DDoS Attacks on the Root DNS

Presented by
Ricardo de Oliveira Schmidt

October 4th, 2016
The Hague, Netherlands
Reference:

**Anycast Vs. DDoS: Evaluating the November 2015 Root DNS Event**

Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei and Cristian Hesselman

To appear at ACM Internet Measurements Conference (IMC), 2016
(Technical Report ISI-TR-2016-709, USC/Information Sciences Institute)
Distributed Denial of Service
Distributed Denial of Service
Distributed Denial of Service
Distributed Denial of Service

**Big** and getting **bigger**

- 2012: 100 Gb/s
- 2016: 100 Gb/s is common, >1 Tb/s is possible
Distributed Denial of Service

New record! 665 Gb/s!!!
Distributed Denial of Service

New record!
665 Gb/s!!!

Even Akamai "gave up"
**Distributed Denial of Service**

New record! **665 Gb/s!!!**

Even **Akamai** "gave up" "Someone has a botnet with capabilities we haven't seen before"

*Martin McKeay, Akamai*
Distributed Denial of Service

**Big** and getting **bigger**

- 2012: 100 Gb/s
- 2016: 100 Gb/s is common, >1 Tb/s is possible

**Easy** and getting **easier**

- 2012: many botnets with 1000+ nodes
- 2016: DDoS-as-a-service (Booters) offer few Gb/s @ US$ 5
Distributed Denial of Service

vDos homepage

More than 150,000 DDoS in two years with profit of US$ 600,000
Distributed Denial of Service

Big and getting bigger
- 2012: 100 Gb/s
- 2016: 100 Gb/s is common, >1 Tb/s is possible

Easy and getting easier
- 2012: many botnets with 1000+ nodes
- 2016: DDoS-as-a-service (Booters) offer few Gb/s @ US$ 5

Frequent and getting frequent-er
- 2002: the October 30 DNS Root event
- 2016: 3 recent big attacks (2015-11-30, 2015-12-01, 2016-06-25)
Distributed Denial of Service

The Internet’s Backbone

DNS Root Servers Hit by a Massive Cyber Attack

Image copyrights © thehackernews.com
Distributed Denial of Service

"Someone Just Tried to Take Down Internet's Backbone with 5 Million Queries/Sec"

Swati Khandelwal, thehackernews.com
Distributed Denial of Service

"Someone Just Tried to Take Down Internet's Backbone with 5 Million Queries/Sec"
Swati Khandelwal, thehackernews.com

"Root DNS servers DDoS'ed: was it a show off?"
Yuri Ilyin, Kaspersky
Distributed Denial of Service

"Someone Just Tried to Take Down Internet's Backbone with 5 Million Queries/Sec"
Swati Khandelwal, thehackernews.com

"Root DNS servers DDoS'ed: was it a show off?"
Yuri Ilyin, Kaspersky

"Someone Is Learning How to Take Down the Internet"
Bruce Schneier, Schneier on Security
DNS is hierarchical
Multiple layers of servers
Root, TLDs, 2nd-level TLDs, ...

The **root** is the very basis of it

www.utwente.nl?

130.89.3.249
The Root DNS

13 nameservers (from a to m)
  Operated by 12 different organizations
Each run a distributed service (anycast)
  Multiple physical locations
  Multiple servers per location

500+ instances of service

More info at
  http://www.root-servers.org
The Nov. 30 Event

DDoS attack on the Root DNS

Peak of 35+ Gb/s
5 million queries/sec
Impact was moderate

Thanks to the robustness of the whole system
The Nov. 30 Event

What was the impact?

Most letters suffered
- a bit (E, F, I, J, K)
- a lot (B, C, G, H)

Did not see attack traffic
- D, L, M

Problems on reachability!
The Nov. 30 Event

What was the impact?

For those that still see service...
...performance problems
...6x higher delay for G
The **Nov. 30 Event**

Collateral damage!

D-Root was not targeted... 
... but *felt* the attack
The **Nov. 30 Event**

**Collateral damage!**

D-Root was not targeted... ... but *felt* the attack

Even SIDN (.nl) felt the attack: *NO* traffic in FRA and AMS
The Lessons Learned

The Root DNS handled the situation quite well...
  ... at no time the service was completely unreachable

Resilience of the Root DNS is not an accident...
  ... consequence of fault tolerant design and good engineering!

True diversity is key to avoid collateral damage
And, What Now?

Learn from the Root DNS experiences

Have in mind the possible very large DDoS attacks when...
   ... designing Internet systems
   ... improving countermeasures and mitigation strategies

It does not matter if...
   ... someone was showing off
   ... someone was testing/scanning the infrastructure
   ... someone is learning how to take down the Internet

It was a big wake up call, this is critical infrastructure!

Things are escalating pretty fast and apparently we are not fully aware of what we are dealing with.
Acknowledgements:

Arjen Zonneveld, Jelte Jansen, Duane Wessels, Ray Bellis, Romeo Zwart, Colin Petrie, Matt Weinberg and Piet Barber

SIDN Labs, NLnet Labs and SURFnet

Self-managing Anycast Networks for the DNS (SAND) project | http://www.sand-project.nl/
NWO DNS Anycast Security (DAS) project | http://www.das-project.nl/