



# UNDERSTANDING & MITIGATING LARGE SCALE DoS ATTACKS

TROOPERS 2013 @ HEIDELBERG

ADEM SEN

SENIZER@GMAIL.COM

TWITTER: @SECURITYFREAX

# AGENDA



➔ PROLOGUE

➔ EVOLUTION OF DDoS

➔ ATTACK TYPES & TOOLS

➔ MITIGATE & RESPOND

➔ DDoS MYTHBUSTING

➔ EARLY WARNINGS

➔ APPENDIX: USEFUL RESOURCES

# Me and myself

- ➔ Graduation in Software Engineering, > 10 years experience in #INFOSEC
- ➔ 09 - present: Network Security Expert@DB System
- ➔ Security-obsessed whitehat, focused on network defense techniques
- ➔ Blood group: "coca cola - positive"
- ➔ Hunting botnets for fun and research purposes, and sometimes for beer & pizza :-)
- ➔ **No sponsor! Comments are welcome during talk!**

## || For the record...

- ➔ Statements do reflect my very own experiences, some may find consent others may not, you're welcome!
- ➔ Statements on Firewalls & IPS may result in #VENDOR PANIC



- ➔ Opinions are mine and do not represent those of my employer

# || Scope and Prerequisites

- ➔ I assume that everybody is familiar with TCP/IP networking, we won't cover it here
- ➔ "Mitigate & Respond" will be covered from a large enterprise's perspective running its own AS with wide range of dynamic websites
- ➔ Due to time given we will focus on major types of attacks and countermeasures
  - ➔ Intentionally skipping SIP / H.323 based attacks and countermeasures, probably in future talks
  - ➔ Skipping DNS / Domain and BGP hijacking
- ➔ OK, let's get started...! :-)



# EVOLUTION OF DDoS

# || Evolution of DDoS - good old...

- ➔ D(DoS) == nothing new at all, but underestimated
- ➔ Covered in various early IETF papers e.g. RFC 2267 / 2827
- ➔ First (usable) attack tools appeared in the 90's
  - ➔ (e.g. Teardrop and LAND)

Network Working Group  
Request for Comments: 2827  
Obsoletes: [2267](#)  
BCP: 38  
Category: Best Current Practice

P. Ferguson  
Cisco Systems, Inc.  
D. Senie  
Amaranth Networks Inc.  
May 2000

**Network Ingress Filtering:  
Defeating Denial of Service Attacks which employ  
IP Source Address Spoofing**

# || Evolution of DDoS - the 90's

- ➔ Early attacks (as in 1996) simply targeted weaknesses in TCP/IP implementations
  - ➔ CA-1996-21 TCP SYN Flooding
- ➔ Simple packet throwing code, **but still working!**
- ➔ No reliable command and control (C2) structures
- ➔ Low powered attacks & far away from app-layer
- ➔ (D)DoS == considered as a „side issue“ than as a serious threat



# || Evolution of DDoS - a rude awakening

- ➔ Significant growth of worldwide network traffic
- ➔ **Most** ISPs missed to implement mitigation techniques
  - ➔ Best practices not implemented
  - ➔ ISPs don't prevent IP spoofing
  - ➔ [...]
- ➔ No „signaling“ between ISPs, no global / regional network visibility
- ➔ Industry still playing reactive
  - ➔ Security tech in place fails to combat DDoS
  - ➔ Lack of knowledge / #INFOSEC resources in #COMPANY

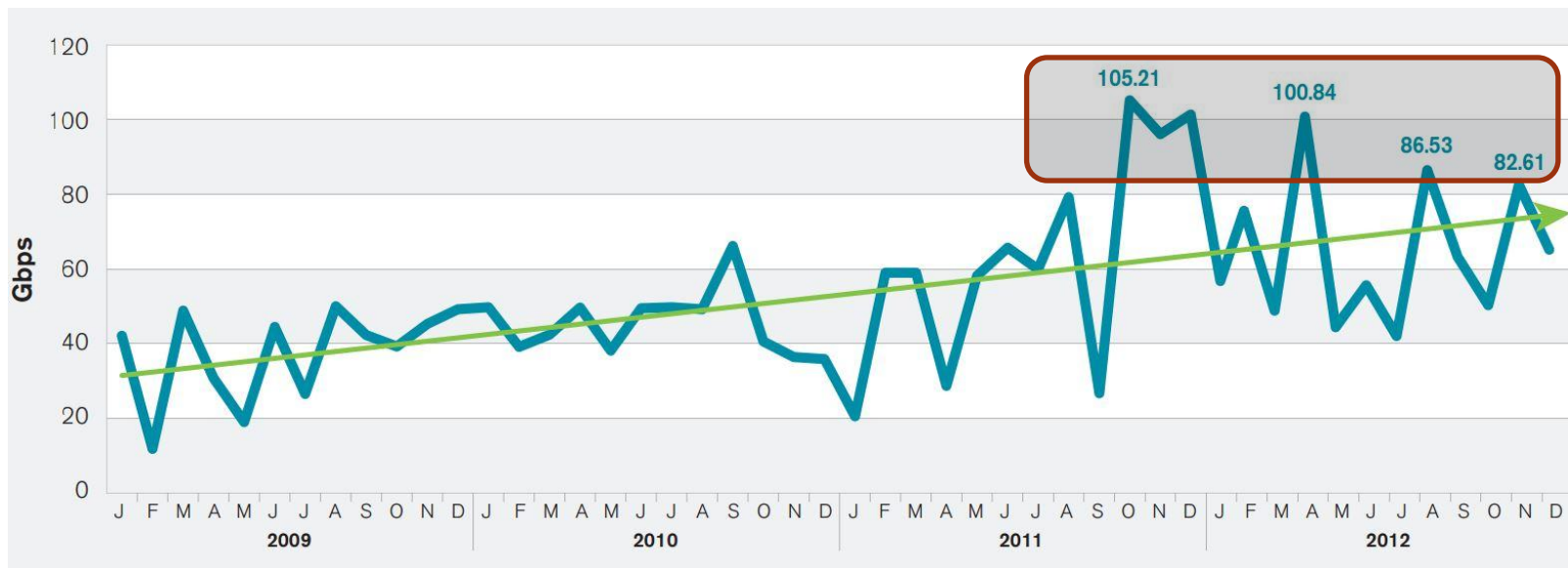


# || Evolution of DDoS - game has changed

- ➡ Hacktivists entered the game after Wikileaks disaster
- ➡ Sophisticated #BOTNETs appeared w/ command & control structures - utilizing hundreds of thousands of victims
- ➡ Significant increase of DDoS attacks
- ➡ **Today :: DDoS has become Mainstream!**

# Evolution of DDoS - attack sizes

- ➡ DDoS attack sizes are increasing continuously
- ➡ Monitored 100+ Gbps DDoS (max.)<sup>1</sup>
- ➡ Average attack size ~ 2 Gbps



# || Evolution of DDoS - Motivation & Threats

## ➤ MOST COMMON THREATS

- 1 - Attacks towards customer services at datacenters
- 2 - Infrastructure attacks (Firewalls, Load balancer) & Services (DNS, Mail)
- 3 - Misconfiguration (WTF!)

## ➤ MOTIVATION

- 1 - Political & Ideology
- 2 - Online Gaming related (yes, seriously!)
- 3 - Vandalism





**ENOUGH BACKGROUND? LET'S DIVE IN....!**





# ATTACK TYPES

# Attack types - introducing the big 4

## ➔ Application Layer Attacks

- ➔ Exhausting system resources, e.g. CPU, memory & sockets
- ➔ HTTP GET/POST flooding is leading this category
- ➔ SlowHTTP attacks belong also to this category
- ➔ Trend: increasing

## ➔ Protocol State Attacks

- ➔ Exhausting state tables of network devices, e.g. firewalls & load balancers
- ➔ Remember: App server are statefull too, due to TCP state machine
- ➔ TCP SYN / RST flooding is leading this category
- ➔ Trend: increasing

# Attack types - introducing the big 4

## ➔ Volumetric Attacks

- ➔ Exhausting network bandwidth resources
- ➔ HTTP(S) & DNS leading this category
- ➔ Expensive to engage, other vectors preferred
- ➔ Trend: constant

## ➔ Multi-Vector attacks == more sophisticated

- ➔ Using a **blend** of attack vectors
  - ➔ HTTP(S), DNS, TCP, UDP, ICMP [..]
- ➔ Utilizing compromised web[servers] at hosting facilities to gain more power
- ➔ **Trend: increasing & difficult to mitigate!**



# Attack types - tools

## ➔ Well known tools

- ➔ LOIC / HOIC and other boring „press F5“ tools
- ➔ Slowloris.pl
- ➔ Apache killer / Nkiller2
- ➔ PHP / JavaScript [...] based attack routines
- ➔ ...any many other tools / scripts

## ➔ Usage of benchmark / diag tools

- ➔ ab - apache bench
- ➔ Jmeter
- ➔ Hping (powerful!)

## ➔ **Most tools invoke same vectors**

- ➔ HTTP request flooding
- ➔ TCP / UDP / ICMP flooding
- ➔ NOT exploiting vulnerabilities

# Attack types - die hard....

- ➔ Hping: easy to use but powerful at packet flooding
- ➔ Generating ~ 140.000 packets per second (pps) by single „VM“ in the cloud
- ➔ Be careful while playing with hping in the cloud - you've been warned! :-)

## ➔ TCP SYN flooding w/ & w/o spoofing

- ➔ 

```
hping3 -S -p 80 --flood -rand-source --tcp-mss 1460 -L syn [IP]
```
- ➔ 

```
hping3 -S -p 80 --flood --tcp-mss 1460 -L syn [IP]
```

# Attack types - die hard...

```
root@ma22290:/home/adem#  
root@ma22290:/home/adem#  
root@ma22290:/home/adem#  
root@ma22290:/home/adem#  
root@ma22290:/home/adem#  
root@ma22290:/home/adem# hping3 -S -p 80 --rand-source --flood --tcp-mss 1460 -L syn [redacted].202.104  
HPING [redacted].202.104 (eth0 [redacted].202.104): S set, 40 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```

```
14271,7 packets/sec          Broadcast bytes:          8811,  
Incoming rates:             60,8 kbits/sec  
                           48,2 packets/sec  
Outgoing rates:             66528,8 kbits/sec          IP checksum errors:          0  
                           144226,2 packets/sec
```

- ➔ ~ 180 kpps of TCP SYN will consume 99.9% CPU on almost every current firewall
  - ➔ Tested on ASA 5585X-SSP-60 & CheckPoint 21400 (as of Nov. 2012)
  - ➔ CheckPoint published multiqueue IRQ drivers to solve this issue, Firewalls w/o multiqueue drivers are still vulnerable

# Attack types - killing me softly....

- ⇒ Slow HTTP / slowloris attacks
- ⇒ (D)owning powerful websites with less than 1000 kbps
  - ⇒ Sending HTTP requests byte by byte, but never sending „carriage return“
  - ⇒ Not exploiting a bug => IDS / IPS won't work for this
  - ⇒ Exhausting sockets to keep server busy
  - ⇒ Difficult to detect on first contact, low bandwidth, low CPU usage
- ⇒ Won't be fixed by apache, you have to fix it yourself
  - ⇒ Apache Modules - mod\_security, mod\_reqtimeout, mod\_antiloris
  - ⇒ Load Balancers - Advanced TCP splicing & delayed forward

# Attack types - killing me softly...

➔ Profiling the #TARGET for best timeout value to choose

➔ `slowloris.pl -dns [domain] -port 80 -test`

```
This test could take up to 14.3666666666667 minutes.  
Connection successful, now comes the waiting game...  
Trying a 2 second delay:  
    Worked.  
Trying a 30 second delay:  
    Worked.  
Trying a 90 second delay:  
    Worked.  
Trying a 240 second delay:  
    Worked.  
Trying a 500 second delay:  
    Failed after 480 seconds.  
Remote server closed socket.  
Use 240 seconds for -timeout.  
root@ma22290:/home/adem#  
root@ma22290:/home/adem#
```

240 seconds  
is the timeout value for  
this target

➔ Attack

➔ `slowloris.pl -dns [TARGET] -port 80 -timeout 240 -num 1024`

➔ Since Apache doesn't log incomplete requests #ADMIN will go crazy as nothing is going to be logged during attack



**MITIGATE & RESPOND**

# || Mitigate & Respond - make or buy

## ➔ Cloud based solutions use same approaches

- ➔ DNS based, acting as reverse proxy, often limited to http traffic only
- ➔ BGP based, off-ramping traffic, piping it back via GRE, not limited to http

## ➔ Vendors

- ➔ AKAMAI (KONA)
- ➔ CLOUDFLARE
- ➔ PROLEXIC (PLXrouted, PLXproxy, PLXconnect)

## ➔ The #Cloud and I won't become friends

- ➔ „Cloudflare outage taking down 785.000 websites“  
<http://tcrn.ch/WoNueA>

# || Mitigate & Respond - make or buy

➔ There is no „Buy only“ or „Make only“ solution

➔ BUY

➔ Involve your ISP to counter volumetric attacks

➔ Telekom, Vodafone, [...] offering DDoS protection

➔ MAKE

➔ Build up STAFF, in-house capabilities are crucial

➔ Visibility is the key, go for Netflow, analyze traffic behavior

➔ Implement **purpose build** solutions to counter sophisticated DDoS attacks

➔ Establish #SIGINT with your ISP

➔ Implement & maintain mitigation plans




# Mitigate & Respond - must have countermeasures

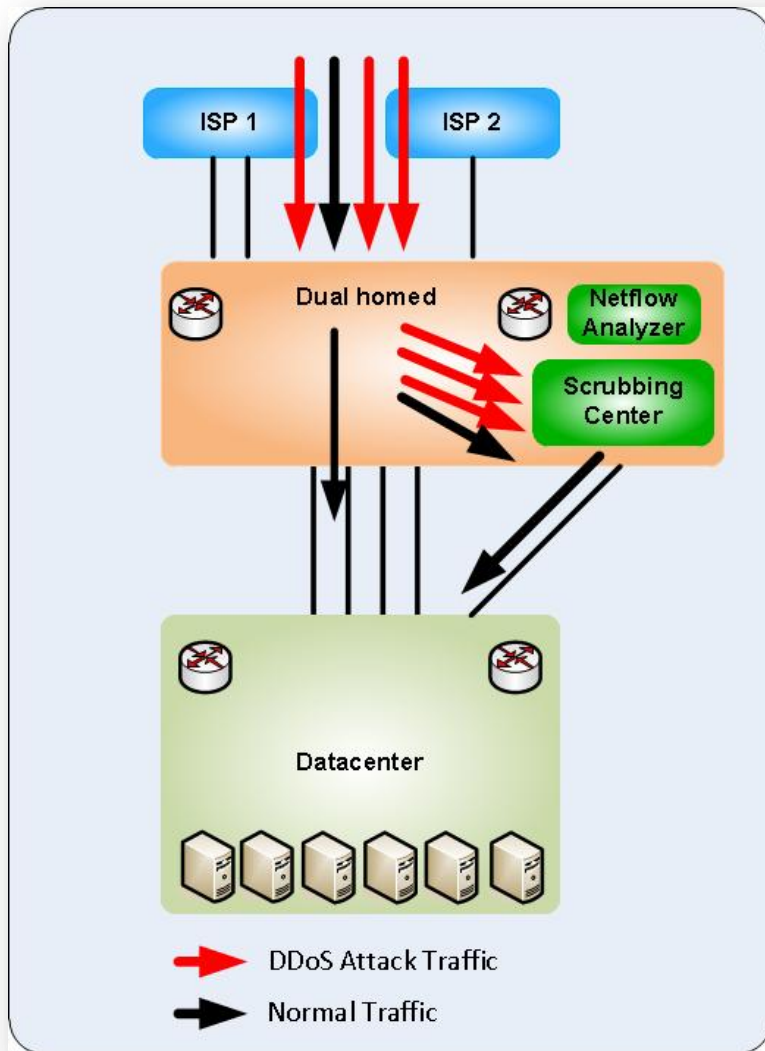
- Flood detection & blocking (pps per source IP)
- Packet level authentication for TCP SYN, RST, [...]
- TCP policy based blocking (timer, bytes send period[...])
- GEO IP & ASN based blacklisting
  - Very useful during large scale attacks
- App-Level Rate Limiting (http, dns, [..])
- DPI / payload based blocking (RegEx...)
  
- **Missing Blackholing?**
- **BH is not a „mitigation“, at least from customer's perspective**
  
- Ever tried this with packet filters, IPS, WAF, LB's?
- **That's why we need purpose build #EQUIP**



# || Mitigate & Respond - If you ask me...

- ➔  ...is doing a great job
- ➔ Hardware based, utilizes Netflow for visibility
- ➔ BGP based mitigation, interacts with your AS
- ➔ Granular Traffic diversion via BGP (/32 announcements)
- ➔ Intelligent countermeasures going far beyond FW & IPS
- ➔ Auto Mitigation capabilities
- ➔ ATLAS, >280 ISPs worldwide feeding ATLAS with stats
- ➔ Works for Enterprise to large ISP
  
- ➔ **It Works!**

# Mitigate & Respond - scrubbing center...



- ➔ Gathering Netflow info from edge routers for visibility and attack detection
- ➔ “Off-ramping” traffic for destination IP of #TARGET only, non attack traffic stays on path
- ➔ “On-ramping” traffic after “scrubbing” back to standard routing path

# Mitigate & Respond - entering the battle...

### Countermeasures

Timeframe: Summary Graph Unit: bps

Status	Countermeasure	
+	Invalid Packets	
+	IPv4 Address Filter Lists	
+	IPv4 Black/White Lists	
+	IP Location Filter Lists	
+	Zombie Detection	4.4
+	TCP SYN Authentication	925
+	DNS Scoping	
+	DNS Authentication	
+	TCP Connection Reset	
+	Payload Regular Expression	
+	Source /24 Baselines	
+	Protocol Baselines	
+	DNS Malformed	
+	DNS Rate Limiting	
+	DNS NXDomain Rate Limiting	
+	DNS Regular Expression	
+	HTTP Malformed	
+	HTTP Scoping	
+	HTTP Rate Limiting	
+	HTTP/URL Regular Expression	
+	SIP Malformed	
+	SIP Request Limiting	
+	Shaping	
+	IP Location Policing	

bps
pps

Summary
30 Minutes
5 Minutes

17:48:30
17:49:45
17:51:00
17:52:15

■ Pass bps
 ■ Drop bps

Total
Per TMS
Per Countermeasure

	1 Minute	5 Minute	Summary
Dropped:	65.6 Mbps / 186.2 Kpps	58.9 Mbps / 167.3 Kpps	14.2 Mbps / 40.5 Kpps
Passed:	8 bps / 0 pps	1.2 bps / 0 pps	0.1 bps / 0 pps
Total:	65.6 Mbps / 186.2 Kpps	58.9 Mbps / 167.3 Kpps	14.2 Mbps / 40.5 Kpps
Percent Dropped:	100.00%	100.00%	100.00%
Average Blocked Hosts:	2 hosts	2 hosts	0.8 hosts



# MYTHBUSTING

# Mythbusting - common myths

- ➔ FW & IPS can protect against DDoS attacks
  - ➔ It won't! Do not even try it! :-)
- ➔ CDN will solve the DDoS problem (e.g. AKAMAI KONA)
  - ➔ No it won't since most sites make use of dynamic content, CDN works only for simple static sites
- ➔ You can counter DDoS with ACL automation?!?
  - ➔ Wait...what?
  - ➔ ACL jockeying will probably knock you out before the attackers can do
  - ➔ „Misconfiguration “ is in the top 3 of “most common threats”

# Early Warnings

- ➔ Ordinary news / press don't work for this
- ➔ Join one of the Information Sharing Alliances (ISAC)
  - ➔ ISACs don't share information with non-ISAC-people :-)
  - ➔ FS-ISAC <https://www.fsisac.com/>
  - ➔ IT-ISAC <https://www.it-isac.org/>
- ➔ Use social media for early warnings
  - ➔ Twitter is awesome for this (e.g. #ddos, #malware)
  - ➔ Google Alerts for shitstorm detection on the entire web
    - ➔ Have a look at free anonymous pasting sites like „Pastebin“



# Q&A



QUESTIONS?





# Useful Resources & Links

- Credits go to „INFOSEC Reactions“ for great GIFs :-)
  - <http://securityreactions.tumblr.com/>
- ARBOR Networks Worldwide Infrastructure Security Report
  - <http://www.arbornetworks.com/research/infrastructure-security-report>
- ARBOR ATLAS & ASERT BLOG
  - <http://atlas.arbor.net/>
  - <http://ddos.arbornetworks.com/>
- Shadowserver - ASN & Netblock Alerting & Reporting Service
  - <http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork>
- Google Safebrowsing Alerts for Administrators
  - <http://www.google.com/safebrowsing/alerts/>
- Related IETF RFCs
  - <https://tools.ietf.org/html/rfc2827.txt>
  - <https://tools.ietf.org/html/rfc3631.txt>
  - <https://tools.ietf.org/html/rfc3882.txt>
  - <https://tools.ietf.org/html/rfc4732.txt>
  - <https://tools.ietf.org/html/rfc4987.txt>
- **Support the hard working „malware crusaders“ community on Twitter, hunting malware and botnets to make the Internet a safer place!**
  - #malwaremustdie