The Rise of DDoS attacks: how, why, and what we can do about it

Giovane C. M. Moura
giovane.moura@sidn.nl

DISSECT 2017 Workshop
IEEE/IM 2017
May 12th, 2017
Lisbon, Portugal

Background

- Short-bio:
  - Data Scientist (SIDN Labs, NL)
  - Previously: Post-doc (TU Delft, NL)
  - Ph.D.: University of Twente (Advisor: Aiko Pras, NL)
- SIDN Labs:
  1. Research arm of SIDN (`.nl` registry)
  2. Topics: DNS, Performance, Security and Stability
     - E.g.: Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei and Cristian Hesselman. *Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event.* ACM IMC 2016 [1]
     - more on `sidnlabs.nl`

Overview

Basics

How is it taken place?

Why is this happening now?

Attacks to the core part: case study DNS

What can we do?

Basics

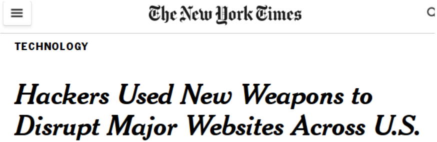
How is it taken place?

Why is this happening now?

Attacks to the core part: case study DNS

What can we do?

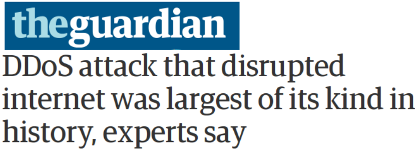
Dyn DDoS October 21, 2016 attack: 1.2 Tbps



The New York Times

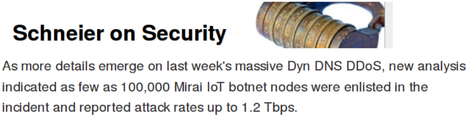
TECHNOLOGY

Hackers Used New Weapons to Disrupt Major Websites Across U.S.



theguardian

DDoS attack that disrupted internet was largest of its kind in history, experts say



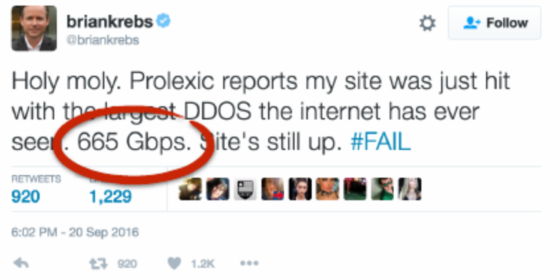
Schneier on Security

As more details emerge on last week's massive Dyn DNS DDoS, new analysis indicated as few as 100,000 Mirai IoT botnet nodes were enlisted in the incident and reported attack rates up to 1.2 Tbps.

Dyn DDoS October 21, 2016 attack: 1.2 Tbps

- Overloaded parts of Dyn DNS service
- Attacked **the core infrastructure** of the Internet
- Dyn is a DNS provider for:
  - Twitter
  - Netflix
  - Spotify
  - Airbnb
  - Reddit
  - Etsy
  - SoundCloud
  - New York Times
  - ...

Other big DDoS



briankrebs
@briankrebs

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

RETWEETS 920 1,229

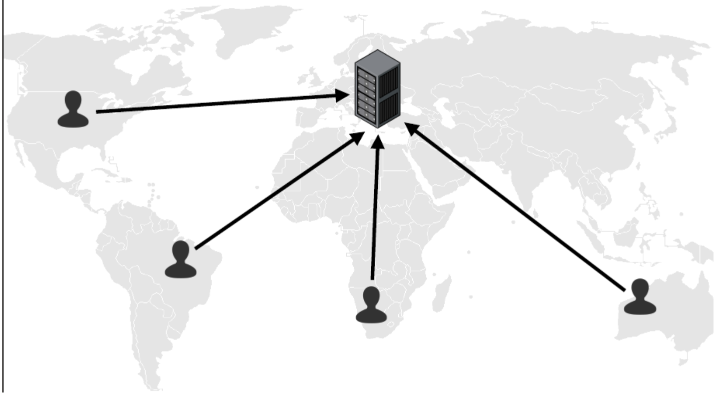
6:02 PM - 20 Sep 2016

Figure: Brian Krebs (665 Gb/s) [2]

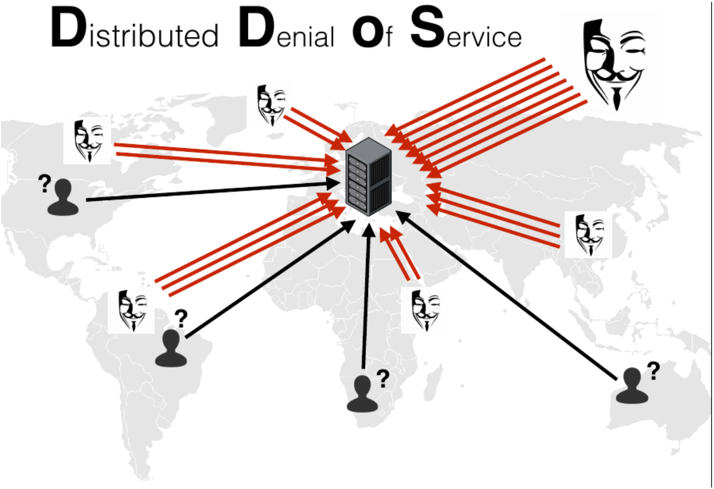
- Many other DDoS attacks lately: Root DNS [1] (35Gb/s), OVH (1Tb/s), Rio2016 Olympic Games (540Gb/s) [3], ProtonMail [4], and others.

DDoS

Distributed Denial Of Service



DDoS



Basics: what is a DDoS attack?

- A distributed denial-of-service is a coordinated attack to slow/bring down a victim
- Done buy overloading some part of the system (pipe, cpu, mem, etc.)
- There are many variations, but the basic idea is the same: overload and bring it down
- Once down, they are prone to extorsion [5]
- It's an old type of attack; **what's new now it's the economics**
- Bad news is: they are getting *bigger, cheaper, and more frequent*

Basics

How is it taken place?

Why is this happening now?

Attacks to the core part: case study DNS

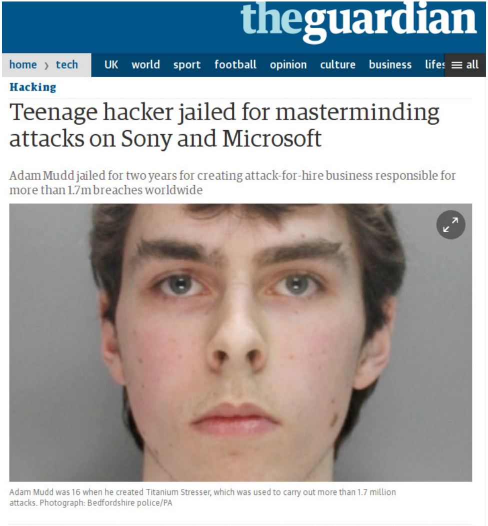
What can we do?

How

What are the realistic current options ($):

1. Botnets: hijack other people computers
   - cycles of infection and cleaning due to software updates
2. Booters: websites that sell DDoS for-hire, for few dollars [6]
3. IoT botnets: brand new
   - botnet on devices that are never updated
   - Behind Brian Krebs [2], Dyn DNS 1.2 Tb/s attacks

How: booters



theguardian
home › tech
UK world sport football opinion culture business lifes ≡ all

Hacking

Teenage hacker jailed for masterminding attacks on Sony and Microsoft

Adam Mudd jailed for two years for creating attack-for-hire business responsible for more than 1.7m breaches worldwide

Adam Mudd was 16 when he created Titanium Stresser, which was used to carry out more than 1.7 million attacks. Photograph: Bedfordshire police/PA

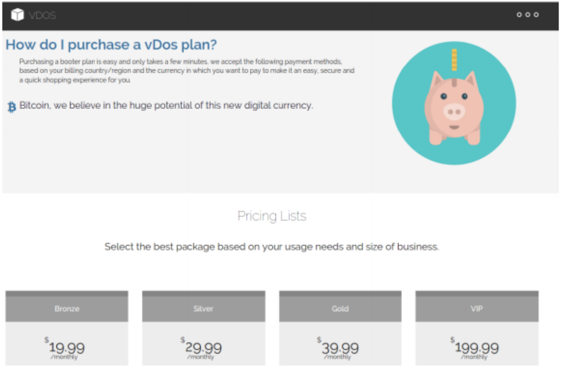
Figure: The Guardian , 2017-04-25 https://www.theguardian.com/technology/2017/apr/25/teenage-hacker-adam-mudd-jailed-masterminding-attacks-sony-microsoft

How: booters

- Adam Mudd, then 16 yrs old, now 20
- Jail time: 2 years
- owner of booter known as Titanium Stresser
- 1.7 million DDoS attacks: Minecraft, Xbox Live and Microsoft
- He made $\sim$ US$ 400,000 in bitcoins
- 112,000 registered users!!! (demand)
- One attack cost the victim 6 million pounds in defenses

How: booters

vDos homepage



How do I purchase a vDos plan?

Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

₿ Bitcoin, we believe in the huge potential of this new digital currency.

Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
$19.99 /monthly	$29.99 /monthly	$39.99 /monthly	$199.99 /monthly

More than

150,000 DDoS

in two years

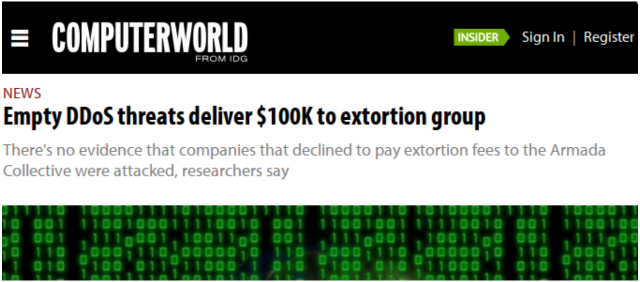
with profit of

US$ 600,000

https://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/

How: booters (DDoS as a service)

- Supplier: vdos and others
- Clients: pay using bitcoin few dollars
- Complexity cost: zero
- Being caught: harder too
- How to make money: extortion



NEWS

Empty DDoS threats deliver $100K to extortion group

There's no evidence that companies that declined to pay extortion fees to the Armada Collective were attacked, researchers say

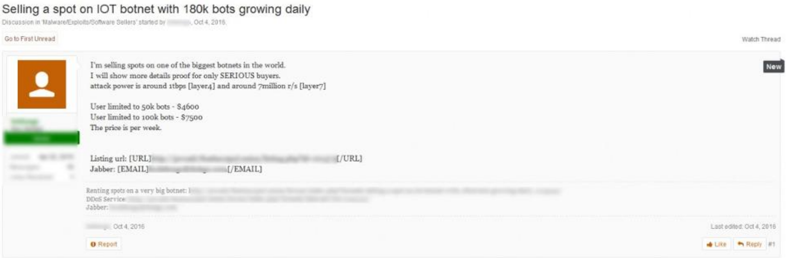
Figure: http://www.computerworld.com/article/3061813/security/empty-ddos-threats-deliver-100k-to-extortion-group.html

How: IoT botnet

- Botnet of IoT devices: cameras, TVs, thermometers, etc.
- Once built, never updated
- **Asymmetrical** incentives:
  - those who built $\neq$ those who suffer attacks
- So once infected, never cleaned
- Has been predicted for years (those “paranoids”)
- It’s a **reality** now: Mirai botnet

How: IoT botnet

- Supplier: vdos and others
- Clients: pay using bitcoin few dollars
- Complexity cost: zero
- Being caught: harder too
- How to make money: extortion
- Bruce Schneier IoT Essay: https://www.schneier.com/blog/archives/2017/02/security_and_th.html



Selling a spot on IOT botnet with 180k bots growing daily

Discussion in 'Malware/Exploits/Software Sellers' started by [redacted], Oct 4, 2016.

[redacted]

I'm selling spots on one of the biggest botnets in the world.
I will show more details proof for only SERIOUS buyers.
attack power is around 1tbps [layer4] and around 7million r/s [layer7]

User limited to 50k bots - $4600
User limited to 100k bots - $7500
The price is per week.

Listing url: [URL][redacted][/URL]
Jabber: [EMAIL][redacted][/EMAIL]

Renting spots on a very big botnet: [redacted]
DDoS Service [redacted]
Jabber: [redacted]

[redacted] Oct 4, 2016

Last edited: Oct 4, 2016

Figure: http://www.forbes.com/sites/thomasbrewster/2016/10/23/massive-ddos-iot-botnet-for-hire-twitter-dyn-amazon

Basics

How is it taken place?

Why is this happening now?

Attacks to the core part: case study DNS

What can we do?

Who? and why?

- who: many actors:
  - school kids that don’t wanna do an exam
  - Gamers on other players
  - criminals for extortion [5]
  - activists trying to make a point (Wikileaks case back in 2011 [7])
  - Nation States (e.g.: North Korea has little too loose)
  - Others

Who? and why?

- why: many reasons:
  1. profit
  2. revenge
  3. cyber war
  4. political reasons
  5. diversion: distract from the real attack
  6. reconnaissance
- Little risk in being caught
- Tools are simple – website & bitcoins

Basics

How is it taken place?

Why is this happening now?

Attacks to the core part: case study DNS

What can we do?

Attacks to the core part: case study of DNS

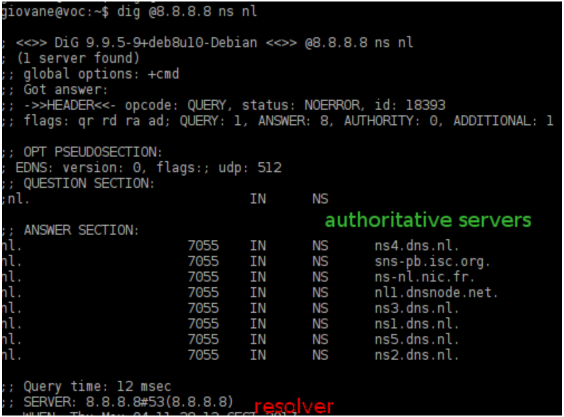
- The impact of a DDoS depends on how crucial is a target
  - E.g.: gaming sites going offline lead to financial losses, and users irritated
  - Different form Government websites
- However, there are some attacks that aim at the core parts of the Internet
- Those have the potential to impair many services/users
- Let’s not forget about collateral damage: ProtonMail [4] datacenter having issues during DDoS

Case Study: DNS

- We will cover two attacks to the core of the Internet: The Root DNS Event of November 2015 [1]

Case Study: DNS

- There are two main types of DNS server:
  1. DNS **Resolvers:** the ones who “ask” (e.g.: 8.8.8.8)
  2. DNS **Authoritatives**: those who know the answers (e.g.: the Root DNS).



```
giovane@voc:~$ dig @8.8.8.8 ns nl

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> @8.8.8.8 ns nl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18393
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nl.                            IN      NS

;; ANSWER SECTION:
nl.                     7055    IN      NS      ns4.dns.nl.
nl.                     7055    IN      NS      sns-pb.isc.org.
nl.                     7055    IN      NS      ns-nl.nic.fr.
nl.                     7055    IN      NS      nl1.dnsnode.net.
nl.                     7055    IN      NS      ns3.dns.nl.
nl.                     7055    IN      NS      ns1.dns.nl.
nl.                     7055    IN      NS      ns5.dns.nl.
nl.                     7055    IN      NS      ns2.dns.nl.

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu May 04 11:28:12 CEST 2017
```

Root DNS: resolving a name

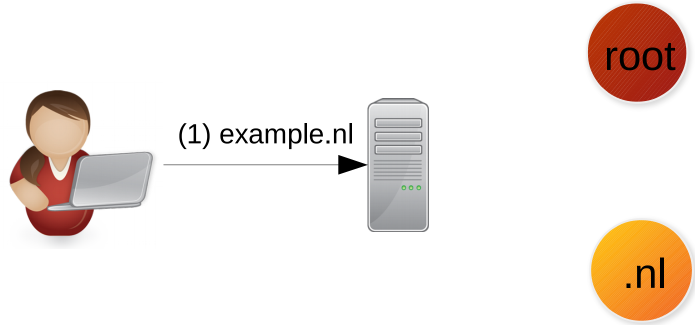


Figure: Resolving a Name

Root DNS: resolving a name

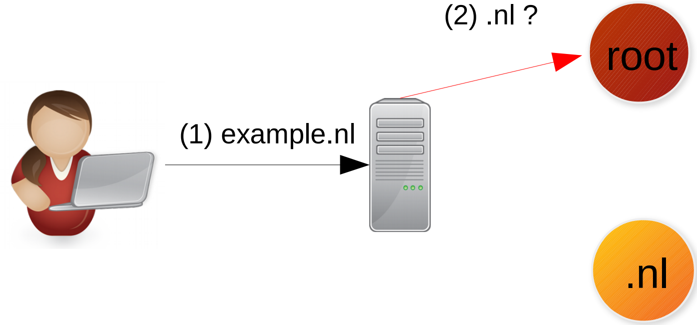


Figure: Resolving a Name

Root DNS: resolving a name

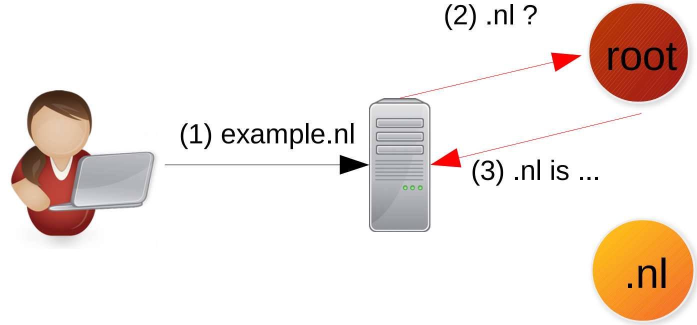


Figure: Resolving a Name

Root DNS: resolving a name

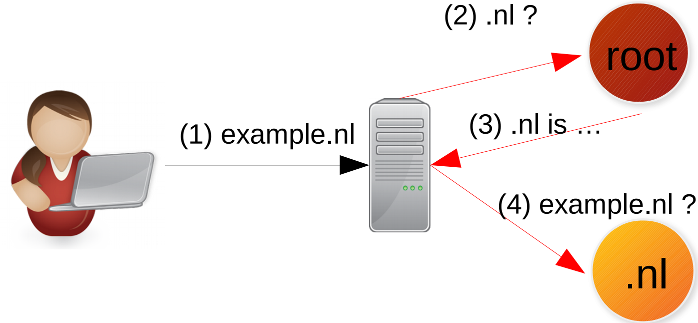


Figure: Resolving a Name

Root DNS: resolving a name

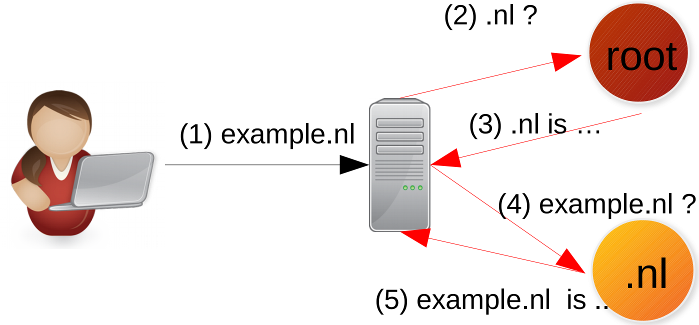


Figure: Resolving a Name

Root DNS: resolving a name

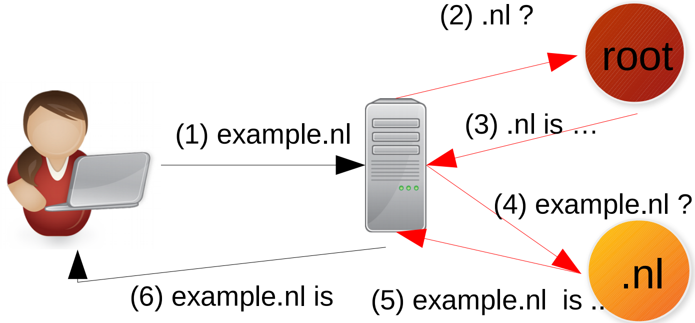


Figure: Resolving a Name

TLD Operations and Datasets

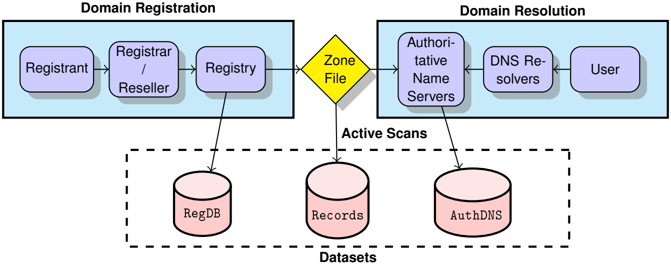


Figure: TLD Operations: registration (left), domain name resolution (right), and derived datasets.

DNS: tree-like structure

- DNS operates in a tree-like structure: to know where is the .nl, you need to know where the Root DNS addresses are
- some domains have their own authoritatives servers (NS records)
  - Wikipedia.org has ns2.wikpedia.org, ns1.wikipedia.org, and ns0.wikipedia.org
  - They manage any *.wikpedia.org domain
- However, if the .org servers are not reachable, some users may not be able to resolve wikipedia.org
- The same occur for the the Root DNS

DNS: core part

- By attacking core Authoritatives servers, an attacker may make unreachable many of their clients
  - E.g.: Dyn DNS is a big DNS provider
  - Their auth servers, who provide authortitative server for Netflix and others, had problems during a DDoS
  - Even though the web servers of their clients were fine, up , and running, their DNS were not
  - In other words: users could not map domains to IP address, thus use their systems

DNS: core part

- So what DNS operators have done to improve DNS resiliency?
- Glad you asked!
- In short: layer after layer of redundancy. For example, the Root DNS:
  1. 13 root server letters (A-M), each of them authoritative for the root zone
  2. each letter has multiple sites (using IP anycast, 1 IP = multiple locations)
  3. each site has multiple servers (load balancers)

IP Anycast Background and Terminology

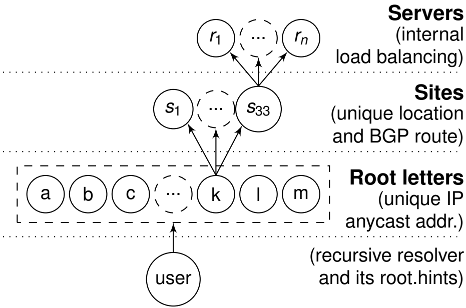


Figure: Root DNS structure, terminology, and mechanisms in use at each level.

Root DNS: 500+ locations, 1000s servers

- 13 Root Server letters (13 IPv4 addrs, 13 IPv6 addrs, 500+ locations)
- 1000s of physical/virtual servers

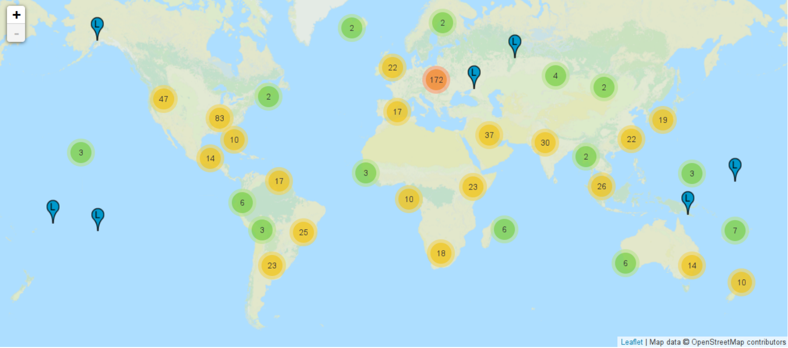


Figure: Root Servers Geo-location (source: root-servers.org)

Root DNS DDoS: Nov 30th, 2015

- 35 Gb/s direct attack on 10 of the 13 letters
- It was a large attack back then
- Due to lots of redundancy, impact on users was minimal
- Last 1 hour, and a second event lasted another hour later
- We analyze these attacks also using Ripe Atlas probes
  - 9000+ small devices that carry out continuous measurements
  - Maintained and supported by Ripe NCC
- We showed how IP anycast behaved under stress [1]

Root DNS DDoS: Nov 30th, 2015

		sites		sites
letter	operator	reported		observed
A	Verisign	5	(5, 0)	5
B	USC/ISI	1	(unicast)	1
C	Cogent	8	(8, 0)	8
D	U. Maryland	87	(18, 69)	65
E	NASA	12	(1, 11)	74
F	ISC	59	(5, 54)	52
G	U.S. DoD	6	(6, 0)	6
H	ARL	2	(pri/back)	2
I	Netnod	49	(48, 0)	48
J	Verisign	98	(66, 32)	69
K	RIPE	33	(15, 18)	32
L	ICANN	144	(144, 0)	113
M	WIDE	7	(6, 1)	6

Table: The 13 Root Letters, each operating a separate DNS service, with their reported architecture (number of sites with local/global sites [8], B unicast, H primary/backup), plus the count of sites we observe

Root DNS DDoS: attack at letter level

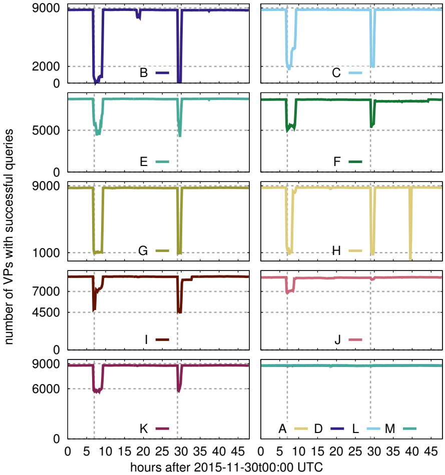


Figure: Number of VPs with successful queries (in 10-minute bins). (All plots are scaled consistently, with nearly 9000 VPs across 48 hours of observation. In all graphs, dotted lines highlight approximate event start times. Here they also show the lowest values for the dips.)

Root DNS DDoS: attack at letter level

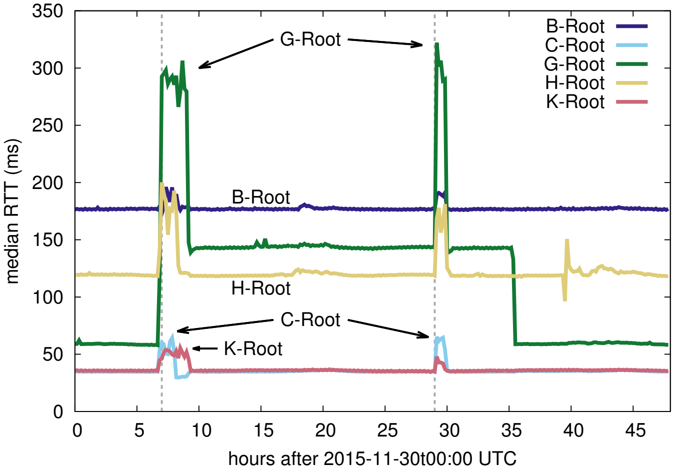


Figure: Median RTT for some letters during the attacks. Letters with no significant change (A, D, E, F, I, J, L, and M) are omitted.

Root DNS DDoS: attack at site level

- Some sites on the same IP are more affected than others

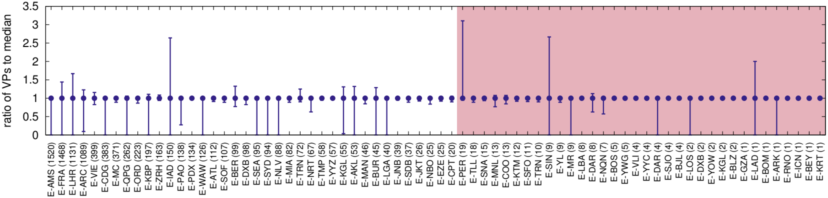


Figure: E-Root

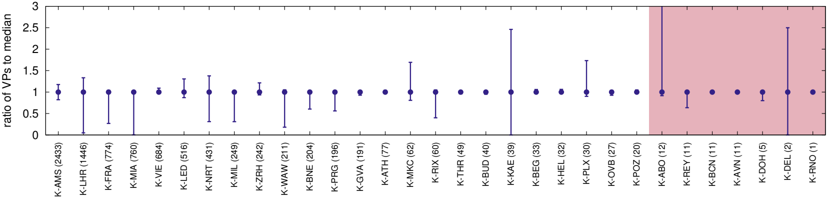


Figure: K-Root

Root DNS DDoS: attack at server level

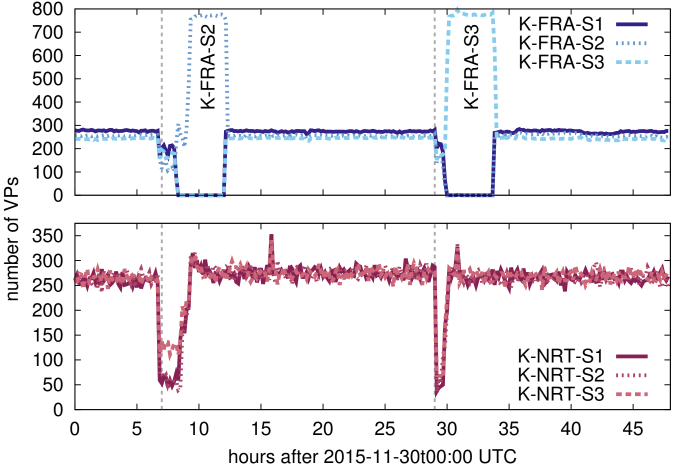


Figure: Reachability for individual servers from K-FRA (top) and K-NRT (bottom).

Basics

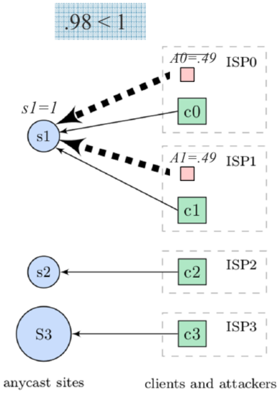
How is it taken place?

Why is this happening now?

Attacks to the core part: case study DNS

What can we do?

What can we do? Anycast (sites isolation)



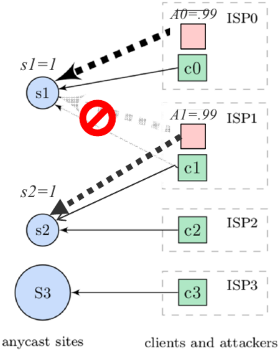
1. A0+A1 < s1: **do nothing; H=4**
2. A0 < s1 and A0+A1 > s2: shed load; H=4
   - vs. H=2 if do nothing
3. A0 > s1 and A0+A1 < s3:
   keep only big site; H=4
   - vs. H=2 if nothing
4. A0+A1 > S3: do nothing (s1 is degraded absorber); H=2

⇒ with today’s uncertainty:
“do nothing” looks good

⇒ future goal: what is needed
(measurement and control) to do better?

What can we do? Anycast

.99 < 1 and 1.98 > 1

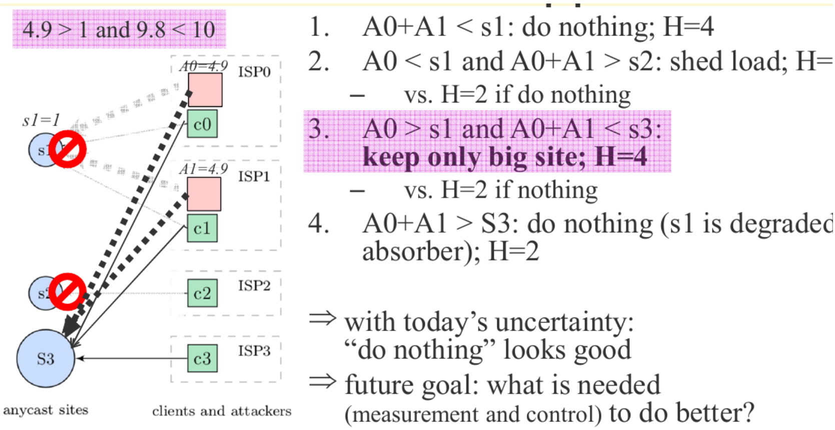


1. A0+A1 < s1: do nothing; H=4
2. A0 < s1 and A0+A1 > s2: **shed load; H=4**
   - vs. H=2 if do nothing
3. A0 > s1 and A0+A1 < s3: keep only big site; H=4
   - vs. H=2 if nothing
4. A0+A1 > S3: do nothing (s1 is degraded absorber); H=2

⇒ with today's uncertainty: "do nothing" looks good

⇒ future goal: what is needed (measurement and control) to do better?

What can we do? Anycast



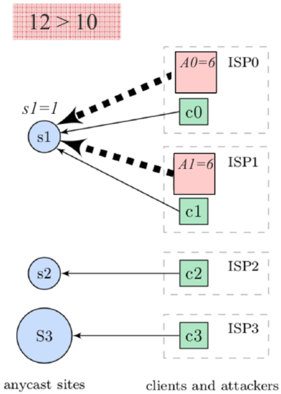
4.9 > 1 and 9.8 < 10

1. A0+A1 < s1: do nothing; H=4
2. A0 < s1 and A0+A1 > s2: shed load; H=
   - vs. H=2 if do nothing
3. A0 > s1 and A0+A1 < s3: **keep only big site; H=4**
   - vs. H=2 if nothing
4. A0+A1 > S3: do nothing (s1 is degraded absorber); H=2

⇒ with today's uncertainty: "do nothing" looks good

⇒ future goal: what is needed (measurement and control) to do better?

What can we do? Anycast



1. A0+A1 < s1: do nothing; H=4
2. A0 < s1 and A0+A1 > s2: shed load; H=4
   - vs. H=2 if do nothing
3. A0 > s1 and A0+A1 < s3: keep only big site; H=4
   - vs. H=2 if nothing
4. A0+A1 > S3: **do nothing** (s1 is degraded absorber); **H=2**

⇒ with today's uncertainty: "do nothing" looks good

⇒ future goal: what is needed (measurement and control) to do better?

What can we do (in general)

- Traditional on-the-fly filtering
- Cloud-based traffic scrubbing ($): big business
  - Cloudfare, Akamai....
- Latest attacks: **core infrastructure** of the Internet → should the government should be involved?
- NaWas: Dutch association for companies
- Enforce standards and practices: BCP 38
- Real issue with IoT: asymmetry, not clear how to solve it
- DARPA IoT Security Challenge: automate defenses
  - http://www.nytimes.com/2016/10/17/technology/security-internet.html
- Forecast: it nothing is done, it will get worse

What can we do

- Bruce Schneier has a great essay on the subject: https://www.schneier.com/blog/archives/2017/02/security_and_th.html
- He advocates government regulation, like the auto industry
- Some not yet convinced
- Issue with market asymmetry: those making vulnerable IoT devices are not the ones experience the attacks
- Nowadays, filtering, cloud-based defense, and overcapacity are your best options
- When is it all going to stop?

Questions?

- Contact:
  - http://sidnlabs.nl
  - giovane.moura@sidn.nl
- Thank you for your attention

Bibliography I

[1] G. C. M. Moura, R. de O. Schmidt, J. Heidemann, W. B. de Vries, M. Müller, L. Wei, and C. Hesselman, “Anycast vs. ddos: Evaluating the november 2015 root dns event,” in *Proceedings of the ACM Internet Measurement Conference*, Nov. 2016. [Online]. Available: http://www.isi.edu/%7ejohnh/PAPERS/Moura16b.html

[2] B. Krebs, “KrebsOnSecurity Hit With Record DDoS https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/,” Sep. 2016.

[3] Arbor Networks, “Rio Olympics Take the Gold for 540gb/sec Sustained DDoS Attacks! https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks/,” Aug. 2016.

Bibliography II

[4] ProtonMail, “Guide to DDoS protection,” https://protonmail.com/blog/ddos-protection-guide/, Dec. 2015.

[5] N. Perlroth, “Tally of cyber extortion attacks on tech companies grows,” New York Times Bits Blog, http://bits.blogs.nytimes.com/2014/06/19/tally-of-cyber-extortion-attacks-on-tech-companies-grows/, Jun. 2016. [Online]. Available: http://bits.blogs.nytimes.com/2014/06/19/tally-of-cyber-extortion-attacks-on-tech-companies-grows/

[6] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Zambenedetti Granville, and A. Pras, “Booters-An analysis of DDoS-as-a-service attacks,” in *IFIP/IEEE Intl. Symposium on Integrated Network Management (IM)*. IEEE, May 2015, pp. 243–251.

Bibliography III

[7] A. Pras, A. Sperotto, G. C. Moreira Moura, I. Drago, R. R. R. Barbosa, R. Sadre, R. de Oliveira Schmidt, and R. J. Hofstede, “Attacks by anonymous wikileaks proponents not anonymous,” http://eprints.eemcs.utwente.nl/19151/, Centre for Telematics and Information Technology University of Twente, Enschede, Technical Report TR-CTIT-10-41, December 2010.

[8] Root Operators, *http:// www.root-servers.org*, Apr. 2016.