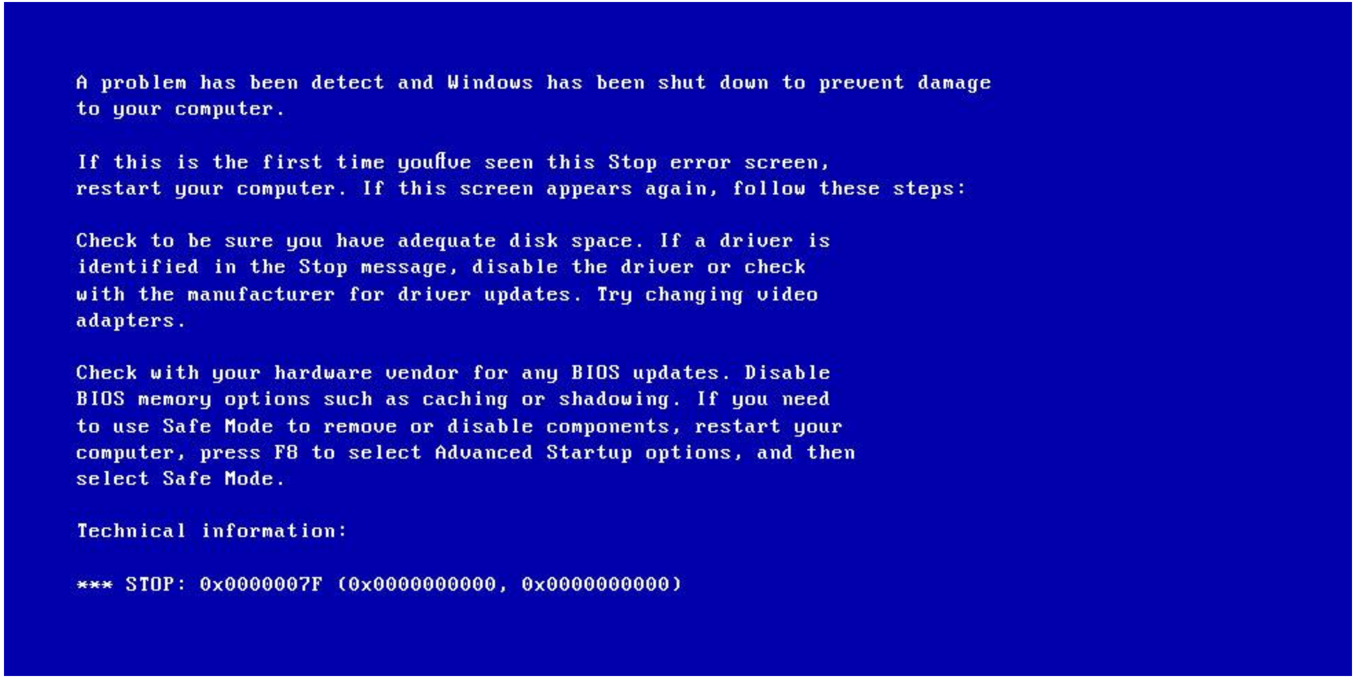
Imma Chargin Mah Lazer

How to protect against (D)DoS attacks

Oliver Matula

omatula@ernw.de

Denial of Service (DoS)



```
A problem has been detect and Windows has been shut down to prevent damage
to your computer.

If this is the first time youflve seen this Stop error screen,
restart your computer. If this screen appears again, follow these steps:

Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.

Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000007F (0x0000000000, 0x0000000000)
```

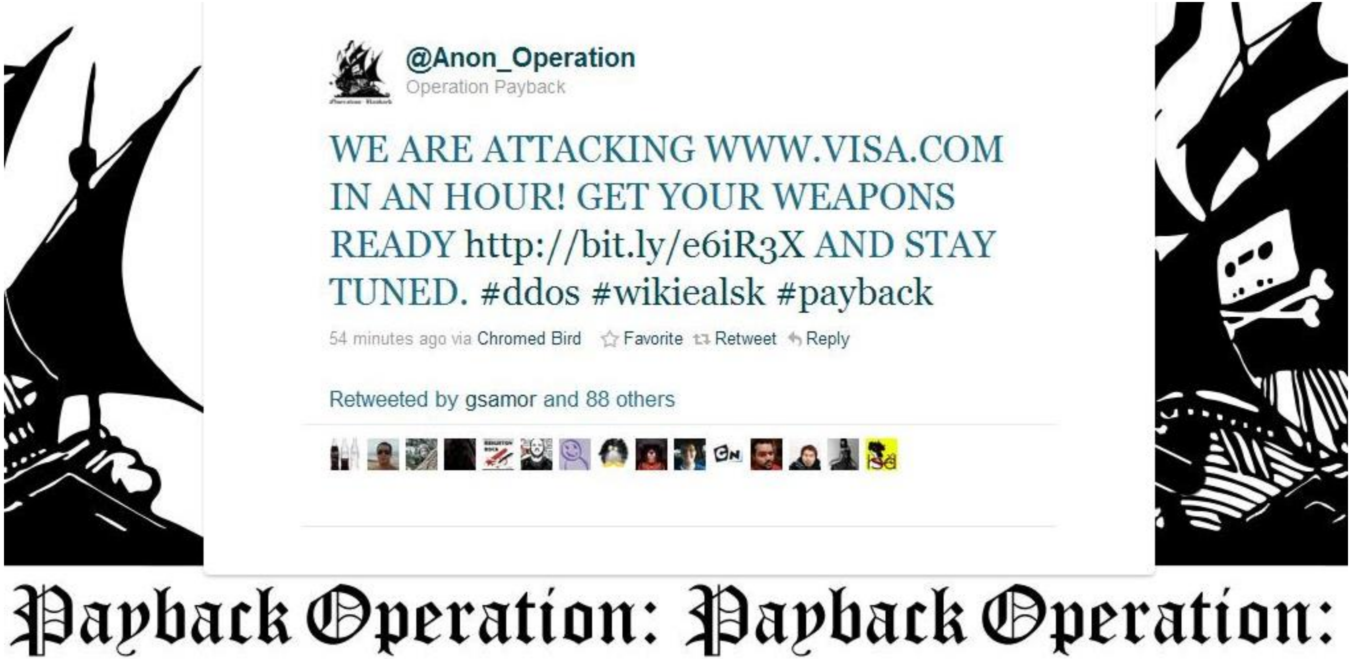
Outline

- Why is (D)DoS protection important?
  - Infamous attacks of the past
- What types of (D)DoS attacks are there?
  - Volume-based attacks
  - Protocol-based attacks
  - Application-based attacks
- How to protect against (D)DoS attacks?
  - Multi-layered strategy

Why is (D)DoS protection important?

Infamous attacks of the past

Operation Payback

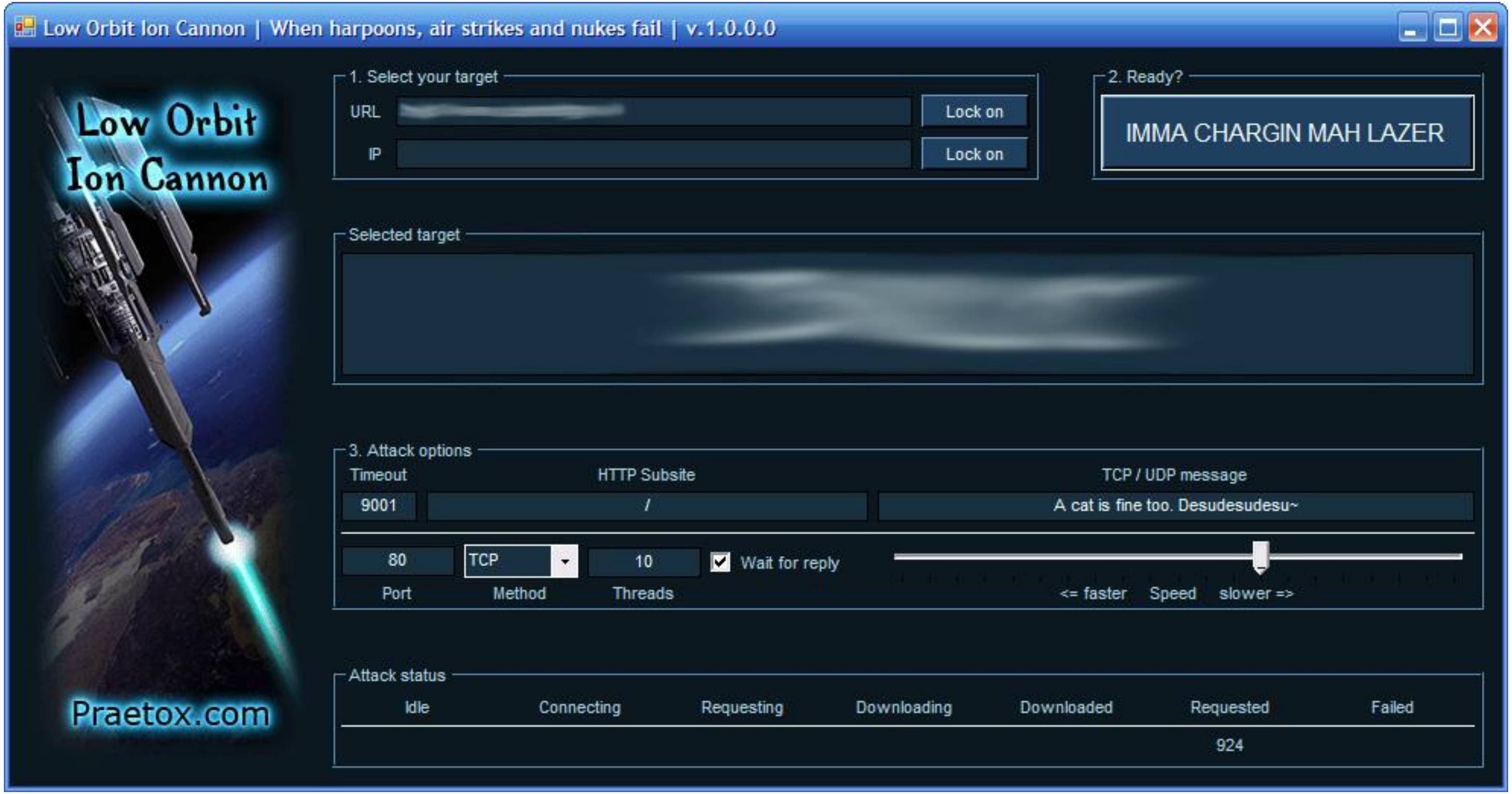


@Anon_Operation
Operation Payback

WE ARE ATTACKING WWW.VISA.COM IN AN HOUR! GET YOUR WEAPONS READY http://bit.ly/e6iR3X AND STAY TUNED. #ddos #wikiealsk #payback

54 minutes ago via Chromed Bird ☆ Favorite ⇄ Retweet ↰ Reply

Retweeted by gsamor and 88 others



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target

URL [redacted] Lock on

IP Lock on

2. Ready?

IMMA CHARGIN MAH LAZER

Selected target

[redacted]

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

Threads: 10

☑ Wait for reply

<= faster Speed slower =>

Attack status

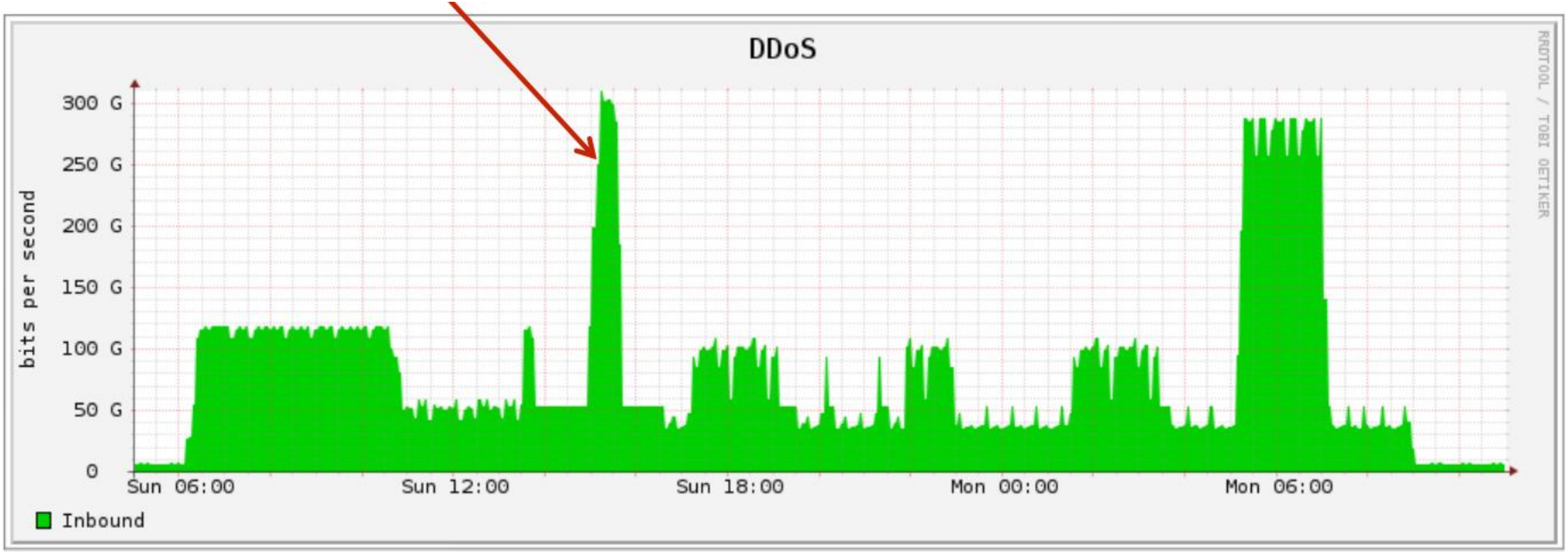
Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					924	

Other (D)DoS campaigns

- DD4BC (DDoS for Bitcoin)
  - Blackmailing of hosting providers, e-commerce platforms, and banks
  - “Pay or get a DDoS attack”
- DDoS against Spamhaus
  - Non-profit anti-spam organization
  - Volume-based DDoS attack after hosting provider *CyberBunker* was added to its blacklist

DDoS against Spamhaus (2013)

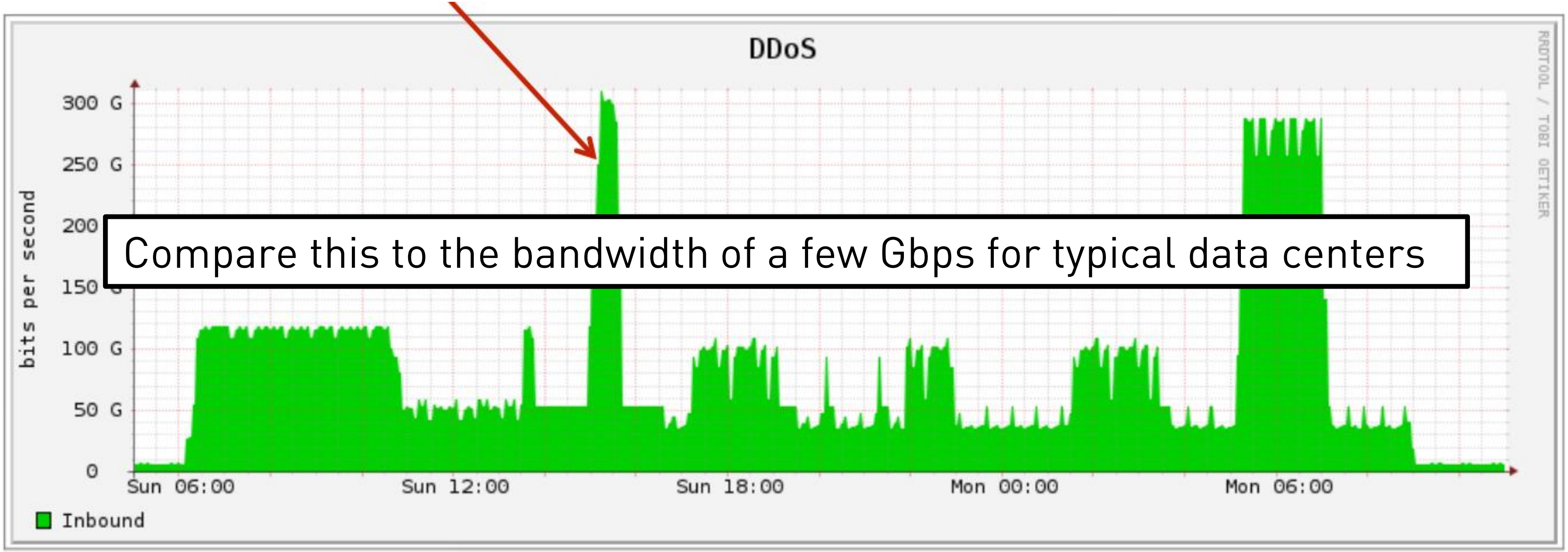
~ 300 Gbps attack, ~ 30,000 open DNS server participated



Talk by Martin J. Levy (Cloudflare) at ENOG8

DDoS against Spamhaus (2013)

~ 300 Gbps attack, ~ 30,000 open DNS server participated



Compare this to the bandwidth of a few Gbps for typical data centers

Talk by Martin J. Levy (Cloudflare) at ENOG8

Reasons for DDoS attacks

- Blackmailing
- (Politically motivated) hacktivism
- Competitive advantage
- Hate crime
- Script kiddies
- Distraction for data exfiltration or other attacks

What types of (D)DoS attacks are there?

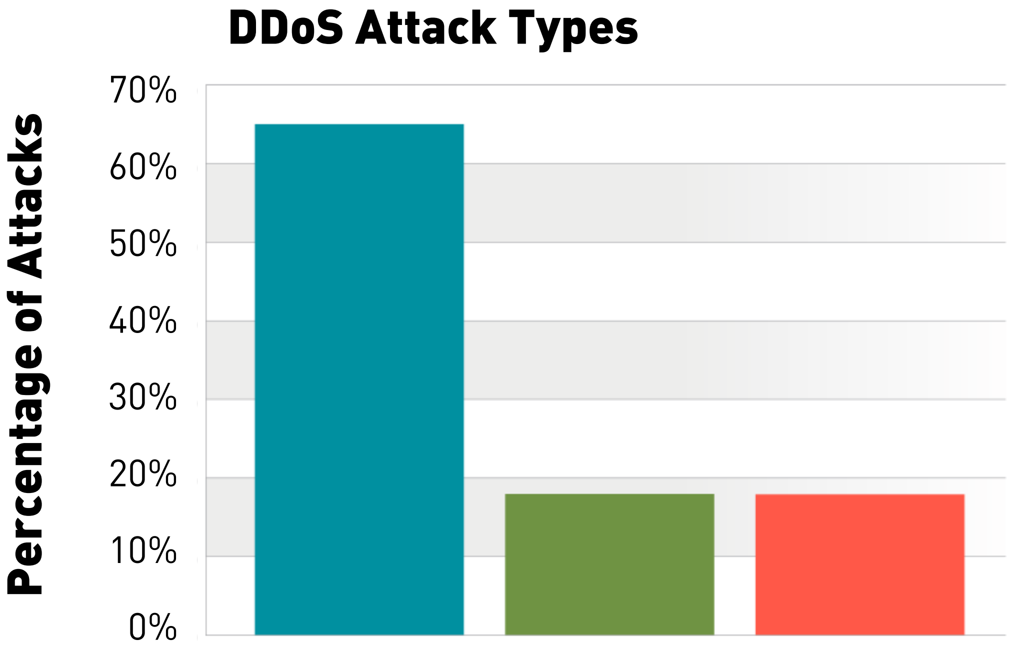
Types of DoS attacks

- Volume-based attacks
  - Exhaust bandwidth of network connections
- Protocol-based attacks
  - Exploit protocol-specific vulnerabilities
- Application-based attacks
  - Exploit application-specific vulnerabilities

Properties of Attack Types

	Volume-Based	Protocol-Based	Application-Based
Measured in	Bits per Second	Packets per Second	Requests per Second
Difficulty	Low	Low-Medium	Medium-High
Level of Customization	Low	Low-Medium	Medium-High
Impact	High	High-Medium	Medium-Low
Examples	DNS- or NTP-Based Amplification Attack	TCP SYN Flood	HTTP Slow Header Attack

Attack Vector Frequency



● **65%** Volume-Based

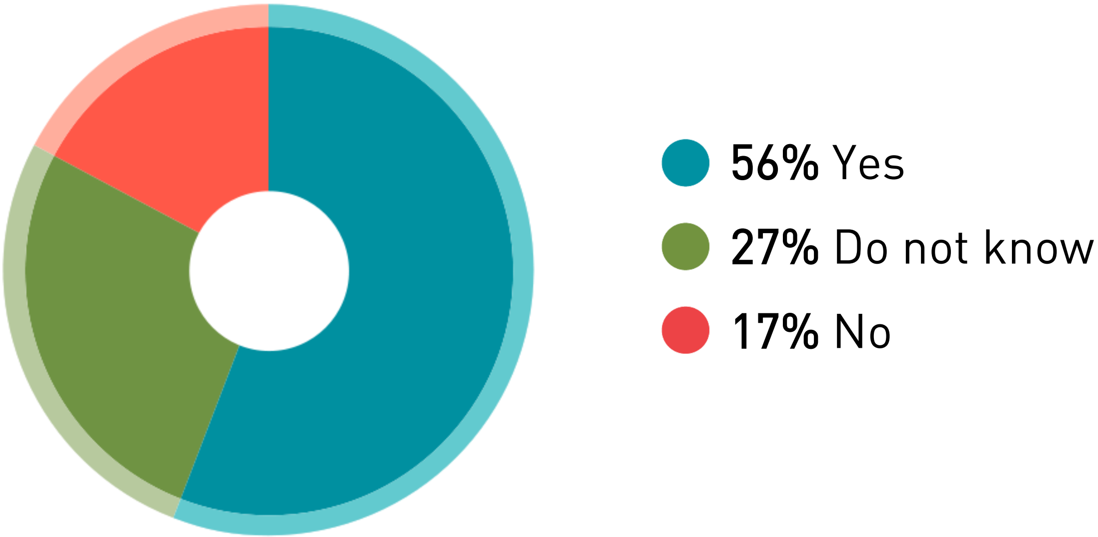
● **18%** Protocol-Based

● **18%** Application-Based

Worldwide Infrastructure Security Report 2016

Multi-Vector Attacks

Multi-Vector DDoS Attacks

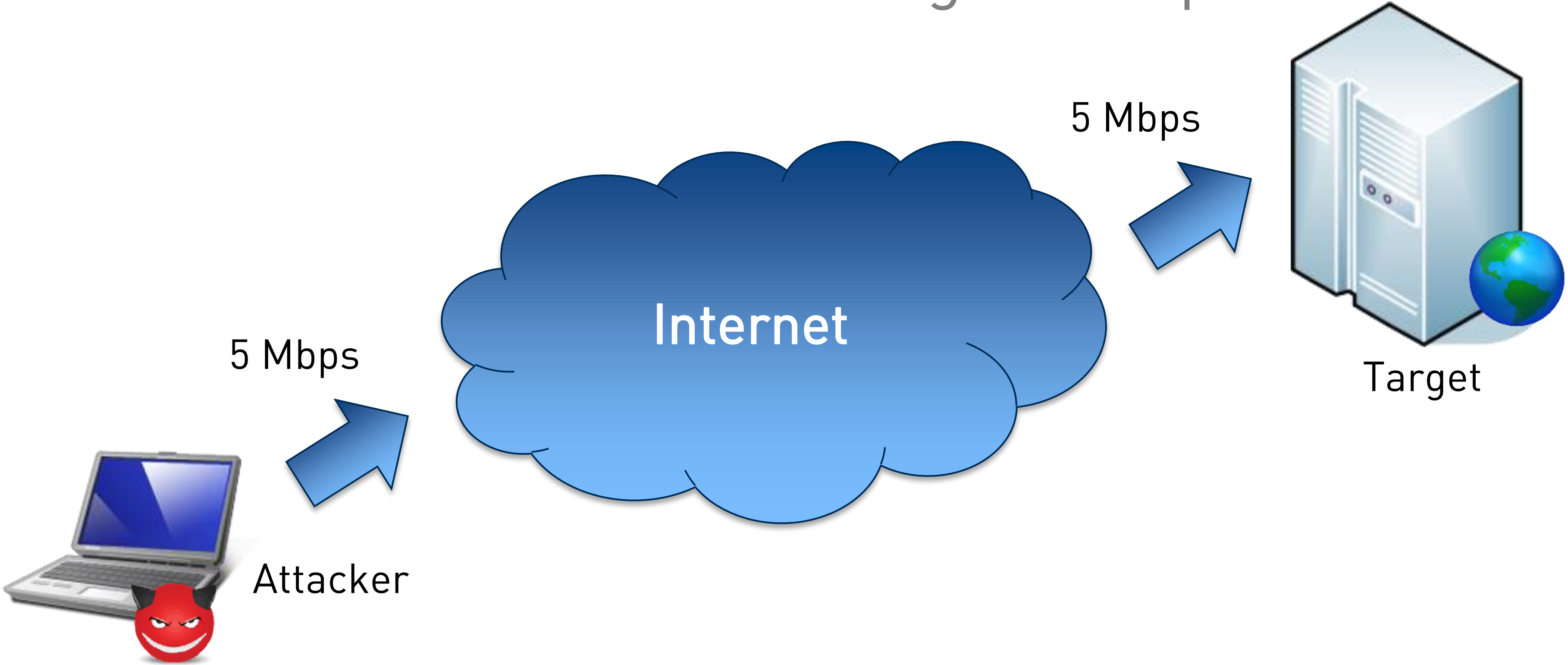


Worldwide Infrastructure Security Report 2016

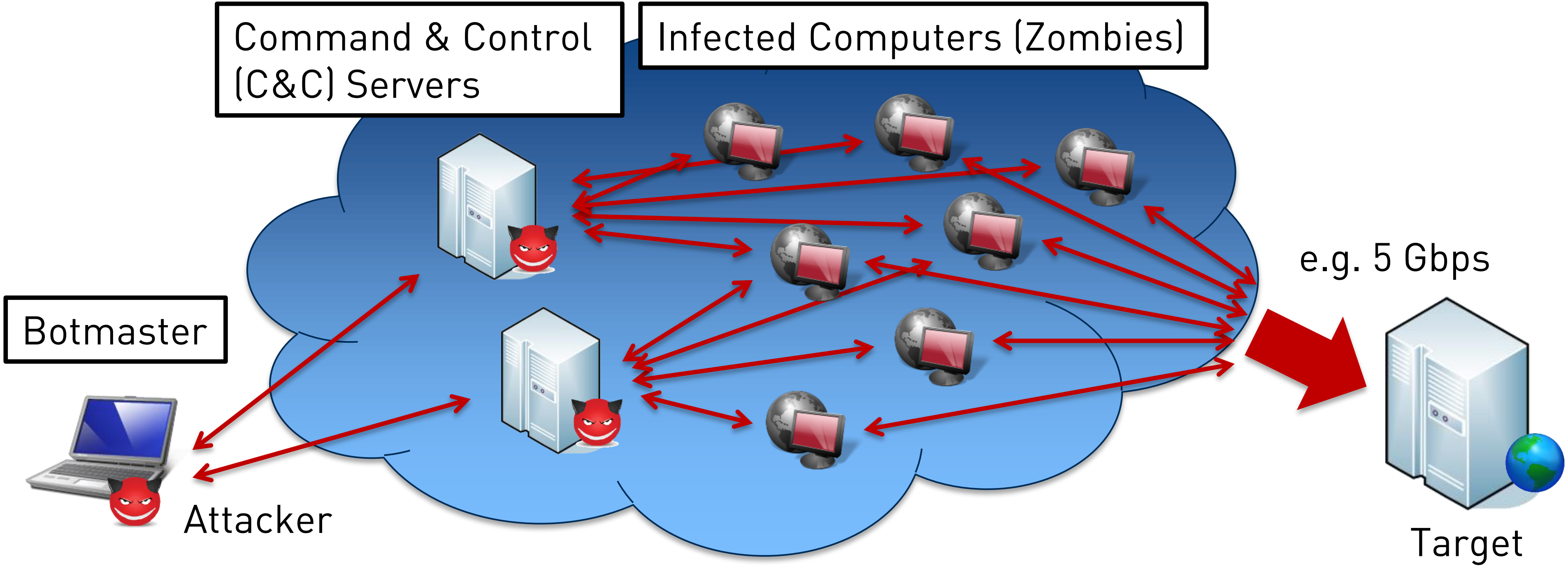
What types of (D)DoS attacks are there?

Volume-Based attacks

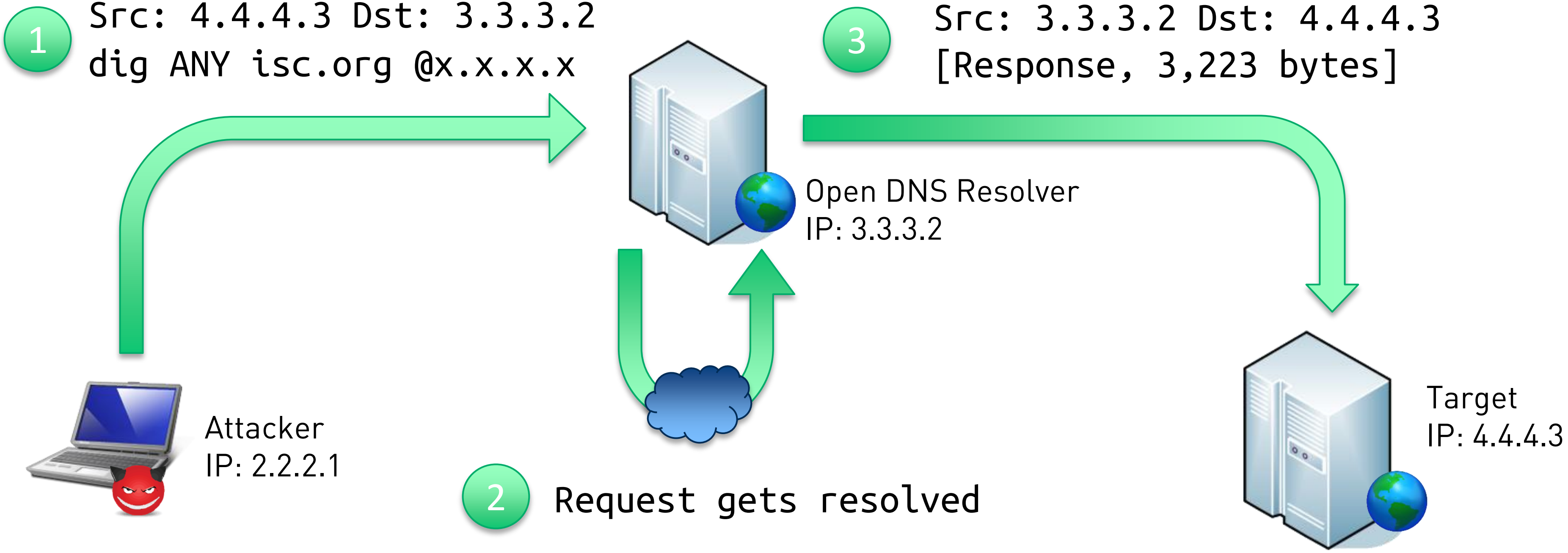
Volume-based attacks – Single Computer



Volume-based attacks – Botnet

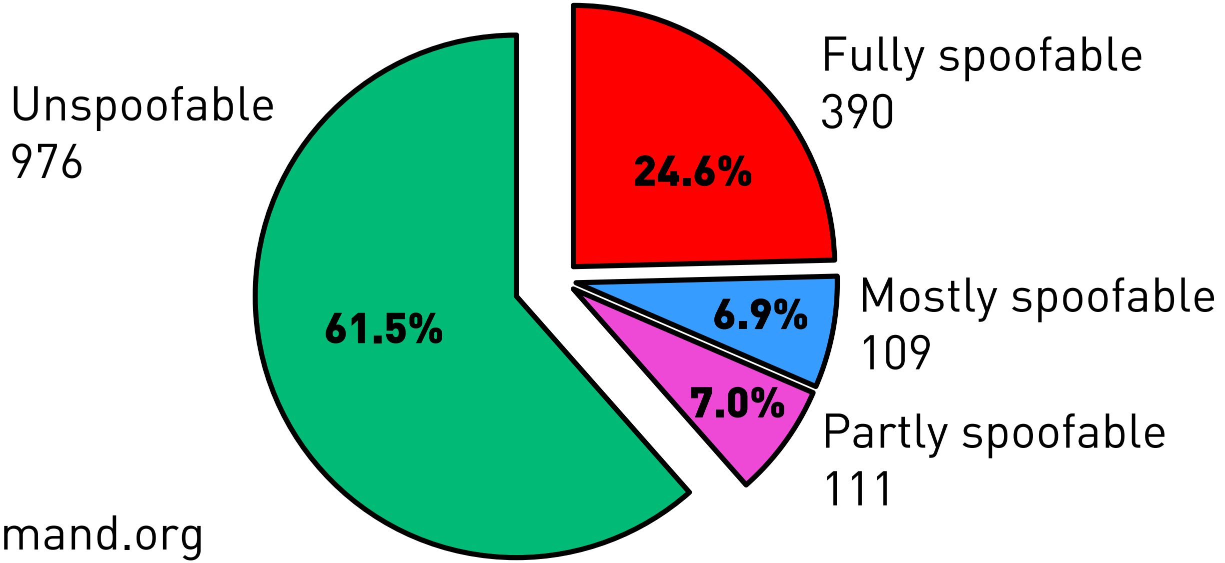


DNS-Based Reflection Attack



State of IP-Spoofing

- ~25% of all autonomous systems allow spoofing



http://spoofer.cmand.org

UDP-Based Amplification

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	Unrestricted recursive domain resolution for any client
NTP	556.9	Monlist request
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
…	…	…

https://www.us-cert.gov/ncas/alerts/TA14-017A

A few facts

- ~ 90% of attacks last less than one hour
  - But: There can be a high attack frequency
- Average attack size ~ 2 Gbps
- Peak attack size ~ 350 Gbps
- ~50% of attacks use multiple attack techniques at the same time

What can be done?
Check UDP services

- DNS servers should not be configured as open resolvers
  - www.us-cert.gov/ncas/alerts/TA13-088A
  - openresolverproject.org
- Monlist command should be disabled on NTP server
  - www.us-cert.gov/ncas/alerts/TA14-013A
  - openntpproject.org

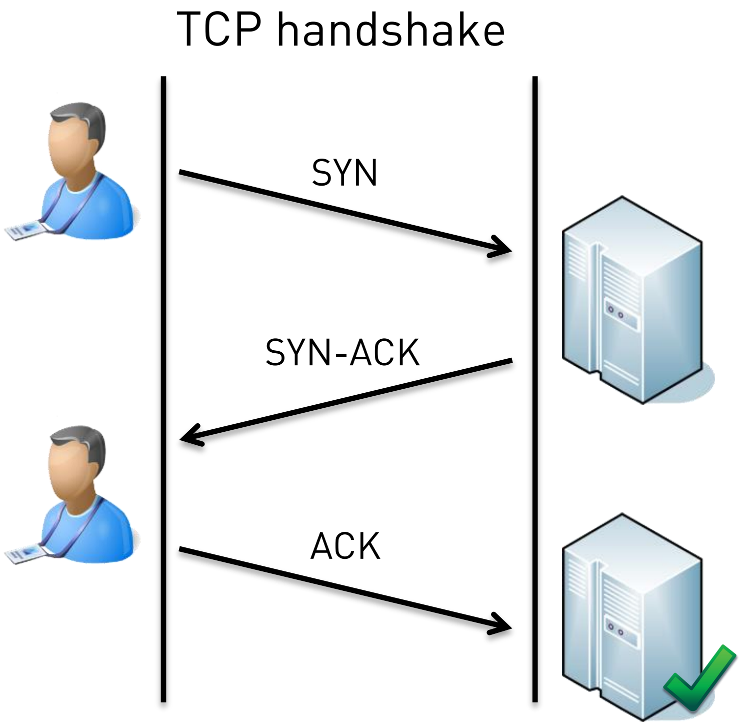
What can be done? Prevent IP Spoofing

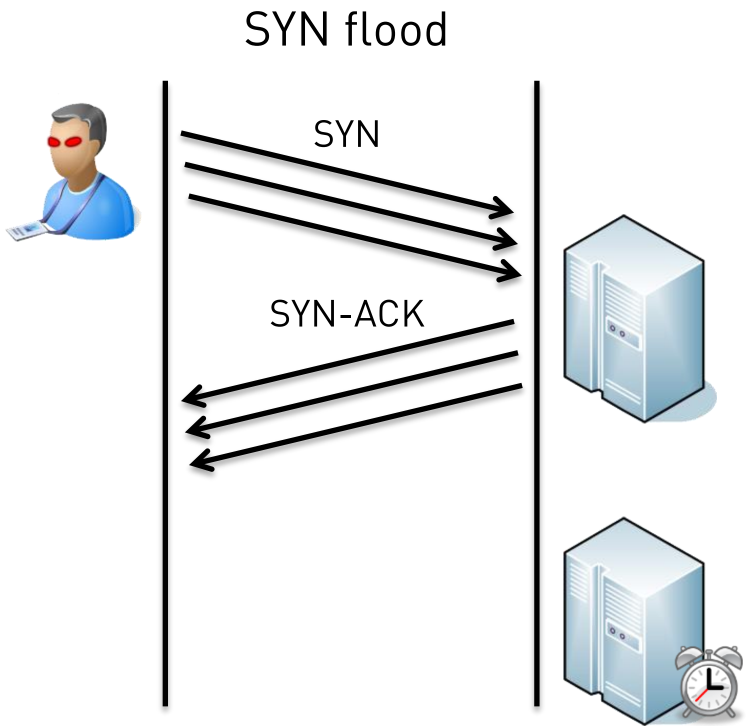
- BCP38 / RFC2827 (ingress filtering)
  - http://www.ietf.org/rfc/bcp/bcp38.txt
  - http://www.ietf.org/rfc/rfc2827.txt
- BCP84 / RFC3704 (solution for multi-homed)
  - http://www.ietf.org/rfc/bcp/bcp84.txt
  - http://www.ietf.org/rfc/rfc3704.txt

What types of (D)DoS attacks are there?

Protocol-Based Attacks

TCP SYN flood





What can be done?
Reduce resource consumption

- SYN Cache, SYN Cookies, ...
  - https://tools.ietf.org/html/rfc4987
  - SYN Cache: Partial state is stored in hash table
  - SYN Cookie: Partial state is stored in exchanged packets
- TCP Cookie Transactions
  - https://tools.ietf.org/html/rfc6013
  - Experimental Status

Ping of Death

- Malformed ICMP packet with size larger than the maximum packet size (65,535 bytes).
  - Leads to buffer overflow.
  - Generally believed that modern systems are secure.
  - BUT: Microsoft operating systems have been vulnerable over IPv6 until late 2013.

What types of (D)DoS attacks are there?

Application-Based Attacks

Application-based attacks

- Highly application specific
  - Computationally expensive operations (database lookup, PDF generation, etc.)
  - Vulnerabilities in the application
- But also some general attacks
  - Slow Header Attack (e.g. Slowloris)
  - Slow Post Attack

Slow Header Attack

- Establish HTTP connections in parallel.
- Requests are never completed, i.e. only partial requests are sent.
- From time to time, new HTTP headers are added to the request.
- Affects only the web server and no other services on the server.

Slow Post Attack

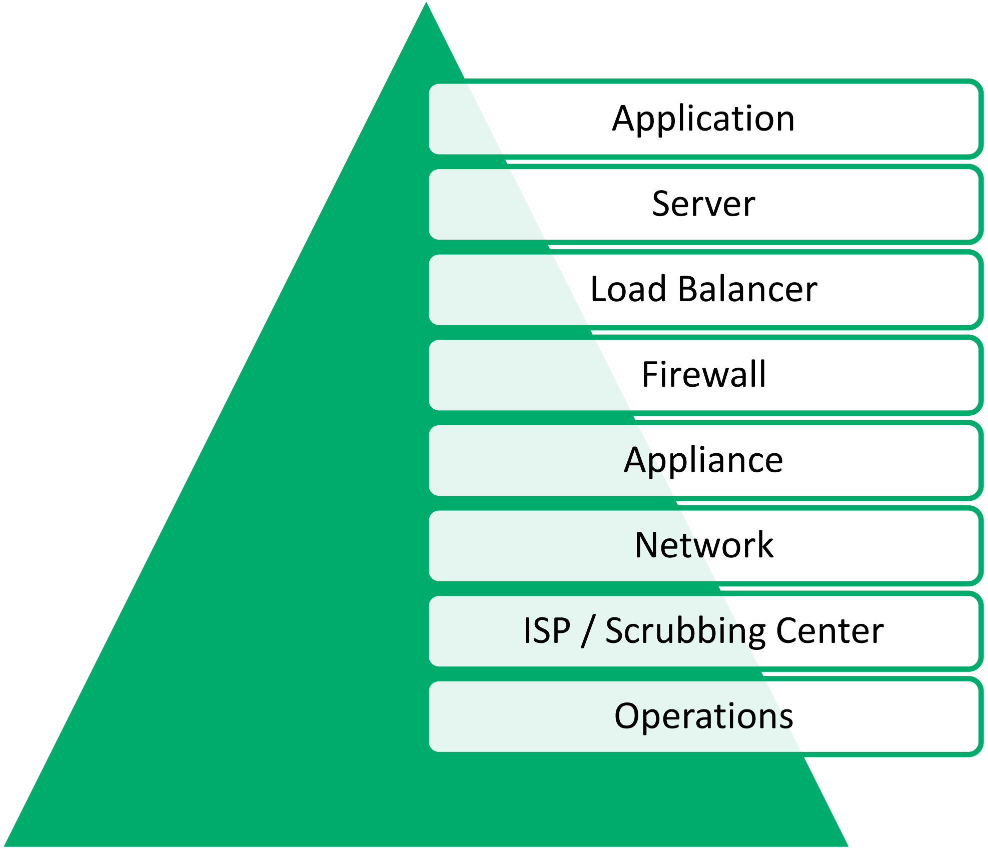
- Similar to Slow Header Attack
- Instead of sending partial headers, partial data is sent.
- Content-Length header specifies how much data will be sent.
- Partial data is sent at regular time intervals to keep connection alive.

What can be done?
Slow Header & Post Attack

- Increase maximum number of concurrent connections.
- Limit maximum number of concurrent connections by same IP.
- Limit time span that a client can stay connected.
- Special modules exist for web servers
  - Apache: mod_reqtimeout, mod_qos, …

How to protect against (D)DoS attacks?

A multi-layered strategy including operational processes



Application

Server

Load Balancer

Firewall

Appliance

Network

ISP / Scrubbing Center

Operations

Multi-layered strategy

Protection against (D)DoS

Application

- Patching Procedure
  - Out-of-support? => Other measures such as isolation, strict access controls, etc.
- Secure Development Lifecycle
  - Secure Coding Guidelines incl. DoS prevention
  - Authentication & Authorization for critical operations (database lookup, etc.)
- Security Assessments
  - DoS in scope?

Server

- Hardening of server systems
  - Web server hardening against SYN floods
  - Web server hardening Slow Header & Post attacks
- Security assessments of server systems

Load Balancer

- Load Balancer vs. Application Delivery Controller
  - Content Manipulation
  - Caching
  - SSL offload
  - Human Checks
- Whitepaper by SANS
  - Leveraging the Load Balancer to Fight DDoS

Firewall

- Good for restriction of access.
- But: Can be part of the problem
  - Resistance against SYN floods?
  - Can be bottleneck during (D)DoS attacks
  - Same is true for other stateful devices
- Conclusion: Firewalls rather pose a problem than a solution to (D)DoS attacks.

(D)DoS Protection Appliance

- Detection Only/Simulation Mode, i.e. alerting without mitigation
- Generate protection groups and rules (before going live)
- Placement next to Edge Routers to protect devices downstream
- Hybrid Solution?
- SSL/TLS traffic inspection?
- Going live?

Appliance Configuration

- Black- (e.g. botnets) and Whitelist (e.g. customers)
- IP reputation (incl. GeoIP)
- Human checks, e.g. compliance to TCP protocol, JavaScript checks, etc.
- Application-aware protection
- Configuration changes for special events

Network

- Prevent IP spoofing (BCP 38/84) at Edge Routers
- Segmentation of network into protection groups with similar traffic patterns
- Appliance inline or out-of-path?
- Monitoring of applications & systems, i.e. are systems up or down?

ISP-Based Solution

- Some ISPs provide (D)DoS protection
  - ISP solution is often based on existing (D)DoS appliances. (Check SLA)
  - Problem: (D)DoS protection is not the main job of an ISP.
- Single ISP? Multi-Homed?
- Remote Triggered Blackhole Filtering is often not a solution but completes attack
  - Last point of resort to protect other services

Cloud-Based Scrubbing Center

- Data Centers around the world filter attack traffic.
- Filter attacks next to the source (can prohibit IP spoofing).
- Provides sufficient bandwidth (~Tbps) for large (D)DoS attacks.
- But: Traffic is re-routed through a 3rd party infrastructure.

Scrubbing Center Implementation Details

- On-demand or always-on?
- Re-routing of traffic? BGP-based (often at least /24 network), DNS-based, etc.
- Activation over dedicated line?
- How to send back clean traffic? GRE-Tunnel, leased line, etc.
- Encrypted traffic?

Operations

- Before: Configuration, Documentation, Incident Response Plan, Dedicated Team, Responsibilities, etc.
- During: According to responsibilities, re-configuration of appliance, etc.
- After: Legal consequences? Customer notification?
- Document by CERT-EU: http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_09_DDoS_final.pdf

Where should you begin?

- 1. Volume-based attacks
  - High likelihood and high impact.
  - Mitigation: Scrubbing of attack traffic upstream (Cloud or ISP).
- 2. Protocol- and application-based attacks
  - Low-medium likelihood and low-medium impact.
  - Mitigation: Dedicated anti-DoS appliance plus secure applications and servers.

Conclusion

- Mitigation measures depend on the DoS attack type.
  - Volume-based attacks must be treated upstream (Cloud or ISP).
  - Protocol- and application-based attacks can be treated on-premise.
- Defence against (D)DoS is complex and needs a multi-layered strategy.
  - An appliance cannot filter all application-based attacks.

Conclusion

- Build solutions, do not just buy them.
  - An appliance can only unfold its full potential if it is managed sufficiently (in interplay with other components).
- Processes need to be well-defined in order to react to the attack.
  - Responsibilities and Escalation Path have to be well-defined.

Questions?

- Thank you for your attention!