Distributed Prevention of DoS

Collaboration is key

DoS Background

What is a Denial of Service attack?

- An attempt to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity
- Effects the availability and utility of computing and network resources
- Attacks can be *distributed* for even more significant effect
  - L7 attacks can be time consuming and involve high levels of manual process to ensure live users remain enabled
- The *collateral damage* caused by an attack can be as bad, if not worse, than the attack itself
- Attacks can be sustained for months

What is Denial of Service?

- The main point:

DoS is an Outage!

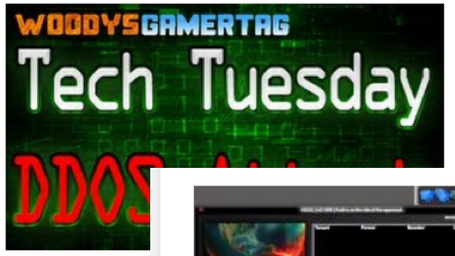
- Slow starvation or volumetric (simple attacks are still hitting the headlines)

DoS vs. DDoS?

- One system is sending the traffic vs many systems are sending the traffic

- Does it really matter?
- …in what cases?

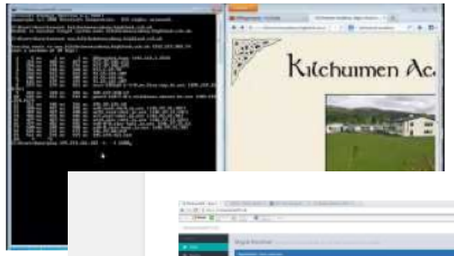
Youtube



DDOS Attacks Explained - Tech Tuesday
by WoodysGamertag
1 year ago • 136,503 views
Join Team Gamertag ▻ http://bit.ly/TeamGamertag Scuf: http://scufgaming.com

How to DDoS w/ Info
by TheHacker0007
2 years ago • 172,979 views
Hope you liked the video! :) If your anti-virus says it a virus, its a "hacking" tool. All

What happens when you DDoS a twitch streamer
by Dat Hacker
7 months ago • 19,715 views
I'll show you what happens when you **DDoS** a twitch streamer, for if you were wondering.



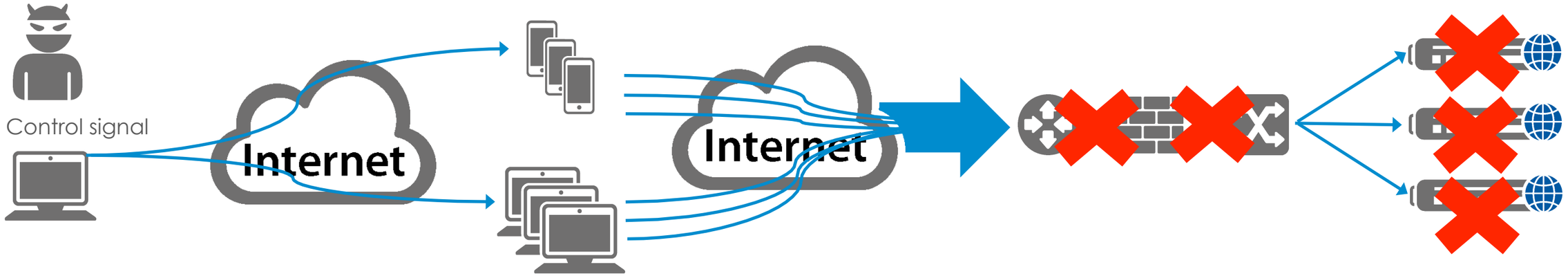
DDoS is not hard. (The noob way)
by MNG Rampant
2 years ago • 394,688 views
Don't be amazed by a random who can **DDoS** something. The easiest way to **DDoS** a

How to DDoS someone using Skype
by Sam Luscombe
5 months ago • 33,066 views
made with ezvid, free download at http://ezvid.com Quick video explaing how to **DDos** Somone using Low Ion Orbit Cannon or a ...
HD

Botnets & C&C Servers

- **Botnet** – (Zombie Army) A collection of internet connected programs to perform certain tasks. The can be used to send spam or launch Ddos attacks.

- **C&C Servers** - A botnet's originator (known as a bot herder or bot master) can control all these compromise programs to basically send bad traffic to a destination machine.



x2000 compromised hosts

Key Considerations For DDoS Protection

- Scalability - How many resources may be brought to bear?
  - Different levels of scale depending on positioning
- Flexibility - What types of attacks may be mitigated & what techniques may be used?
- Specialized Resources, Expertise & Focus - Who or what is analyzing the attacks, what resources are available, and who has the responsibility to coordinate the defense?
- What is the full breadth of tools at your disposal?
- Cost, not just monetary, but collateral damage (Brand damage)
- Insurance or Loss?

Contributing factors (what can you influence?)

- Not patched Content Management Systems (CMSes)

- Available reflectors (DNS, NTP, SSDP)
- …with ability to amplify

- More bandwidth available

- Unpatched embedded devices – version control awareness
- Misconfigured nodes
- Vulnerable network elements i.e. CPEs
- Weak security

Reflective attacks

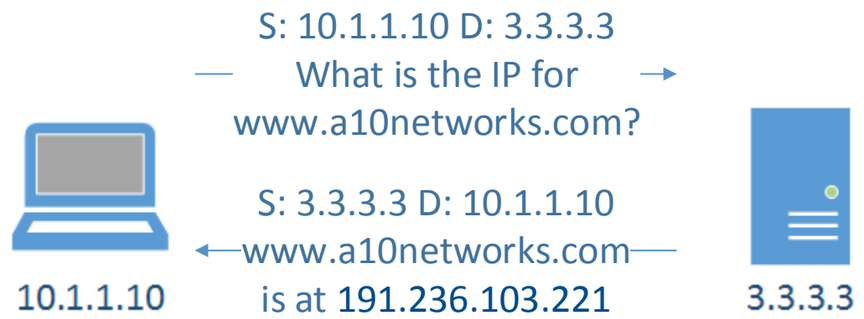
- Attacks where the an unwilling intermediary is used to deliver the attack traffic
- The attacker would normally send a packet with a forged/spoofed source IP address to the intermediary. The forged address is going to be the one of the target. The intermediary will deliver a response which will go to the target instead of the attacker
- Note to audience: think what protocols we can use for that?

Reflector types

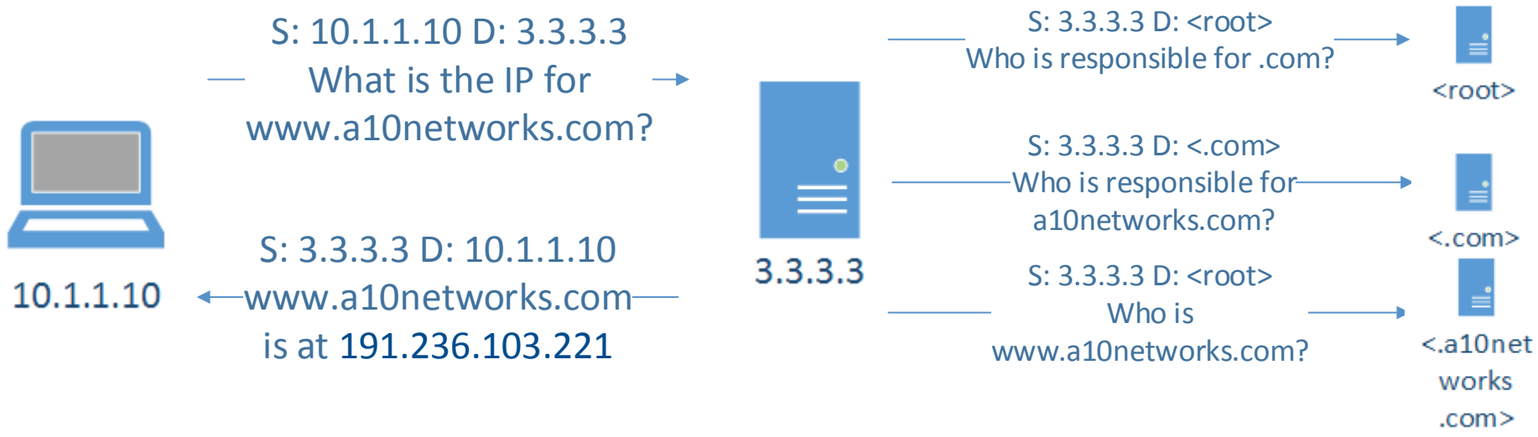
- The ones that are of interest and provide reflections are:
- DNS
- NTP
- SNMP
- SSDP
- Other UDP???

What is DNS resolution?

- The process of mapping: www.a10networks. com => 191.236.103.221

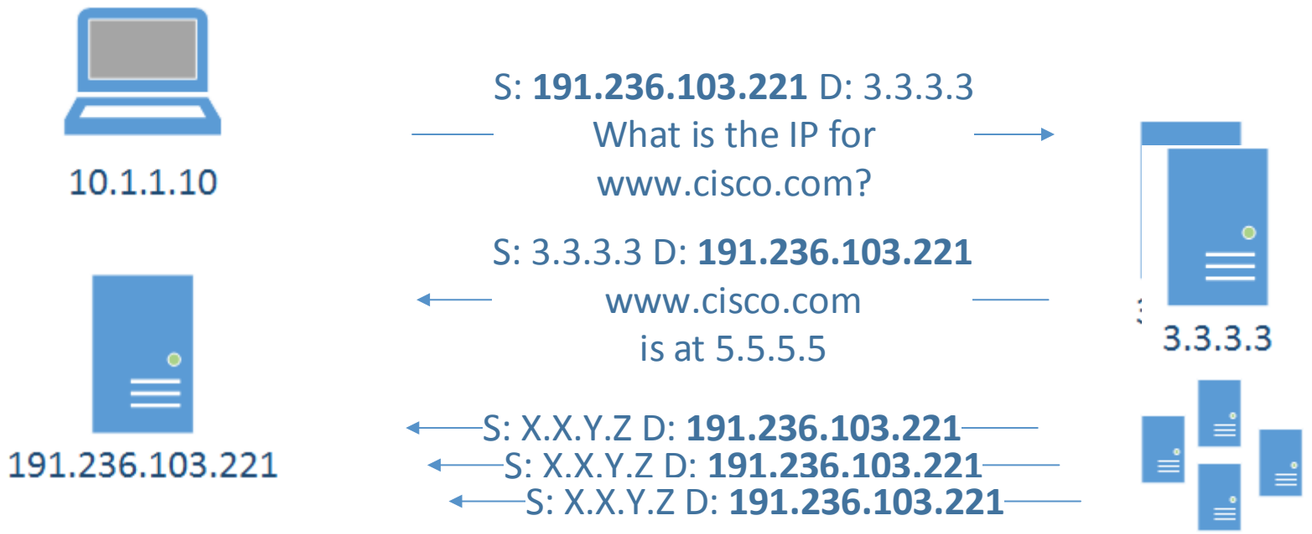


…if the answer was cached



What is DNS reflection?

- What happens if an attacker forges the victim address as its source?

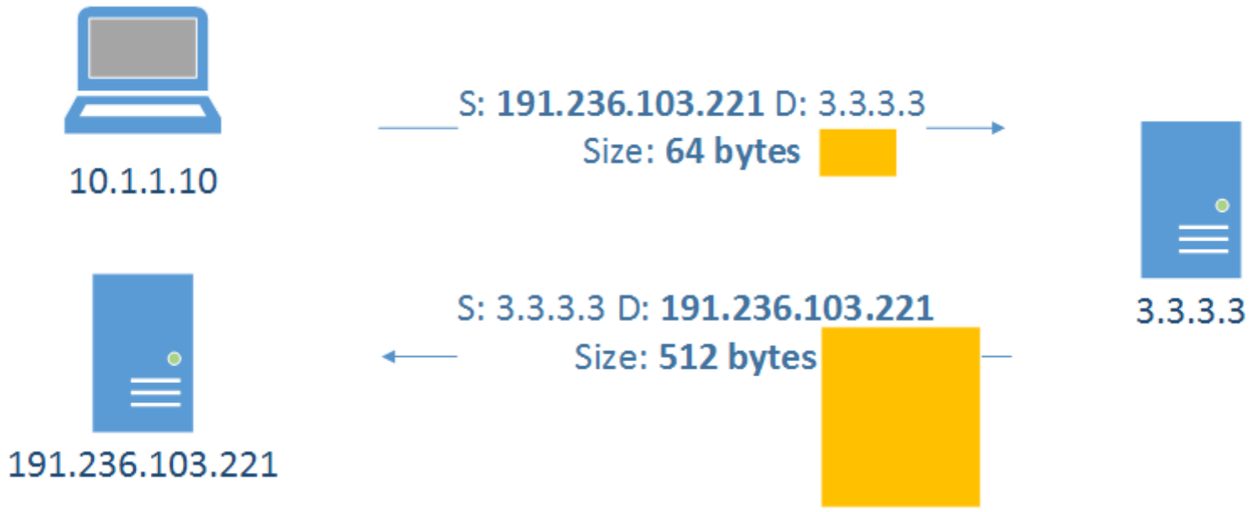


…the reflected traffic goes to the target server

- … and what if hundreds of misconfigured open DNS resolvers are used?

What is an amplification attack?

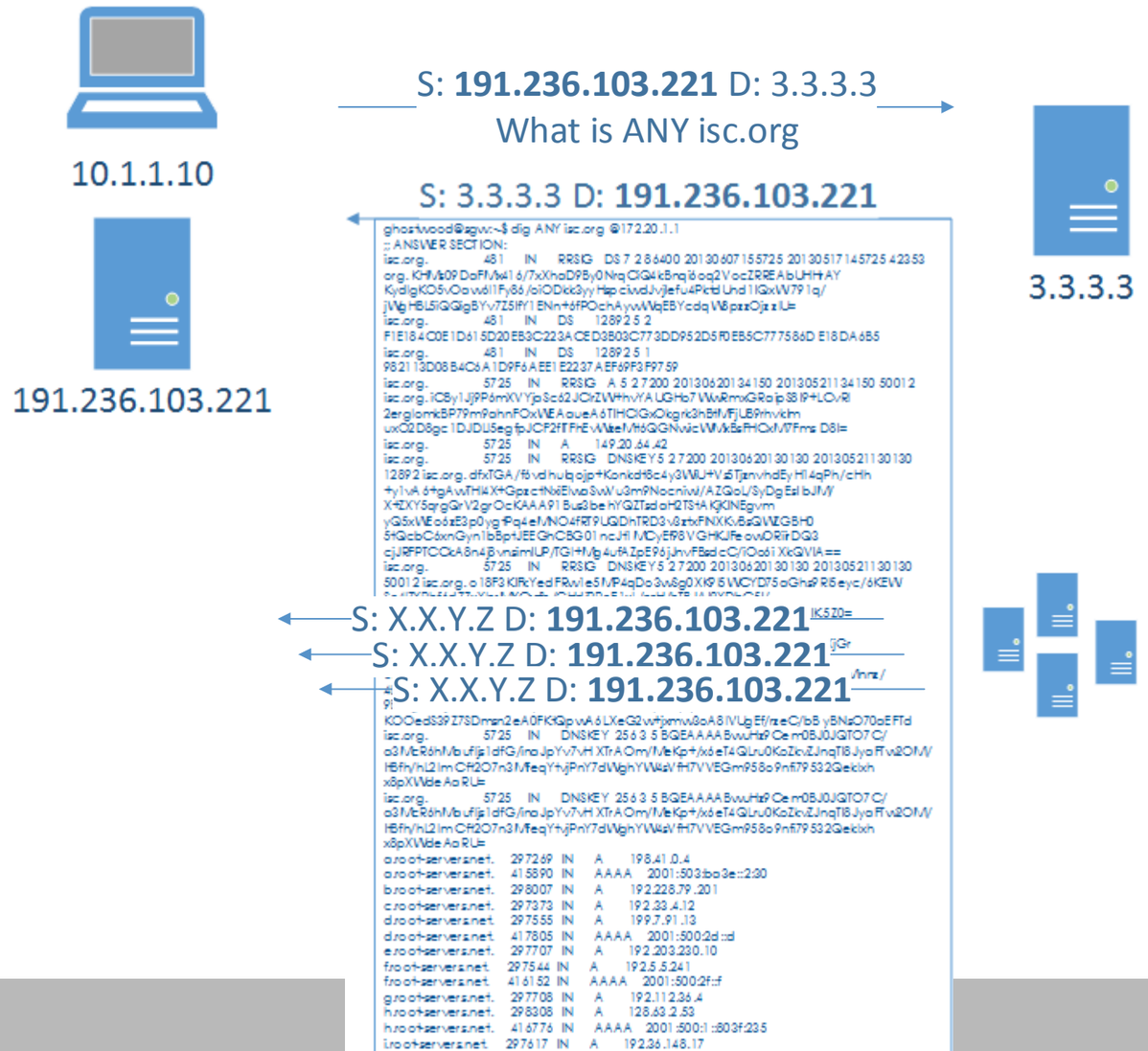
- Asymmetric attack where the response is much larger than the original query



Amplification types

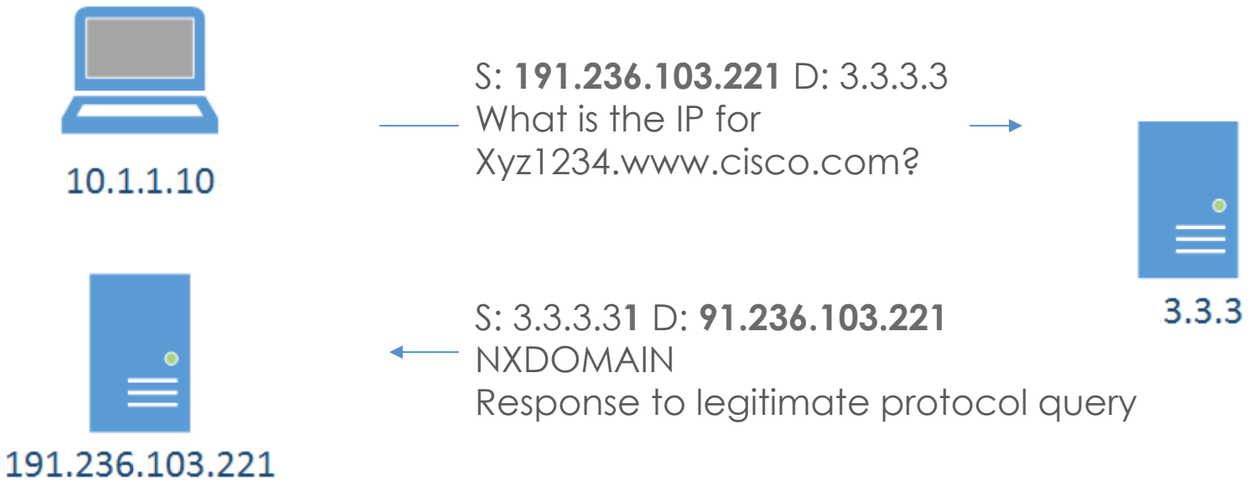
- The ones that are of interest and provide reflections are:
- DNS
- NTP
- SNMP
- SSDP
- What else?

Reflection and Amplification



What is a subdomain attack?

- Direct or Reflection attack where the intermediary and victim spend cycles on nonsense

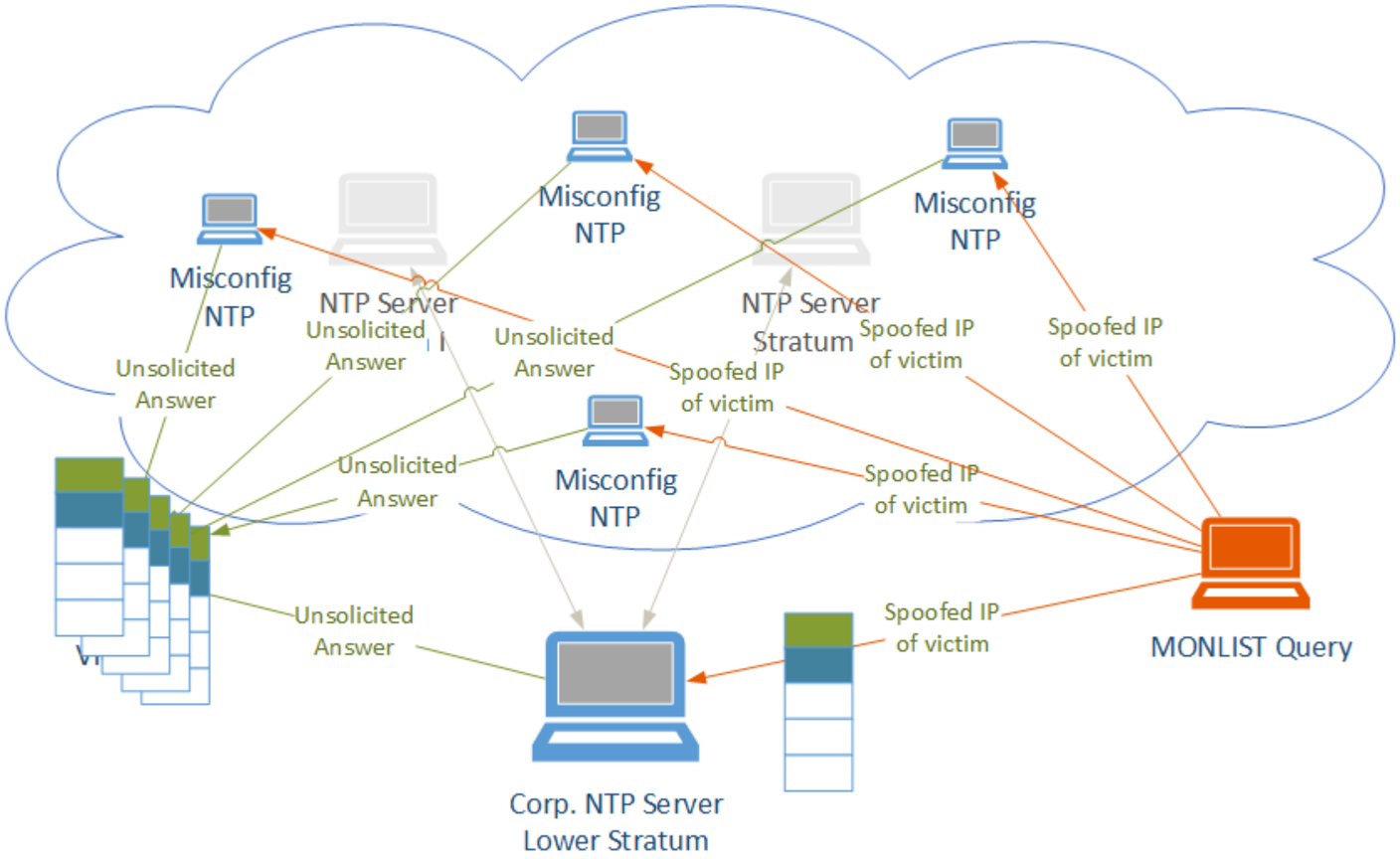


NTP servers

- Stratum servers
- NTP queries

- MONLIST command
  - provides
    a list of clients that have
    time readings

- What's next?



Solution?

- **DNS "Any" Request Filtering**
  - DNS "Any" requests can be used for a DDoS attack, since they occupy DNS server resources as the target server sends its many records to the requesters.

- **DNS Request Rate Limiting—by FQDN**
  - IP address – Limits the rate of queries from a given source.
  - Requested domain name – Limits the rate of requests for the same domain name, from any sender, i.e. DNS Birthday attack
  - Scope for FQDN rate limiting– Specify how many labels of the FQDN to consider together when applying the rate limit
  - Maximum label length – Specify the maximum length for a given label within the FQDN, either at any suffix position or beginning at a specific suffix position.

- **DNS Request Rate Limiting—by Record Type**
- **NXDomain Inspection and Rate Limiting**

Solution?

- **Label Inspection and Label Length Limiting**
  - Limit the label length of the FQDN after a number of suffixes
    - Anything greater than suffix x will be limited

Ddos template dns tp-dns

fqdn-label-length 15 suffix 2

fqdn-label-length 10 suffix 3

www.googlegooglegoogle.com

test.www.google.com

randominvalidstring.google.com — Does not pass label length 15 after suffix 2 check

alongstring.www.google.com — Passes label length 15 after suffix 2 check, but does not pass label length 10 after suffix 3 check

Backscatter

- What is backscatter and why do I care?
- Traffic that is a by-product of the attack
- Why is that interesting?
  - It is important to distinguish between the actual attack traffic and unintended traffic sent by the victim
  - Classify the attacker and victim differently

Metrics

- Bandwidth (Kbps, Gbps)
- PPS
- QPS
- Storage
- CPU
- Application specific – usually latency
- Bad actors
- Victims
- Geo-temporal

Good Internet citizenship

Mitigations (Assumption – preaching to the converted)

- Defend yourself
  - Anycast
  - Some form of IPS/DDoS mitigation gear – inline or asymmetric (service dependent or independent?)
  - Overall network architecture
- Defend the Internet
  - Rate-limiting
  - BCP38/140 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - No open resolvers
- Talk to other security professionals like yourself
- Talk to vendors like A10 Networks

Are you noticing the imbalance?

Defend yourself/your consumers

- Anycast (DNS)
- Some form of IPS/DDoS mitigation gear

- **Lots of money**
- **Effective, scalable, faster to rollout**

Defend the Internet

- Rate-limiting
- BCP38/140 (outbound filtering) source address validation
- Securely configured authoritative DNS servers
- No open resolvers

- **Somewhat cheap**
- **More touch points, slower to rollout**

What's the point I'm trying to make?

- It's not feasible to mitigate those attacks single handedly all of the time

- Companies need to start including "defending the Internet from themselves" as a part of their budget – not only "defending themselves from the Internet"
- We need cooperation amongst Service Providers **and Security Vendors**
  - More can always be done, the war continues
  - Shared intelligence is key

In Summary (Assumption – this is part of your strategy already)

- Evaluate the quick wins in your own network
  - RFC 2827/BCP 38
  - If possible filter all outgoing traffic and use proxy
  - BCP 140: "Preventing Use of Recursive Nameservers in Reflector Attacks"
- Collaborate with your peers to raise the bar collectively
- Use high-scale, high performance mitigation infrastructure that defends your network and gives your consumers and peers levels of protection that keep pace and exceed the pace of change
- Use dedicated DDoS platforms that understand the in-the-wild attacks
  - Don't exacerbate the situation, reduce the backscatter
- Share the key metrics, KPIs and mitigation techniques (public forum?)

THANK YOU

www.a10networks.com