Content and popularity analysis of Tor hidden services

Ivan Pustogarov, University of Luxembourg

30 June 2014

Summary (1/2)

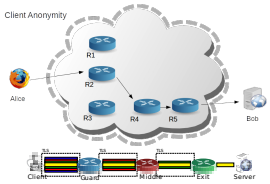
- 39824 hidden service descriptors on 4th February 2013
  -- Port scanning
  -- Popularity
- Content analysis of 3050 HTTP services

Summary (2/2)

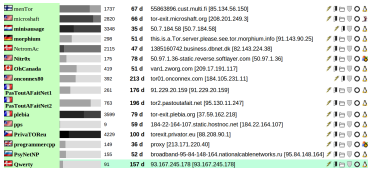
- A good chunk of Tor hidden services are not bad
- Massively used by botnets
- Most popular hidden services are shady
- One can catch clients of those shady services

Tor hidden services

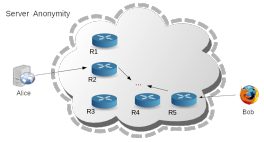
Tor

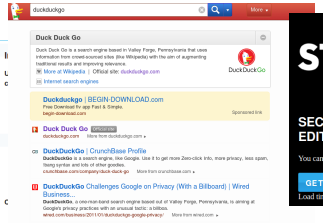


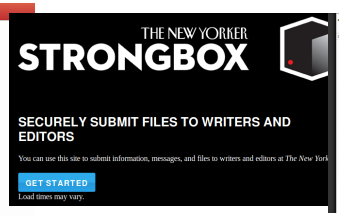
Consensus

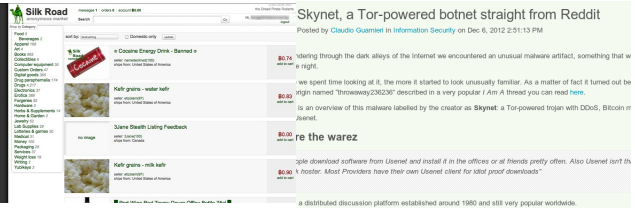


Tor hidden services

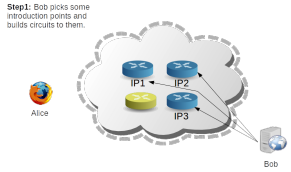




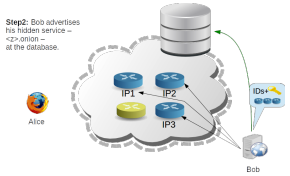




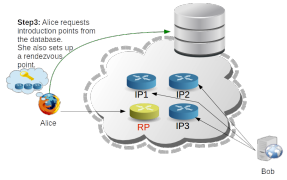
Tor Rendezvous Protocol



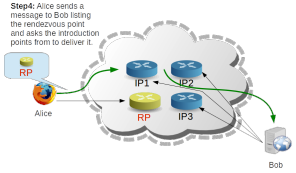
Tor Rendezvous Protocol



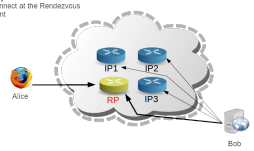
Tor Rendezvous Protocol



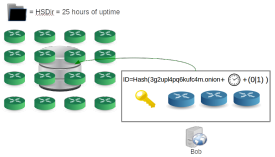
Tor Rendezvous Protocol



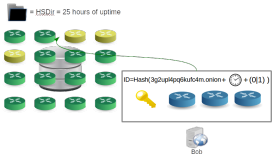
Tor Rendezvous Protocol



Responsible Hidden Service Directories



Responsible Hidden Service Directories

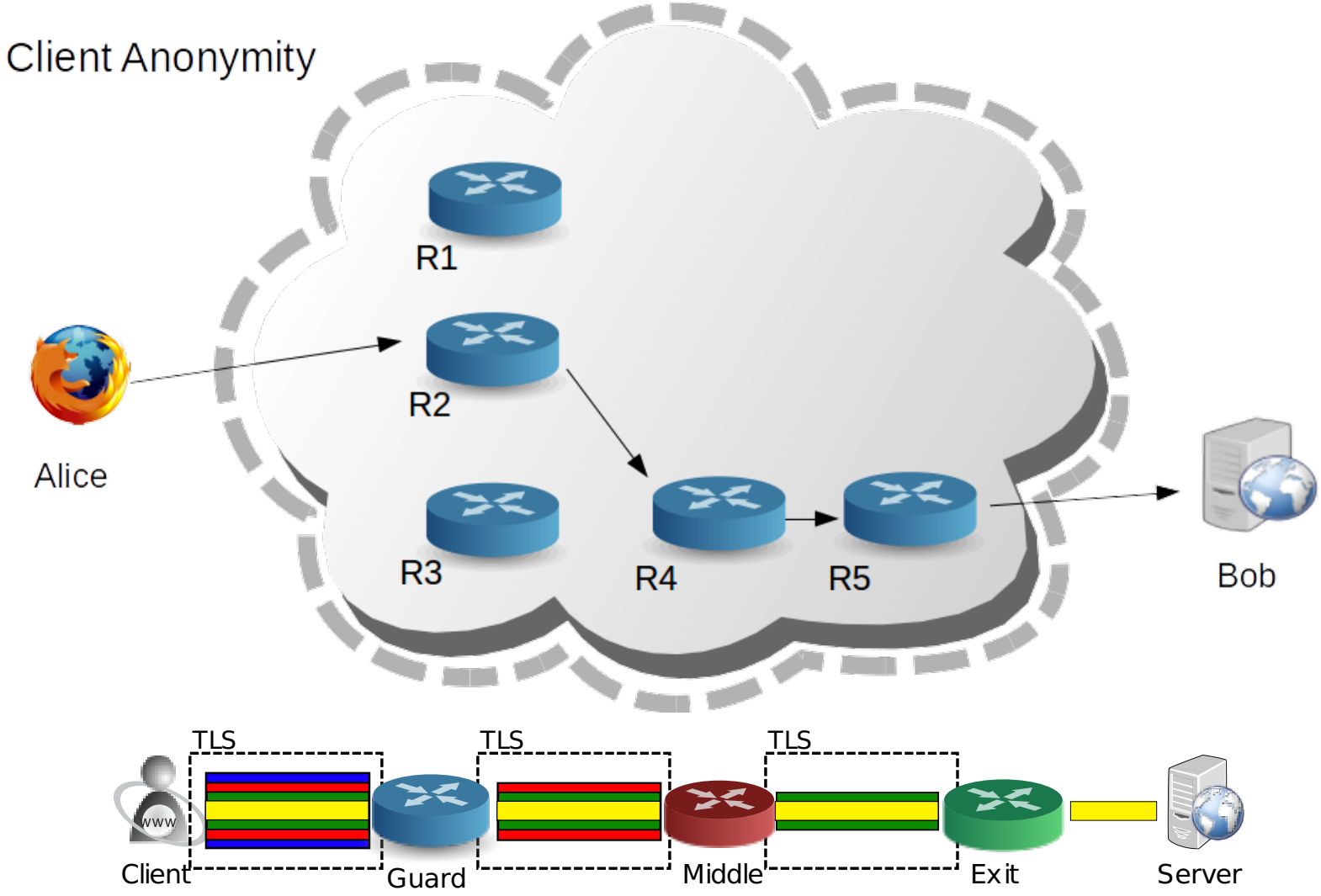


Shadowing

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

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

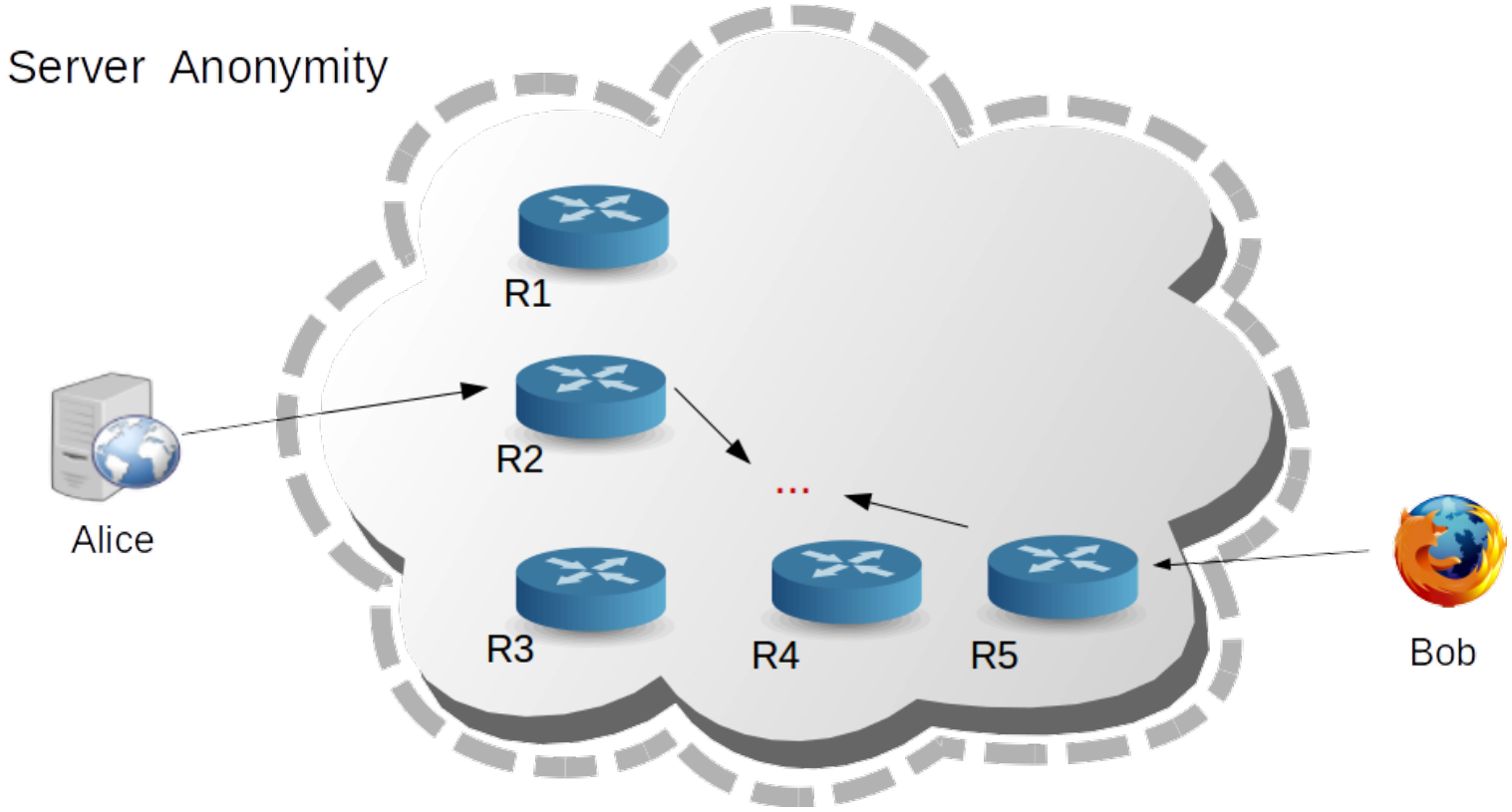
Tor


Client Anonymity
R1
R2
R3
R4
R5
Alice
Bob
TLS
TLS
TLS
www
Client
Guard
Middle
Exit
Server

Consensus

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

Tor hidden services



Public Library of US Diplomacy: Kissinger Cables

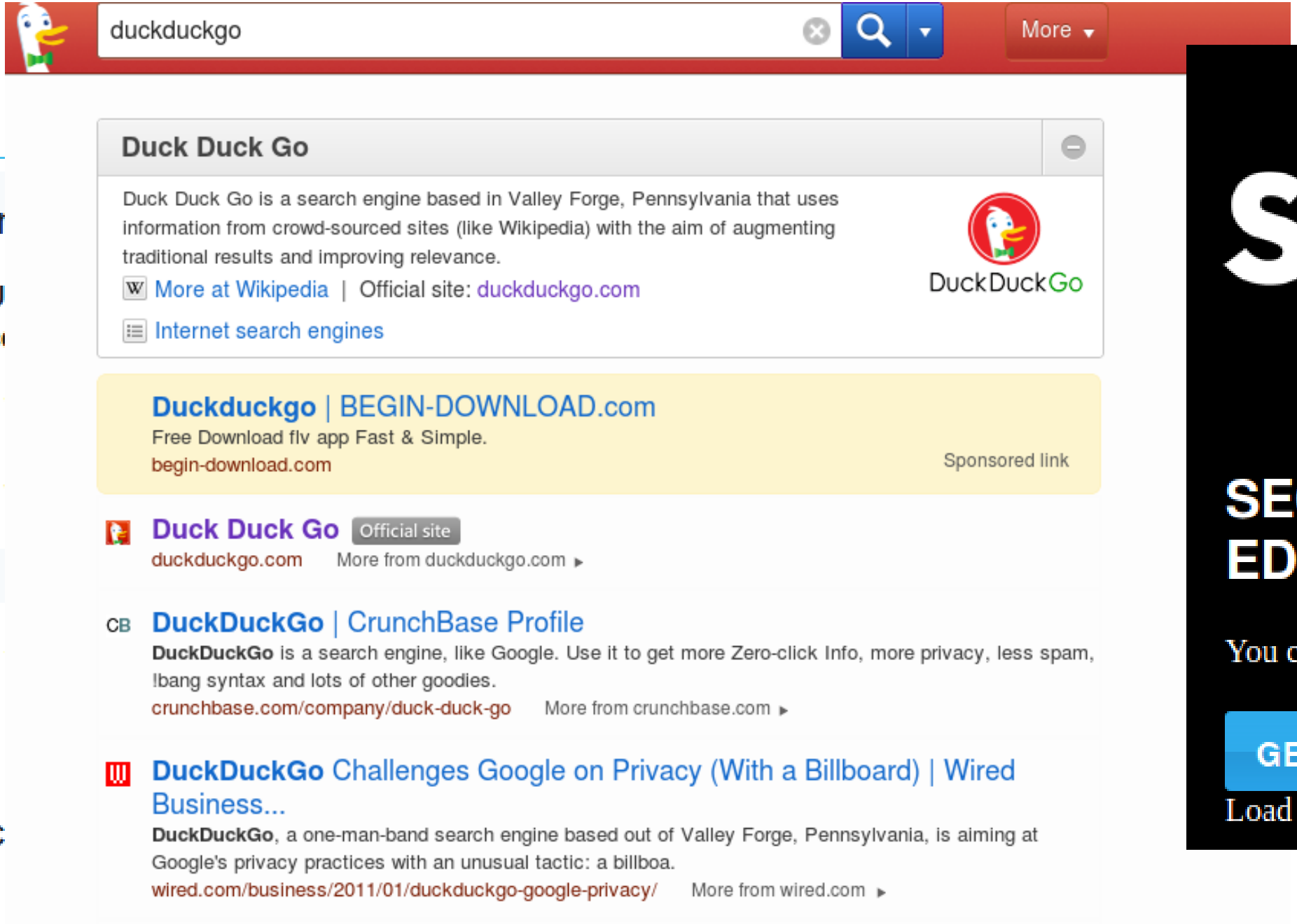
2013-04-08

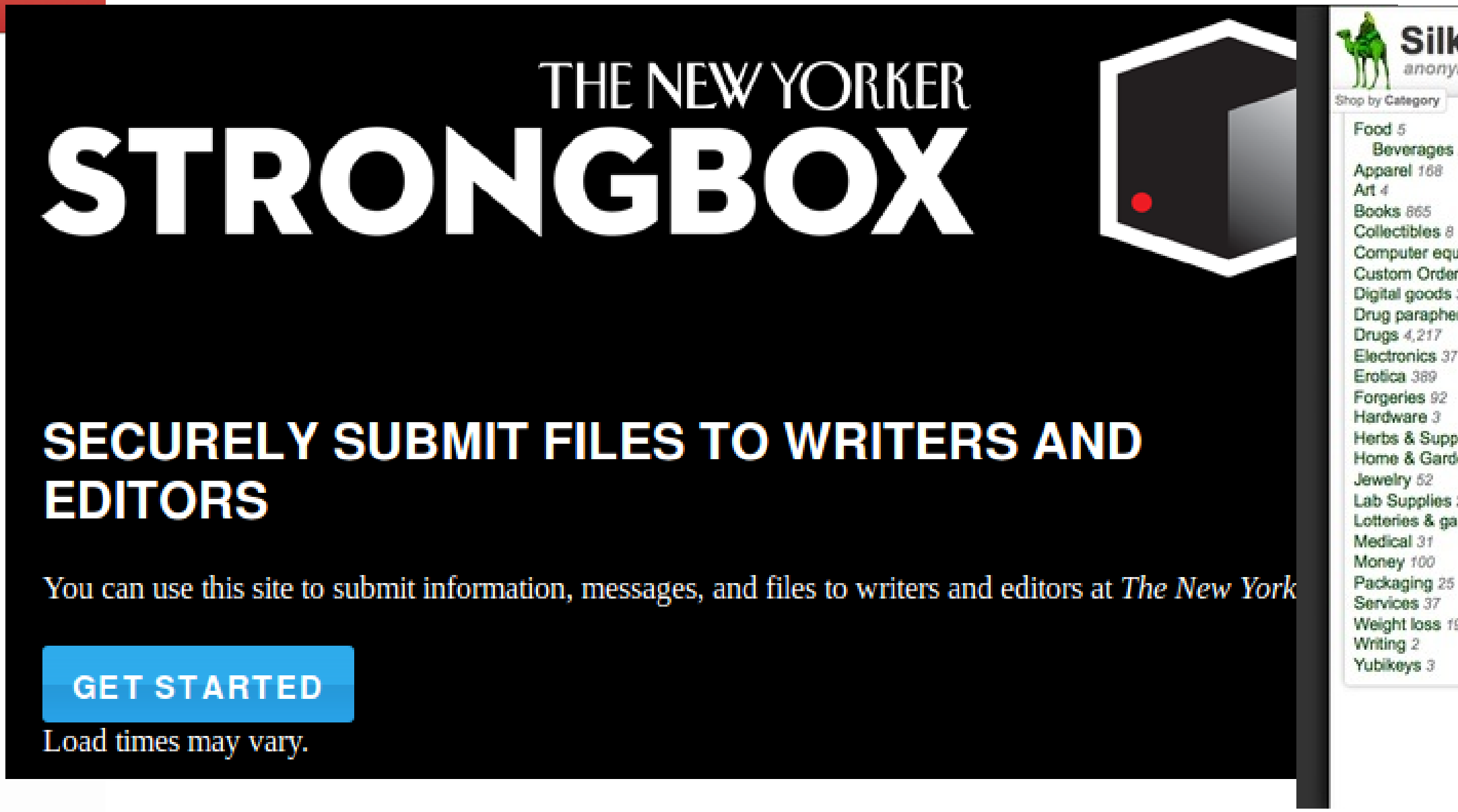
The Kissinger Cables are part of today's launch of the WikiLeaks Public Library of US Diplomacy (PlusD), which holds the world's largest searchable collection of United States confidential, or formerly confidential, diplomatic communications. As of its launch on April 8, 2013 it holds 2 million records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

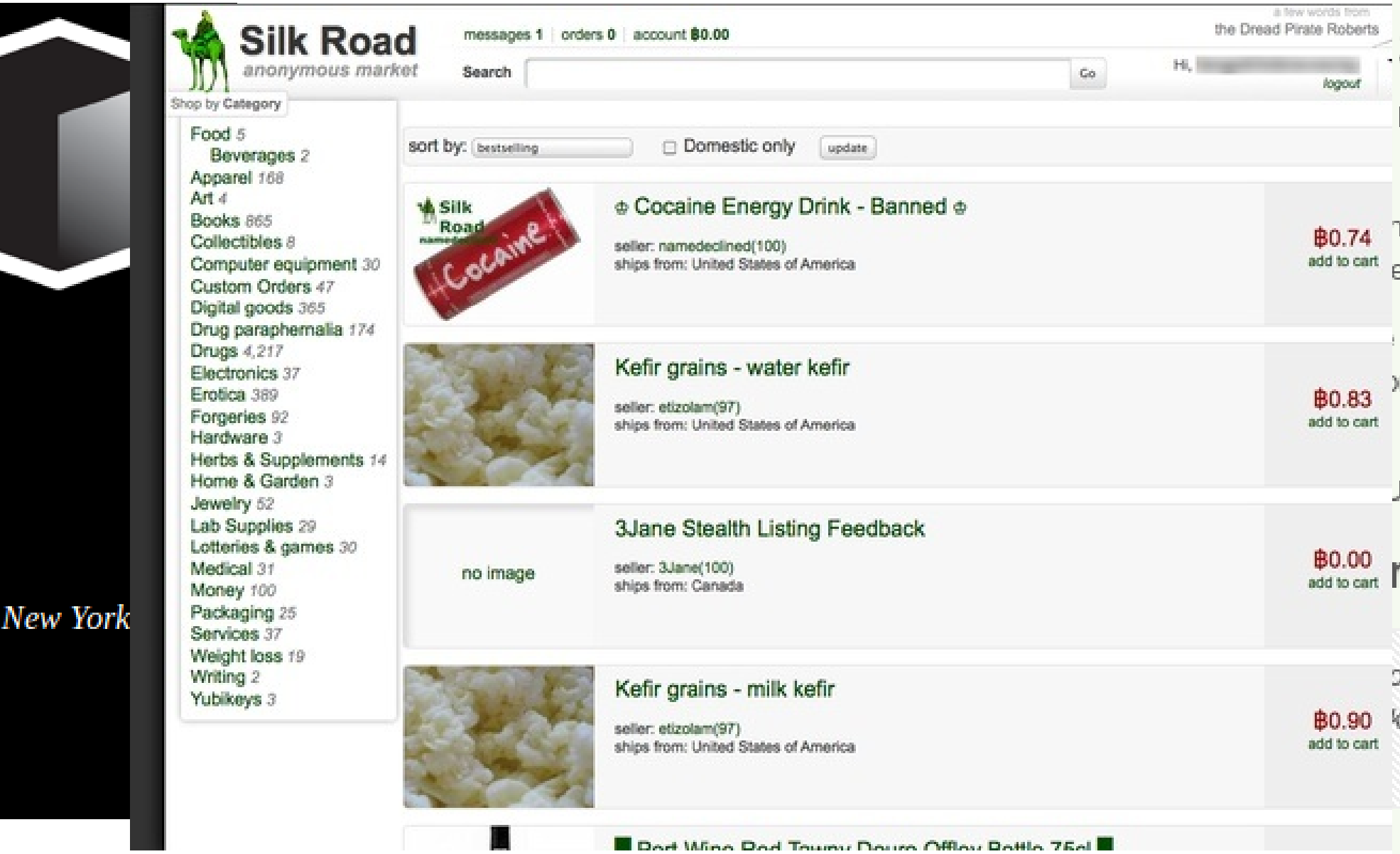
Detainee Policies

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


duckduckgo
More
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 ▸
DuckDuckGo | CrunchBase Profile
DuckDuckGo is a search engine, like Google. Use it to get more Zero-click Info, more privacy, less spam, !bang 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 ▸


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
Shop by Category
Food 5
Beverages
Apparel 168
Art 4
Books 865
Collectibles 8
Computer equ
Custom Order
Digital goods
Drug paraphe
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
Writing 2
Yubikeys 3



New York

Skynet,

Posted by Clau

ndering through
e night.

we spent time
origin named "th

is an overview
Usenet.

re the wa

ople download s
k hoster. Most

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

ndering through the dark alleys of the Internet we encountered an unusual malware artifact, something that w
e night.

we spent time looking at it, the more it started to look unusually familiar. As a matter of fact it turned out be
rigin named "throwaway236236" described in a very popular *I 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 m
Usenet.

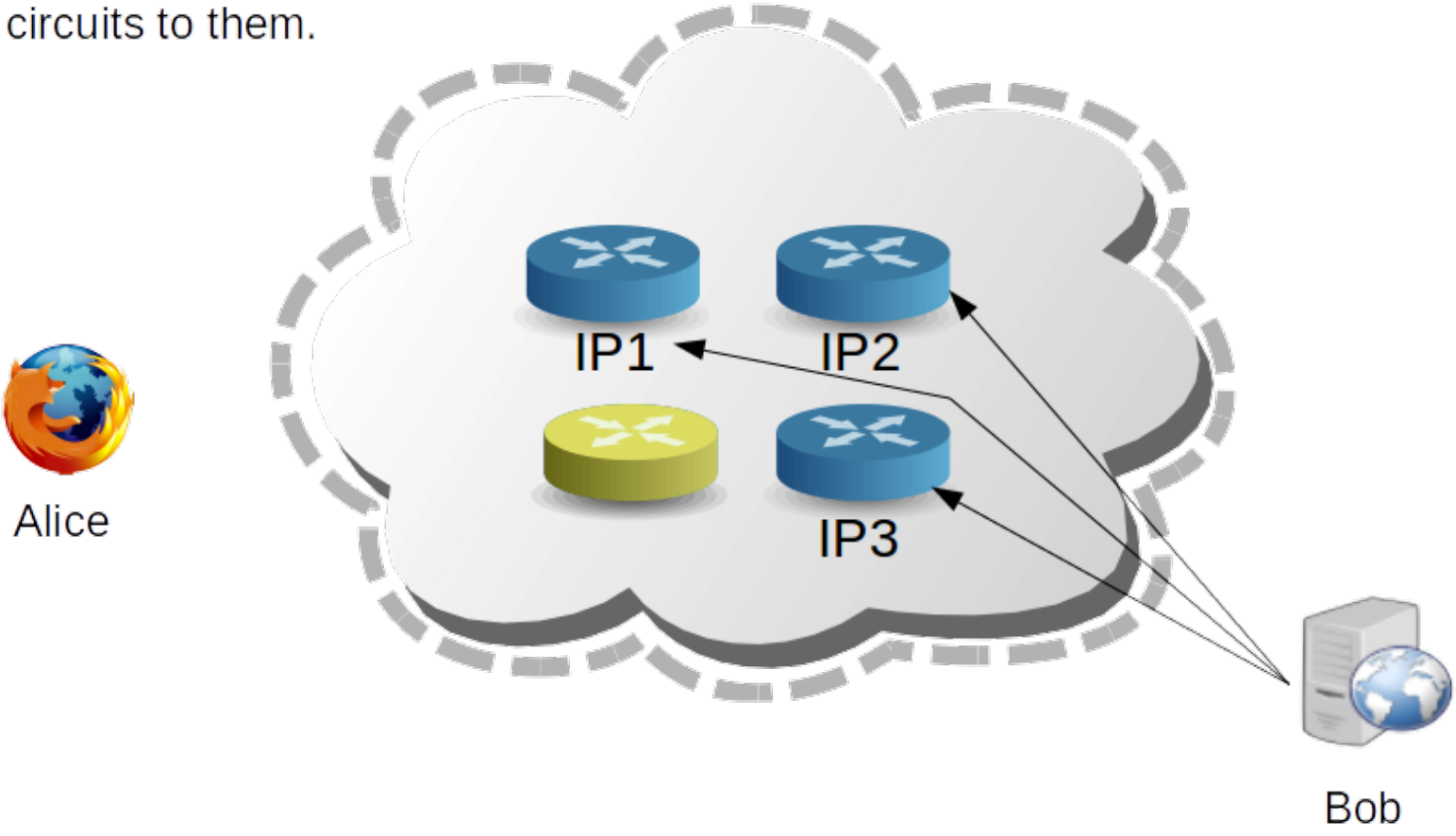
re the warez

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

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

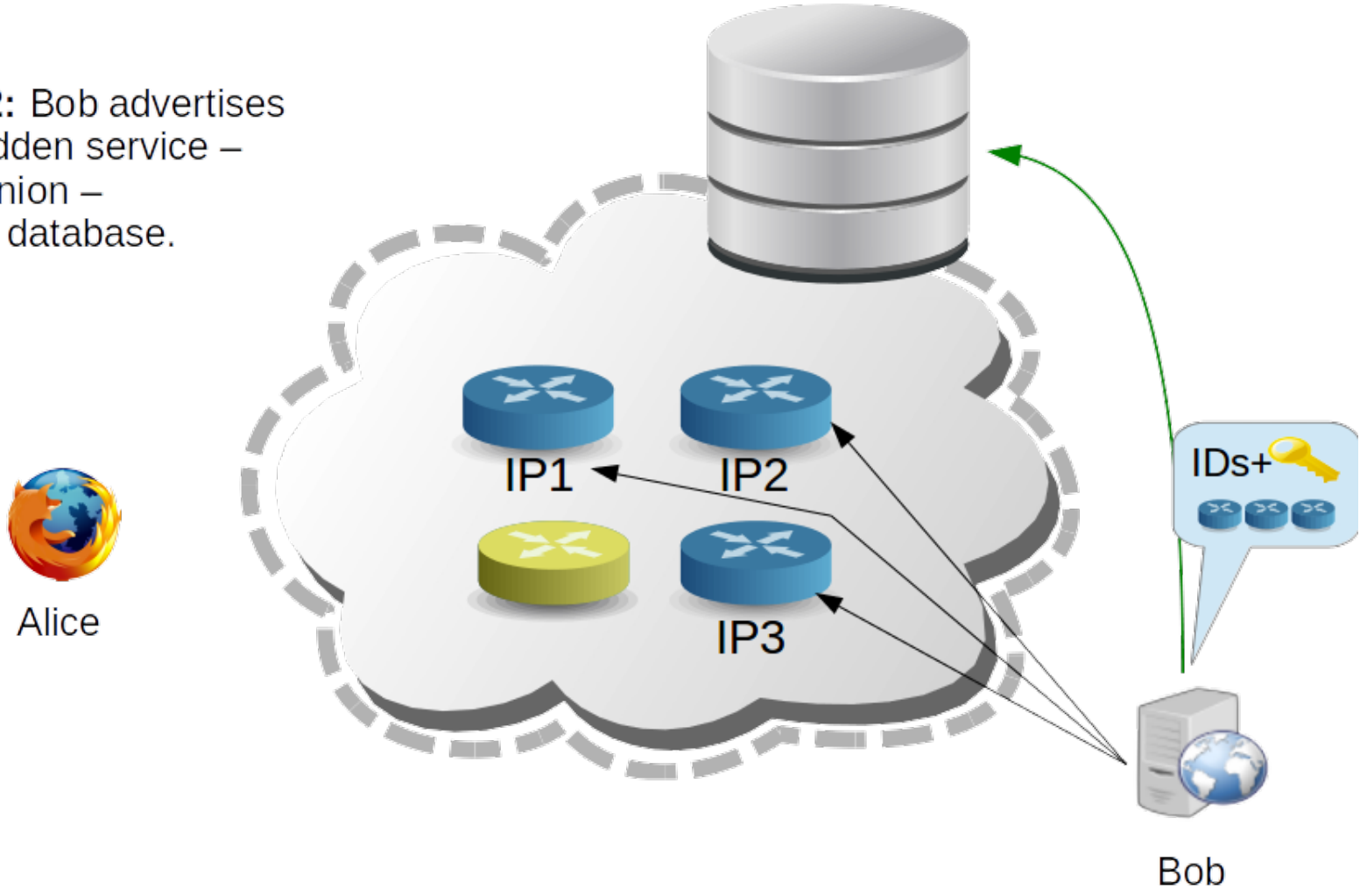
Tor Rendezvous Protocol

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

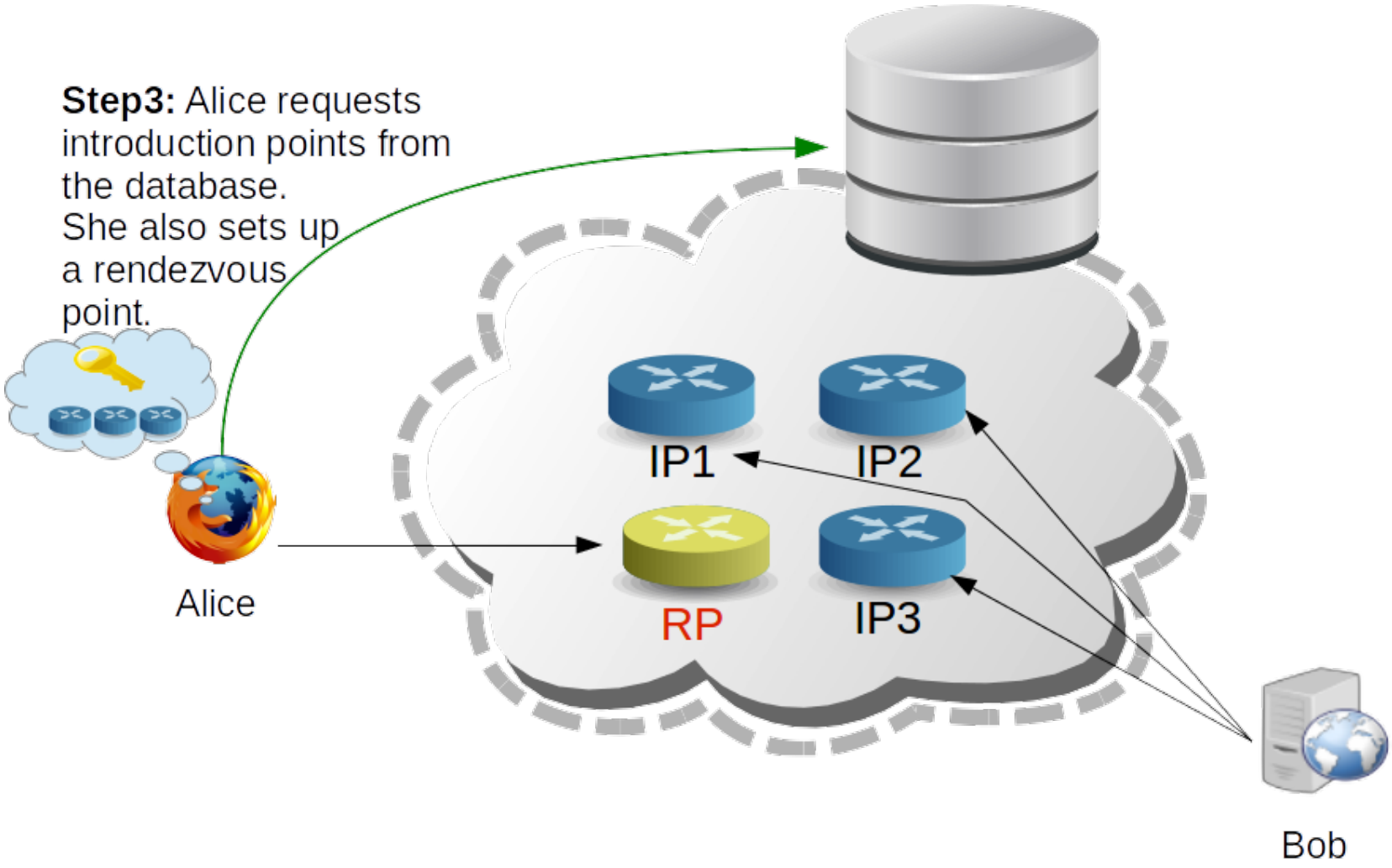


Tor Rendezvous Protocol

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

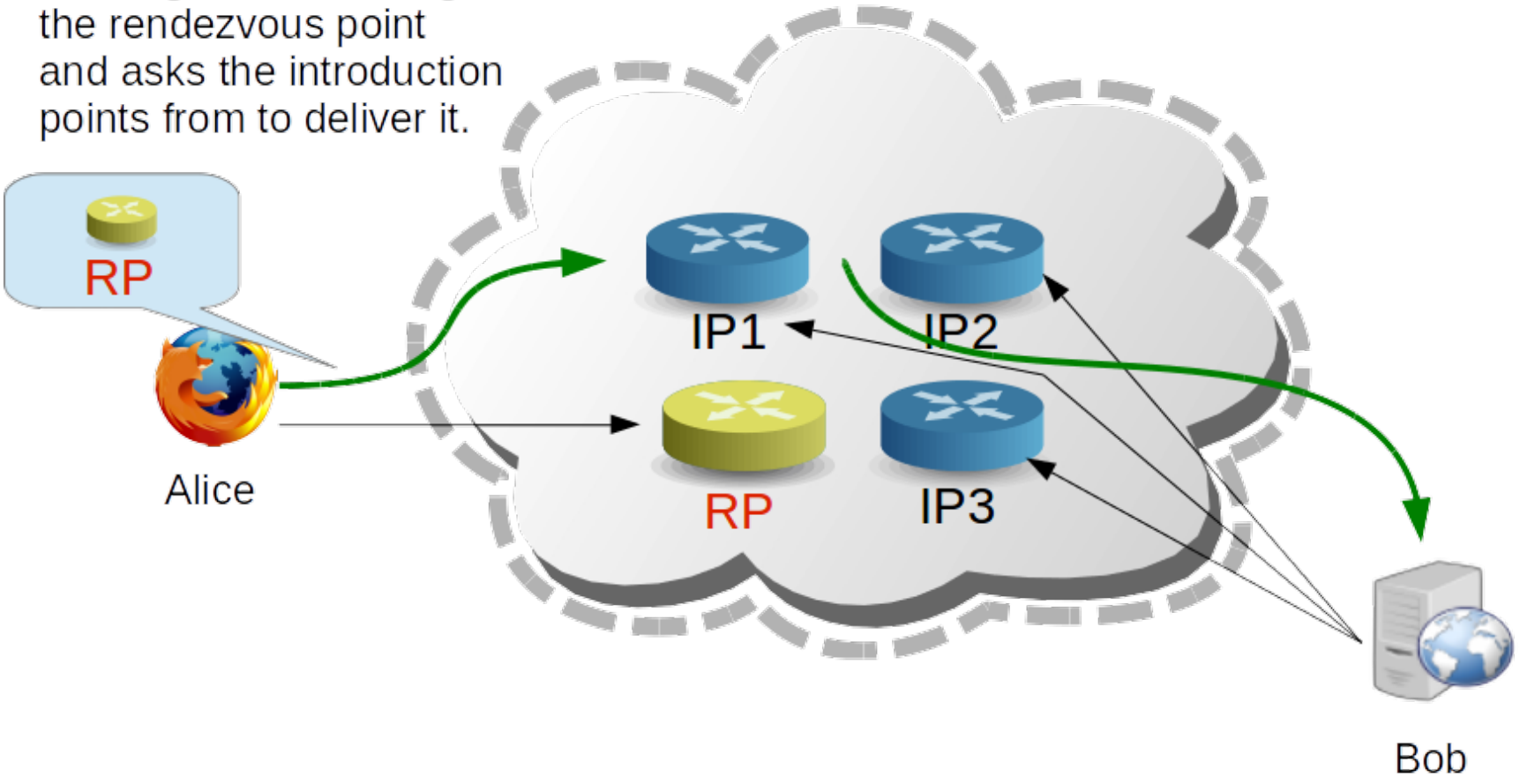


Tor Rendezvous Protocol



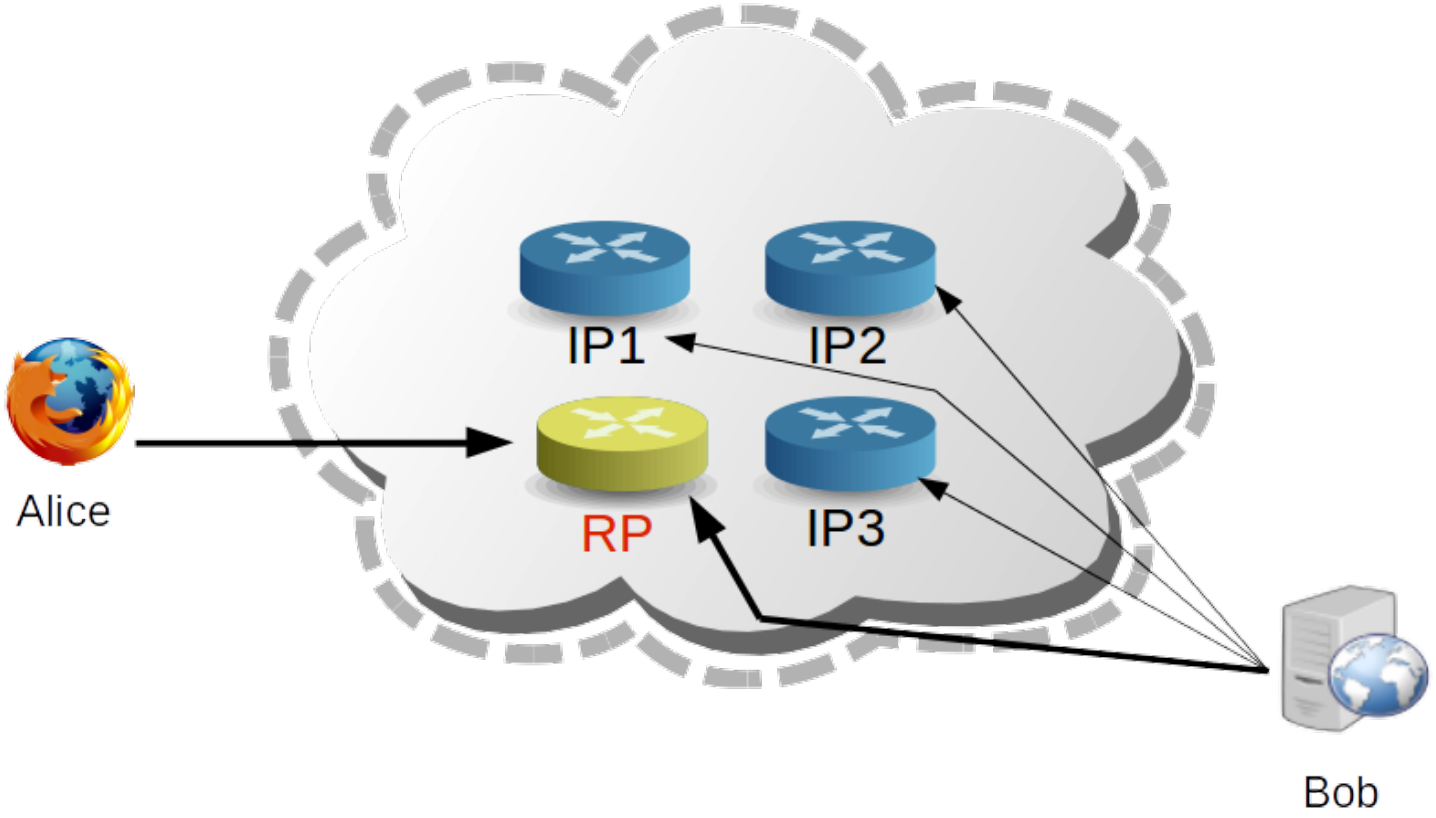
Tor Rendezvous Protocol

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

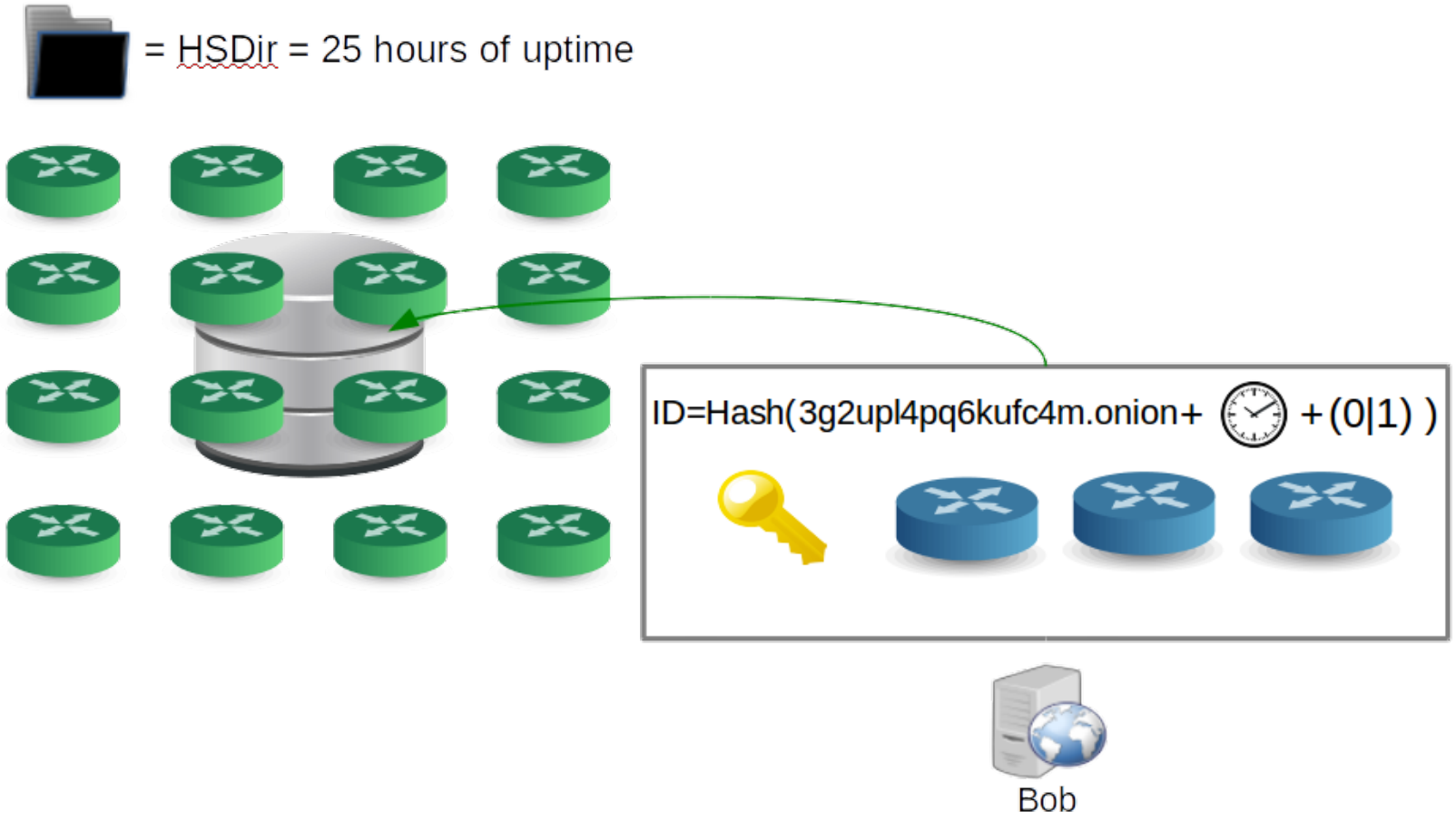


Tor Rendezvous Protocol

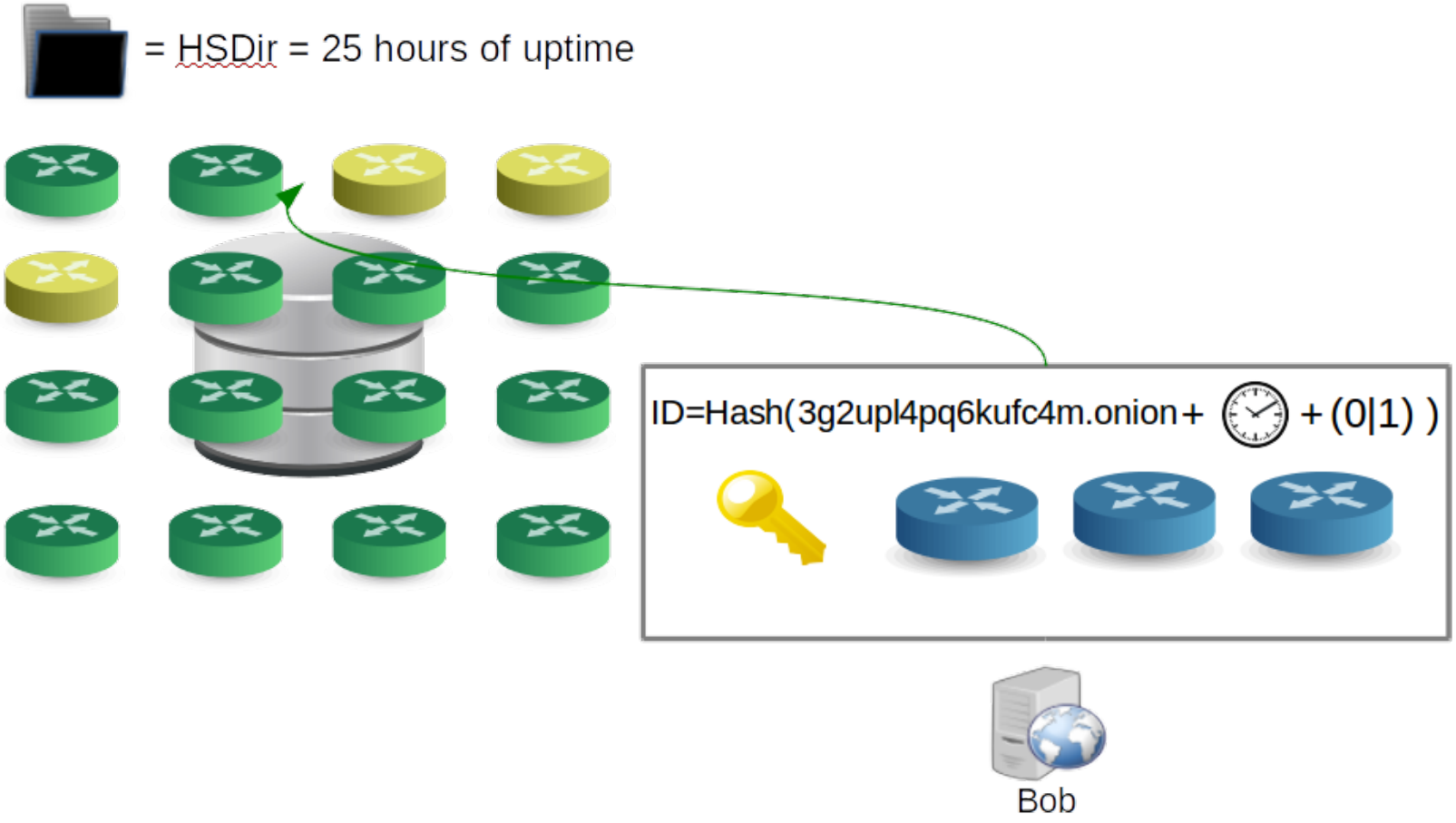
Step5: Alice and Bob Connect at the Rendezvous point



Responsible Hidden Service Directories



Responsible Hidden Service Directories

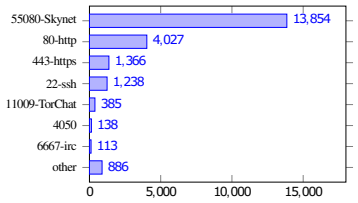


Shadowing

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

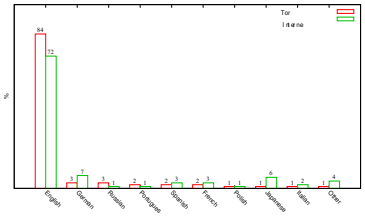
[1] Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization, IEEE Symposium on Security and Privacy

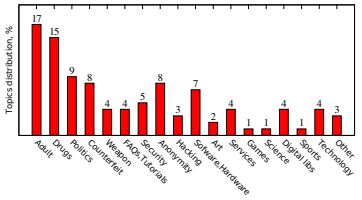
Statistics



HTTP classification

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



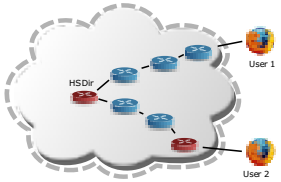


Mevade botnet

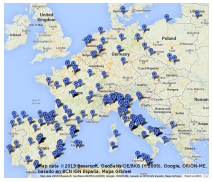
#	RQSTS	Addr	Desc	#	RQSTS	Addr	Desc
1	13714	uecbcfgfofuwkcrd.onion	Goldnet	22	899	qdzjxwujdtxrjkrz.onion	Skynet
2	11582	arloppepzch53w3i.onion	Goldnet	23	898	6tkpktox73usm5vq.onion	Skynet
3	11315	pomyeasfnmtn544p.onion	Goldnet	24	889	kk2wajy64oip2***.onion	Adult
4	7324	lqqciuwa5yzxewc3.onion	Goldnet	25	781	gpt2u5hhaqvmnwhr.onion	Skynet
5	7183	eqlbyxrpd2wdjeig.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	f2ylgv2jochpzm4c.onion	Skynet
8	4941	qxc7mc24mj7m4e2o.onion	< n/a>	29	585	kdq2y44aaas2a***.onion	Adult
9	3746	mwjjmmahc4cjjlqp.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	firelol5skg6e***.onion	Adult	62	172	5onwnspjvuk7cwvk.onion	BlckMrktReloaded
16	1481	niazgxzlrbpevgvq.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

- 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

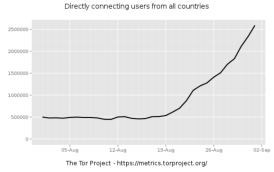
- Command and control connectivity via Tor .onion links
- Seems that the purpose of this malware network is to load additional malware onto the system and that the infected systems are for sale

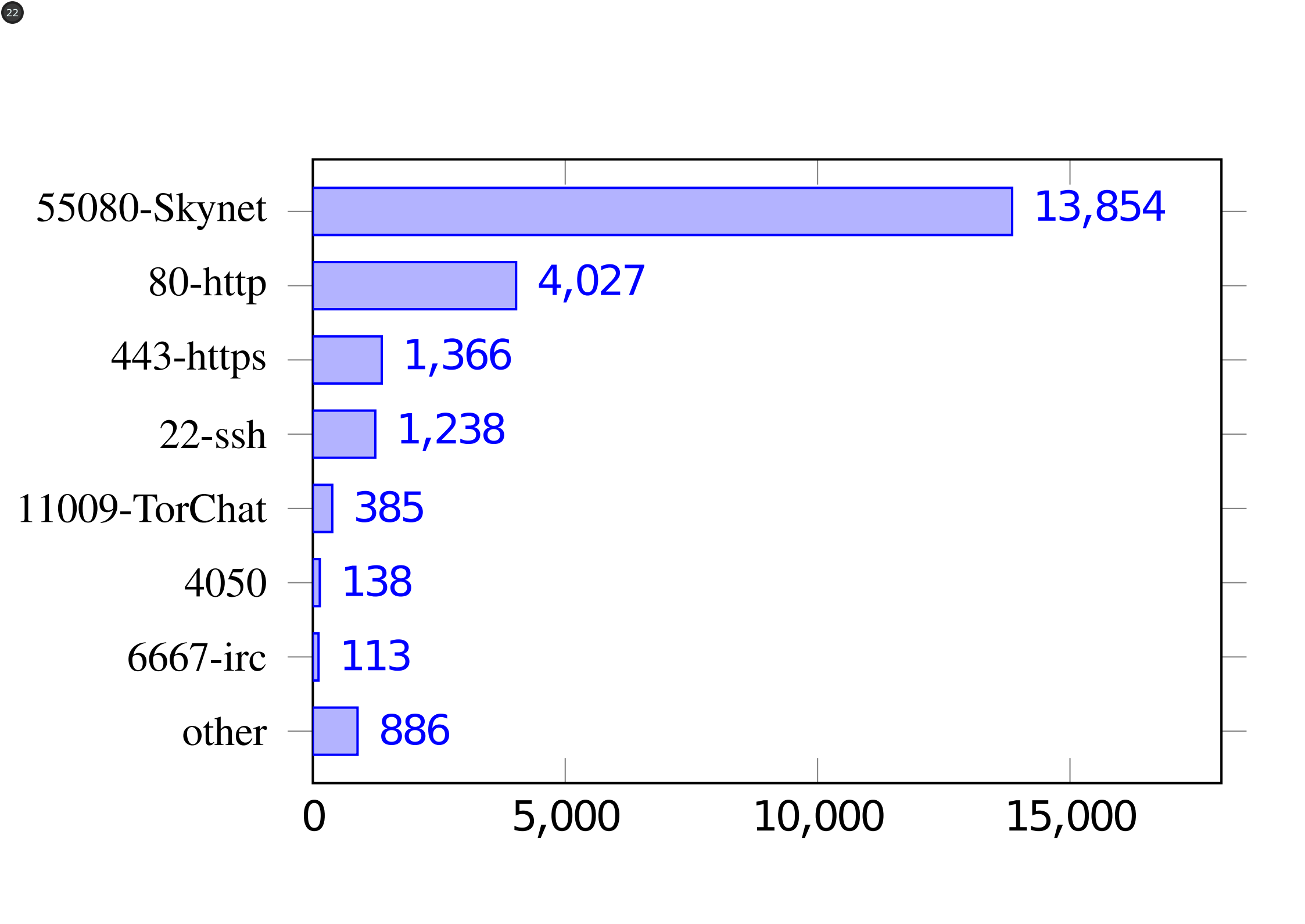
Tracking detection

- One entiity 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

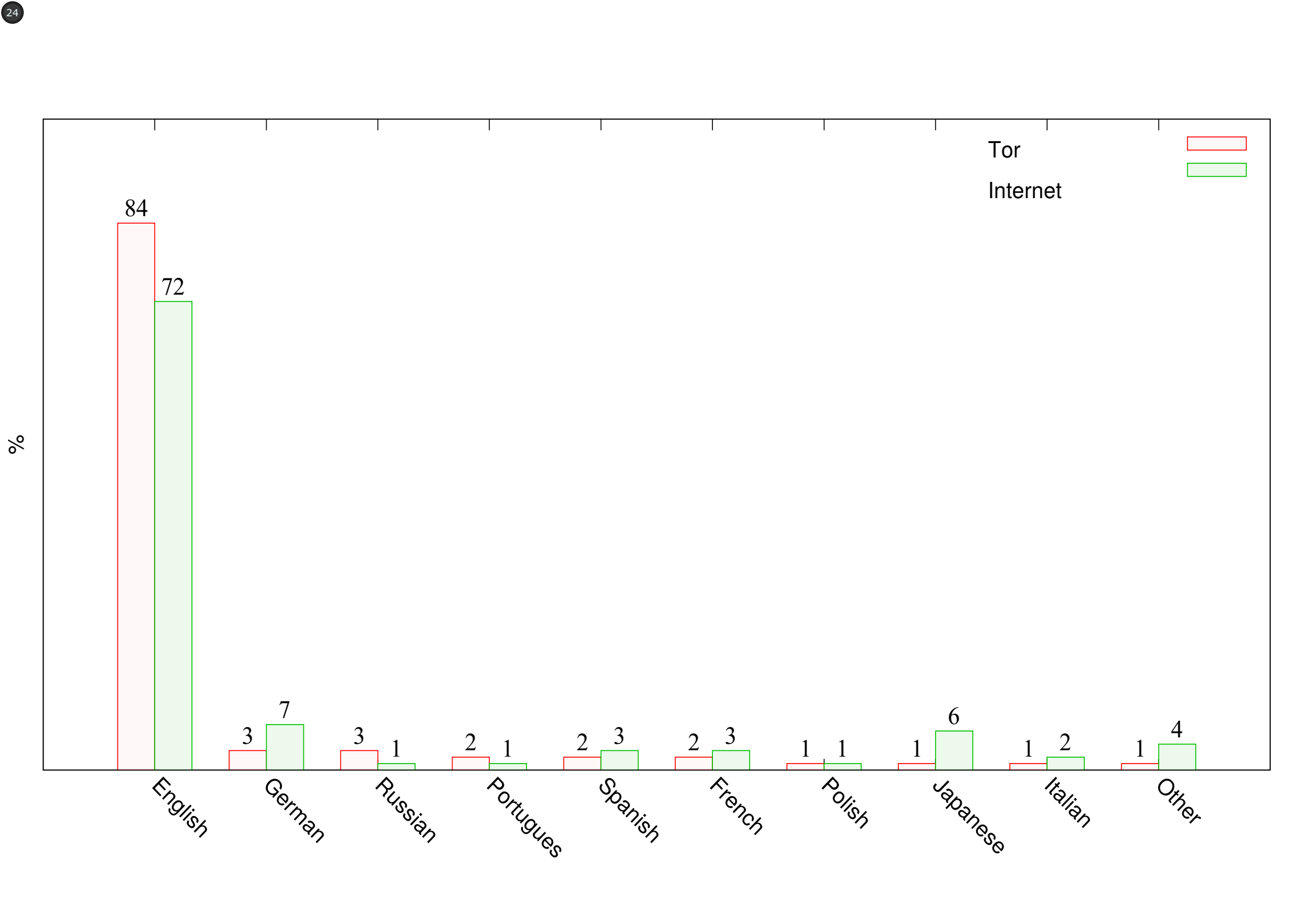
Mevade botnet

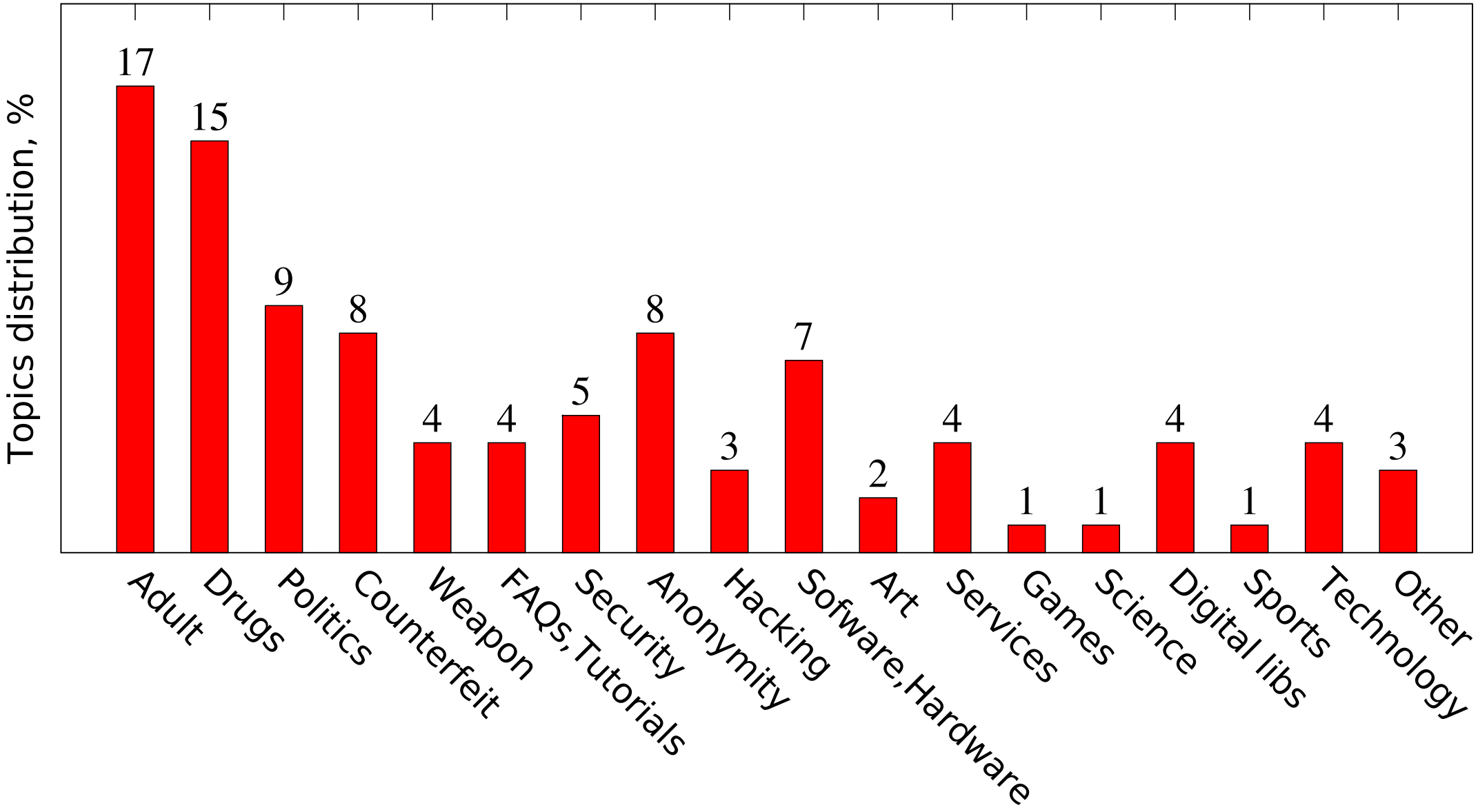



55080-Skynet
13,854
80-http
4,027
443-https
1,366
22-ssh
1,238
11009-TorChat
385
4050
138
6667-irc
113
other
886
0
5,000
10,000
15,000

HTTP classification

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

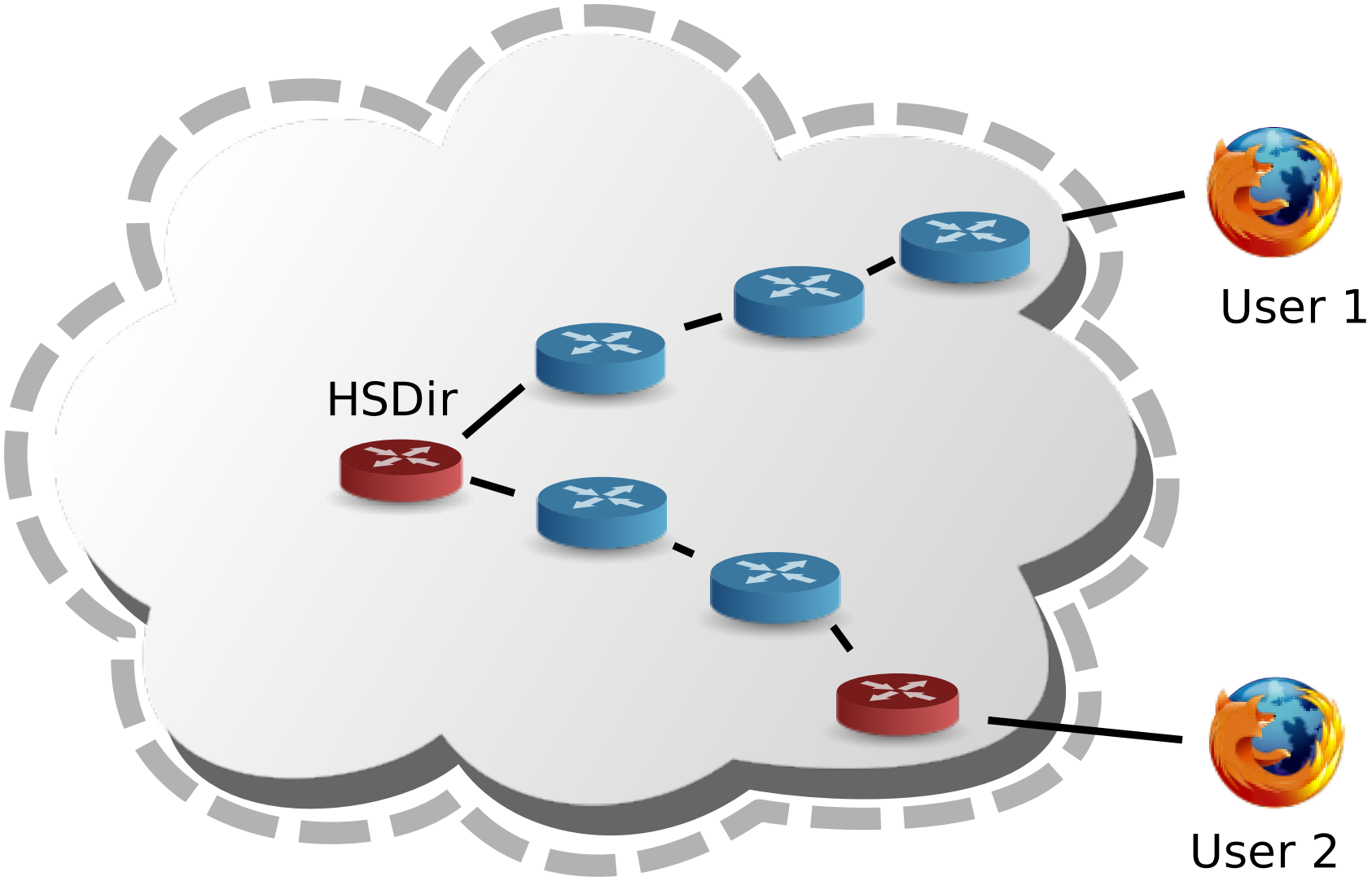

Tor
Internet
%
84
72
3
7
3
1
2
1
2
3
2
3
1
1
1
6
1
2
1
4
English
German
Russian
Portugues
Spanish
French
Polish
Japanese
Italian
Other


Topics distribution, %
17
15
9
8
4
4
5
8
3
7
2
4
1
1
4
1
4
3
Adult
Drugs
Politics
Counterfeit
Weapon
FAQs, Tutorials
Security
Anonymity
Hacking
Sofware, Hardware
Art
Services
Games
Science
Digital libs
Sports
Technology
Other

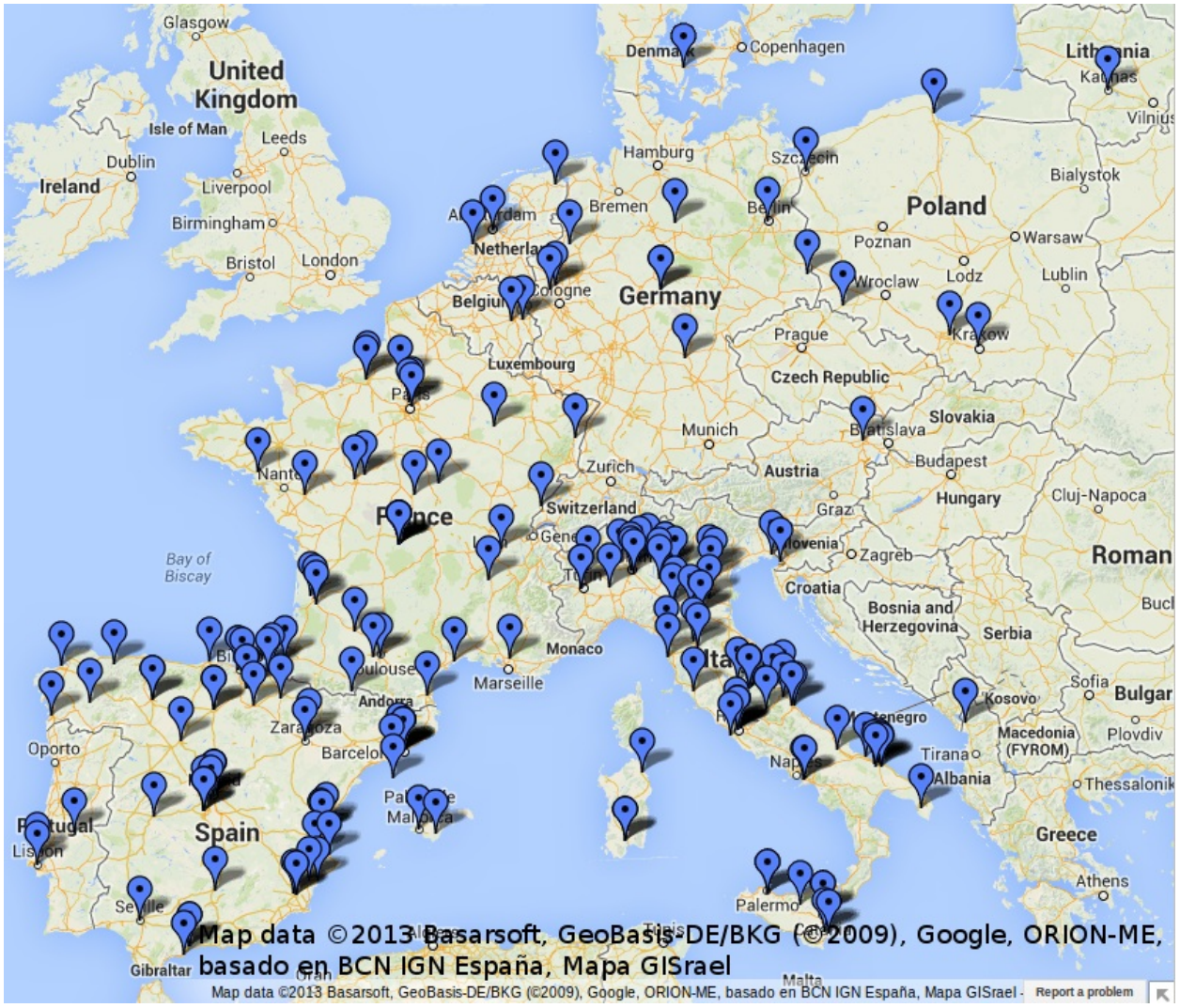
#	RQSTS	Addr	Desc	#	RQSTS	Addr	Desc
1	13714	uecbcfgfofuwkcrd.onion	Goldnet	22	899	qdzjxwujdtxrjkrz.onion	Skynet
2	11582	arloppepzch53w3i.onion	Goldnet	23	898	6tkpktox73usm5vq.onion	Skynet
3	11315	pomyeasfnmtn544p.onion	Goldnet	24	889	kk2wajy64oip2***.onion	Adult
4	7324	lqqciuwa5yzxewc3.onion	Goldnet	25	781	gpt2u5hhaqvmnwhr.onion	Skynet
5	7183	eqlbyxrpd2wdjeig.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	f2ylgv2jochpzm4c.onion	Skynet
8	4941	qxc7mc24mj7m4e2o.onion	<n/a>	29	585	kdq2y44aaas2a***.onion	Adult
9	3746	mwjjmmahc4cjjlqp.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	firelol5skg6e***.onion	Adult	62	172	5onwnspjvuk7cwvk.onion	BlckMrktReloaded
16	1481	niazgxzlrbpevgvq.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



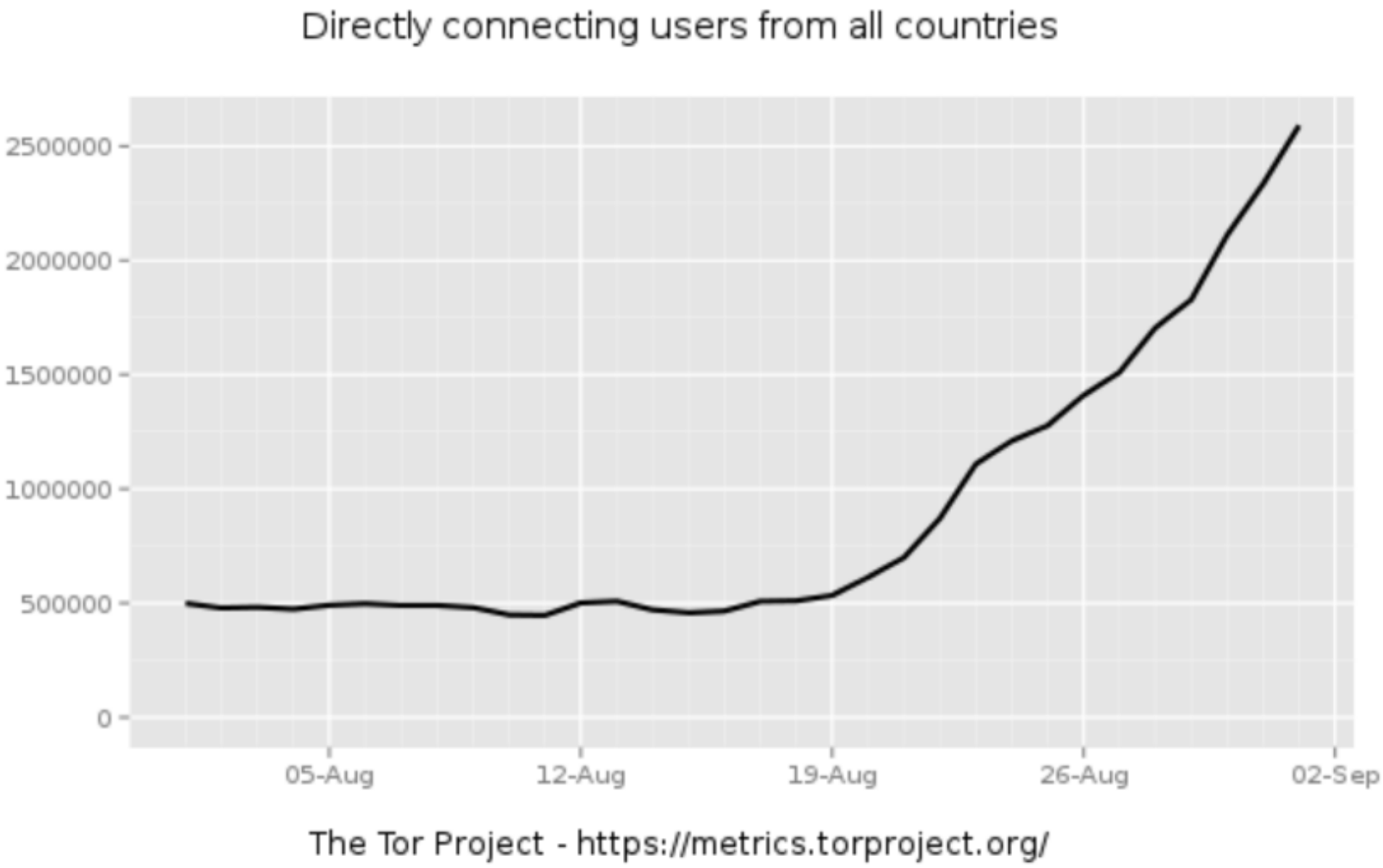
Mevade botnet

#	RQSTS	Addr	Desc	
1	13714	uecbcfgfofuwkcrd.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	mwjjmmahc4cjjlqp.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



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 entiity 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