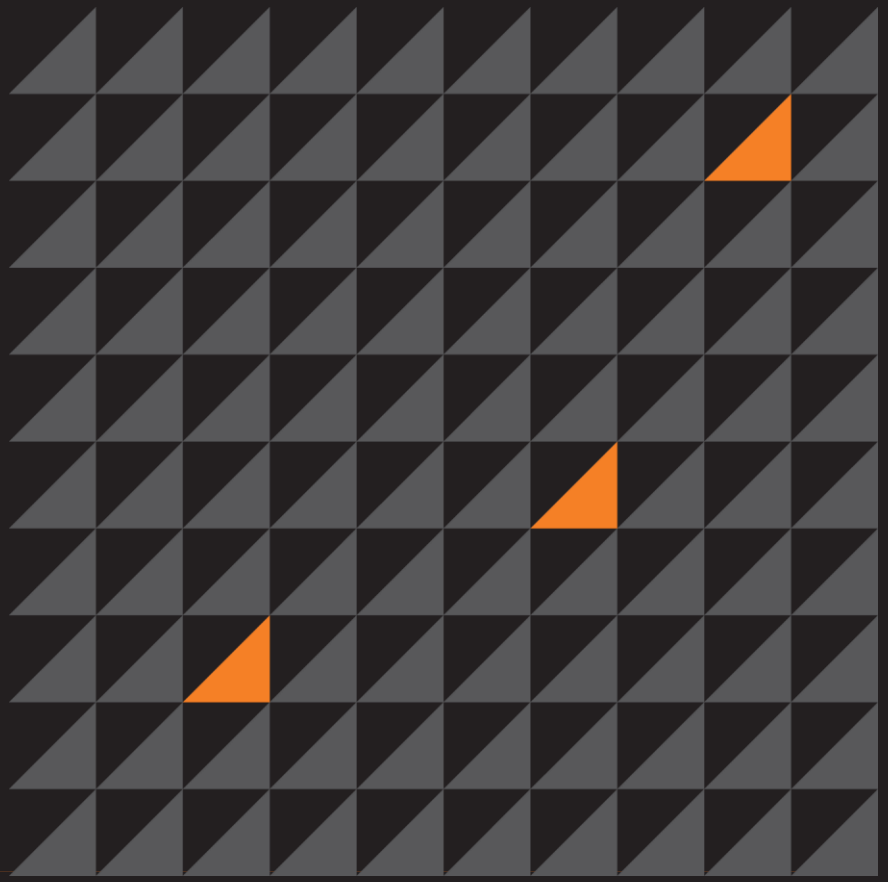
MWR LABS

BSIDES 2015 MANCH35T3R

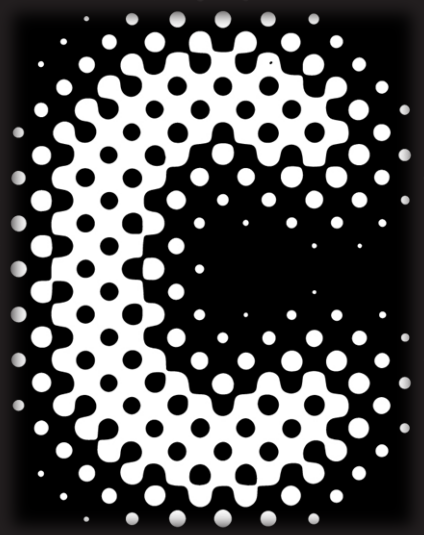
“Who uses LOIC these days anyway?”

Matt Watkins | @MattWatkins93

25/08/15



whoami



- Network Intrusion Analyst
  - Countercept | MWR InfoSecurity
- Staffordshire University Graduate
  - BSc Computer Networks & Security
  - Dissertation/FYP – “Evolution of DDoS Attacks”
- Perimeter Operations Analyst – GlaxoSmithKline
  - Firewall Engineer
  - Cisco/Check Point junkie

CSC/WHA mentions

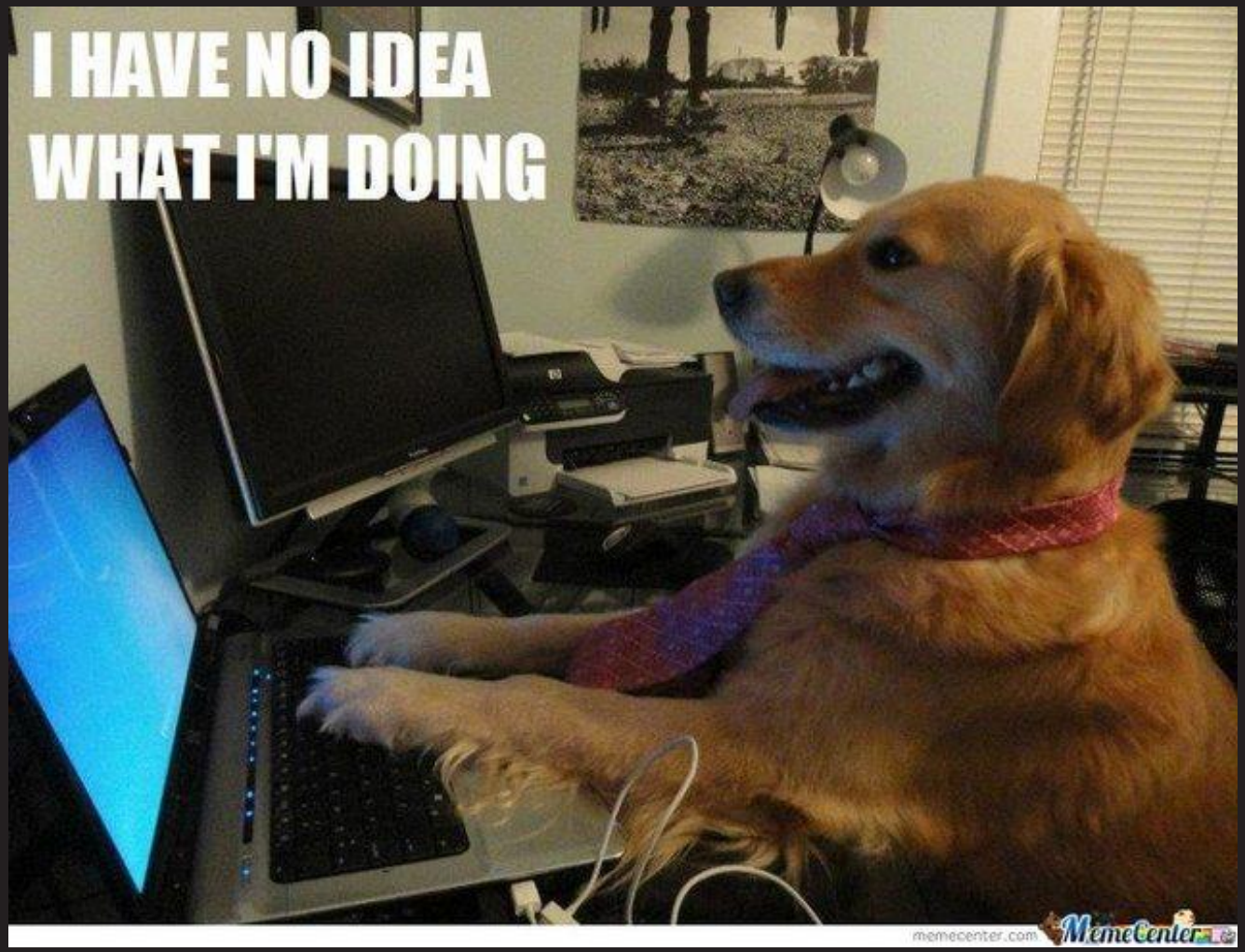
- http://cybersecuritychallenge.org.uk/
  - Fantastic resource for anyone looking to get into Cyber
  - Need help building/developing challenges/games

- https://www.whitehatters.academy/
  - CSC Alumni Group
  - Community for anyone who has previously attended a CSC F2F
  - Dedicated industry channel

Agenda

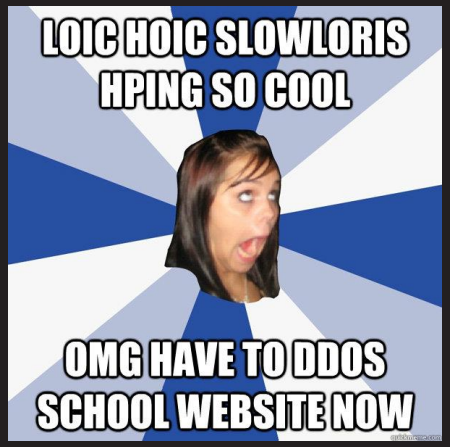
- What is DDoS
- Attack Types
  - Volumetric
  - Protocol
  - Application
- Motives
- Prevention/Mitigation
- Summary

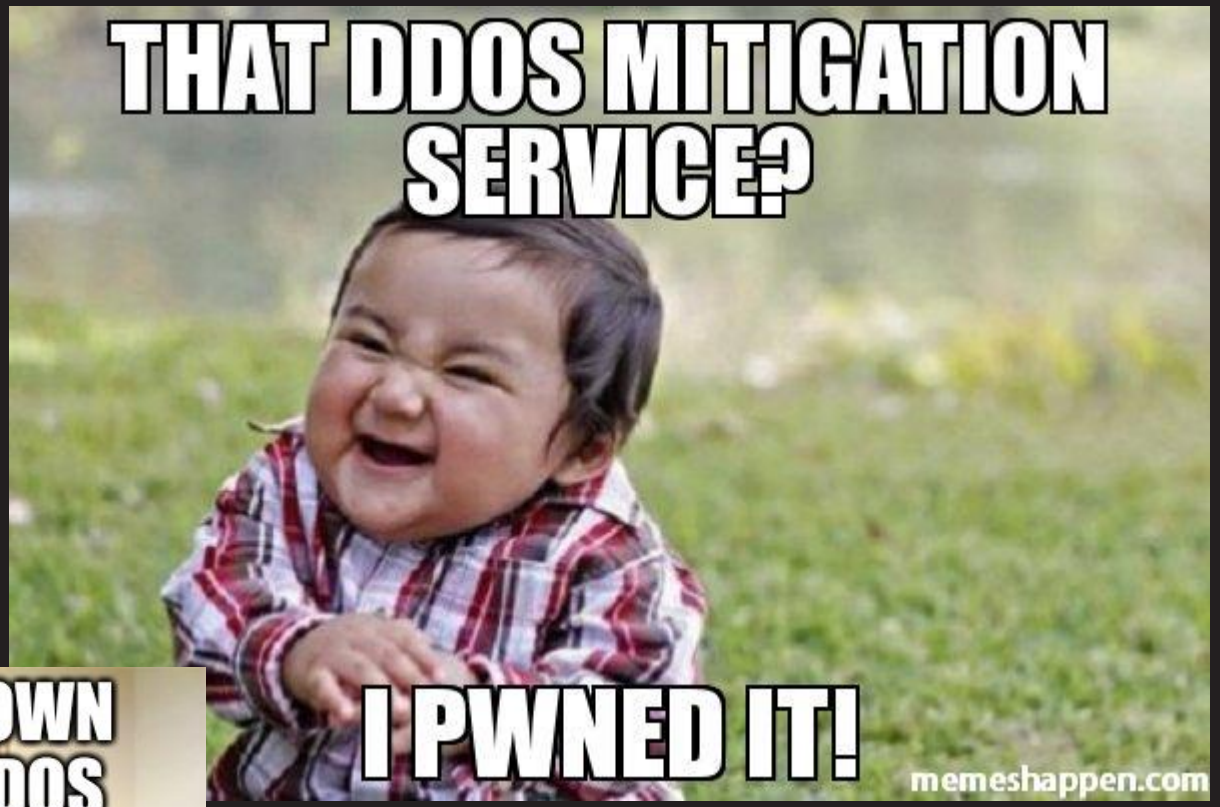
What is a DDoS attack?

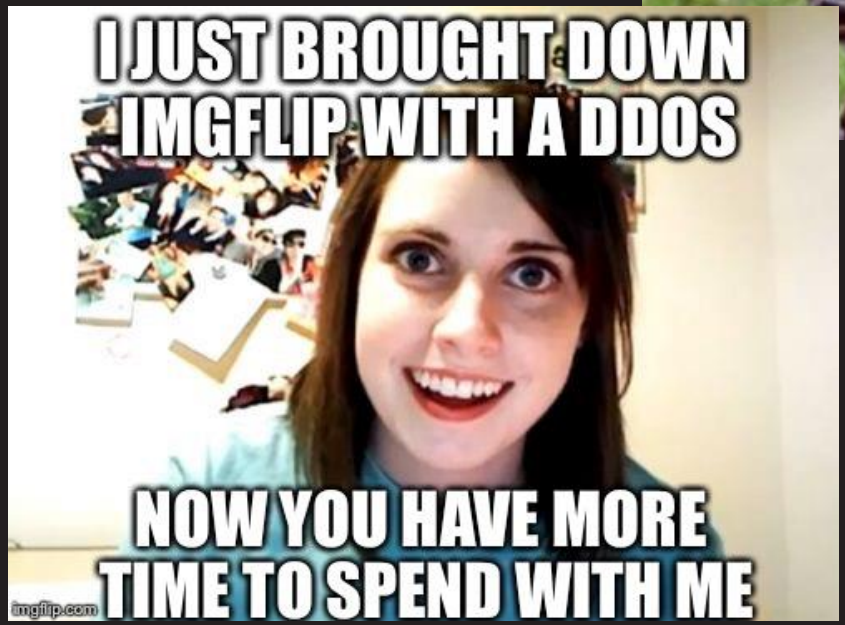


Or

Or


LOIC HOIC SLOWLORIS
HPING SO COOL
OMG HAVE TO DDOS
SCHOOL WEBSITE NOW


THAT DDOS MITIGATION SERVICE?
I PWNED IT!
memeshappen.com


I JUST BROUGHT DOWN IMGFLIP WITH A DDOS
NOW YOU HAVE MORE TIME TO SPEND WITH ME
imgflip.com

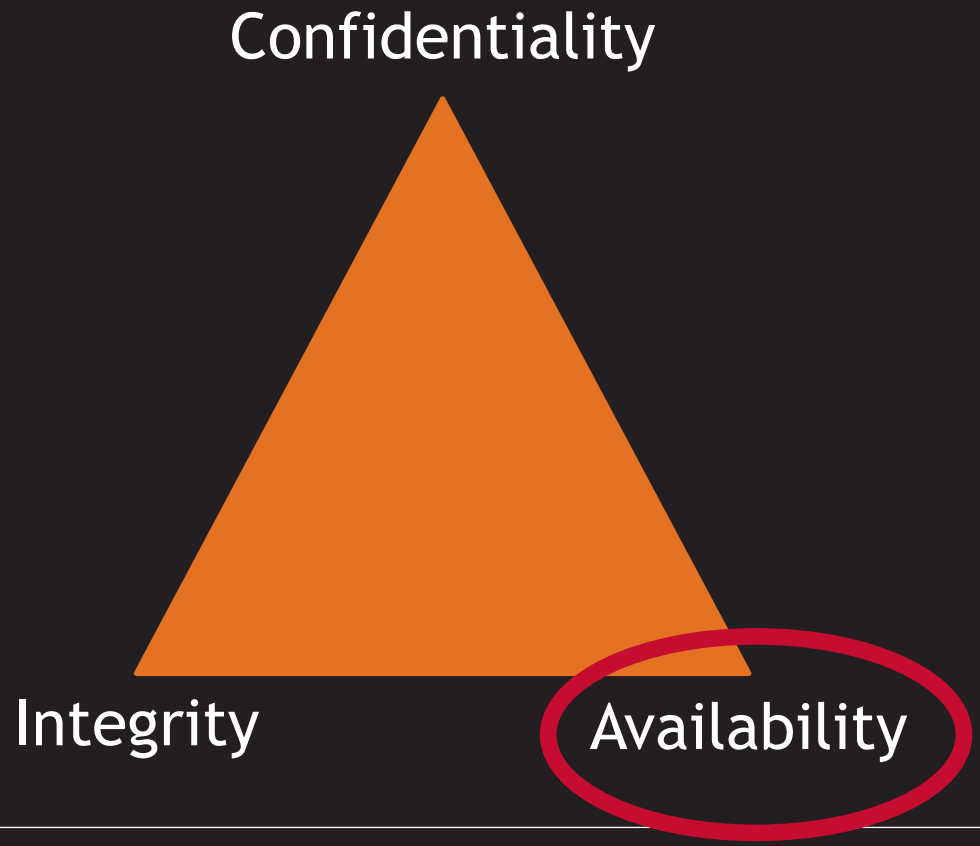

Dont bother me...
Im sending a DDoS attack

MWR LABS

Resulting in…

Essentially…

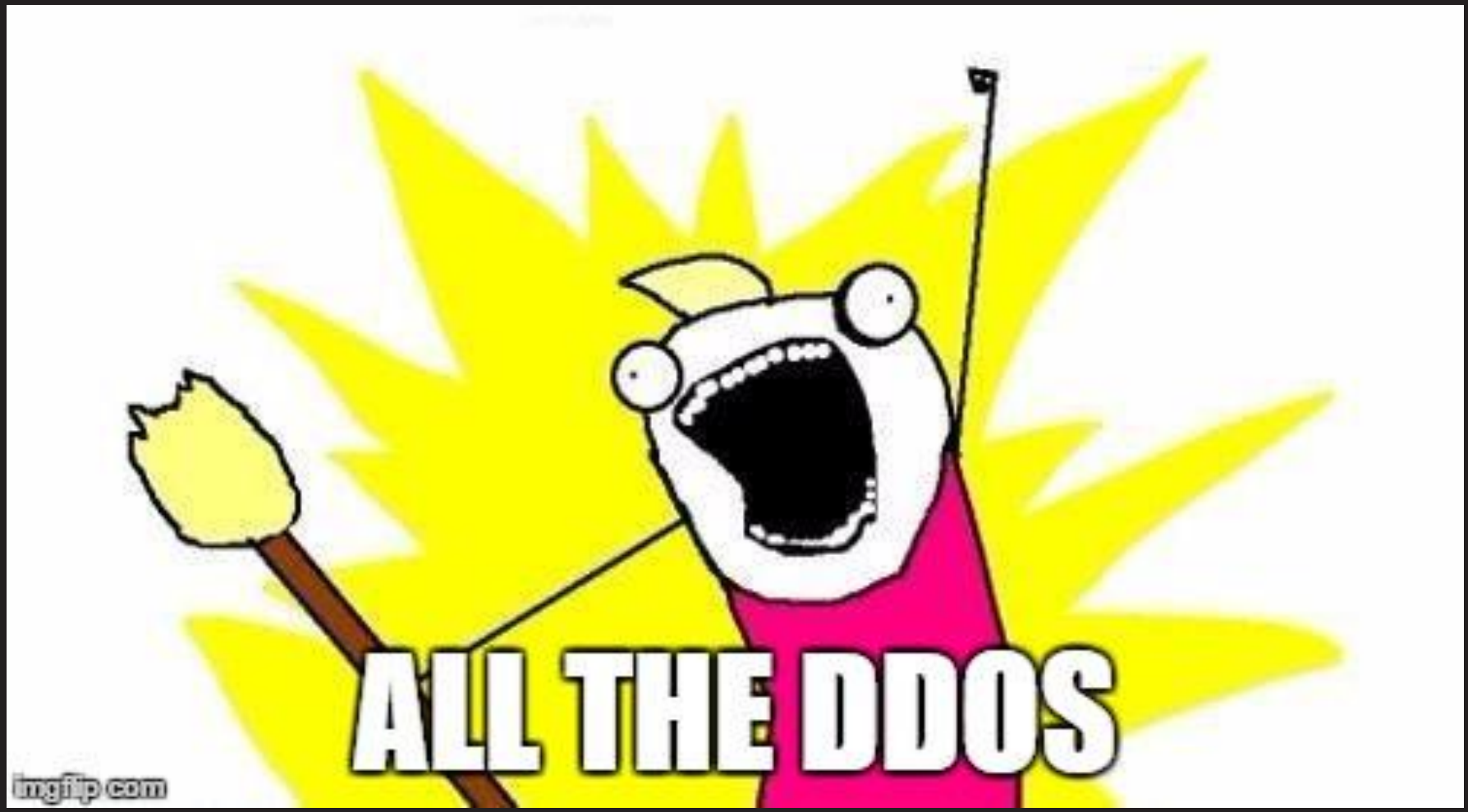
- It’s an attack on the availability of a resource or service



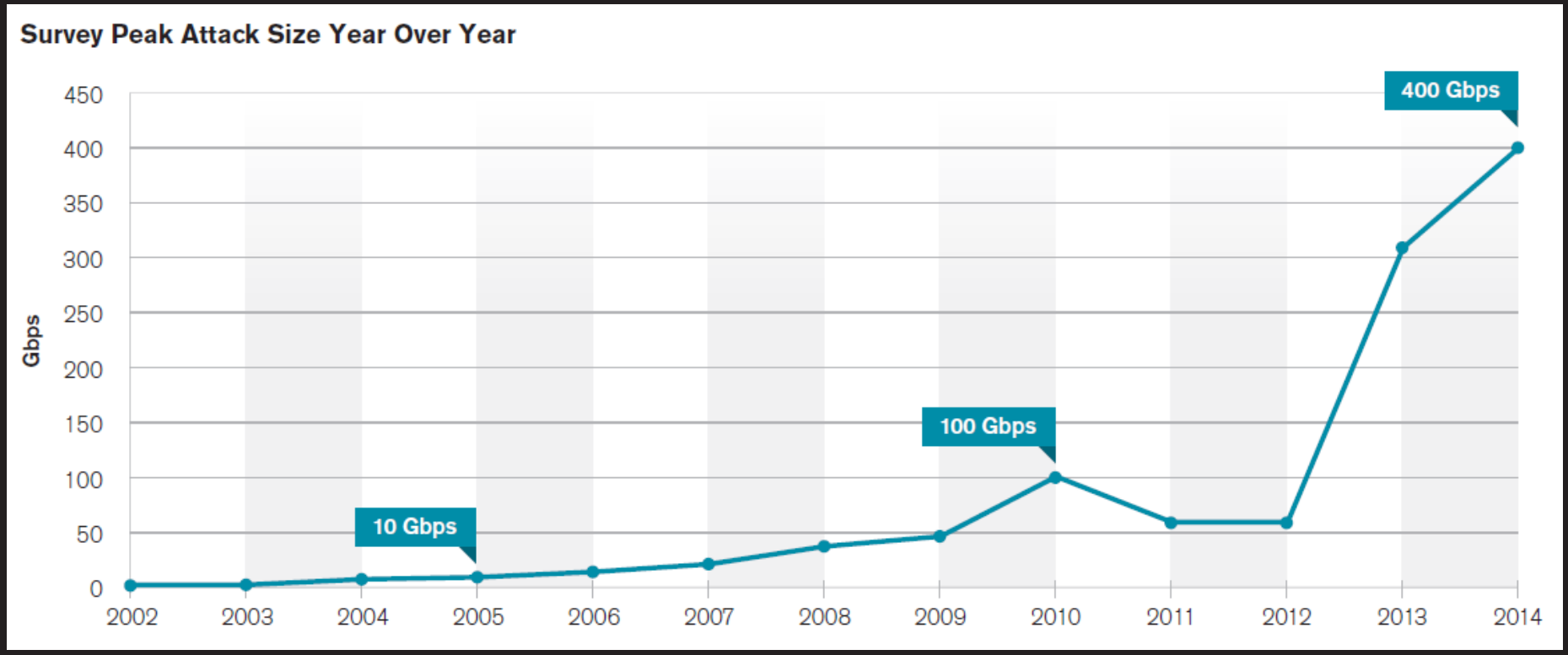
How?

- We'll get to that…

Why?



DDoS attacks are growing!



(Arbor Networks, Inc WSIR 2014)

But…

- Everyone always thinks of DDoS attacks in terms of size

DDoS attacks are growing!

CLOUDFLARE Blog home

The DDoS That Almost Broke the Internet

27 Mar 2013 by Matthew Prince.

g+1 681 Share 336 Like 12 Tweet 11

DDoS attacks are getting worse, as attackers shift tactics and targets

Attackers are using smaller bandwidth attacks to last longer, and do more damage.

By Zack Whittaker for Zero Day | May 19, 2015 -- 15:41 GMT (16:41 BST) | Topic: Security

DDoS attacks that crippled GitHub linked to Great Firewall of China

Whitehat hacker's traceroute wizzardry pinpoints origin of denial-of-service code.

by Dan Goodin - Apr 2, 2015 11:31pm BST

Share Tweet 45

Ryan McLaughlin

Home › News › Security › World's largest DDoS attack reached 400Gbps, says Arbor Networks

World's largest DDoS attack reached 400Gbps, says Arbor Networks

NTP amplification fuelling era of super-massive DDoS

By John E Dunn | Jan 27, 2015

PRIVACY AND SECURITY FANATIC

By Ms. Smith | Follow

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Akamai report: DDoS attacks doubled in Q1 2015, SSDP top attack vector

Akamai Technologies published its 2015 State of the Internet Security report, which says DDoS attacks have more than doubled in the first quarter of 2015.

RELATED

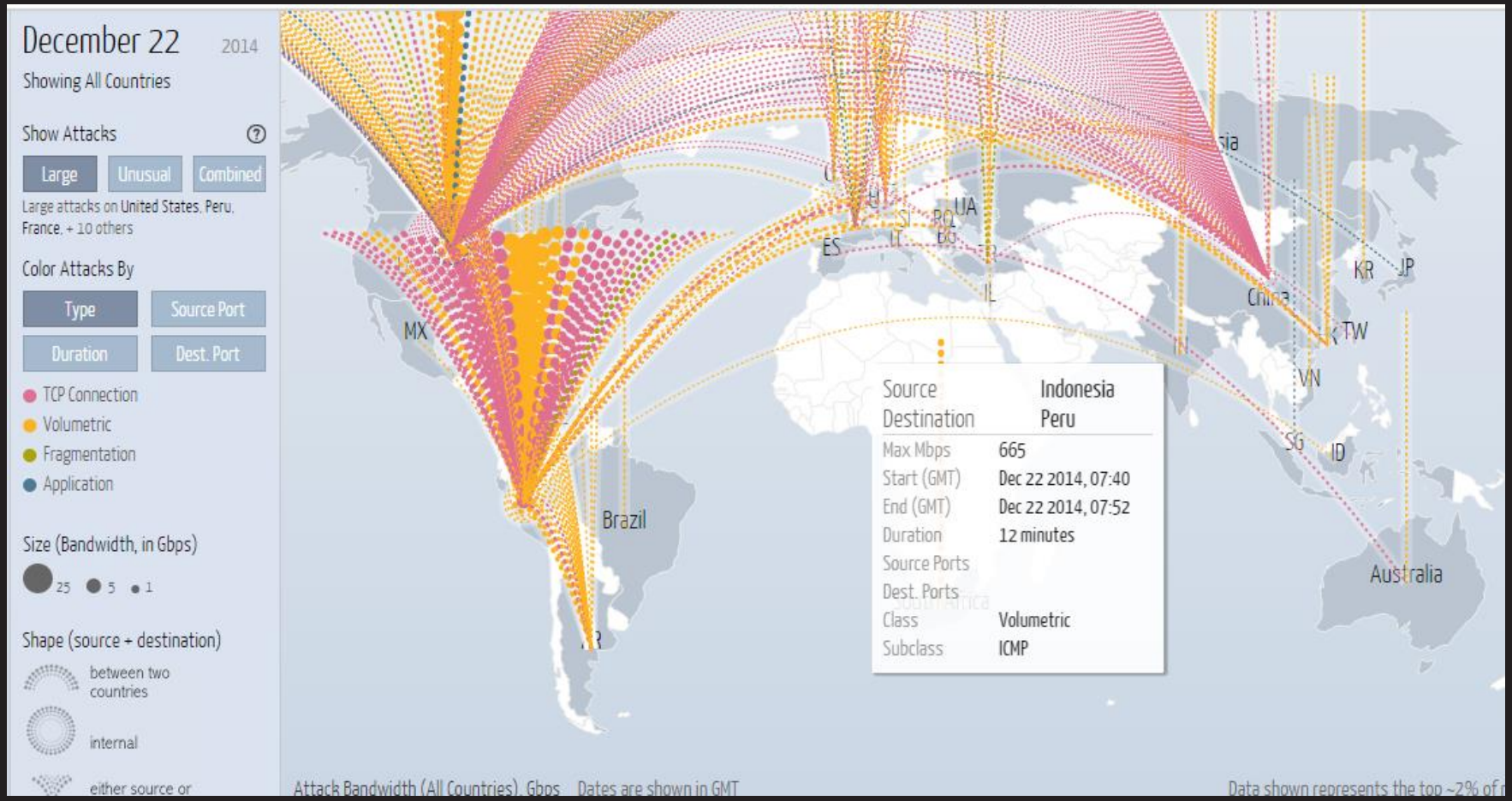
DDoS attacks almost doubled i year: Akamai State of the Internet Security...

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENC

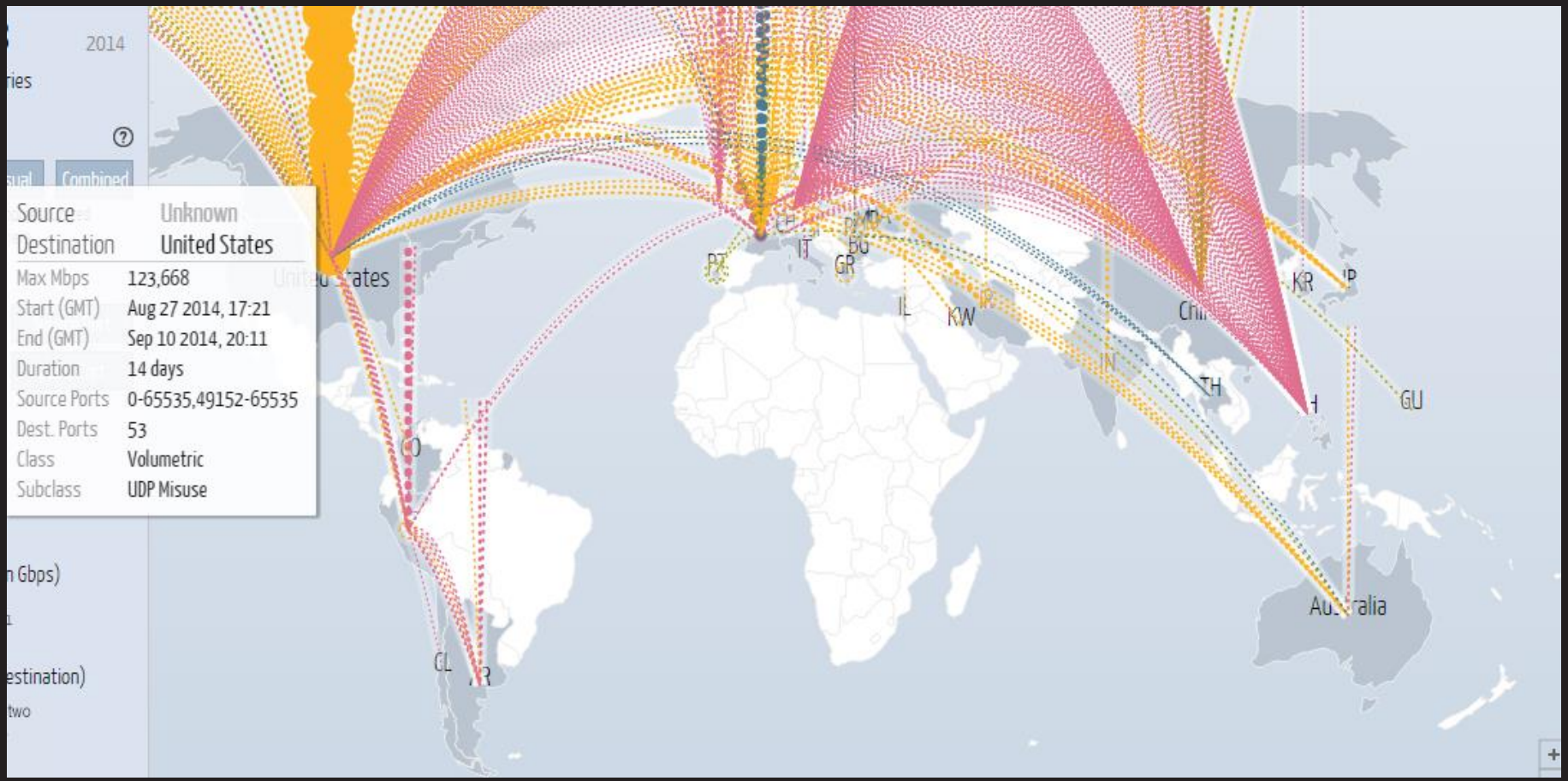
Hackers exploiting wide-open Portmap to amp up DDoS attacks

Careless net adminds leave systems with cleartext trousers down

http://www.digitalattackmap.com/



http://www.digitalattackmap.com/



But…

- Bandwidth/size isn't everything!

- Sometimes a more strategic/tactical approach is more effective ;)
  - Cleverly crafted
  - Stealthy

Historically…

- Bandwidth was limited
  - Harder to attack/defend
- Attacks were misunderstood
  - Firewalls/IDP
  - Lack of dedicated SP's/dedicated hardware
- Outlawed in 2006

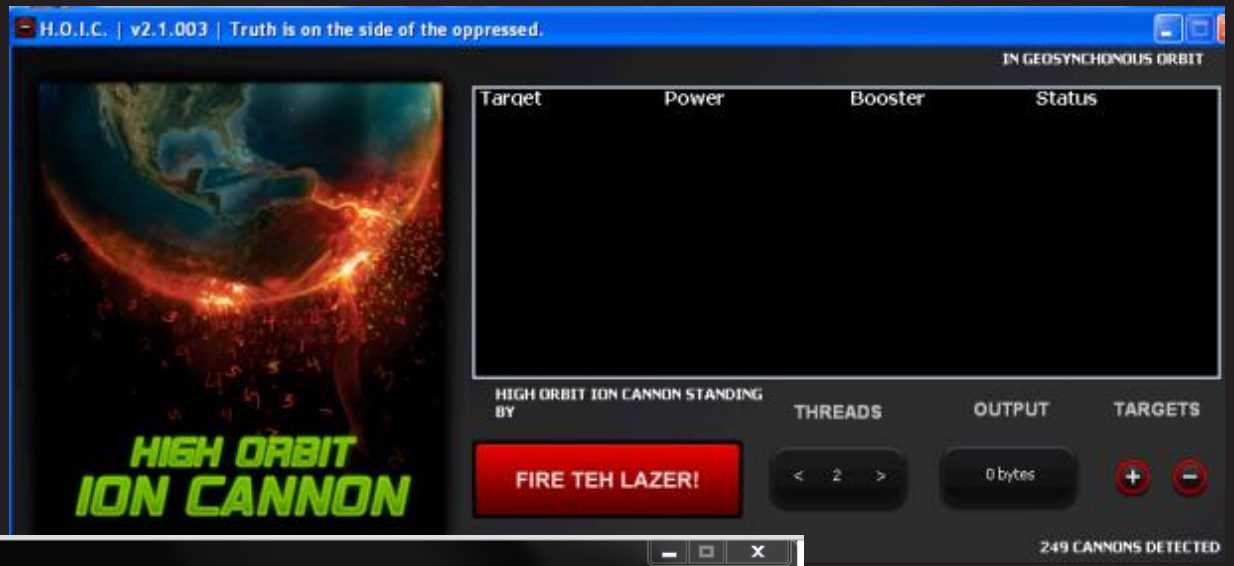
Types of Attacks

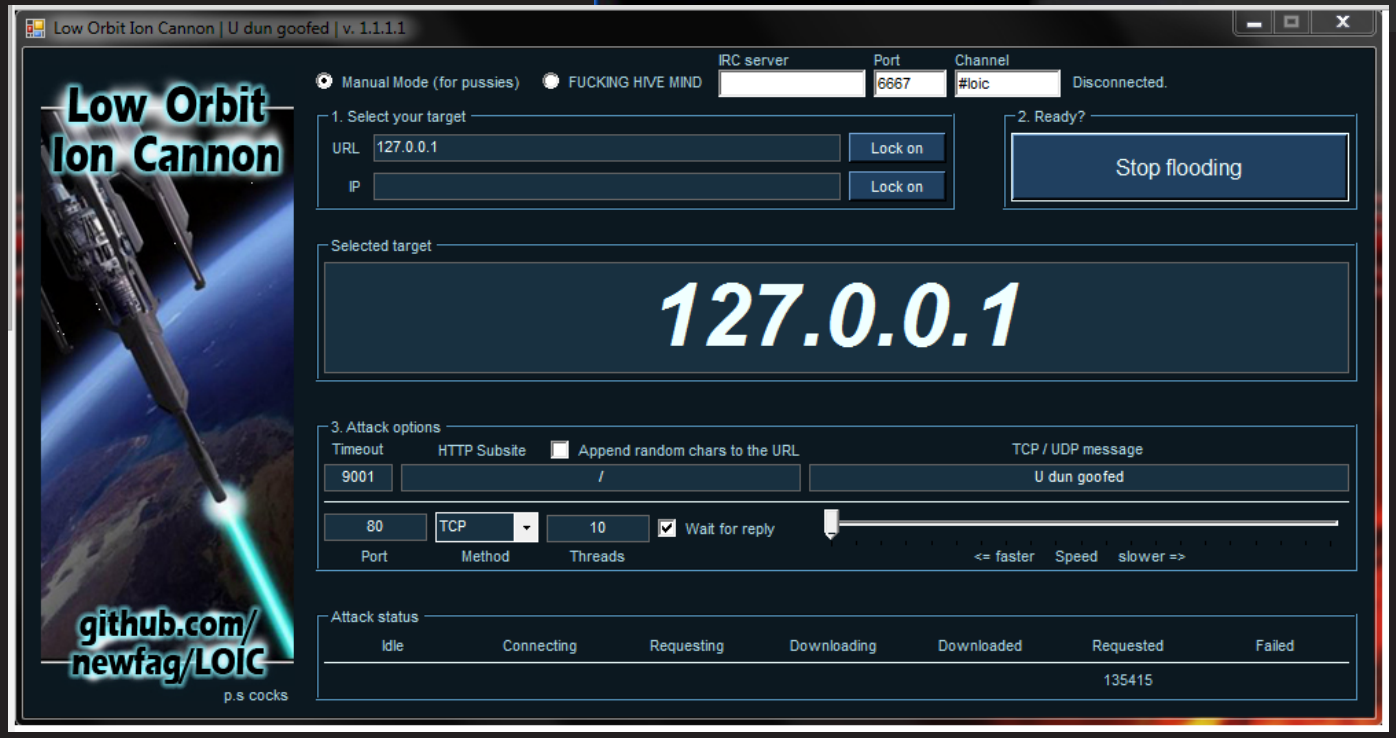
- Volumetric – Bandwidth based
  - ICMP Flood/Smurf/UDP Flood/UDP Amplification
- Protocol Attacks
  - SYN Flood/Sockstress/HTTP Flood
- Application Attacks
  - Slowloris/R-U-Dead-Yet

Volumetric Attacks

- The one we've all heard of!
  - ICMP Floods/HTTP Floods/UDP Floods
    - UDP Reflection/Amplification
- Sheer brute force attacks! (cave-man style)
  - Minimal complexity
  - Utilises massive botnets of compromised hosts
  - Large amounts of bandwidth required

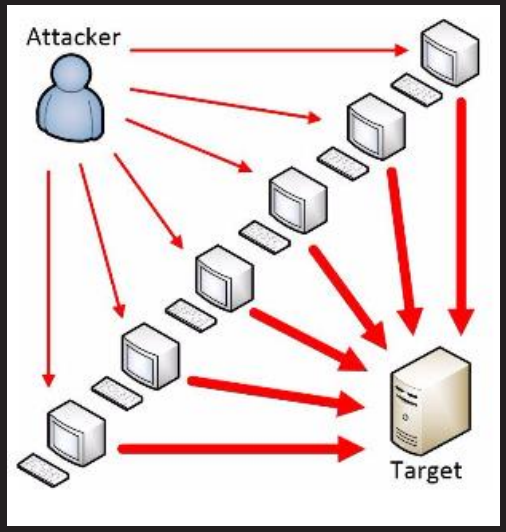
Volumetric Attacks





Volumetric Attacks – how?

- How can we improve on standard volumetric attacks?
  - Reflection
    - Spoof source address so attack is firstly sent to target1, and a response is sent to target2
    - Works best with session-less/stateless protocols (UDP)
    - Hides the source address making attack more difficult to block



Volumetric Attacks – how?

- How can we improve on standard volumetric attacks?
  - Amplification
    - Abuse services/protocols to result in the amplification of traffic
    - DNS - Open recursive DNS resolvers
    - NTP - NTP servers supporting the MONLIST command

Volumetric Attacks – Amplification

Protocol	Bandwidth Amplification Factor
DNS	28 – 54
NTP	556
SNMPv2	6.3
NetBIOS	3.8
SSDP	30
CharGEN	358
QOTD	140

Volumetric Attacks – how?

- Target only has a limited amount of resource!
  - A) Bandwidth Saturation
    - Flood targets' links so no legitimate traffic can get through (most common)
  - B) Resource Starvation
    - Flood targets' infrastructure and overload it such that it cannot deal with legitimate traffic (more complex)

Volumetric Attacks – how?

- If an attacker can generate and deliver more traffic than the target can take, a Denial of Service occurs

```
if sizeof(attacker.traffic()) > sizeof(target.bandwidth()) {
        gameover() //DoS occurs here
}
```

- It's that simple!
- That's why people use LOIC!

Volumetric Attacks – Smokescreen attacks

- More commonly volumetric attacks are being used as part of a smokescreen attack
- Large DDoS attacks are used to divert the attention of companies
- More commonly volumetric attacks are being used as a smokescreen attack
- Large DDoS attacks are used to divert the attention of companies

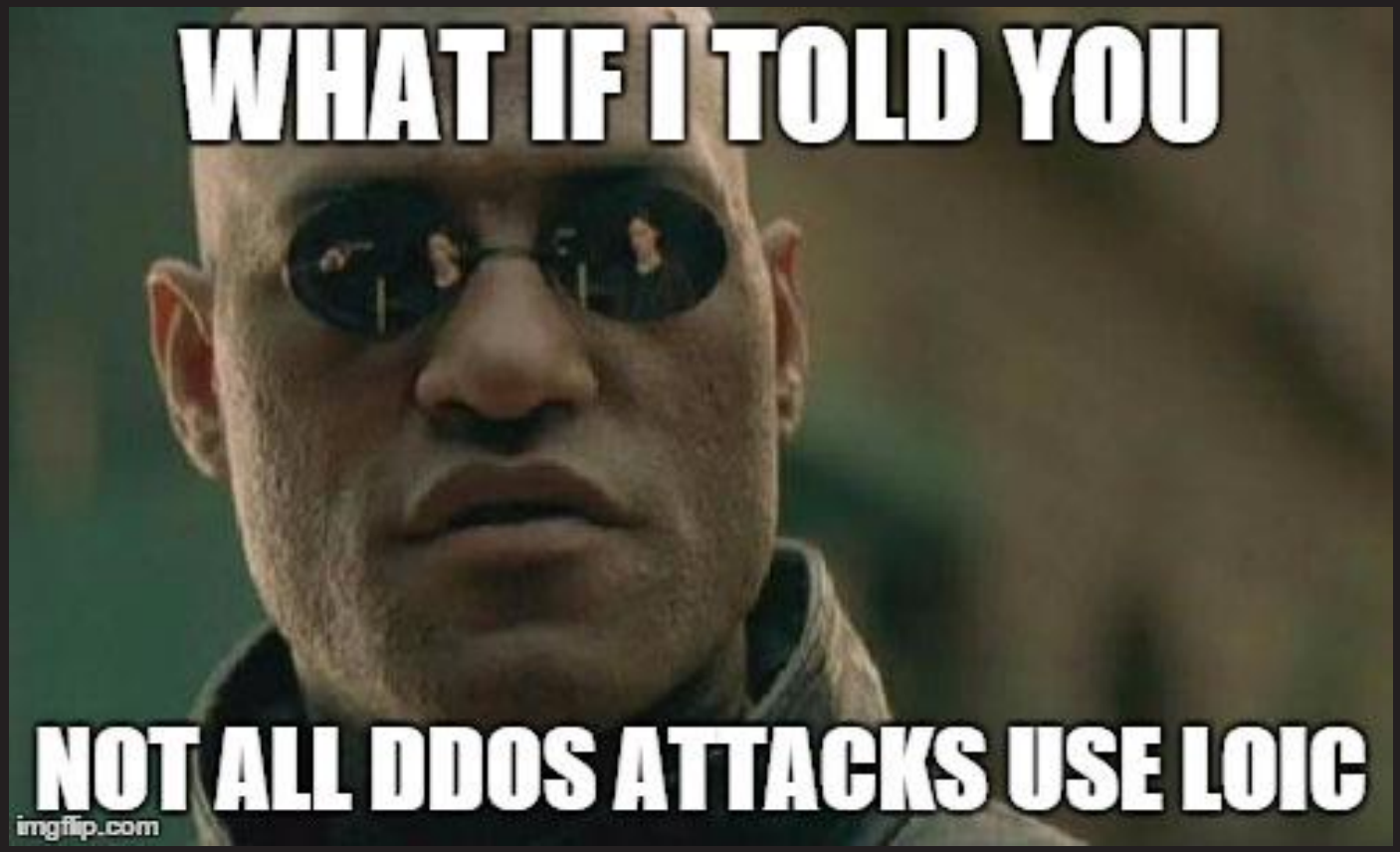
Volumetric Attacks – how?

- So why use any other attack?

  - Volumetric attacks are noisy and easy to spot!
  - With the correct mitigation in place, traffic can be redirected before it floods the target
  - ISP's can easily block or rate-limit traffic
  - Bandwidth is becoming cheaper, so attacks need to be larger for them to be successful!

Alternatives?

- Plenty



Protocol Attacks

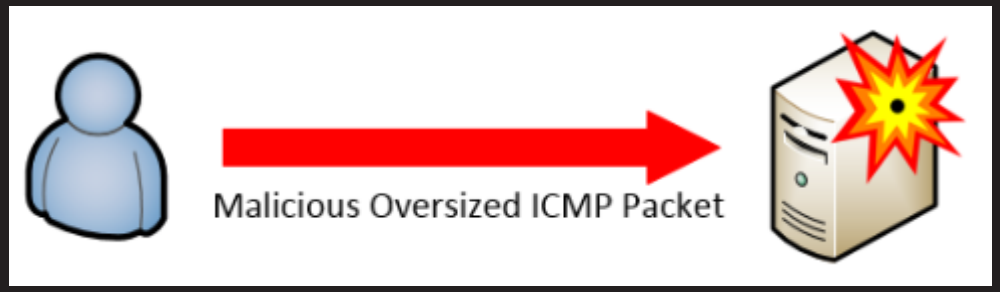
- Network communication relies on an array of different protocols
- Some of these can be abused to result in a DoS occurring

  - TCP SYN Flood
    - Flood a target with TCP SYN packets
    - Results in half open connections
    - Limit reached = no more connections accepted

  - Slightly more complex, less bandwidth required

Protocol Attacks

- If we jump back 15 years:
  - Ping of Death
    - Oversized packet which was commonly mishandled and resulting in the target crashing (65,535+ bytes)



Protocol Attacks

- Sockstress
  - A collection of attacks which utilise raw TCP sockets to establish non-standard TCP sessions
  - Connection Flood Stress - Based on NAPTHA, does not keep track of TCP connection states
  - Zero Window Flood – Advertises a window size of 0, resulting in the target buffering data to memory and leads to memory exhaustion

- Reasonably complex, less bandwidth required

Application Attacks

- Attacks the application protocols themselves – typically layer 7

  - Slowloris
    - Uses partial HTTP requests to fill up the connection pool of a target
    - Carriage Return Line Feed (CRLF) is missed off requests

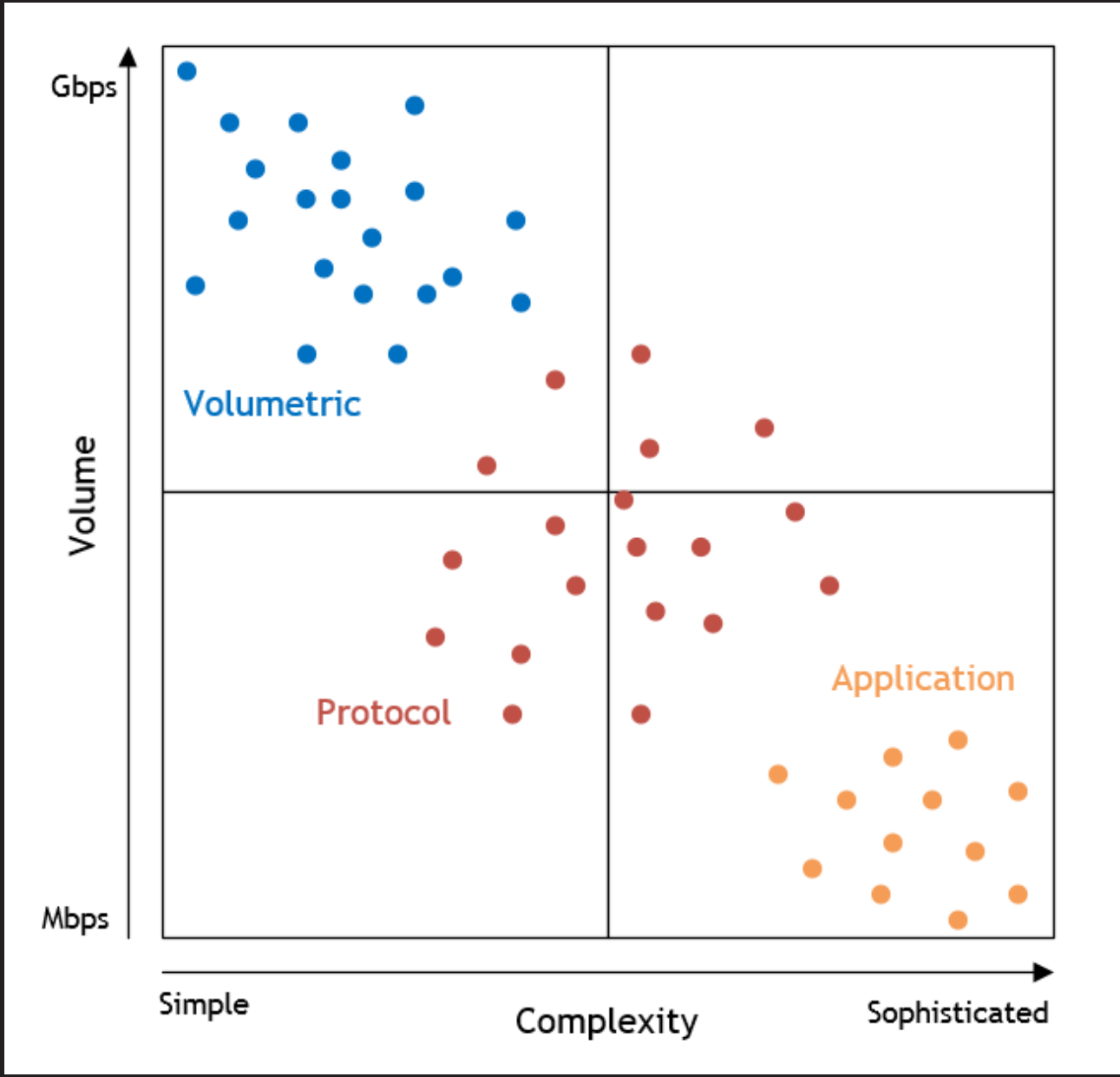
Application Attacks

- RUDY (R-U-DEAD-Yet)
  - Similar to Slowloris, but utilises the HTTP POST method
  - Advertises a long content-length, before drip feeding data holding the session open
  - Repeated until all sessions are exhausted

- Requires minimal bandwidth and very little resource (mobile phone over 2G)

Attack Summary

High level overview of the different attack characteristics



Motives

- Why do people perform DDoS attacks?

- Common presumptions
  - Extortion – profit
  - Smokescreen Attacks
  - Hacktivism
  - Script Kiddies? (Targeting online games/generic websites)


SO YOUR TELLING ME
ATTACKERS WILL DDOS ME AND DEMAND MONEY
imgflip.com

Interestingly…

Attack Motivations

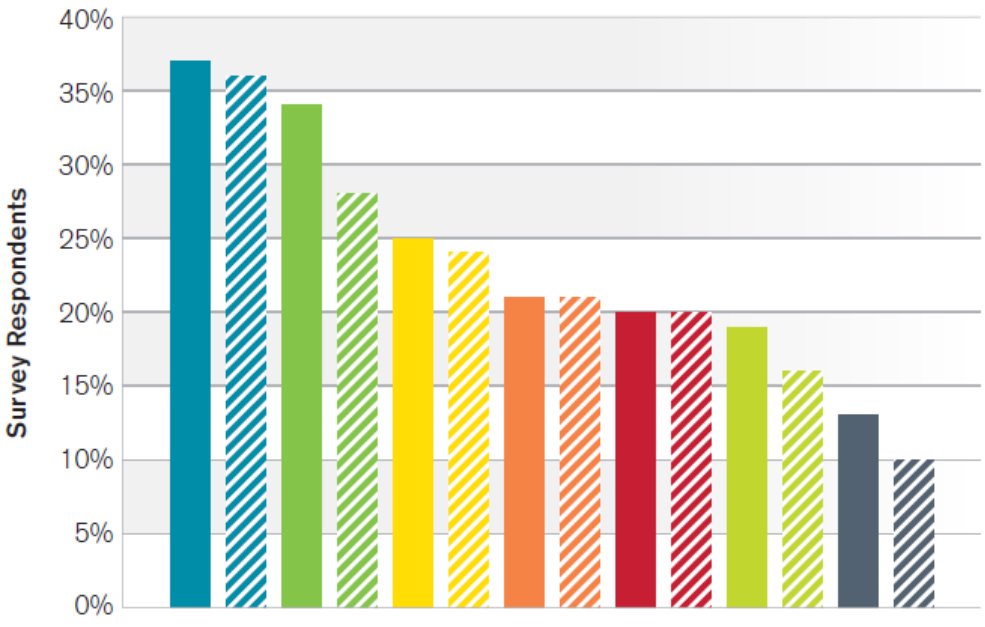


Figure 26 Source: Arbor Networks, Inc.

- **37%** Nihilism/vandalism
- **36%** Online gaming-related
- **34%** Political/ideological disputes (i.e., WikiLeaks/Anonymous, nationalism, religious controversy, etc.)
- **28%** Criminals demonstrating DDoS attack capabilities to potential customers
- **25%** Social networking-related (i.e., IRC, chat networks, Facebook, Twitter, Google+, etc.)
- **24%** Online gambling-related
- **21%** Misconfiguration/accidental
- **21%** Inter-personal/inter-group rivalries (i.e., individual disputes, schools, sports teams, etc.)
- **20%** Criminal extortion attempt
- **20%** Financial market manipulation
- **19%** Diversion to cover compromise/data exfiltration
- **16%** Flash crowds
- **13%** Competitive rivalry between business organizations
- **10%** Intra-criminal disputes

(Arbor Networks, Inc WSIR 2014)

Prevention/Mitigation

- Depends entirely on the type of attack!

- Best practises!
  - Implement BCP38/RFC2827 – Source IP address spoofing
  - Not relying on traditional defences!
  - Defence in Depth

Prevention/Mitigation

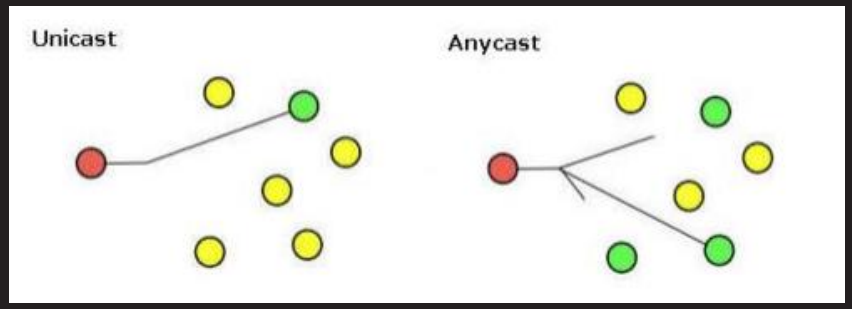
MWR LABS

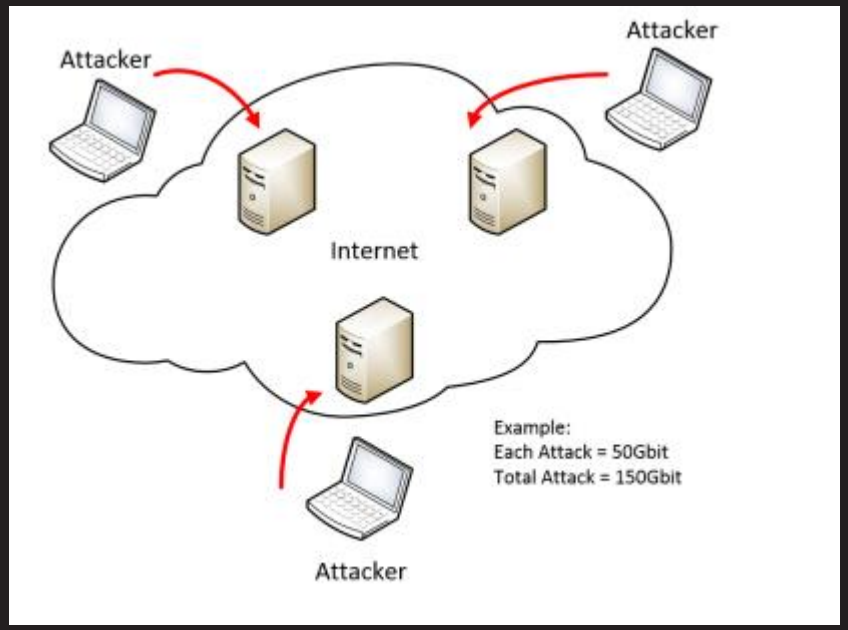
Volumetric Prevention/Mitigation

- Application Reverse Proxies
  - Front end for applications (proxies connection)
- Load Balancing
  - Global/Local load balancing
- Dedicated DDoS Mitigation/Prevention Appliance
  - Lots!
- Route Blackholing/Sinkholing
  - Re-route traffic for analysis or to drop it
- IPv4 Anycast

Volumetric Prevention/Mitigation – IPv4 Anycast

- Single IP assigned to multiple hosts
- Traffic is routed to nearest instance
- Allows for volumetric attacks to be spread across geographical locations





Protocol Prevention/Mitigation

- Firewalls - packet filtering
  - Deep packet inspection
- IDP – signature analysis
- Application Reverse Proxies
  - Understand application requests
- Host based controls
  - Apache/IIS Modules
- Traffic statistical analysis

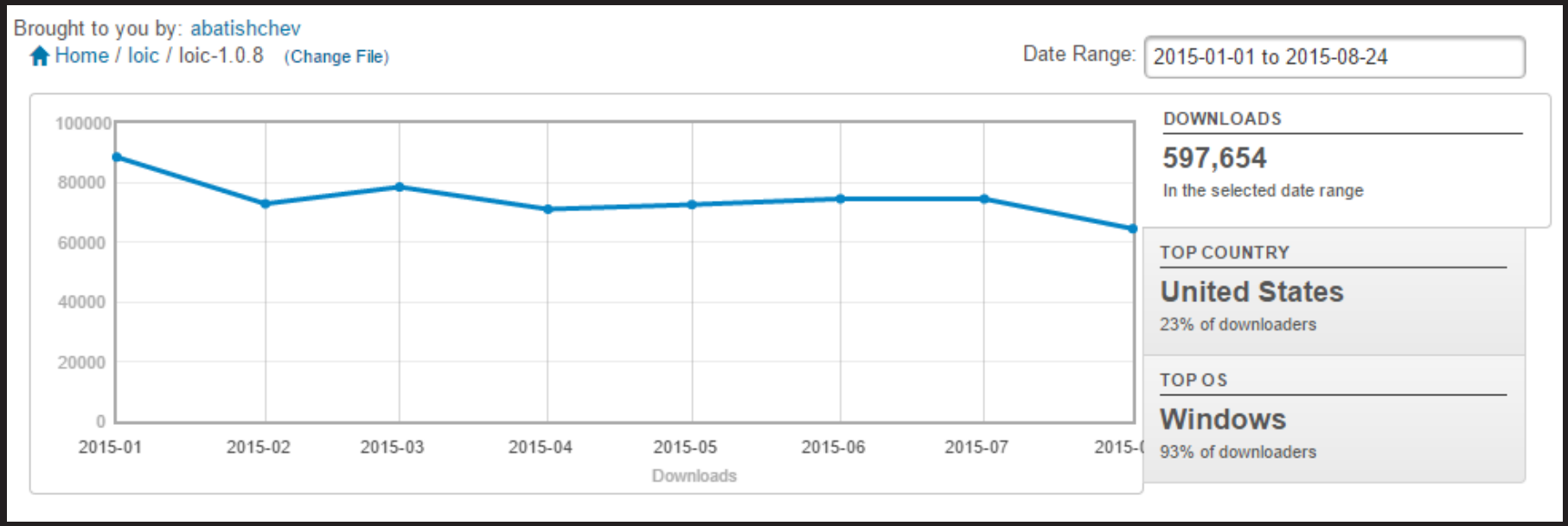
Application Prevention/Mitigation

- Traffic statistical analysis
  - Traffic profile analysis – bursty/probes
- IDP – signature analysis
- Firewalls - packet filtering
  - Deep packet inspection
- Application Reverse Proxies
  - Understand application requests
- Host based controls
  - Apache/IIS Modules

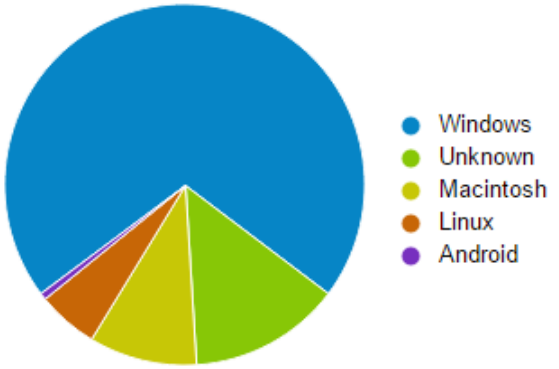
Defence in Depth!

Who uses LOIC these days anyway?

- 600,000 downloads from sourceforge so far this year!



Mac and Linux users too apparently



DOWNLOADS

660

In the selected date range

TOP COUNTRY

United States

16% of downloaders

TOP OS

Windows

70% of downloaders

Operating System	Downloads
Windows	466
Unknown	90
Macintosh	64
Linux	36
Android	4
	660

15%

MWR LABS

Summary

- Not all DDoS attacks are the same!
  - Understand the difference!
- DDoS Attacks are going to keep growing
  - Both in complexity and in size!
- Fully understand the different attacks to be able to properly mitigate each of them.
- Never, ever give in to DDoS threats and pay
  - Attacker is still likely to perform the attack after receiving payment

Future Work

- Further explore use of IPv4 Anycast with TCP traffic
- Explore further popular protocols that can be exploited
  - Fuzzing
  - IPv6 (little more fresh)
- IOT – What network defences are being built in
- Case Study – “Use of DDoS attacks in Cyber Warfare”
  - DaaS/Booter Services

Thanks to…

- Sam Brown – for using his face (@_samdb_)
- Alexios Mylonas – University tutor who helped guide my research

Questions?

@MattWatkins93 | @mwrlabs