Distributed Denial of Service (DDoS)

Thomas McDonald

Associate Director – Has +25 years experience in the IT industry (specialising in computer security). Worked for many Global Corporations and in several National Defense Organizations as well as a large number of SME's across all industry sectors.

Akhilesh Mathur

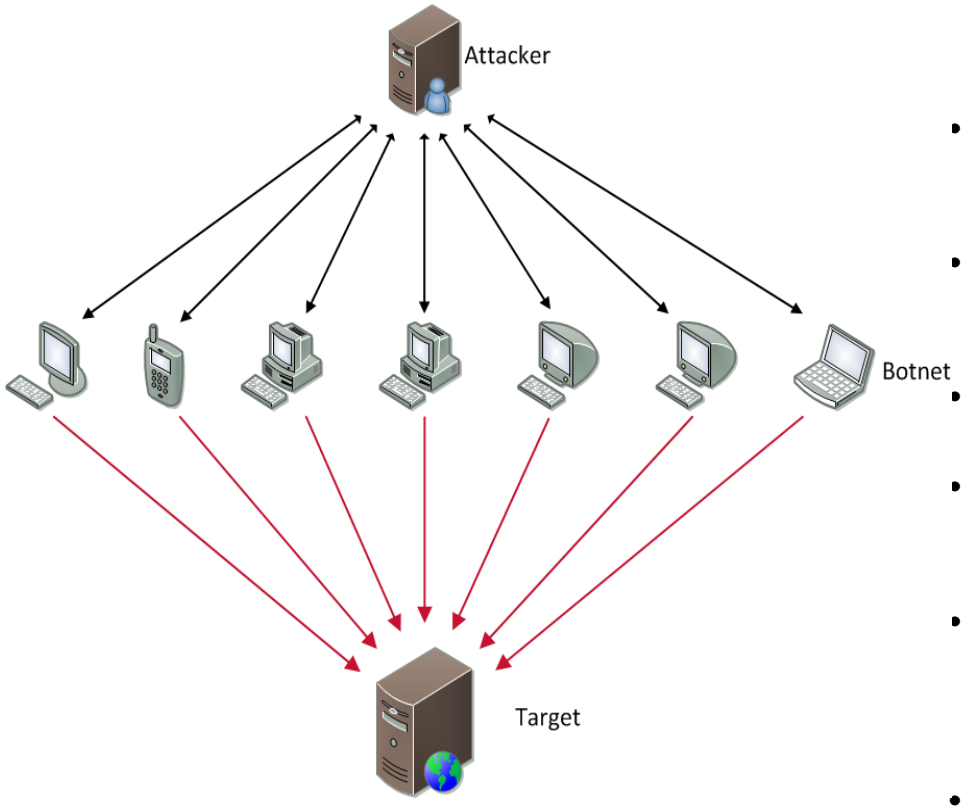
Technical Account Manager – Has 9 years experience in IT security, specialising in DDoS testing using NCC Group's in-house developed botnet platform. Has scoped and delivered numerous DDoS exercises for customers, as well as providing follow up analysis of results and remediation plans.

Agenda

- DDoS: Why should you be concerned?
- Common Defence Approaches
- The Evolving DDoS Threat Landscape and Defence Failings
- Our DDoS Assured Test Findings

Please feel free to ask questions on the live chat at any time

What is DDoS – A Quick 101



A hacktivist tool of choice

- A DDoS attack is an attempt to make a target system or service unavailable for its intended users or purpose
- First reported appearance against Yahoo in 2000
- DDoS Attacks are for extortion, political and ideological disputes, or just for fun
- An increasing plague across the Internet
- Spamhaus attack in 2013 achieved 300Gbps and slowed down the Internet
- In 2014 a 33% larger attack (400Gbps) was reported by CloudFlare against an unreported target
- DDoS attacks can last anywhere from a few minutes to a few weeks

5 Reasons to be Concerned

nccgroup
freedom from doubt

Costs per incident dependent on business

Longer a DDoS lasts the more it costs a business

Long term reputational damage more devastating than the financial implications

Can be used as a smoke screen for targeted hacking attempts

40% of businesses estimate DDoS financial loss to be $1m+[1] per day.[2]

[1] Equivalent to £620,000+

[2] http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

Who is a Target?

nccgroup
freedom from doubt

Critical threat that your business needs to understand

Do your employees know what to do when a DDoS attack hits?

Do you know how they would react?

Do you know what would be the fallout?

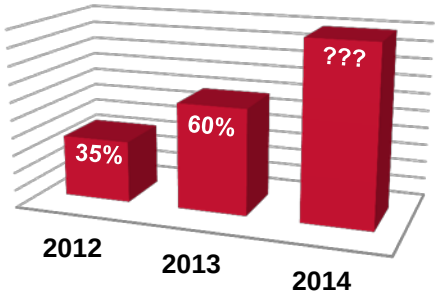
Do you know the risk associated with this threat?

Do you know how you would deal with your customers?

Remember you cannot stop someone from targeting you, all you can do it mitigate the risk

Defense Common Approaches

1. Do nothing
   - No longer an option!
   - Nearly twice as many business attacked in 2013 than in 2012
   - A trend which is continuing to increase into 2014



Businesses attacked each year

2. Utilise your current infrastructure to its best potential

In-House Solutions

Advantages

In-house solutions deployed as a first resort
Easy and cost effective

Disadvantages

Dependent on in-house technical knowledge
Not always effective against evolving attacks
Can cause additional bottlenecks in volumetric attacks

Next-gen firewalls

Switches

Intrusion Protection System

Defenses – Outsourcing Approach

When companies lose $50k per hour this is the tipping point for investing in purpose built solutions [1]

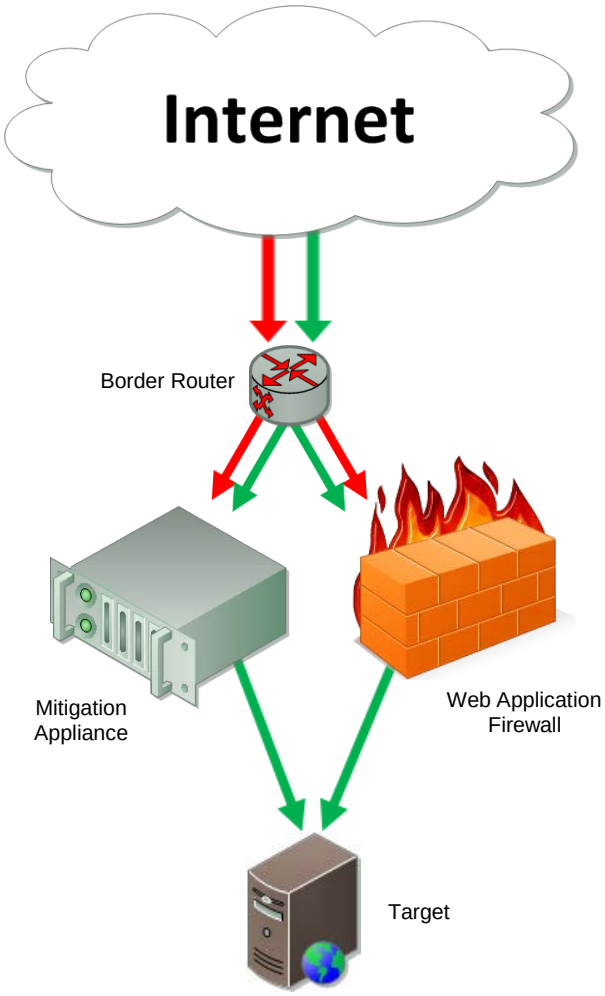
Why?

Outsourcing to relieve workforce burden → Dedicated solutions more effective → Managed Services allows for external expertise → 24/7 monitoring

Often best used as a multi-tiered approach with in-house defences

[1] http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

Defense – Appliance/WAF Solutions



Appliance/Web Application Firewall Mitigation

• Devices employ deep packet inspection on incoming traffic •

• Can be more cost effective •

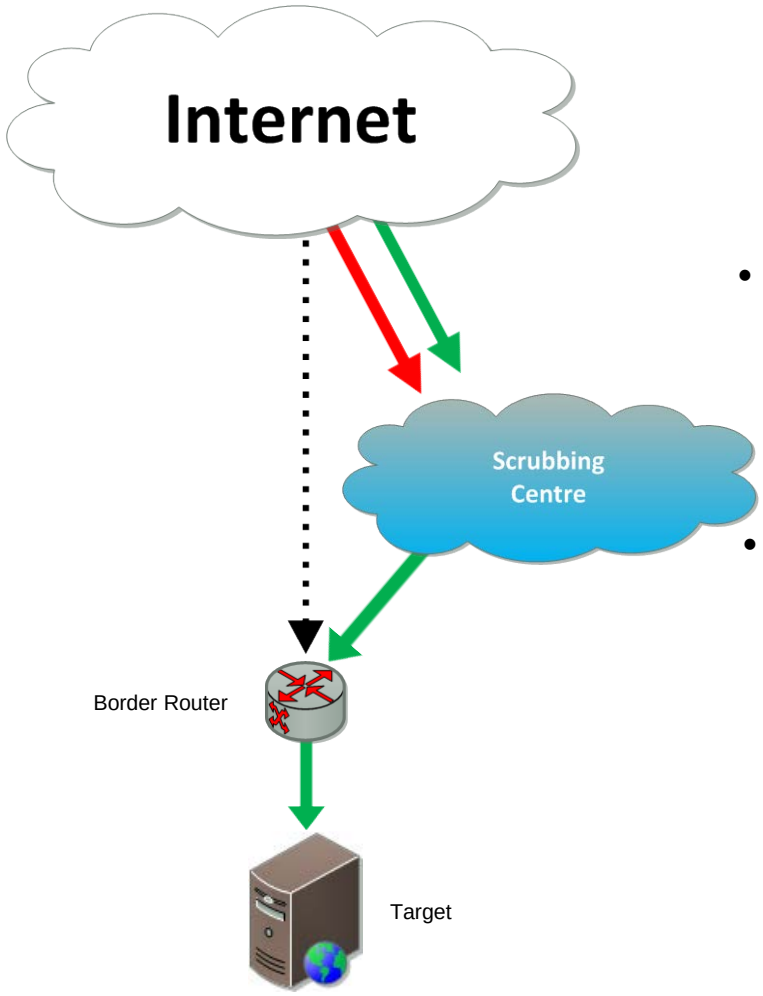
• Can be easier to use and customised to suit target •

• Can allow control over mitigation at SSL encryption endpoints •

• Can be produced in-house •

• Can be limited by system bandwidth capacity •

Defense – Cloud Solutions



Cloud-based Mitigation

- Can stop attack traffic ever reaching target network
- Can be either an always on or activated service
- Can absorb huge amounts of bandwidth
- Can employ additional managed human resources
- Highly scalable
- Generally more expensive

Volumetric Threats - Examples

- Size of attacks have increased over time
- Peaks over +300Gbps when new techniques are discovered *(DNS Amplification, NTP Reflection, etc.)*

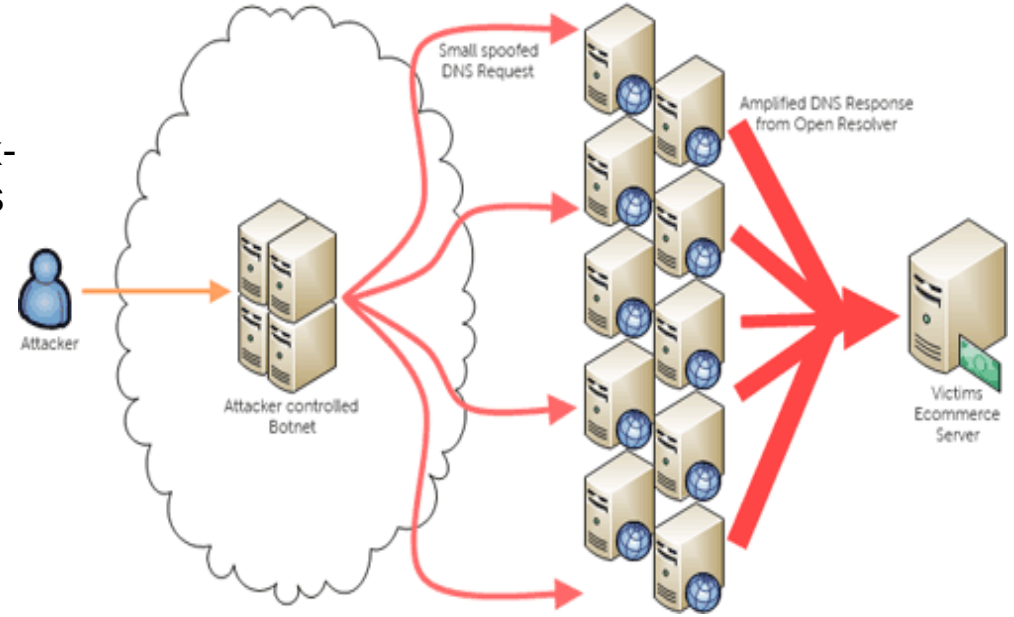
	BPS
2012	• 100.84Gb/sec, destination unknown • Lasted 20 mins
2013	• 245Gb/sec (TCP SYN) • Lasted 16 mins
2014 (so far)	• 325Gb/sec (NTP), France • Lasted 4 h 22 mins

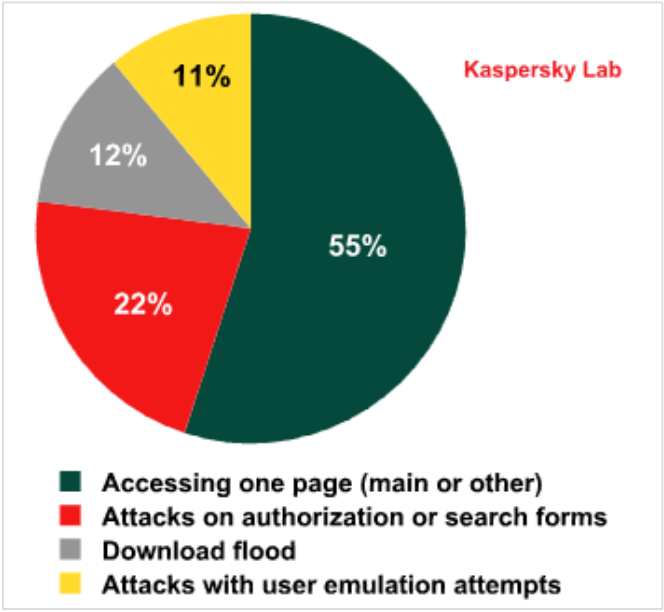
Arbor Networks Q1 2014 report

Evolving DDoS Threat Landscape

nccgroup
freedom from doubt

Many current attacks are pure network-based (e.g. DNS Amplification) but this is changing.



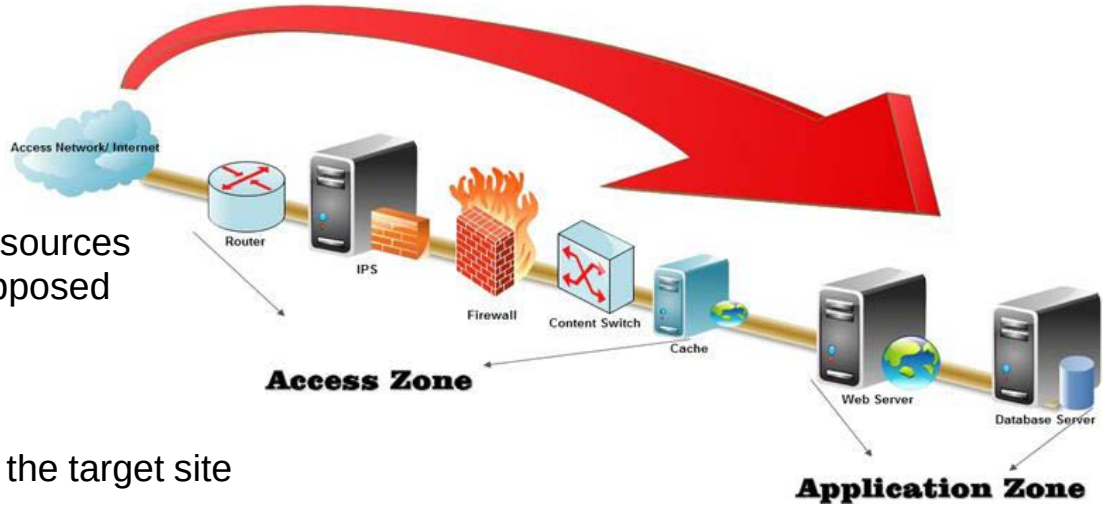


- Volumetric network attacks are starting to give way to ‘low and slow’
- Application layer attacks get under the radar

Application Layer Attacks

Characteristics of a Application Layer attack:

- Look like legitimate user requests
- Harder to detect than network layer
- Designed to consume application resources (e.g. database, CDN systems) as opposed to network bandwidth



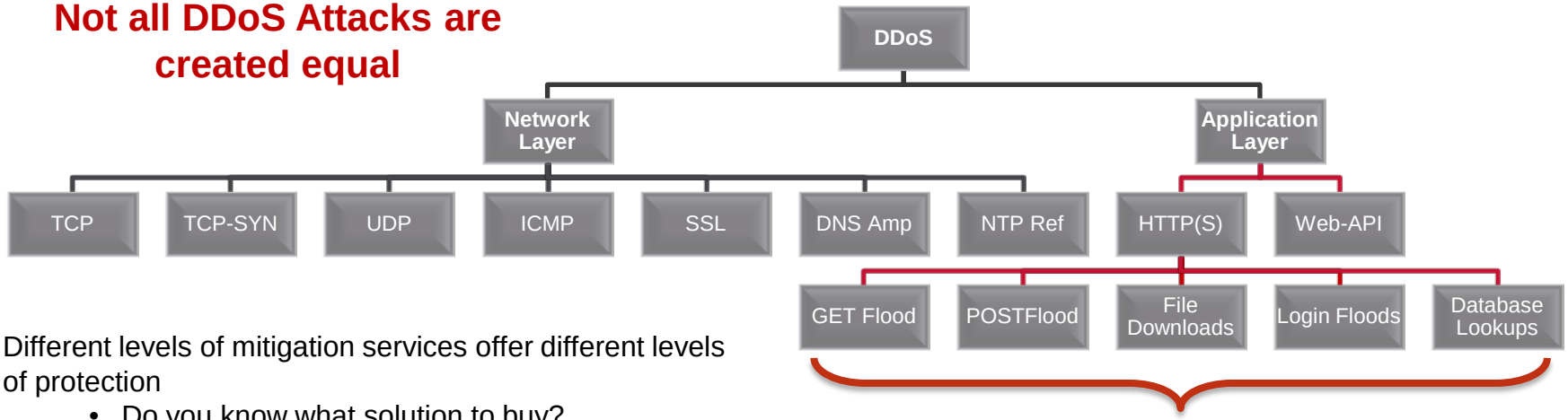
Hit specific features ('pinch points') of the target site

- Contact us forms
- Site search tools
- User registration pages
- Large file downloads
- Streaming (e.g. RTMP)
- SSL Encrypted functionality (deep packet inspection bypass)

Network traffic and bandwidth protection is often ineffective against Application Layer attacks

Common Failings

Not all DDoS Attacks are created equal



Different levels of mitigation services offer different levels of protection

- Do you know what solution to buy?
- Do you know the capabilities and limitations of the solution you have purchased?
- Does your mitigation team know how to deploy different protections when under attack?

Is what you purchased best suited for your business?

Application Layer attacks on the rise

Increase complexity of websites offers a range of attack vectors.

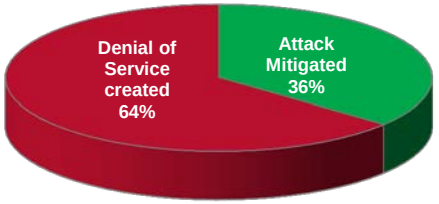
In 72% of failed DDoS Assured exercises mitigation solutions could not protect against Layer 7 HTTP(S) Floods

Statistical data gathered from +50 customer test scenarios

General Test Findings

Statistical data gathered from +50 customer test scenarios

64% of our DDoS Assured tests highlighted defence failures despite the mitigation being operational



In **21%** of tests, related infrastructure and services were also impacted as a result.

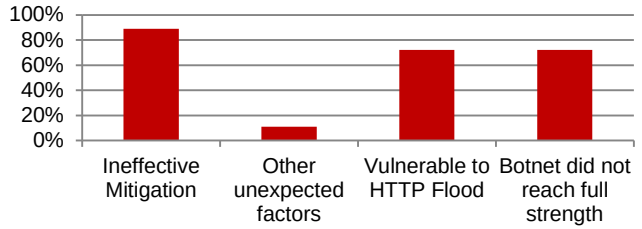
In 89% of failed DDoS Assured exercises ineffective mitigation solutions were to blame

In many cases customers were unaware of exactly what level of protection their mitigation SLA's provided

11% of failed DDoS Assured exercises were due to unexpected factors:

- Incorrect mitigation configuration
- Incorrect features enabled
- Unexpected bottlenecks in infrastructure

Failed Test Statistics



In **72%** of failed DDoS Assured exercises our botnet did not reach full strength.

92% of these were the more advanced HTTP(s) floods.

Real Examples

The below highlight two of many DDoS test examples where the outcomes were unexpected and, in the second case, had a devastating impact on adjacent systems.

EXAMPLE 1

Customer Business: Major Bank

3rd Party Stakeholders: ISP Mitigation Provider

Details: With all preparatory work having been completed the DDoS Assured test was pulled last minute due to the DDoS mitigation solution having been identified to not be correctly configured to protect the target systems during final checks by the ISP. Until the exercise was about to start this service had been believed to be protecting a live environment.

EXAMPLE 2

Customer Business: Major Bank

3rd Party Stakeholders: Dedicated Mitigation Provider

Details: During a routine network flood a standard border router configuration caused an unexpected and devastating failure in the device. Subsequently all outgoing internet communication was lost for that portion of the business. Additional failings were found with the DDoS mitigation's ability to protect against a sophisticated Application Layer attack. We run regular retests for this customer to significantly improve their ability to withstand various DDoS attack vectors.

Testing & Verifying

NCC Group's DDoS Assured services

- **DDoS Advisory**

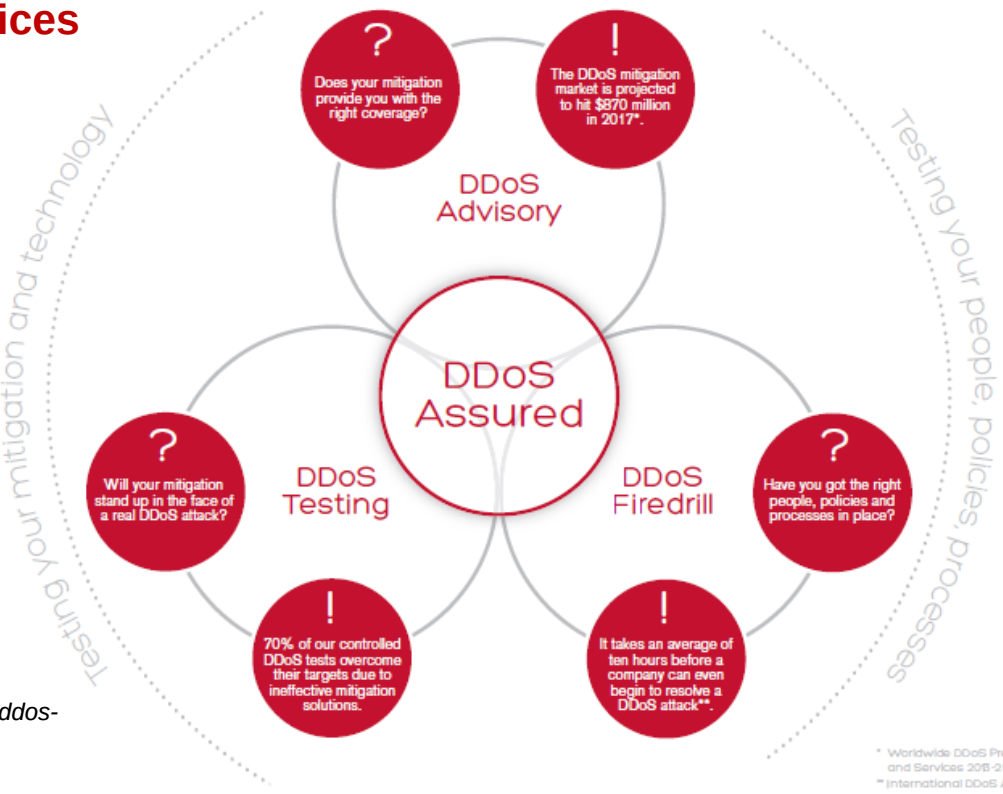
  Audit your businesses policies and procedures

- **DDoS Fire Drill**

  Test your people in the event of an attack

- **DDoS Testing**

  Test your technological solutions



Whitepapers

- **Assuring Your DDoS Defences**

  https://www.nccgroup.com/en/learning-and-research-centre/white-papers/assuring-your-ddos-defences

- **The New DDoS Battleground**

  https://www.nccgroup.com/en/learning-and-research-centre/white-papers/application-layer-attacks-the-new-ddos-battleground

Top 5 Lessons Learned

nccgroup
freedom from doubt

- Understand key differences between DDoS attacks vectors (network/application)
- Review your business' policies and procedures
- Ensure your staff are adequately trained
- Know your DDoS mitigation's capabilities (bandwidth is not always the failing point)
- Test your DDoS response strategy and technology regularly

Don't wait until you are attacked to see how you would react

nccgroup
freedom from doubt

Questions?

Presentations live on our site (www.nccgroup.com)
now along with whitepapers