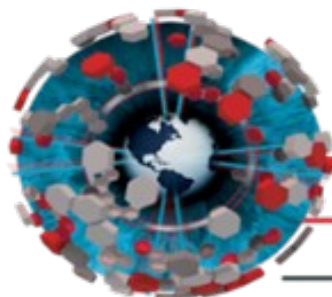


SPLITTER



ABOUT ME



AGENDA

- Motivation.
- The basic about TOR.
- The anatomy of TOR related attacks
- Common Weakness of De-Anonymization Techniques.
- The Exploit Challenge.
- The SPLITTER
- The SPLITTER NETWORK
- Proof of Concept.
- Questions
- Bonus

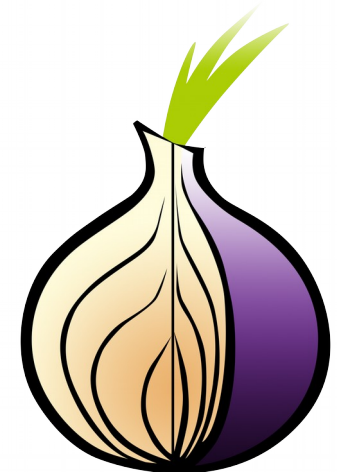
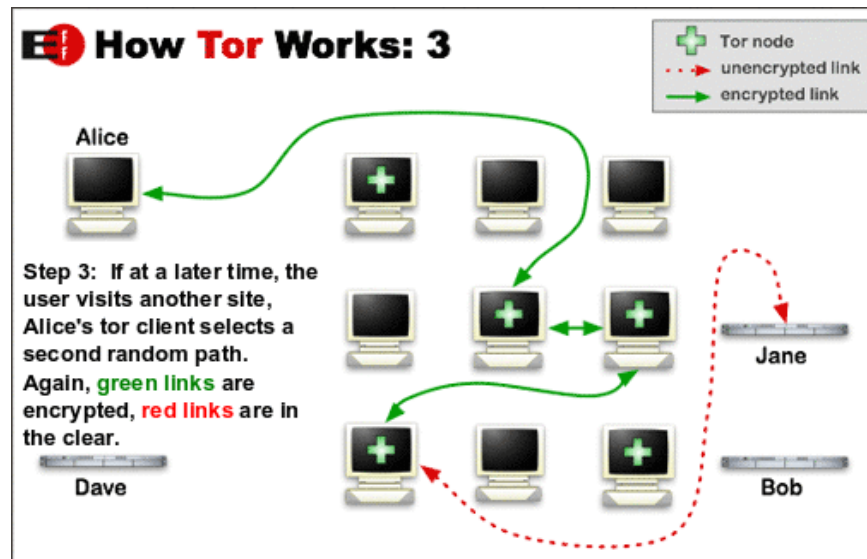
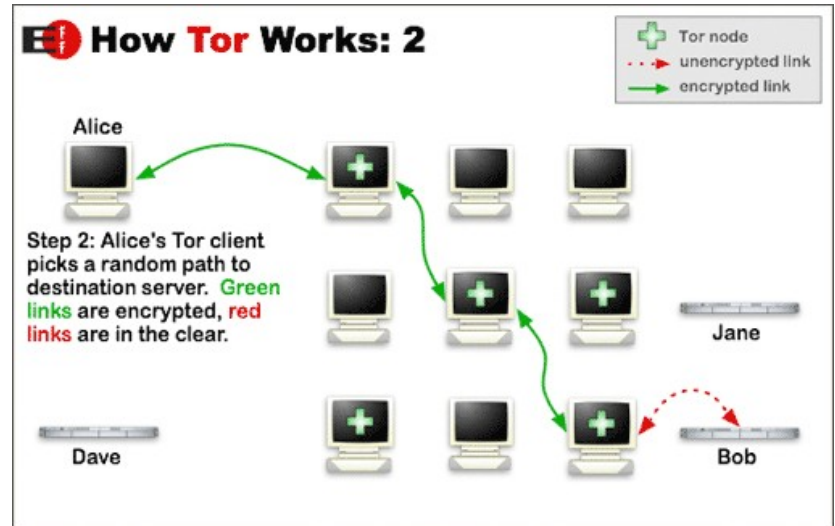
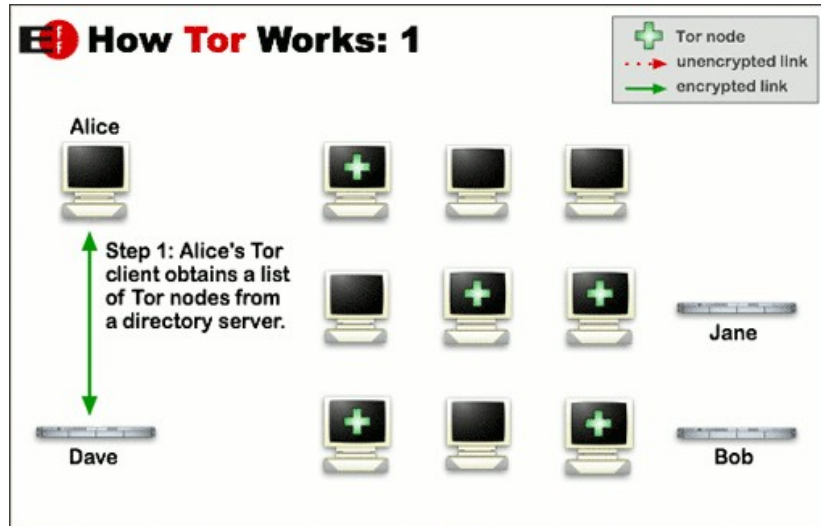


Motivation

- Privacy is just a dream.
- TOR Network is slow and unstable!
- Many de-anonymization techniques impacting the trust of users on TOR network.
- The challenge to difficult the correlation and traffic analysis attacks.
- The challenge to use TOR network for everything without suffer with speed or stability.



The basic about TOR



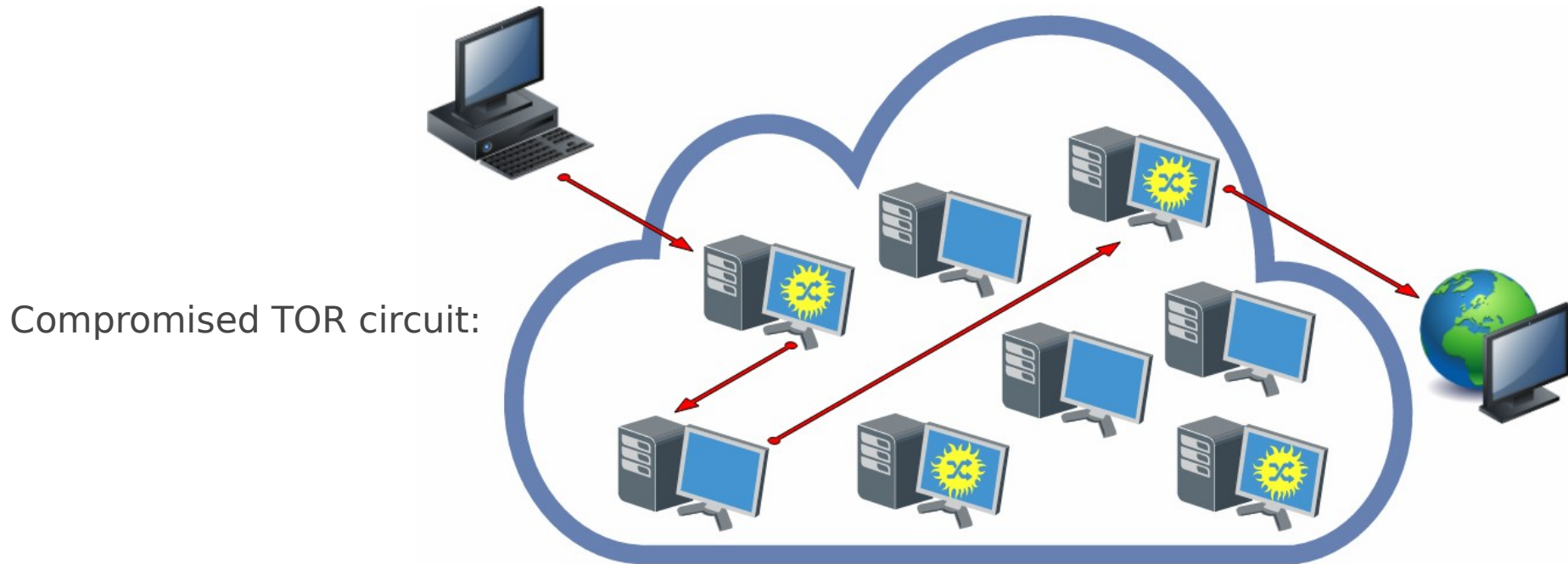
The anatomy of attacks

About TOR nodes:

ENTRY NODE: If the adversary controls the TOR ENTRY NODE it means that adversary already knows the IP address from the victim.

MIDDLE NODE: Breaks the natural correlation between the TOR user and the destination.

EXIT NODE: If the adversary controls the EXIT NODE he knows the final destination of packets.



The anatomy of attacks

Paper:

“Low-Resource Routing Attacks Against Anonymous Systems” - Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker
[Online] Available:

<http://www.cs.colorado.edu/departments/publications/reports/docs/CU-CS-1025-07.pdf>

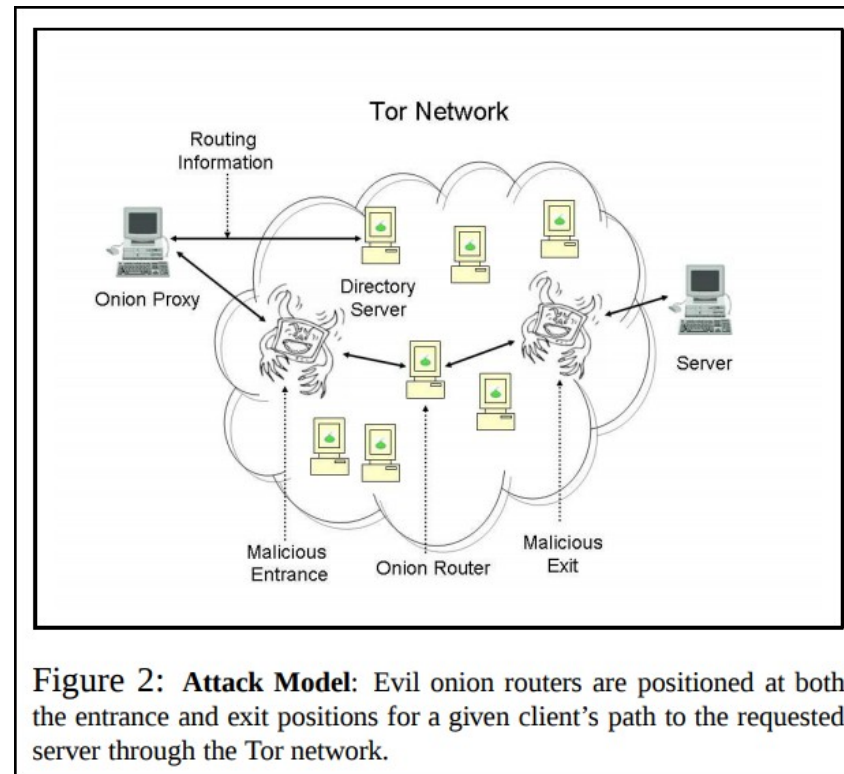


Figure 2: **Attack Model:** Evil onion routers are positioned at both the entrance and exit positions for a given client's path to the requested server through the Tor network.



Paper: “Low-Resource Routing Attacks Against Anonymous Systems”

Using the data logged by malicious routers, our path linking algorithm was able to link a relatively high percentage of paths through Tor to the initiating client. In the 40 onion router deployment, we conducted experiments by adding two (2/42) and four (4/44) malicious nodes. The malicious routers composed roughly 5% and 9% of the network. In the 2/42 experiment, the malicious nodes were able to compromise approximately 9% of the 4,774 paths established through the network. We then performed the 4/44 experiment, and were able to correlate ap-

proximately 34% of the 10,199 paths through the network. Thus, the attack is able to compromise the anonymity of over one-third of the circuit-building requests transported through the experimental network. These experiments are repeated for a network of 60 onion routers. With

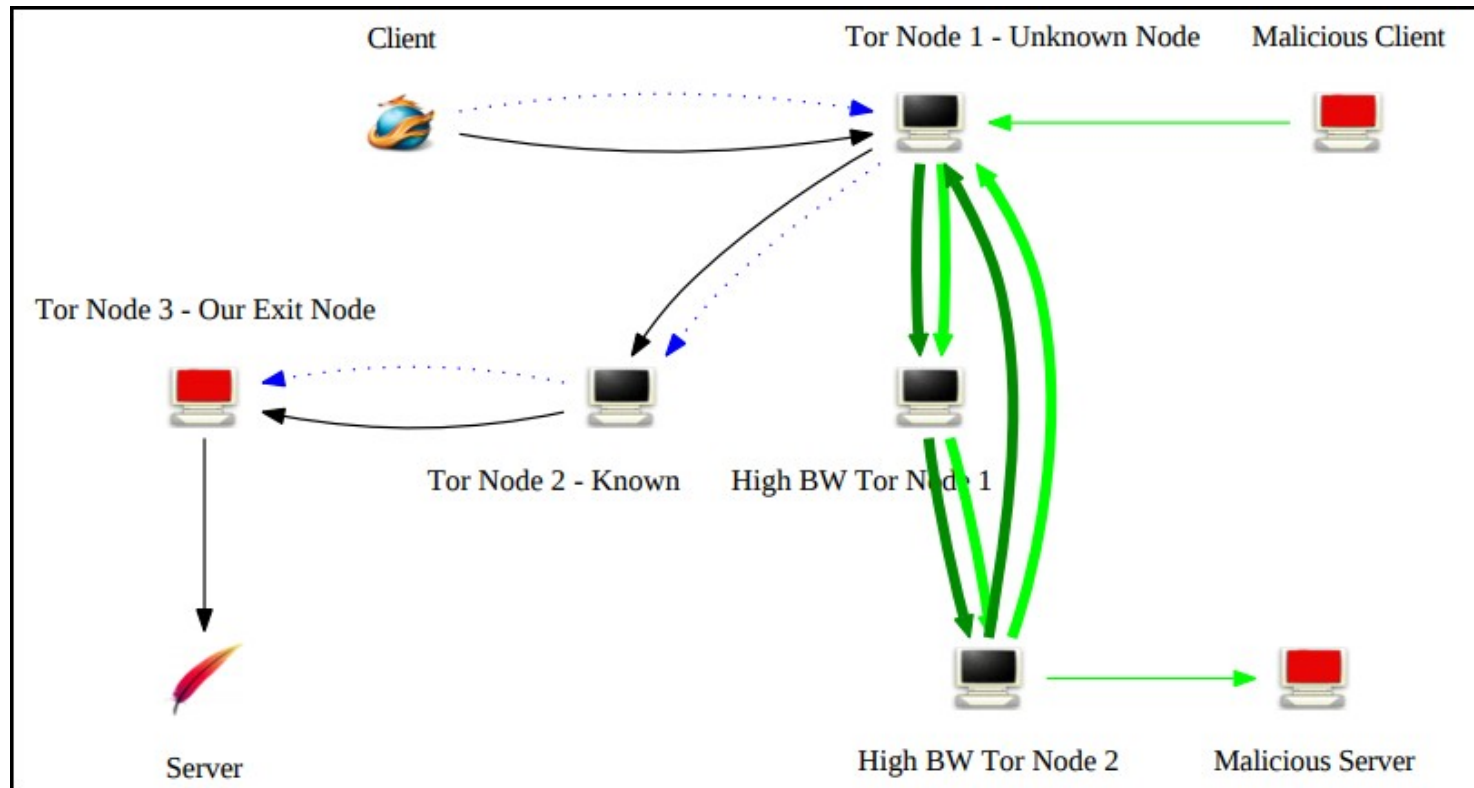


The anatomy of attacks

Paper:

“A Practical Congestion Attack on Tor Using Long Paths”. - Nathan S. Evans, Roger Dingledine and Christian Grothoff

[Online]Available: https://www.usenix.org/legacy/event/sec09/tech/full_papers/evans.pdf



The anatomy of attacks

Paper:

“How Much Anonymity does Network Latency Leak?”. - Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-Tin

[Online]Available: <https://www-users.cs.umn.edu/~hoppernj/tissec-latency-leak.pdf>

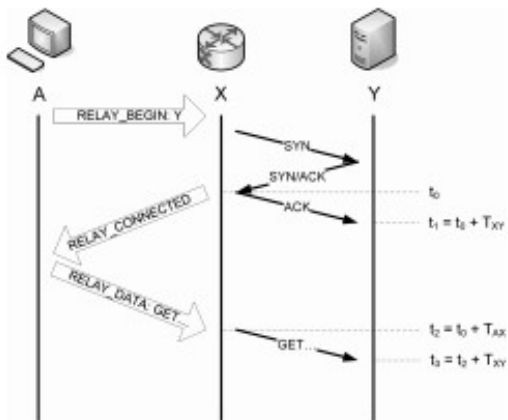


Fig. 1. Measuring Tor circuit time without application-layer ACKs: The estimate for T_{AX} is $t_3 - t_1$. We abuse notation and write T_{XY} for the one-way delay from $X - Y$.

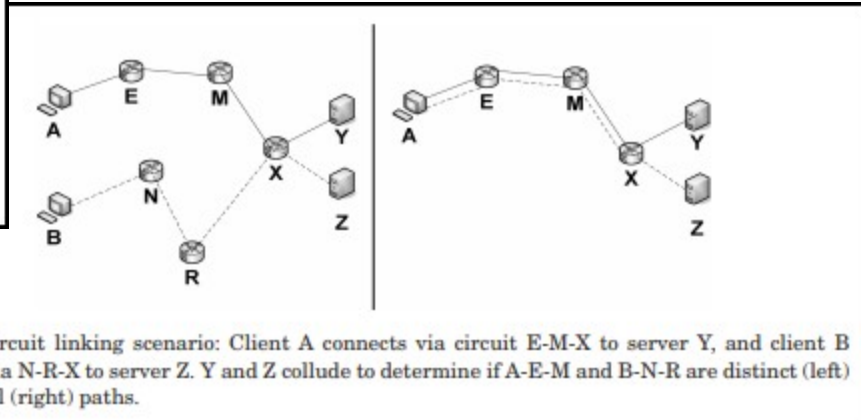


Fig. 3. Circuit linking scenario: Client A connects via circuit E-M-X to server Y, and client B connects via N-R-X to server Z. Y and Z collude to determine if A-E-M and B-N-R are distinct (left) or identical (right) paths.



The anatomy of attacks

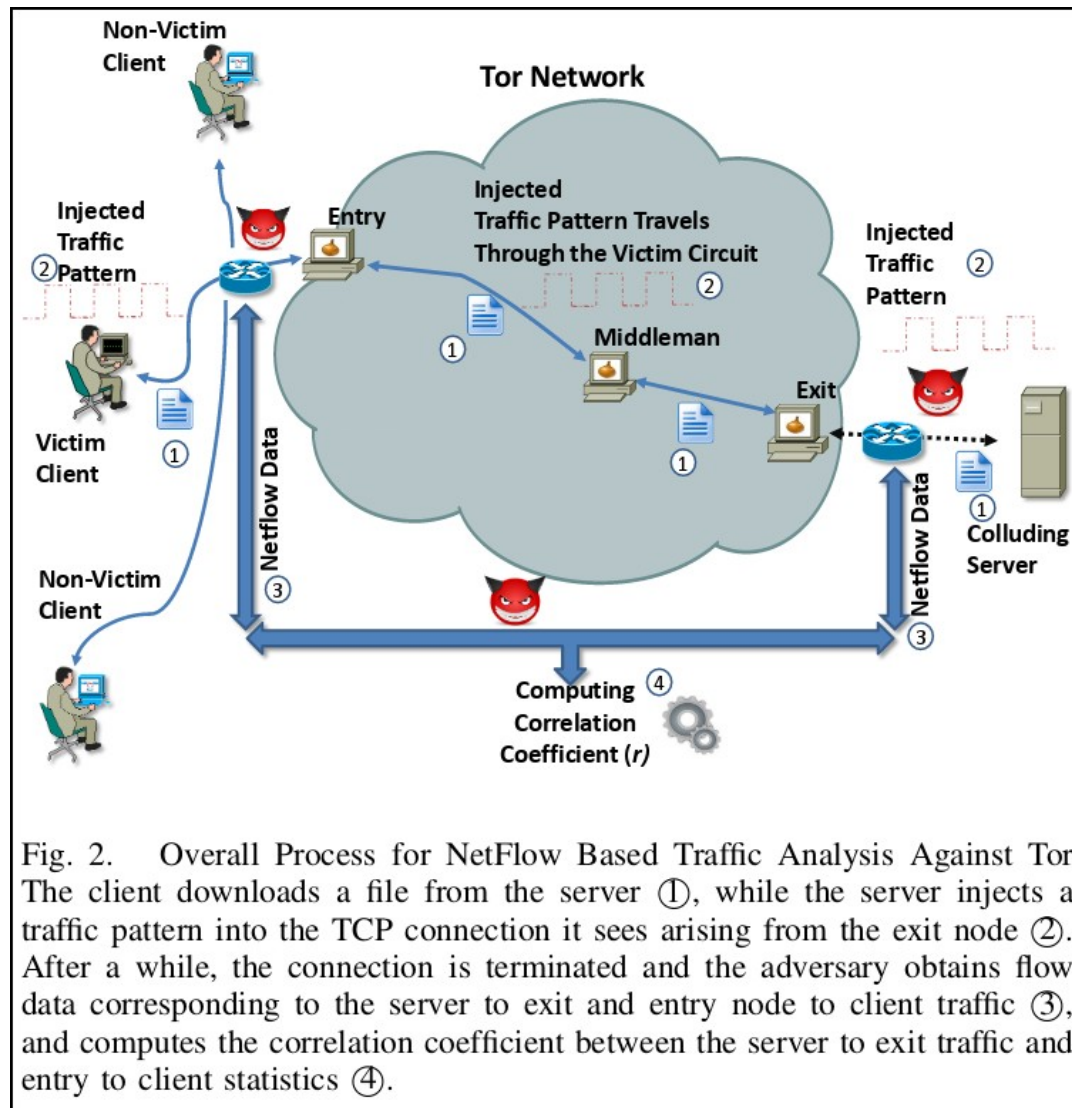
Paper:

“On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records”, - Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis and Angelos D. Keromytis -- [Online]Available: <https://www-users.cs.umn.edu/~hoppernj/tissec-latency-leak.pdf>

We do not focus on finding appropriate vantage points and monitoring hosts, but rather on the logical “next-step” once such routers have been determined. We focus on studying how successful such an attack is in practice to identify the source of anonymous traffic. We rely on correlation of traffic statistics to identify the source of anonymous traffic amidst various flows corresponding to clients using our entry node. Our research, demonstrates such an attack first on an in-lab set-up involving a private Tor network and client which we controlled. In such an environment, free from external network congestion and various artefacts due to link characteristics and path asymmetries, we were able to determine the actual source of anonymous traffic with 100% accuracy. In experiments that involved data from public Tor relays, using both open source Netflow emulation packages and our institutional Cisco router that monitored traffic using Netflow framework, we were able to correctly identify the source of anonymous traffic in about 81.4% of our experiments, with about 6.4% false positives.



Paper: "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records"



Common Weakness from De-anonymization Techniques

The majority of De-anonymization Techniques rely that victim will use:

- The same TOR circuit to transfer the injected pattern.
- The same global network path from the compromised web server or compromised EXIT NODE to the client.
- The same TCP STREAM or the same global path to transfer a cert amount of data necessary to transmit a specific pattern during a specific time frame.
- The victim will exchange a minimum amount of data with the server.



Common Weakness from De-anonymization Techniques

The majority of De-anonymization Techniques could fail if the anonymous network user can affect the adversary ability of:

- Collect the minimum amount of data to analyze and correlate.
- Create time related disturbs to difficulty the time correlation of intercepted packets.
- Identify the injected pattern among the intercepted packets.



The “exploit” challenge

The TOR network user should have the ability to enforce for every single TCP stream:

- A different TOR circuit from the previous TCP stream. It means, ensures that the ENTRY NODE or the EXIT NODE will be different from the previous TCP stream.
- A different global network path for packets traveling from his machine, crossing the TOR network and arriving in the final destination server.
- Control or disturb the time which TOR could generate the same compromised TOR CIRCUIT again.
- Disturb the TCP stream lifetime, interrupting the transmission if the stream is being used for more than “X” minutes.



SPLITTER - DcLabs Security Team

Twitter: @Gr1nchDC Mail: rener.silva@protonmail.com

SPLITTER source code available in:

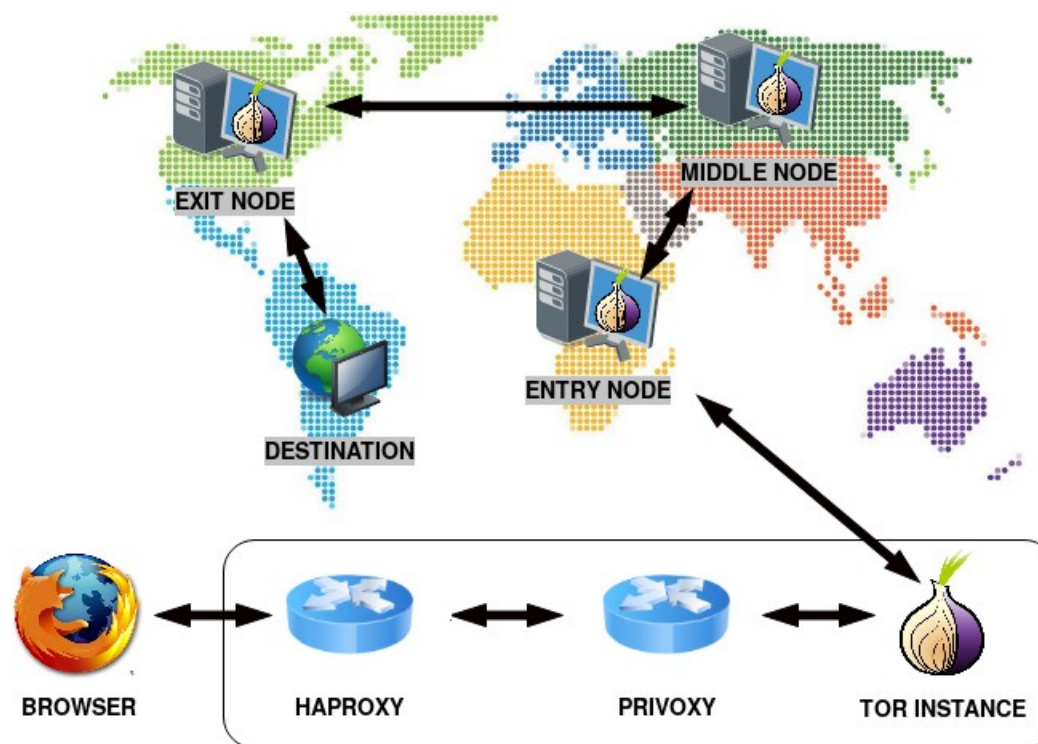
<https://github.com/renergr1nch/splitter>

SPLITTER Docker Image available in:

#docker pull gr1nchdc/splitter:v.0.0.1



The SPLITTER solution: TCP Packet Path



```
Aug 14 21:05:32.000 [notice] New control connection opened from 127.0.0.1.  
Aug 14 21:05:32.000 [notice] Rate limiting NEWNYM request: delaying by 10 second(s)  
Aug 14 21:05:34.000 [notice] New control connection opened from 127.0.0.1.  
Aug 14 21:05:34.000 [notice] Rate limiting NEWNYM request: delaying by 8 second(s)  
Aug 14 21:05:35.000 [notice] New control connection opened from 127.0.0.1.  
Aug 14 21:05:35.000 [notice] Rate limiting NEWNYM request: delaying by 7 second(s)  
Aug 14 21:05:35.000 [notice] New control connection opened from 127.0.0.1.  
Aug 14 21:05:36.000 [notice] Rate limiting NEWNYM request: delaying by 6 second(s)
```



The SPLITTER solution

Enforcing countries in TOR config file:

```
splitter@d578a753305d:/tmp/splitter/tor1$ cat tor_1.cfg | grep "{"  
EntryNodes {DE}  
ExitNodes {AU},{AT},{BE},{BG},{CA},{CZ},{DK},{FI},{FR},{HU},{IS},{LV},{LT},{LU},{MD},{NL},{NO},{PA},{PL},{RO},{RU},{SC},{SG},{SK},{ES},{SE},{CH},{TR},{UA},{GB},{US}  
ExcludeNodes {ZA},{KN},{JP},{IT},{IE},{ID},{HR},{CR},{AL},{MY},{HK},{EE},{CL},{NZ},{TH},{IN},{AR},{KR},{BR},{VN},{IL},{SI},{GR},{DZ},{AM},{AZ},{BD},{BY},{MO},{CO},{CI},{CY},{EC},{EG},{SV},{ET},{GA},{GT},{HN},{IR},{KZ},{KE},{KW},{KG},{LB},{MT},{MQ},{MR},{MX},{MN},{MA},{MZ},{NG},{PK},{PH},{QA},{SA},{SN},{RS},{TN},{UY},{VE},{YE},{DO},{LR},{MA},{NG},{PK},{PY},{QA},{SA},{UY},{SN},{VE}
```

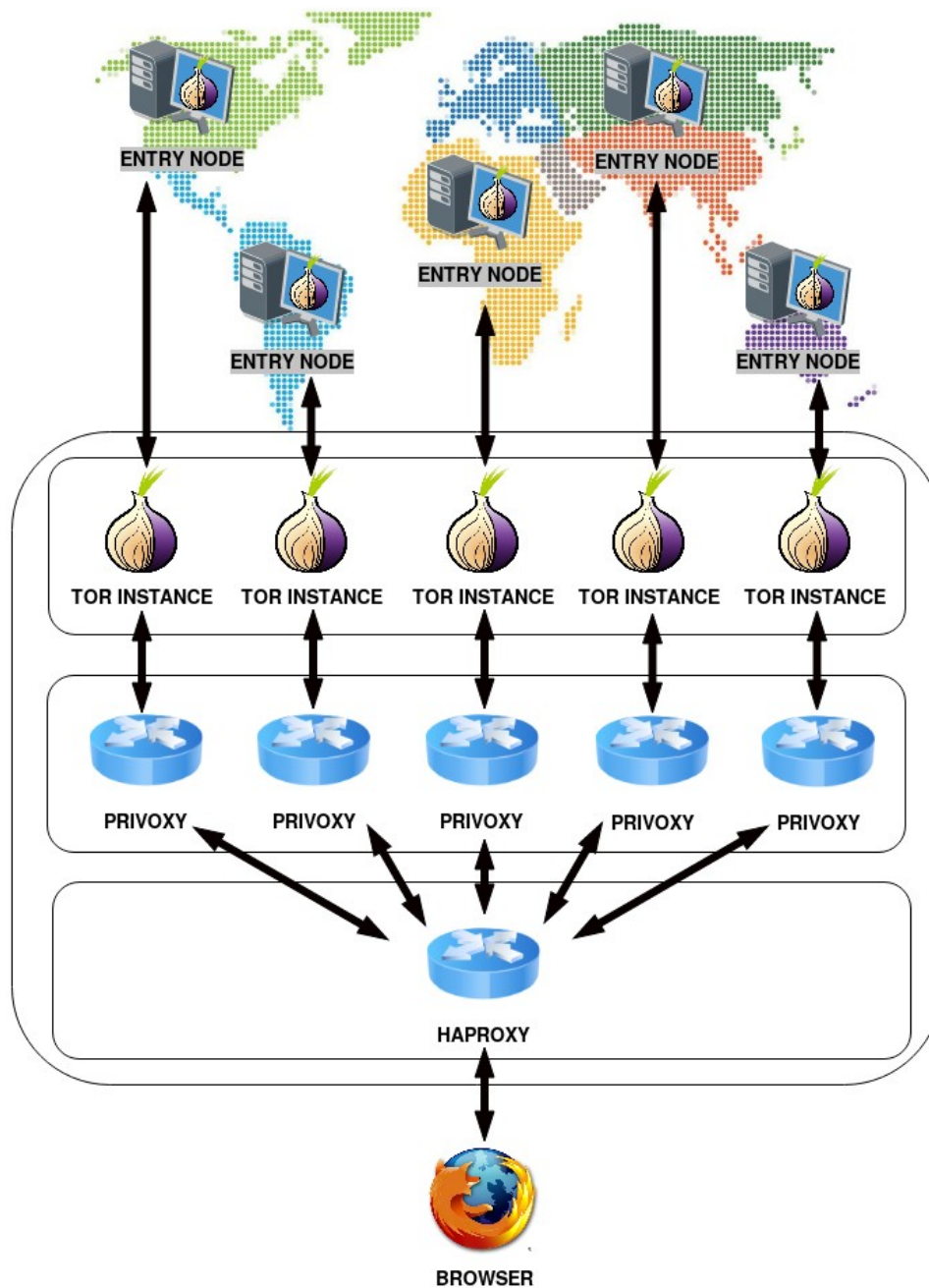
Only Germany (DE) can be used as ENTRY NODE.

Germany (DE) can't be used as EXIT NODE.

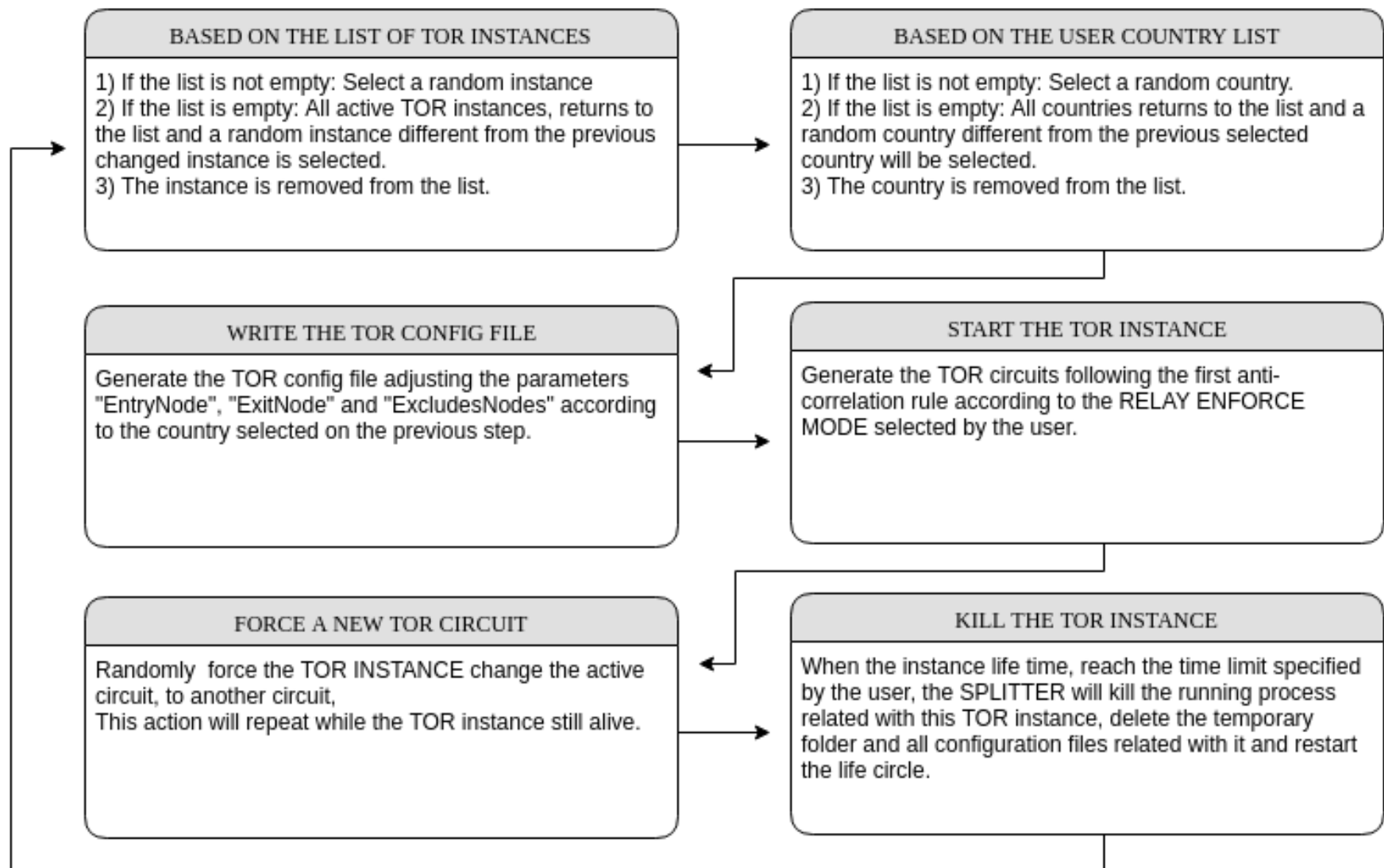
Germany (DE) is not included as a option.

List of countries that can't be used.





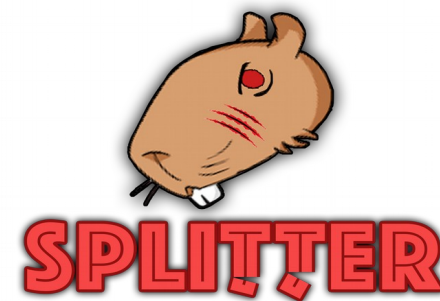
SPLITTER TOR instance life circle overview:



The SPLITTER solution

HAPROXY config file:

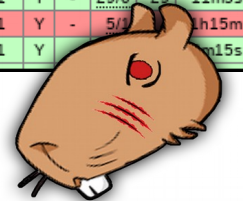
```
##Health Check request header spoofing the TOR Browser header##
balance roundrobin
option httpchk GET https://[REDACTED]/ HTTP/1.1\r\nHost:\ [REDACTED]\r\nUser-Agent:\ Mozilla/5.0\
(Windows\ NT\ 6.1;\ rv:52.0)\ Gecko/20100101\ Firefox/52.0\r\nAccept:\ text/html,application/xhtml+xml,applica
tion/xml;q=0.9,*/*;q=0.8\r\nAccept-Language:\ en-US,en;q=0.5\r\nAccept-Encoding:\ gzip,\ deflate\r\nConnection
:\ keep-alive\r\nUpgrade-Insecure-Requests:\ 1
##
default-server error-limit 1 on-error mark-down
server TOR_INSTANCE_15 127.0.0.1:7034 check inter 12s fall 1 rise 1 observe layer7 minconn 1 maxconn 20
server TOR_INSTANCE_2 127.0.0.1:7021 check inter 12s fall 1 rise 1 observe layer7 minconn 1 maxconn 20
server TOR_INSTANCE_13 127.0.0.1:7032 check inter 12s fall 1 rise 1 observe layer7 minconn 1 maxconn 20
server TOR_INSTANCE_3 127.0.0.1:7022 check inter 12s fall 1 rise 1 observe layer7 minconn 1 maxconn 20
server TOR_INSTANCE_12 127.0.0.1:7031 check inter 12s fall 1 rise 1 observe layer7 minconn 1 maxconn 20
server TOR_INSTANCE_17 127.0.0.1:7036 check inter 12s fall 1 rise 1 observe layer7 minconn 1 maxconn 20
```



The SPLITTER solution

HAPROXY status screen:

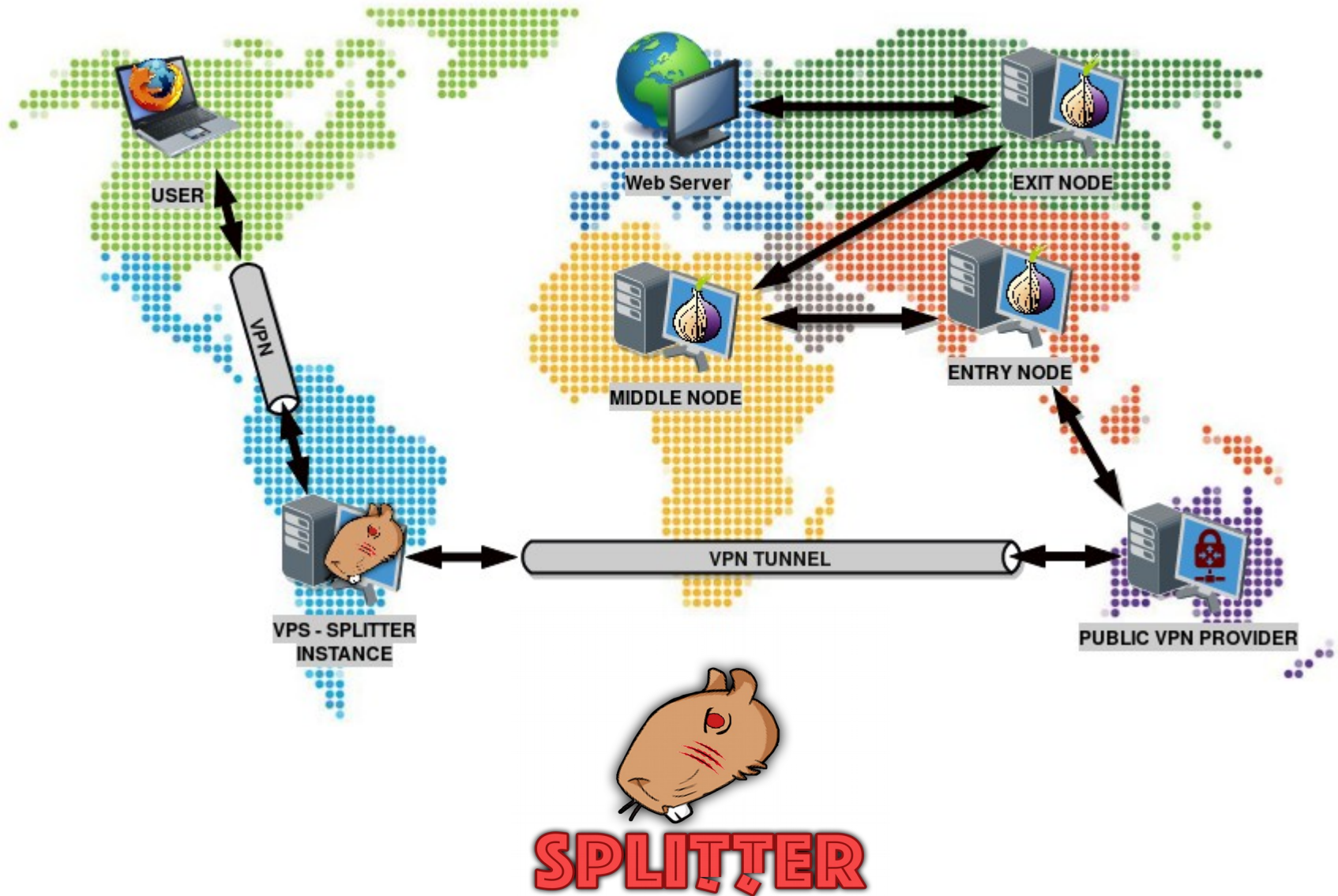
TOR_INSTANCES																																
	Queue			Session rate			Sessions					Bytes		Denied		Errors		Warnings		Server												
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle		
TOR_INSTANCE_27	0	0	-	1	1		1	1	20	33	33	0s	49 401	32 744	0	0	0	0	0	0	0	4m23s UP	L7OK/200 in 238ms	1	Y	-	17/0	17	6m52s	-		
TOR_INSTANCE_13	0	0	-	0	1		0	1	20	37	37	42s	24 614	66 171	0	0	0	1	0	0	0	10s DOWN	L7TOUT in 15001ms	1	Y	-	12/1	11	6m58s	-		
TOR_INSTANCE_3	0	0	-	0	1		0	1	20	30	30	1m14s	47 108	27 393 633	0	0	0	0	0	0	0	5m45s UP	* L7OK/200 in 129ms	1	Y	-	23/0	23	11m5s	-		
TOR_INSTANCE_1	0	0	-	0	1		0	2	20	40	40	1m34s	43 252	403 672	0	0	0	0	0	0	0	2m47s UP	L7OK/200 in 89ms	1	Y	-	3/0	3	43s	-		
TOR_INSTANCE_23	0	0	-	0	1		0	1	20	37	37	1m49s	34 028	435 718	0	0	0	0	0	0	0	16m35s UP	L7OK/200 in 102ms	1	Y	-	2/0	2	6m47s	-		
TOR_INSTANCE_14	0	0	-	0	1		0	2	20	33	33	8m59s	68 683	128 758	0	0	0	0	0	0	0	56s UP	L7OK/200 in 11433ms	1	Y	-	8/0	8	10m6s	-		
TOR_INSTANCE_32	0	0	-	0	1		0	1	20	37	37	3m35s	24 494	197 522	0	0	0	0	0	0	0	2m55s DOWN	* L7TOUT in 15001ms	1	Y	-	5/1	5	5m41s	-		
TOR_INSTANCE_35	0	0	-	0	1		1	2	20	35	35	4m6s	115 111	56 568	0	0	0	0	0	0	0	23m35s UP	L7OK/200 in 140ms	1	Y	-	4/0	4	50s	-		
TOR_INSTANCE_7	0	0	-	0	1		0	1	20	27	27	3m37s	19 996	144 240	0	0	0	0	0	0	0	2m42s DOWN	L7TOUT in 15001ms	1	Y	-	31/1	30	11m31s	-		
TOR_INSTANCE_29	0	0	-	0	1		0	1	20	34	34	2m27s	22 097	20 609	0	0	0	0	0	0	0	8s DOWN	L7TOUT in 15001ms	1	Y	-	17/0	17	4m46s	-		
TOR_INSTANCE_11	0	0	-	0	1		0	1	20	31	31	58s	186 142	120 778	0	0	0	0	0	0	0	5m23s UP	L7OK/200 in 193ms	1	Y	-	18/0	18	8m45s	-		
TOR_INSTANCE_36	0	0	-	0	1		0	1	20	38	38	1m24s	129 770	574 847	0	0	0	0	0	0	0	23m39s UP	L7OK/200 in 163ms	1	Y	-	3/0	3	39s	-		
TOR_INSTANCE_26	0	0	-	0	1		0	1	20	36	36	1m3s	102 973	145 427	0	0	0	0	0	0	0	10m45s UP	L7OK/200 in 313ms	1	Y	-	8/0	8	2m2s	-		
TOR_INSTANCE_33	0	0	-	0	1		0	2	20	36	36	1m14s	23 986	230 740	0	0	0	0	0	0	0	2m13s UP	L7OK/200 in 105ms	1	Y	-	11/0	11	3m12s	-		
TOR_INSTANCE_39	0	0	-	0	1		1	1	20	16	16	17s	6 966	5 279	0	0	0	0	0	0	0	1m24s UP	L7OK/200 in 154ms	1	Y	-	55/0	55	18m30s	-		
TOR_INSTANCE_19	0	0	-	0	1		1	1	20	8	8	32s	2 415	273	0	0	0	0	0	0	0	3m4s UP	L7OK/200 in 591ms	1	Y	-	24/0	24	1h5m	-		
TOR_INSTANCE_20	0	0	-	0	1		0	2	20	38	38	37s	24 306	5 368 117	0	0	1	0	0	0	0	3m6s UP	L7OK/200 in 269ms	1	Y	-	5/1	4	5m23s	-		
TOR_INSTANCE_25	0	0	-	0	1		0	2	20	37	37	1m29s	15 519	11 599	0	0	0	0	0	0	0	9m57s UP	L7OK/200 in 342ms	1	Y	-	7/0	7	3m37s	-		
TOR_INSTANCE_16	0	0	-	0	1		0	2	20	40	40	2m31s	39 547	2 968 847	0	0	0	0	0	0	0	21m55s UP	L7OK/200 in 215ms	1	Y	-	2/0	2	1m18s	-		
TOR_INSTANCE_6	0	0	-	0	1		1	1	20	39	39	5s	110 921	759 061	0	0	0	0	0	0	0	6m51s UP	L7OK/200 in 165ms	1	Y	-	3/0	3	53s	-		
TOR_INSTANCE_24	0	0	-	0	1		0	2	20	37	37	1m19s	17 206	14 406	0	0	0	0	0	0	0	2m15s UP	L7OK/200 in 125ms	1	Y	-	8/0	8	2m41s	-		
TOR_INSTANCE_34	0	0	-	0	1		0	2	20	37	37	2m31s	41 035	44 422	0	0	0	0	0	0	0	20s UP	L7OK/200 in 181ms	1	Y	-	15/0	15	4m16s	-		
TOR_INSTANCE_28	0	0	-	0	1		0	1	20	35	35	1m23s	14 201	20 914	0	0	0	0	0	0	0	3m38s UP	L7OK/200 in 518ms	1	Y	-	8/0	8	5m57s	-		
TOR_INSTANCE_4	0	0	-	0	1		1	1	20	29	29	10s	102 547	445 544	0	0	0	0	0	0	0	5m47s UP	L7OK/200 in 94ms	1	Y	-	29/0	29	11m5s	-		
TOR_INSTANCE_18	0	0	-	0	1		0	1	20	7	7	4m31s	2 415	428	0	0	1	0	0	0	0	1m56s DOWN	L7TOUT in 15001ms	1	Y	-	5/0	5	1h15m	-		
TOR_INSTANCE_30	0	0	-	0	1		0	1	20	37	37	1m49s	36 747	121 244	0	0	1	0	0	0	0	40s UP	L7OK/200 in 217ms	1	Y	-			1m15s	-		



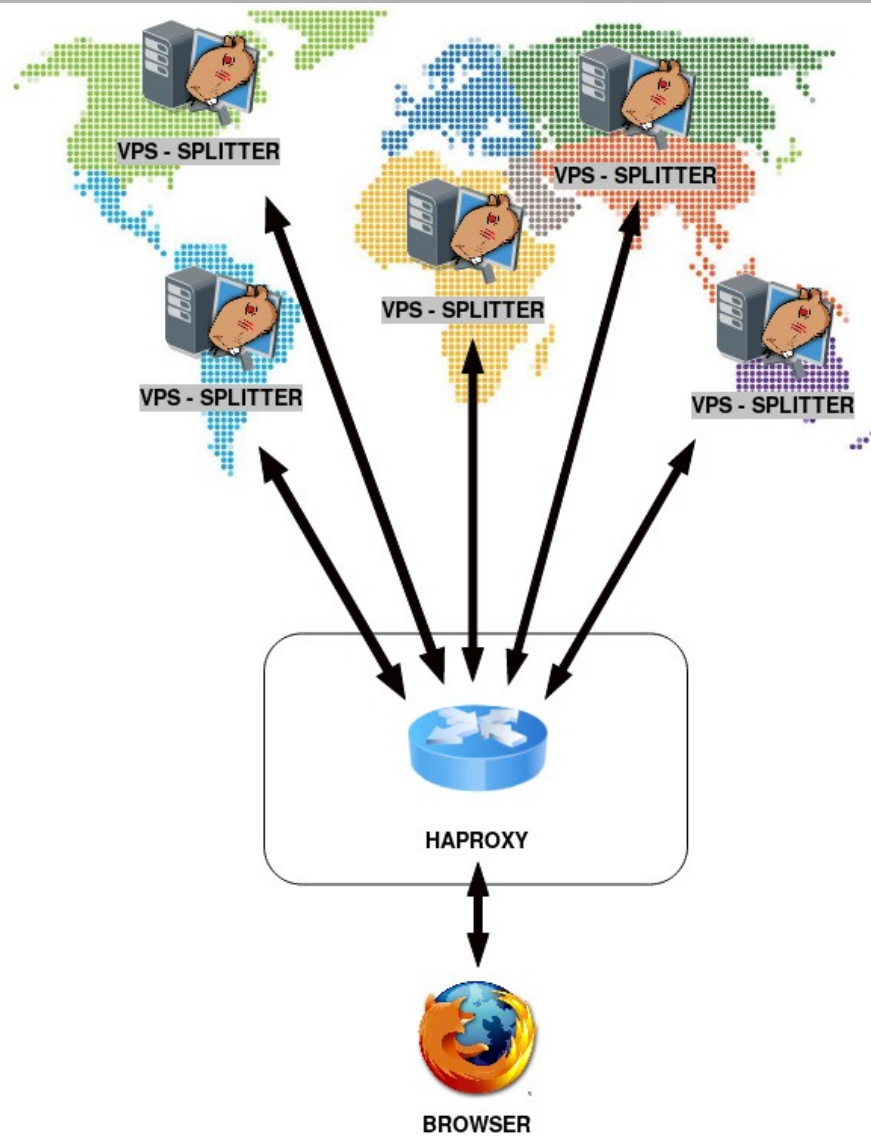
SPLITTER



SPLITTER NETWORK



SPLITTER NETWORK

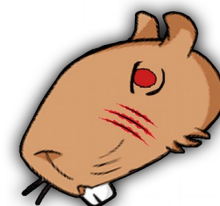


SPLITTER - Proof of Concept

Checking which TOR EXIT NODE that the SPLITTER is using for HTTP requests:

```
#!/bin/bash
show_ip_function() {
echo "$(echo -n "$(date | awk '{print $4}'); " && echo
"$(curl -x http://127.0.0.1:3536 http://ipinfo.io/ip
2> /dev/null)")"&}
time for c in $(seq 1 10000) ; do show_ip_function ;done
2> /dev/null
```

```
grinch@dclabs:~$ time for c in $(seq 1 10000) ; do [148/2008$
ne2>&l | grep ":"
02:32:16; 185.220.101.3
02:32:16; 37.187.94.86
02:32:16; 171.25.193.78
02:32:16; 185.220.102.6 → TOR EXIT node IP address.
02:32:16; 185.220.102.7
02:32:16; 5.9.158.75
02:32:16; 176.10.99.200
```



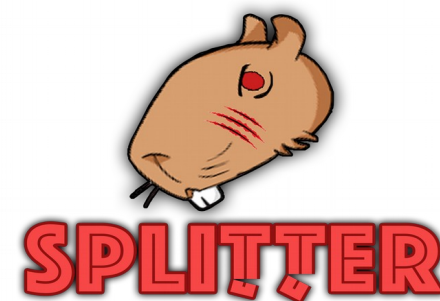
SPLITTER



SPLITTER - Proof of Concept

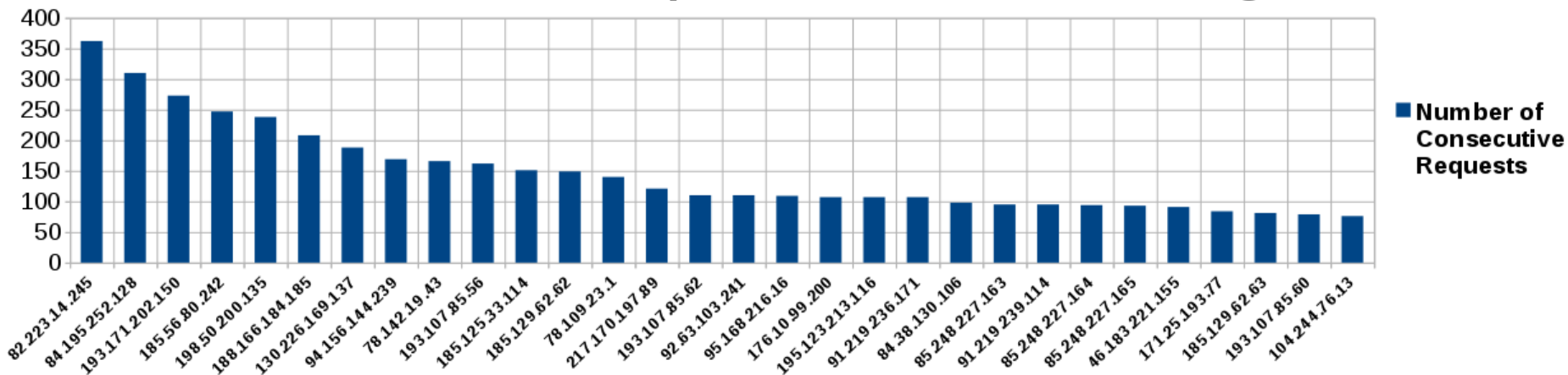
The LAB setup:

Available countries	32
Simultaneous active Countries / Instances	20
Simultaneous countries changed during the country rotation	10
Interval between the country rotation	2 minutes
Concurrent requests per second.	5~20
Time of exposition or interaction between the user and the supposed compromised web server.	34 minutes and 14 seconds



TOP 30 MOST REPEATED TOR EXIT NODES

From 10.000 HTTP Requests Sent to the Same Target



FROM 10.000 REQUESTS SENT TO THE SAME WEB SERVER

EXIT NODE	Country	CONSECUTIVE REQUESTS	PERCENT
82.223.14.245	Spain (ES)	362	3.6%
84.195.252.128	Belgium (BE)	310	3.1%
193.171.202.150	Austria (AT)	273	2.7%
185.56.80.242	Seychelles (SC)	247	2.4%
198.50.200.135	Panama (PA)	238	2.3%
188.166.184.185	Netherlands (NL)	208	2.8%
130.226.169.137	Denmark (DK)	188	1.8%
Total amount of data collected by this adversary			17.9%



















Relay Search

country:ES flag:exit

country:ES flag:exit

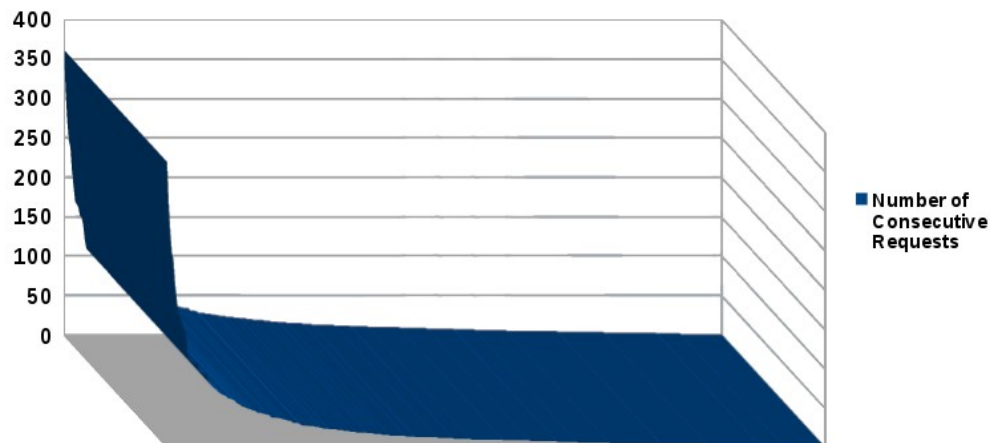
Show 10 entries

Nickname [†]	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
● coffswifi4 (5)	10 MiB/s	6d 4h		82.223.14.245	-	   		443	80	Relay
● nagusi (1)	519.27 KiB/s	188d 14h		212.81.199.159	-	   		9001	9030	Relay
● coffswifi (5)	350 KiB/s	61d 14h		82.223.27.82	-	   		9001	80	Relay
Total	10.85 MiB/s									

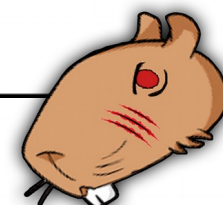
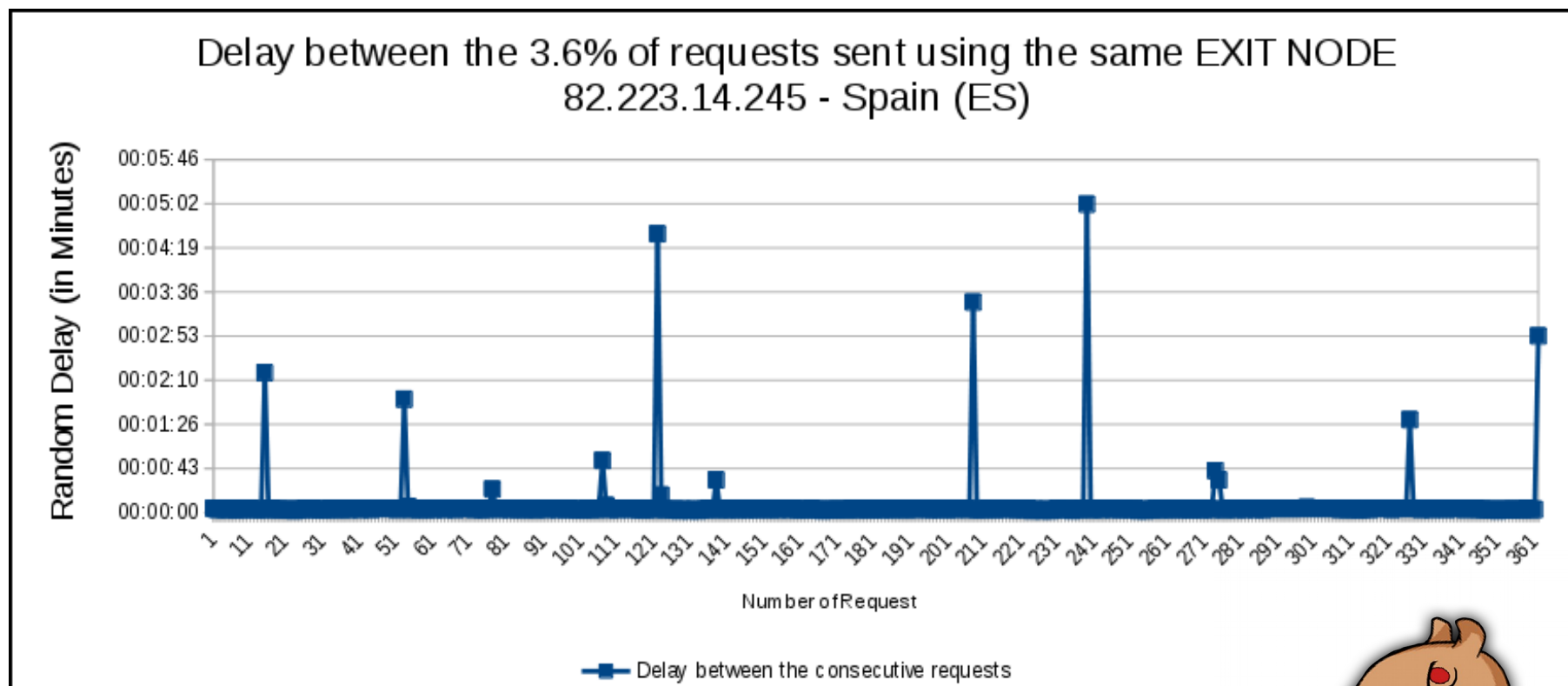
Showing 1 to 3 of 3 entries

Previous 1 Next

Distribution of 10.000 Requests
over the 413 used EXIT NODES



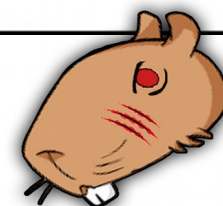
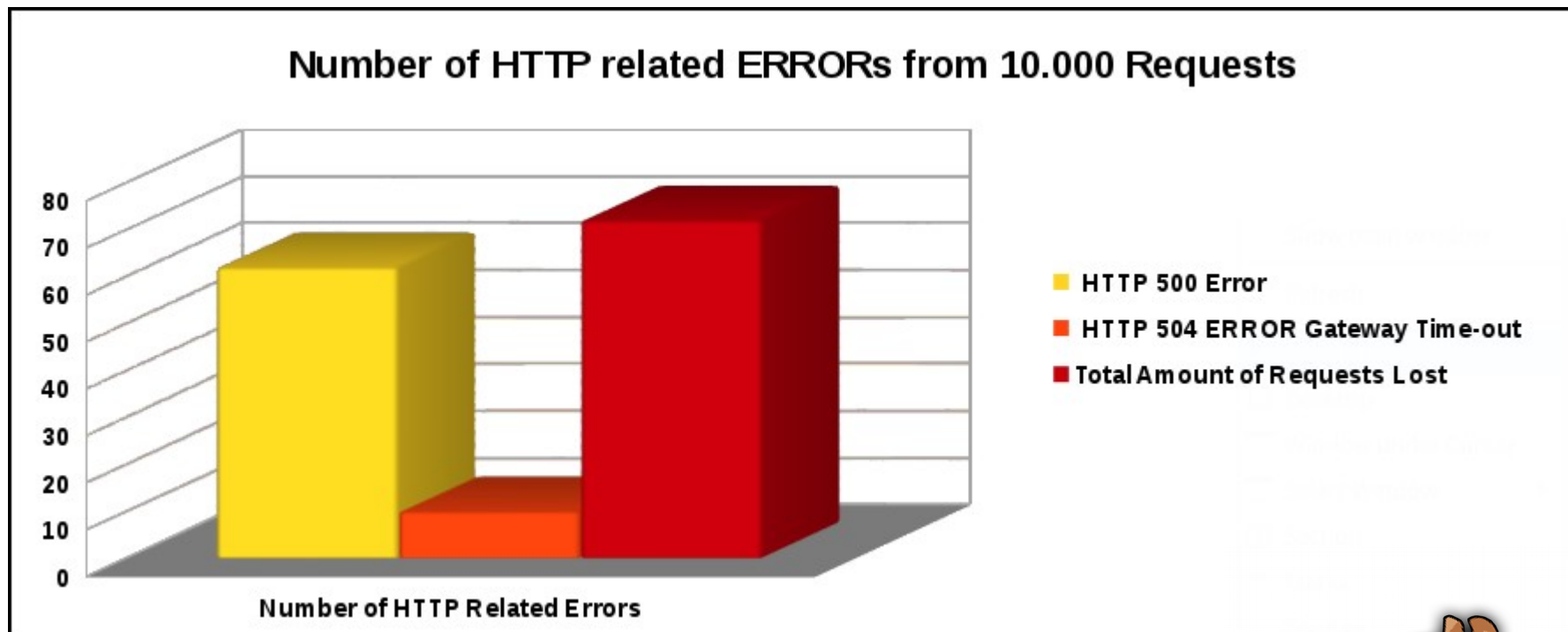
SPLITTER - Proof of Concept



SPLITTER



SPLITTER - Proof of Concept



SPLITTER



FINAL CONSIDERATIONS

- Use TOR without a VPN + VPS combination can be considered a risk.
- Based on the average of 0.5% of all data sent by the user, be transmitted to the final destination using the same supposed compromised TOR EXIT NODE. There is no doubts that the SPLITTER can difficult the correlation and traffic analyses attacks on TOR network.
- HAPROXY can be used to provide a better stability and performance for TOR related solutions.
- The SPLITTER approach sets a new bar for future de-anonymization techniques.



QUESTIONS?



Twitter: @Gr1nchDc
Blog: <https://blog.dclabs.com.br>
Mail: rener.silva@protonmail.com
LinkedIn: <https://www.linkedin.com/in/reneralberto/>



REFERENCES

[1] Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis and Angelos D. Keromytis - **“On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records”**.

[Online] Available: <https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545&format=pdf>

[2] Nathan S. Evans, Roger Dingledine and Christian Grothoff - **“A Practical Congestion Attack on Tor Using Long Paths”**.

[Online] Available: https://www.usenix.org/legacy/event/sec09/tech/full_papers/evans.pdf

[3] Steven J. Murdoch and George Danezis - **“Low-Cost Traffic Analysis of Tor”**.

[Online] Available: <https://murdoch.is/papers/oakland05torta.pdf>

[4] Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-Tin - **“How Much Anonymity does Network Latency Leak?”**.

[Online] Available: <https://www-users.cs.umn.edu/~hoppernj/tissec-latency-leak.pdf>

[5] Rob Jansen, Marc Juarez, Rafa Gálvez, Tariq Elahi and Claudia Diaz - **“Inside Job: Applying Traffic Analysis to Measure Tor from Within”**.

[Online] Available: <https://www.robjansen.com/publications/insidejob-ndss2018.pdf>

[6] Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno and Douglas Sicker - **“Low-Resource Routing Attacks Against Anonymous Systems”**

[Online] Available: <http://www.cs.colorado.edu/departments/publications/reports/docs/CU-CS-1025-07.pdf>



BONUS

Secure | <https://arstechnica.com/information-technology/2018/06/fbi-recovered-hundreds-of-encrypted-messages-from>

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORU

HANNITY ACID WASH FAIL —

FBI recovers WhatsApp, Signal data stored on Michael Cohen's BlackBerry

Letter to judge reveals 731 pages of messages, call logs uncovered on one of two phones.

SEAN GALLAGHER - 6/15/2018, 11:00 PM

A photograph showing Michael Cohen, a man with dark hair and a beard, wearing a dark suit and a blue tie, walking past a building. The building has a large gold number '500' on its facade. Other people, including a man in a dark suit and a police officer in a blue uniform, are also visible in the background.

BONUS

