Anycast vs. DDoS

The Nov. 2015 DNS Root Event

Presented by

Ricardo de Oliveira Schmidt

October 25, 2016
Madrid, Spain

Reference:

Anycast vs. DDoS: Evaluating the November 2015 DNS Root Event

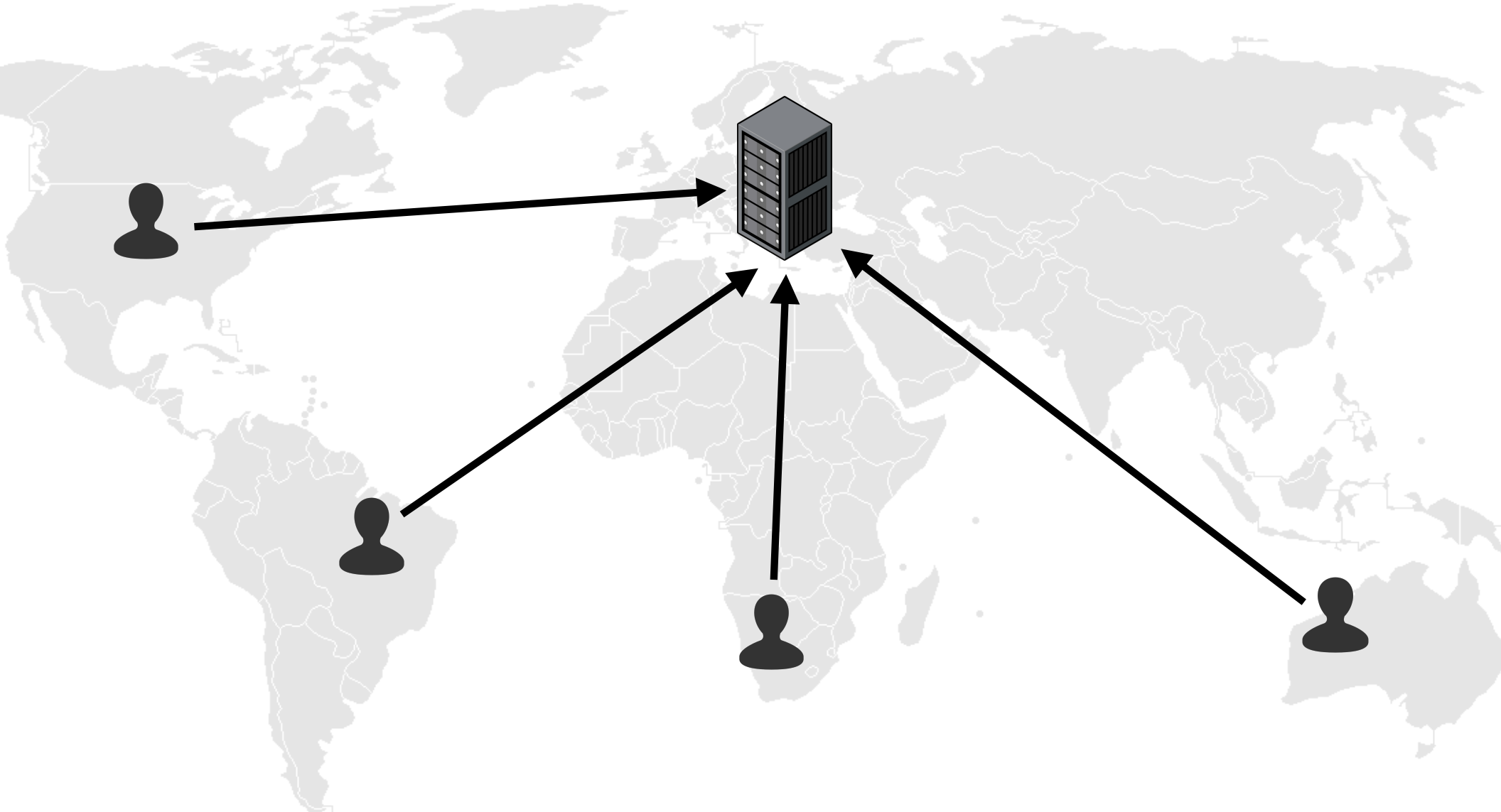
Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei and Cristian Hesselman

In: ACM Internet Measurement Conference (IMC), 2016, Santa Monica, USA.

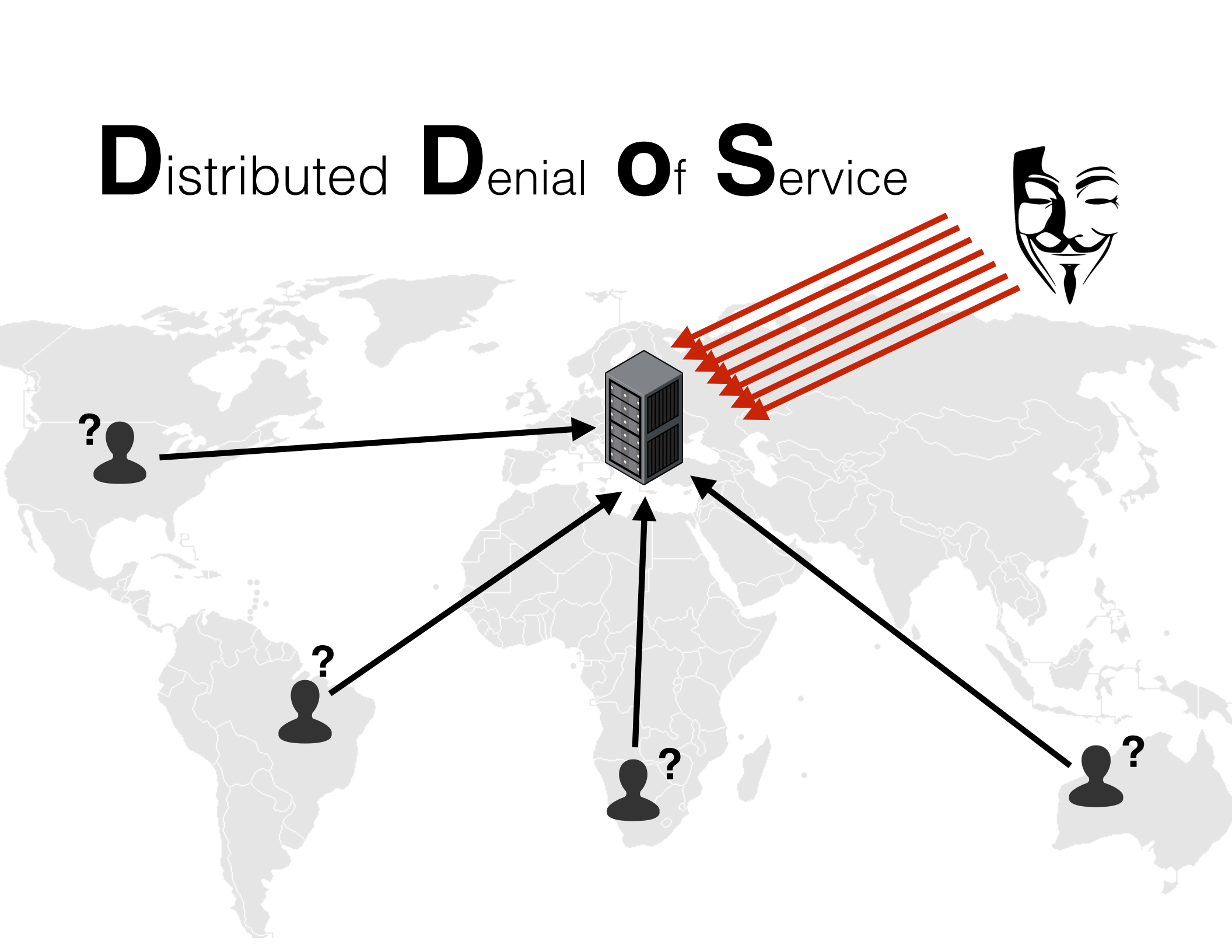
Technical Report ISI-TR-2016-708, USC/Information Sciences Institute, May 2016

- *http://www.isi.edu/~johnh/PAPERS/Moura16a.pdf*

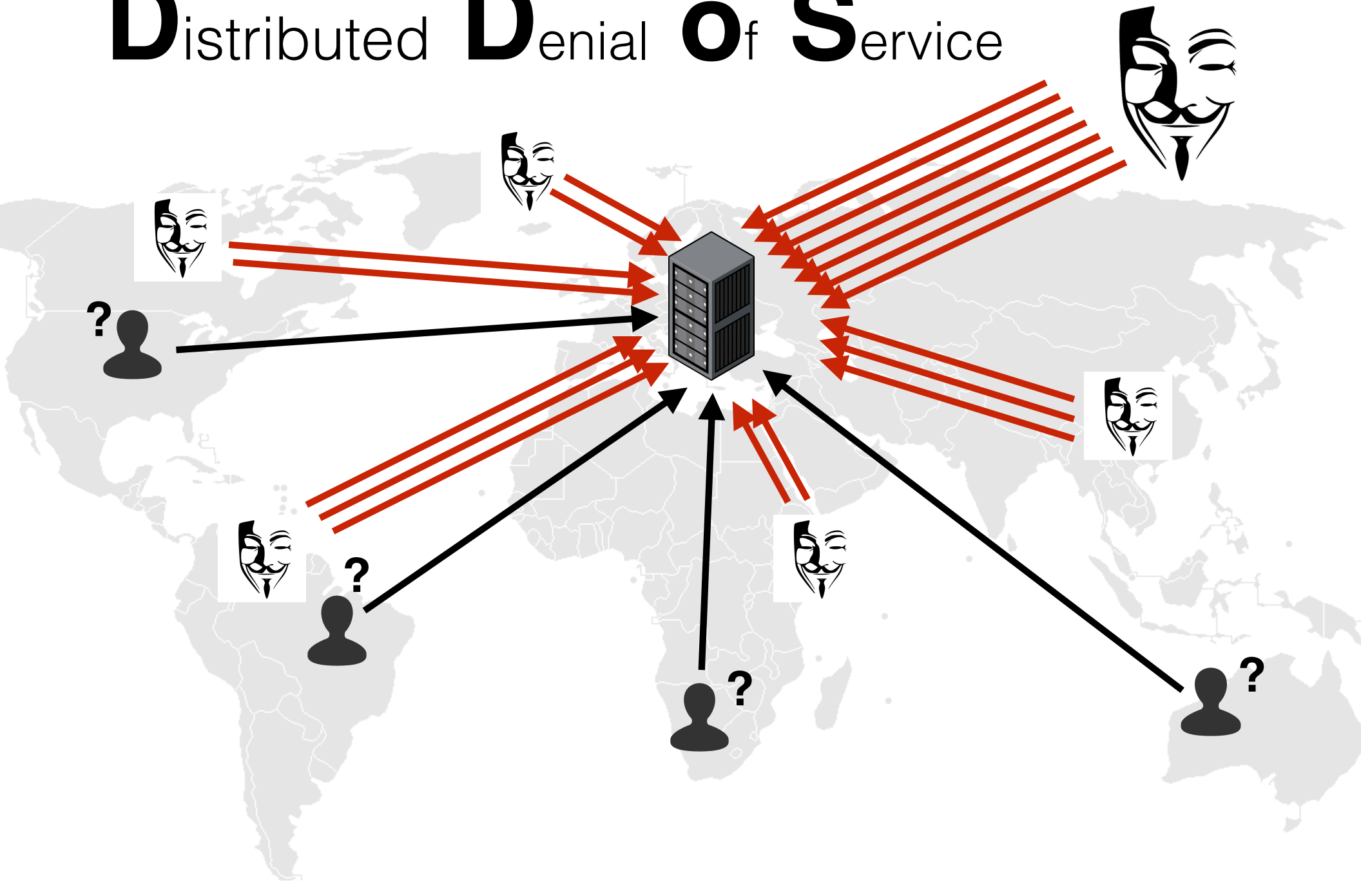
Distributed **D**enial **o**f **S**ervice



Distributed **D**enial **o**f **S**ervice



Distributed Denial of Service

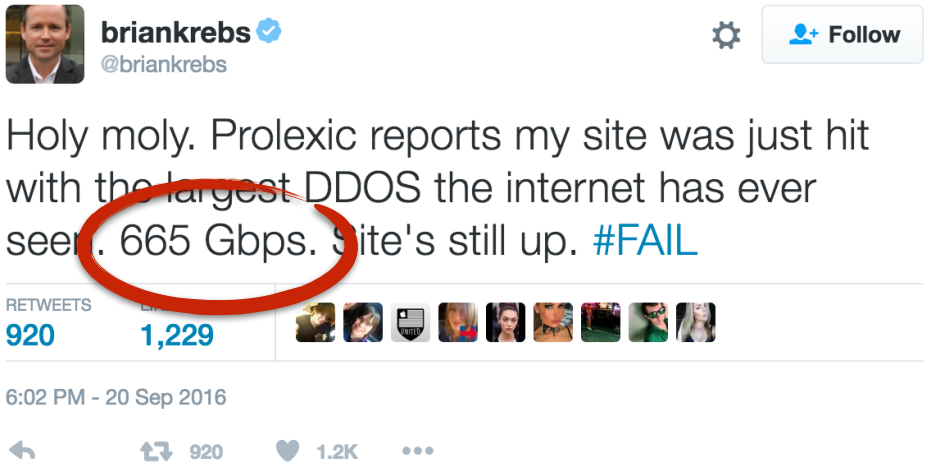


Distributed **D**enial **o**f **S**ervice

Big and getting **bigger**

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

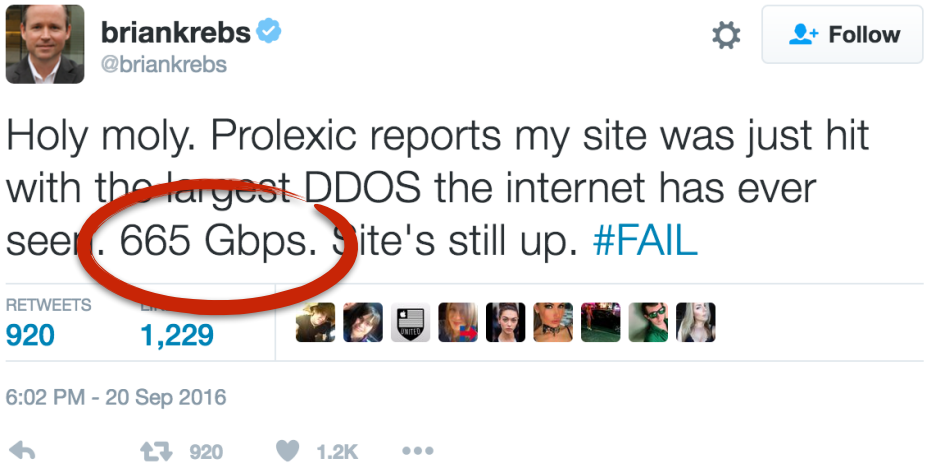
Distributed Denial of Service



New record!

665 Gb/s!!!

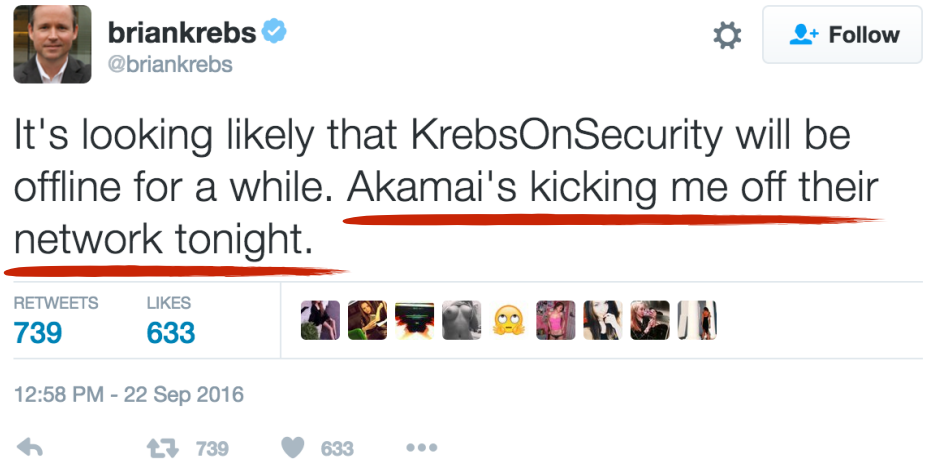
Distributed Denial of Service



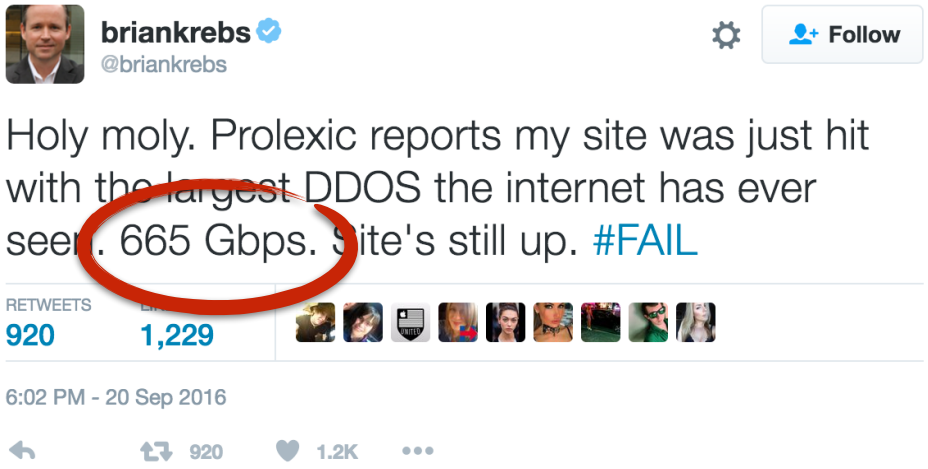
New record!

665 Gb/s!!!

Even **Akamai** "gave up"



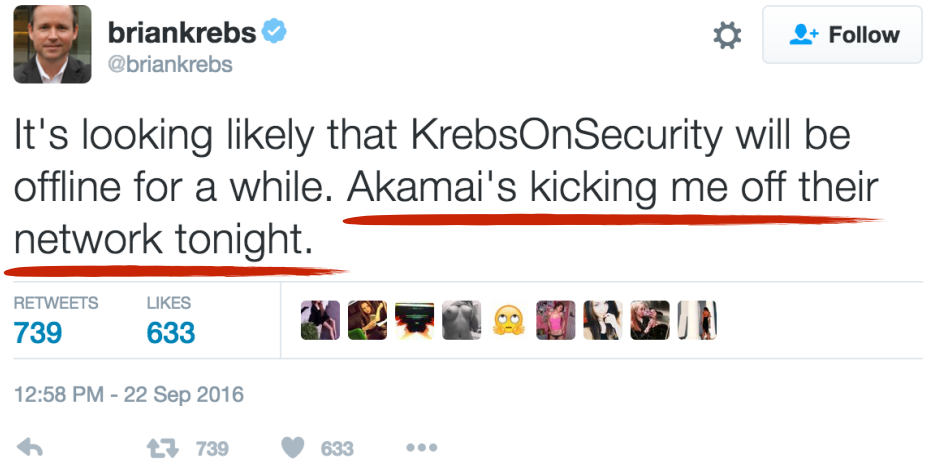
Distributed Denial of Service



New record!

665 Gb/s!!!

Even **Akamai** "gave up"



"Someone has a botnet with capabilities we haven't seen before"

Martin McKeay, Akamai

Distributed **D**enial **o**f **S**ervice

Big and getting **bigger**

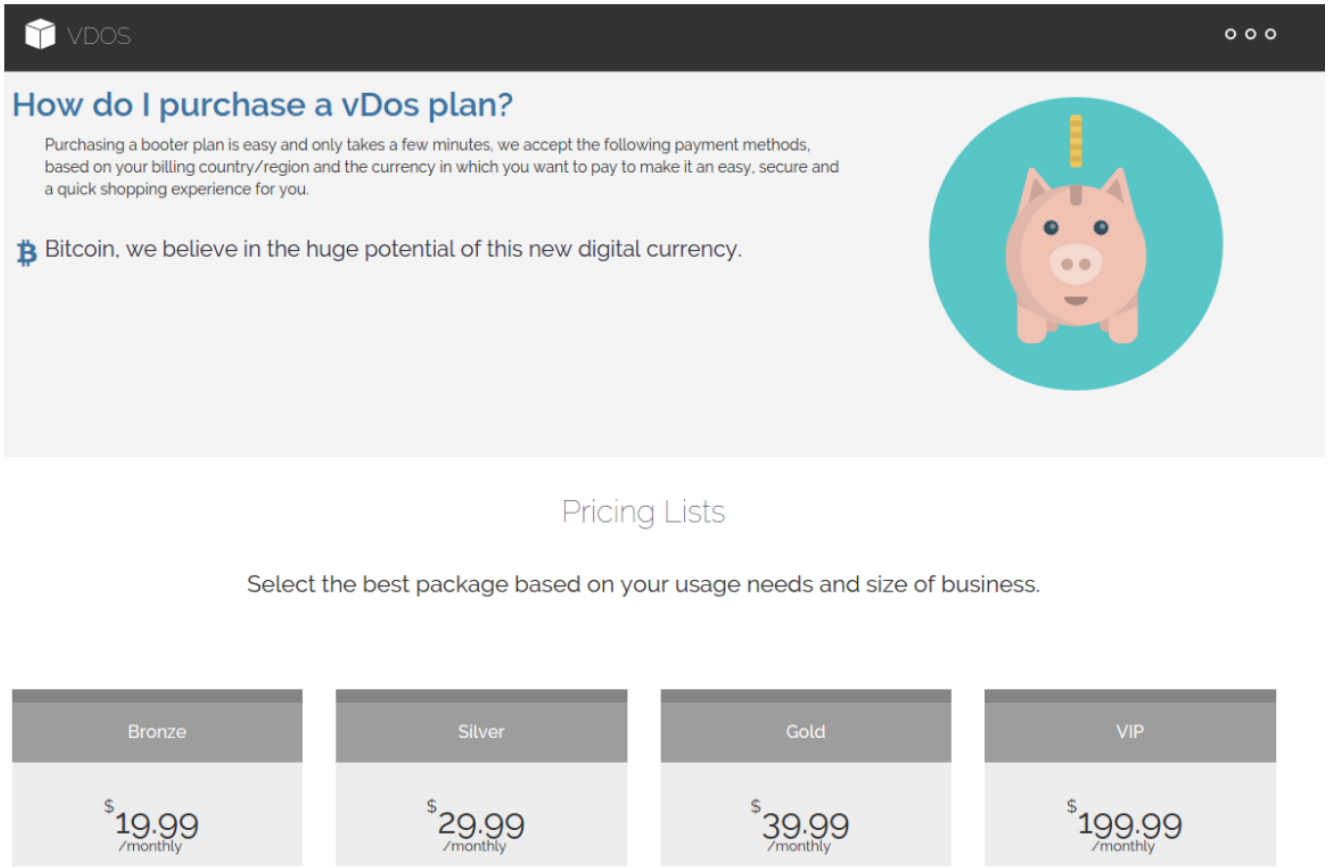
2012: 100 Gb/s
2016: 100 Gb/s is common, >1 Tb/s is possible

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 **D**enial **o**f **S**ervice

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 **D**enial **o**f **S**ervice

Distributed **D**enial **o**f **S**ervice

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

Swati Khandelwal, thehackernews.com

Distributed **D**enial **o**f **S**ervice

"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 **D**enial **o**f **S**ervice

"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"

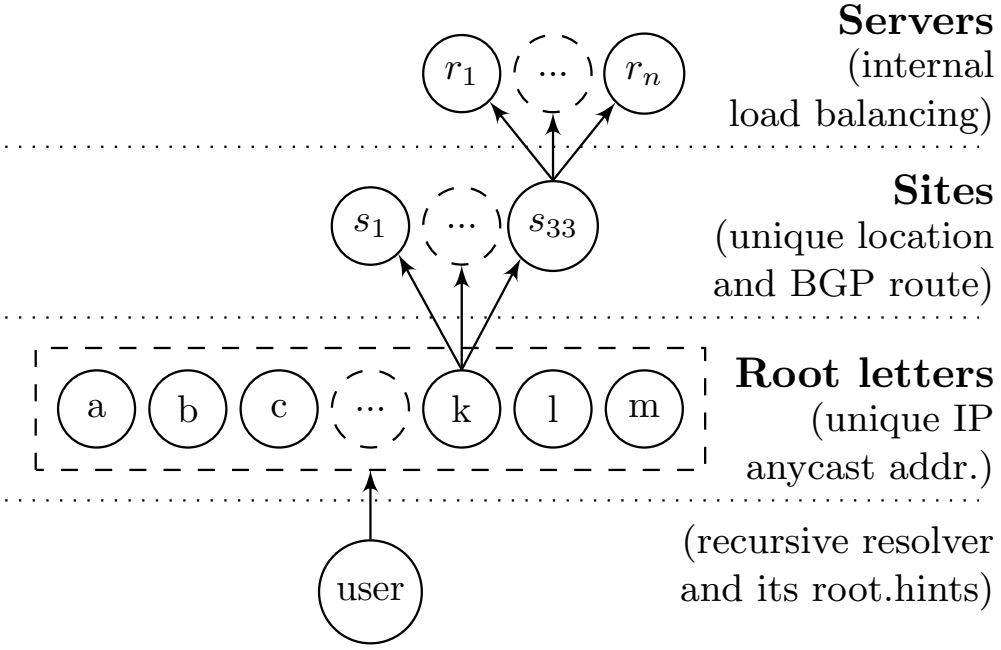
Bruce Schneier, Schneier on Security

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 redundancy of the whole system

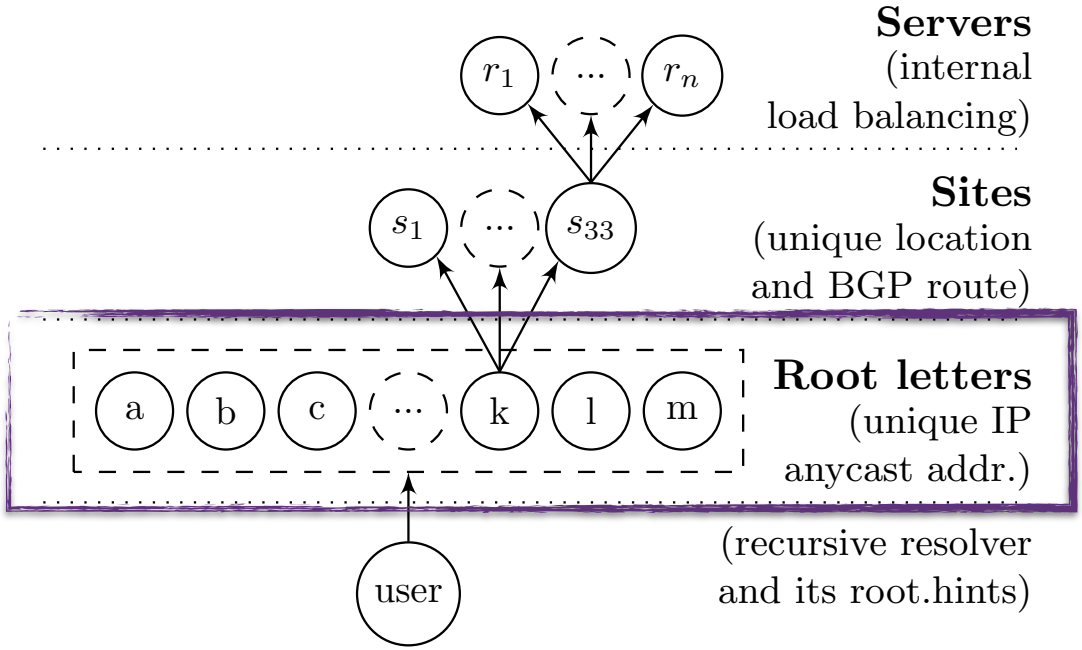
The **Root DNS**


r_1
...
r_n
Servers
(internal
load balancing)
s_1
...
s_{33}
Sites
(unique location
and BGP route)
a
b
c
...
k
l
m
Root letters
(unique IP
anycast addr.)
user
(recursive resolver
and its root.hints)

The **Root DNS**

Horizontal distribution

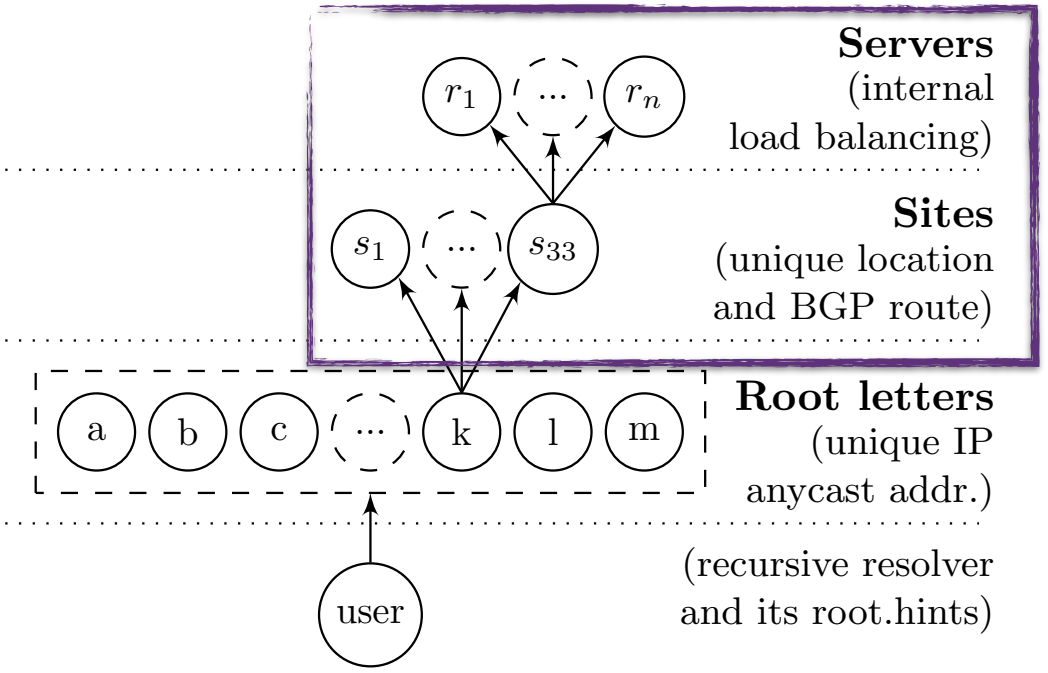
- Multiple letters
- Multiple operators



The **Root DNS**

Vertical distribution

- Multiple sites
- Multiple servers



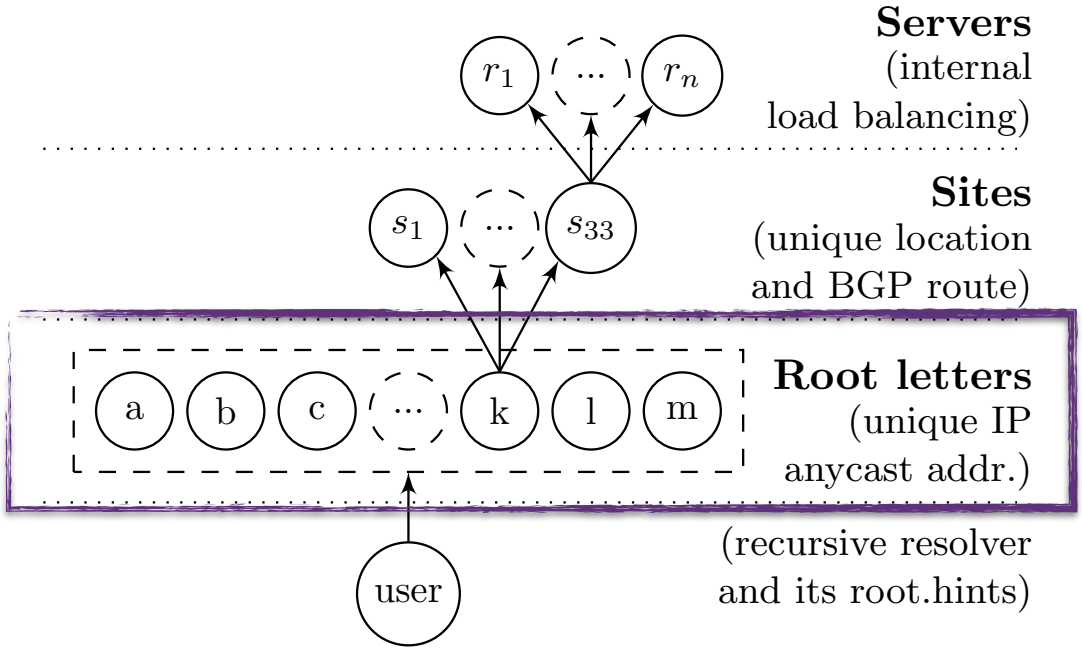
Measurement Data

Measurement data:

- Built-in periodical CHAOS queries @Atlas
- RSSAC-002 data
- BGPmon

The **Impact** of the **Attack**

What was the impact at individual **letters**?



The **Impact** of the **Attack**

What was the impact?

Problems on *reachability*!

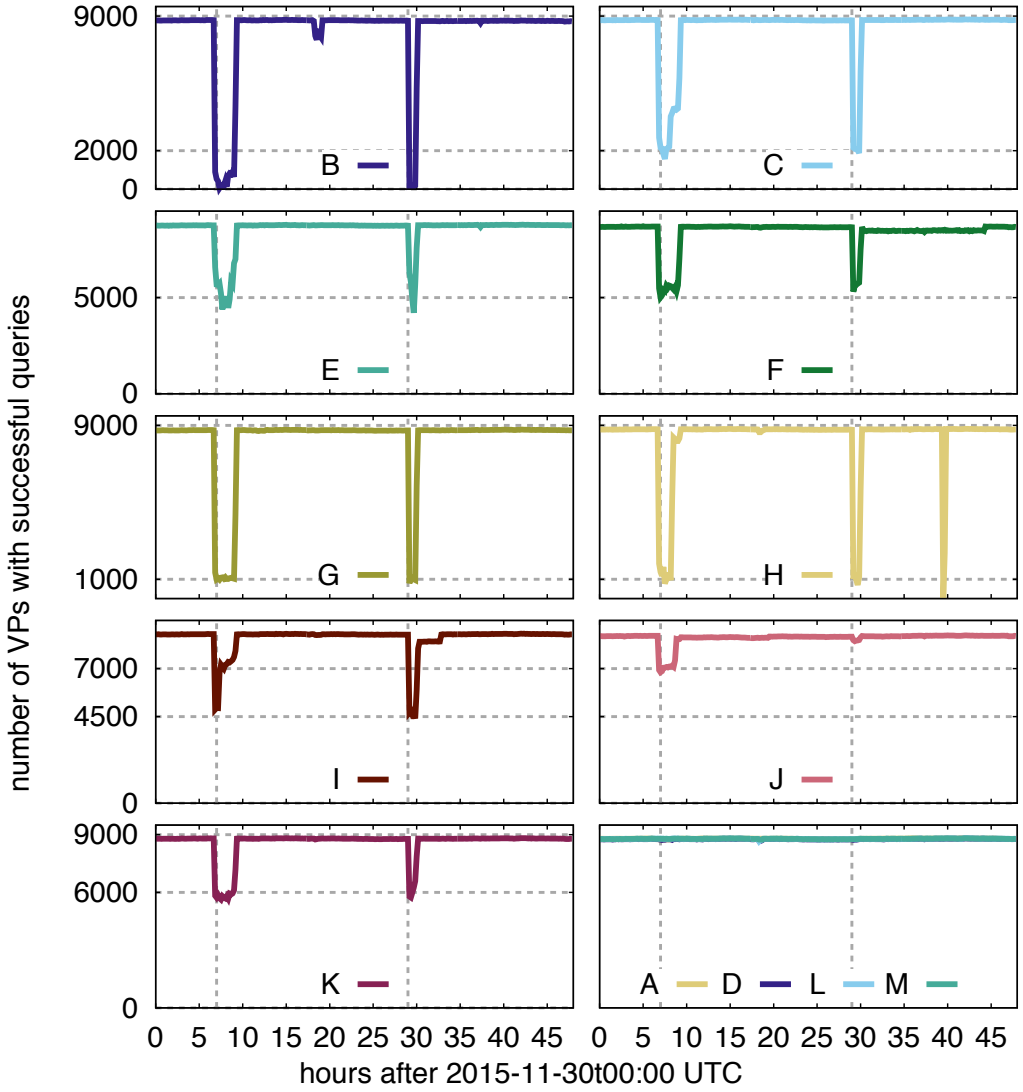
Most letters suffered

a bit (E, F, I, J, K)

a lot (B, C, G, H)

Did not see attack traffic

D, L, M



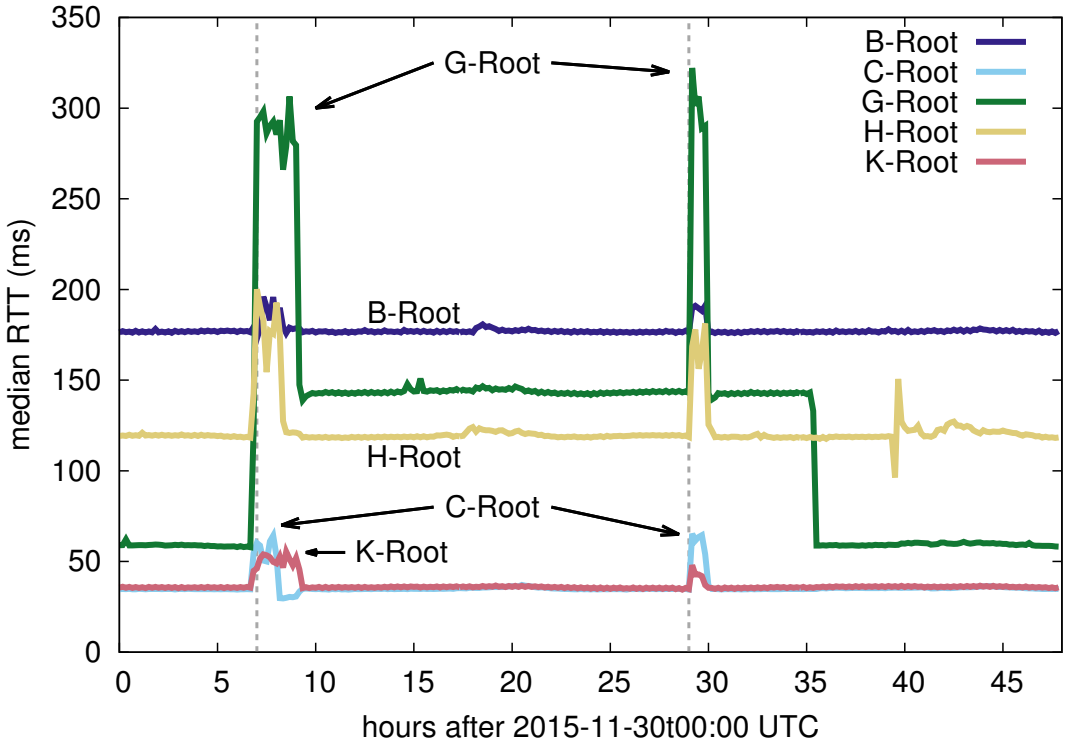
The **Impact** of the **Attack**

What was the impact?

For those that still see service...

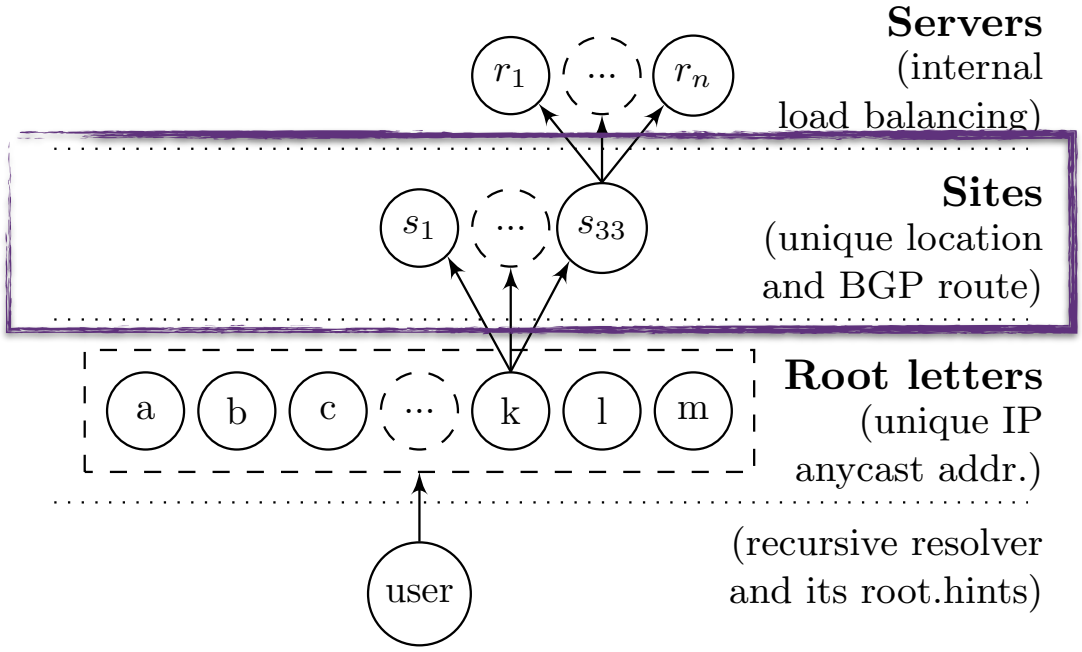
...performance problems

... 6x higher delay for **G**

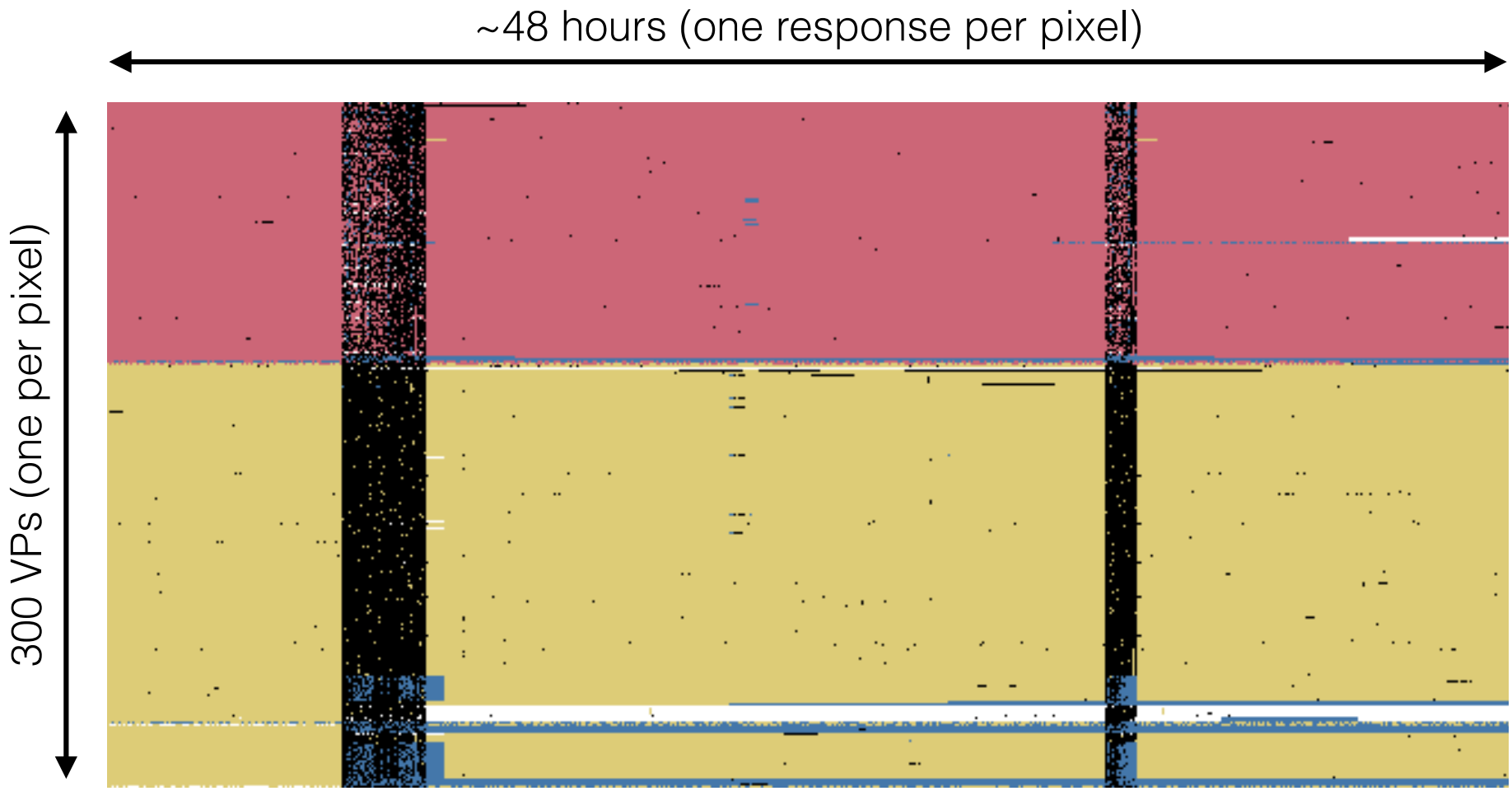


The **Impact** of the **Attack**

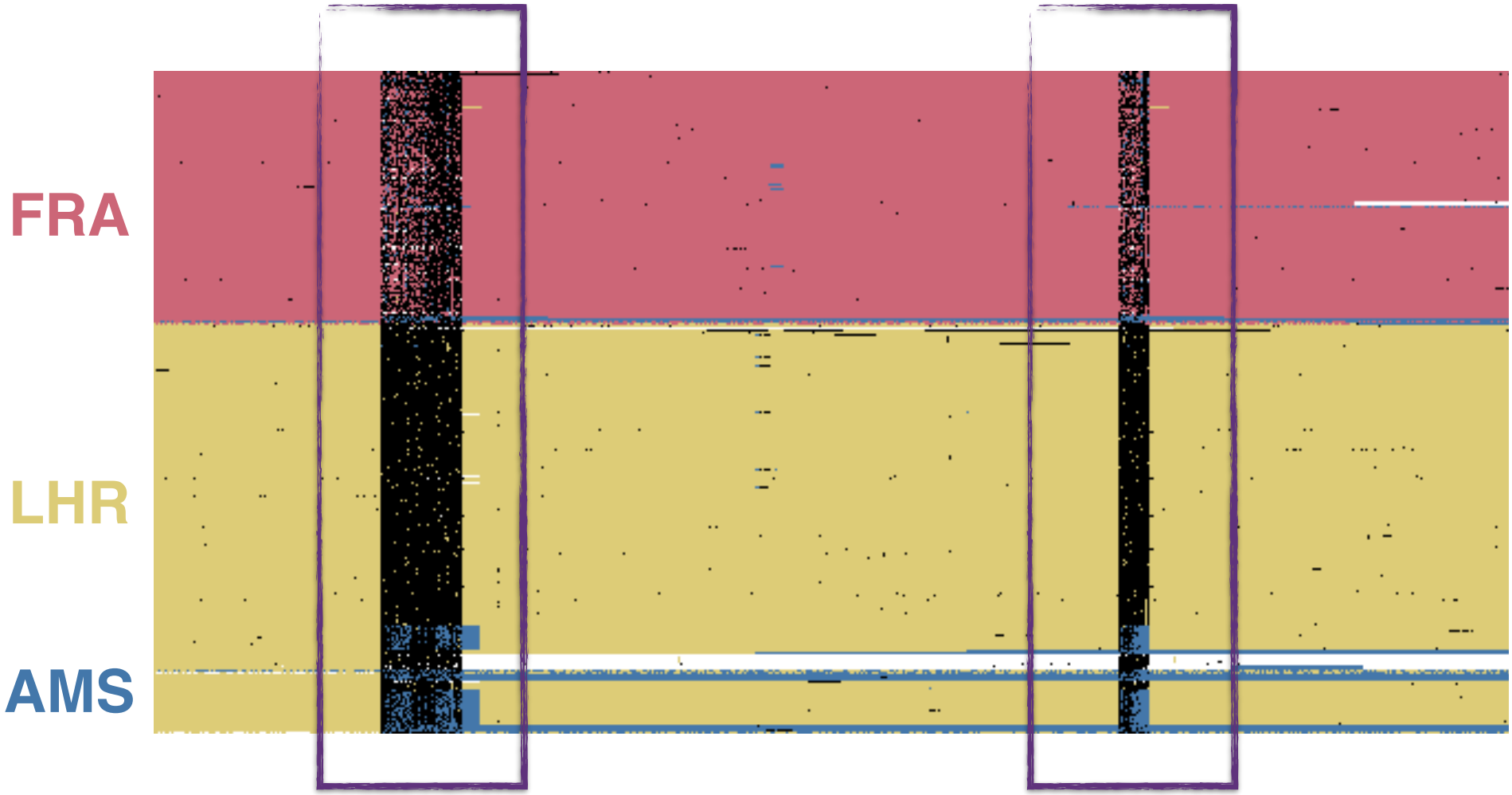
What was the impact at individual **sites**?



The **Impact** of the **Attack**

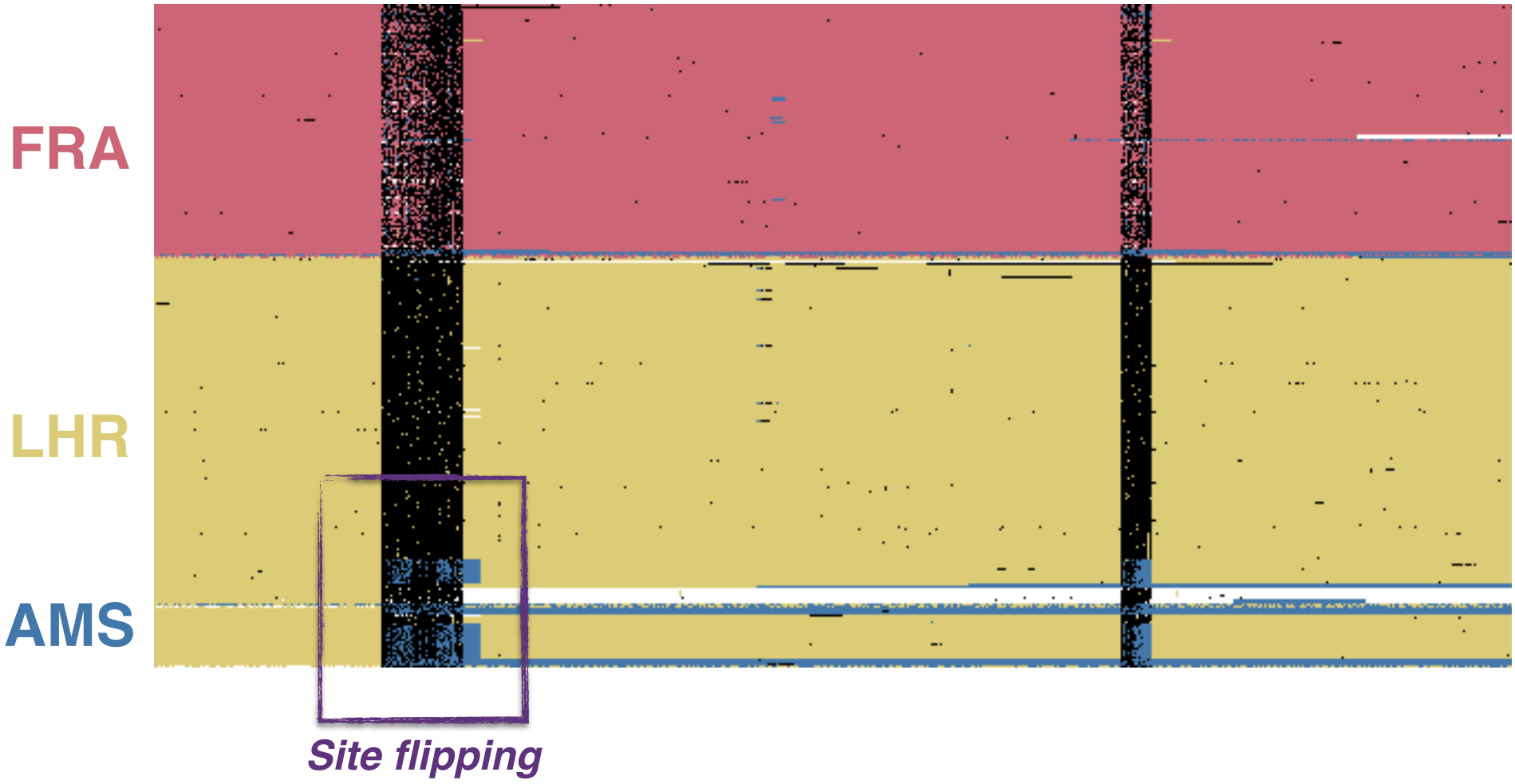


The **Impact** of the **Attack**



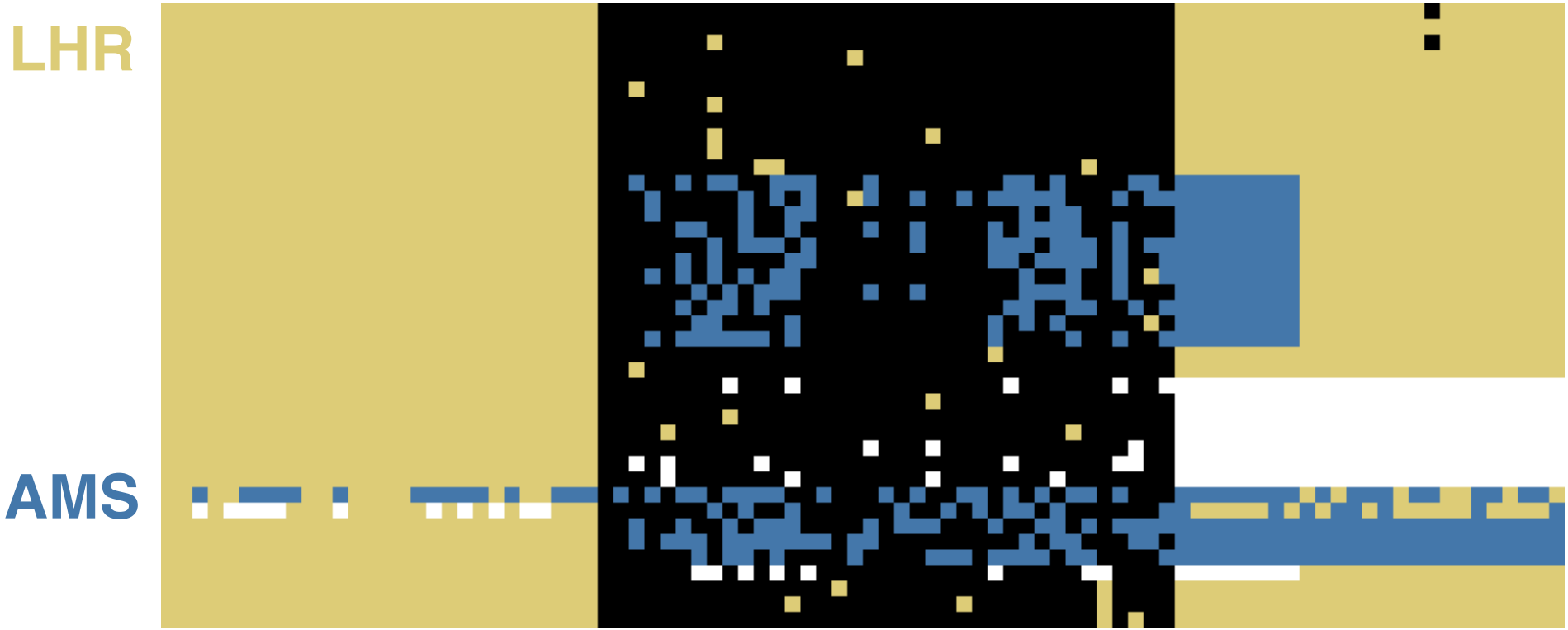
Blackout during attacks

The **Impact** of the **Attack**



The **Impact** of the **Attack**

Zoomed in: 40 VPs initially reaching LHR site

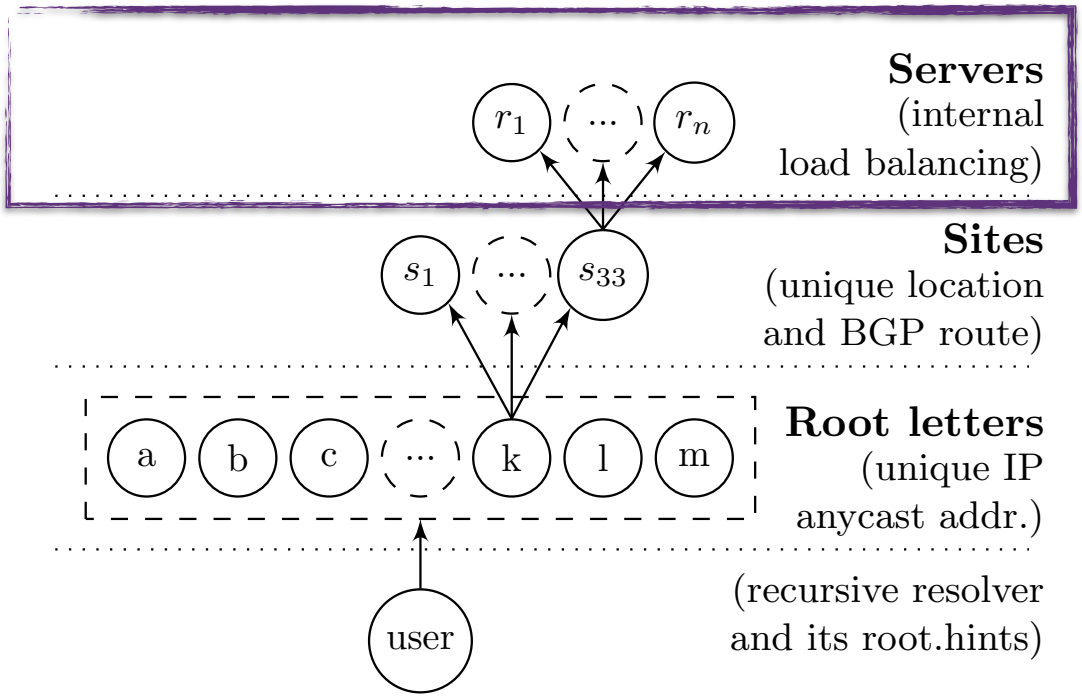


Nov. 30th

06:50 - 09:30 (UTC)

The **Impact** of the **Attack**

What was the impact
at individual **servers**?



The **Impact** of the **Attack**

What was the impact?

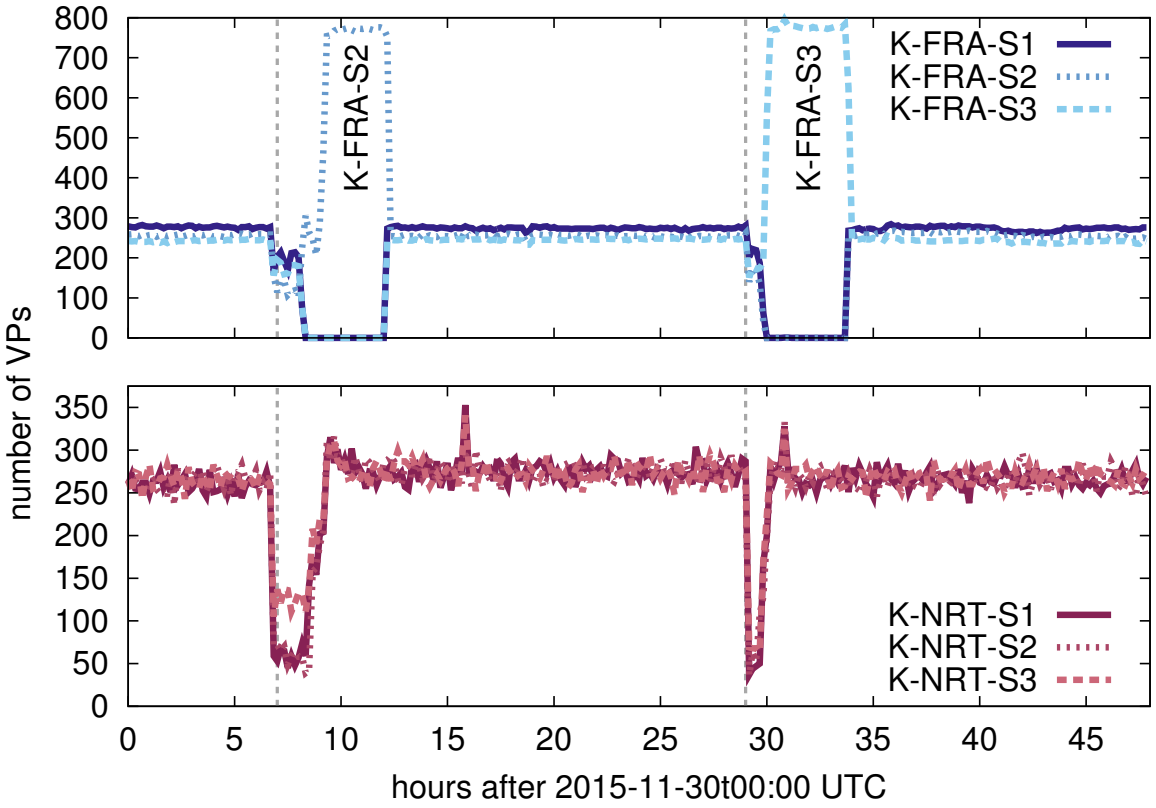
Impact at sites may depend...

... on load balancing

... on link resource

... on queuing

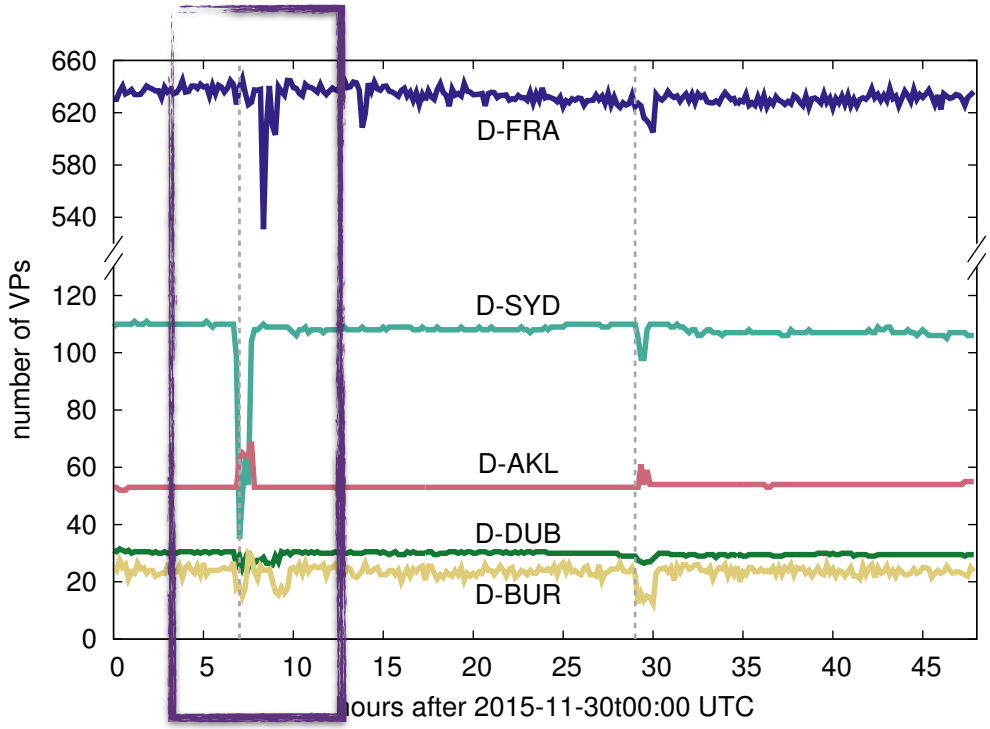
Individual server performance and reachability may not reflect site-wide situation.



The **Additional Impact**

Collateral damage!

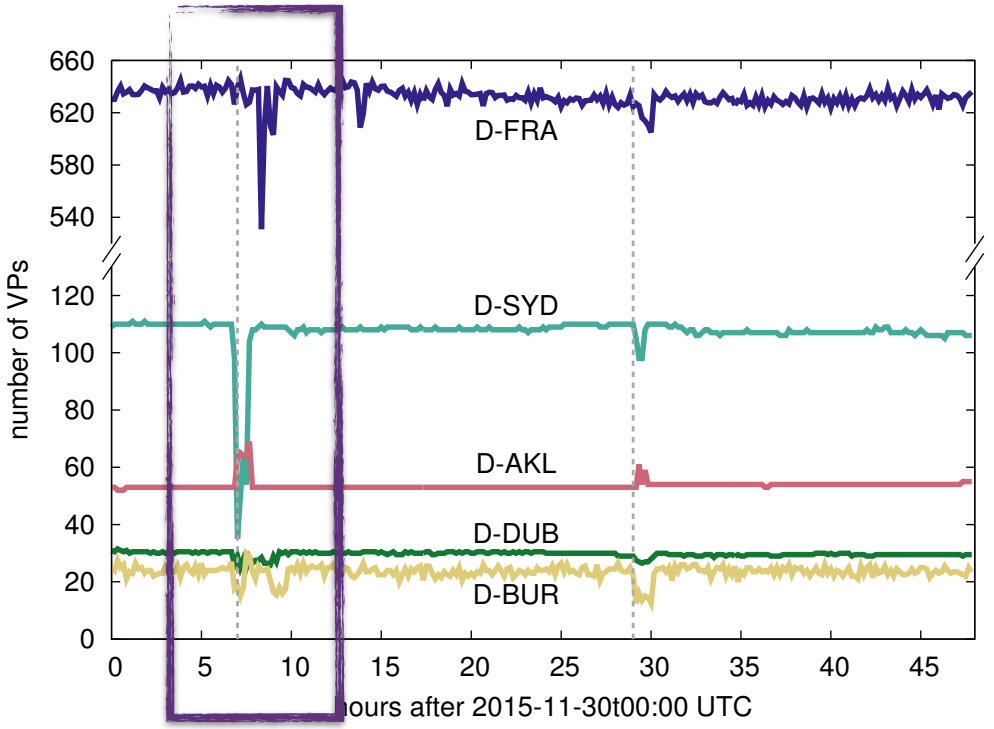
D-Root was not targeted...
... but *felt* the attack



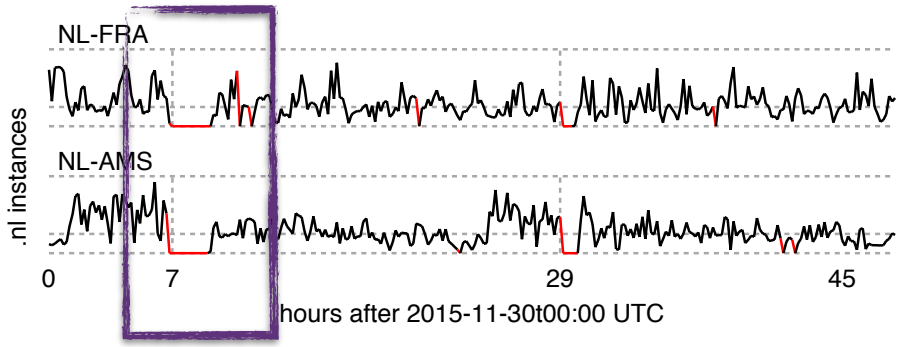
The **Additional Impact**

Collateral damage!

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



Even SIDN (TLD) 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 distributed 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.

r.schmidt@utwente.nl
http://www.ricardoschmidt.com

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/