

# Content and popularity analysis of Tor hidden services

Ivan Pustogarov, University of Luxembourg  
30 June 2014

# Summary (1/2)

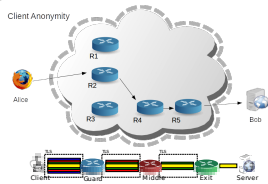
- 39824 hidden service descriptors on 4th February 2013
  - Port scanning
  - Popularity
- Content analysis of 3050 HTTP services

# Summary (2/2)

- A good chunk of Tor hidden services are not bad
- Massively used by botnets
- Most popular hidden services are shady
- One can catch clients of those shady services

# Tor hidden services

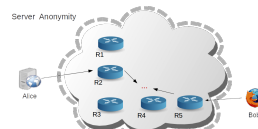
Tor



Consensus

tor-relay	2177	67.4	5508896.usd.met.it [95.134.56.155]	/	🗄️	🗄️	🗄️
tor-relay	2820	64.6	tor-relay.mozzart.org [208.305.249.3]	/	🗄️	🗄️	🗄️
tor-relay	3346	35.6	50.7.148.58 [50.7.148.58]	/	🗄️	🗄️	🗄️
tor-relay	3381	53.4	tor-relay.torserver.com [143.164.130.25]	/	🗄️	🗄️	🗄️
tor-relay	3715	47.6	189546742.business.broadcom [81.143.124.38]	/	🗄️	🗄️	🗄️
tor-relay	3791	79.6	50.97.1.36.usadac.commerce.software.com [50.97.1.36]	/	🗄️	🗄️	🗄️
tor-relay	419	61.4	tor-relay.energy.com [209.17.131.13]	/	🗄️	🗄️	🗄️
tor-relay	392	23.8	tor-relay.comcast.com [184.105.231.11]	/	🗄️	🗄️	🗄️
tor-relay	241	139.6	tor-relay.20120.com [91.229.20.109]	/	🗄️	🗄️	🗄️
tor-relay	193	109.4	tor-relay.ghostal.net [95.103.124.75]	/	🗄️	🗄️	🗄️
tor-relay	169	79.6	tor-relay.jetex.org [37.58.162.238]	/	🗄️	🗄️	🗄️
tor-relay	6	58.6	184.22.164.107.mesa.horizon.net [184.22.164.107]	/	🗄️	🗄️	🗄️
tor-relay	4208	100.4	tor-relay.primera.eu [80.208.90.12]	/	🗄️	🗄️	🗄️
tor-relay	144	34.6	tor-relay.proweb.com [131.171.220.65]	/	🗄️	🗄️	🗄️
tor-relay	181	52.4	tor-relay.95.64.148.164.supportnetworks.eu [95.64.148.164]	/	🗄️	🗄️	🗄️
tor-relay	66	107.4	tor-relay.95.179.103.97.943.com	/	🗄️	🗄️	🗄️

Tor hidden services



**Public Library of US Diplomacy: Kissinger Cables**  
2012-04-08

The Kissinger Cables are part of today's launch of the WikiLeaks Public Library of US Diplomacy (PLUD), which hosts the world's largest searchable collection of United States confidential, or formerly confidential, diplomatic communications. As of its launch on April 8, 2013 it holds 2 million records comprising approximately 1 billion words.

**Detainee Policies**  
2012-03-24

WikiLeaks has begun releasing the 'Detainee Policies', more than 100 classified or otherwise restricted files from the United States Department of Defense covering the rules and procedures for operations in U.S. military custody. Over the next month, WikiLeaks will release in chronological order the 'Detainee Policies' and other documents related to the release of...

**Duck Duck Go**

Duck Duck Go is a search engine based in Valley Forge, Pennsylvania that does not store or sell personal data like the majority with the aim of safeguarding individual privacy and supporting open source.

More at WikiLeaks | Official site: duckduckgo.com

Internet search engines

Duck Duck Go | [BILGİN DOWNLOAD.com](#)

Duck Duck Go | [CrunchBase Profile](#)

Duck Duck Go | [Challenges Google on Privacy \(With a Billboard\) | Wired Business](#)

**THE NEW YORKER STRONGBOX**

SECURELY SUBMIT FILES TO WRITERS AND EDITORS

You can use this site to submit information, messages, and files to writers and editors at The New Yorker.

GET STARTED

Load times may vary.

**Silk Road**

Skynet, a Tor-powered botnet straight from Reddit

Posted by Claudio Guarnieri in Information Security on Dec 6, 2012 2:51:13 PM

...ing through the dark alleys of the Internet we encountered an unusual malware artifact, something that was right.

... we spent time looking at it, the more it started to look unusually familiar. As a matter of fact it turned out the origin named "threeway236230" described in a very popular / Am A thread you can read [here](#).

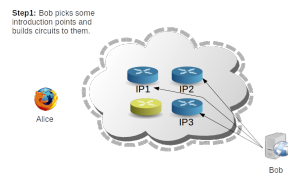
... is an overview of this malware labelled by the creator as "Skynet" a Tor-powered trojan with DDoS, Bitcoin or "jwars".

... re the warez

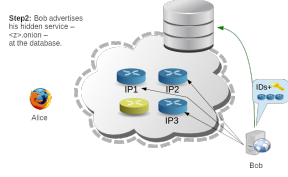
... gple download software from Usenet and install it in the offices or at friends pretty often. Also Usenet isn't th... 's trojan. Most Providers have their own Usenet client for ideal proof downloads"

... a distributed discussion platform established around 1980 and still very popular worldwide.

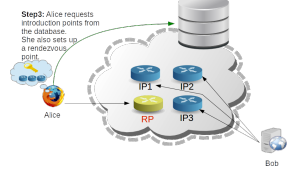
Tor Rendezvous Protocol



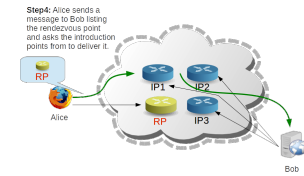
Tor Rendezvous Protocol



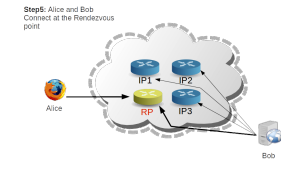
Tor Rendezvous Protocol



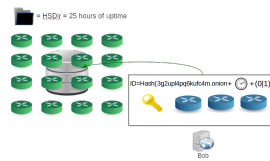
Tor Rendezvous Protocol



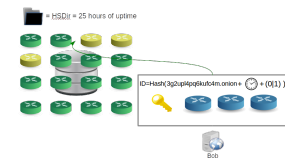
Tor Rendezvous Protocol



Responsible Hidden Service Directories



Responsible Hidden Service Directories



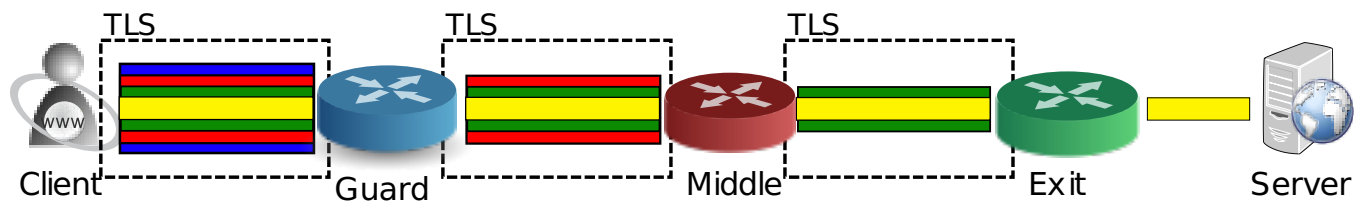
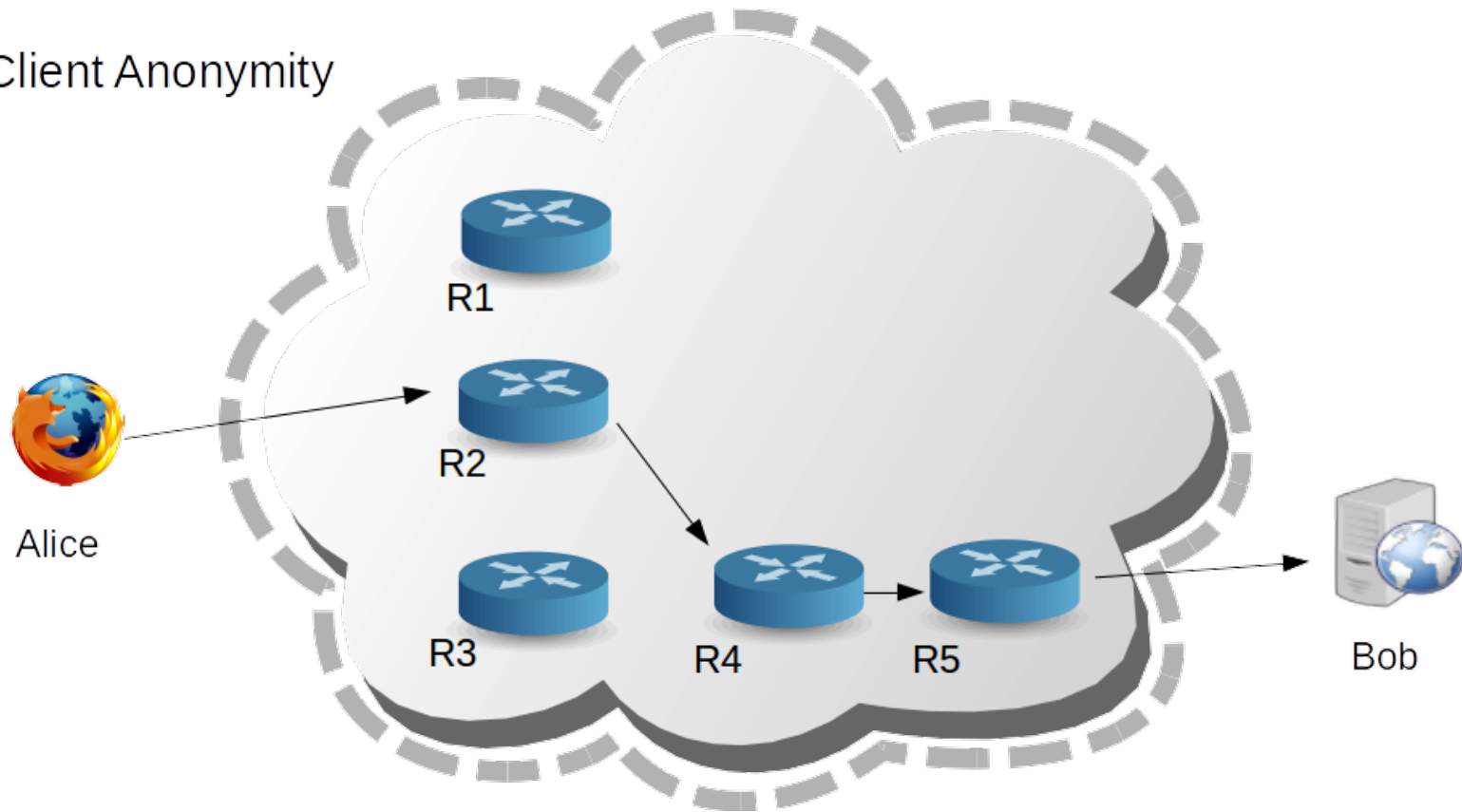
## Shadowing

A technique described in [1] allowed us to collect onion addresses fast and cheaply






















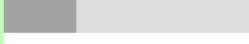
























































































[1] Trawling for Tor Hidden Services: Detection, Measurement, Deanonimization, IEEE Symposium on Security and Privacy

# Tor

Client Anonymity

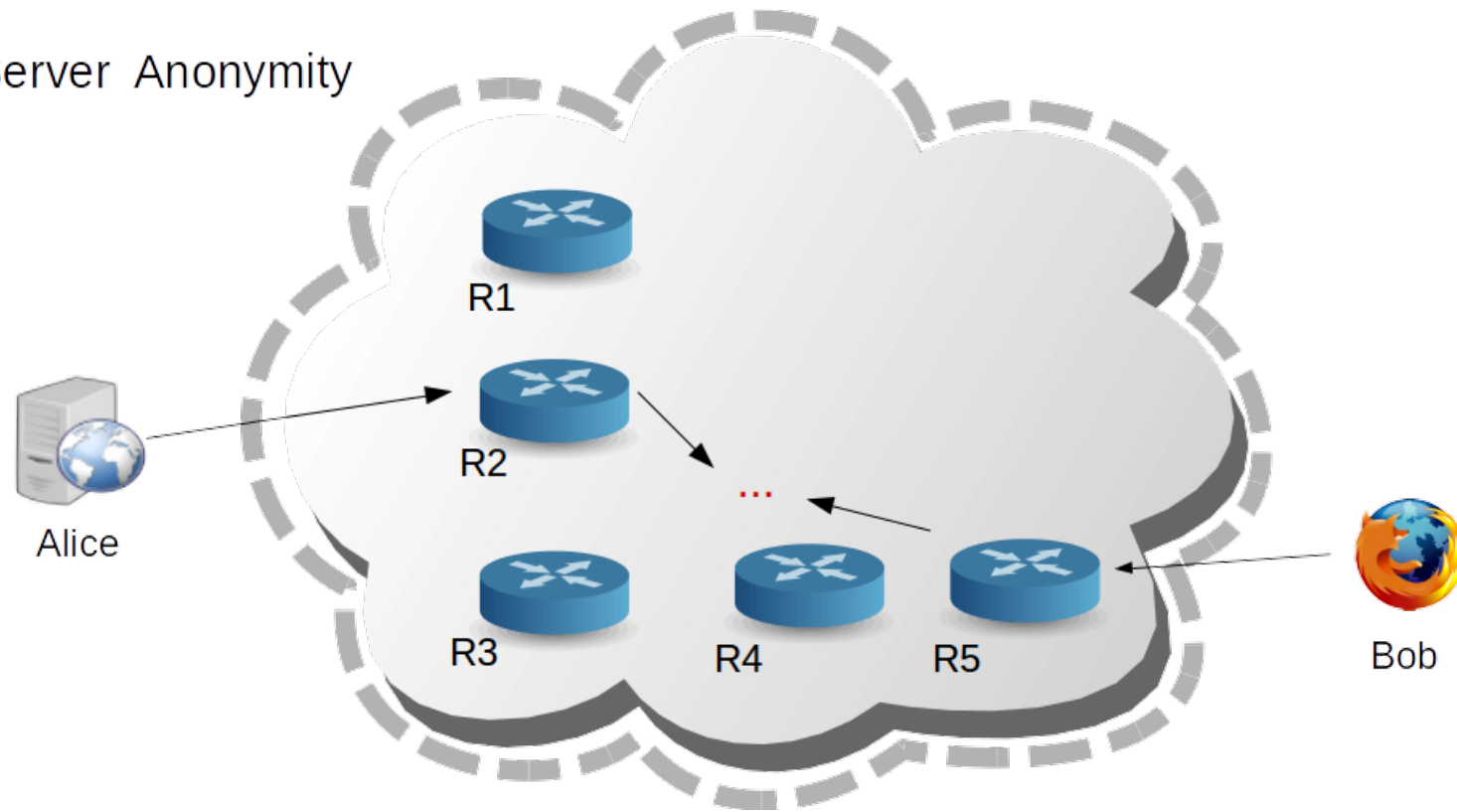


# Consensus

 menTor		1737	<b>67 d</b>	55863896.cust.multi.fi [85.134.56.150]	    
 microshaft		2820	<b>66 d</b>	tor-exit.microshaft.org [208.201.249.3]	    
 minisausage		3348	<b>35 d</b>	50.7.184.58 [50.7.184.58]	   
 morphium		298	<b>51 d</b>	this.is.a.Tor.server.please.see.tor.morphium.info [91.143.90.25]	    
 NetromAc		2115	<b>47 d</b>	1385160742.business.dbnet.dk [82.143.224.38]	    
 Nitr0x		175	<b>78 d</b>	50.97.1.36-static.reverse.softlayer.com [50.97.1.36]	    
 OhCanada		419	<b>51 d</b>	van1.zworg.com [209.17.191.117]	    
 onconnex80		392	<b>213 d</b>	tor01.onconnex.com [184.105.231.11]	   
 PasToutAFaitNet1		261	<b>176 d</b>	91.229.20.159 [91.229.20.159]	    
 PasToutAFaitNet2		763	<b>196 d</b>	tor2.pastoutafait.net [95.130.11.247]	    
 plebia		3599	<b>79 d</b>	tor-exit.plebia.org [37.59.162.218]	    
 pps		9	<b>59 d</b>	184-22-164-107.static.hostnoc.net [184.22.164.107]	    
 PrivaTOReu		4229	<b>100 d</b>	torexit.privator.eu [88.208.90.1]	    
 programmercpp		149	<b>36 d</b>	proxy [213.171.220.40]	    
 PsyNetNP		155	<b>52 d</b>	broadband-95-84-148-164.nationalcablenetworks.ru [95.84.148.164]	    
 Qwerty		91	<b>157 d</b>	93.167.245.178 [93.167.245.178]	    

# Tor hidden services

Server Anonymity





## Public Library of US Diplomacy: Kissinger Cables

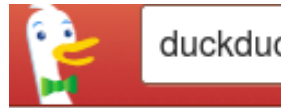
2013-04-08

The Kissinger Cables are part of today's launch of the WikiLeaks Public Library of US Diplomacy (PlusD), which holds the world's largest searchable collection of United States confidential, or formerly confidential, diplomatic communications. As of its launch on April 8, 2013 it holds 2 million records comprising approximately 1 billion words.

## Detainee Policies

2012-10-24

WikiLeaks has begun releasing the 'Detainee Policies': more than 100 classified or otherwise restricted files from the United States Department of Defense covering the rules and procedures for detainees in U.S. military custody. Over the next month, WikiLeaks will release in chronological order the United States' military detention policies followed for more than a



**Duck**  
 Duck Du  
 informat  
 tradition  
 W More  
 Inter

**Duc**  
 Free  
 begin

**Duc**  
 duck

CB **Duc**  
 Duck  
 Ibang  
 crunc

**W** **Duc**  
 Bus  
 Duck  
 Goog  
 wired


Ir  
 U  
 ct  
 C



**Duck Duck Go** ⊖

Duck Duck Go is a search engine based in Valley Forge, Pennsylvania that uses information from crowd-sourced sites (like Wikipedia) with the aim of augmenting traditional results and improving relevance.

 [More at Wikipedia](#) | Official site: [duckduckgo.com](#)

 [Internet search engines](#)


  
 DuckDuckGo

**Duckduckgo | BEGIN-DOWNLOAD.com**

Free Download flv app Fast & Simple.  
[begin-download.com](#) Sponsored link


**Duck Duck Go** Official site  
[duckduckgo.com](#) More from duckduckgo.com ▶

CB **DuckDuckGo | CrunchBase Profile**  
**DuckDuckGo** is a search engine, like Google. Use it to get more Zero-click Info, more privacy, less spam, lbang syntax and lots of other goodies.  
[crunchbase.com/company/duck-duck-go](#) More from crunchbase.com ▶


**DuckDuckGo Challenges Google on Privacy (With a Billboard) | Wired Business...**  
**DuckDuckGo**, a one-man-band search engine based out of Valley Forge, Pennsylvania, is aiming at Google's privacy practices with an unusual tactic: a billboa.  
[wired.com/business/2011/01/duckduckgo-google-privacy/](#) More from wired.com ▶

STAR

SECURE  
EDITORS

You can use this s

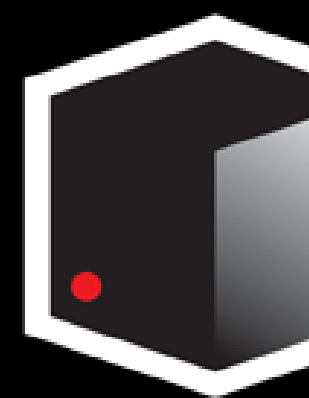
GET START

Load times may v

Ir  
 U  
 ci  
 blic  
 dential,  
 2  
 00  
 ment of  
 itary  
 al  
 then

C

# THE NEW YORKER STRONGBOX



## SECURELY SUBMIT FILES TO WRITERS AND EDITORS

You can use this site to submit information, messages, and files to writers and editors at *The New York*

[GET STARTED](#)

Load times may vary.



Silk  
anonym

Shop by Category

- Food 5
- Beverages
- Apparel 168
- Art 4
- Books 665
- Collectibles 8
- Computer equ
- Custom Order
- Digital goods
- Drug parapher
- Drugs 4,217
- Electronics 37
- Erotica 389
- Forgeries 92
- Hardware 3
- Herbs & Supp
- Home & Gard
- Jewelry 52
- Lab Supplies
- Lotteries & ga
- Medical 31
- Money 100
- Packaging 25
- Services 37
- Weight loss 19
- Writing 2
- Yubikeys 3



New York

Search

Go

Hi,

logout

Shop by Category

- Food 5
- Beverages 2
- Apparel 168
- Art 4
- Books 865
- Collectibles 8
- Computer equipment 30
- Custom Orders 47
- Digital goods 365
- Drug paraphernalia 174
- Drugs 4,217
- Electronics 37
- Erotica 389
- Forgeries 92
- Hardware 3
- Herbs & Supplements 14
- Home & Garden 3
- Jewelry 52
- Lab Supplies 29
- Lotteries & games 30
- Medical 31
- Money 100
- Packaging 25
- Services 37
- Weight loss 19
- Writing 2
- Yubikeys 3

sort by:

Domestic only



### ☯ Cocaine Energy Drink - Banned ☯

seller: namedclined(100)  
ships from: United States of America

**\$0.74**  
add to cart



### Kefir grains - water kefir

seller: etizolam(97)  
ships from: United States of America

**\$0.83**  
add to cart

no image

### 3Jane Stealth Listing Feedback

seller: 3Jane(100)  
ships from: Canada

**\$0.00**  
add to cart



### Kefir grains - milk kefir

seller: etizolam(97)  
ships from: United States of America

**\$0.90**  
add to cart

Red Wine Red Toumy Dams Office Bottle 75cl

# Skynet,

Posted by [Clau](#)

ndering through  
e night.

we spent time  
origin named "th

is an overview  
Jsenet.

## re the war

ople download s  
k hoster. Most h

a distributed di

# Skynet, a Tor-powered botnet straight from Reddit

Posted by [Claudio Guarnieri](#) in [Information Security](#) on Dec 6, 2012 2:51:13 PM

฿0.74  
add to cart

Wandering through the dark alleys of the Internet we encountered an unusual malware artifact, something that we didn't see at night.

฿0.83  
add to cart

As we spent time looking at it, the more it started to look unusually familiar. As a matter of fact it turned out to be of origin named "throwaway236236" described in a very popular *I Am A* thread you can read [here](#).

This is an overview of this malware labelled by the creator as **Skynet**: a Tor-powered trojan with DDoS, Bitcoin mining and Usenet.

฿0.00  
add to cart

## Are the warez

฿0.90  
add to cart

"...people download software from Usenet and install it in the offices or at friends pretty often. Also Usenet isn't the best file hoster. Most Providers have their own Usenet client for idiot proof downloads"

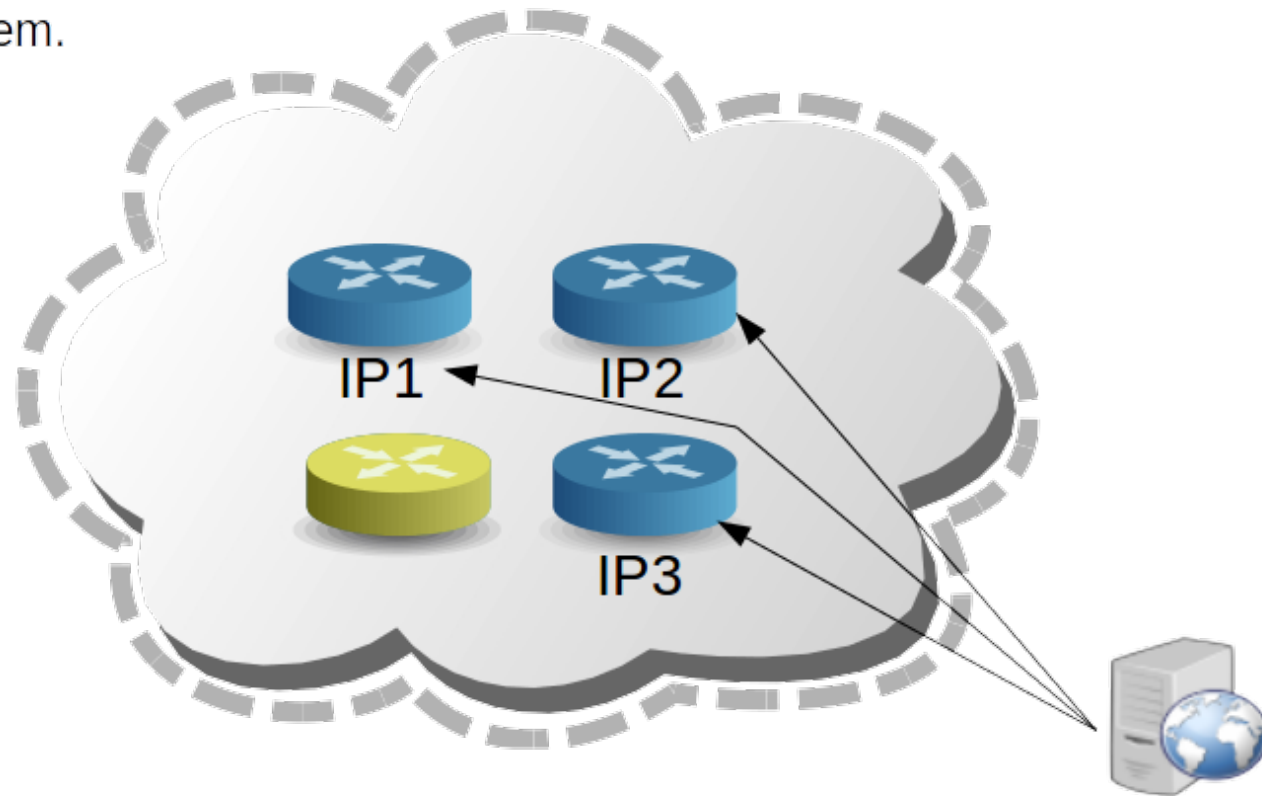
Usenet is a distributed discussion platform established around 1980 and still very popular worldwide.

# Tor Rendezvous Protocol

**Step1:** Bob picks some introduction points and builds circuits to them.



Alice



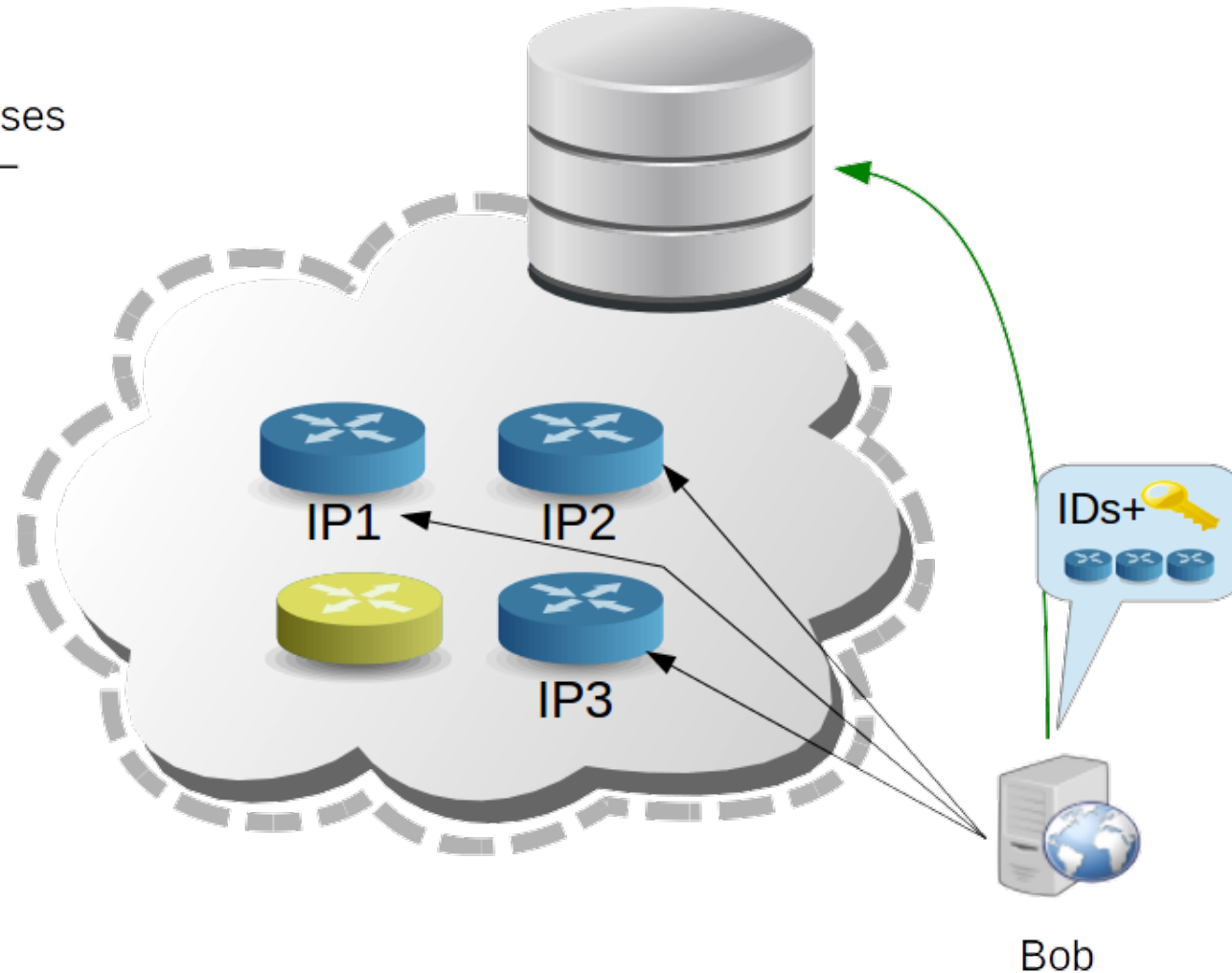
Bob

# Tor Rendezvous Protocol

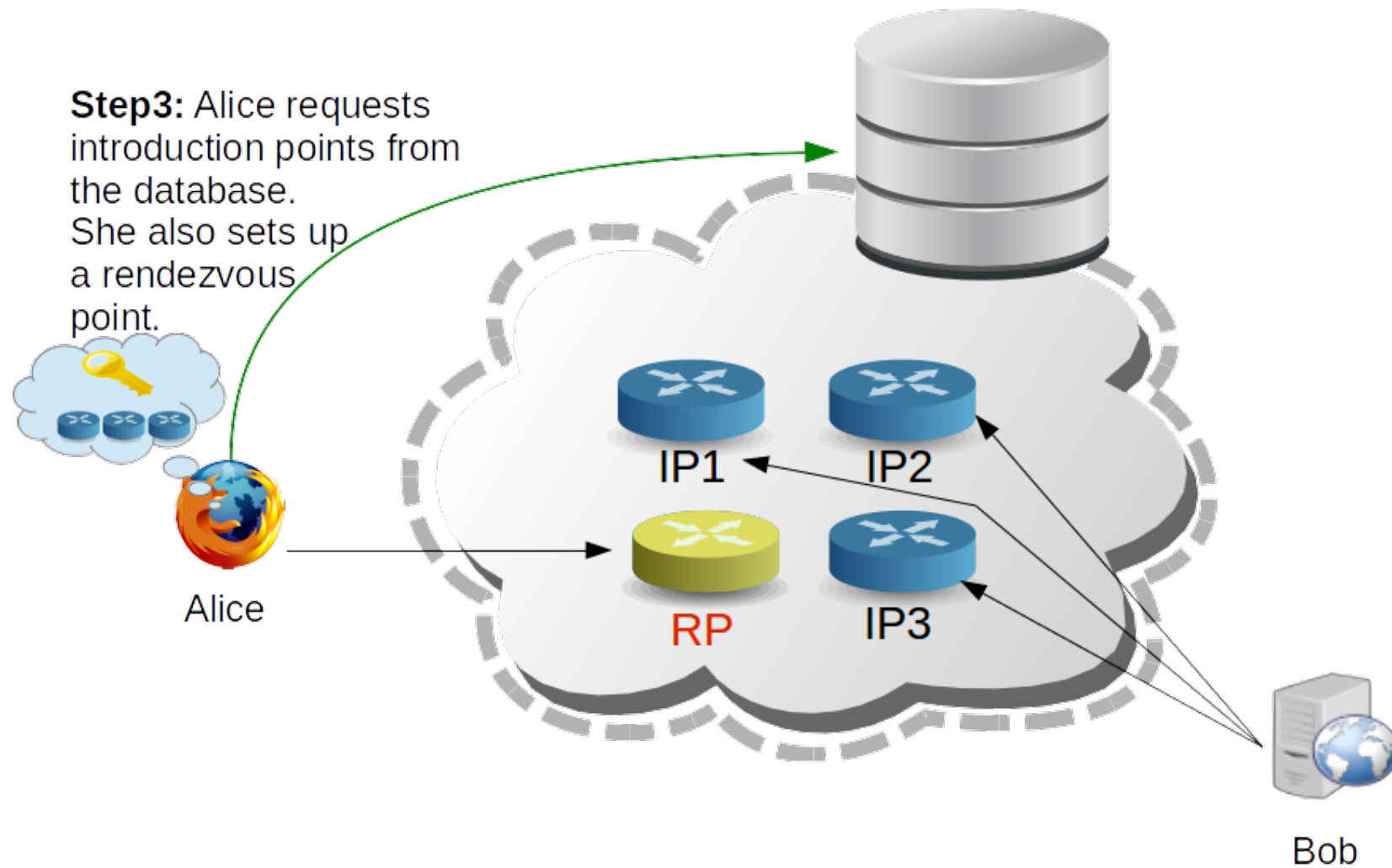
**Step2:** Bob advertises his hidden service – `<z>.onion` – at the database.



Alice

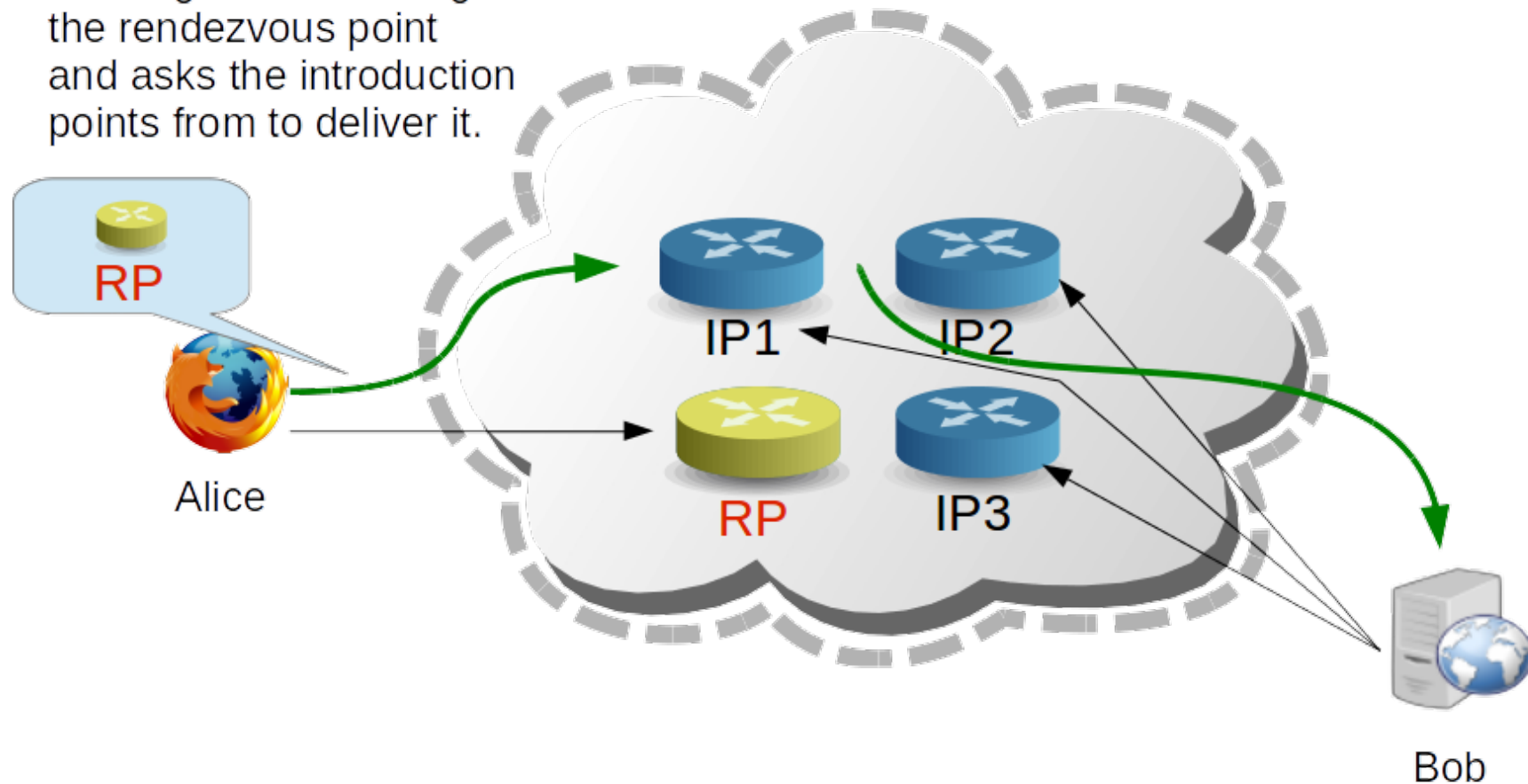


# Tor Rendezvous Protocol



# Tor Rendezvous Protocol

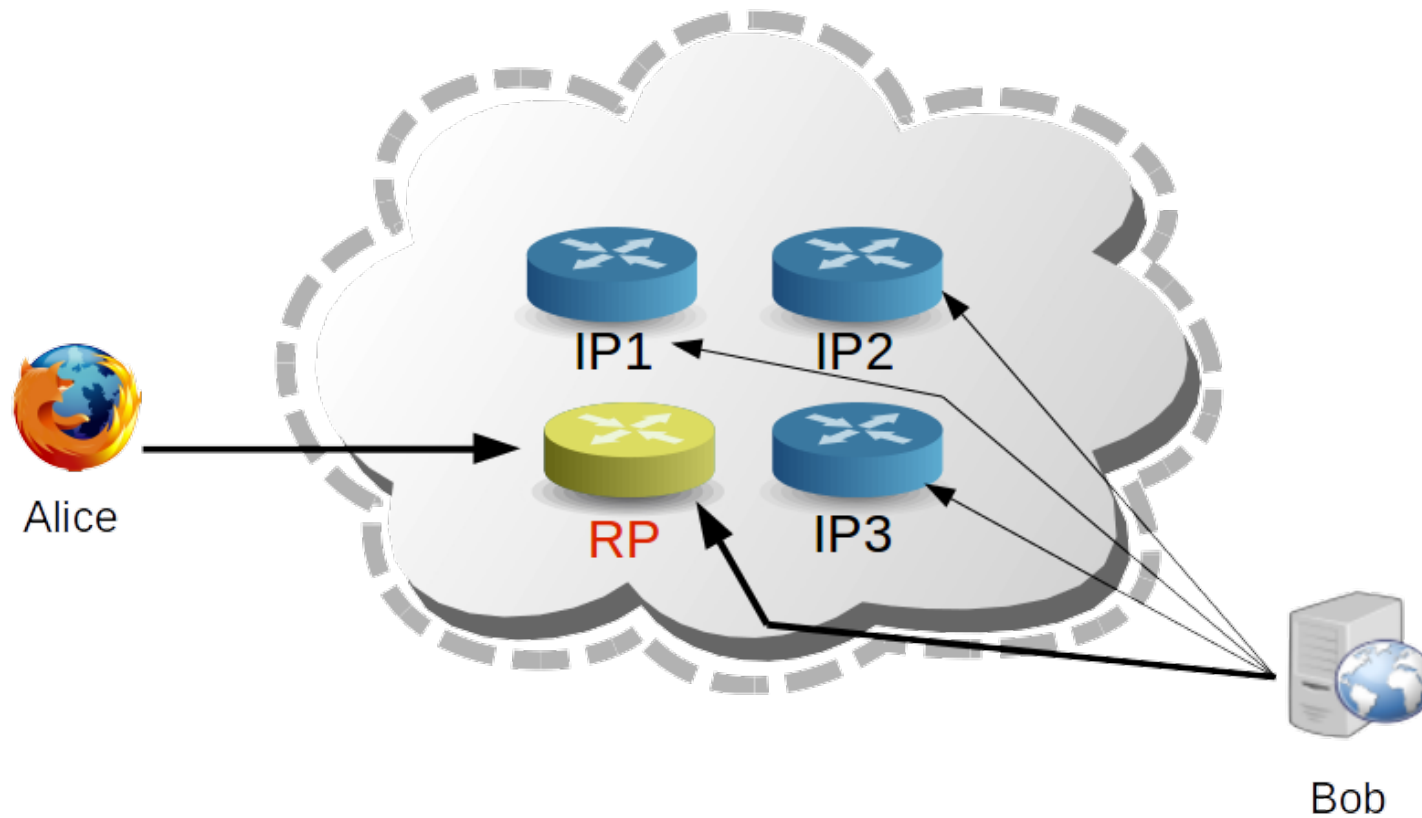
**Step4:** Alice sends a message to Bob listing the rendezvous point and asks the introduction points from to deliver it.



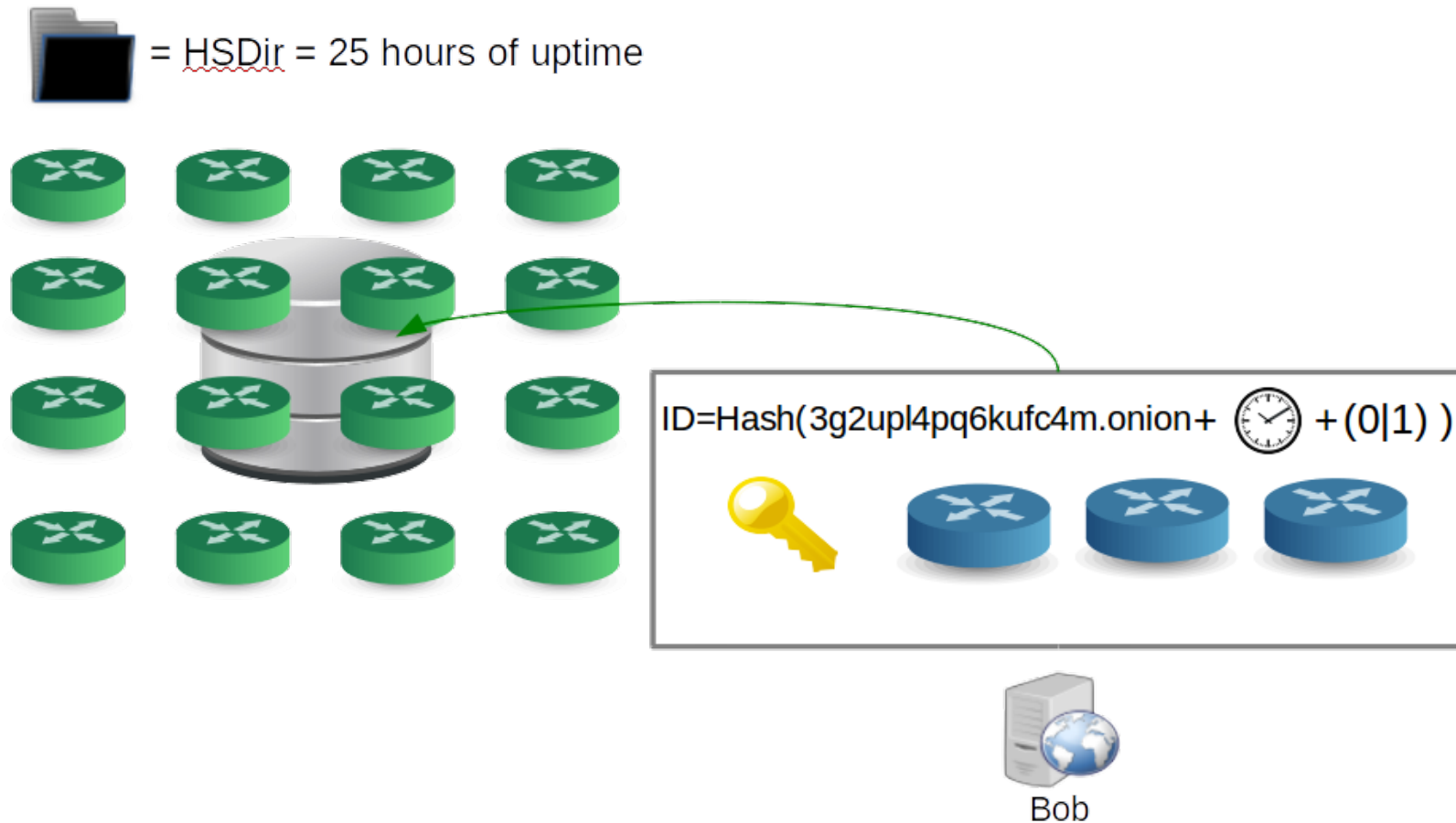


# Tor Rendezvous Protocol

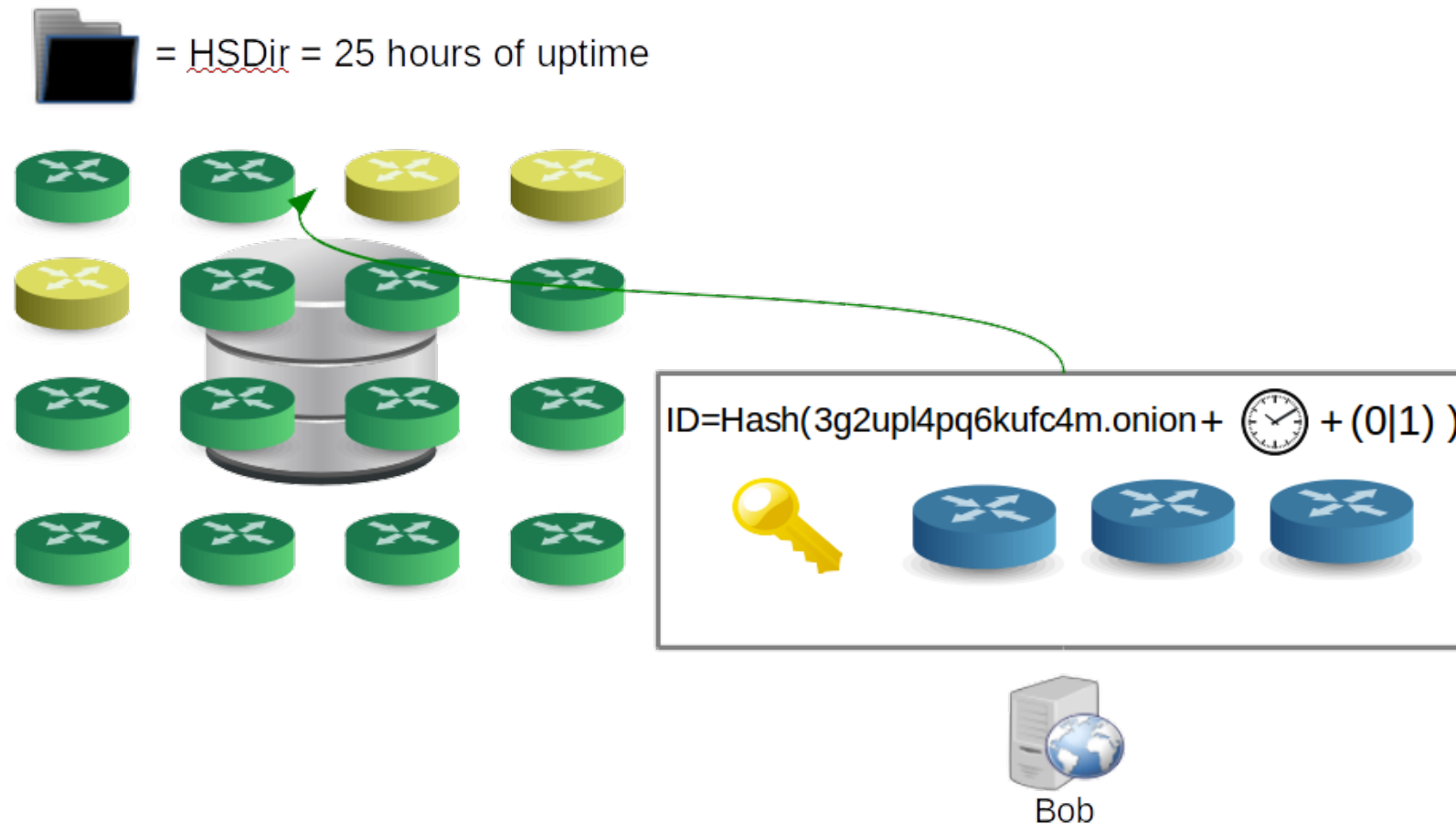
**Step5:** Alice and Bob  
Connect at the Rendezvous  
point



# Responsible Hidden Service Directories



# Responsible Hidden Service Directories

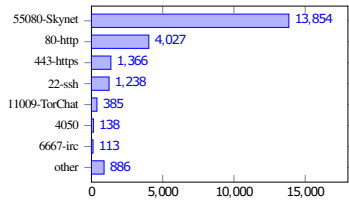


# Shadowing

A technique described in [1] allowed us to collect onion addresses fast and cheaply

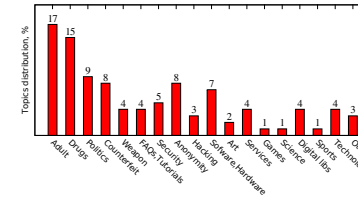
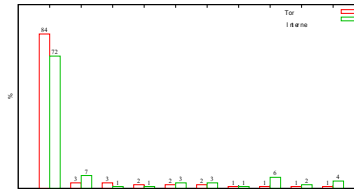
[1] Trawling for Tor Hidden Services: Detection, Measurement, Deanononymization, IEEE Symposium on Security and Privacy

# Statistics



## HTTP classification

- 8,153 tried
- Were able to connect to 6,579 using HTTP/HTTPS
- 3529 were inappropriate for classification

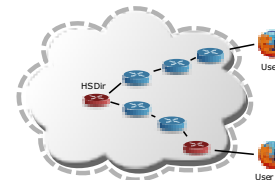


## Mevade botnet

#	RQSTS	Addr	Desc	#	RQSTS	Addr	Desc
1	13714	uecbcfqfofufwckrd.onion	Goldnet	22	899	qdzjxwujdtxrjkrz.onion	Skynet
2	11582	arlopppezch53w3i.onion	Goldnet	23	898	6tkpktox73usm5vq.onion	Skynet
3	11315	pomyeasfnmtn544p.onion	Goldnet	24	889	kk2wajy64oip2***.onion	Adult
4	7324	lqqciywa5yzzxewc3.onion	Goldnet	25	781	gpt2u5hhaqvmnwhr.onion	Skynet
5	7183	eqlbyxrpdp2wdjeig.onion	Goldnet	26	746	smouse21bzrgeof4.onion	< n/a>
6	6852	onhimfogy4acjv4.onion	< n/a>	27	694	xqz3u5drneuzhaeo.onion	FreedomHosting
7	6528	saxtca3ktuhcyqx3.onion	Goldnet	28	667	f2y1gv2jochpzm4c.onion	Skynet
8	4941	qxc7mc24mj7m4e2o.onion	< n/a>	29	585	kdq2y44aaas2a***.onion	Adult
9	3746	mwjjmahc4cj1qp.onion	BcMine	30	542	4pms4sejrryc***.onion	Adult
10	3678	mepogl2rljvj374e.onion	Skynet	...	...	...	...
11	2573	m3hjrfrh4hlqc6***.onion	Adult	34	453	dkn255hz262ypmii.onion	SilkRoad(wiki)
12	1950	ua4ttfm47jt32igm.onion	Skynet	...	...	...	...
13	1863	opva2pilsncvt***.onion	Adult	47	255	dppmfxaacucguzpc.onion	TorDir
14	1665	nbo32e147o5cl***.onion	Adult	...	...	...	...
15	1631	firel015skg6e***.onion	Adult	62	172	5onwnspjvuk7cwvk.onion	BlckMrktReloaded
16	1481	niazgxzlrpbevvgq.onion	Skynet	...	...	...	...
17	1326	owbm3sgjgdndmydf.onion	Skynet	157	55	3g2up14pg6kufc4m.onion	DuckDuckGo
18	1175	silkroadvb5piz3r.onion	Silk Road	...	...	...	...
19	1094	candy4ci6id24***.onion	Adult	250	30	x7yxqg5v4j6yzhti.onion	Onion Bookmarks
20	1021	x3wyzqg6cfbqrwht.onion	Skynet	...	...	...	...
21	942	4njzpz3wi6leo772.onion	Skynet	547	10	torhostg5s7pa2sn.onion	Tor Host

TABLE II  
RANKING OF MOST POPULAR HIDDEN SERVICES

## Opportunistic deanonymisation of clients



## Opportunistic deanonymisation of clients



## Mevade botnet

- Popular but no results in search engines
- Port 80 (503 error)
- They forgot to disable Server-status page =)
- 330 KBytes/sec, 10 req/sec
- From uptime: two different physical servers

## Mevade botnet

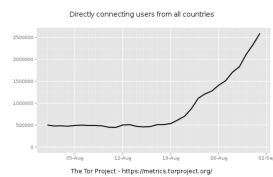
- Command and control connectivity via Tor.onion links
- Seems that the purpose of this malware network is to load additional malware onto the system and that the infected systems are for sale

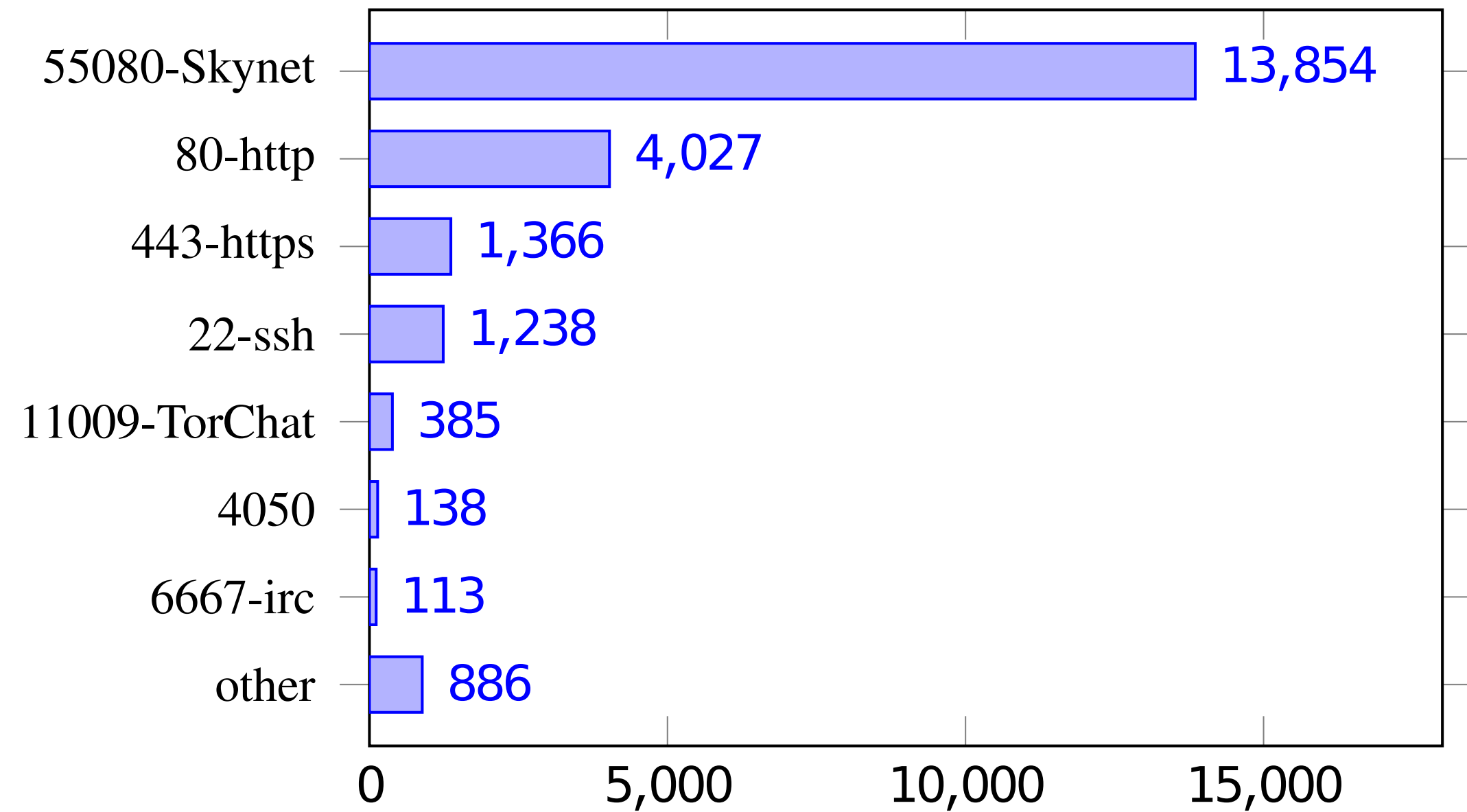
## Tracking detection

- One entity has taken over all 6 HSDRs for a single time period, a month before the silkroad was taken down by the FBI

Thank you

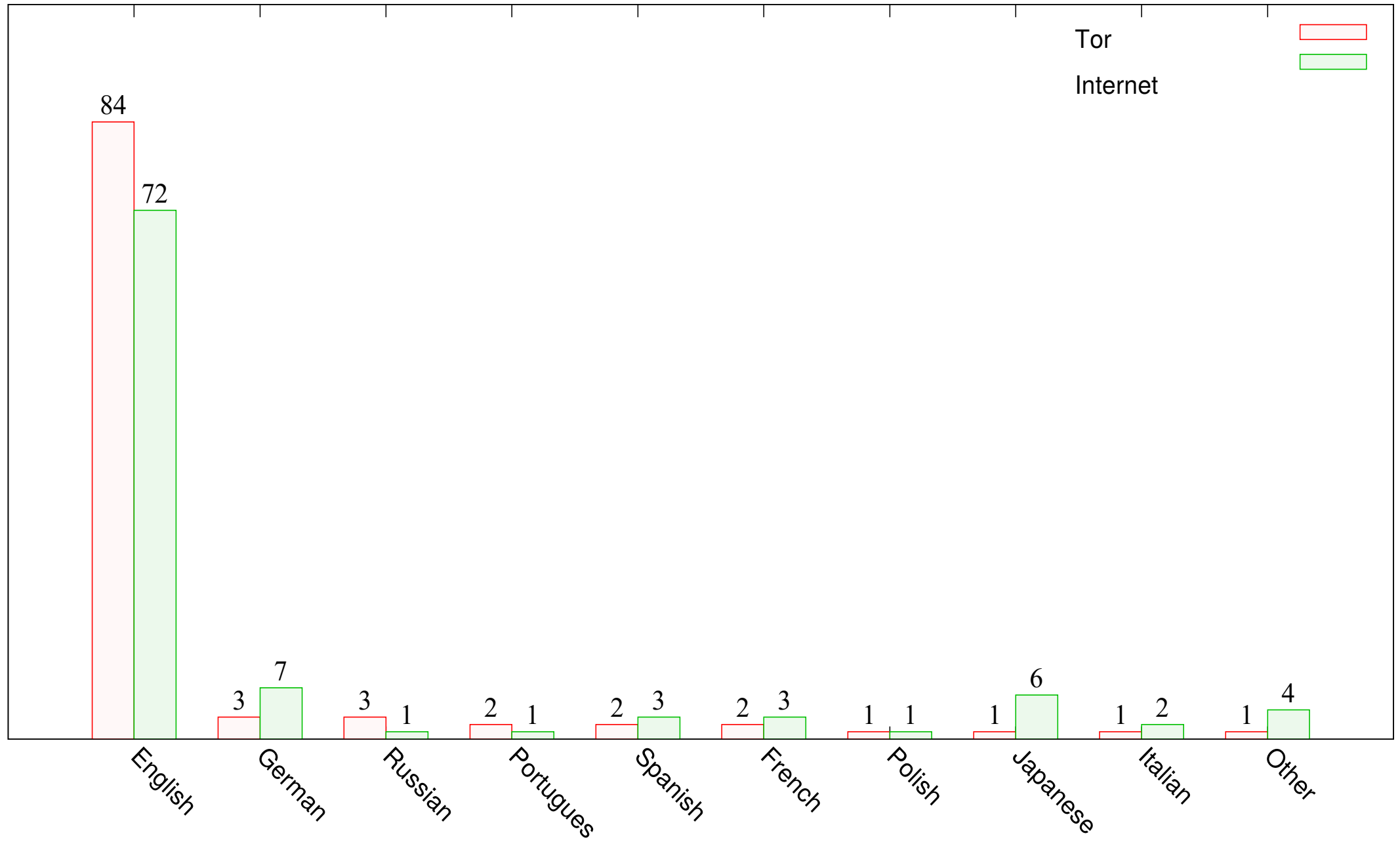
## Mevade botnet



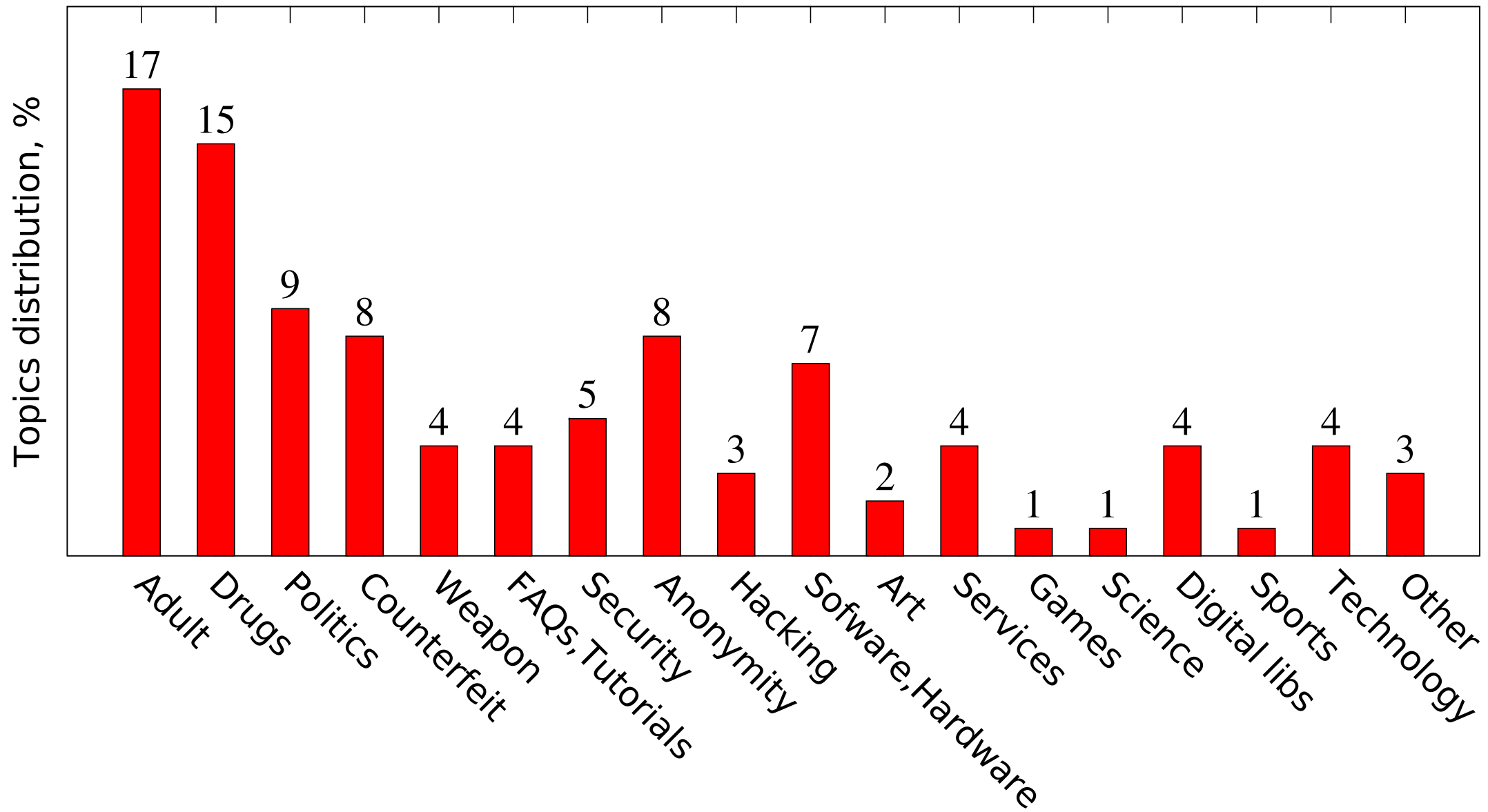


# HTTP classification

- 8,153 tried
- Were able to connect to 6,579 using HTTP/HTTPS
- 3529 were inappropriate for classification



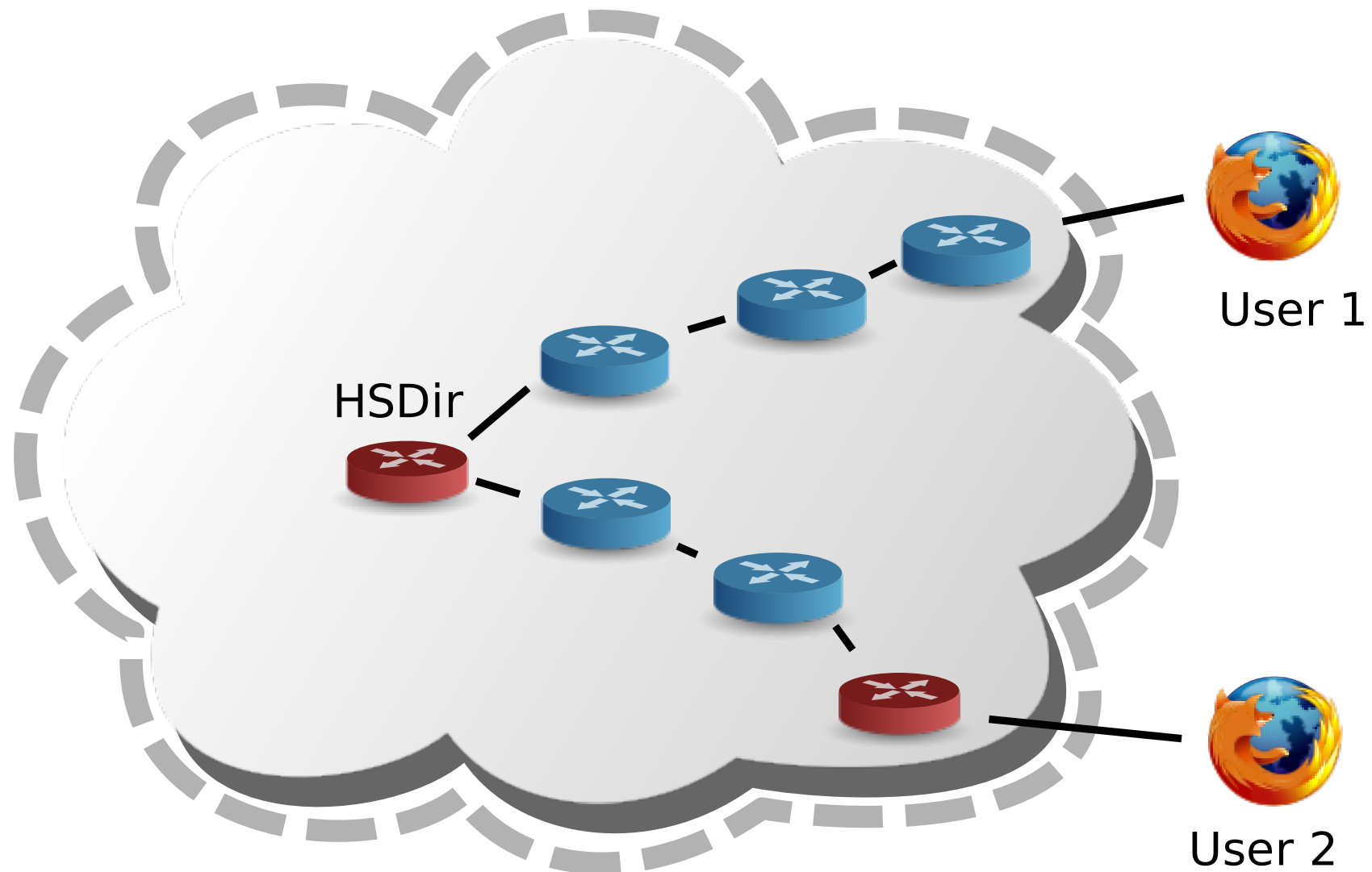




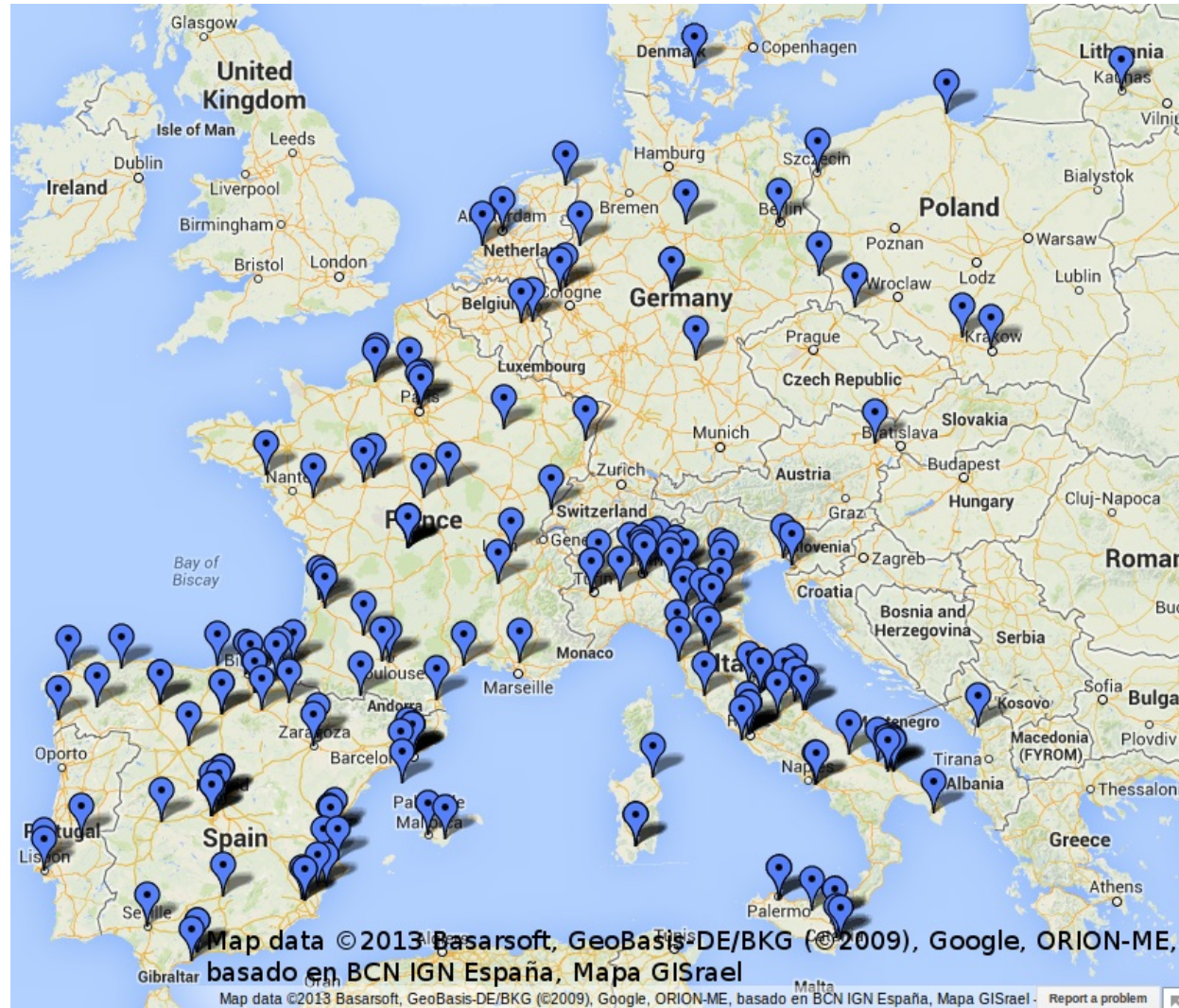
#	RQSTS	Addr	Desc	#	RQSTS	Addr	Desc
1	13714	uecbcfgfofuwkcrd.onion	Goldnet	22	899	qdzjxwujdtxrjkrz.onion	Skynet
2	11582	arloppepzch53w3i.onion	Goldnet	23	898	6tkpktox73usm5vq.onion	Skynet
3	11315	pomyeasfnmtn544p.onion	Goldnet	24	889	kk2wajy64oip2***.onion	Adult
4	7324	lqqciywa5yzzewc3.onion	Goldnet	25	781	gpt2u5hhaqvmnwhr.onion	Skynet
5	7183	eqlbyxrp2wdjeig.onion	Goldnet	26	746	smouse2lbzrgeof4.onion	<n/a>
6	6852	onhiimfoqy4acjv4.onion	<n/a>	27	694	xqz3u5drneuzhaeo.onion	FreedomHosting
7	6528	saxtca3ktuhcyqx3.onion	Goldnet	28	667	f2y1gv2jochpzm4c.onion	Skynet
8	4941	qxc7mc24mj7m4e2o.onion	<n/a>	29	585	kdq2y44aaas2a***.onion	Adult
9	3746	mwjjmahc4cj1qp.onion	BcMine	30	542	4pms4sejqrryc***.onion	Adult
10	3678	mepogl2rljvj374e.onion	Skynet	...	...	...	...
11	2573	m3hjrfh4hlqc6***.onion	Adult	34	453	dkn255hz262ypmii.onion	SilkRoad(wiki)
12	1950	ua4ttfm47jt32igm.onion	Skynet	...	...	...	...
13	1863	opva2pilsncvt***.onion	Adult	47	255	dppmfxaacucguzpc.onion	TorDir
14	1665	nbo32el47o5cl***.onion	Adult	...	...	...	...
15	1631	firelol15skg6e***.onion	Adult	62	172	5onwnspjvuk7cwk.onion	BlckMrktReloaded
16	1481	niazgxz1rbpevgvq.onion	Skynet	...	...	...	...
17	1326	owbm3sjqdnndmydf.onion	Skynet	157	55	3g2upl4pq6kufc4m.onion	DuckDuckGo
18	1175	silkroadvb5piz3r.onion	Silk Road	...	...	...	...
19	1094	candy4ci6id24***.onion	Adult	250	30	x7yxqg5v4j6yzhti.onion	Onion Bookmarks
20	1021	x3wyzqg6cfbqrwht.onion	Skynet	...	...	...	...
21	942	4njzp3wzi6leo772.onion	Skynet	547	10	torhostg5s7pa2sn.onion	Tor Host

TABLE II  
RANKING OF MOST POPULAR HIDDEN SERVICES

# Opportunistic deanonymisation of clients



# Opportunistic deanonymisation of clients



# Mevade botnet

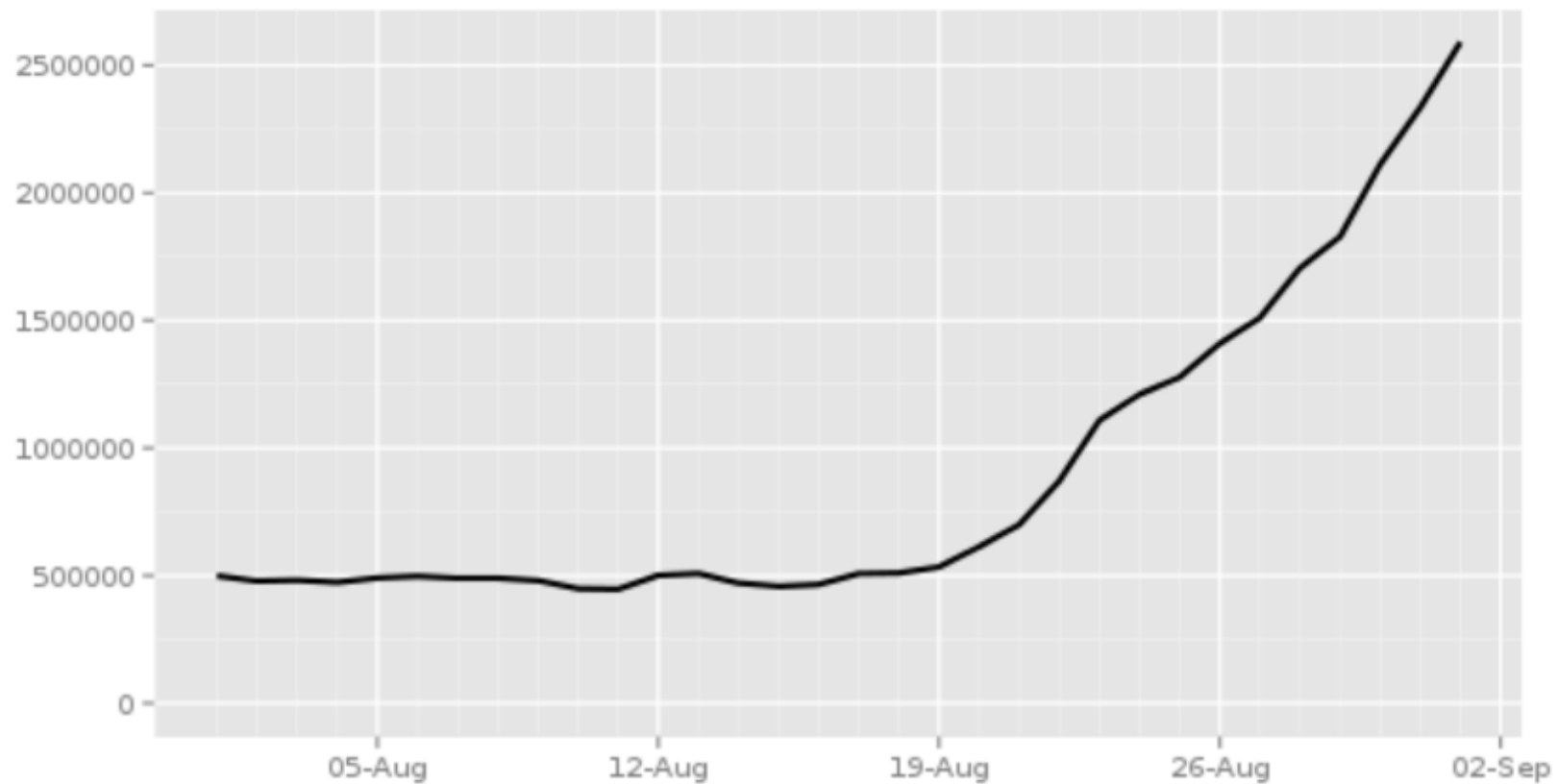
#	RQSTS	Addr	Desc	
1	13714	uecbcfgfufuwkcrd.onion	Goldnet	2
2	11582	arloppepzch53w3i.onion	Goldnet	2
3	11315	pomyeasfnmtn544p.onion	Goldnet	2
4	7324	lqqciuwa5yzxewc3.onion	Goldnet	2
5	7183	eqlbyxrpd2wdjeig.onion	Goldnet	2
6	6852	onhiimfoqy4acjv4.onion	<n/a>	2
7	6528	saxtca3ktuhcyqx3.onion	Goldnet	2
8	4941	qxc7mc24mj7m4e2o.onion	<n/a>	2
9	3746	mwjjmahc4cjjlqp.onion	BcMine	3

# Mevade botnet

- Popular but no results in search engines
- Port 80 (503 error)
- They forgot to disable  
Server-status page =)
- 330 KBytes/sec, 10 req\sec
- From uptime: two different physical servers

# Mevade botnet

Directly connecting users from all countries



The Tor Project - <https://metrics.torproject.org/>

# Mevade botnet

- Command and control connectivity via Tor .onion links
- Seems that the purpose of this malware network is to load additional malware onto the system and that the infected systems are for sale



# Tracking detection

- One entity has taken over all 6 HSDir's for a single time period, a month before the silkroad was taken down by the FBI

Thank you