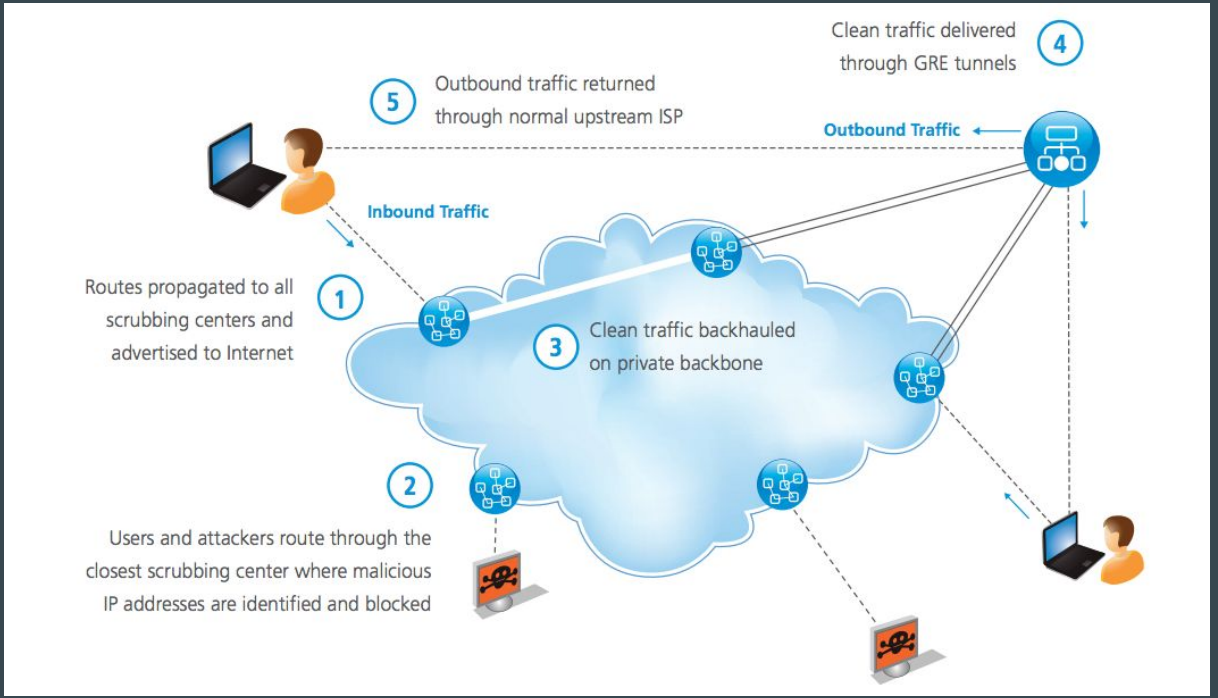


On-Premise vs Cloud vs Hybrid

- ➔ Saturation
- ➔ SSL Based attacks
- ➔ Layer 7 Floods
- ➔ Response time
- ➔ Always on mitigation
- ➔ Traffic divertment
- ➔ Tune your machines

Cloud DDoS Solutions

- ➔ Distributed attacks require a distributed defense
- ➔ Industry SLA
- ➔ 24/7 SOCs
- ➔ Routes announced via BGP
- ➔ Leverages Anycast
- ➔ Tbps of dedicated attack capacity
- ➔ SSL?
- ➔ Threat intelligence



Thank you for listening!

Questions ?