

# DDoS

## What are the Scientific Challenges



Aiko Pras

[a.pras@utwente.nl](mailto:a.pras@utwente.nl)

<https://people.utwente.nl/a.pras>

University of Twente

the Netherlands



# University of Twente





# Internet Security group

---



Aiko Pras



Jeroen v.d. Ham  
NCSC



Jessica Steinberger  
FH Darmstadt



Anna Sperotto



João Ceron



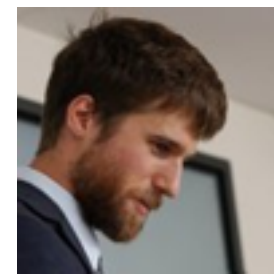
Christian Dietz  
UNIBWM



Jair Santanna



Luuk Hendriks



Olivier v.d. Toorn



Roland van Rijswijk  
SURFnet



Mattijs Jonker



Moritz Muller  
SIDN



Cristian Hesselman  
SIDN



Wouter de Vries



Nils Rodday  
UNIBWM

# Scientific Challenges ...

---



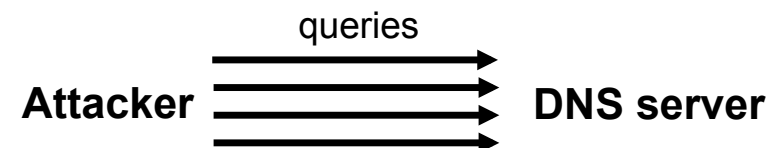


# Scientific Challenges ...



## Denial-Of-Service (DoS)

- Goal: overload or crash the server



- Problems:
  - Attacker may be too slow (CPU, network bandwidth,...)
  - Defense: block the attacker's IP address is easy

# Scientific Challenges ...

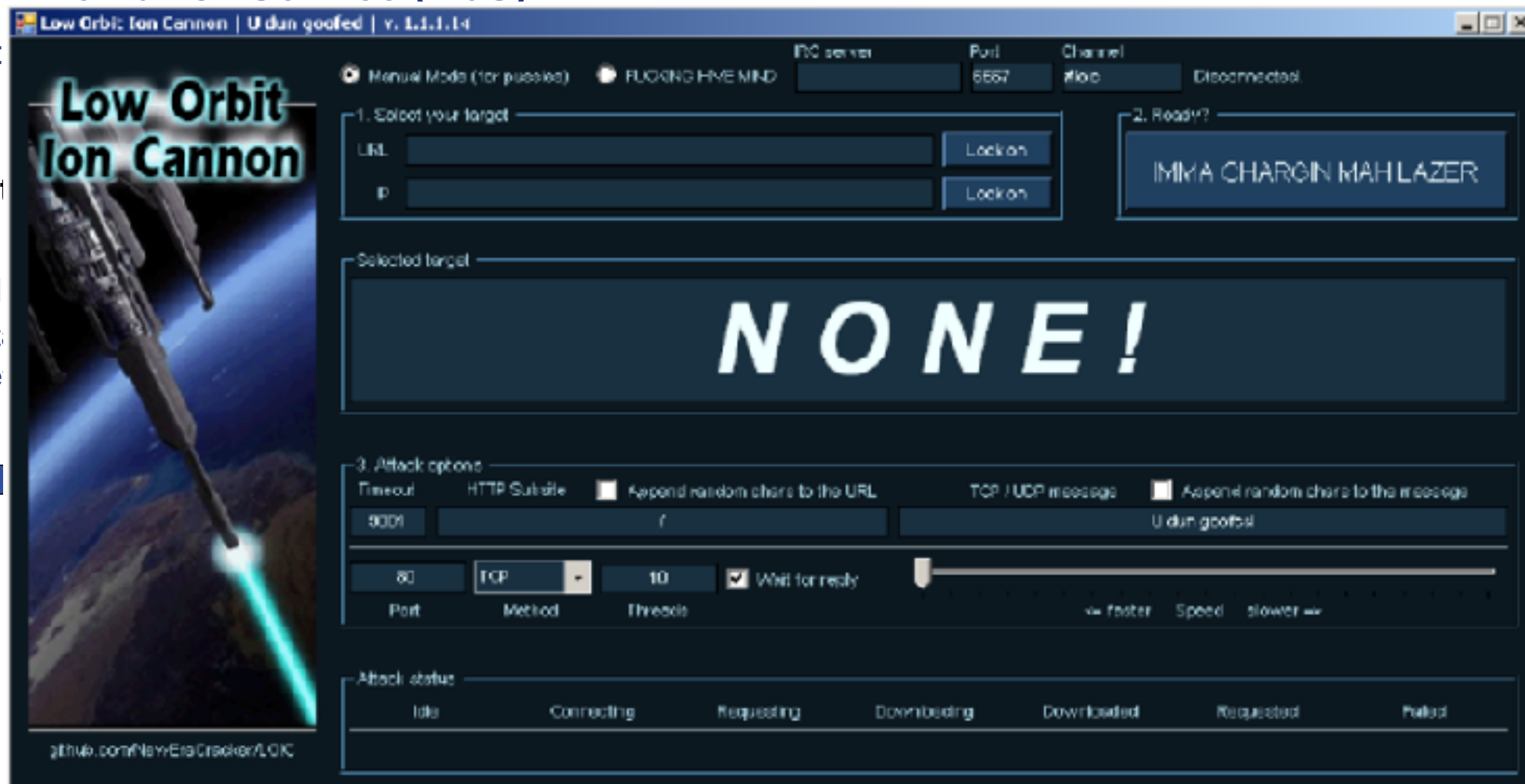
## Denial-Of-Service (DoS)

- Goal:

At

- Problem

- Attack
- Defense





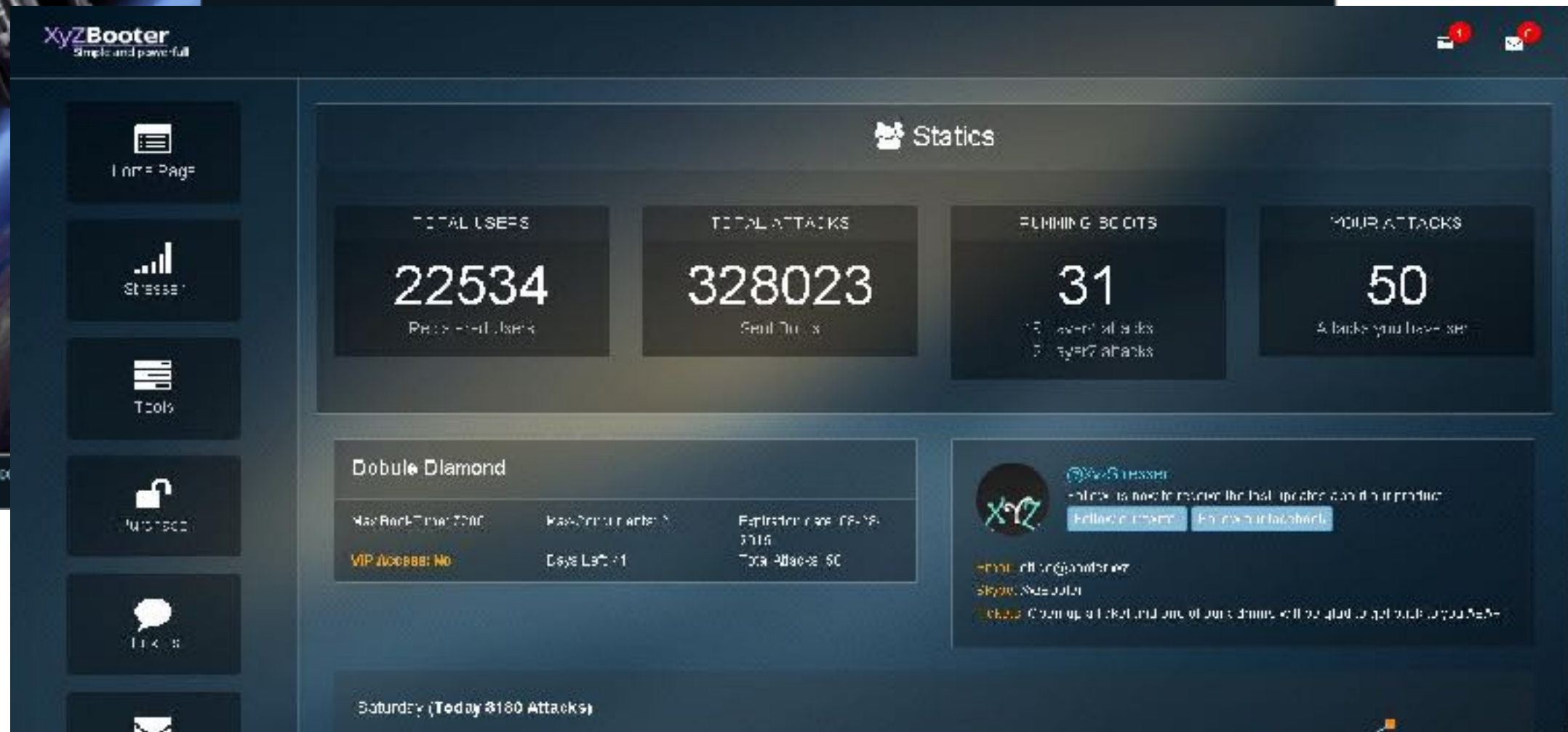
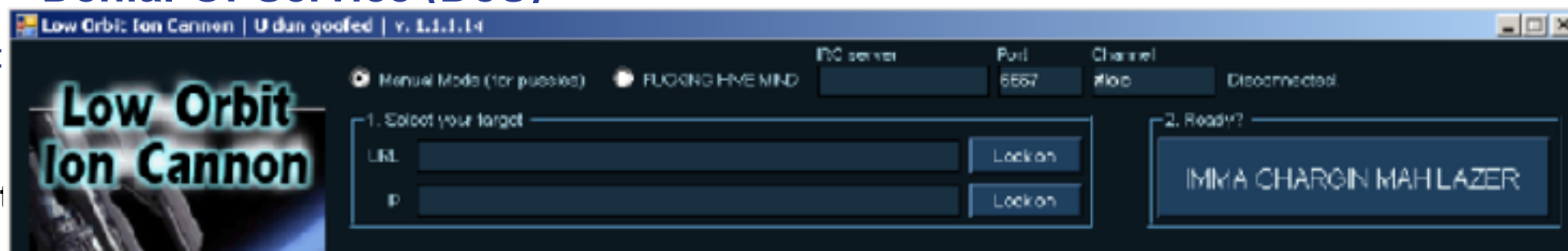
# Scientific Challenges ...

## Denial-Of-Service (DoS)

- Goal:

At

- Problem:
  - Attack
  - Denial





# Scientific Challenges ...

---

## DDoS 3.0 - How terrorists bring down the Internet

Aiko Pras, José Jair Santanna, Jessica Steinberger and Anna Sperotto

University of Twente  
Enschede, The Netherlands

`a.pras@utwente.nl`, `j.j.santanna@utwente.nl`, `jessica.steinberger@h-da.de`,  
`a.sperotto@utwente.nl`

**Abstract.** Dependable operation of the Internet is of crucial importance for our society. In recent years Distributed Denial of Service (DDoS) attacks have quickly become a major problem for the Internet. Most of these attacks are initiated by kids that target schools, ISPs, banks and web-shops; the Dutch NREN (SURFNet), for example, sees around 10 of such attacks per day. Performing attacks is extremely simple, since many websites offer “DDoS as a Service”; in fact it is easier to order a DDoS attack than to book a hotel! The websites that offer such DDoS attacks are called “Booters” or Stressers”, and are able to perform attacks with a strength of many Gbps. Although current attempts to mitigate attacks seem promising, analysis of recent attacks learns that it is quite easy to build next generation attack tools that are able to generate DDoS attacks with a strength thousand to one million times higher than the ones we see today. If such tools are used by nation-states or, more likely, terrorists, it should be possible to completely stop the Internet. This paper argues that we should prepare for such novel attacks.

MMB&DFT 2016  
Springer LNCS 9629



# Some Questions ...

---

- Where to get DDoS data from?
- How big is a typical attack?
- Who is attacked?
- What financial damage is caused by attacks?
- What does a typical attack structure look like?
- What are the most important booters?
- Which booter is responsible for the attack?
- Who is protected by DPS?
- Is blackholing being used?
- What happens if booters are seized by the police?



# Intro:

# Where to get DDoS data from?



# Where to get DDoS data from?

---

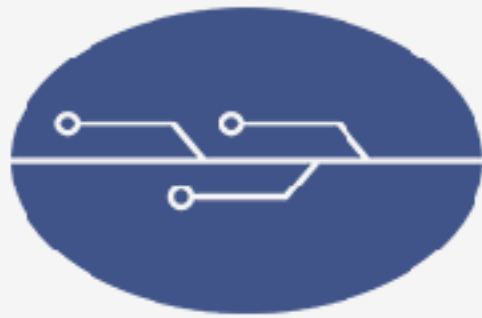
- Targets of attacks
- ISPs
- Akamai / Cloudflare
- Symantic: high-interaction IoT honeypots
- ...

# Leaked Databases

<b>Booter domain name</b>	<b>Total Attacks</b>	<b>Dataset span* [days]</b>	<b>First attack</b>
booter.tw	48844	403	24/01/13
legionbooter.info	38248	134	04/04/13
pokeboot.com	6915	83	10/12/12
superstresser.com	5565	36	12/02/14
national-stresser.com	2756	93	05/09/13
212-booter.net	1993	57	04/07/13
notoriousbooter.com	879	99	20/01/14
vaporizebooter.info	725	971	05/09/11
xrshellbooter.com	629	41	19/03/12
flashstresser.net	580	32	24/05/13
Nullboot.net	343	65	20/01/14
panicstresser.com	209	0	30/07/12
hazardstresser.com	173	88	15/03/13
vstresser.com	157	423	01/02/13
pandabooter.com	104	258	05/09/11



# SISSDEN / Shadowserver



## ***SISSDEN***

Secure Information Sharing Sensor Delivery Event Network

### **About**

SISSDEN will improve the cybersecurity posture of EU organisations and citizens through the development of increased situational awareness and the effective sharing of actionable information. SISSDEN builds on the experience of The Shadowserver Foundation, a non-profit organisation well known in the security community for its successful efforts in the mitigation of botnets and fighting malware propagation. SISSDEN will provide free-of-charge victim notification services, and work in close collaboration with Law Enforcement Agencies, national CERTs, network owners, service providers, small and medium-sized enterprises (SMEs) and individual citizens.



*This project has received funding from the European Union's Horizon 2020 research and Innovation programme under grant agreement No 700176. [More info..](#)*

<https://sisssden.eu>

# Cambridge Cybercrime Centre



Search

[Contact us](#) | [A-Z](#) | [Advanced search](#)

## Computer Laboratory

### Cambridge Cybercrime Centre: Process for working with our data

This page sets out the steps in the process for obtaining data from the Cybercrime Centre.

#### Assess whether you will be allowed to use our data

Our datasets are intended for research and analysis into methods to find, understand, investigate and counter cybercrime so your project must clearly fall into this space. Although we do not require researchers to be academics, there are significant restrictions on using our data for commercial purposes.

Although some of our data was generated internally and so we can make it available for other types of project and for commercial purposes, much of our data has come from third parties and they have only provided us with the data because of the framework under which it will be shared.

#### Identify the data you wish to use

We describe our various datasets [on this page](#). The descriptions are public and necessarily fairly high level. We do however try to indicate the size of the datasets, the period over which they was collected, along with possible causes of bias.

We strongly encourage the use of prepacked datasets rather than "live feeds". Although a live feed may be superficially attractive it makes it harder to arrange that other researchers can receive the same data that you did -- a key aim of the Cybercrime Centre is to enable reproducible research. If the issue is that you need to collect a further "field" over and above what we supply then talk with us and we may well be able to do this for you.

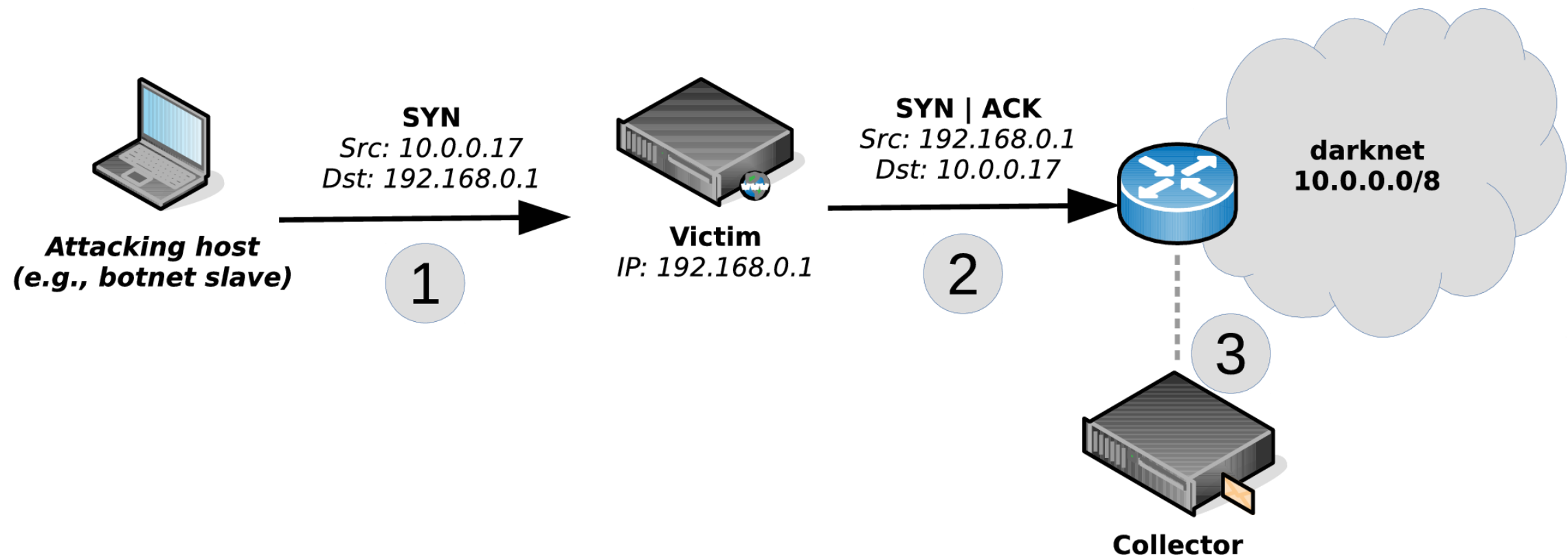
#### Read about our legal framework

It is important that you understand the basis on which we share data and the paperwork that will need to be signed.

There's several pages of explanations and FAQs about our agreements, starting here at <https://www.cambridgecybercrime.uk/data.html>, which you should read before contacting us.

# UCSD Network Telescope

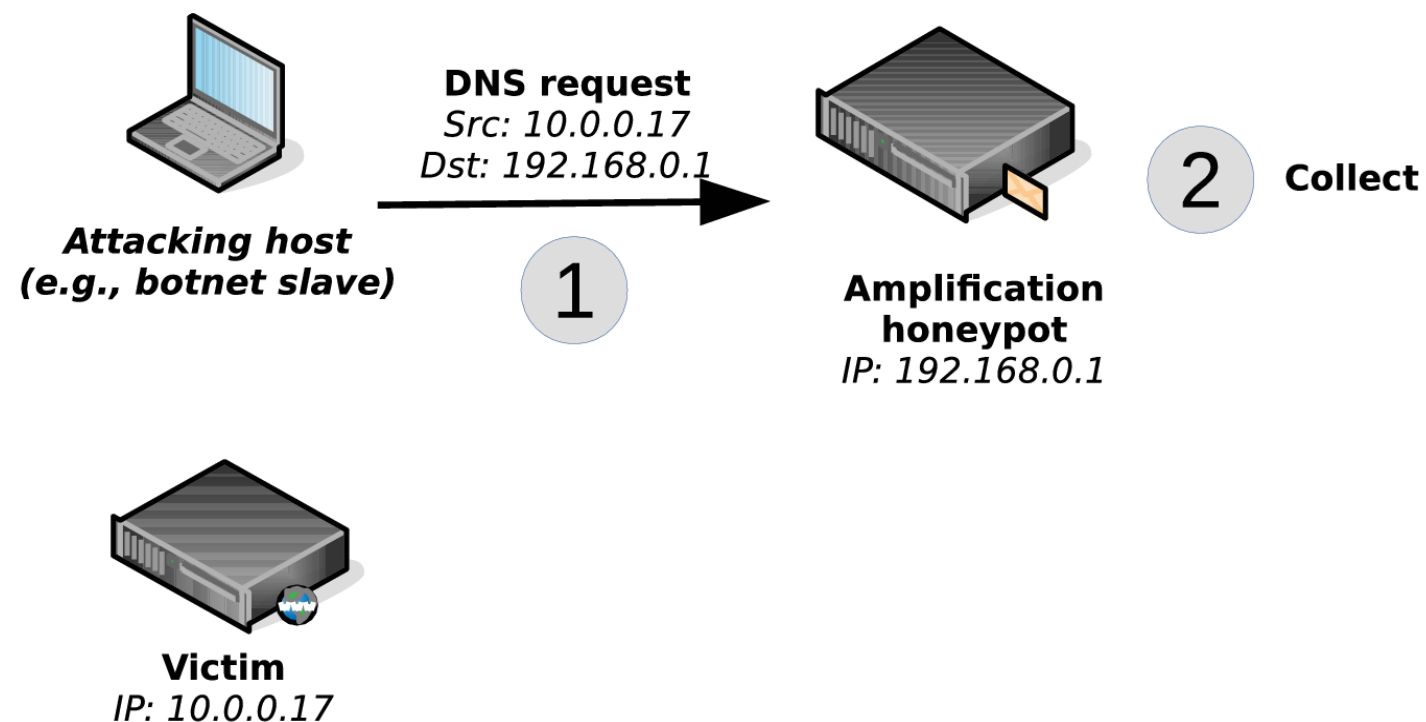
- A /8 darknet
- Captures DoS attacks with randomly (and uniformly) spoofed IP addresses
- Captures  $\sim 1/256$ th of IPv4 address space Any sizeable attack should be visible



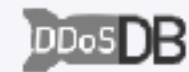


# AmpPot

- Honeypot that mimicks reflectors
  - various protocols (e.g., NTP, DNS, and CharGen)
- Tries to be appealing to attackers
  - i.e., by offering large amplification
- Twenty-four AmpPot instances
  - Geographically & logically distributed



# DDoSDB

[About](#)[Log in](#)[Request access](#)

Collecting and Sharing the most important information  
of DDoS attacks

[Search](#)

## What is DDoSDB?

DDoSDB is a platform for helping victims of DDoS attacks, the academic community, and the security community to share and get access to actual and enriched information of DDoS attacks. The purpose of sharing attacks is to enable comparison with other attacks, facilitate legal attribution, and improve detection and mitigation strategies.

DDoSDB provides an interface for searching unique characteristics of attacks (fingerprints) and also provides a sample of its actual attack data (ex. pcap and nfdump file). All data within DDoSDB come from collaborators that own attack data (usually collected as victim). We facilitate collaborators data sharing by providing an open source code that analyses an attack, generates fingerprints, and anonymizes the identity of the victim ([link](#)).

<https://ddosdb.org>



# Research Question 1

How big is a typical attack?



# Follow the news

---



# Follow the news

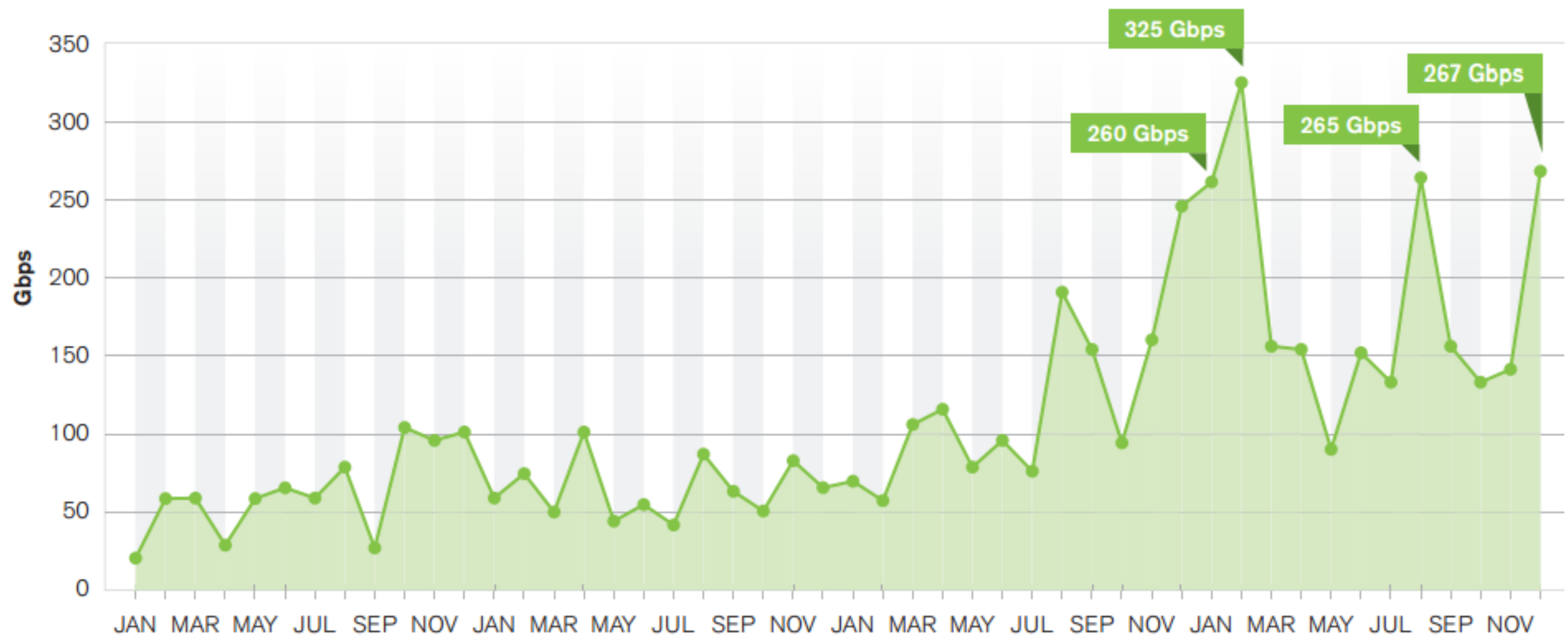
**Krebs on Security**

In-depth security news and investigation



2014

**ATLAS Peak Attack Sizes Month by Month (Gbps)**





## DDoS Attacks on Krebs on Security

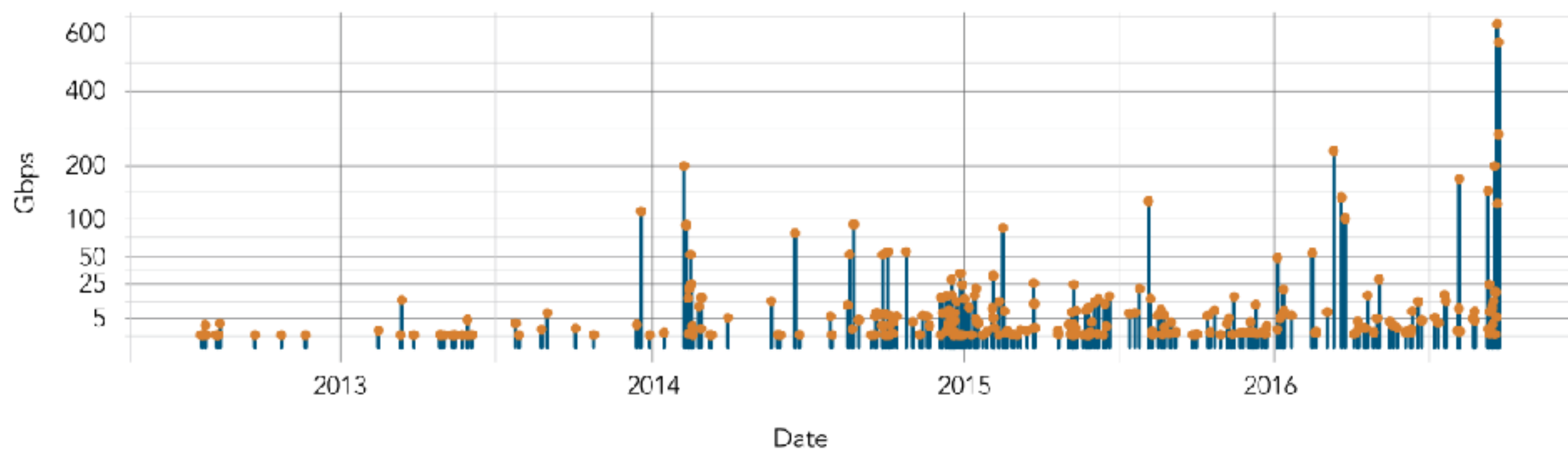


Figure 2-6: All attacks mitigated for krebsonsecurity.com while on the routed platform

SUPER SOAKER —

# In-the-wild DDoSes use new way to achieve unthinkable sizes

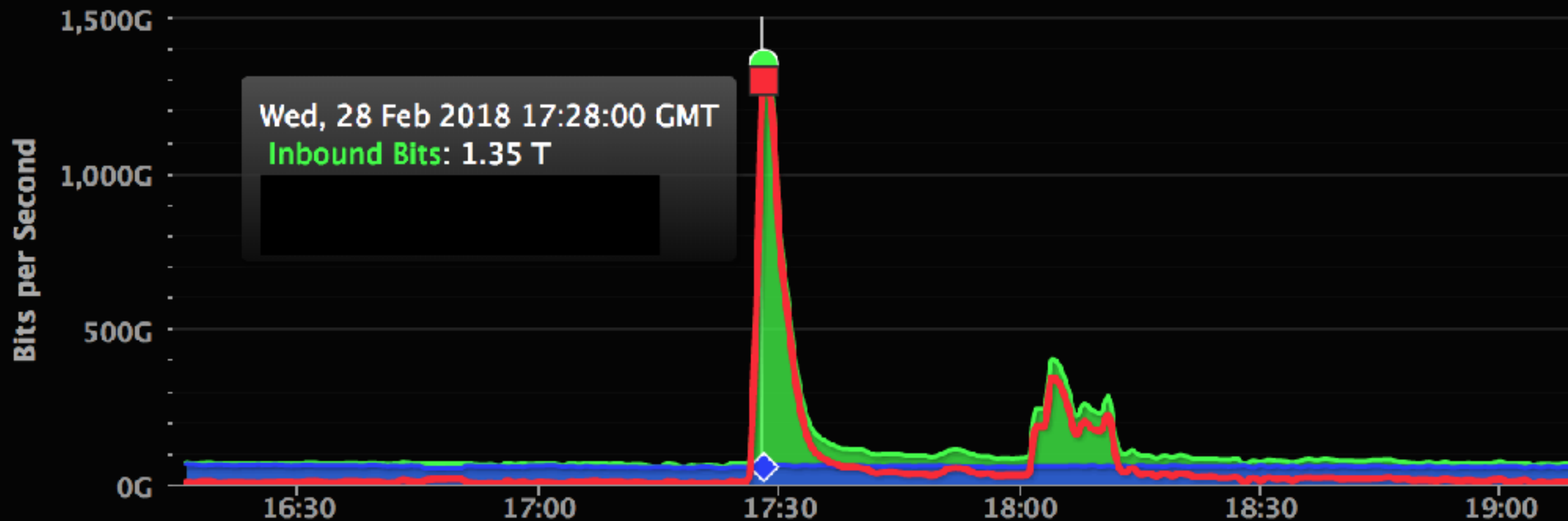
Attackers abuse “memcached” to amplify volumes by an unprecedented factor of 51k.

DAN GOODIN - 2/27/2018, 9:18 PM

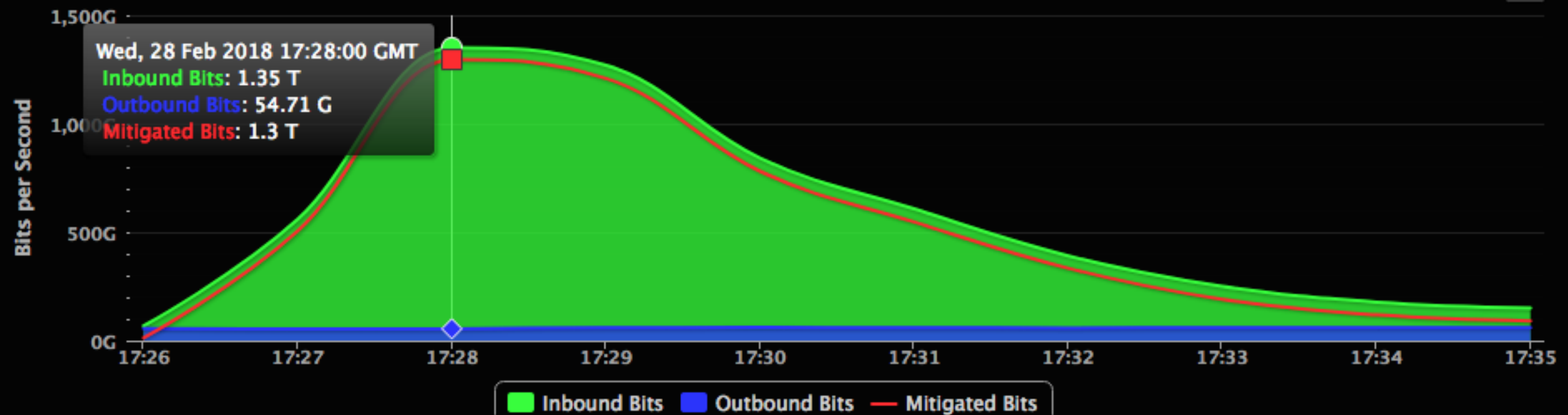
## GitHub survives massive DDoS attack relatively unscathed

Despite 1.3 Tbps of traffic, the site was only bogged down for 10 minutes.

## ALL BORDER Bits per Second



## ALL BORDER Bits per Second

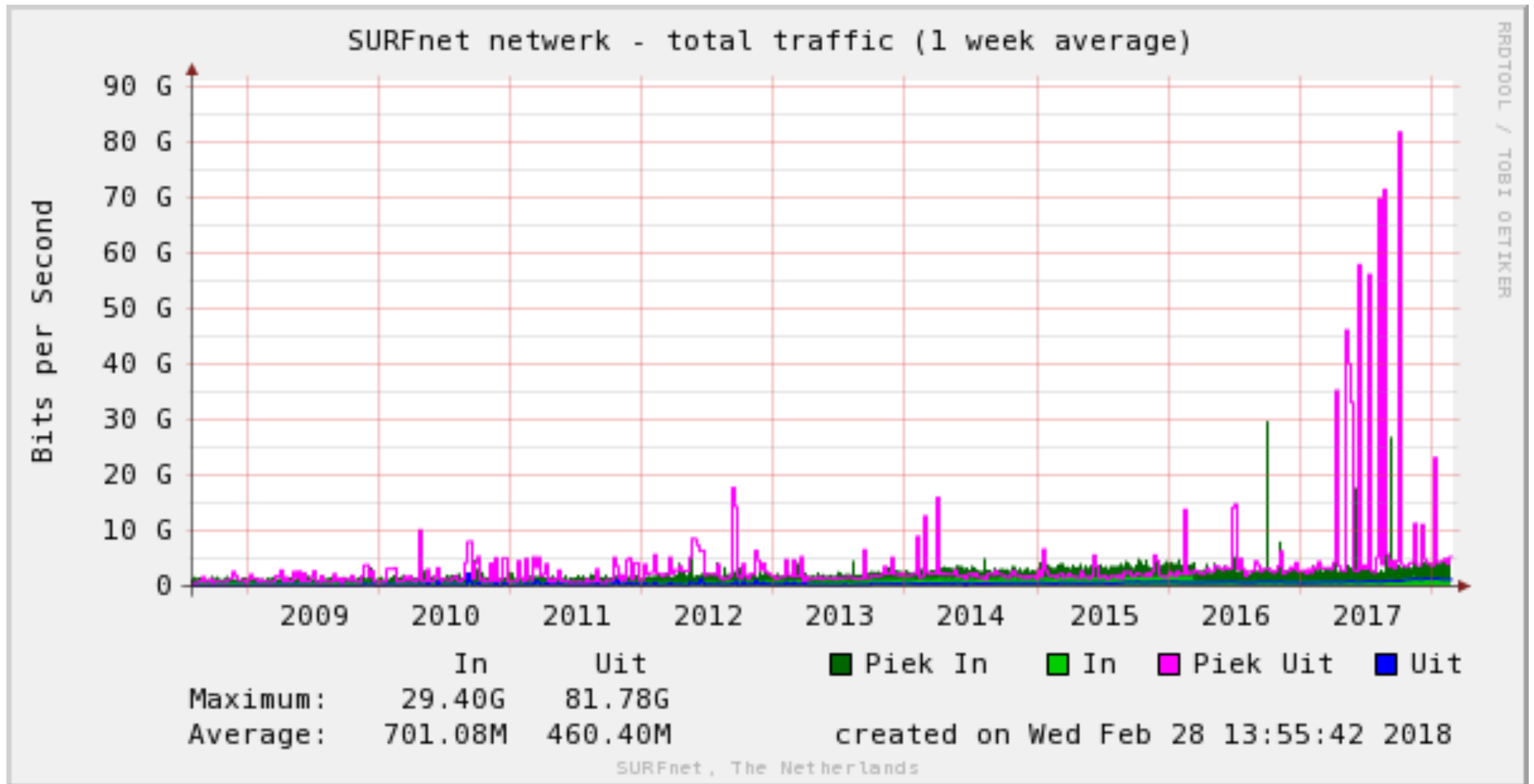




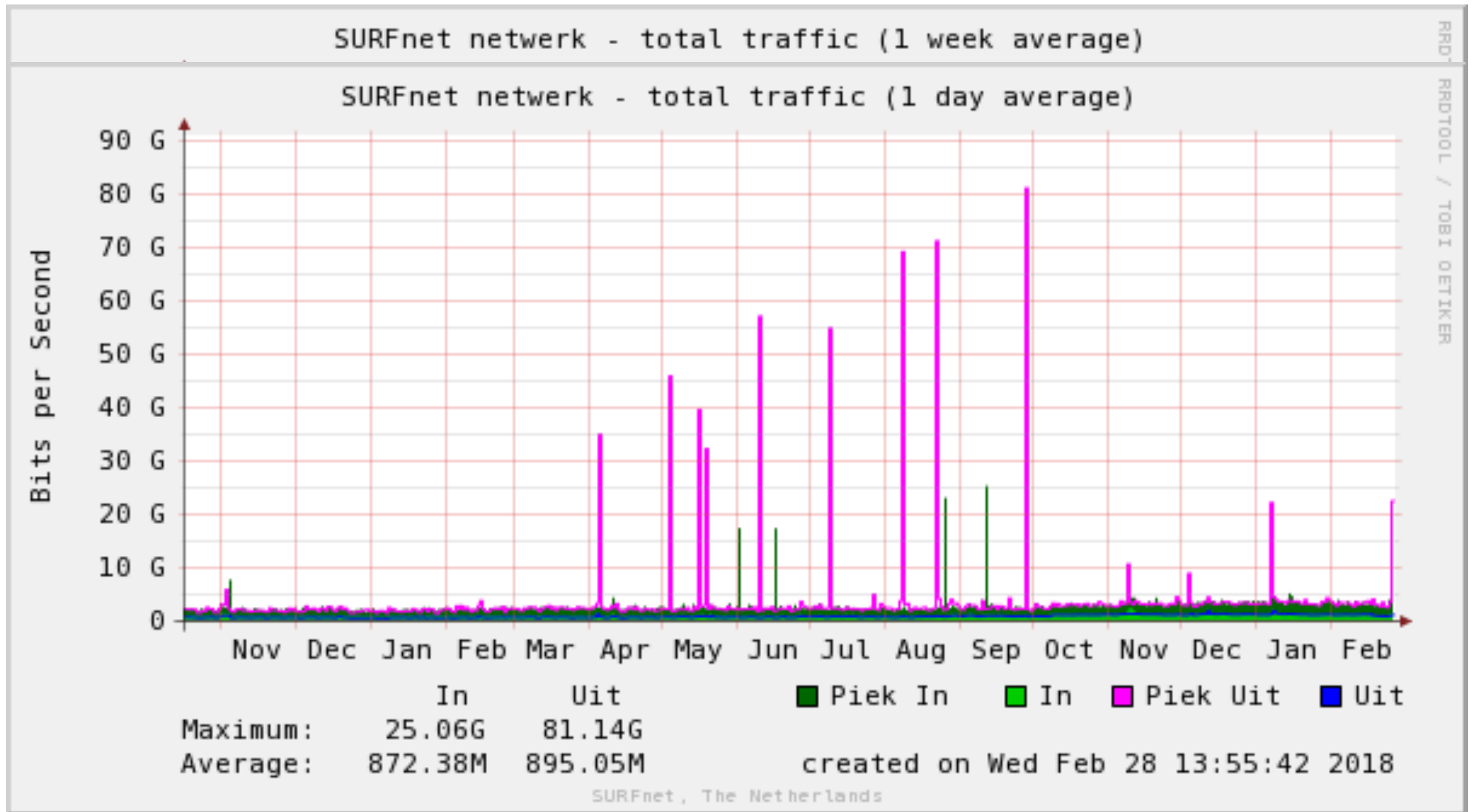
# Get provider data

---

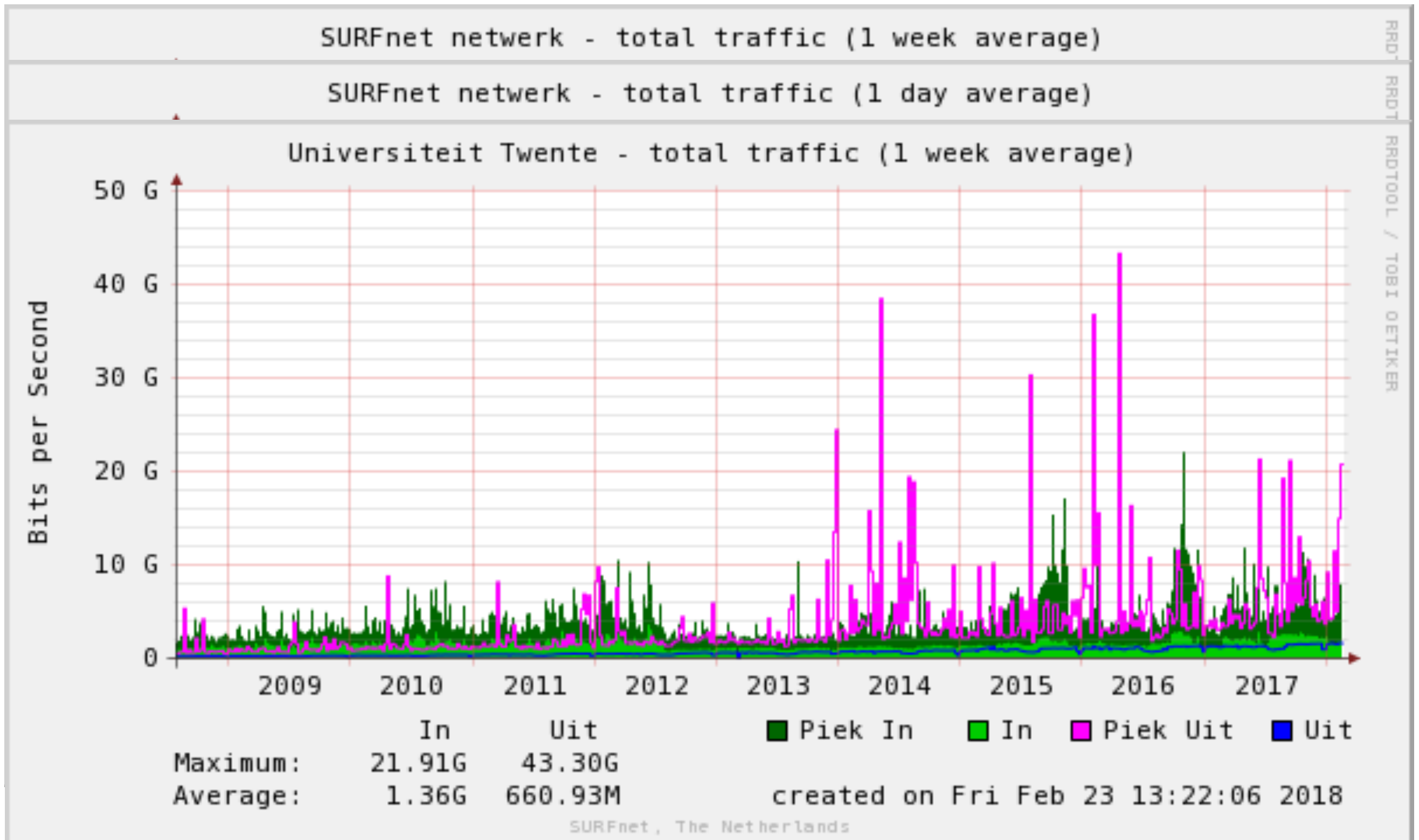
# Get provider data



# Get provider data

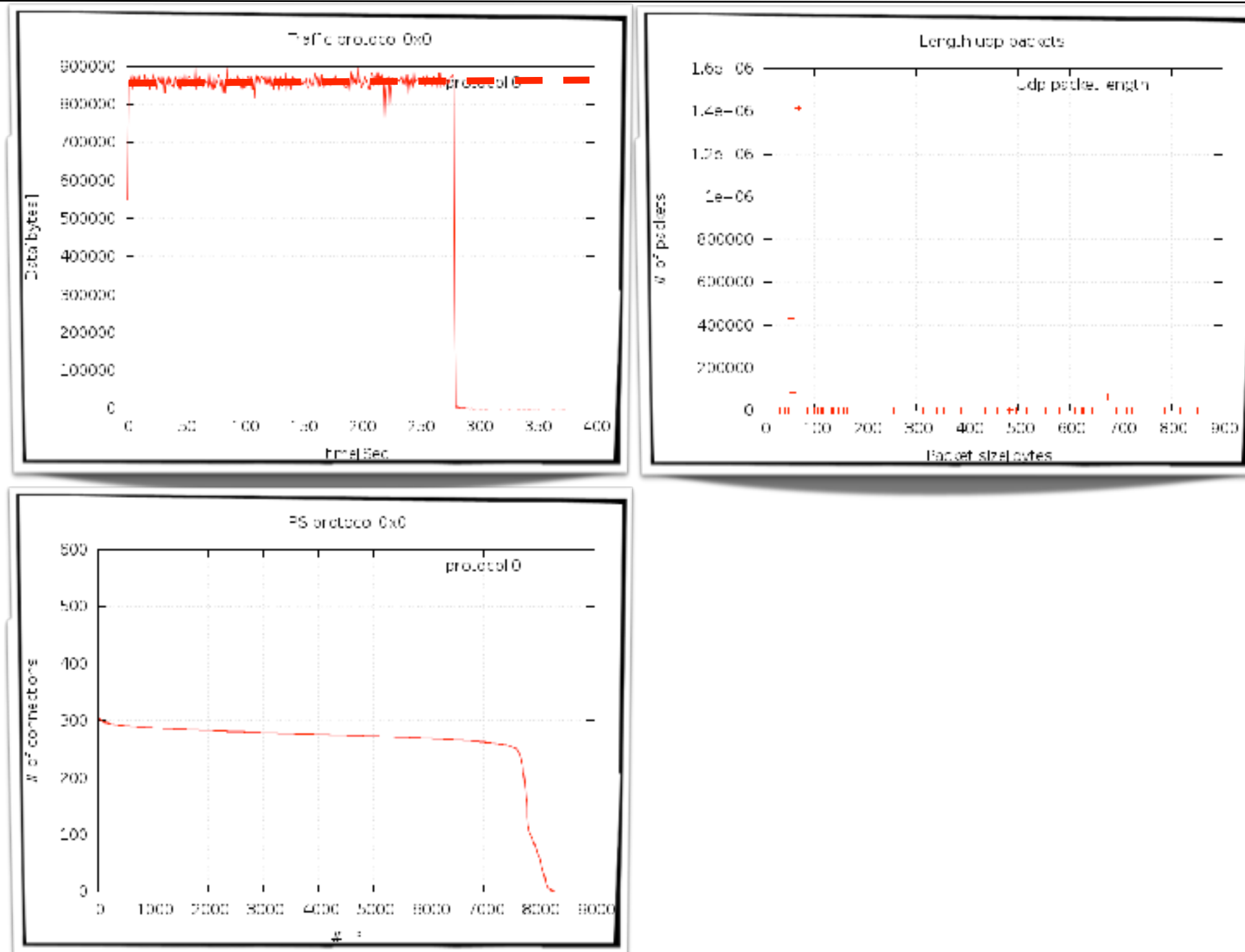


# Get provider data

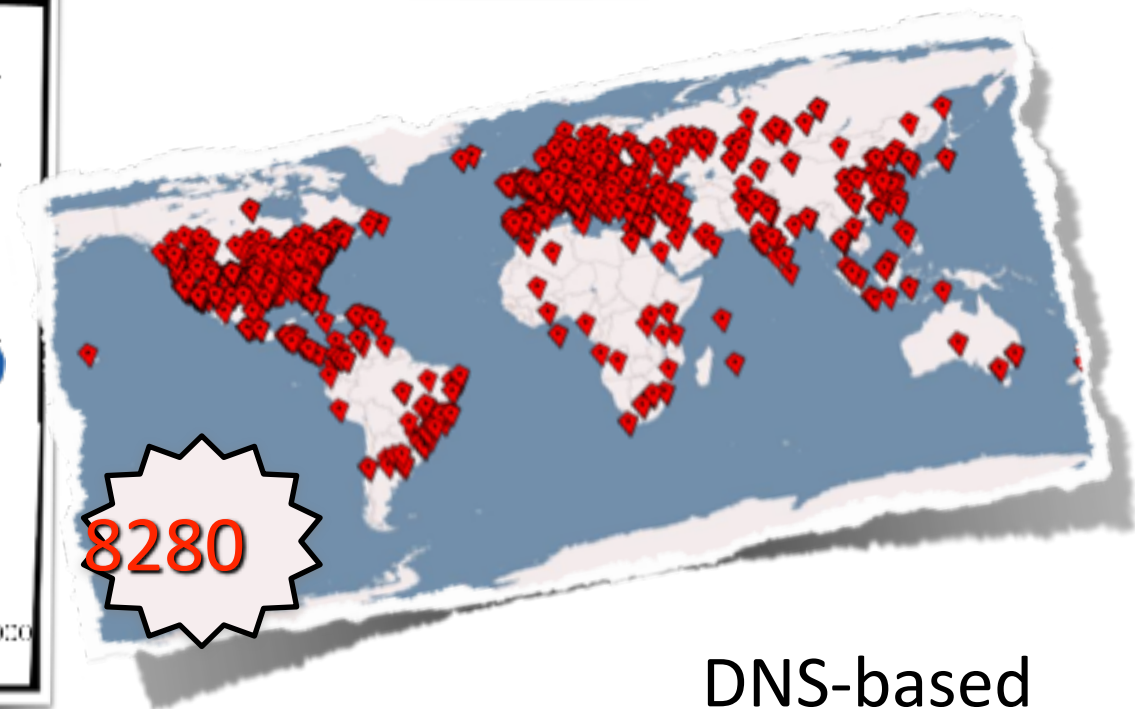
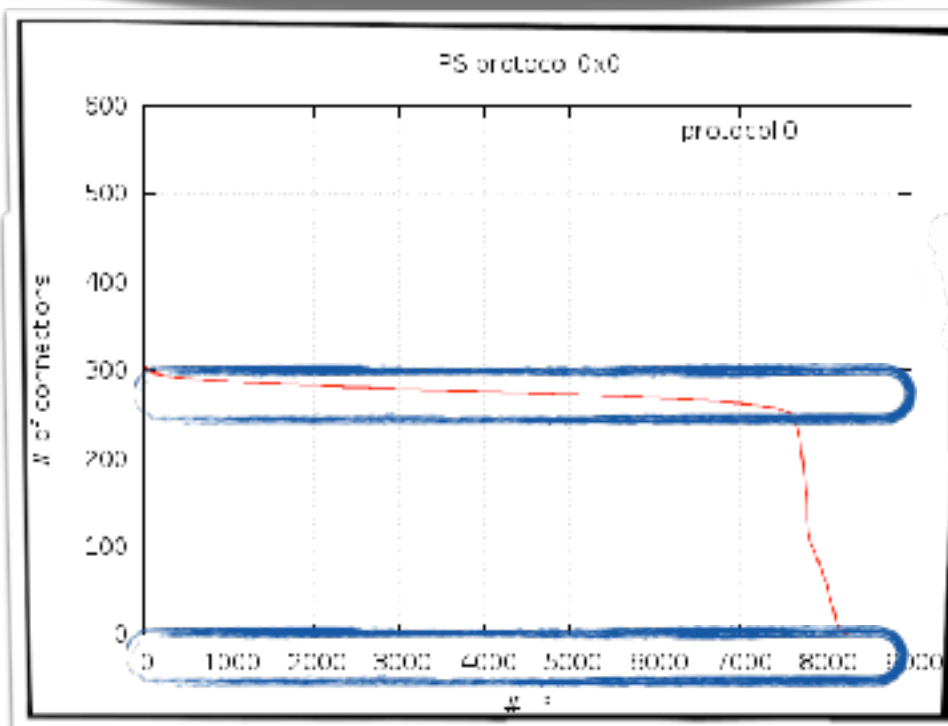
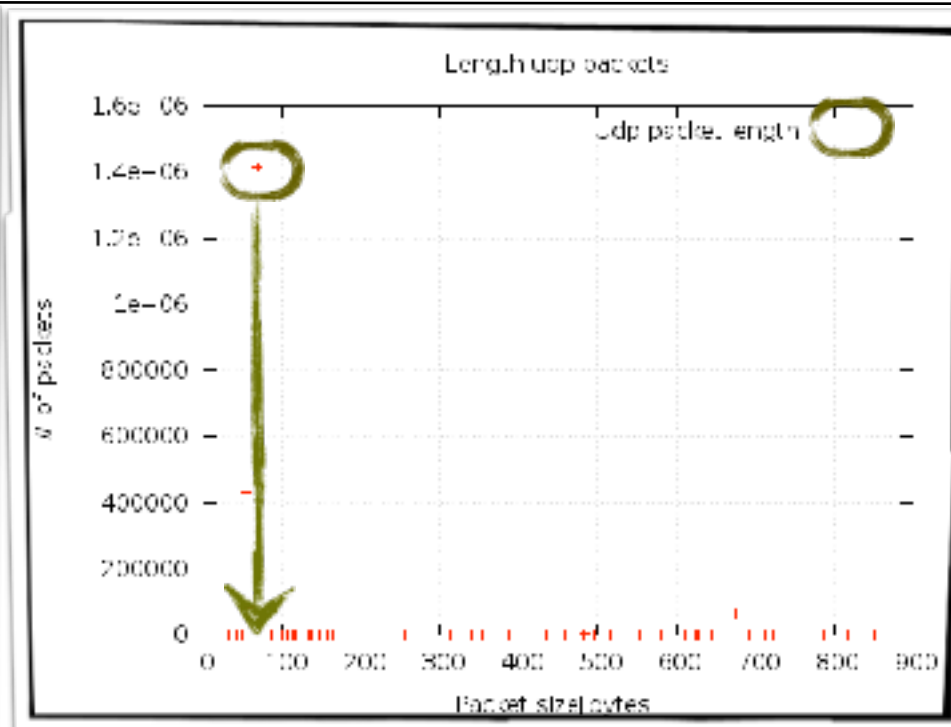
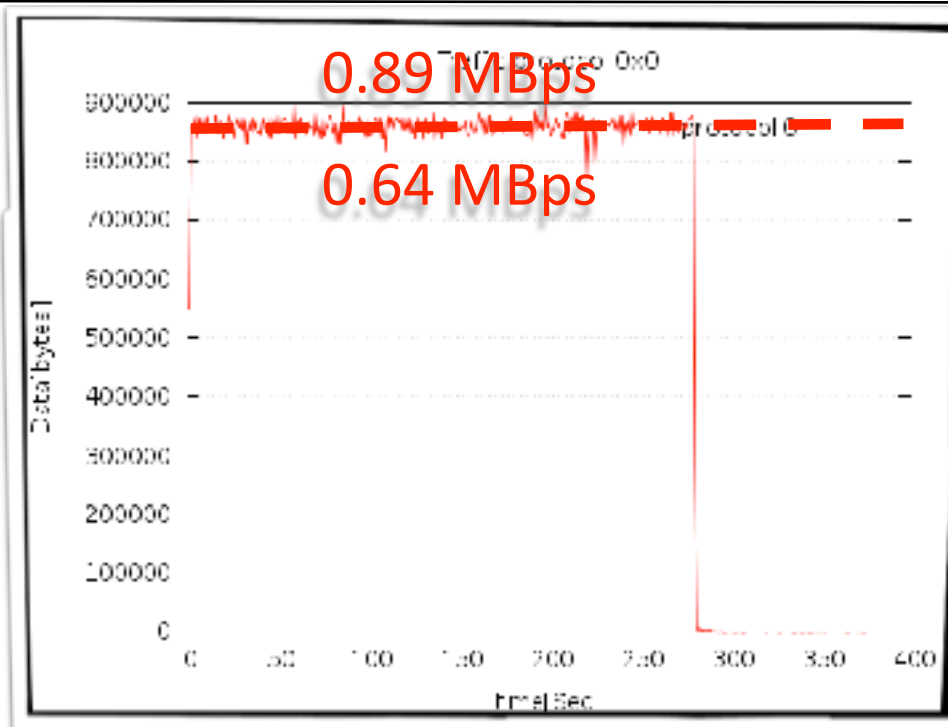




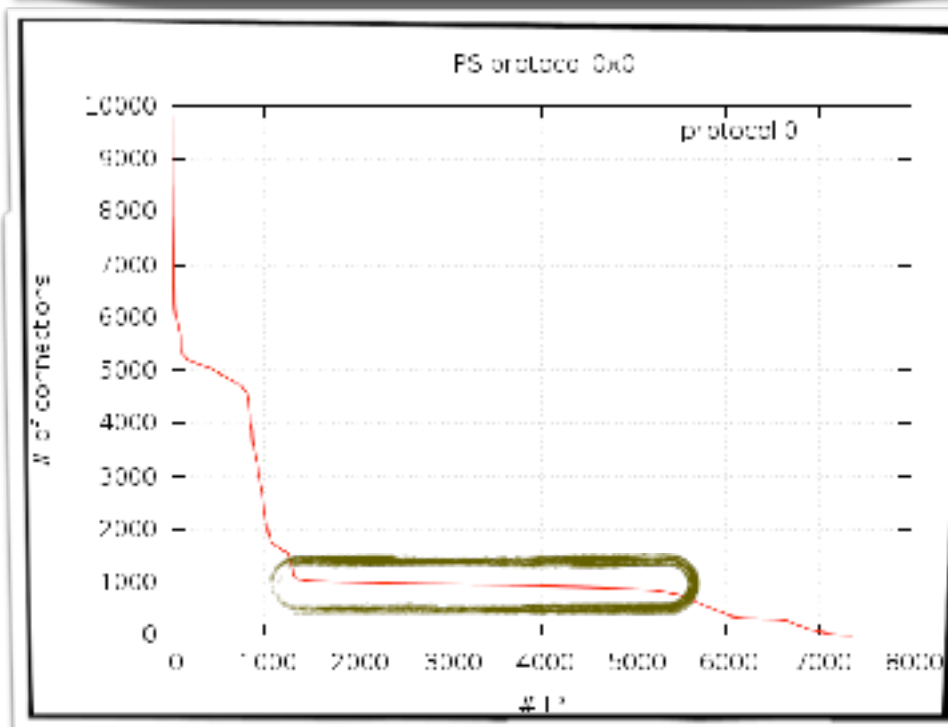
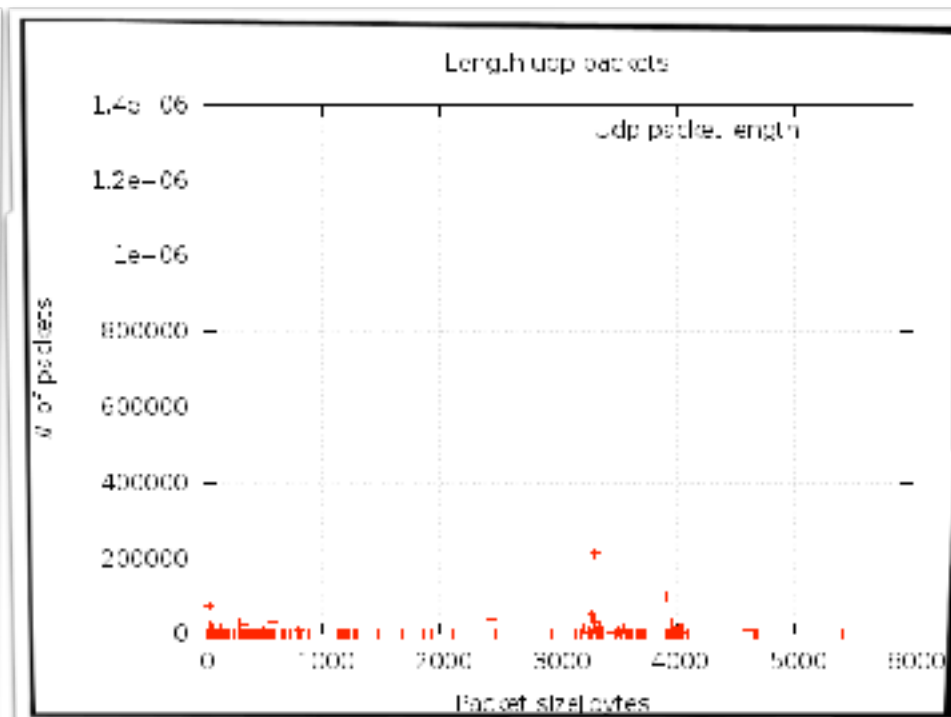
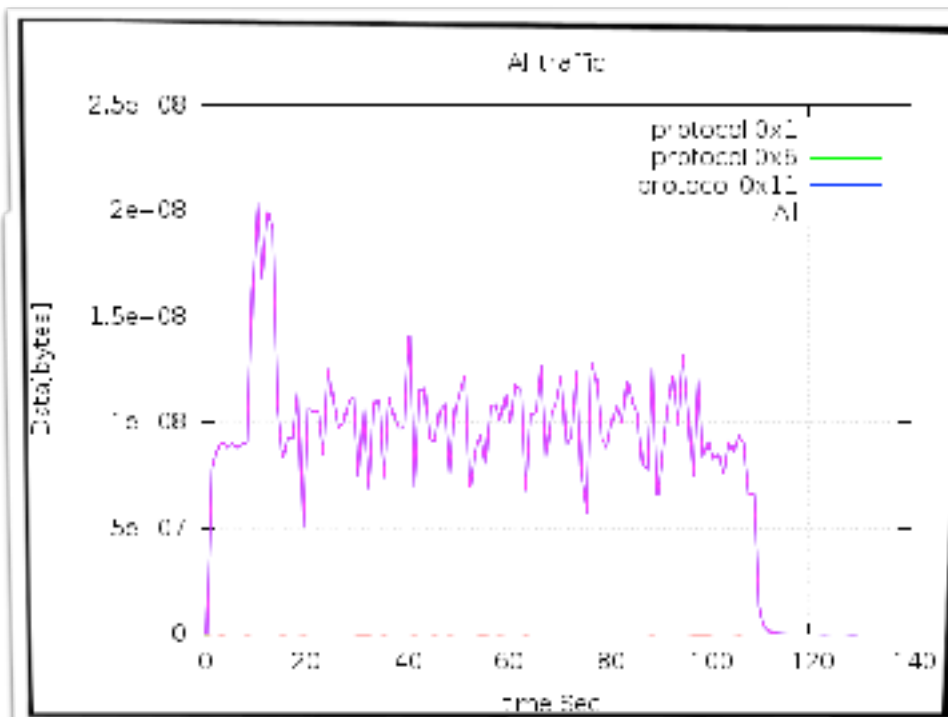
# Measure at the target

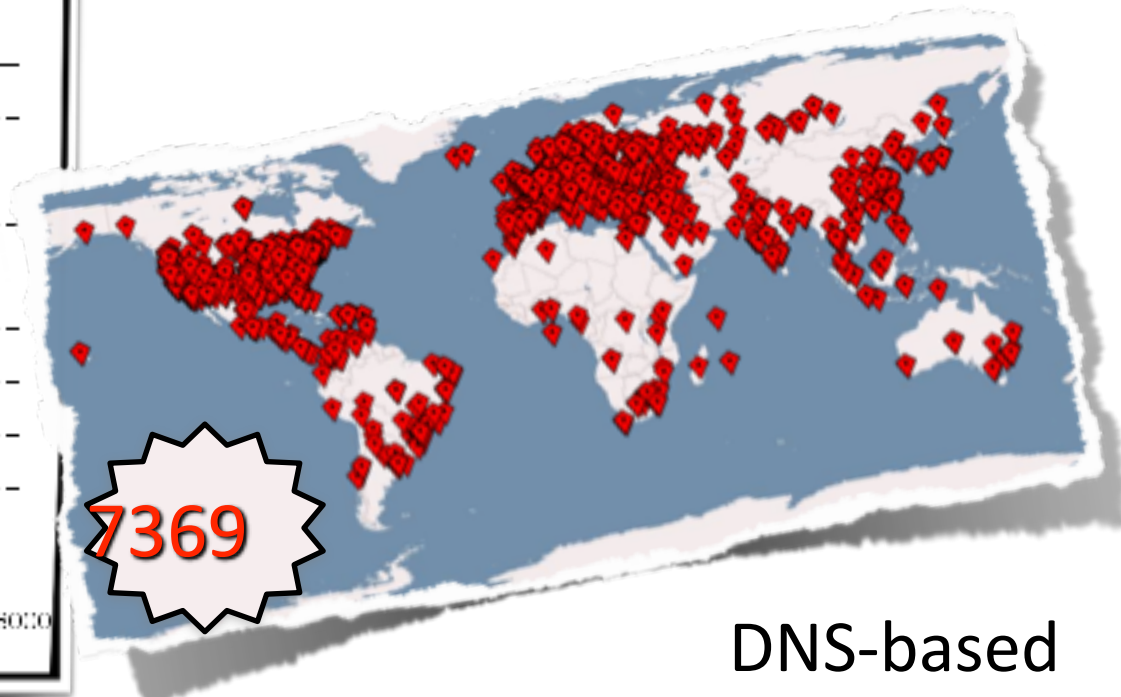
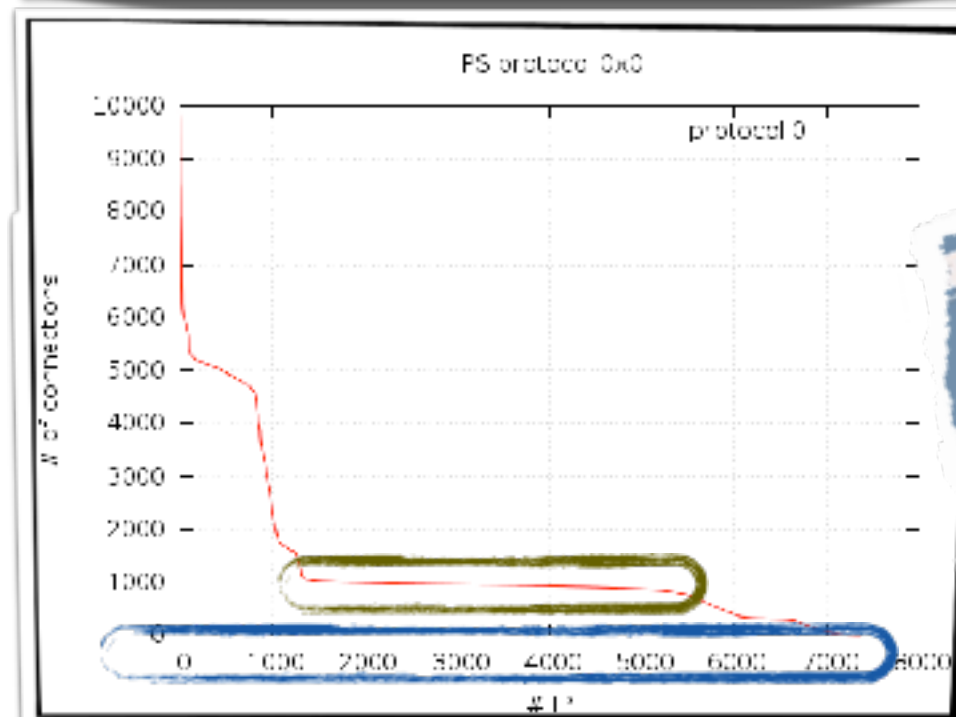
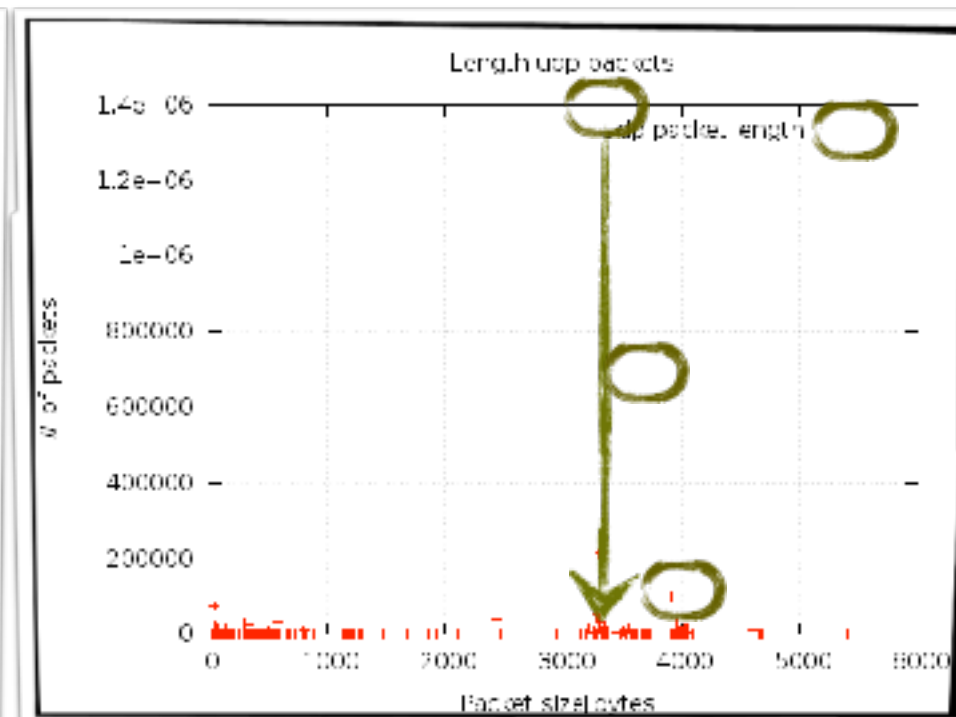
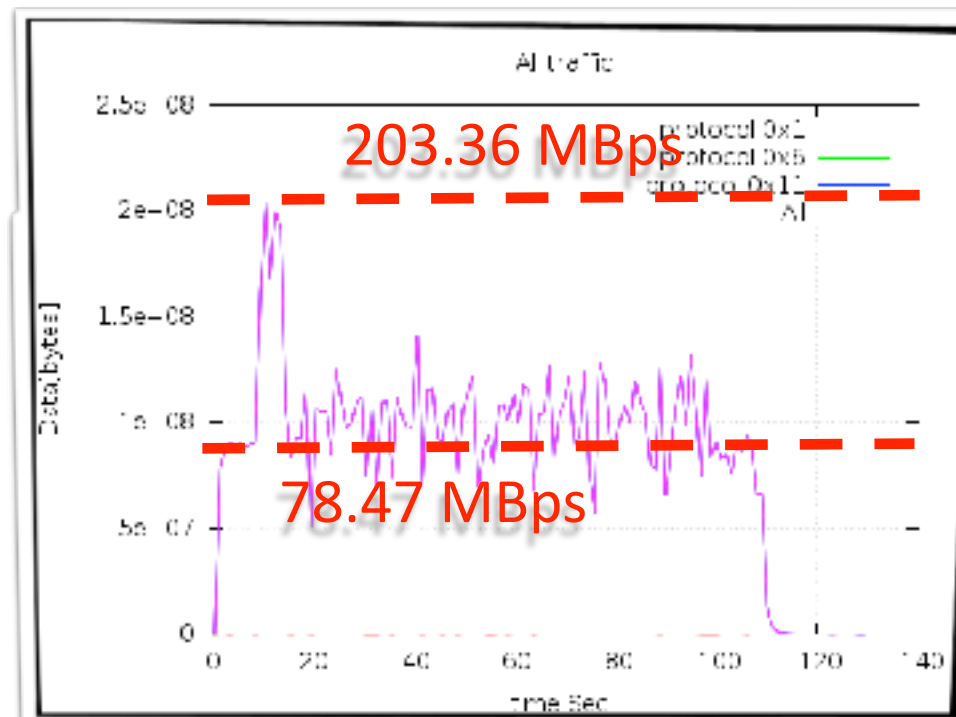


# Measure at the target



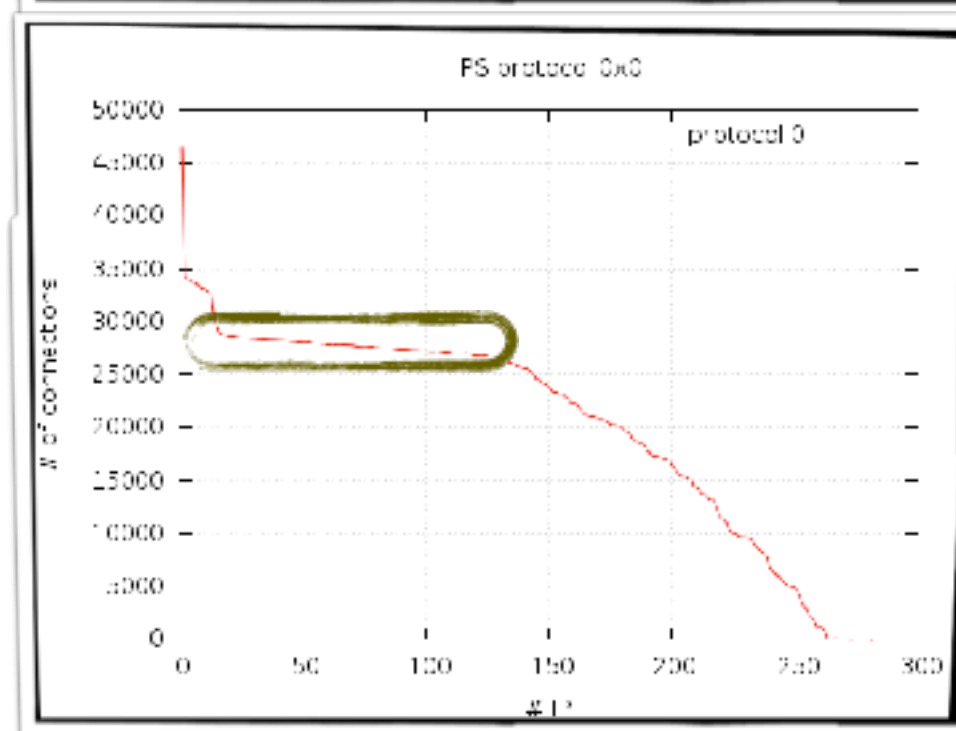
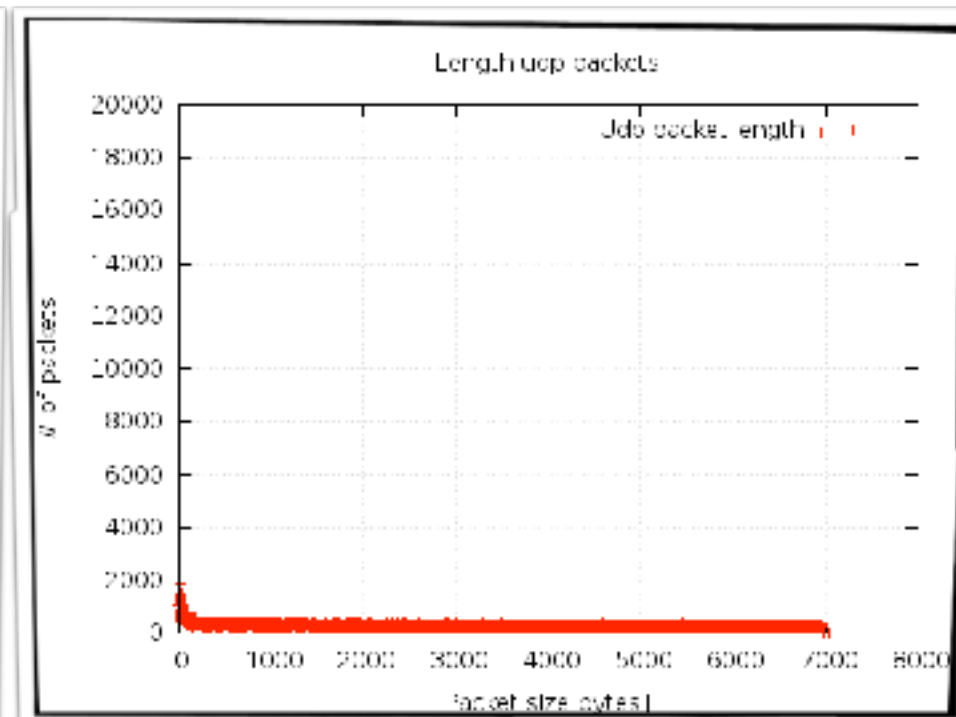
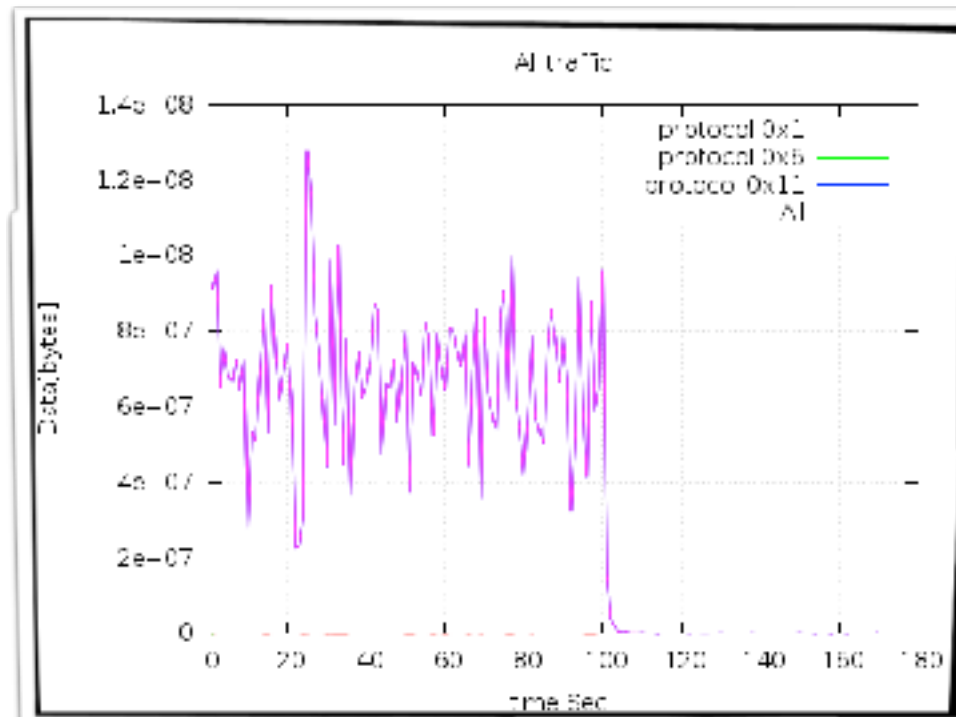
DNS-based

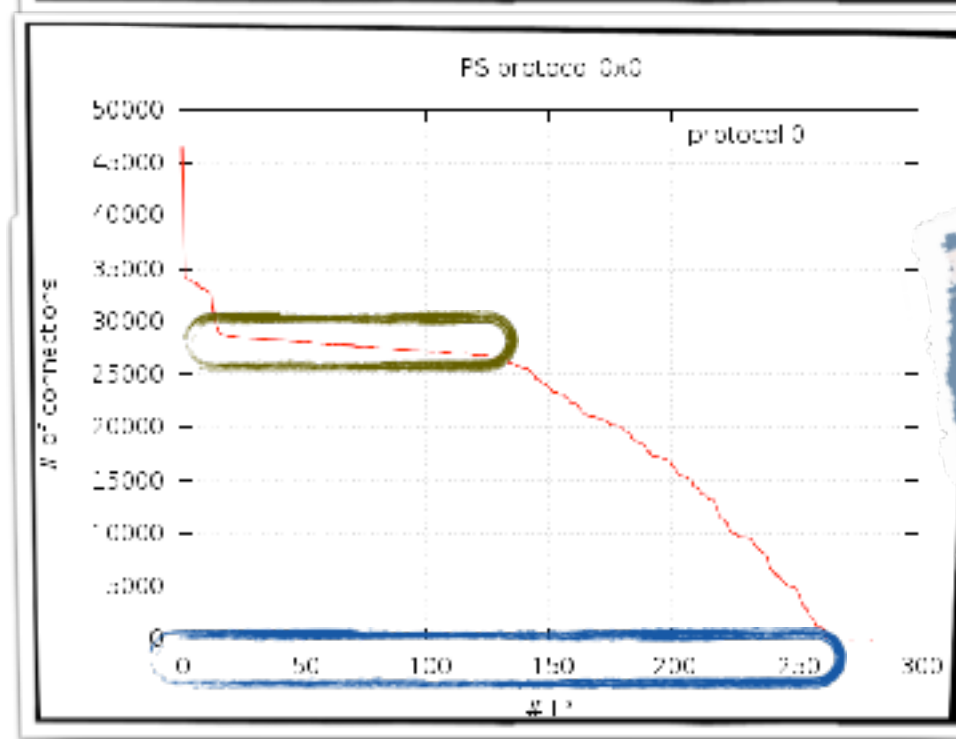
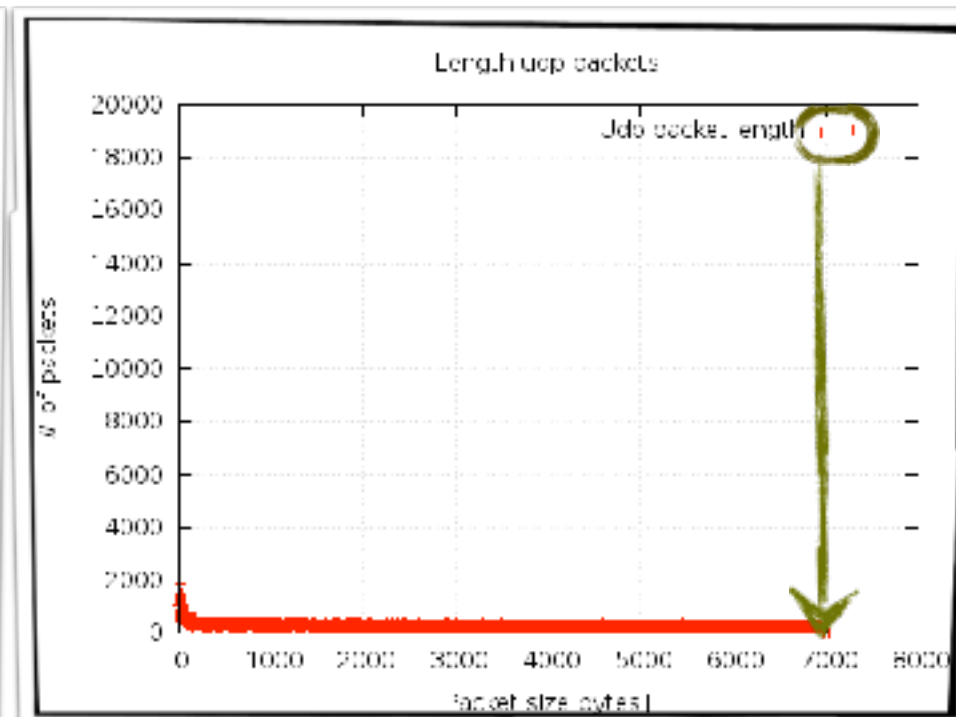
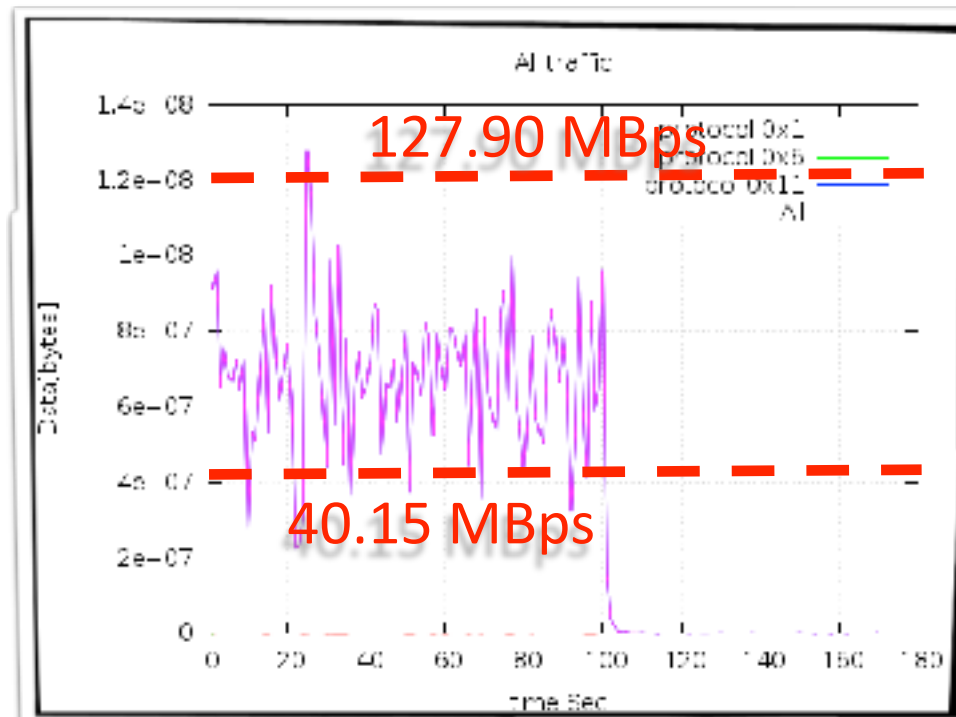




DNS-based







Based on Chargen (Port 19)

# How big is a typical attack?

---

# How big is a typical attack?

---

- But what is a *typical* attack?

# How big is a typical attack?

---

- But what is a *typical* attack?
- How representative is *our* data?



# How big is a typical attack?

---

- But what is a *typical* attack?
- How representative is *our* data?
- How does size change over time?

# How big is a typical attack?

---

- But what is a *typical* attack?
- How representative is *our* data?
- How does size change over time?
- What means *big*?
  - Number of bytes?
  - Number of packets?
  - Type of packets?
  - Length of attack?



# Research Question 2

## Who is attacked?



# Millions of Targets Under Attack

## a Macroscopic Characterization of the DoS Ecosystem

Mattijs Jonker<sup>†</sup>, A. King<sup>‡</sup>, J. Krupp<sup>§</sup>, C. Rossow<sup>§</sup>, A. Sperotto<sup>†</sup>, A. Dainotti<sup>‡</sup>  
<sup>†</sup>University of Twente; <sup>‡</sup>CAIDA, UC San Diego; <sup>§</sup>CISPA, Saarland University

# Millions of targets under attack

---

- March 1, 2015 – Feb 28, 2017
- AmpPot
  - reflection attacks
- UCSD Network Telescope
  - randomly spoofed attacks
- 21 million attacks over 2 years
  - average of 30k daily
- 2.19 million /24s observed
  - 2.19 million /24s observed
  - One third of the IPv4 address space



# Millions of targets under attack

---

- March 1, 2015 – Feb 28, 2017
- AmpPot
  - reflection attacks
- UCSD Network Telescope
  - randomly spoofed attacks
- 21 million attacks over 2 years
  - average of 30k daily
- 2.19 million /24s observed
  - 2.19 million /24s observed
  - One third of the IPv4 address space

**Do we see all DDoS attacks???**

# Millions of targets under attack

---

- Direct attacks not visible
- Comparison to recent Blackholing study:

attack source	#blackholing events	#prefixes
UCSD-NT	159.9 k (12.3%)	20.6 k (14.1%)
AmpPot	306.4 k (23.5%)	33.5 k (23.0%)
<b>Combined</b>	363.0 k (27.8%)	45.2 k (30.9%)

# Millions of targets under attack

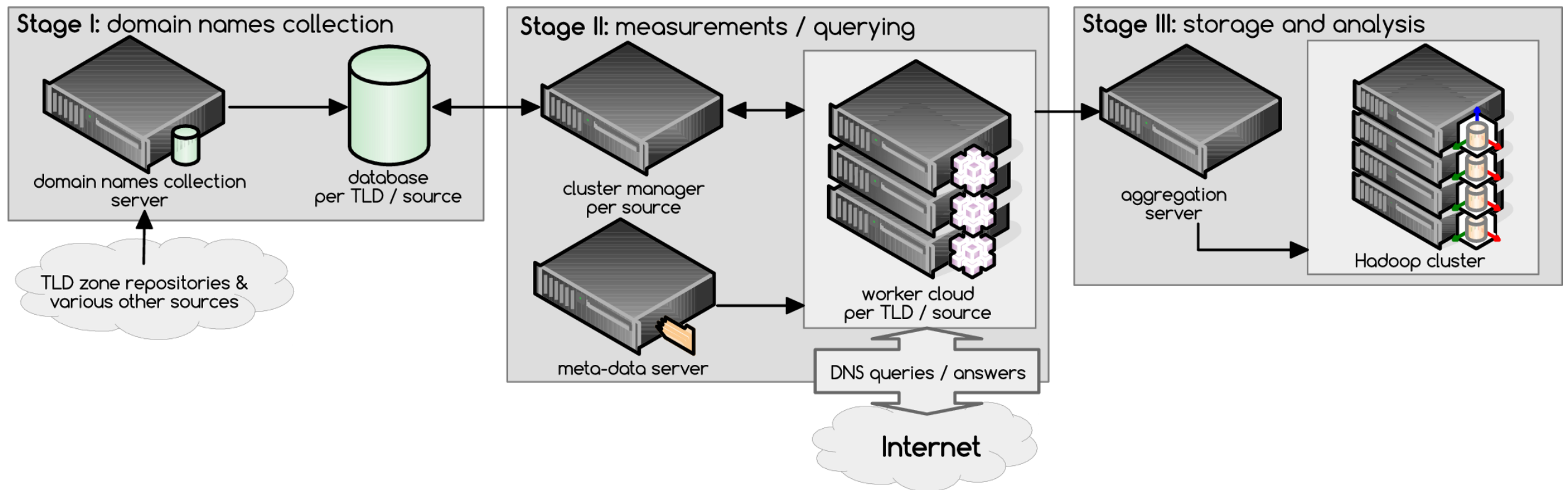
---

- Direct attacks not visible
- Comparison to recent Blackholing study:

attack source	#blackholing events	#prefixes
UCSD-NT	159.9 k (12.3%)	20.6 k (14.1%)
AmpPot	306.4 k (23.5%)	33.5 k (23.0%)
<b>Combined</b>	363.0 k (27.8%)	45.2 k (30.9%)

But WHO is attacked???

# Who is attacked?



# OpenIntel

Open **INTEL**

[HOME](#)

[BACKGROUND](#)

[DATA ACCESS](#)

[COVERAGE](#)

[PROBLEMS](#)

[CONTACT](#)

[NEWS](#)

[PAPERS](#)

Open **INTEL** in numbers:

**209**  
MILLION

domains measured on a  
daily basis

**2.2**  
BILLION

data points collected daily

**2.4**  
TRILLION

data points collected since  
the start in 2015

OPENINTEL IS A JOINT PROJECT

UNIVERSITY  
OF TWENTE.

SURF  
NET

SDN  
LABS

Through this website, we provide information on our project, how our measurement works and how you can reach us if you have [questions about using the data for your research.](#)

<https://openintel.nl>



# Who is attacked?

---

# Who is attacked?

---

- Do we see *all* attacks?

# Who is attacked?

---

- Do we see *all* attacks?
- Which domains belong to attacked IPs?

# Who is attacked?

---

- Do we see *all* attacks?
- Which domains belong to attacked IPs?
- Which websites are targeted?

# Who is attacked?

---


- Do we see *all* attacks?
- Which domains belong to attacked IPs?
- Which websites are targeted?
- Who owns these websites?

# Who is attacked?

---

- Do we see *all* attacks?
- Which domains belong to attacked IPs?
- Which websites are targeted?
- Who owns these websites?
- Or was the attack “collateral damage”?





# Research Question 3

## What financial damage is caused by attacks?

# Measuring the Impact of a Successful DDoS Attack on the Customer Behaviour of Managed DNS Service Providers

Abhishta  
University of Twente  
Enschede, The Netherlands  
s.abhishta@utwente.nl

Roland van Rijswijk-Deij  
University of Twente and SURFnet bv  
Enschede, The Netherlands  
r.m.vanrijswijk@utwente.nl

Lambert J.M. Nieuwenhuis  
University of Twente  
Enschede, The Netherlands  
l.j.m.nieuwenhuis@utwente.nl

## ABSTRACT

Distributed Denial-of-Service (DDoS) attacks continue to pose a serious threat to the availability of Internet services. The Domain Name System (DNS) is part of the core of the Internet and a crucial factor in the successful delivery of Internet services. Because of the importance of DNS, specialist service providers have sprung up in the market, that provide managed DNS services. One of their key selling points is that they protect DNS for a domain against DDoS attacks. But what if such a service becomes the target of a DDoS attack, and that attack succeeds?

In this paper we analyse two such events, an attack on NS1 in May 2016, and an attack on Dyn in October 2016. We do this by analysing the change in the behaviour of the service's customers. For our analysis we leverage data from the OpenINTEL active DNS measurement system, which covers large parts of the global DNS over time. Our results show an almost immediate and statistically significant change in the behaviour of domains that use NS1 or Dyn as a DNS service provider. We observe a decline in the number of domains that exclusively use NS1 or Dyn as a managed DNS service provider, and see a shift toward risk spreading by using multiple providers. While a large managed DNS provider may be better equipped to protect against attacks, these two case studies show they are not impervious to them. This calls into question the wisdom of using a single provider for managed DNS. Our results show that spreading risk by using multiple providers is an effective countermeasure, albeit probably at a higher cost.

## ACM Reference Format:

Abhishta, Roland van Rijswijk-Deij, and Lambert J.M. Nieuwenhuis. 2018. Measuring the Impact of a Successful DDoS Attack on the Customer Behaviour of Managed DNS Service Providers. In *WTMC'18: ACM SIGCOMM 2018 Workshop on Traffic Measurements for Cybersecurity*, August 20, 2018, Budapest, Hungary. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3229598.3229599>

## 1 INTRODUCTION

Distributed Denial-of-Service (DDoS) attacks continue to pose a serious threat to the availability of Internet-based services. In the last decade we have seen a constant increase in the intensity of these attacks [1–3]. An immediate impact of a successful DDoS attack is the unavailability of services provided by the victim to its customers. For instance, for an e-commerce firm this unavailability might result in decrease of sales during the attack and can also cause damage to the reputation of the victim [7].

These attacks also threaten the availability of services that support the Internet usage for an everyday user. One of the core services on which the Internet is built is the Domain Name System (DNS). DNS is responsible for translating easy to remember domain names into machine readable IP addresses. Thus, unavailability of the DNS leads to unavailability of web services for most users. On several occasions, attackers have targeted the DNS with a DDoS attack to bring down web services. Hence, it is important for firms that prioritise availability to choose a DNS provider that is resilient in the face of DDoS attacks. There are several managed DNS providers



# Research Question 4

What does a typical attack structure look like?

# Attack structure

---



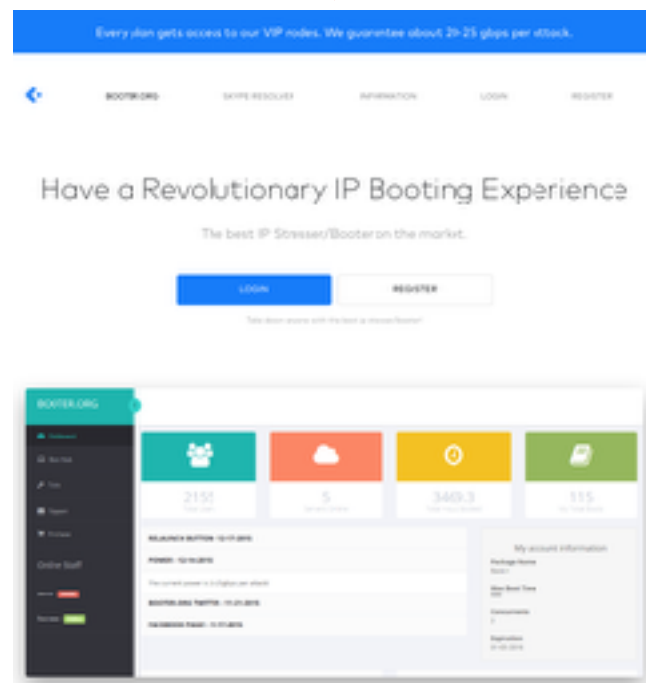
# Attack structure

---

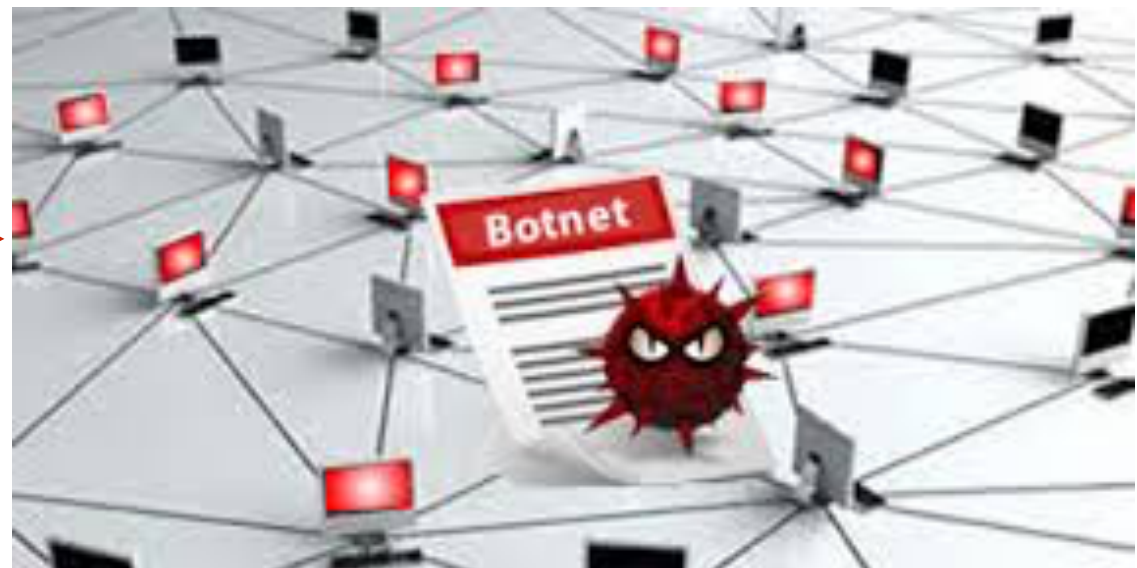


Web frontend

# Attack structure



Web frontend



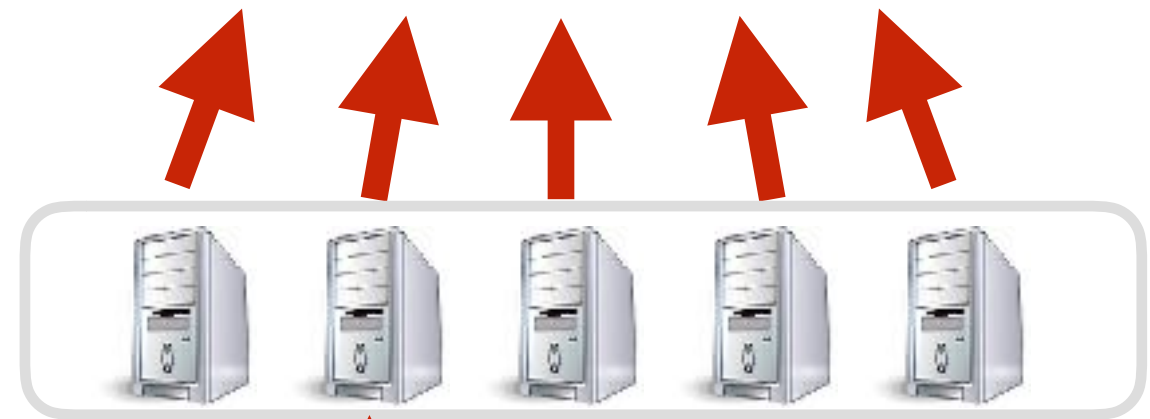
Distribution



# Attack structure



Web frontend

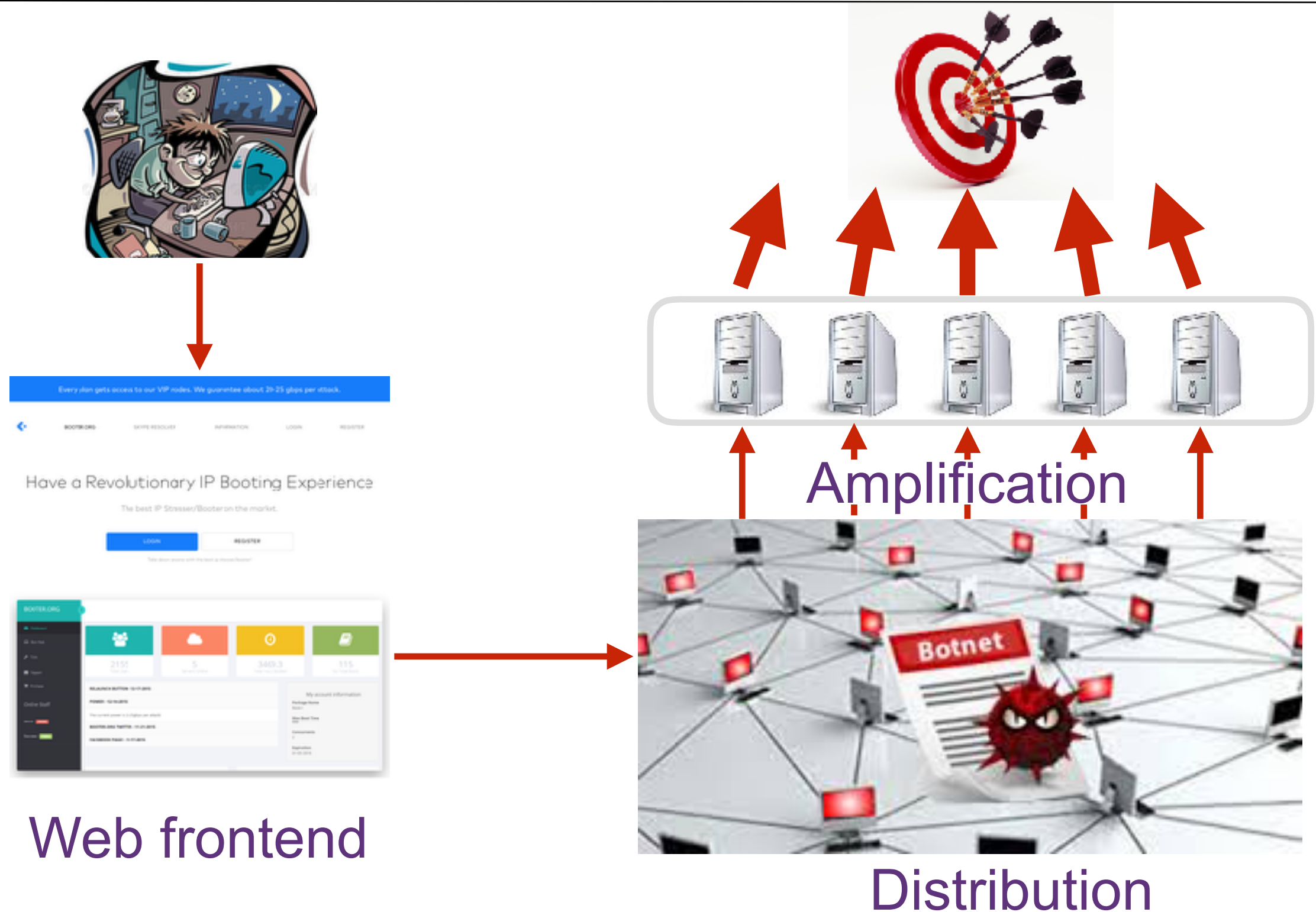


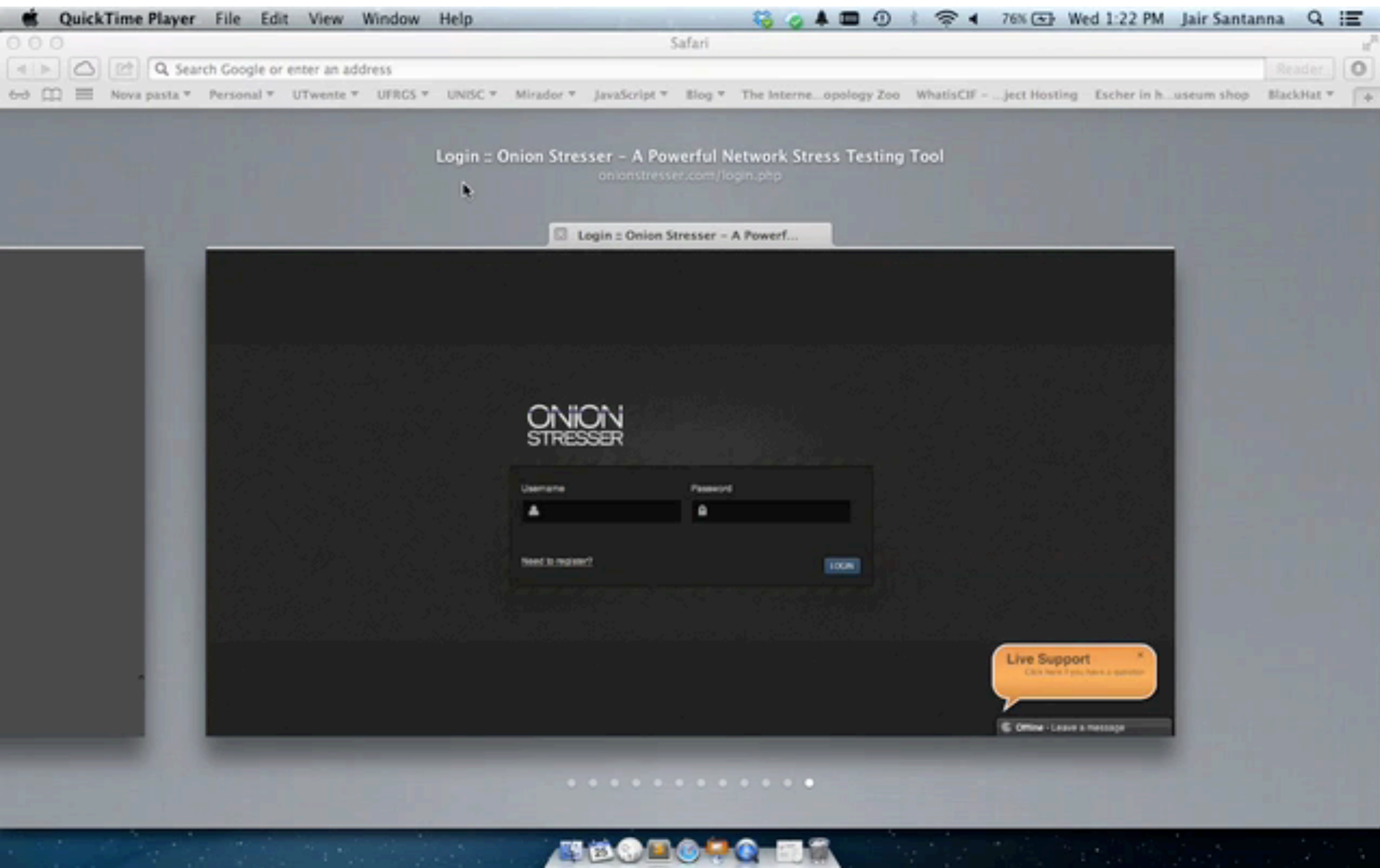
Amplification

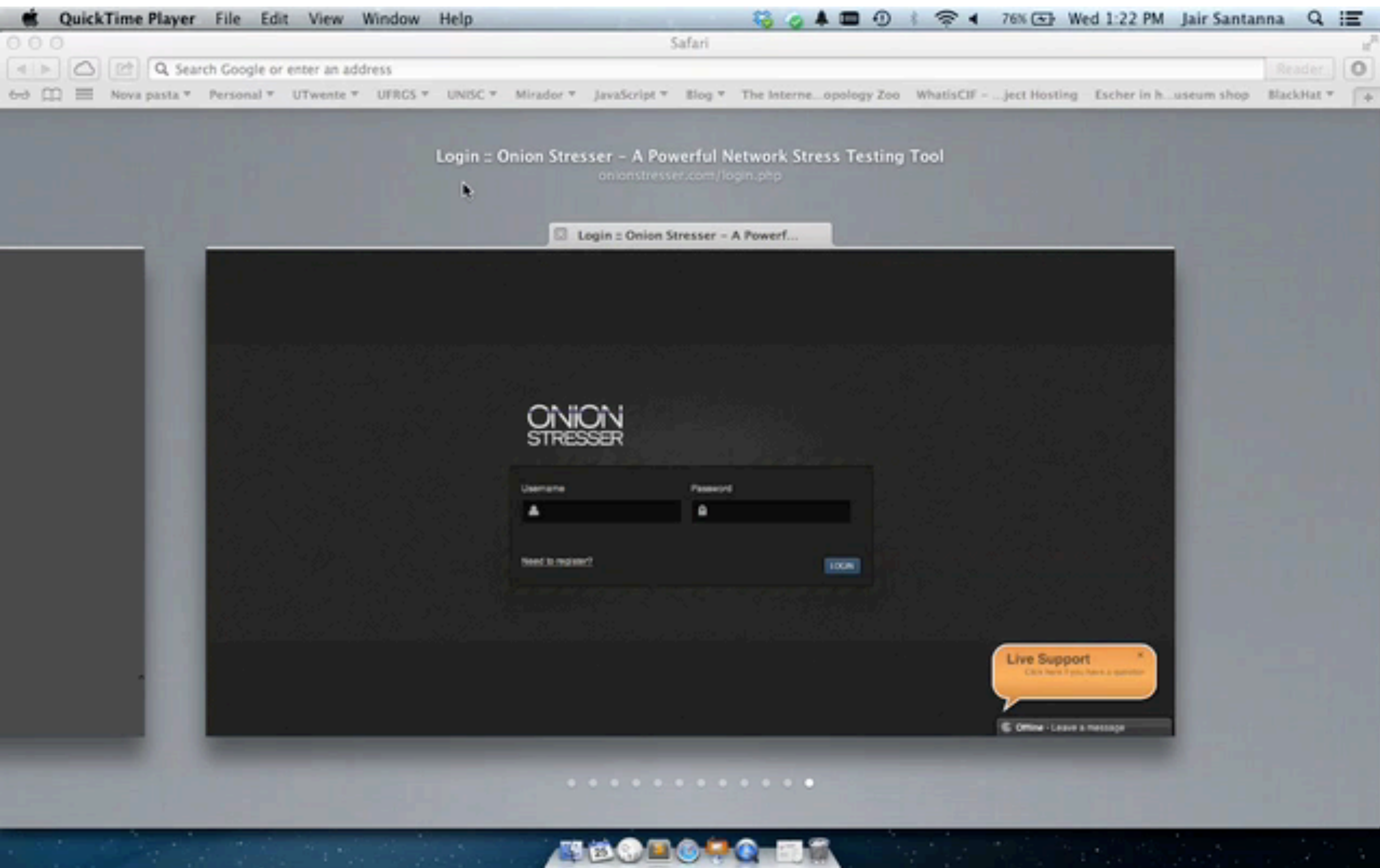


Distribution

# Attack structure







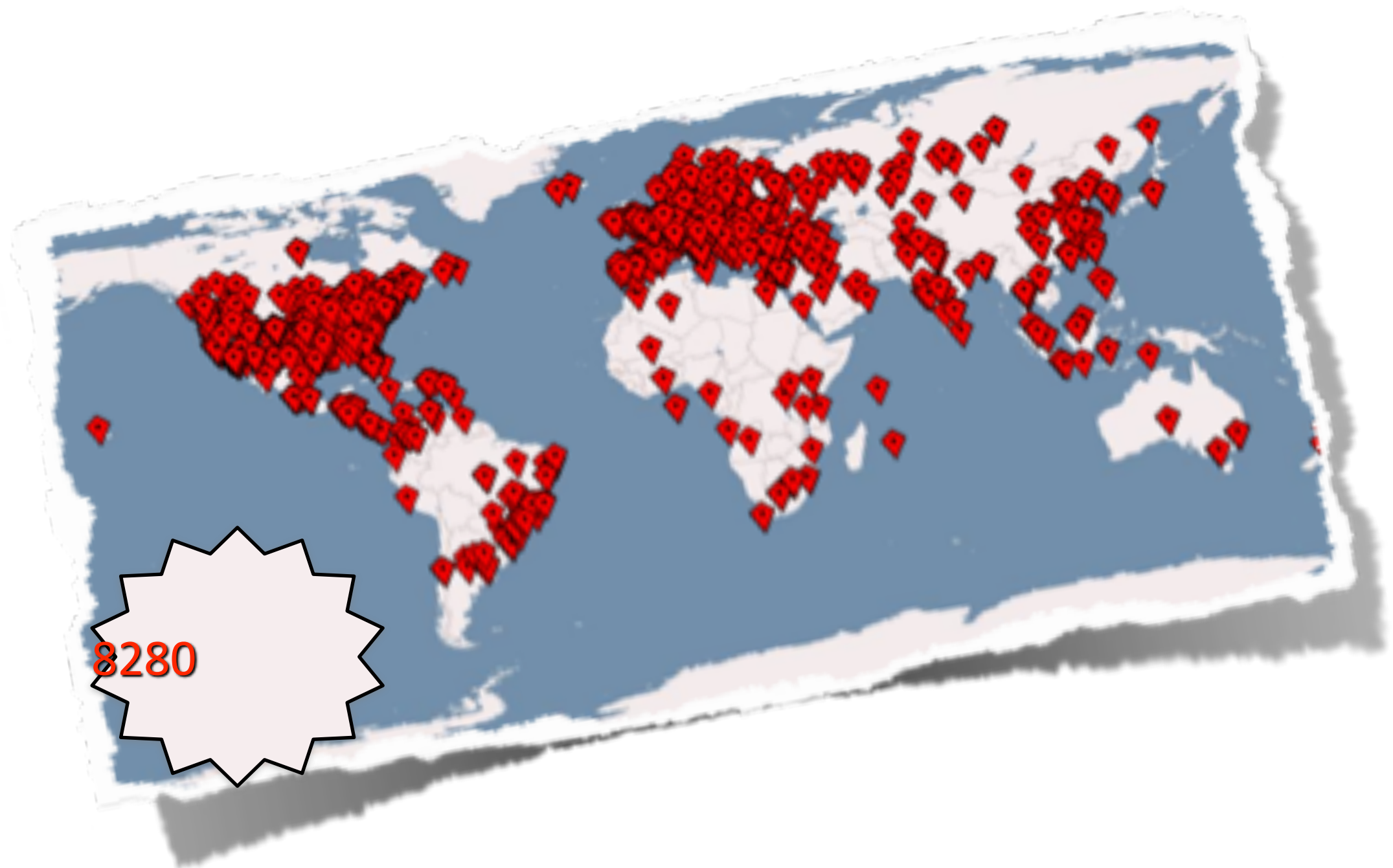
# How dynamic is the botnet?

---



# How dynamic is the botnet?

---





# What does a typical attack structure look like?

---

# What does a typical attack structure look like?

---

- Are all attacks by booters?

# What does a typical attack structure look like?

---

- Are all attacks by booters?
- Operate all booters in a similar way?

# What does a typical attack structure look like?

---

- Are all attacks by booters?
- Operate all booters in a similar way?
- Can you select attack details?

# What does a typical attack structure look like?

---

- Are all attacks by booters?
- Operate all booters in a similar way?
- Can you select attack details?
- Do they own a botnet?

# What does a typical attack structure look like?

---

- Are all attacks by booters?
- Operate all booters in a similar way?
- Can you select attack details?
- Do they own a botnet?
- Is the botnet changing over time?



# What does a typical attack structure look like?


---

- Are all attacks by booters?
- Operate all booters in a similar way?
- Can you select attack details?
- Do they own a botnet?
- Is the botnet changing over time?
- Are the amplifiers changed over time?

# What does a typical attack structure look like?

---

- Are all attacks by booters?
- Operate all booters in a similar way?
- Can you select attack details?
- Do they own a botnet?
- Is the botnet changing over time?
- Are the amplifiers changed over time?
- Are the amplifiers “prepared”?



# Research Question 5

## What are the most important booters?

# Quiet Dogs Can Bite: Which Booters Should We Go After, and What Are Our Mitigation Options?

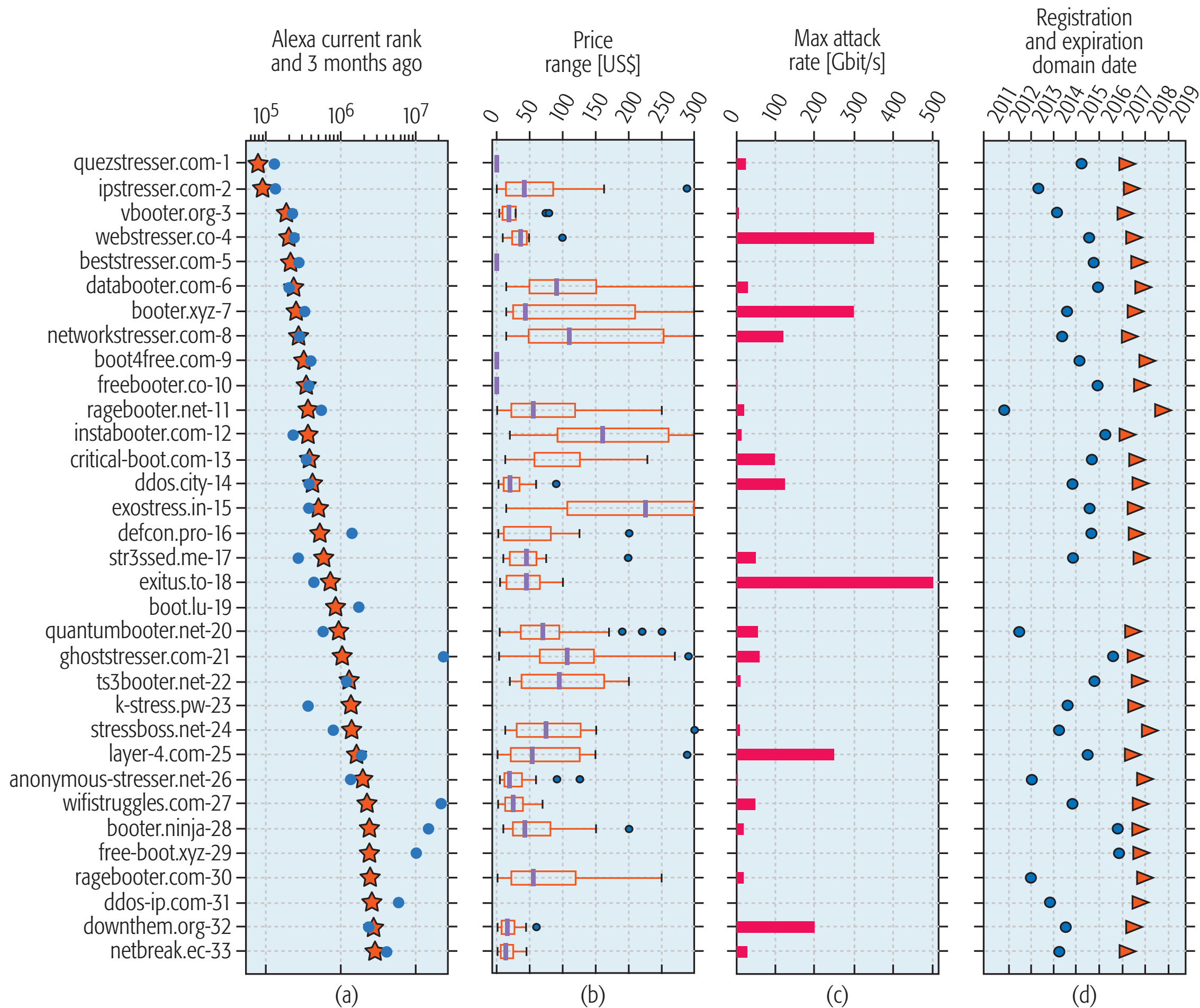
José Jair Santanna, Ricardo de O. Schmidt, Daphne Tuncer, Anna Sperotto, Lisandro Z. Granville, and Aiko Pras

### ABSTRACT

Large network security companies often report websites, called Booters, that offer DDoS attacks as a paid service as the primary reason for the increase in occurrence and power of attacks. Although hundreds of active Booters exist today, only a handful of those that promoted massive attacks faced mitigation and prosecution actions.

Large network security companies often report websites, called Booters, that offer DDoS attacks as a paid service as the primary reason for the increase in occurrence and power of attacks. Although hundreds of active Booters exist today, only a handful of those that promoted massive attacks faced mitigation and prosecution actions. In this tutorial article we focus our attention on Booters that are “under the radar” of security initiatives, by advertising high attack power and being very popular on the Internet. We discuss and provide grounds for critical thinking on what should be further done toward Booter mitigation.

ed to have launched more than 170,000 DDoS attacks in less than four months; as a consequence, vDos owners were arrested. In 2016, a sustained 540 Gb/s attack, launched by the LizardStresser Booter (<https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks>, accessed 21 March 2017), was also witnessed during the Olympic Games in Brazil, as well as a staggering terabit-per-second attack using the Mirai botnet (also related to Booters — <https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar>, accessed 21 March 2017) targeting OVH (<https://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/>, accessed 21 March 2017) and Dvn (<http://dvn>



[View on GitHub](#)



# Booters (Black)List and Ecosystem Analysis

Sharing the most extensive list of Booter Websites!

Booters are Websites that publicly offer Distributed Denial of Service (DDoS) attacks as a paid service. Accordingly to the Federal Bureau of Investigation (FBI), [Booters usage are considered 'crime if they are used against a Website without the owner's permission'](#). Our intention to generate/share this list is to facilitate the investigation of the entire market/ecosystem. NOTE that the following list includes offline Booters (for historical purposes). *For only ONLINE booters, please clone [our GitHub repository](#) and re-run the 6th and 7th steps.*

**DOWNLOAD!**

If you use, for academic purposes, the Booter (Black)List **OR** our methodology **OR** our [analyses script](#), **PLEASE** don't forget to cite the publicly available [Jair Santanna's Ph.D. thesis](#):



# DDOS-AS-A-SERVICE

Investigating Booter Websites



José Jair Cardoso de Santanna



# Research Question 6

Which booter  
is responsible  
for the attack?

# Attack fingerprinting

AboutLog inRequest access

Collecting and Sharing the most important information of DDoS attacks

Search



## What is DDoSDB?

DDoSDB is a platform for helping victims of DDoS attacks, the academic community, and the security community to share and get access to actual and enriched information of DDoS attacks. The purpose of sharing attacks is to enable comparison with other attacks, facilitate legal attribution, and improve detection and mitigation strategies.

DDoSDB provides an interface for searching unique characteristics of attacks (fingerprints) and also provides a sample of its actual attack data (ex. pcap and nfdump file). All data within DDoSDB come from collaborators that own attack data (usually collected as victim). We facilitate collaborators data sharing by providing an open source code that analyses an attack, generates fingerprints, and anonymizes the identity of the victim ([link](#)).



# Research Question 7

## Who is protected by DPS?

# Measuring the Adoption of DDoS Protection Services

Mattijs Jonker  
University of Twente  
m.jonker@utwente.nl

Anna Sperotto  
University of Twente

Roland van Rijswijk-Deij  
University of Twente and SURFnet bv

Ramin Sadre  
Université catholique de Louvain

Aiko Pras  
University of Twente

## ABSTRACT

Distributed Denial-of-Service (DDoS) attacks have steadily gained in popularity over the last decade, their intensity ranging from mere nuisance to severe. The increased number of attacks, combined with the loss of revenue for the targets, has given rise to a market for DDoS Protection Service (DPS) providers, to whom victims can outsource the cleansing of their traffic by using traffic diversion.

In this paper, we investigate the adoption of cloud-based DPSs worldwide. We focus on nine leading providers. Our outlook on adoption is made on the basis of active DNS measurements. We introduce a methodology that allows us, for a given domain name, to determine if traffic diversion to a DPS is in effect. It also allows us to distinguish various methods of traffic diversion and protection. For our analysis we use a long-term, large-scale data set that covers well over 50% of all names in the global domain namespace, in daily snapshots, over a period of 1.5 years.

Our results show that DPS adoption has grown by  $1.24\times$  during our measurement period, a prominent trend compared to the overall expansion of the namespace. Our study also reveals that adoption is often lead by big players such as large Web hosters, which activate or deactivate DDoS protection for millions of domain names at once.

The growth in number of attacks [6], combined with the loss of revenue for the targets, has given rise to a market for DDoS Protection Service (DPS) providers. The protection of a specific application, or even an entire network, can be outsourced to a DPS. Protection can take place on-site, by means of dedicated appliances [7], or be handled in the cloud, where malicious traffic is filtered or absorbed, thus effectively thwarting the attack. Hybrid solutions also exist, where on-site appliances are combined with a cloud-based component. Attacks can be volumetric (i.e., saturating the target's bandwidth) or semantic (e.g., denying service access with minimal bandwidth effects).

*Traffic diversion* is the key mechanism that allows traffic to be routed through the DPS infrastructure, either in an always-on or on-demand manner. An effective way to divert traffic for applications that are reached on the basis of a domain name, is to exploit the Domain Name System (DNS), similarly to what is done in content delivery networks for implementing load balancing [8, 9]. An alternative is to use the Border Gateway Protocol (BGP) to divert traffic towards the DPS infrastructure.

In this paper, we investigate the adoption of cloud-based DPSs worldwide. We focus on nine leading providers according to [13], namely Akamai, CenturyLink, CloudFlare, DOSarrest, F5 Networks, Incapsula, Level 3, Neustar, and



VERISIGN™



CenturyLink™



neustar®

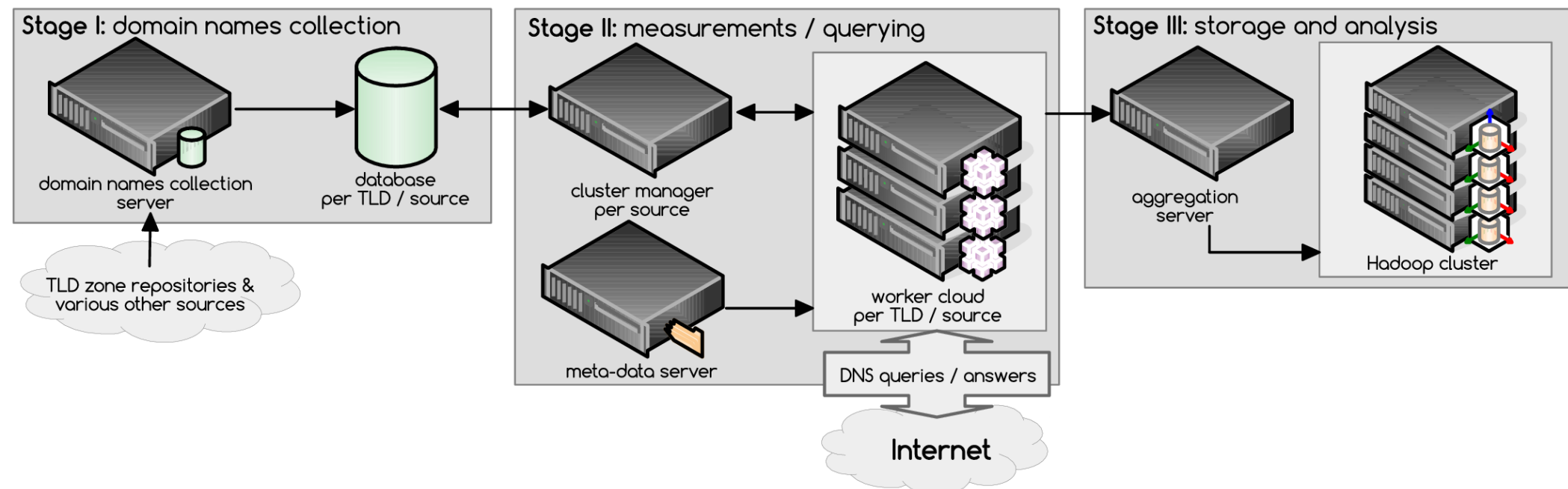


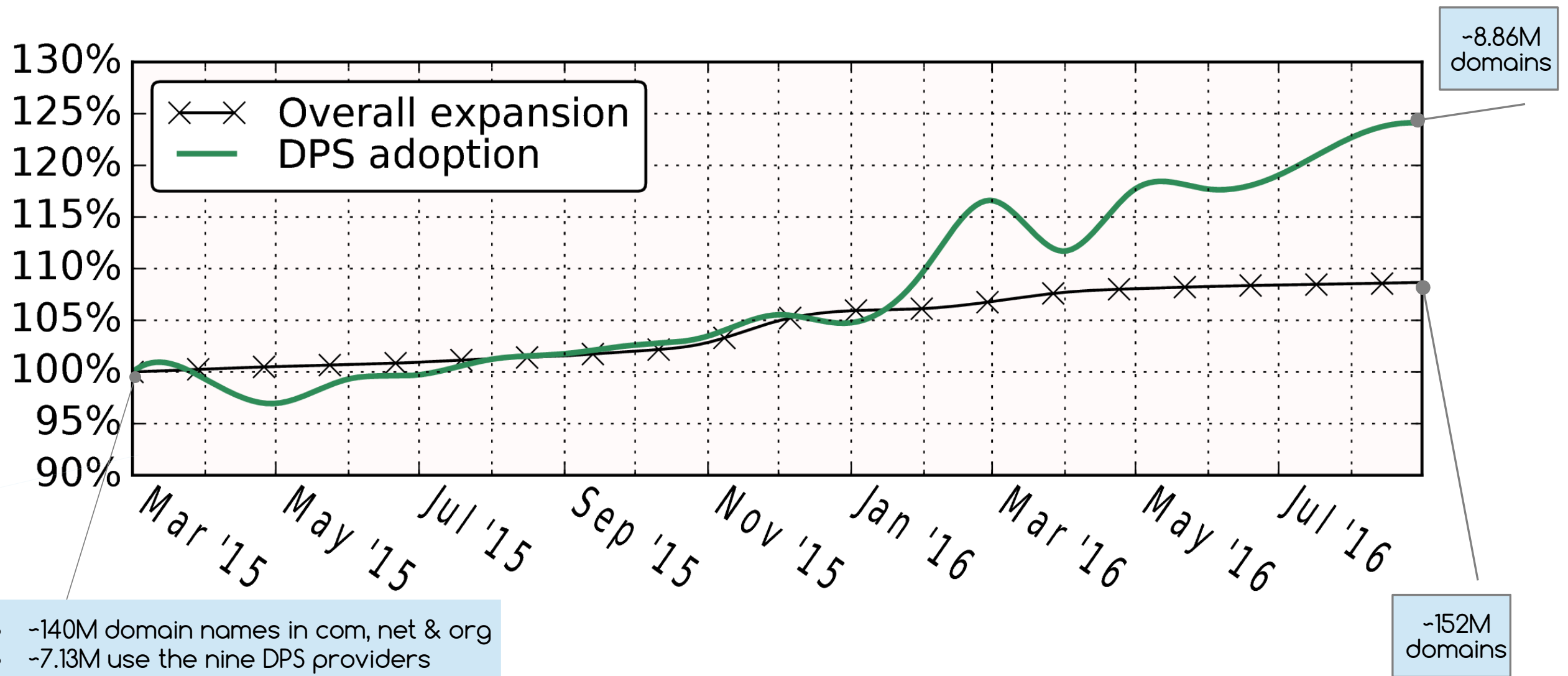


VERISIGN™

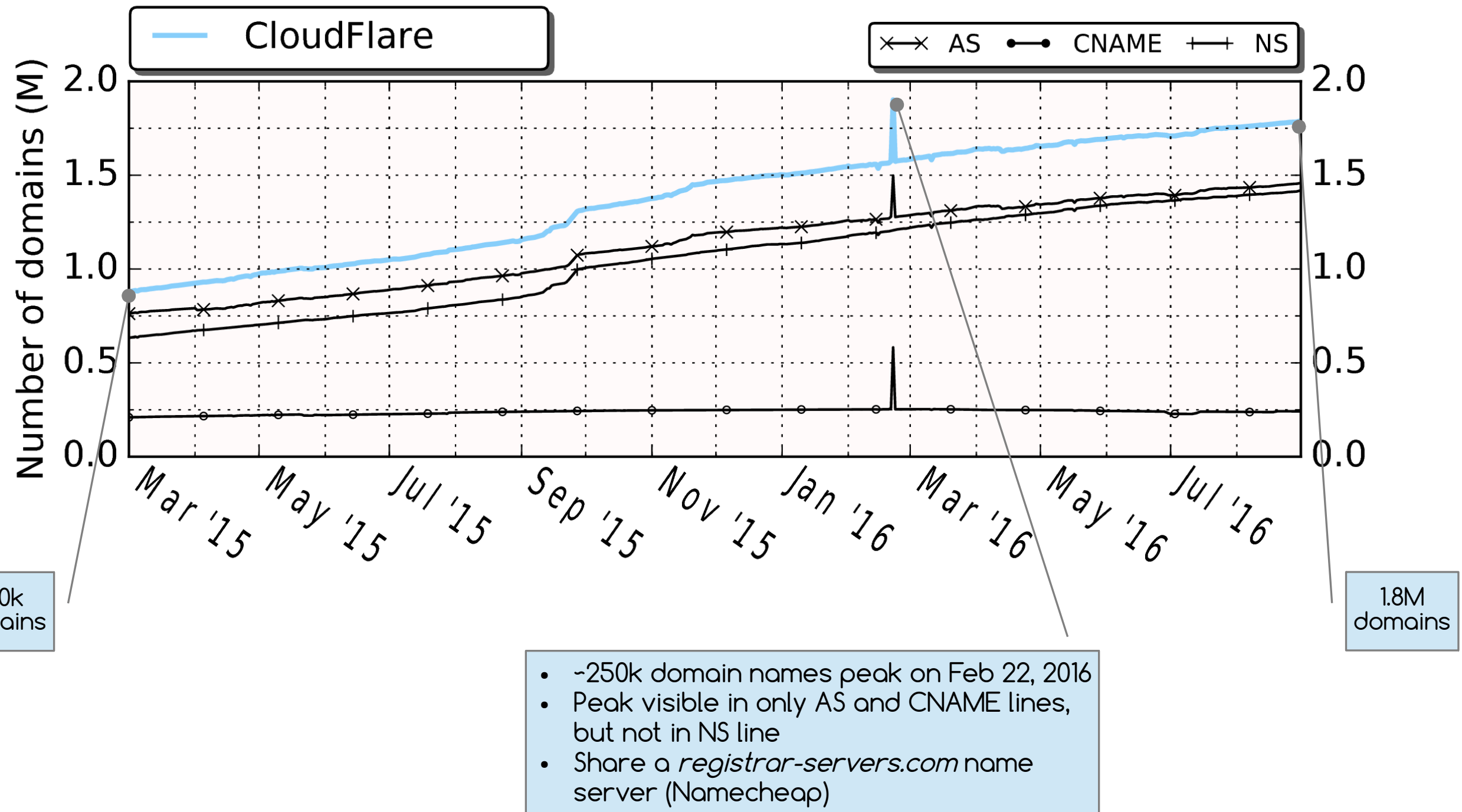


CenturyLink™

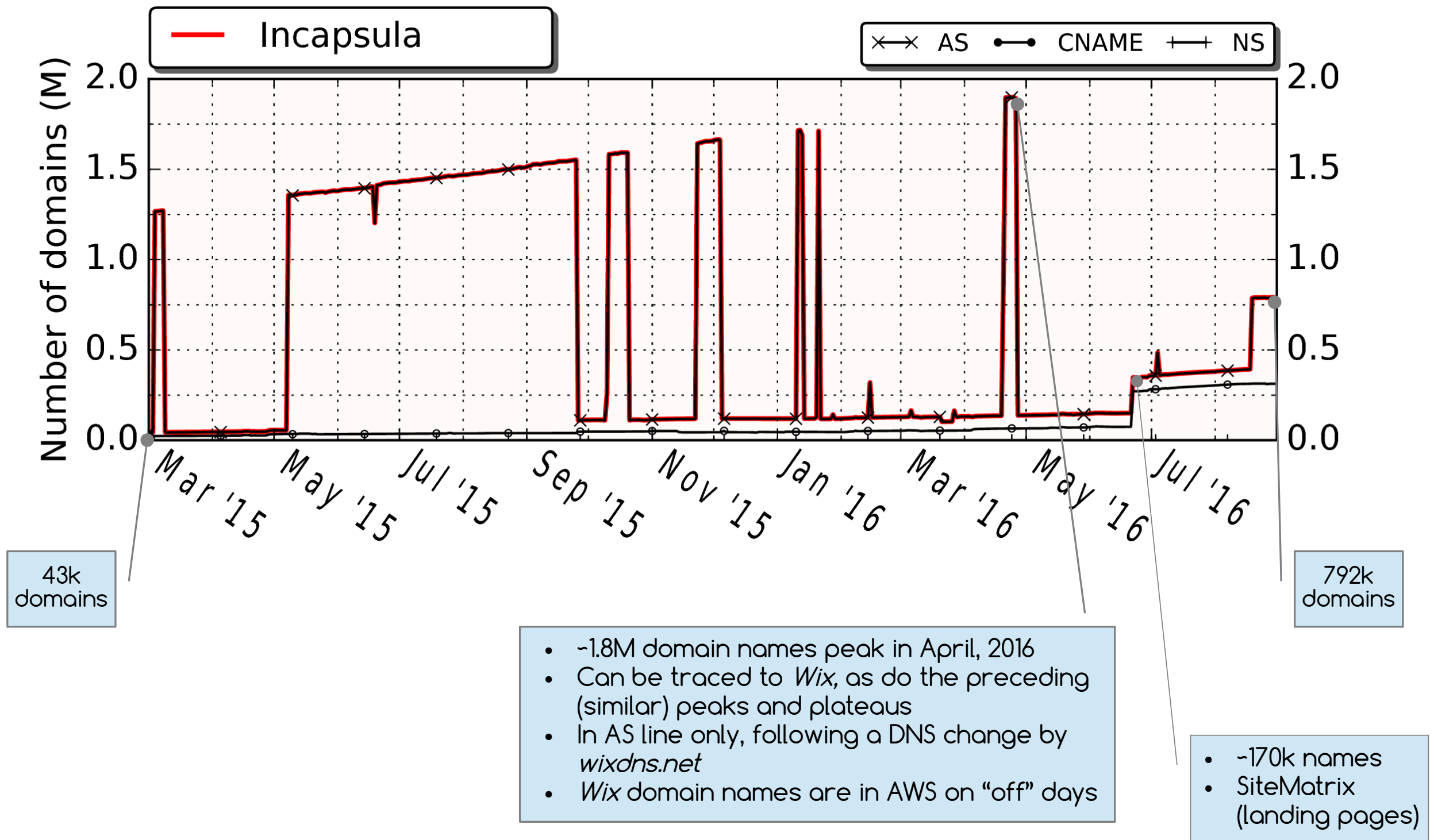




# Results: use of CloudFlare



# Results: use of Incapsula



# Who is protected by DPS?

---

# Who is protected by DPS?

---

- What about privacy?



# Who is protected by DPS?

---

- What about privacy?
- Is it always legal?

# Who is protected by DPS?

---

- What about privacy?
- Is it always legal?
- Can it be circumvented?
  - RR history
  - Other RRs (like MX)

# Who is protected by DPS?

---

- What about privacy?
- Is it always legal?
- Can it be circumvented?
  - RR history
  - Other RRs (like MX)
- National dependance?
  - Netherlands: NaWas



# Research Question 8

## Is blackholing being used?

# A First Joint Look at DoS Attacks and BGP Blackholing in the Wild

Mattijs Jonker      Aiko Pras      Alberto Dainotti      Anna Sperotto  
University of Twente    University of Twente    CAIDA / UC San Diego    University of Twente

## ABSTRACT

BGP blackholing is an operational countermeasure that builds upon the capabilities of BGP to achieve DoS mitigation. Although empirical evidence of blackholing activities are documented in literature, a clear understanding of how blackholing is used in practice when attacks occur is still missing.


This paper presents a first joint look at DoS attacks and BGP blackholing in the wild. We do this on the basis of two complementary data sets of DoS attacks, inferred from a large network telescope and DoS honeypots, and on a data set of blackholing events. All data sets span a period of 1100 day, thus proving a longitudinal overview of operational deployment of blackholing during DoS attacks.

## 1. INTRODUCTION

tion prefix (the one of the victim) [10].

Although empirical evidence of blackholing activities is documented in literature [11], a clear understanding about how BGP blackholing is used in practice when attacks occur is still missing. The goal of this paper is to provide a first joint look at DoS attacks and BGP blackholing in the wild. To this end, we rely on two DoS attack data sets and one BGP blackholing event data set, all spanning a period of 1100 days. To the best of our knowledge, this is the first large-scale empirical observation of DoS events and corresponding blackholing mitigation. Our main findings are:

- Mitigation via blackholing happens within minutes. Our analysis shows that 44% of the attacks for which blackholing is put in place are mitigated within one minute, and 85% within 10 minutes.



# Research Question 9

## What happens if booters are seized by the police?





# THIS SITE HAS BEEN SEIZED

The domain name [Webstresser.org](http://Webstresser.org) has been seized by the United States Department of Defense, Defense Criminal Investigative Service, Cyber Field Office in accordance with a warrant issued by the United States District Court for the Eastern District of Virginia. This domain name has been seized in conjunction with Operation Power OFF

Operation Power OFF is a coordinated effort by law enforcement agencies from The Netherlands, United Kingdom, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada and the United States of America, in cooperation with Europol.

The operation is aimed at the takedown of the illegal DDoS-for-hire-service [Webstresser.org](http://Webstresser.org).



# WORLD'S BIGGEST MARKETPLACE SELLING INTERNET PARALYSING DDOS ATTACKS TAKEN DOWN

*25 April 2018*

*Press Release*



Webstresser.org sold Distributed Denial of Service attacks that could knock the internet offline for as little as EUR 15.00 a month

The administrators of the DDoS marketplace *webstresser.org* were arrested on 24 April 2018 as a result of Operation Power Off, a complex investigation led by the Dutch Police and the UK's National Crime Agency with the support of Europol and a dozen law enforcement agencies from around the world. The administrators were located in the United Kingdom, Croatia, Canada and Serbia. Further measures were taken against the top users of this marketplace in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong. The illegal service was shut down and its infrastructure seized in the Netherlands, the US and Germany.







A man with a beard and glasses, wearing a grey suit and a white shirt, stands in front of the Europol building. He is smiling and has his hands clasped in front of him. The building is a large, modern structure with a grey brick facade and many windows. The word 'EUROPOL' is visible on the building's facade. The ground is paved with grey stones.

60% less attacks

Akamai: 10% less attacks

# How to determine the effect?

---

# How to determine the effect?

---

- Where to get data from?
  - Booter database?
  - AmpPot, UCSD Network Telescope, Shadowserver?
  - Akamai? Cloudflare?
  - ISPs? IX-es?



# How to determine the effect?

---

- Where to get data from?
  - Booter database?
  - AmpPot, UCSD Network Telescope, Shadowserver?
  - Akamai? Cloudflare?
  - ISPs? IX-es?
- Is there a difference between countries?

# How to determine the effect?

---

- Where to get data from?
  - Booter database?
  - AmpPot, UCSD Network Telescope, Shadowserver?
  - Akamai? Cloudflare?
  - ISPs? IX-es?
- Is there a difference between countries?
- What is the effect over time?

# Summary

---

- DDoS is a real problem
- High financial loss
- Attacks will not disappear soon
- Many interesting research challenges exist

Thanks for your attention!

Questions?

