Turris

Who is attacking our routers?

Michal Hrušecký • Michal.Hrusecky@turris.com

TURRIS

How it all started

Big question:

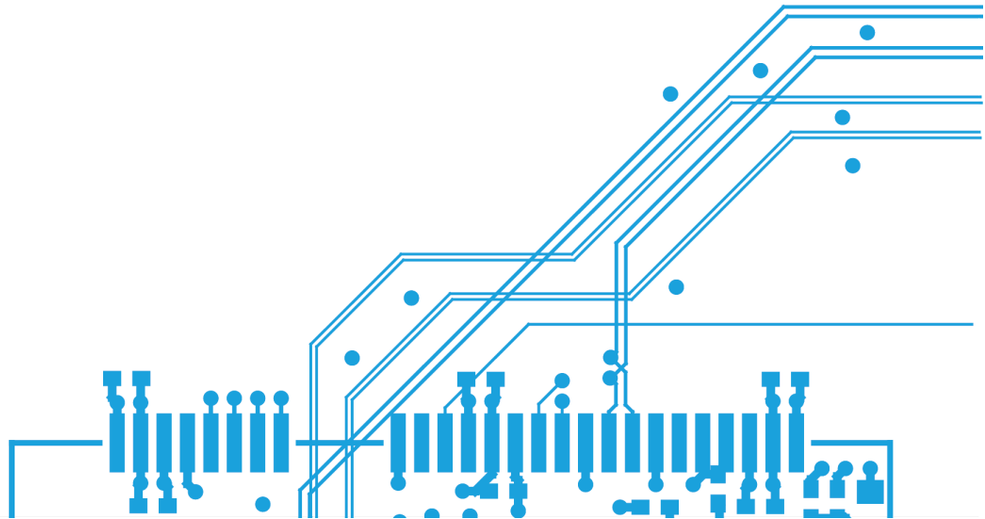
How safe are home users from network attacks?

Is anybody attacking them?

How often?

What kind of attacks are they facing?

Is it safe to have a public IPv4?



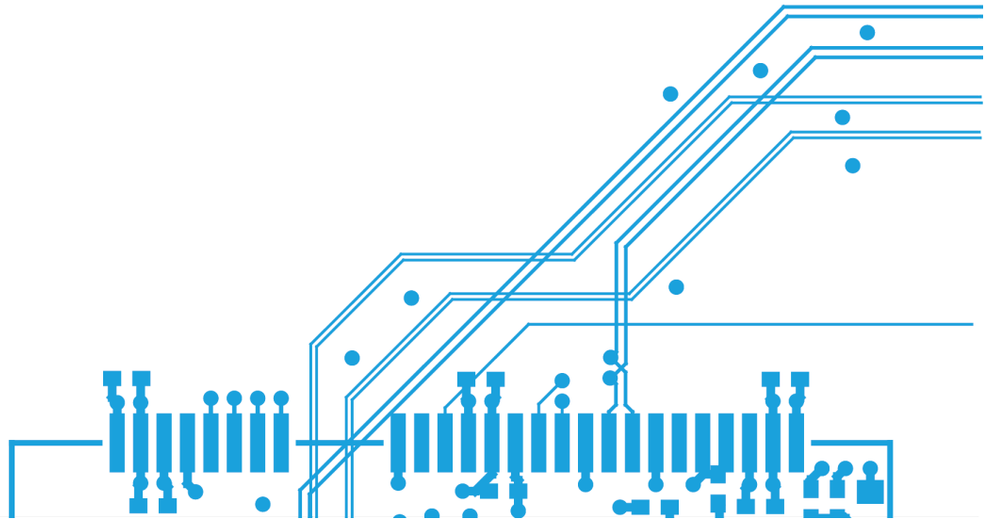
Turris is born

Let’s make a security probe 💪

- give it to people for free
- collect data about the attacks from the outside

How to do it?

- has to be the main gateway in every home
  - it has to be able to do at least NAT 🤔
- people have to be willing to install it and give us data 🤔
  - let’s make it more than just a simple pass through gateway
  - let’s make a full fledged router! 💡



Fast forward ⇒ We are in retail!

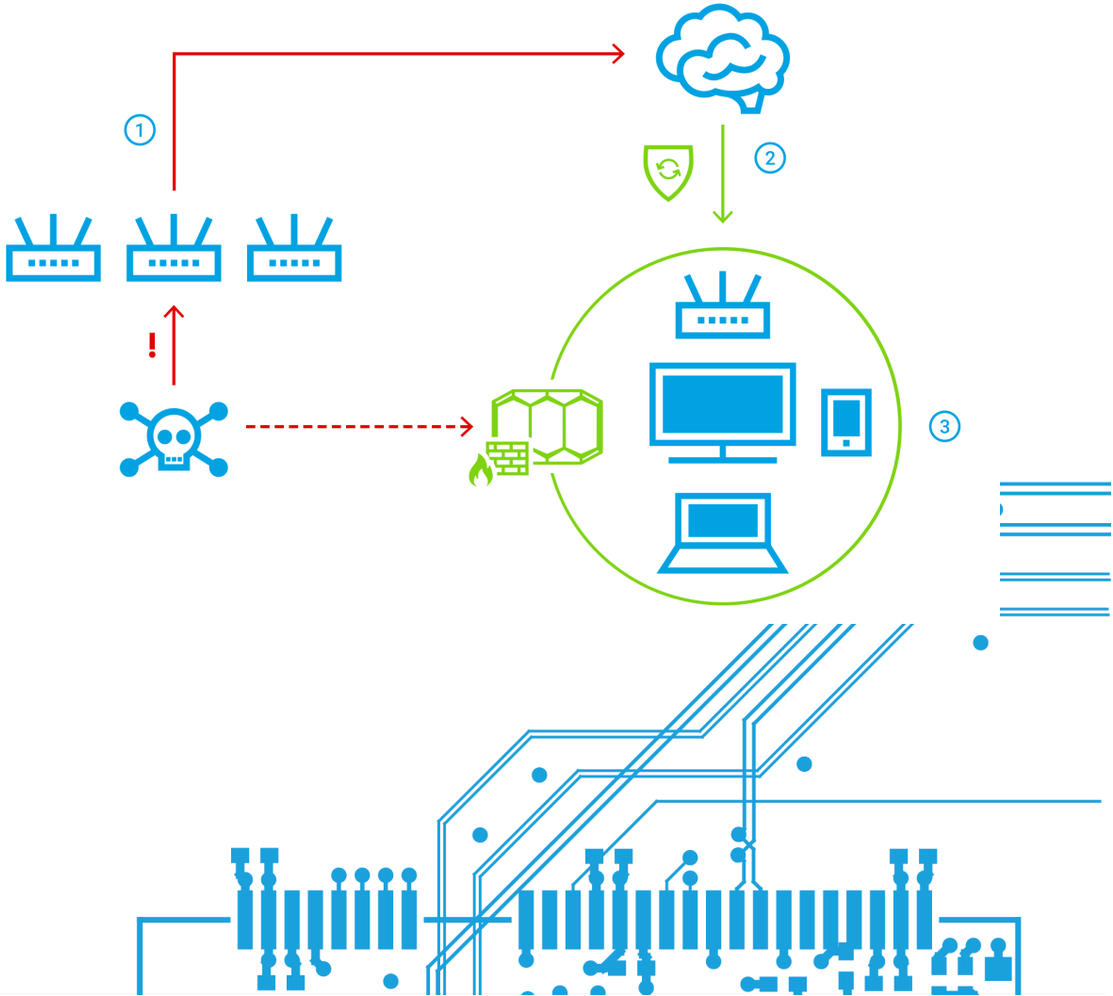
Turris Omnia NG

- 4 core ARMv8 @ 2,2 GHz
- 2 x 10 GBps SFP+
- 4 x 2.5 GBps RJ45
- 2G RAM

Back to the security research

Turris Sentinel

- nowadays opt-in
- minimal honeypots
  - http, telnet, smtp, ftp
- ssh honeypot (on CZ.NICs servers)
- firewall logs
- dynamic firewall
  - https://view.sentinel.turris.cz

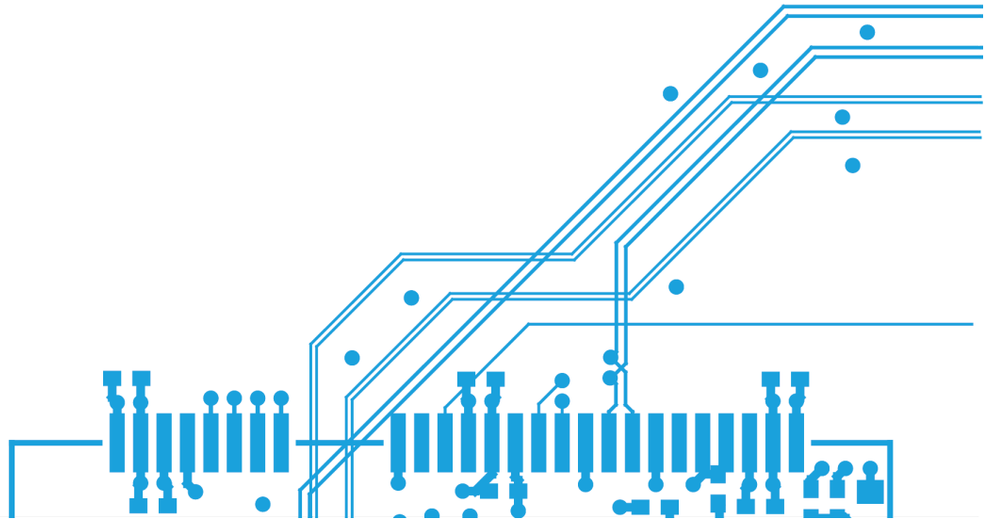


The IPv6 part

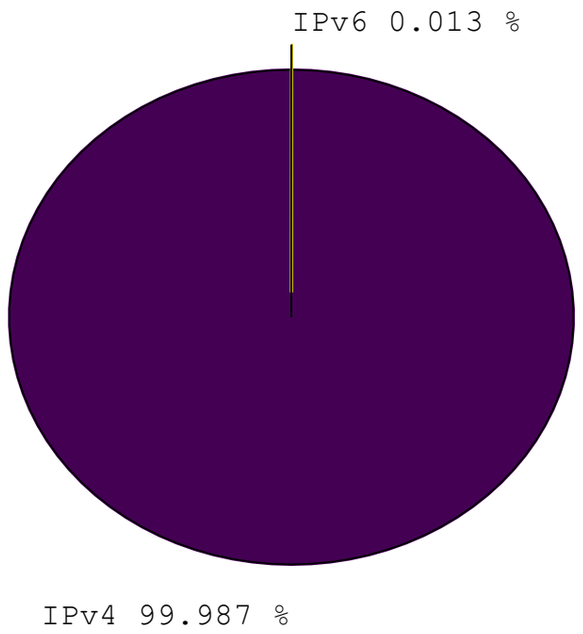
- we started collecting data from IPv6 as well
  - originally insignificant, so implementation was delayed
  - since 2024 we are collecting again
- there is a bias
  - about third of updates is over IPv6

New questions!

- Are there any attackers using IPv6?
- Are attackers using IPv6 different? How?

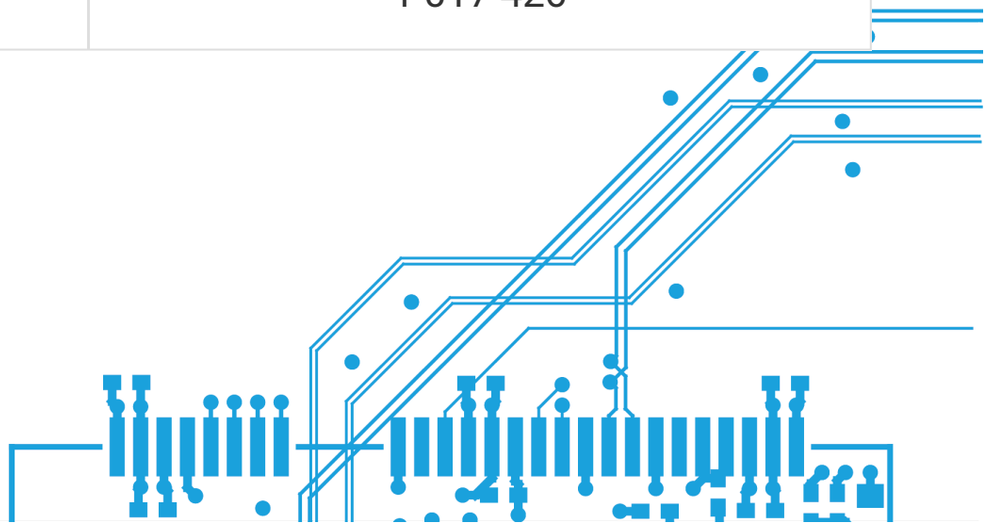


Incidents per protocol

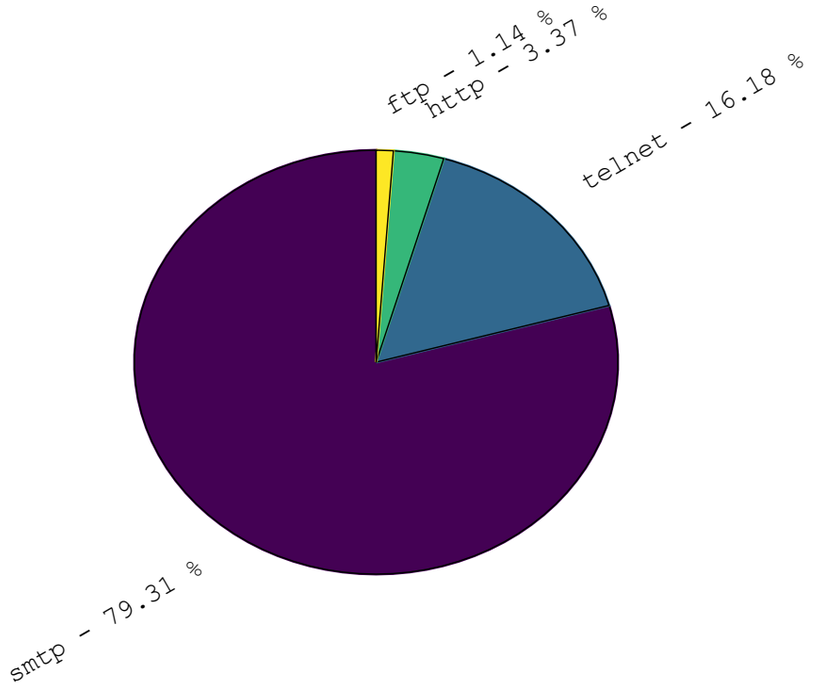


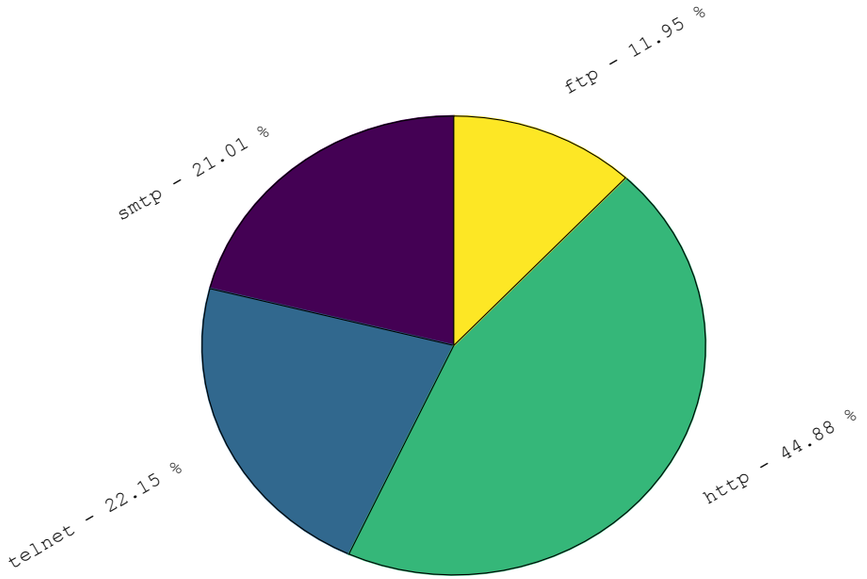
Incidents per protocol (in numbers)

Protocol	IPv4	IPv6
smtp	6 043 800 347	213 791
telnet	1 232 963 285	225 369
http	256 975 885	456 643
ftp	86 757 664	121 623
total	7 620 497 181	1 017 426



Incidents per protocol (in pies)



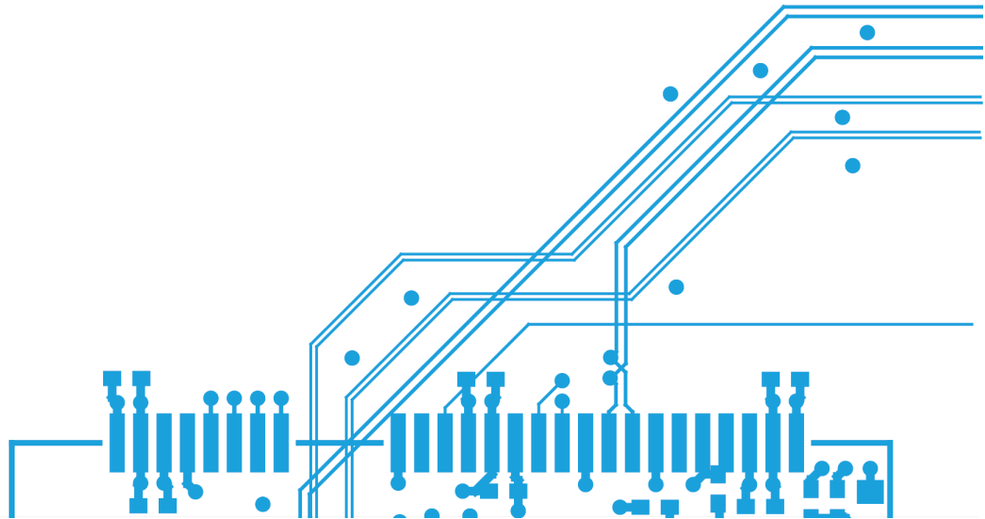


Theory

Attackers might be clustered.

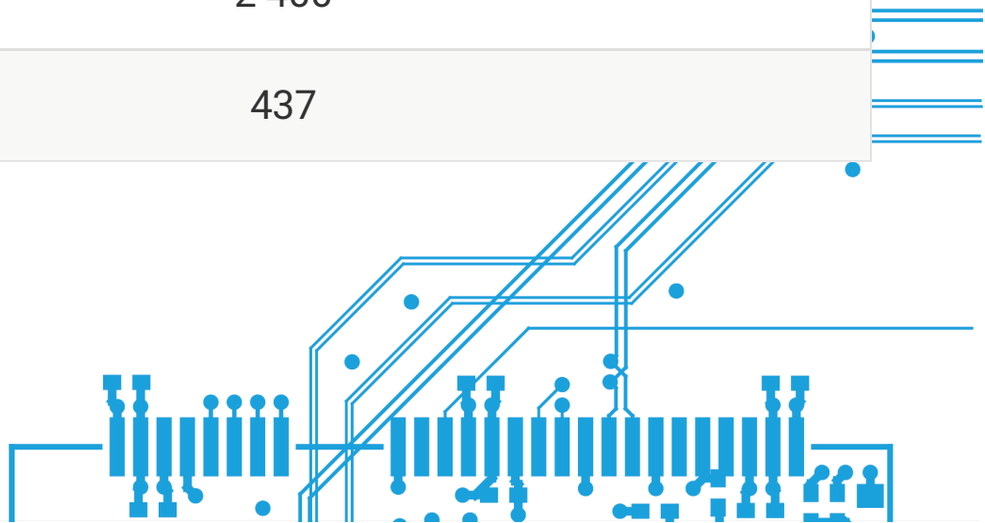
- using dynamic IP
- using more IPs from their segments
- using "attacker friendly" networks

Let’s verify the theory!



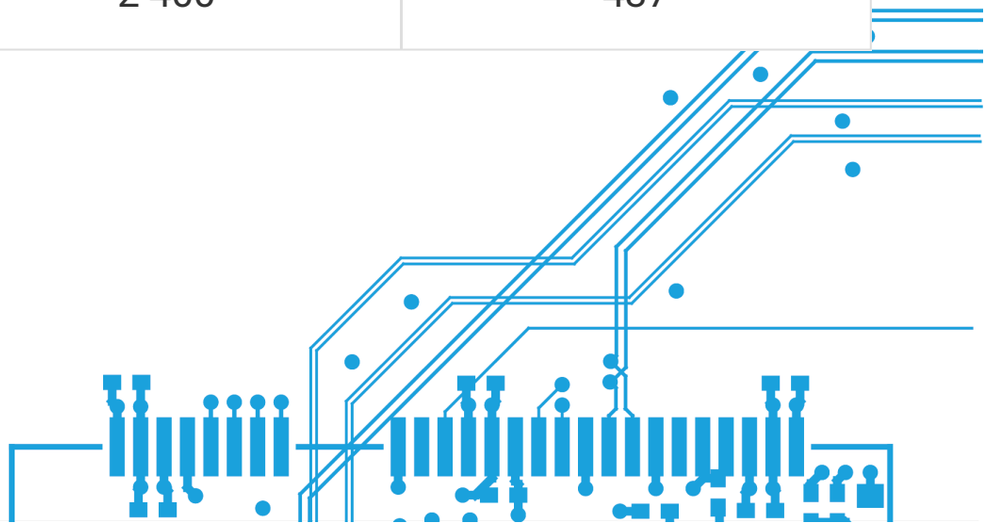
Unique attackers IPs

Network	Unique IPs
IPv4 /32	4 689 342
IPv4 /24	894 514
IPv6 /64	3 682
IPv6 /56	3 189
IPv6 /48	2 400
IPv6 /32	437

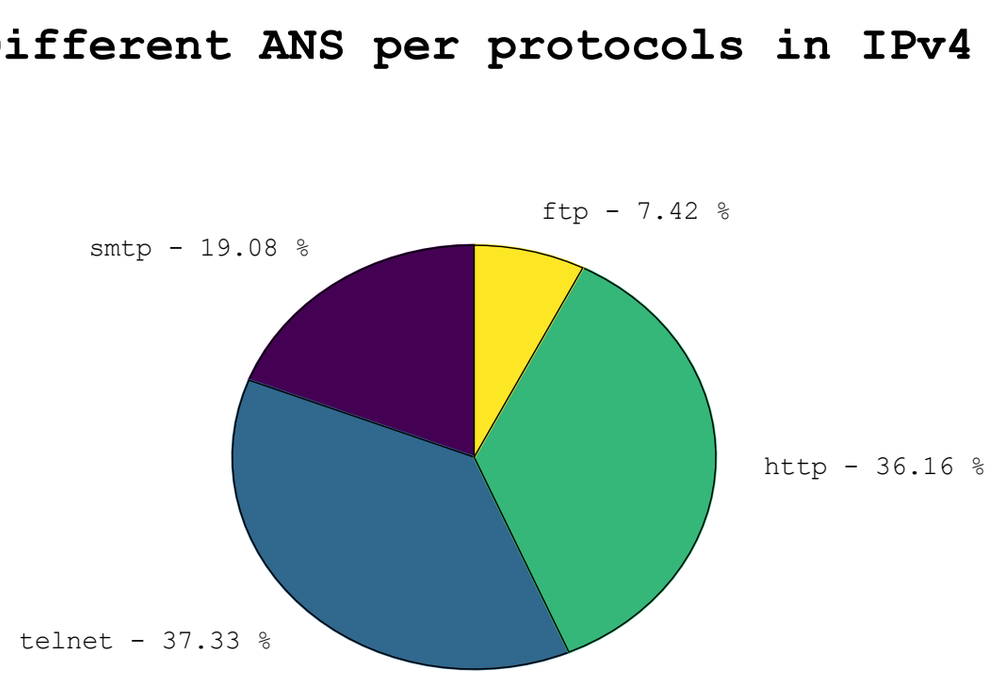


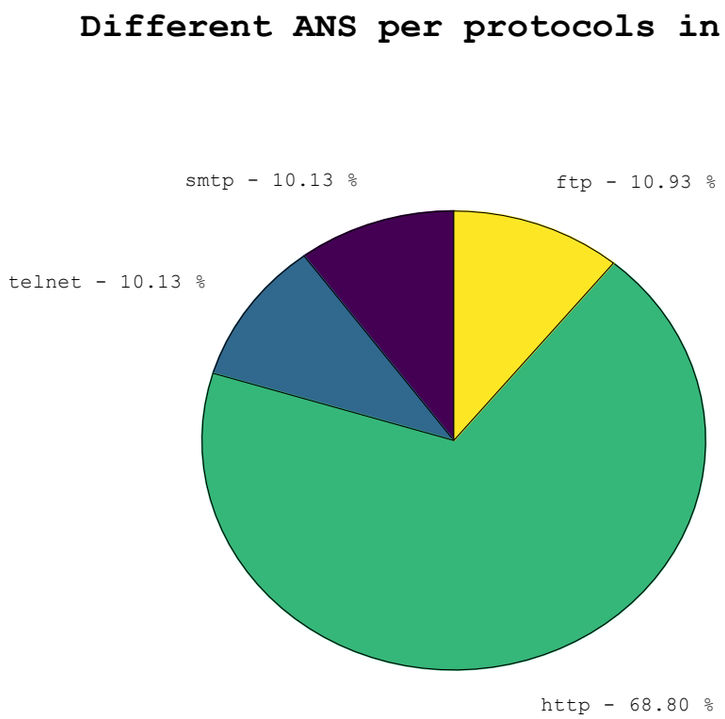
How do subnets behave?

Protocol	IPv4 /24	IPv6 /56	IPv6 /48	IPv6 /32
smtp	78 992	115	104	62
telnet	654 290	592	582	68
http	383 746	3 094	2 319	425
ftp	38 421	592	583	73
total	894 514	3 189	2 400	437



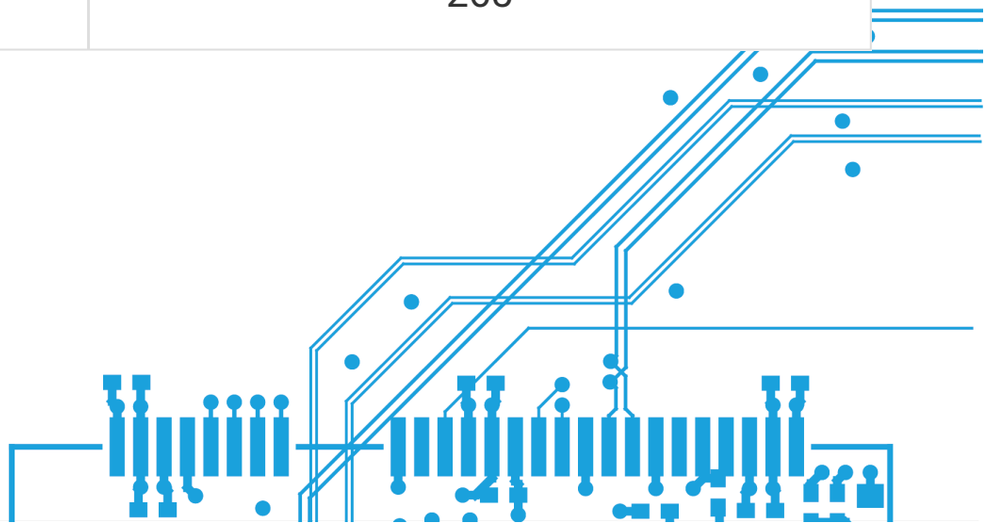
Unique ASNs (pies)





Unique ASNs

Protocol	IPv4	IPv6
smtp	8 227	38
telnet	16 093	38
http	15 589	258
ftp	3 200	41
total	21 926	265



Top IPv4 countries

Country	Number of "malicious" IPs
India	1 158 550
China	761 783
United States of America	410 325
Taiwan	197 593
Russian Federation	148 469
Iran	143 539
Brazil	131 501
Thailand	131 037

Top IPv6 countries

Country	Number of "malicious" IPs
Germany	1 727
United States of America	480
France	371
Viet Nam	346
China	89
Austria	53
India	48
Singapore	47

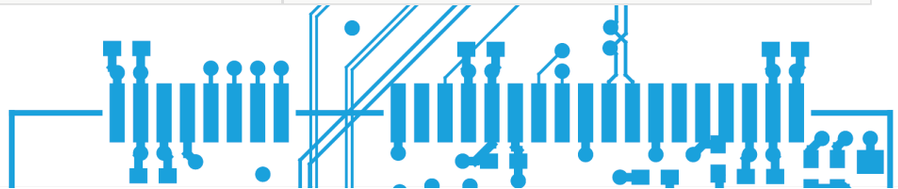
Are attackers faithful or needy?

Promiscuity

Protocol	Mean	Median	Maximum
IPv4	14,51	3	1 766
IPv6	3,55	1	379

Neediness

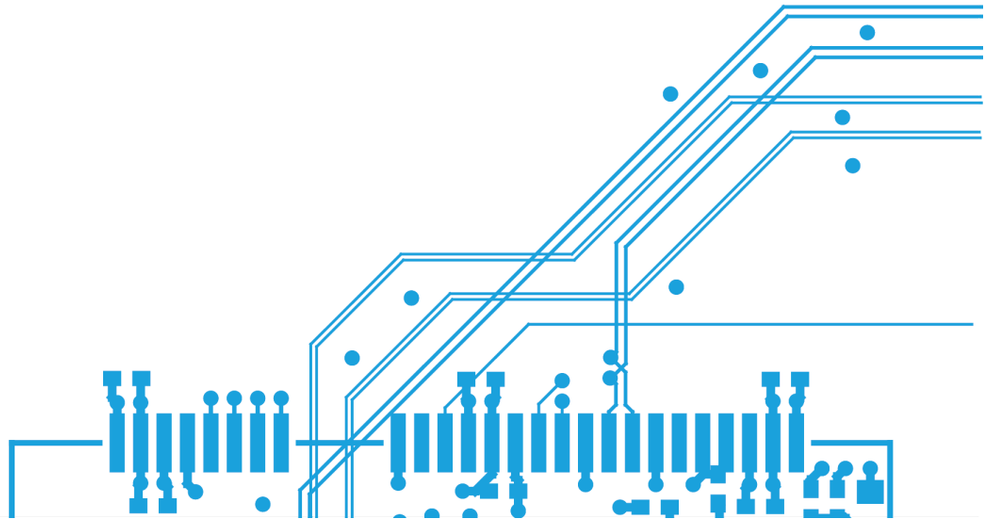
Protocol	Mean	Median	Maximum
IPv4	250,51	2	7 622 845
IPv6	15,19	2	9 841



Conclusion

- There are IPv6 attackers
  - And there is high chance that they are German
- They are much less common
- They are more polite
- They prefer modern technologies

⇒ IPv6 Internet is much nicer Internet!



Thank you

Few useful links

🐘 @turris@fosstodon.org

https://www.turris.cz

https://view.sentinel.turris.cz

https://docs.turris.cz