



ONION NETWORK SECURITY

PREVIEW OF AN ACADEMIC PAPER ABOUT "SURVEYING
TOR SECURITY GUIDELINES BY SCANNING RELAY NODES"

(aka "slicing the onion")

Alessandro "Scinawa" Luongo



127.0.0.1

(aka "about me")

Me: proud member of the Italian Embassy
(Italian Grappa!)

Currently: Master in CS @ UniMI.
(yes, this should be a serious dissertation)

Loves: Information Security, Mathematics,
babes, alcohol.
(not necessarily in this order)

Work: presenting a "will be formal paper"
about compliance with Tor security to
hackers that can understand it
(and not to academics...)

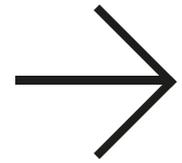


→ PURPOSE

- **THEORY:** Given the “Operational Security Document” by Tor, measure the distance from the suggested implementation[1];
- **PRACTICE:** Portscan all the Tor network!



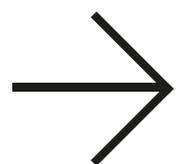
[1] <https://trac.torproject.org/projects/tor/wiki/doc/OperationalSecurity>



FIRE! FIRE! FIRE & FLAMES!

- [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Fabio Pietrosanti (naif)*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Andrew Lewman*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Fabio Pietrosanti (naif)*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Nick Mathewson*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Fabio Pietrosanti (naif)*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Chris*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *grarpamp*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Robin Kipp*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Chris*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Mike Damm*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Chris*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Justin Aplin*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Chris*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Lee*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Eugen Leidl*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *John Case*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Sebastian Hahn*
 - [\[tor-talk\] Automatic vulnerability scanning of Tor Network?](#) *Jon*

Main idea for this talk coming from a long thread on Tor-Talk about the feasibility and ethics of Tor Relay node scanning by notorious security troll expert **Fabio “naif” Pietrosanti** -> <3



NOT REALLY SO SIMPLE

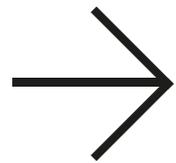
“...after all it wasn't so difficult, a couple of lines in console should suffice...” (me, ~2012/09)

(GOD, I was WRONG....)

```
wget -q -O /tmp/Tor_ip_list_ALL.csv \  
http://torstatus.blutmagie.de/ip\_list\_all.php/  
Tor\_ip\_list\_ALL.csv  
  
nmap -iL /tmp/Tor_ip_list_ALL.csv -F -sS -sV -PI -T  
Insane \  
-oM Tor-Scan-20-12-2011_00_30.out
```

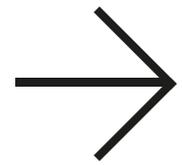
Code ©2012 Fabio “naif” ~~trøll~~ Pietrosanti from the Mailing List Thread

Be safe, ~~use a condom~~ follow “Operational Security Document” Guidelines



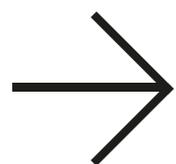
COMPLEX ISSUES

- **Should this data be publicly disclosed?**
Can it be misused by evil guys around the world? Will it trigger Third World War?
- **You'll end up annoying the node maintainer, triggering IDS.**
Or scaring the s*it out of him/her. Will they flee in Guatemala after the scan?
- **Is this useful?**
(hint: yes, it is!)



ONION SCANNING TECHNIQUES

- **Purpose:** Avoid annoying Tor relay operators and not triggering IDS;
- **Low and distributed** scan ... using TOR! :)
- A relay receive **MAX 5** different connect from **5 different IP** a day;
- Scanning all networks for 500 (actually ~300) ports takes about **10 days**;
- Exit node **selection**:
 - **different exit route** used as source of the scan (*no reuse of Tor exit within 10 days*)
 - only exit node that **allow to reach targeted destination** (*exitlist.pt by Nick Mathewson <3*)



TARGET SELECTION

- Only relevant Tor relay are scanned.;
- A relay is meant to be relevant if and only if :
 - The total uptime in 45 days was > than 30 days and the average uptime was > than 15 days.
 - (about 1800 Tor relay over 4k active on average and about 14k different relay sampled in the last 45 days.)

```
SELECT *
FROM (SELECT fp,
      Sum(Timestampdiff(day, `last_restarted`, `maxscandate`)) AS
      uptime,
      Avg(Timestampdiff(day, `last_restarted`, `maxscandate`)) AS
      average
FROM (SELECT *,
      Max(scandate) AS MaxScanDate
FROM torSample2
WHERE `scandate` >= Date_sub(Curdate(), INTERVAL 45 day)
GROUP BY Round(Unix_timestamp(`last_restarted`) / 10, -1),
      fp) AS correctTuple
GROUP BY fp) AS filterMe
WHERE uptime >= 30 AND average >= 15;
```

Days	Avg	Total	N°
12	3	6	3152
24	6	12	2703
45	15	30	1832

```
# Fields in this file are: Service name, portnum/protocol, open-frequency,
#
tcpmux 1/tcp 0.001995 # TCP Port Service Multiplexer [rfc-1078]
tcpmux 1/udp 0.001236 # TCP Port Service Multiplexer
compressnet 2/tcp 0.000013 # Management Utility
compressnet 2/udp 0.001845 # Management Utility
compressnet 3/tcp 0.001242 # Compression Process
compressnet 3/udp 0.001532 # Compression Process
```

PORT SELECTION

```
unknown 4/tcp 0.000477
rje 5/udp 0.000593
unknown 6/tcp 0.000502
echo 7/tcp 0.004855
echo 7/udp 0.024679
echo 7/sctp 0.000000
unknown 8/tcp 0.000013
discard 9/tcp 0.003764
discard 9/udp 0.015733
discard 9/sctp 0.000000
unknown 10/tcp 0.000063
systat 11/tcp 0.000075
systat 11/udp 0.000577
unknown 12/tcp 0.000063
daytime 13/tcp 0.003927
daytime 13/udp 0.004827
unknown 14/tcp 0.000038
netstat 15/tcp 0.000038
unknown 16/tcp 0.000050
gotd 17/tcp 0.002346
```

- To have a non arbitrary port list to scan we took the file “nmap-services”: we extract port to be scanned based on the frequency we found in the nmap file.
- `cat /usr/share/nmap/nmap-services | grep '([0-9]\|tcp)'`
`| sort -k3 -n | head -n 1000 | sed 's/[^0-9]*//g' >`
`OKports.conf`
- `or_port` and `dir_port` are filtered after the scan...

```
if ("errNumber" in dir(error.type)):
    # I'm sorry.
    if (error.type.errNumber==1):
        f.state="1" #damn!
```

```
class SScanFactory(Factory):
    #Magic. Do not touch.
    def __init__(self, fingerprint, addr, port, scanDate): #, internalConn, ):
```

QUALITY SOFTWARE

*(Software used only after in-depth QA hamster-delivered clearance)
(NO HAMSTER was hurt during this QA testing)*

```
#When I wrote this, only God and I understood what I was doing
#Now, God only knows
print "-> Start at ", scanDate, " [K]"
```

```
# drunk, fix later
def run(self, nodeScanList, exitRouteList, configDic, dictionarylookup):
```

```
from logic import *
```

```
# sometimes I believe compiler ignores all my comments
```

```
configFile = "/opt/config.ini"
configPar = ConfigParser.ConfigParser()
```

RESULTS

Yeah, every now and then I get some....

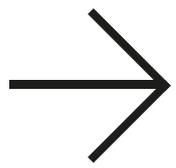
“INTRESTING” PORTS



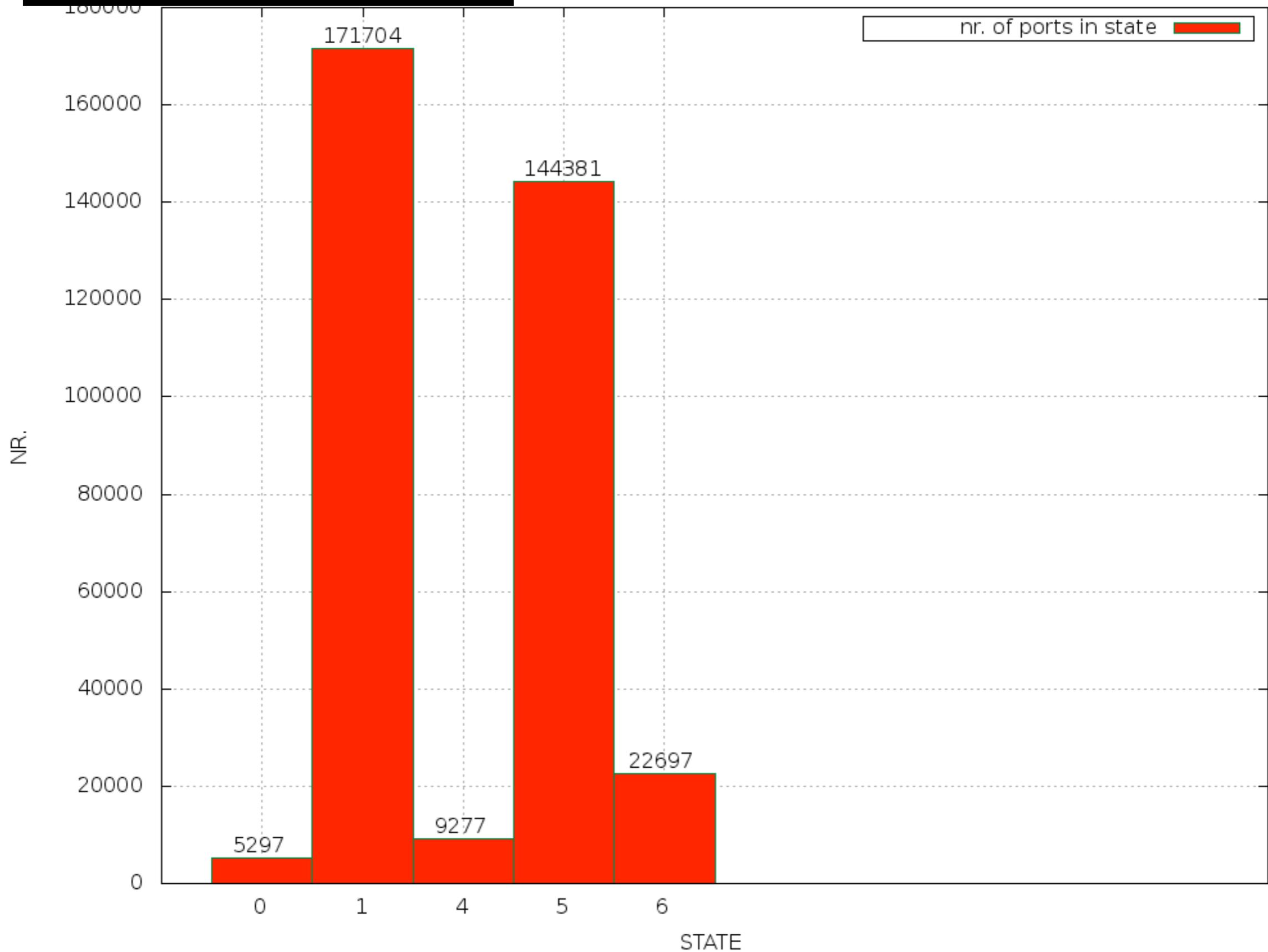
RETARDS

We all know one.

Port	n° (tot 1800)
3306 (mysql)	40
995 (pop3 ssl)	86
110 (pop3)	77
135 (rpc)	8
3389 (rem. desk)	21
21 (ftp)	139
5900 (vnc)	4

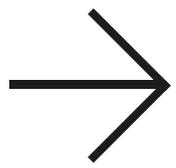


THE RESULTS

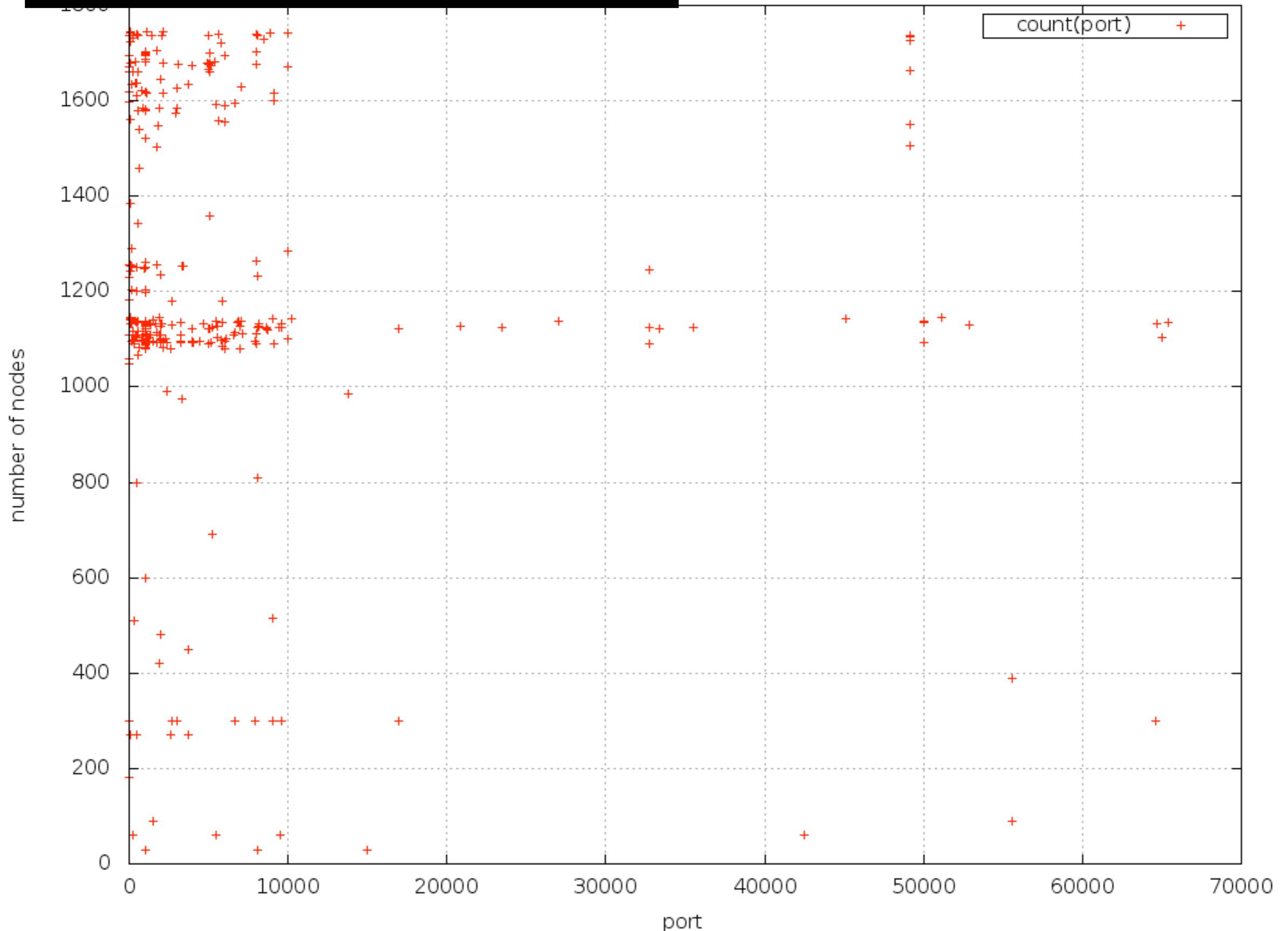


```
select state,count(*) from results2FilteredUnique where state="1" or state="0" or state="6" or state="4" or state="5" group by state;
```

Be safe, use a condom follow "Operational Security Document" Guidelines

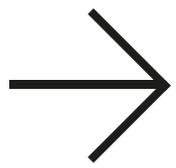


HOW MUCH DO I SCAN?

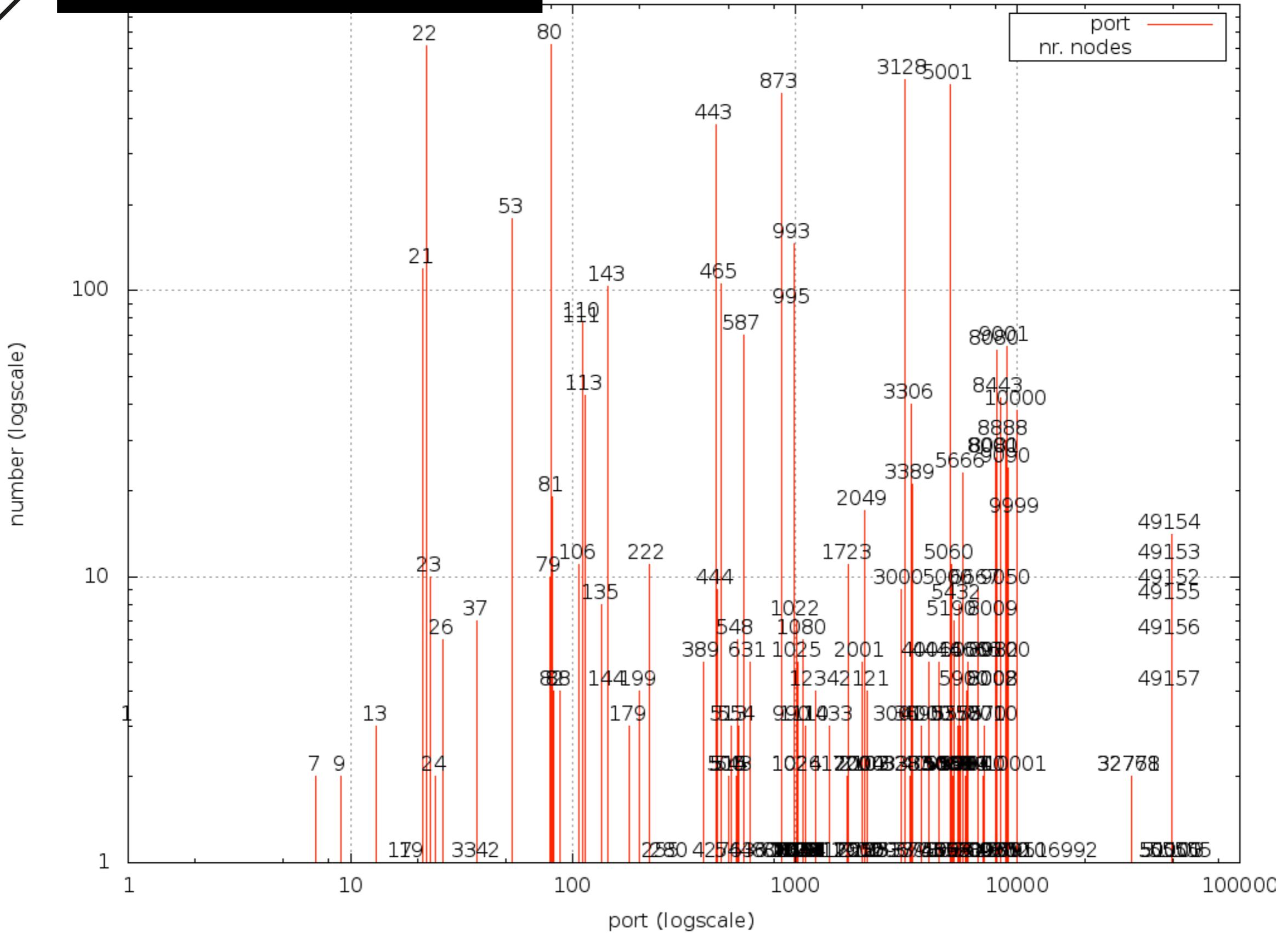


```
select port,count(port) from results2FilteredUnique group by port;
```

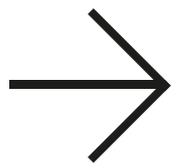
Be safe, use a condom follow "Operational Security Document" Guidelines



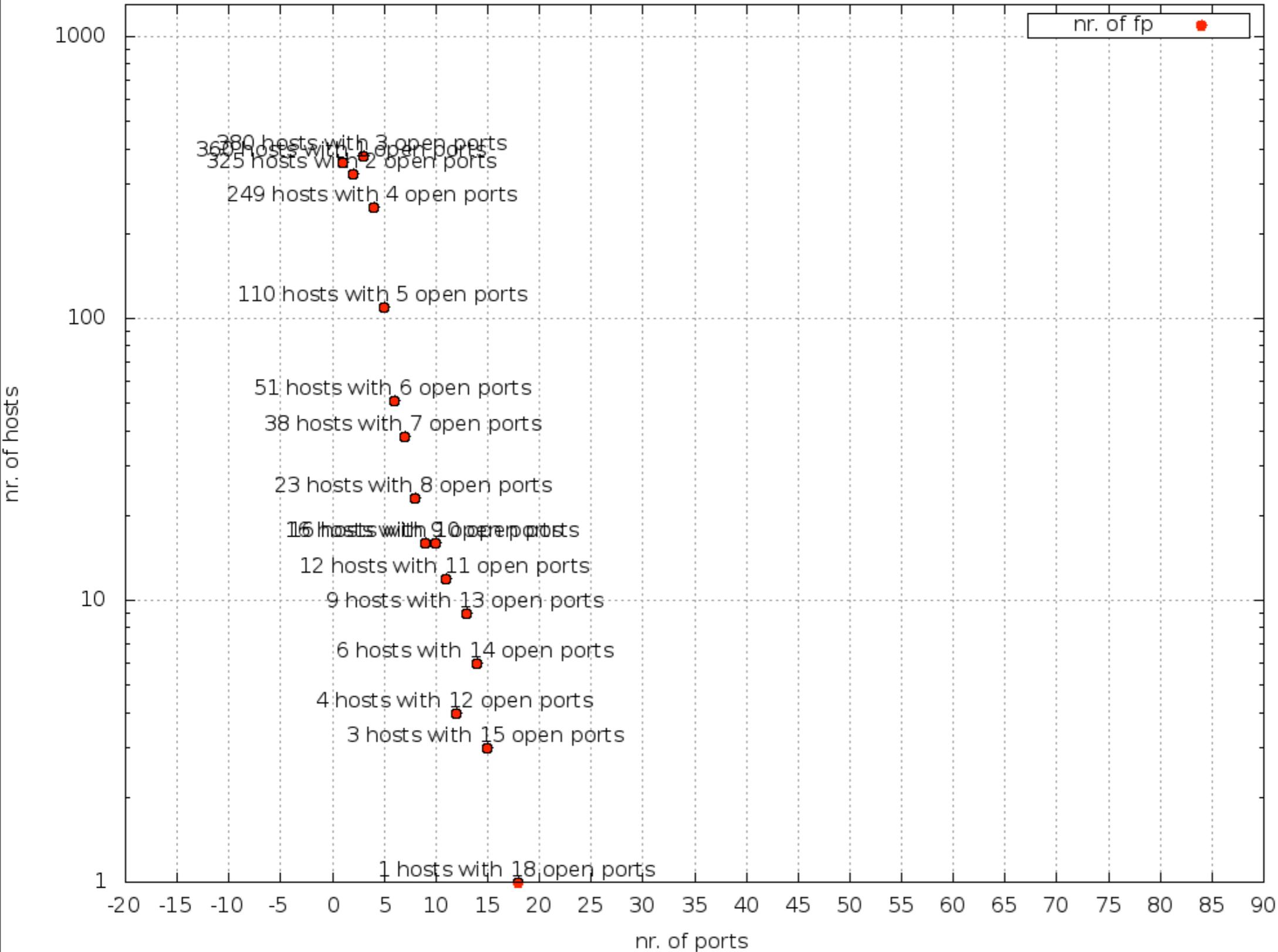
OPEN PORT



```
select port,count(*) as numero from results2FilteredUnique where state='0' group by port order by numero asc;
```



THE RANK

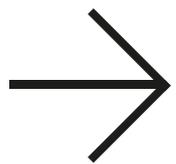


Open Hosts

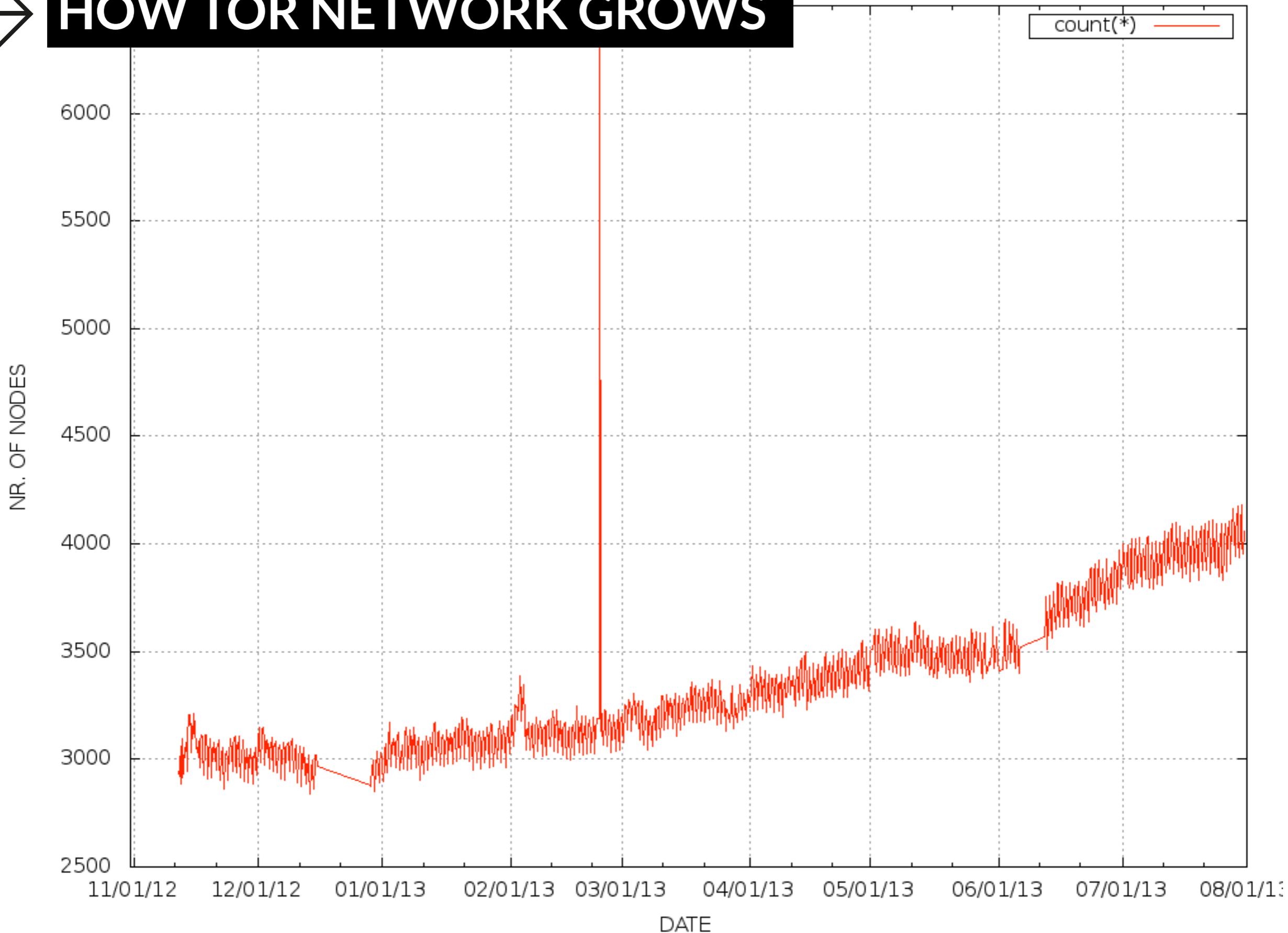
1	360
2	325
3	380
4	249
5	110
6	51
7	38
8	23
9	16
10	16
11	12
12	4
13	9
14	6
15	3
18	1
97	1

```
select contatore,count(fp) from ( select count(port) as contatore, fp from results2FilteredUnique
where state='0' group by fp order by contatore desc) as deriv group by contatore
```

Be safe, use a career follow "Operational Security Document" Guidelines



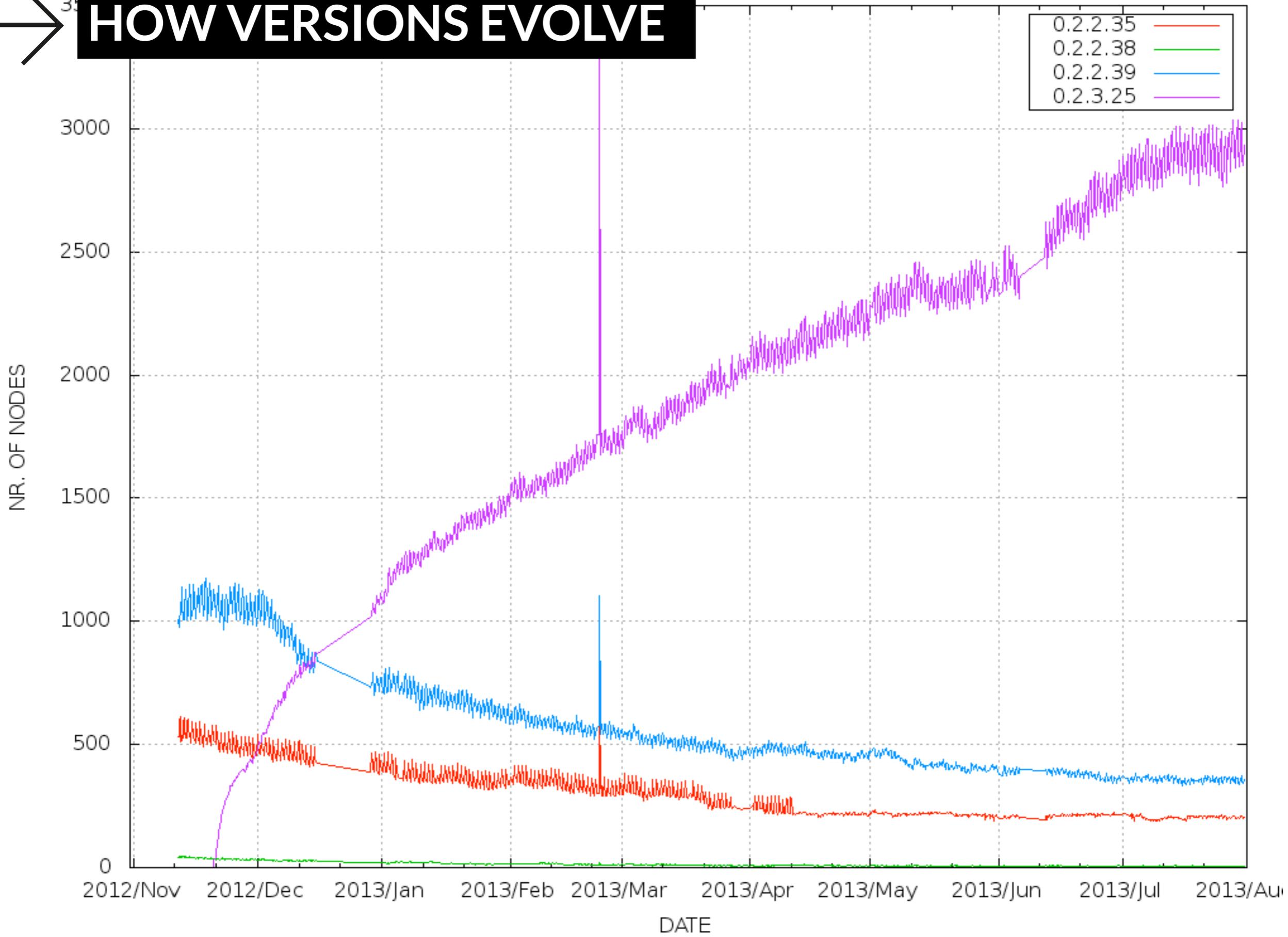
HOW TOR NETWORK GROWS



```
select contatore, count(fp) from ( select count(port) as contatore, fp from results2FilteredUnique where state='0' group by fp order by contatore desc) as deriv group by contatore
```

Be safe, use a career follow "Operational Security Document" Guidelines

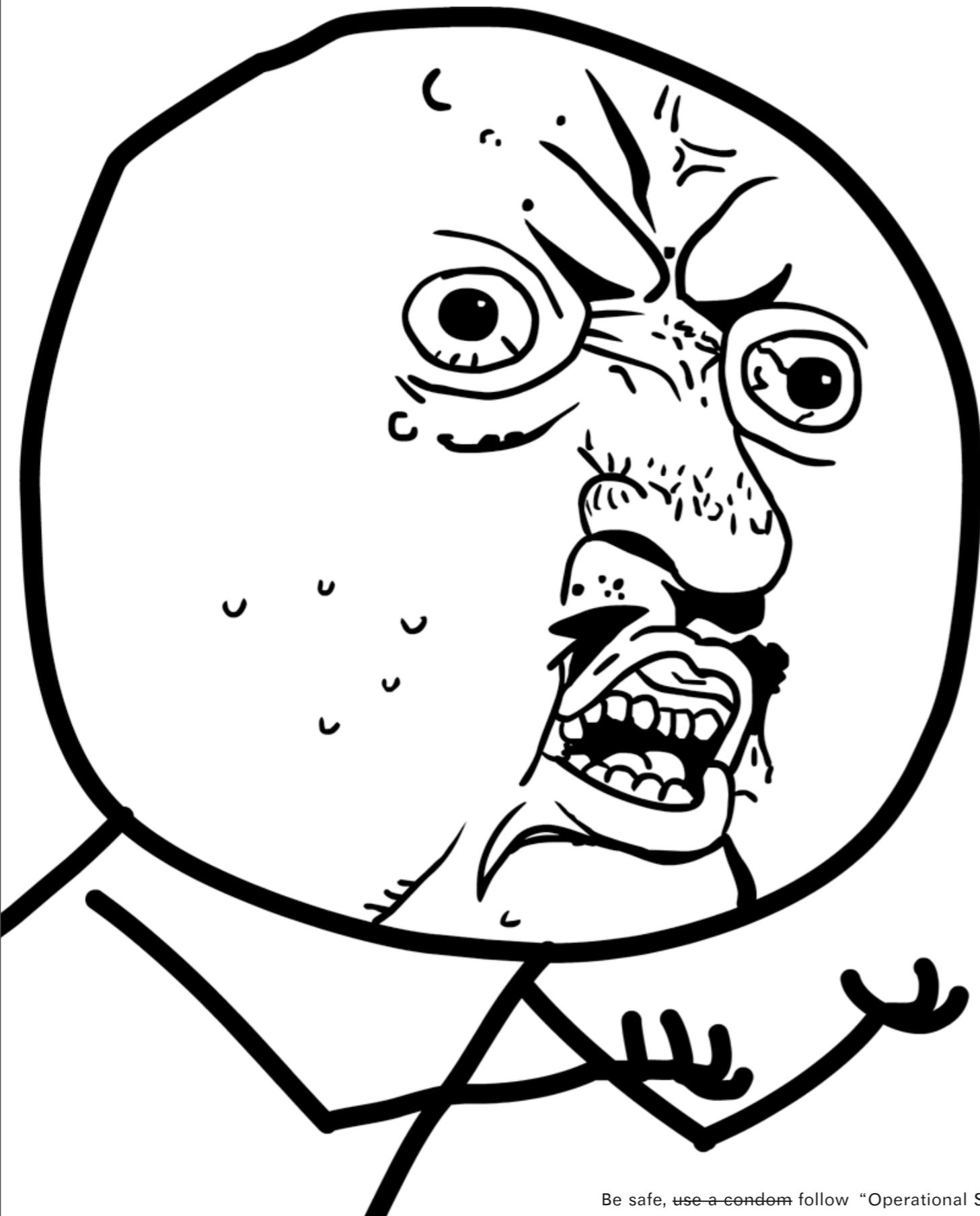
HOW VERSIONS EVOLVE



```
select contatore, count(fp) from ( select count(port) as contatore, fp from results2FilteredUnique where state='0' group by fp order by contatore desc) as deriv group by contatore
```

Be safe, use a career follow "Operational Security Document" Guidelines

→ CONCLUSIONS



YUNO

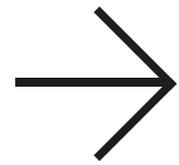
SECURE RELAY NODES? 11!?

Results:

- There is a **HUGE** need of training and informing nodes maintainers about **security guidelines**;
- Survey denotes that Guidelines are **seldom applied** by **too many** relay nodes;

Proposal:

- Is there a real need to implement this as a **continuous service** that **proactively inform** node maintainers?



FUTURE IMPLEMENTATIONS

- Refactor the software (python+twisted)
- Drink italian grappa @ Italian Embassy (Q&A)
- Expose RESTful API of scanned results.
- Find other awesome comments for code[1]

[1] <http://stackoverflow.com/questions/184618/what-is-the-best-comment-in-source-code-you-have-ever-encountered>

Q&A

(will be held "drunk" @ Italian Embassy)

For comments, questions, insults, free pizza gift, sexual favours & co:

alessandro@luongo.pro
lordscinawa@gmail.com (<- evil Google)

Get the Sauce:

<http://github.com/torscanner/torScanner>



**IGLU
ASCI**



presentation officially pimped
by Matteo "LK" Flora with
support from Hermes Center