Security Evaluation of Dual-Stack Systems

Troopers 2016

Patrik Fehrenbach

Prof Dr. Friedbert Kaspar / Dipl. Ing. (BA) Christopher Scheuring

Disclaimer

- There will be a lot of numbers,charts....
- They could be wrong
- ...I did my best so they are not☺

Talk Roadmap

- About dualstack
- Motivation
- Previous work
- Results
- Conclusion

About Dualstack

Dual-Stack
Domain: Google.com

IPv6 : 2a00:1450:400a:805::1008
{…}

IPv4: 109.193.193.104
{…}

Security?

Motivation

- RFC 7381 -**Enterprise IPv6 Deployment Guidelines**

„It should be noted that in a dual-stack network, the security implementation for ***both*** *IPv4 and IPv6 needs to be considered, in addition to security considerations related to the interaction of (and transition between) the two, while they coexist.“*

Motivation

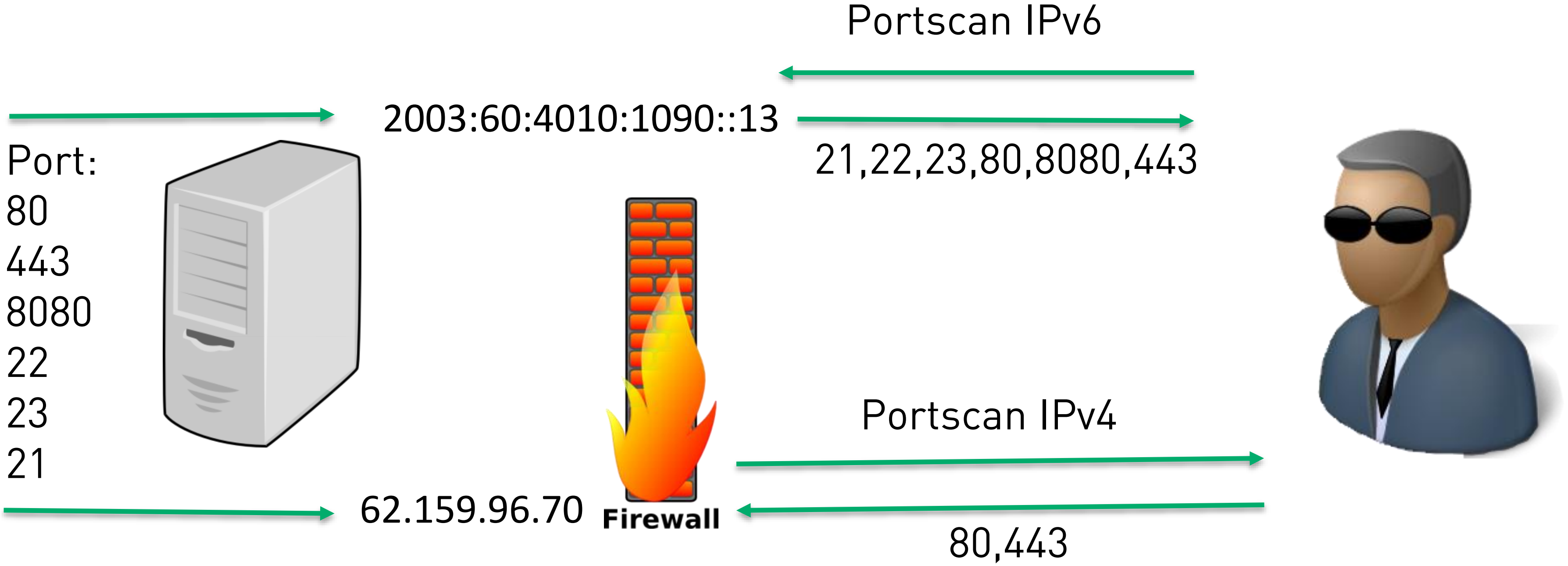
- RFC 7381 -**Enterprise IPv6 Deployment Guidelines**

„This simply means that all routers and hosts operating in a dual-stack environment with both protocol families enabled (even if by default) must have a ***congruent*** *security policy for* ***both*** *protocol versions. For example, permit TCP ports 80 and 443 to all web servers and deny all other ports to the same servers must be implemented both for IPv4* ***and*** *IPv6.“*

Well…

What if they haven't?

Attack scenario



Portscan IPv6

2003:60:4010:1090::13

21,22,23,80,8080,443

Port:
80
443
8080
22
23
21

Portscan IPv4

62.159.96.70

80,443

How?

- 1. Write a script
- 2. Get a list of domains
- 3. Scan them
- 4. Store them
- 5. Analyse them

Getting a list of suitable Targets

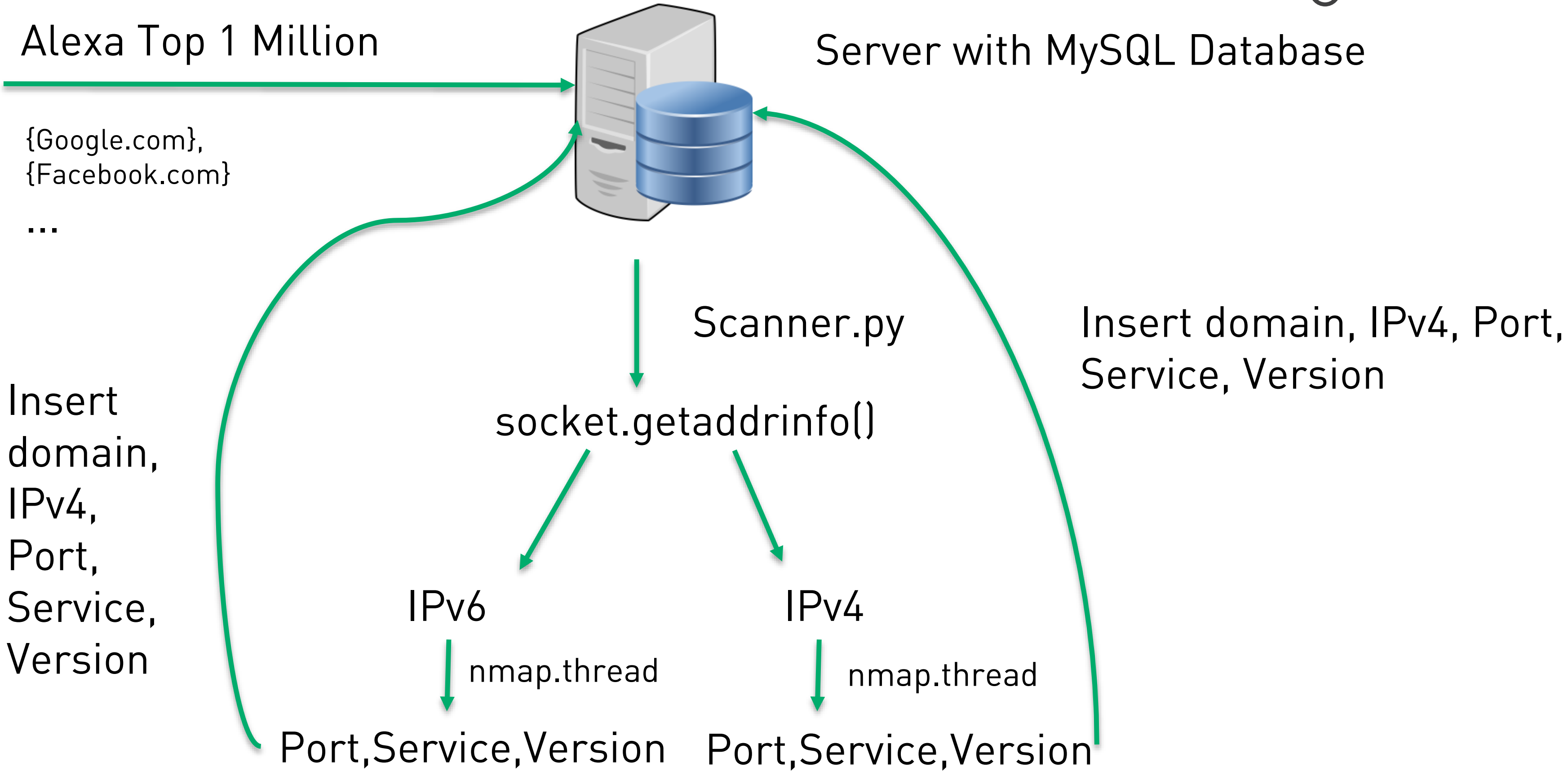
- Alexa Top 1 Million
- Frequently used
- (should) be well maintained
- CSV

```
1,google.com
2,facebook.com
3,youtube.com
4,baidu.com
5,yahoo.com
{...}
```

Let´s sum it up

- 1 Million Domains
- Full TCP Port Scan (65535 Ports)
- Version detection
- Product detection

Procedure



Alexa Top 1 Million

{Google.com},
{Facebook.com}
...

Server with MySQL Database

Scanner.py

socket.getaddrinfo()

Insert domain, IPv4, Port, Service, Version

Insert
domain,
IPv4,
Port,
Service,
Version

IPv6

nmap.thread

Port,Service,Version

IPv4

nmap.thread

Port,Service,Version

Ethical Considerations

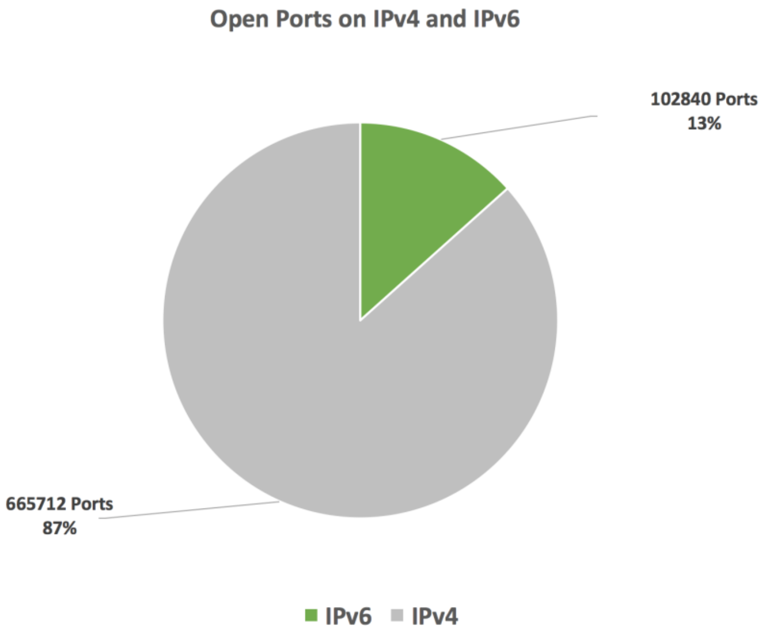
- We have responded to every abuse mail
- We only used RFC compliant SYN-ACK packets
- We believe this research contributes to IPv6 security
- We want to make the world a safer place

Results (Some Numbers)

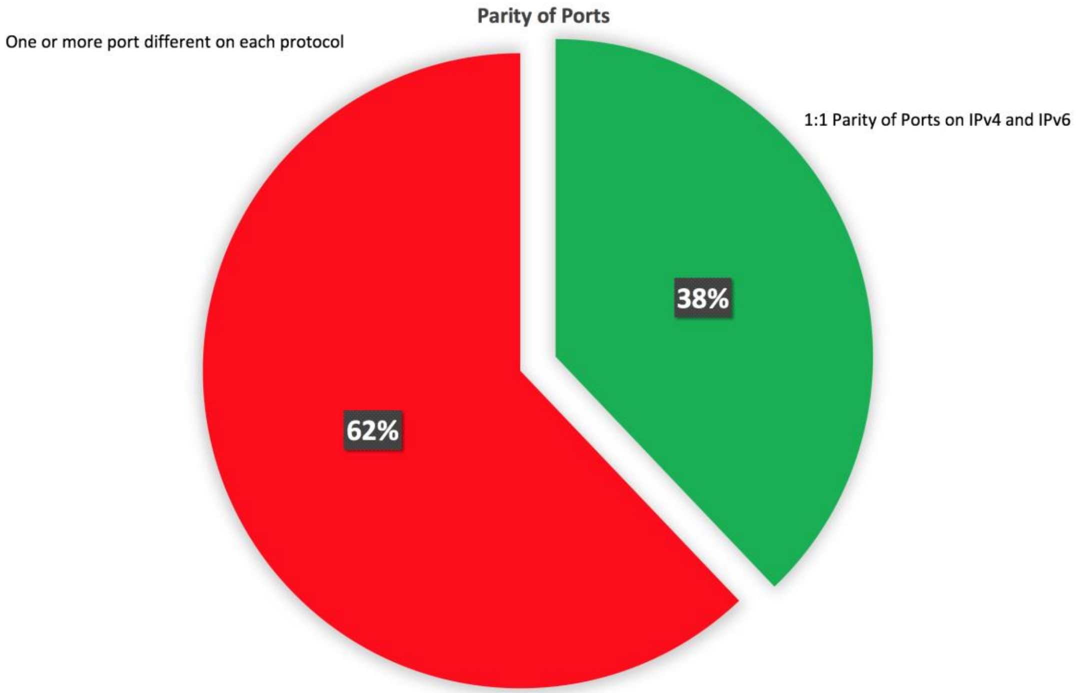
57,168 Domains
114,336 IP Adresses
976,998 Open Ports (IPv4&IPv6)

1,148,502 Total Datasets

204,877 Open Ports on IPv6
- 102840 (80,443)
772,121 Open Ports on IPv4
- 106409 (80,443)

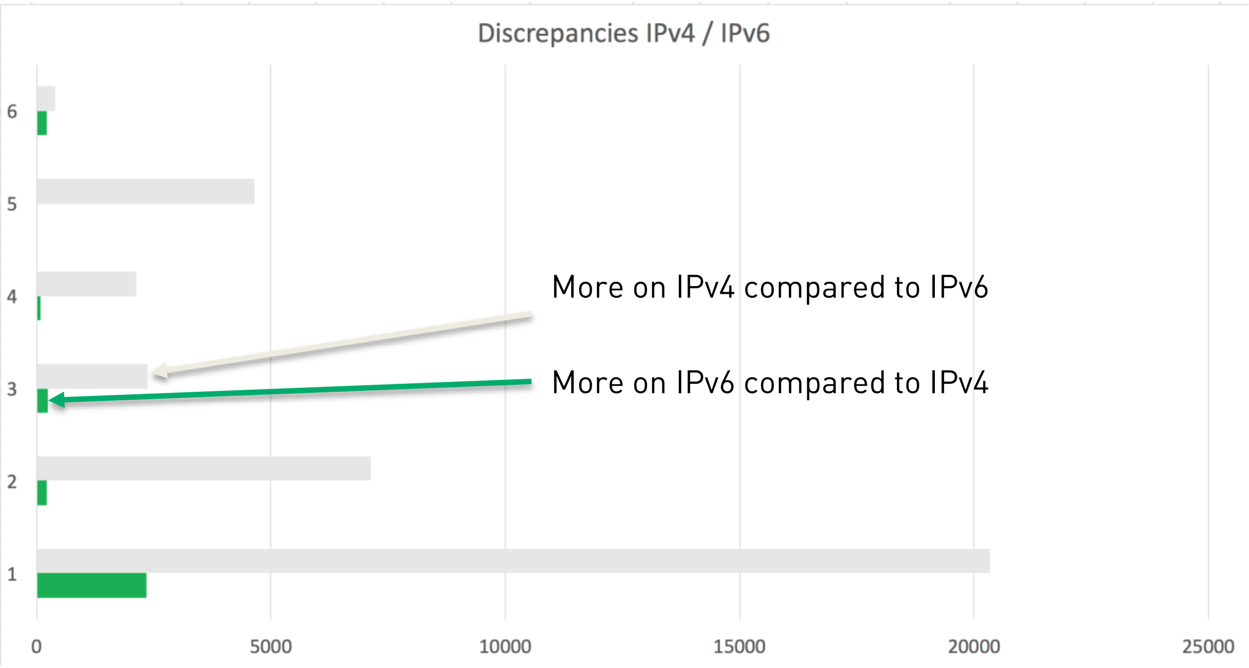


Parity (same amount of ports on IPv4 & IPv6)



Discrepancies

Deviant amount of
Ports



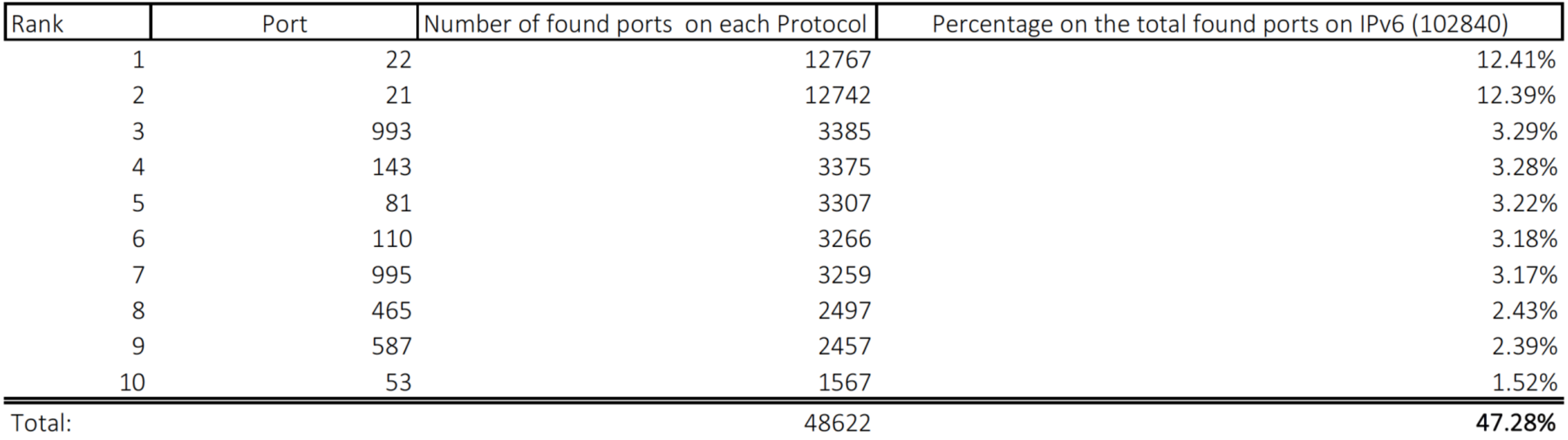
More on IPv4 compared to IPv6

More on IPv6 compared to IPv4

Cloudflare

- About 40% of the found IPv6 addresses belong to CF
- Only Web-Ports open (80,443,8080)
- Excluded from the statistics

Most used Ports on IPv6

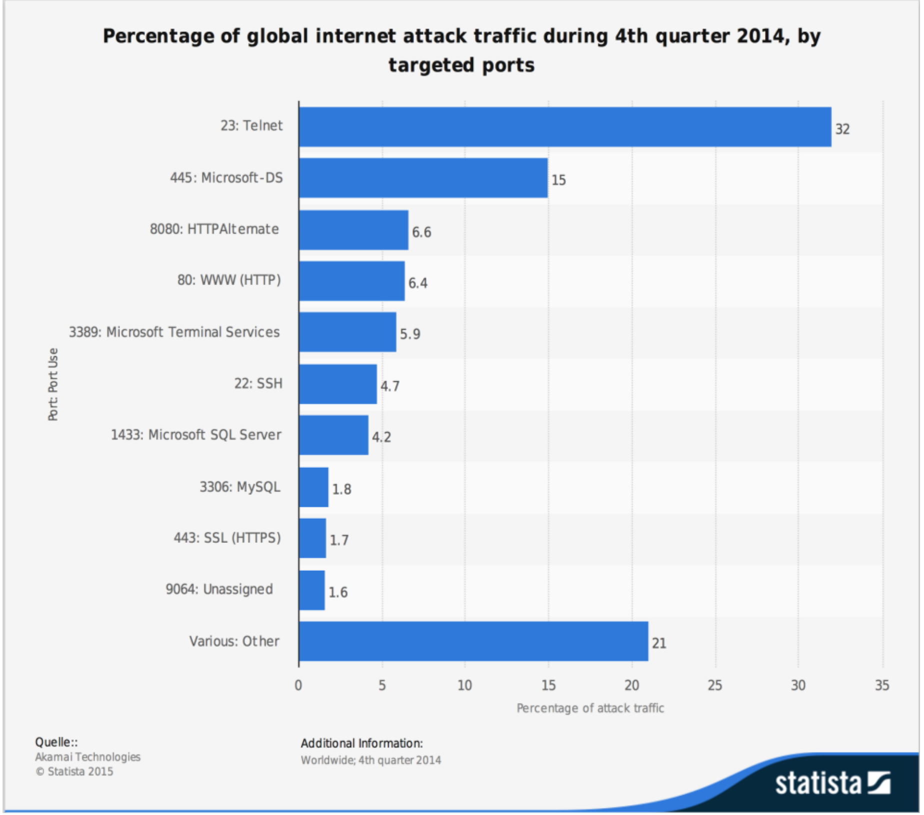


Rank	Port	Number of found ports on each Protocol	Percentage on the total found ports on IPv6 (102840)
1	22	12767	12.41%
2	21	12742	12.39%
3	993	3385	3.29%
4	143	3375	3.28%
5	81	3307	3.22%
6	110	3266	3.18%
7	995	3259	3.17%
8	465	2497	2.43%
9	587	2457	2.39%
10	53	1567	1.52%
Total:		48622	**47.28%**

Most used Ports on IPv4

Rank	Port	Number of found ports on each Protocol	Percentage on the total found ports on IPv4 (665712)
1	8443	22796	3.42%
2	21	15144	2.27%
3	22	13533	2.03%
4	25	6621	0.99%
5	143	5205	0.78%
6	110	5111	0.77%
7	993	4809	0.72%
8	995	4667	0.70%
9	587	4440	0.67%
10	3306	4293	0.64%
Total:		86619	**13.01%**

Most targeted Ports by Akami Technologies

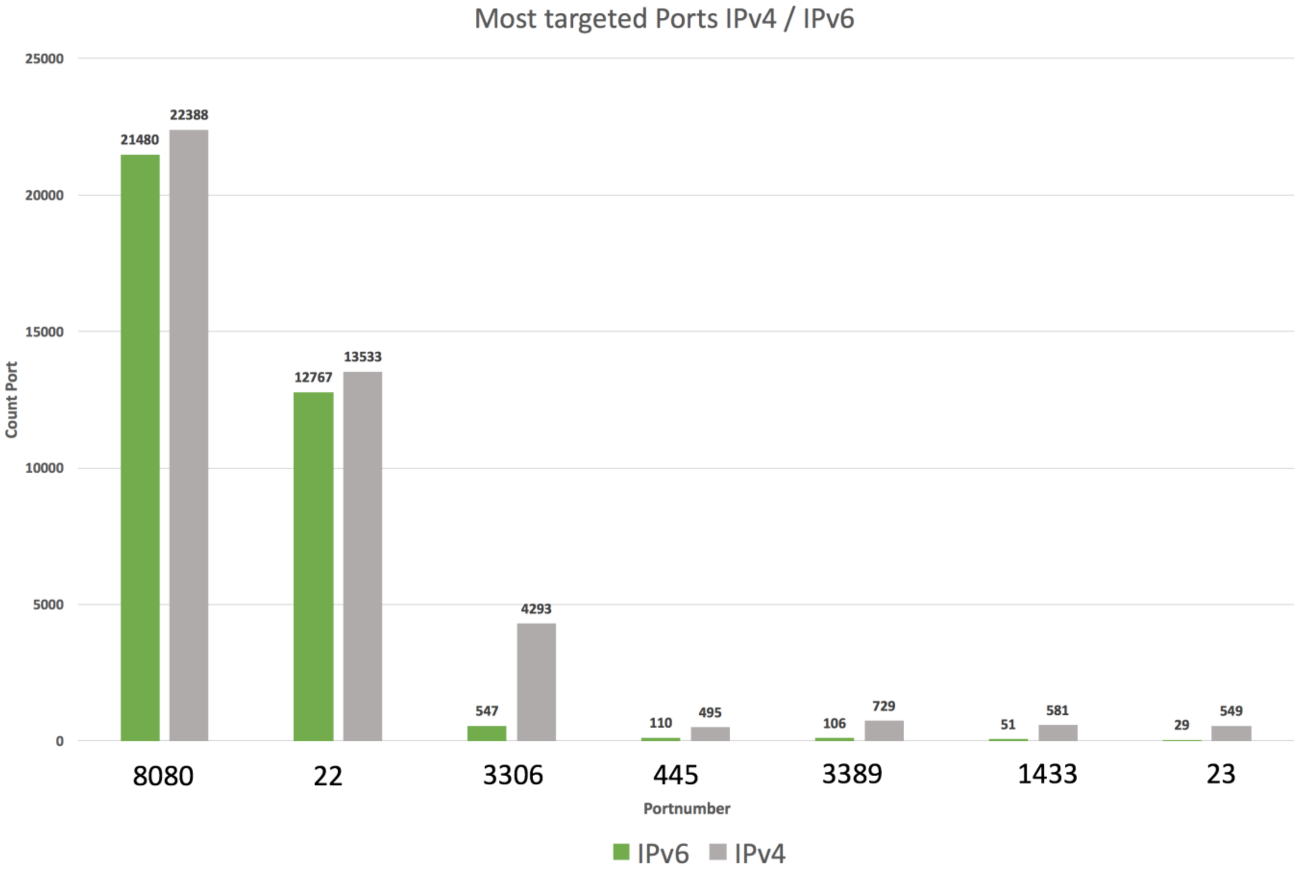


Percentage of global internet attack traffic during 4th quarter 2014, by targeted ports

Quelle::
Akamai Technologies
© Statista 2015

Additional Information:
Worldwide; 4th quarter 2014

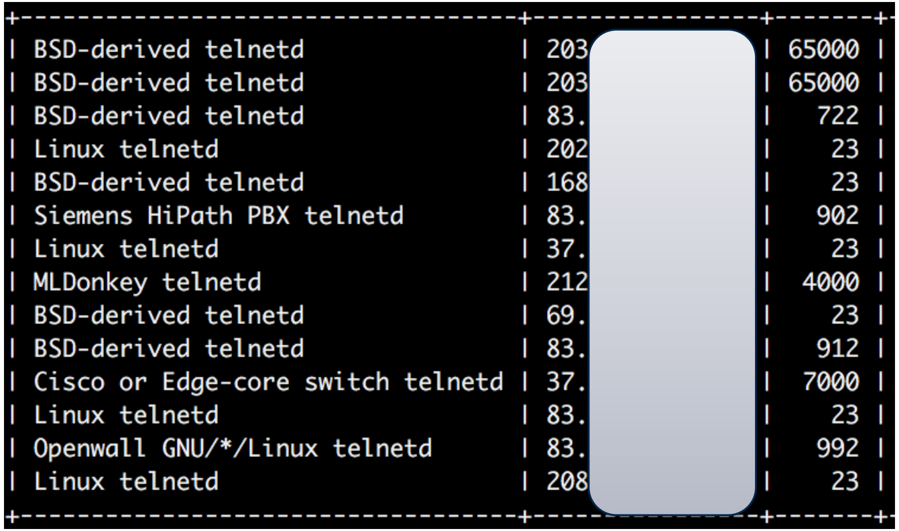
Results on this Research



Percentage

Port Number	% on IPv6 Addresses	% on IPv4 Addresses
8080	41,49%	43,25%
8080 without Cloudflare	0,57%	1,92%
22	24,66%	26,14%
3306	1,06%	8,29%
445	0,21%	0,96%
3389	0,20%	1,41%
1433	0,10%	1,12%
23	0,06%	1,06%

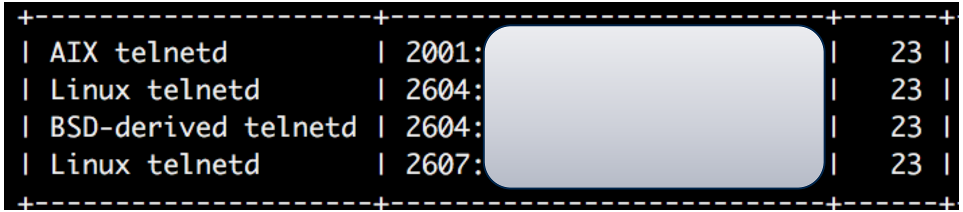
Results (Telnet on IPv4/IPv6)



```
+-----------------------------------+----------------+-------+
| BSD-derived telnetd               | 203[redacted]  | 65000 |
| BSD-derived telnetd               | 203[redacted]  | 65000 |
| BSD-derived telnetd               | 83.[redacted]  |   722 |
| Linux telnetd                     | 202[redacted]  |    23 |
| BSD-derived telnetd               | 168[redacted]  |    23 |
| Siemens HiPath PBX telnetd        | 83.[redacted]  |   902 |
| Linux telnetd                     | 37.[redacted]  |    23 |
| MLDonkey telnetd                  | 212[redacted]  |  4000 |
| BSD-derived telnetd               | 69.[redacted]  |    23 |
| BSD-derived telnetd               | 83.[redacted]  |   912 |
| Cisco or Edge-core switch telnetd | 37.[redacted]  |  7000 |
| Linux telnetd                     | 83.[redacted]  |    23 |
| Openwall GNU/*/Linux telnetd      | 83.[redacted]  |   992 |
| Linux telnetd                     | 208[redacted]  |    23 |
+-----------------------------------+----------------+-------+
```

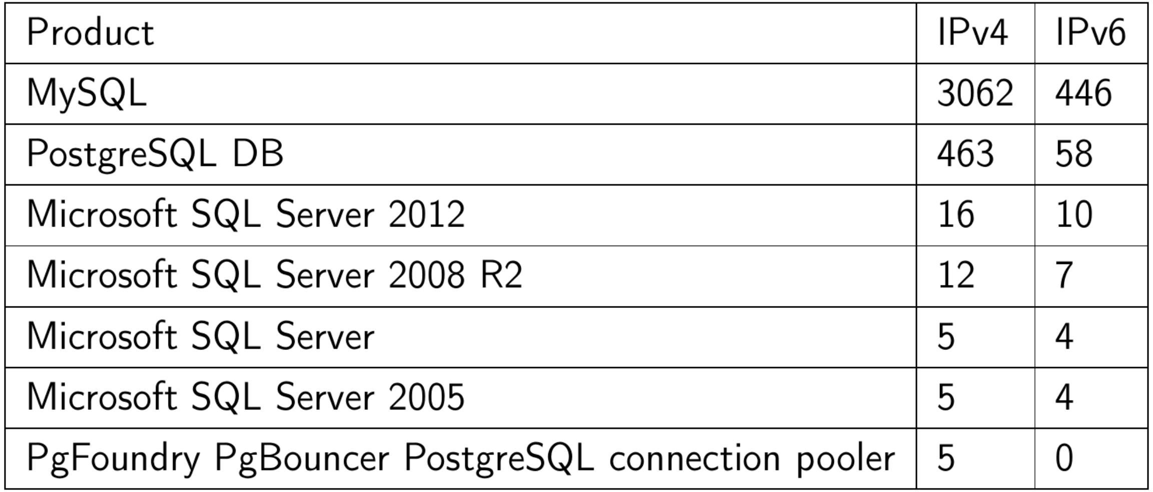
<- IPv4

IPv6 ->



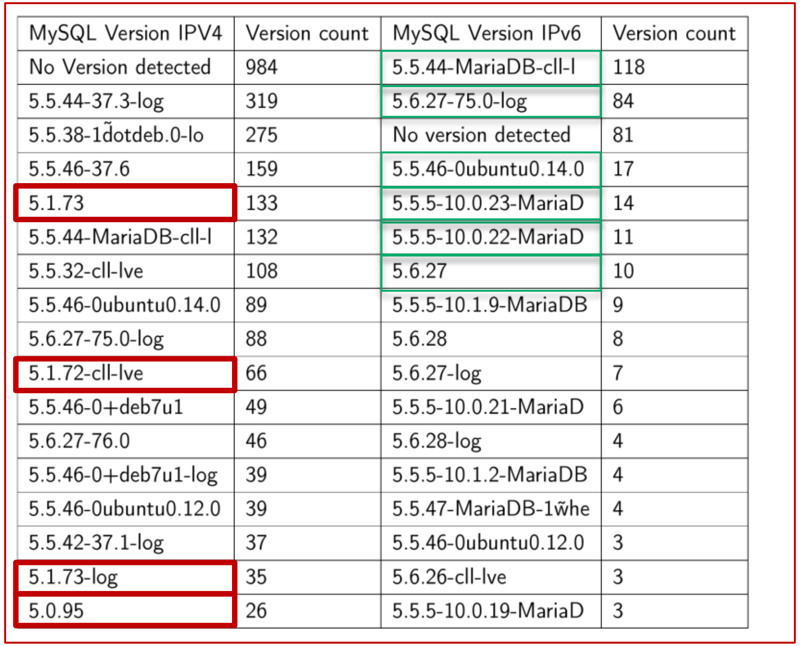
```
+---------------------+------------------------+------+
| AIX telnetd         | 2001:[redacted]        |   23 |
| Linux telnetd       | 2604:[redacted]        |   23 |
| BSD-derived telnetd | 2604:[redacted]        |   23 |
| Linux telnetd       | 2607:[redacted]        |   23 |
+---------------------+------------------------+------+
```

Results (SQL-Servers on IPv4/IPv6)



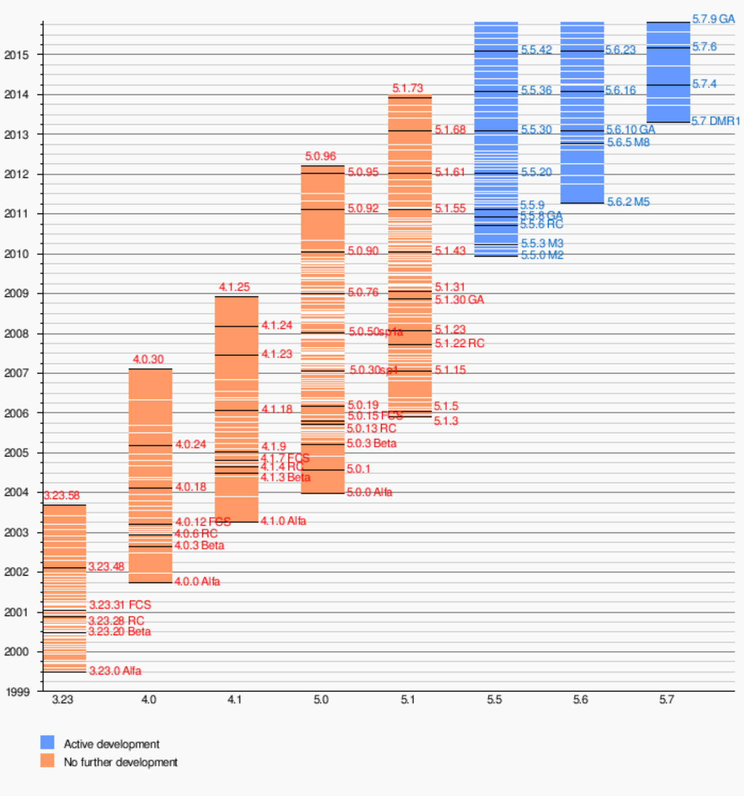
Product	IPv4	IPv6
MySQL	3062	446
PostgreSQL DB	463	58
Microsoft SQL Server 2012	16	10
Microsoft SQL Server 2008 R2	12	7
Microsoft SQL Server	5	4
Microsoft SQL Server 2005	5	4
PgFoundry PgBouncer PostgreSQL connection pooler	5	0

Looking a bit closer: MySQL



MySQL Version IPV4	Version count	MySQL Version IPv6	Version count
No Version detected	984	5.5.44-MariaDB-cll-l	118
5.5.44-37.3-log	319	5.6.27-75.0-log	84
5.5.38-1d̃otdeb.0-lo	275	No version detected	81
5.5.46-37.6	159	5.5.46-0ubuntu0.14.0	17
5.1.73	133	5.5.5-10.0.23-MariaD	14
5.5.44-MariaDB-cll-l	132	5.5.5-10.0.22-MariaD	11
5.5.32-cll-lve	108	5.6.27	10
5.5.46-0ubuntu0.14.0	89	5.5.5-10.1.9-MariaDB	9
5.6.27-75.0-log	88	5.6.28	8
5.1.72-cll-lve	66	5.6.27-log	7
5.5.46-0+deb7u1	49	5.5.5-10.0.21-MariaD	6
5.6.27-76.0	46	5.6.28-log	4
5.5.46-0+deb7u1-log	39	5.5.5-10.1.2-MariaDB	4
5.5.46-0ubuntu0.12.0	39	5.5.47-MariaDB-1w̃he	4
5.5.42-37.1-log	37	5.5.46-0ubuntu0.12.0	3
5.1.73-log	35	5.6.26-cll-lve	3
5.0.95	26	5.5.5-10.0.19-MariaD	3

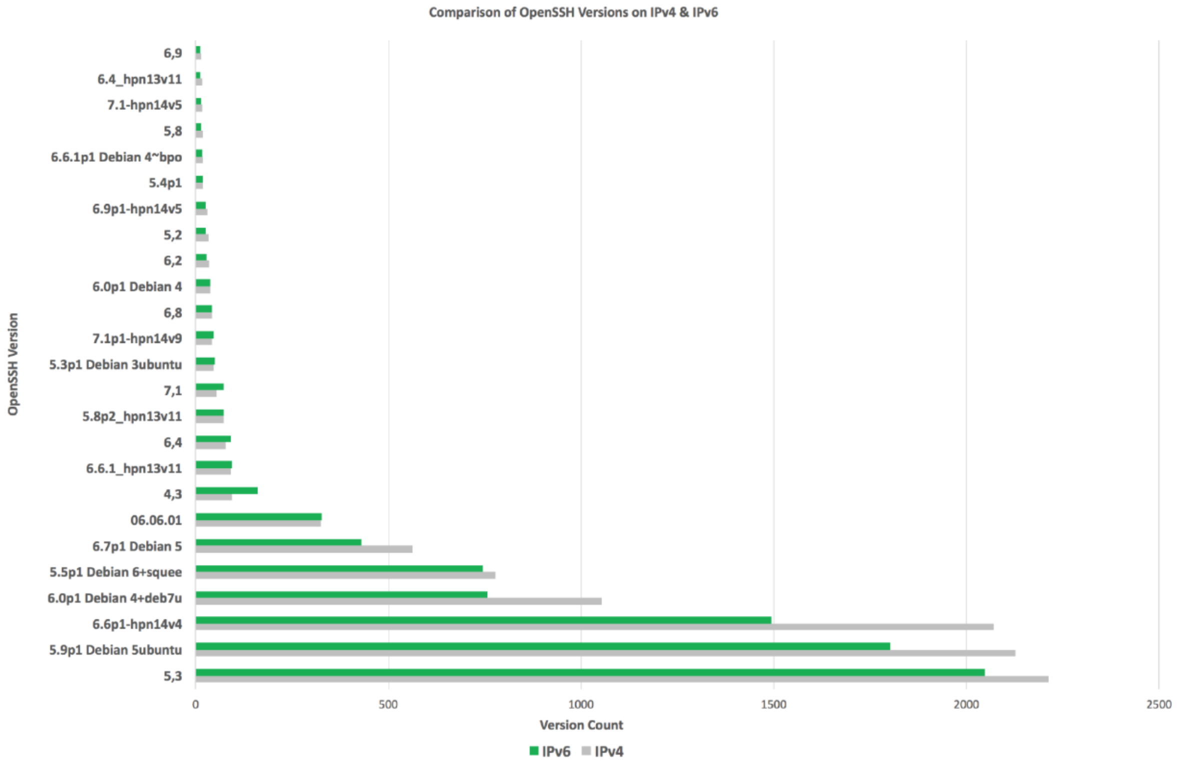
*MariaDB version numbers follow the MySQL's numbering scheme up to version 5.5.



Results (SSH-Servers on IPv4/IPv6

Product	IPv4	IPv6
OpenSSH	10154	8640
Linksys WRT45G modified dropbear sshd	2638	2870
SunSSH	3	2
Dropbear sshd	6	2
Cyberoam firewall sshd	1	1
SCS sshd	0	1
VanDyke Vshell sshd	1	0
WeOnlyDo sshd	1	0

Looking a bit closer : OpenSSH



Recommandation

- Always check both IPv4 and IPv6
- Check yourself using our script ☺ (soon on github.com)
- Check your security devices for IPv6 support

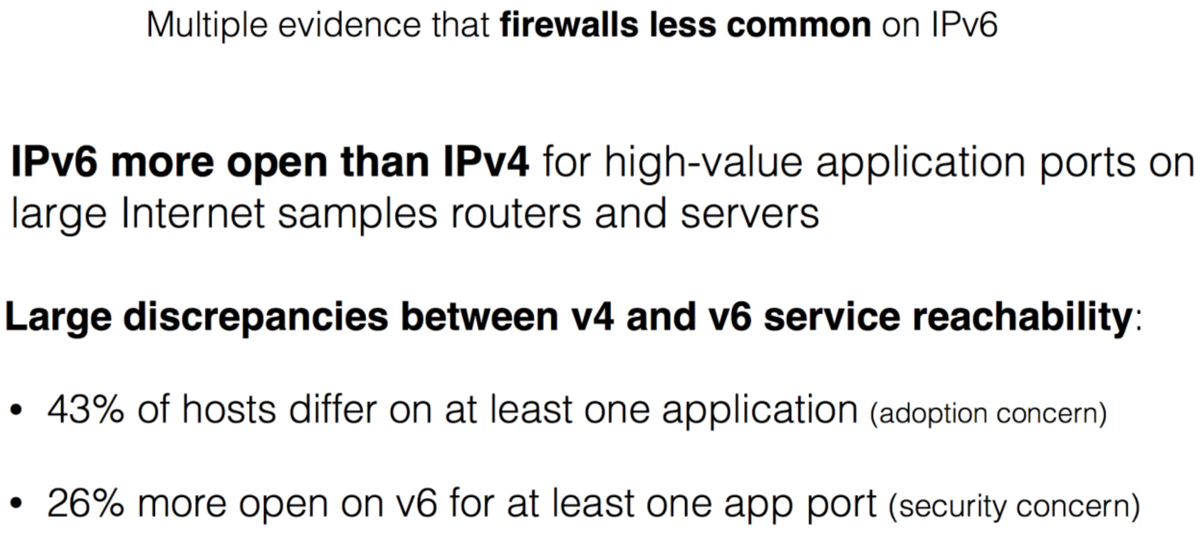
Conclusion

ERNW
providing security.

- IPv4 Ports are about six times more open as they are on IPv6
- 40% of the dual-stack hosts belong to Cloudflare CDN
- There is a higher Patch-Level of MySQL on IPv6
- Potentially vulnerable Ports are more likely to find on IPv4
- IPv6 is there and use it ☺

Don‘t forget to lock the Backdoor (Dec. 2015)

Mark Allman



Multiple evidence that **firewalls less common** on IPv6

IPv6 more open than IPv4 for high-value application ports on large Internet samples routers and servers

Large discrepancies between v4 and v6 service reachability:

- 43% of hosts differ on at least one application (adoption concern)
- 26% more open on v6 for at least one app port (security concern)

Questions?

@itsecurityguard

https://www.insinuator.net/