Fast Internet-Scanning – Challenges and new approaches

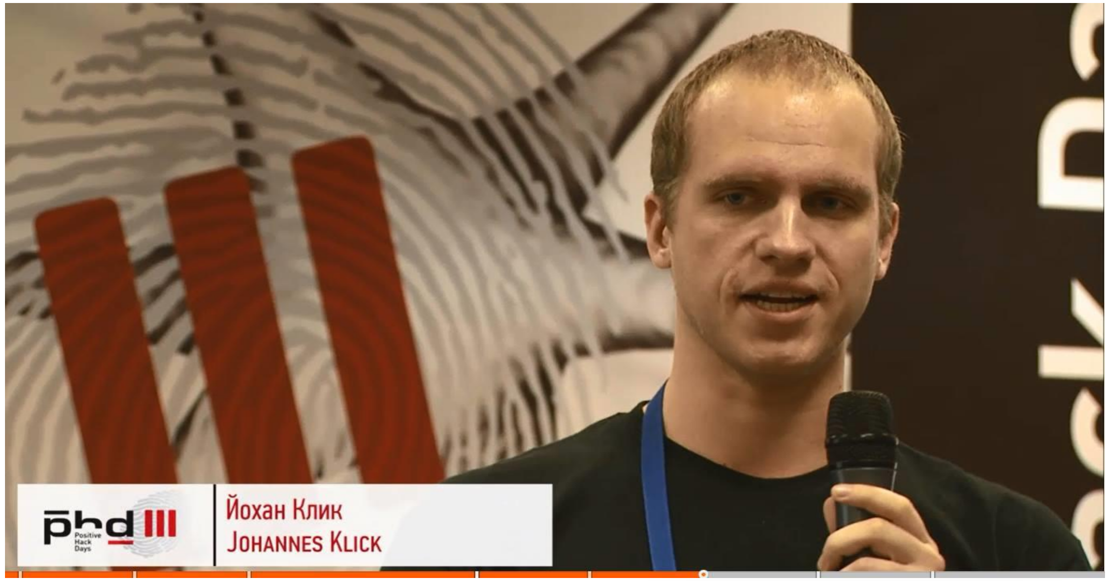
Or how to become your own ISP

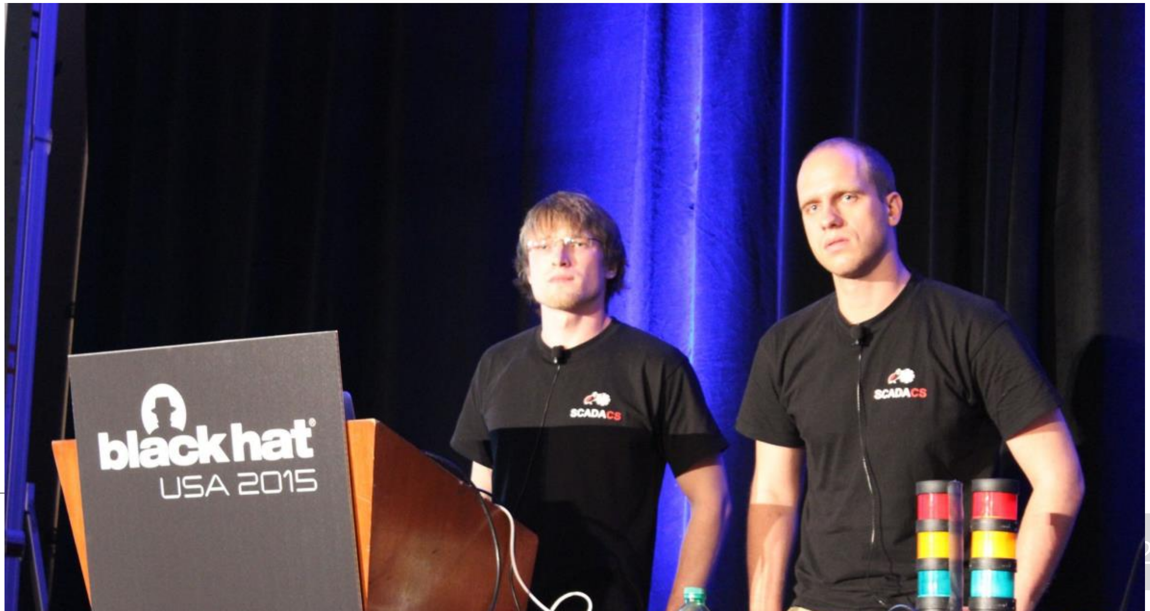
May I introduce myself?

- **Johannes Klick,**
- CEO | Co-Founder of Alpha Strike Labs
- Internet Scanning Expert, ICS/OT Hacker

- Discovered vulnerabilities:
  - CVE-2015-2177, DoS of Siemens SIMATIC S7-300
  - CVE-2014-6617, Softing FG-100 PB
  - CVE-2015-6616, Softing FG-100 PB XSS
  - Security Advisory 2015/12/02 (Traeger Industry Comp. GmbH) S7 Firewall

- Publications on academic and applied security conferences:
  - Blackhat 2015, USA | PHDays III, Russia | ACM IMC | ACM SIGSAC | IEEE CNS | …





Motivation for this Talk

FAQ: What about Shodan.io?

Shodan:

- No raw data, not free
- No clean snapshot scans, same host appears multiple times due to dynamic IPv4 addresses

FAQ: What about Censys.io?

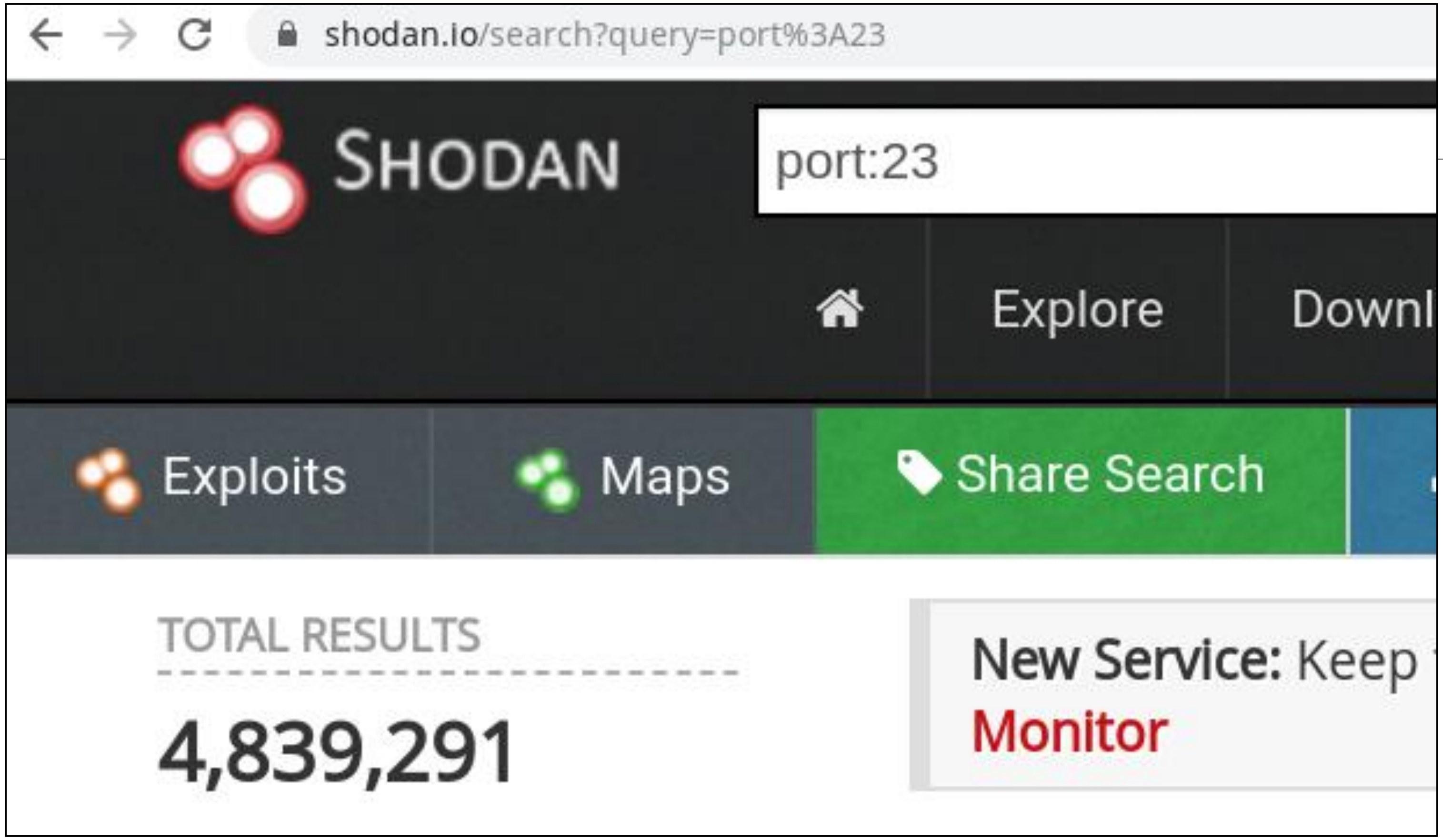
Censys:

- No raw data, not free
- Some inconsistencies in the database

Both platforms know what are you looking for!

What are they doing with this data?

Who might be interested in this data?



TOTAL RESULTS

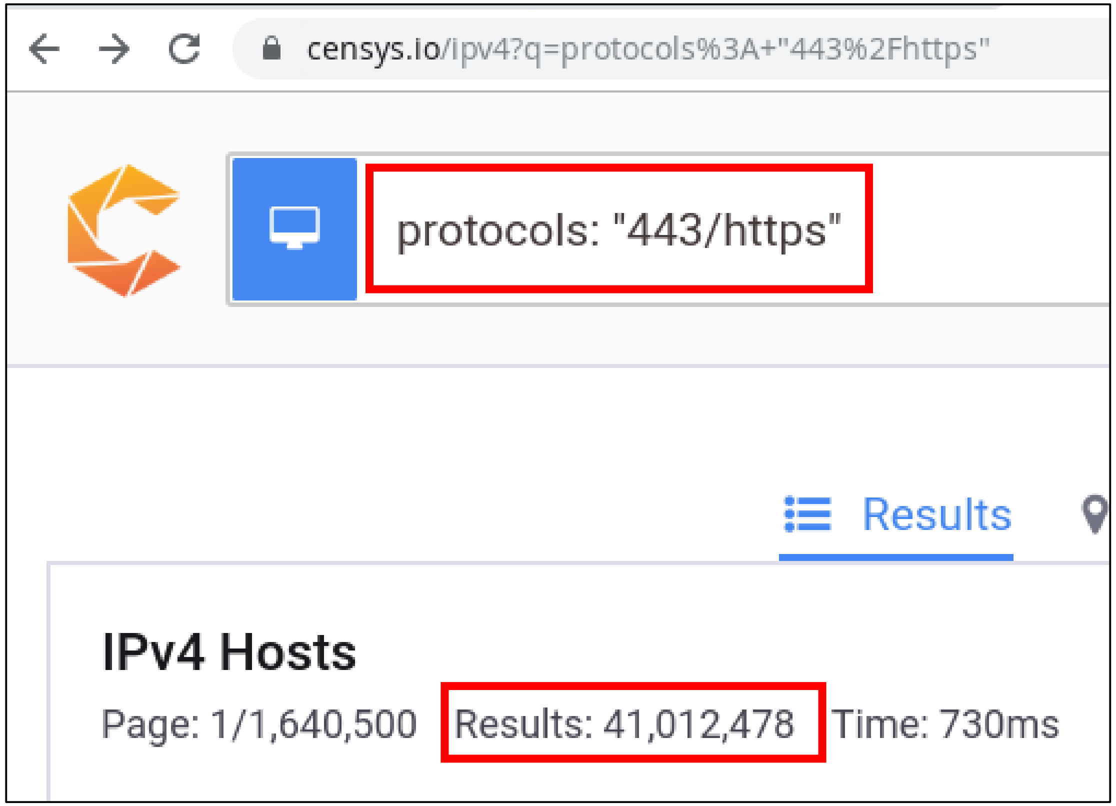
4,839,291

New Service: Keep
Monitor

No clean snapshot scans, same host appears multiple times
due to dynamic IPv4 addresses. This increases the number of results -.-

Our Scans	Censys	Shodan
3,137,164	3,069,539	4,839,291

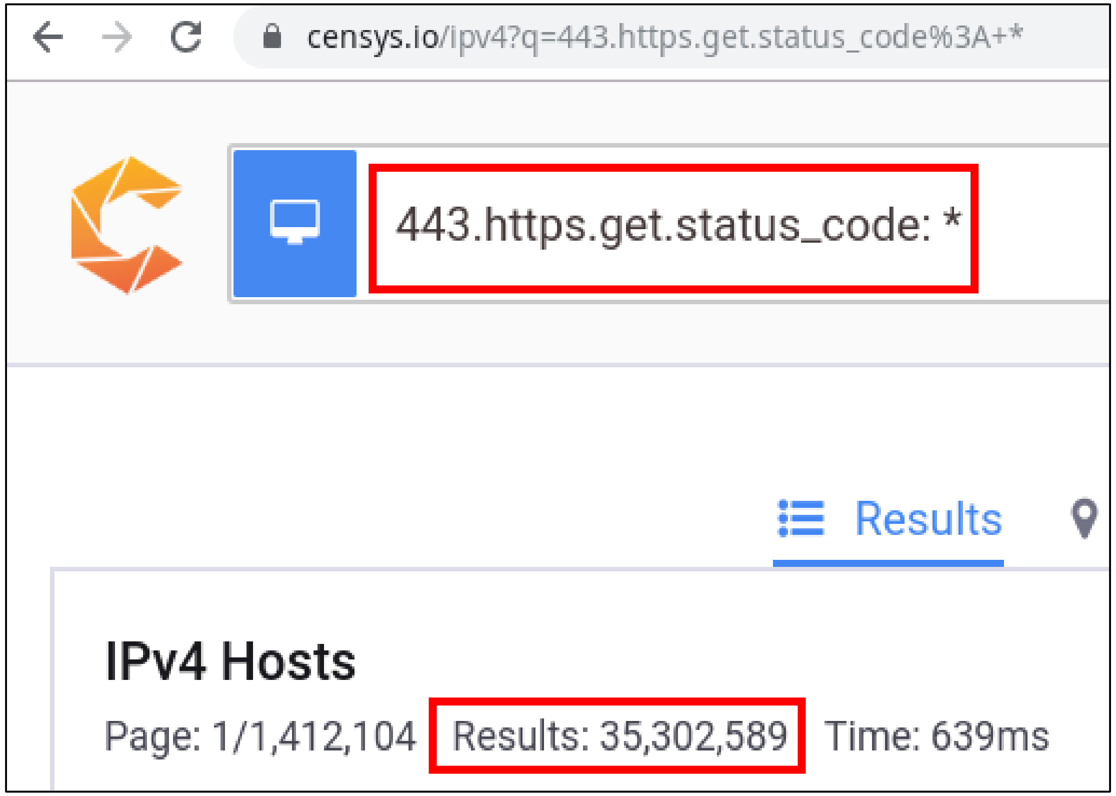
Censys Inconsitencies


censys.io/ipv4?q=protocols%3A+"443%2Fhttps"

protocols: "443/https"

IPv4 Hosts

Page: 1/1,640,500 Results: 41,012,478 Time: 730ms


censys.io/ipv4?q=443.https.get.status_code%3A+*

443.https.get.status_code: *

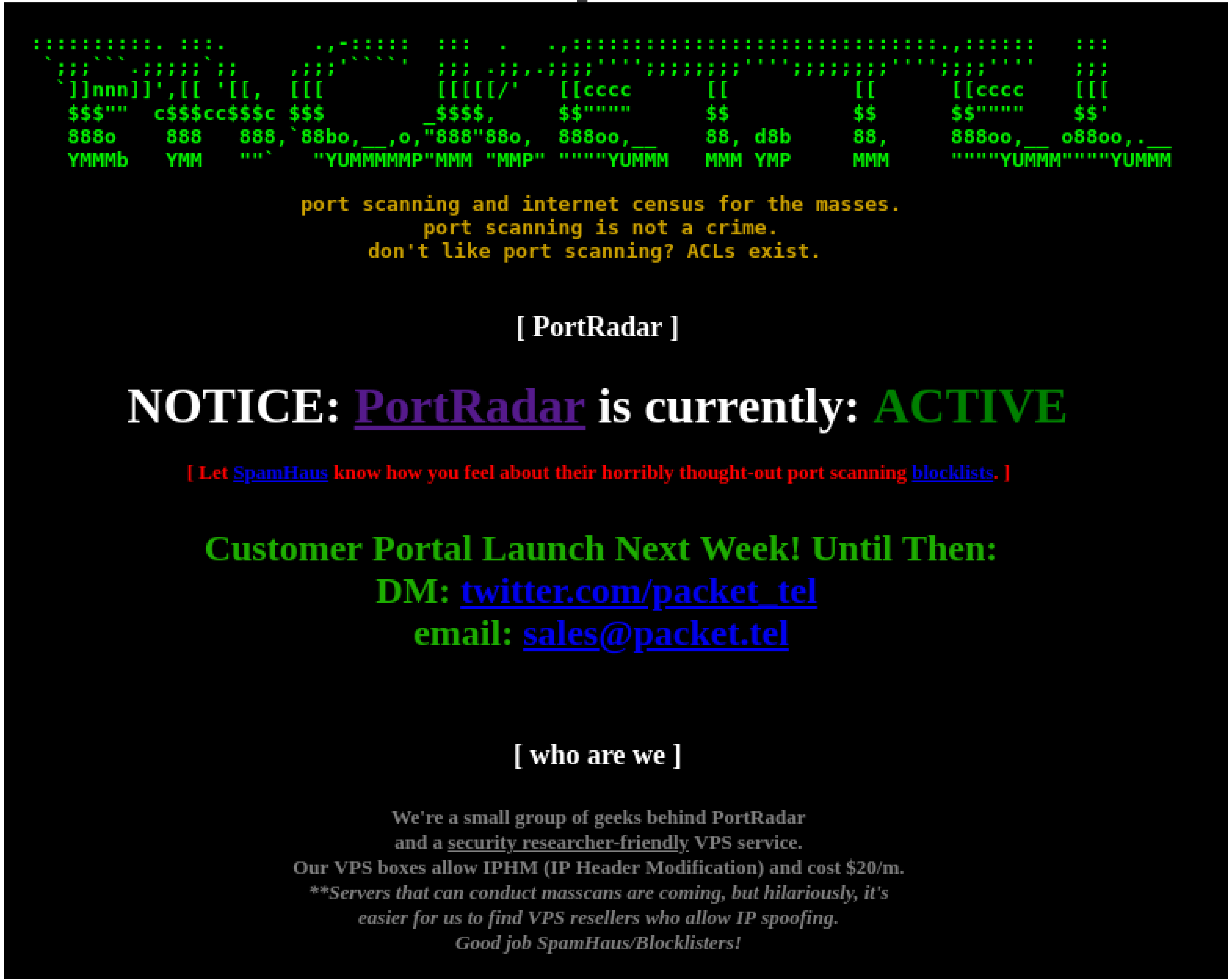
IPv4 Hosts

Page: 1/1,412,104 Results: 35,302,589 Time: 639ms

41 vs 35 million HTTPS hosts?

A status code is required for a full HTTP(S) handshake

Packet.tel … port scans only using masscan for ~2hours per scan



```
:::::::::::. :::.       .,-:::::  :::  .   .,::::::::::::::::::::::::::::::::.,::::::   :::
 `;;;```.;;;;;;`;;    ,;;;'````'  ;;; .;;,.;;;;'''';;;;;;;;''''';;;;;;;;''''';;;;''''   ;;;
  `]]nnn]]',[[ '[[,  [[[          [[[[[/'   [[cccc      [[           [[      [[cccc    [[[
   $$$""   c$$$cc$$$c $$$        _$$$$,     $$"""""     $$           $$      $$"""""   $$'
   888o    888   888,`88bo,__,o,"888"88o,  888oo,__    88, d8b      88,     888oo,__ o88oo,.__
   YMMMb   YMM   ""`   "YUMMMMMP"MMM "MMP" """"YUMMM   MMM YMP      MMM     """"YUMMM""""YUMMM
```

port scanning and internet census for the masses.
port scanning is not a crime.
don't like port scanning? ACLs exist.

[PortRadar]

NOTICE: PortRadar is currently: ACTIVE

[Let SpamHaus know how you feel about their horribly thought-out port scanning blocklists.]

Customer Portal Launch Next Week! Until Then:
DM: twitter.com/packet_tel
email: sales@packet.tel

[who are we]

We're a small group of geeks behind PortRadar
and a security researcher-friendly VPS service.
Our VPS boxes allow IPHM (IP Header Modification) and cost $20/m.
***Servers that can conduct masscans are coming, but hilariously, it's*
easier for us to find VPS resellers who allow IP spoofing.
Good job SpamHaus/Blocklisters!

Motivation for this Talk

I am interessted in the distribution of (vulnerable or exotic) network services on the Internet over the time, AS and BGP prefixes.

This talk will explain how to build a framework for repeated global Internet scans with good data quality.

Content of this talk:

- **50% How to scan the Internet in the right way.**
  - Hardware setup (Server for ~30.000 Euro)
  - Network setup (multiple VPS vs Colocation)
  - Scanning strategy & software (architecture and principles, elastic search optimizations)
  - Data enrichment (GeoIP, BGP, AS, Whois)
- **50% Scan results investigations**
  - Network topology maps of autonomous systems (AS)
  - Distribution of vulnerable Services
  - Complex combination analyses and interesting Results

How to scan

- **#1st try:**
  - Take a very fast scanner and scan the internet from a single IP address?
  - Bad idea, you will get blocked very fast and receive a lot of abuse messages
- **#2nd try:**
  - Rent ~20 vserver for $4-10USD per month (globally distributed)?
  - Results might be better, but nevertheless you have a big abuse message problem and will get kicked out by your vserver provider
- **#3rd try:**
  - Rent a /29 IPv4 address block from an ISP, get you own whois DB entry with special abuse m@il contact
  - Result: Some abuse messages are going directly to ISP/Maintainer
  - But still a lot of abuse and block messages

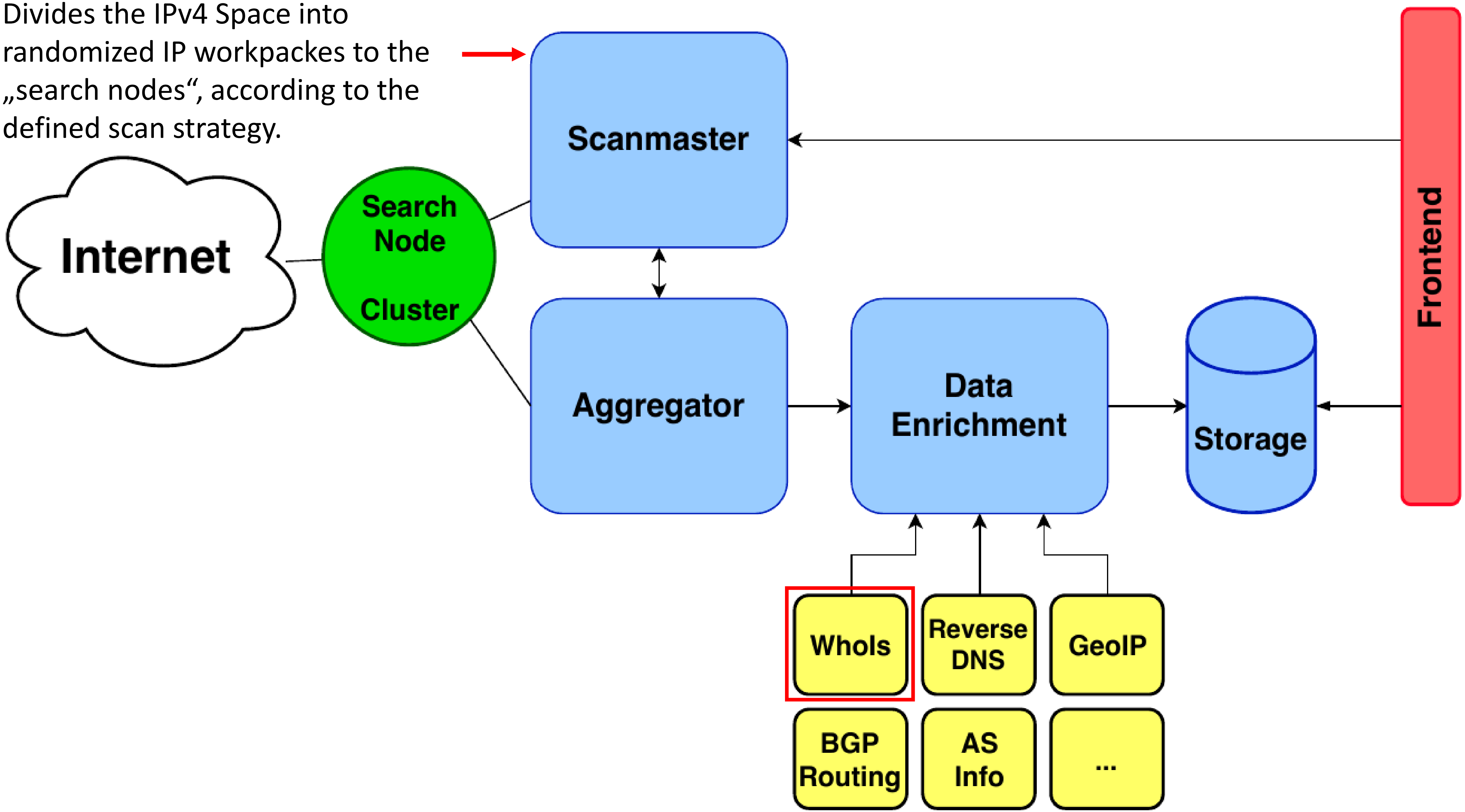
How to scan

- **#4 Final Solution – BECOME YOUR OWN ISP**
  - Become a RIPE member: Get your own Autonomous System (AS) and a /22 IPv4 network:
    - Sign-up fee: 2000€, membership fee 1400€ / year
  - Rent 2 different colocation spaces incl. an additional /29 for +350€ / month
  - Buy a server for ~30.000€
  - Use auto replies for abuse messages to inform about your research project
  - Provide a way to get excluded from scans (blacklist)

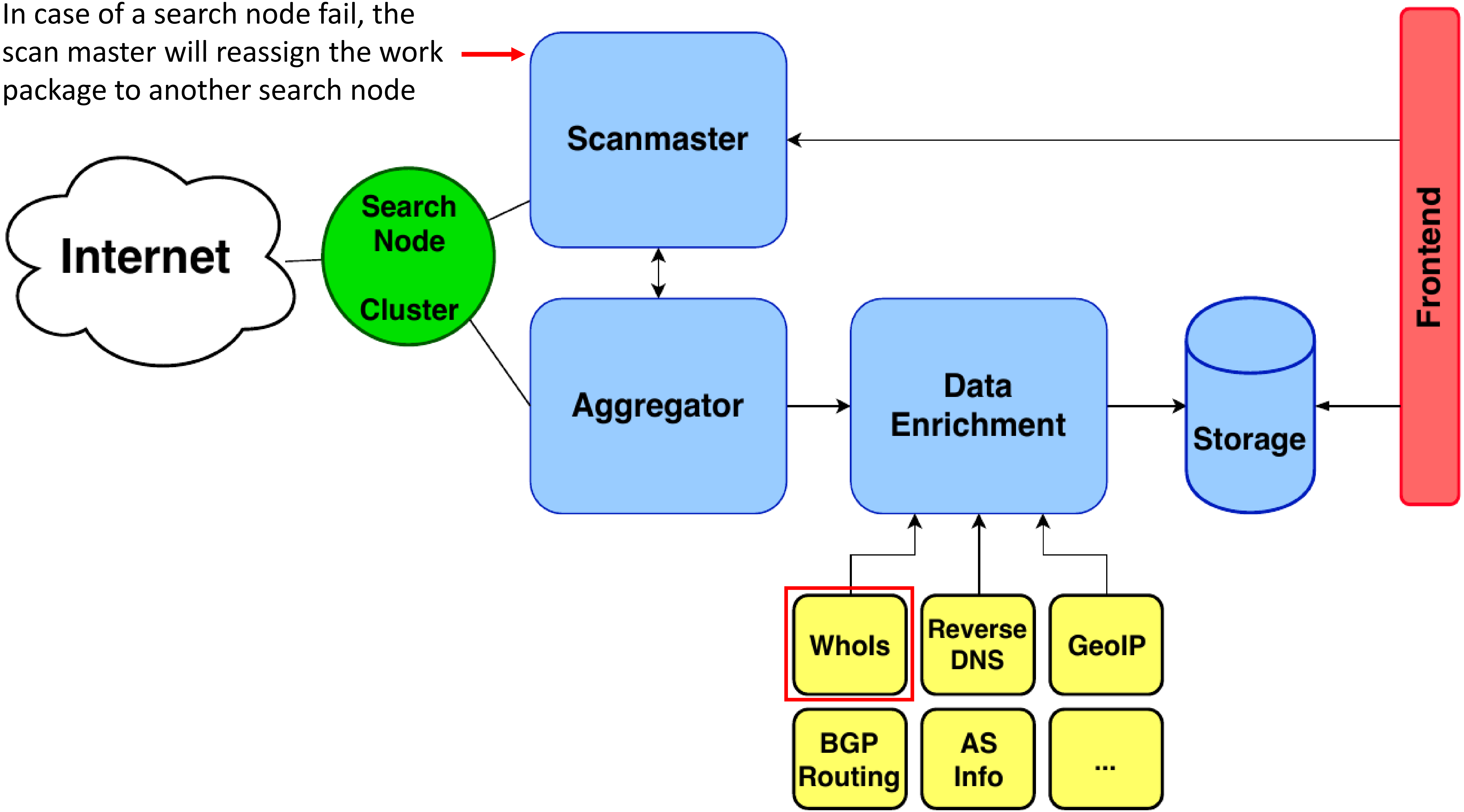
  Result:
  - Abuse messages reduced by ~90%
  - Messages about being blocked massivly reduced.
  - Abuse message handling 100% done yourself

More than 1024 different source IP addresses help very much! ;-)

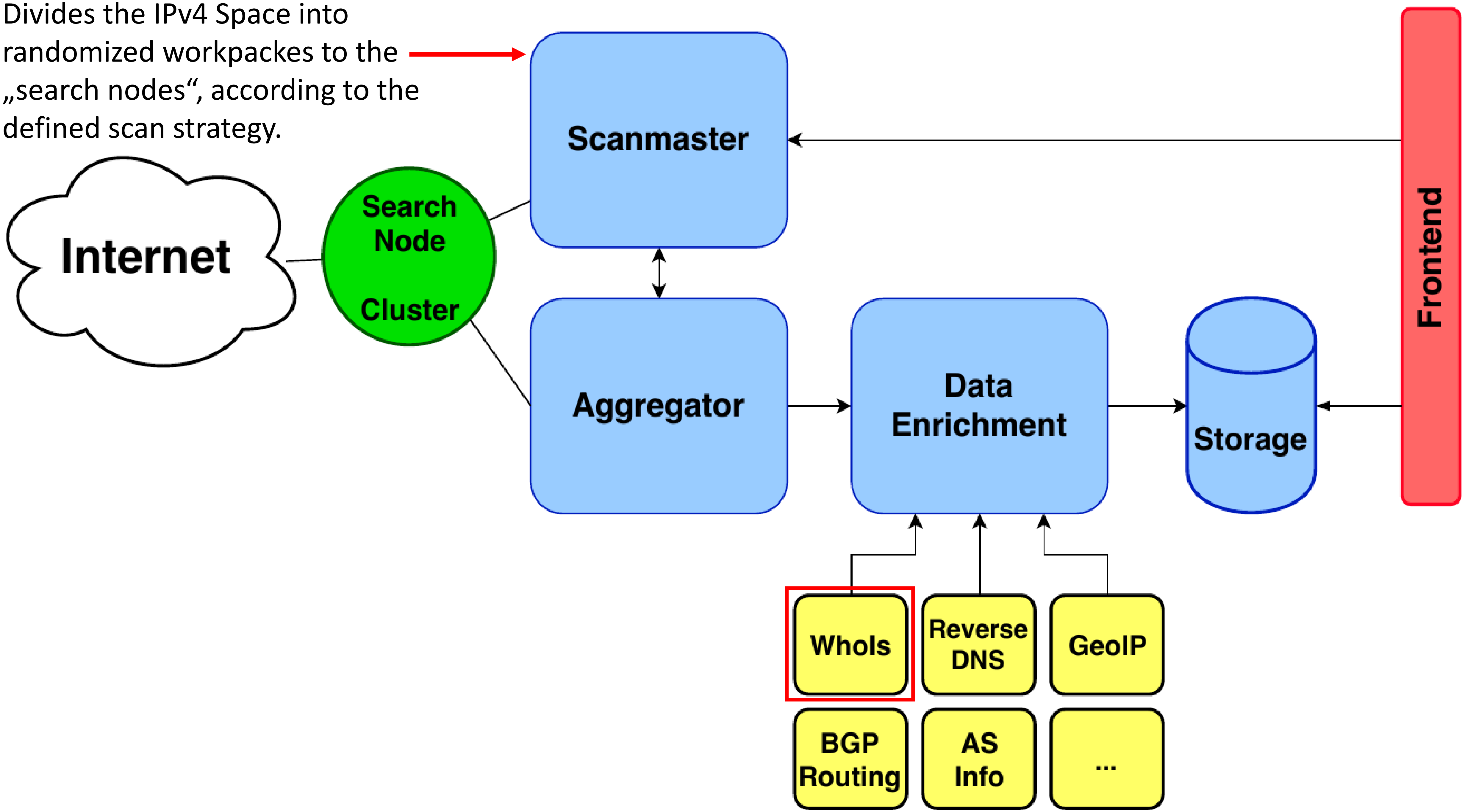
Divides the IPv4 Space into randomized IP workpackes to the „search nodes“, according to the defined scan strategy.

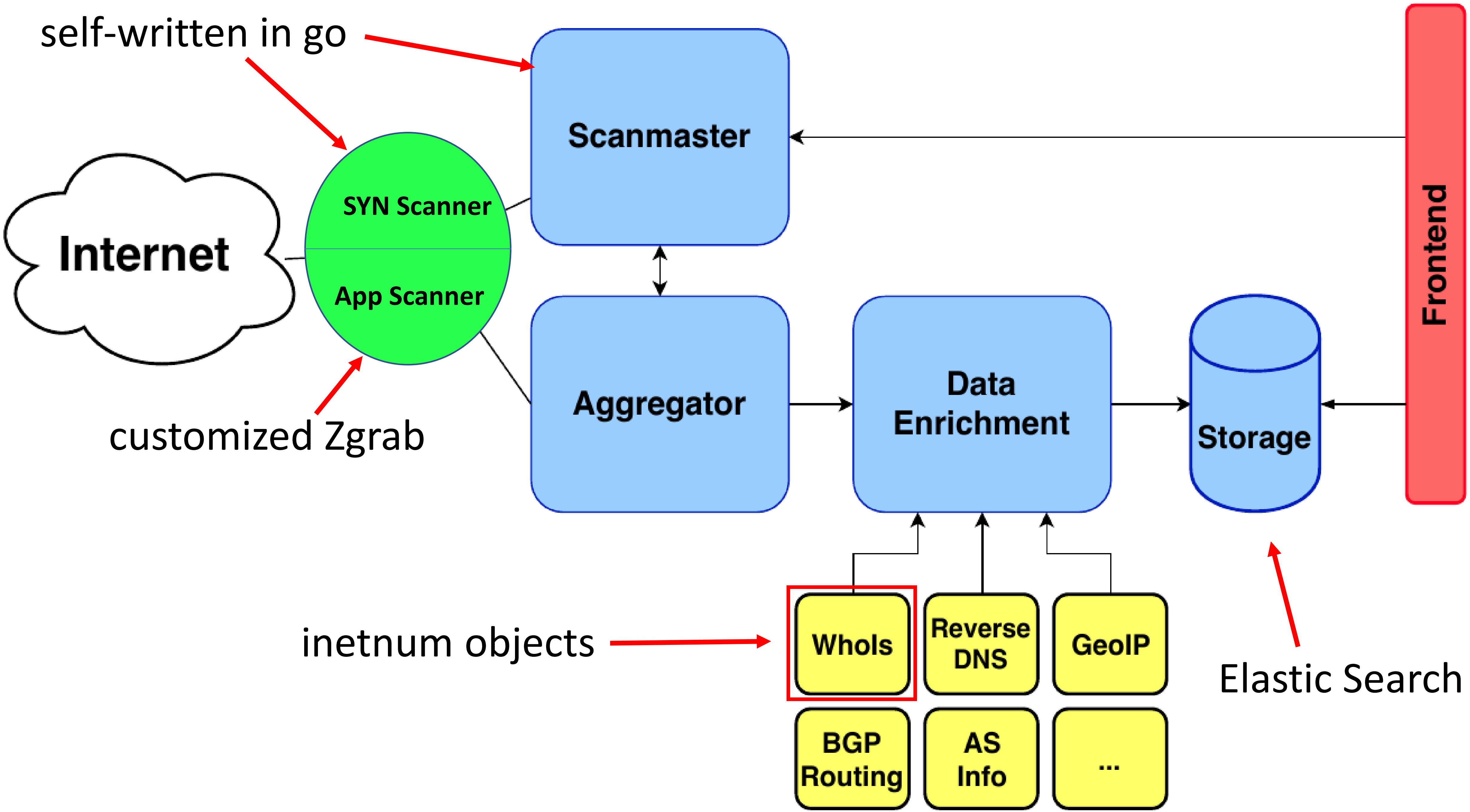


In case of a search node fail, the scan master will reassign the work package to another search node



Divides the IPv4 Space into randomized workpackes to the „search nodes“, according to the defined scan strategy.





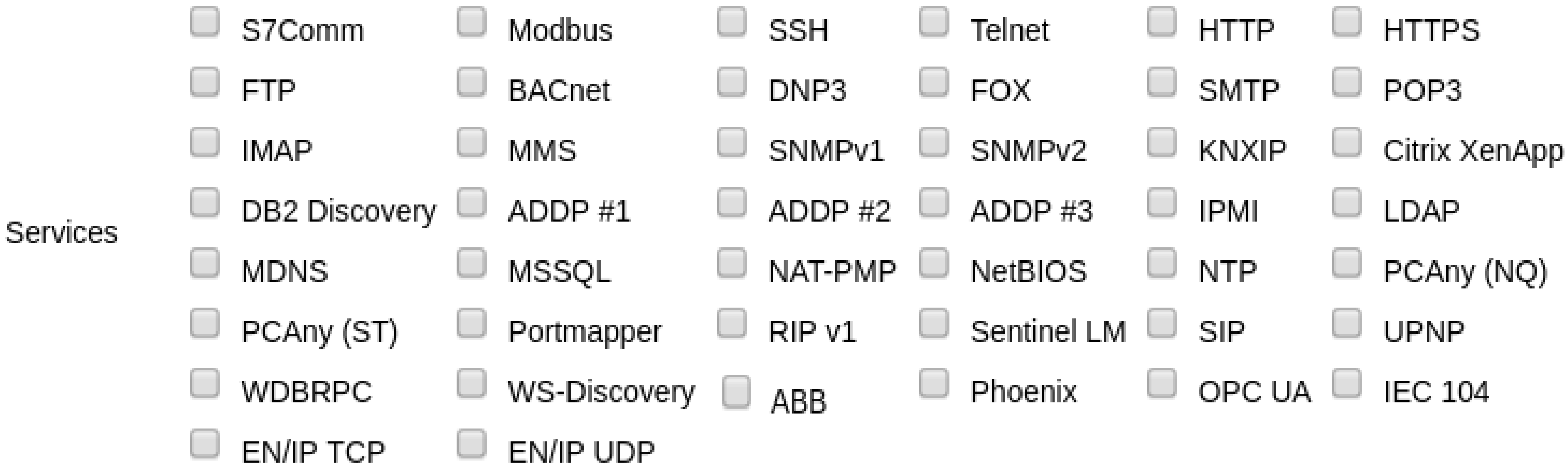
self-written in go

customized Zgrab

inetnum objects

Elastic Search

Snippet of Supported Protocols – Banner Grabbing (modified zgrab version)



Services	□ S7Comm	□ Modbus	□ SSH	□ Telnet	□ HTTP	□ HTTPS
	□ FTP	□ BACnet	□ DNP3	□ FOX	□ SMTP	□ POP3
	□ IMAP	□ MMS	□ SNMPv1	□ SNMPv2	□ KNXIP	□ Citrix XenApp
	□ DB2 Discovery	□ ADDP #1	□ ADDP #2	□ ADDP #3	□ IPMI	□ LDAP
	□ MDNS	□ MSSQL	□ NAT-PMP	□ NetBIOS	□ NTP	□ PCAny (NQ)
	□ PCAny (ST)	□ Portmapper	□ RIP v1	□ Sentinel LM	□ SIP	□ UPNP
	□ WDBRPC	□ WS-Discovery	□ ABB	□ Phoenix	□ OPC UA	□ IEC 104
	□ EN/IP TCP	□ EN/IP UDP				

Some Numbers and Settings

- Get a BGP feed to reduce the set of possible 4.3 billion IPv4 addresses to 2.8 billion IPv4 addresses in your routing table (35% reduction of SYN packets)
- Use (pseudo) randomized IPv4 addresses

- 70 Bytes per SYN packet * 2.8 billion IPv4 addresses = ~200 GB data
- Keep in mind: >~98% off all SYN traffic is overhead / unanswered
  - HTTP: 56 mio. hosts (most used protocol) – 56 mio / 2.8 billion = 2%

Some Numbers and Settings

- Send 1 or 2 SYNs per IPv4 address? **1 SYN seems to be sufficient**

Full Handshake	1 SYN	2 SYN	Censys
HTTPS	35.5 Mio	35.8 Mio	35.3 Mio
SSH	16.7 Mio	16.5 Mio	15.3 Mio
Telnet	3.1 Mio	3.2 Mio	3,1 Mio

*

HTTPS results with status_codes existing

SSH results with server_key_algorithm existing

Telnet results with a banner existing

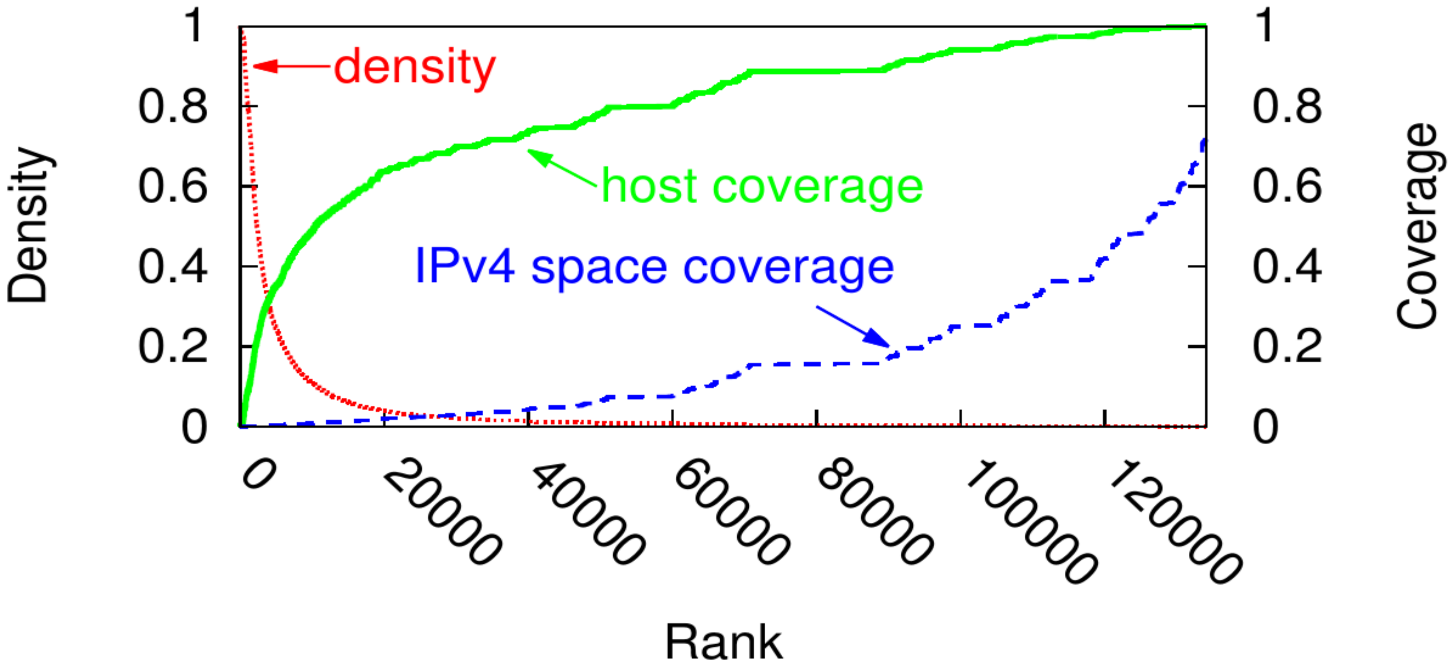
What about speed?

- We scan at 70mbit/s -> 6-7 hours per scan
- What happens if you **scan faster than ~2 hours** like *packet.tel* did from a single source IP?

	Our scan	Packet.tel	Difference
Open port: 443	75.8 Mio	50.7 Mio	- 33%
Open port: 80	64.7 Mio	57.6 Mio	- 11%
Open port: 23	7.3 Mio	6.2 Mio	- 15,5%

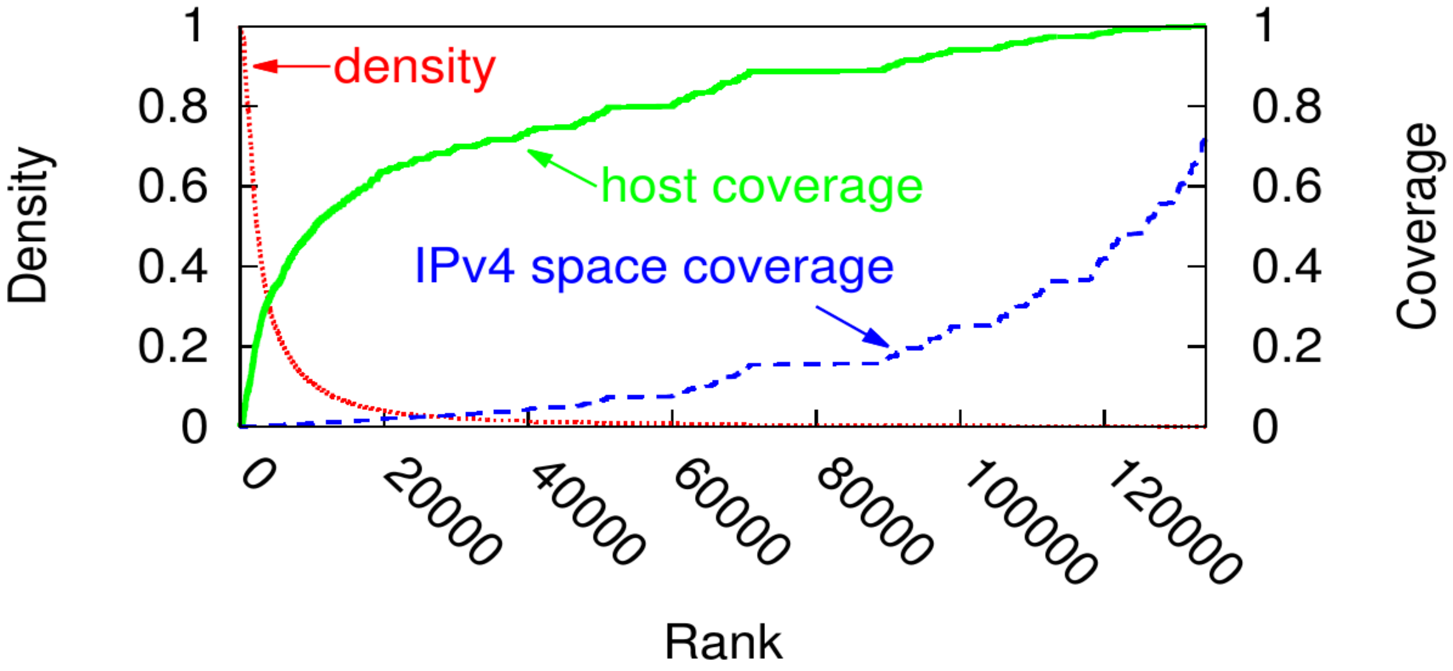
Your data will degrade by 10-30 percent.

Advanced Scanning Strategy



Shows responsive prefixes ranked by their density (dotted), the cumulative relative host coverage (solid), and the cumulative relative address space coverage (dashed) with density ρ > 0.

- **Want to scan the Internet very often for same protocol in short time?**
  - Scan the complete Internet once
  - Then rescan only BGP prefixes with atleast 1 host in it
  - You will save 25-50% of the routed IPv4 adress space and scan time!
  - This is called **BGP Prefix Hitlist**



Shows responsive prefixes ranked by their density (dotted), the cumulative relative host coverage (solid), and the cumulative relative address space coverage (dashed) with density ρ > 0.

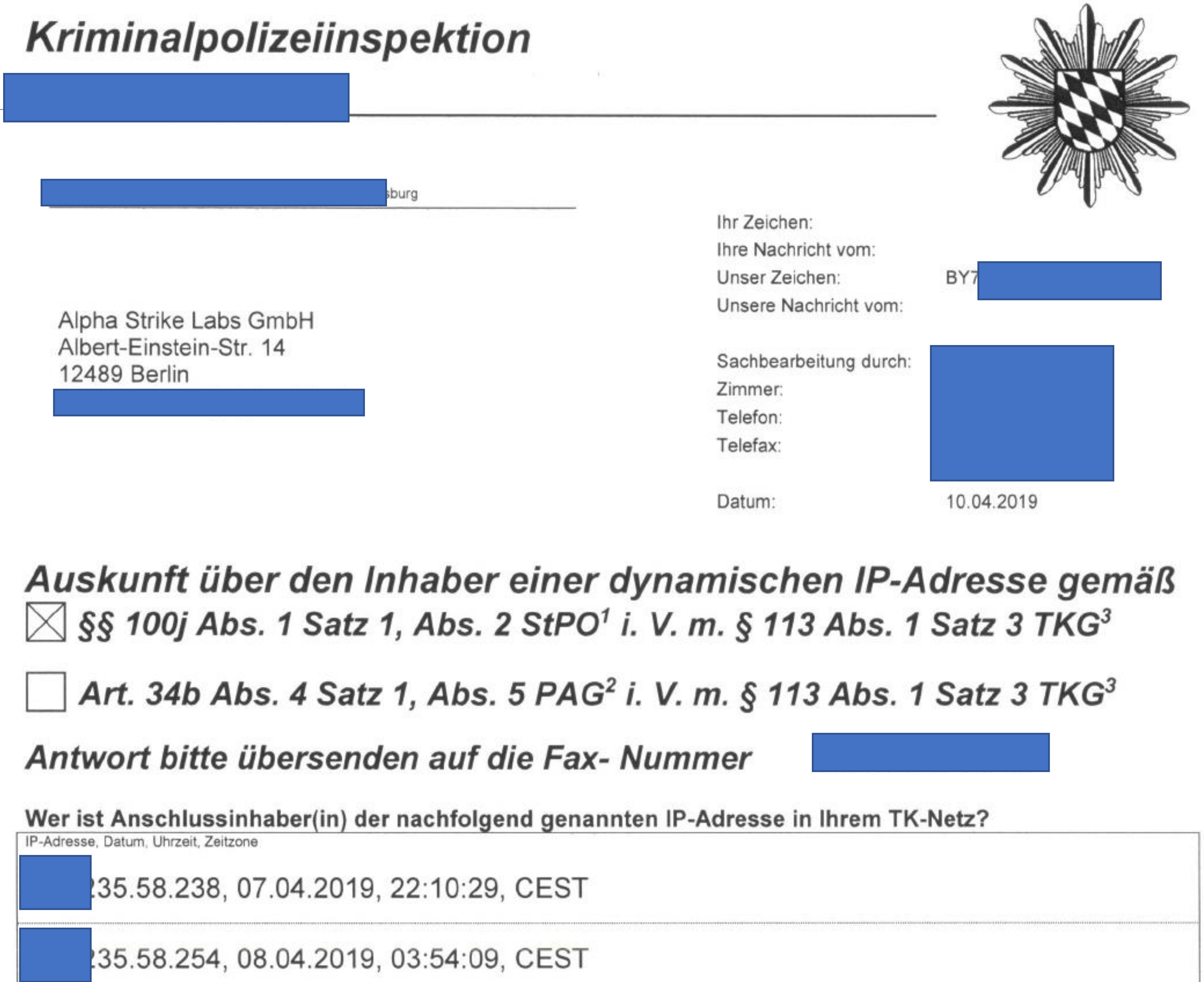
- **Want to scan the Internet very often for same protocol in short time?**
  - Scan the complete Internet once
  - Then rescan only BGP prefixes with atleast 1 host in it
  - You will save 25-50% of the routed IPv4 adress space and scan time!
  - This is called **BGP Prefix Hitlist**

Towards Better Internet Citizenship: Reducing the Footprint of Internet-wide Scans by Topology Aware Prefix Selection
J Klick, S Lau, M Wählisch, V Roth
Proceedings of the 2016 Internet Measurement Conference, 421-427

https://arxiv.org/pdf/1605.05856

Police o.O

The bavarian (german) police asked us as Internet Service Provider for the owners of our Scan-IPs.



Kriminalpolizeiinspektion

[redacted]

[redacted]sburg

Alpha Strike Labs GmbH
Albert-Einstein-Str. 14
12489 Berlin
[redacted]

Ihr Zeichen:
Ihre Nachricht vom:
Unser Zeichen: BY7[redacted]
Unsere Nachricht vom:

Sachbearbeitung durch: [redacted]
Zimmer:
Telefon:
Telefax:

Datum: 10.04.2019

Auskunft über den Inhaber einer dynamischen IP-Adresse gemäß

☒ ***§§ 100j Abs. 1 Satz 1, Abs. 2 StPO[1] i. V. m. § 113 Abs. 1 Satz 3 TKG[3]***

☐ ***Art. 34b Abs. 4 Satz 1, Abs. 5 PAG[2] i. V. m. § 113 Abs. 1 Satz 3 TKG[3]***

Antwort bitte übersenden auf die Fax- Nummer [redacted]

Wer ist Anschlussinhaber(in) der nachfolgend genannten IP-Adresse in Ihrem TK-Netz?

IP-Adresse, Datum, Uhrzeit, Zeitzone
[redacted]35.58.238, 07.04.2019, 22:10:29, CEST
[redacted]35.58.254, 08.04.2019, 03:54:09, CEST

Hardware Setup

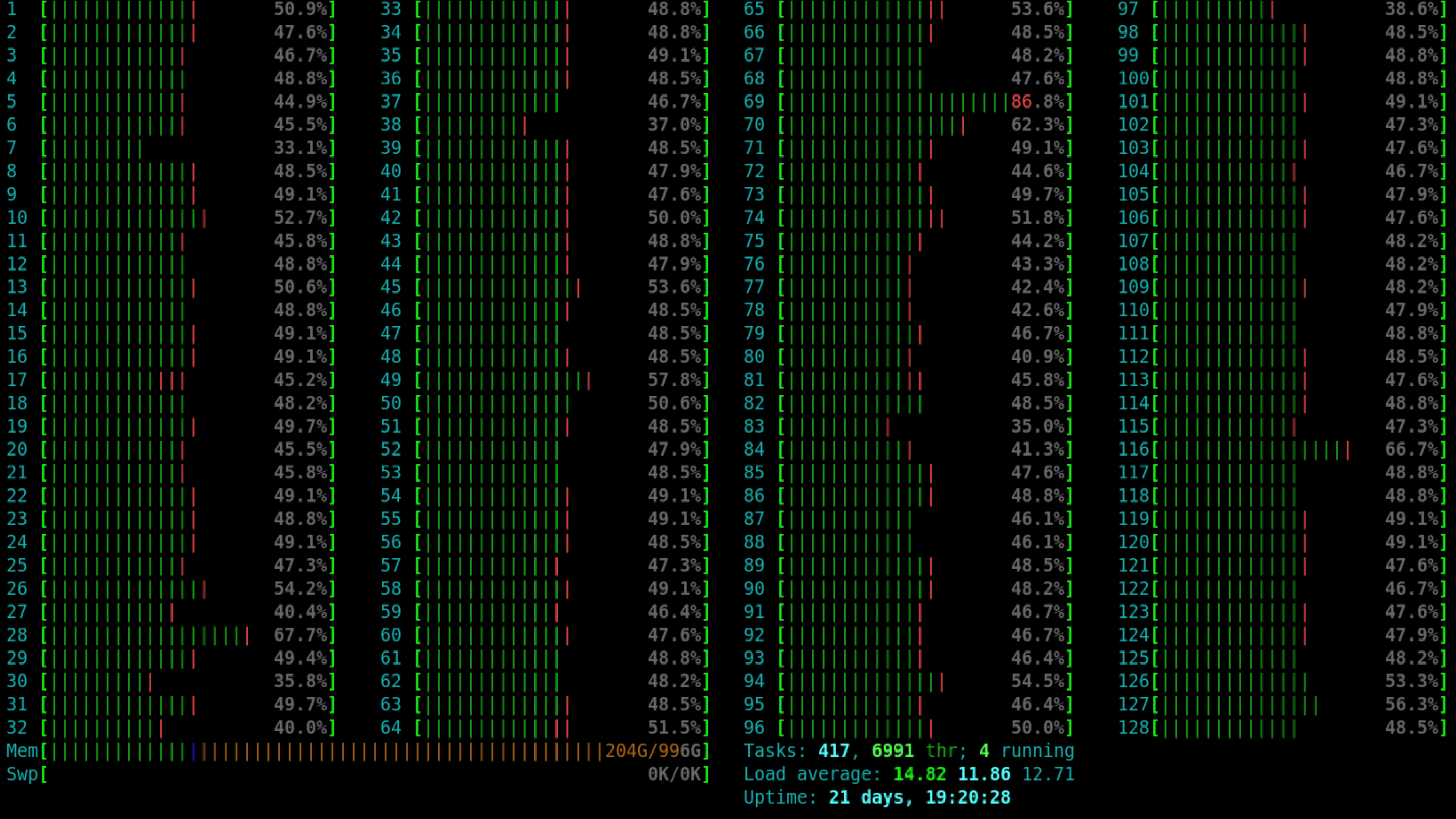
We need compute power and storage for recurrent scans:

Data sizes of scan results (uncompressed json):

HTTPS	→ 700GB
HTTP	→ 300 GB
SSH	→ 35 GB
Telnet	→ 2 GB

Hardware Setup – Server 3 HU – 200W (idle)

- 64 CPU Cores (AMD Epyc 7551)
- 1 TB RAM
  - 16x 64 GB Dimms
  - 50% of ram used for elastic search heap another 50% ram used for caching
- 40 TB SSD
  - 10x 860 4TB EVO SSD - 2400 TBW and 5 year warranty
  - Speed 5,8 GByte/s read and 2,6 Gbyte/s write - 40 GB data sample
  - Raid 0 – for elastic search index
- 72 TB HDD
  - 6x 12TB WD Ultrastar DC HC520 SATA 6Gb/s
  - Raid 5 – longterm storage for raw data and elastic index backup



```
1  [||||||||||||||      50.9%]  33 [||||||||||||||      48.8%]  65 [|||||||||||||||     53.6%]  97 [|||||||||||         38.6%]
2  [||||||||||||||      47.6%]  34 [||||||||||||||      48.8%]  66 [||||||||||||||      48.5%]  98 [||||||||||||||      48.5%]
3  [|||||||||||||       46.7%]  35 [||||||||||||||      49.1%]  67 [|||||||||||||       48.2%]  99 [||||||||||||||      48.8%]
4  [|||||||||||||       48.8%]  36 [||||||||||||||      48.5%]  68 [|||||||||||||       47.6%]  100[|||||||||||||       48.8%]
5  [|||||||||||||       44.9%]  37 [|||||||||||||       46.7%]  69 [|||||||||||||||||||||86.8%]  101[||||||||||||||      49.1%]
6  [|||||||||||||       45.5%]  38 [||||||||||          37.0%]  70 [|||||||||||||||||   62.3%]  102[|||||||||||||       47.3%]
7  [|||||||||           33.1%]  39 [||||||||||||||      48.5%]  71 [||||||||||||||      49.1%]  103[||||||||||||||      47.6%]
8  [||||||||||||||      48.5%]  40 [||||||||||||||      47.9%]  72 [|||||||||||||       44.6%]  104[|||||||||||||       46.7%]
9  [||||||||||||||      49.1%]  41 [||||||||||||||      47.6%]  73 [||||||||||||||      49.7%]  105[||||||||||||||      47.9%]
10 [|||||||||||||||     52.7%]  42 [||||||||||||||      50.0%]  74 [|||||||||||||||     51.8%]  106[||||||||||||||      47.6%]
11 [|||||||||||||       45.8%]  43 [||||||||||||||      48.8%]  75 [|||||||||||||       44.2%]  107[|||||||||||||       48.2%]
12 [|||||||||||||       48.8%]  44 [||||||||||||||      47.9%]  76 [||||||||||||        43.3%]  108[|||||||||||||       48.2%]
13 [||||||||||||||      50.6%]  45 [|||||||||||||||     53.6%]  77 [||||||||||||        42.4%]  109[||||||||||||||      48.2%]
14 [|||||||||||||       48.8%]  46 [||||||||||||||      48.5%]  78 [||||||||||||        42.6%]  110[|||||||||||||       47.9%]
15 [||||||||||||||      49.1%]  47 [|||||||||||||       48.5%]  79 [|||||||||||||       46.7%]  111[|||||||||||||       48.8%]
16 [||||||||||||||      49.1%]  48 [||||||||||||||      48.5%]  80 [||||||||||||        40.9%]  112[||||||||||||||      48.5%]
17 [|||||||||||||       45.2%]  49 [||||||||||||||||    57.8%]  81 [|||||||||||||       45.8%]  113[||||||||||||||      47.6%]
18 [|||||||||||||       48.2%]  50 [||||||||||||||      50.6%]  82 [|||||||||||||       48.5%]  114[||||||||||||||      48.8%]
19 [||||||||||||||      49.7%]  51 [||||||||||||||      48.5%]  83 [||||||||||          35.0%]  115[|||||||||||||       47.3%]
20 [|||||||||||||       45.5%]  52 [|||||||||||||       47.9%]  84 [||||||||||||        41.3%]  116[||||||||||||||||||  66.7%]
21 [|||||||||||||       45.8%]  53 [|||||||||||||       48.5%]  85 [||||||||||||||      47.6%]  117[|||||||||||||       48.8%]
22 [||||||||||||||      49.1%]  54 [||||||||||||||      49.1%]  86 [||||||||||||||      48.8%]  118[|||||||||||||       48.8%]
23 [||||||||||||||      48.8%]  55 [||||||||||||||      49.1%]  87 [||||||||||||        46.1%]  119[||||||||||||||      49.1%]
24 [||||||||||||||      49.1%]  56 [||||||||||||||      48.5%]  88 [||||||||||||        46.1%]  120[||||||||||||||      49.1%]
25 [|||||||||||||       47.3%]  57 [|||||||||||||       47.3%]  89 [||||||||||||||      48.5%]  121[||||||||||||||      47.6%]
26 [|||||||||||||||     54.2%]  58 [||||||||||||||      49.1%]  90 [||||||||||||||      48.2%]  122[|||||||||||||       46.7%]
27 [||||||||||||        40.4%]  59 [|||||||||||||       46.4%]  91 [|||||||||||||       46.7%]  123[||||||||||||||      47.6%]
28 [||||||||||||||||||  67.7%]  60 [||||||||||||||      47.6%]  92 [|||||||||||||       46.7%]  124[||||||||||||||      47.9%]
29 [||||||||||||||      49.4%]  61 [|||||||||||||       48.8%]  93 [|||||||||||||       46.4%]  125[|||||||||||||       48.2%]
30 [||||||||||          35.8%]  62 [|||||||||||||       48.2%]  94 [|||||||||||||||     54.5%]  126[||||||||||||||      53.3%]
31 [||||||||||||||      49.7%]  63 [||||||||||||||      48.5%]  95 [|||||||||||||       46.4%]  127[|||||||||||||||     56.3%]
32 [|||||||||||         40.0%]  64 [||||||||||||||      51.5%]  96 [||||||||||||||      50.0%]  128[|||||||||||||       48.5%]
Mem[||||||||||||||||||||||||||||||||||||||||||||||||||204G/996G]  Tasks: 417, 6991 thr; 4 running
Swp[                                                     0K/0K]  Load average: 14.82 11.86 12.71
                                                                 Uptime: 21 days, 19:20:28
```

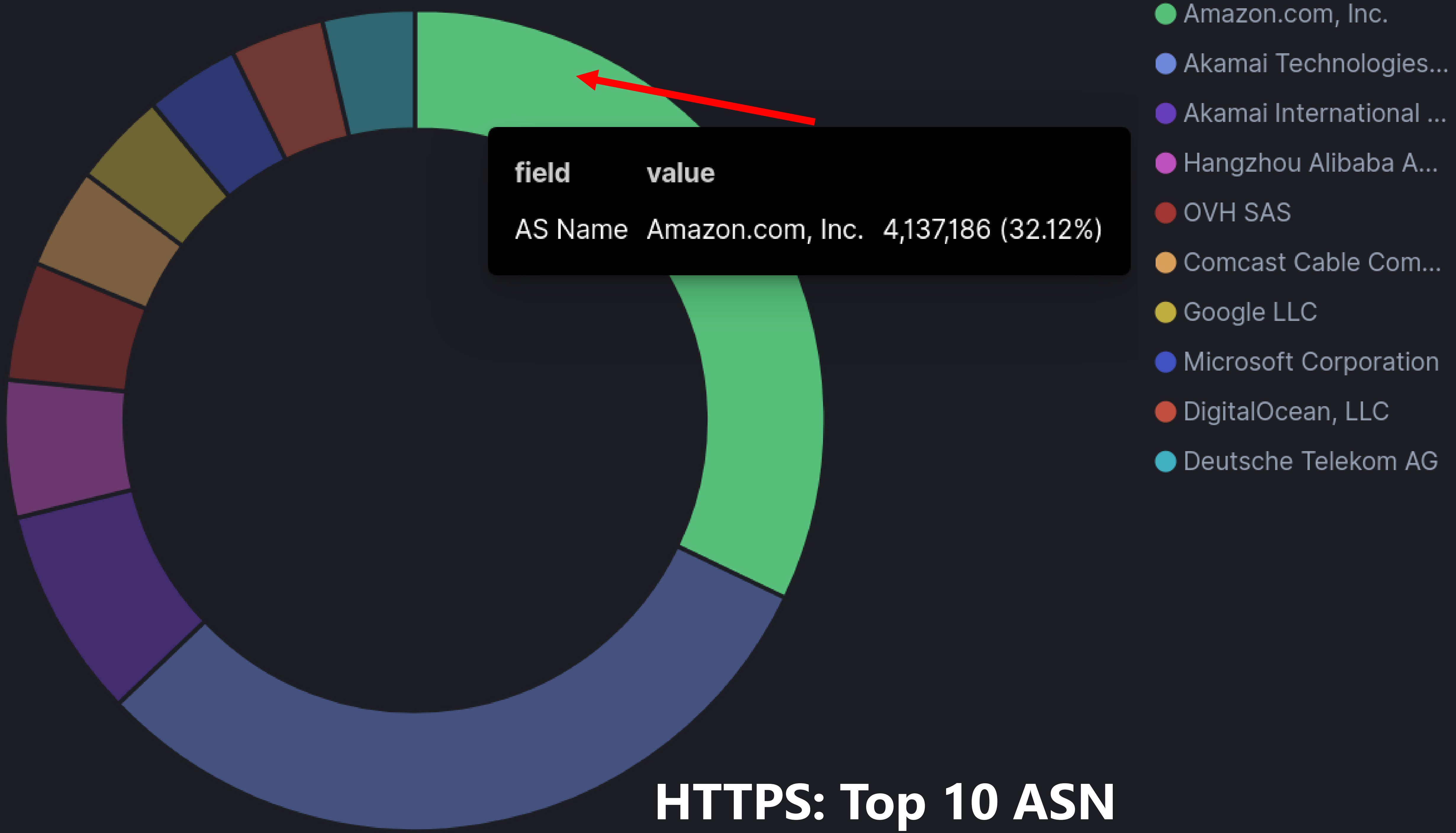
Elastic Search Setup

- Elastic Search 7.3
  - Setup several nodes with a max heap of 26 GB per node
  - Otherwise JAVA VM will use 64 bit pointers instead of *commpressed oop* 32 bit pointer
  - 64bit pointer slowed our system by ~30-40%
  - 32bit pointer using half of the memory, leading to more garbage collection cycles -> much more performance
  - For more background information read this very good article:

https://www.elastic.co/de/blog/a-heap-of-trouble#fn3

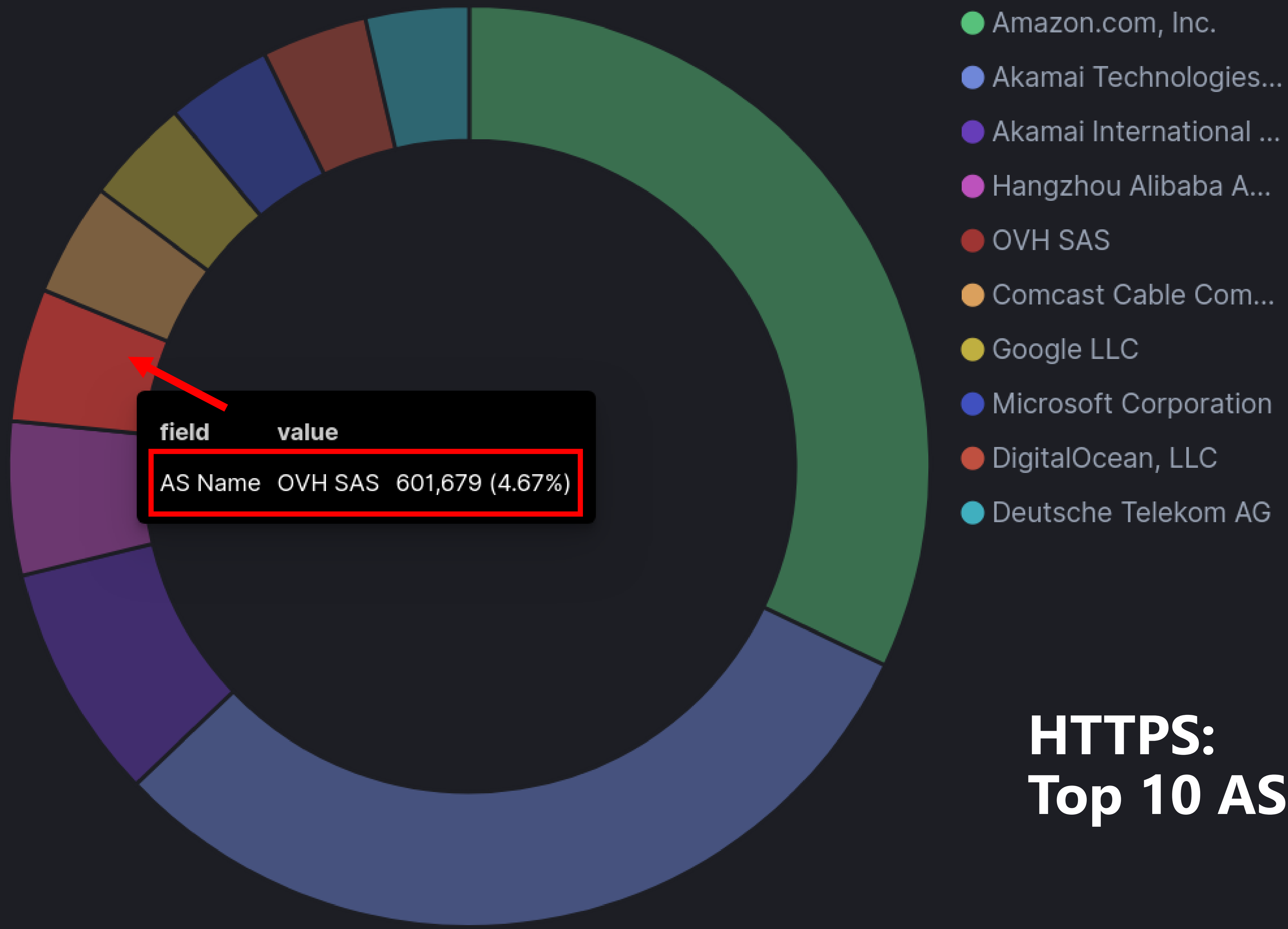
Let´s go the results

HTTPS: Top 10 ASN

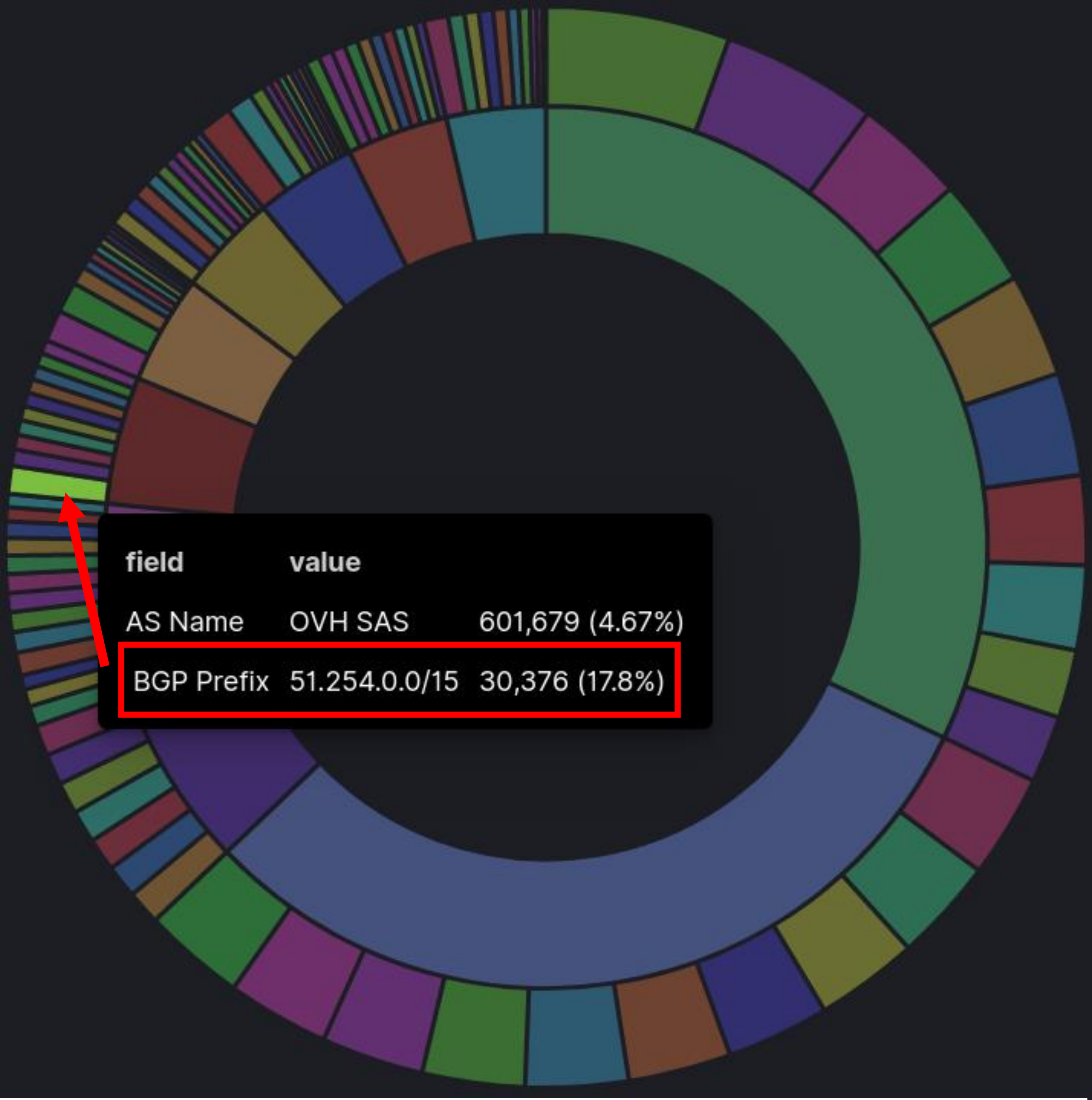


field	value	
AS Name	Amazon.com, Inc.	4,137,186 (32.12%)

HTTPS:
Top 10 ASN

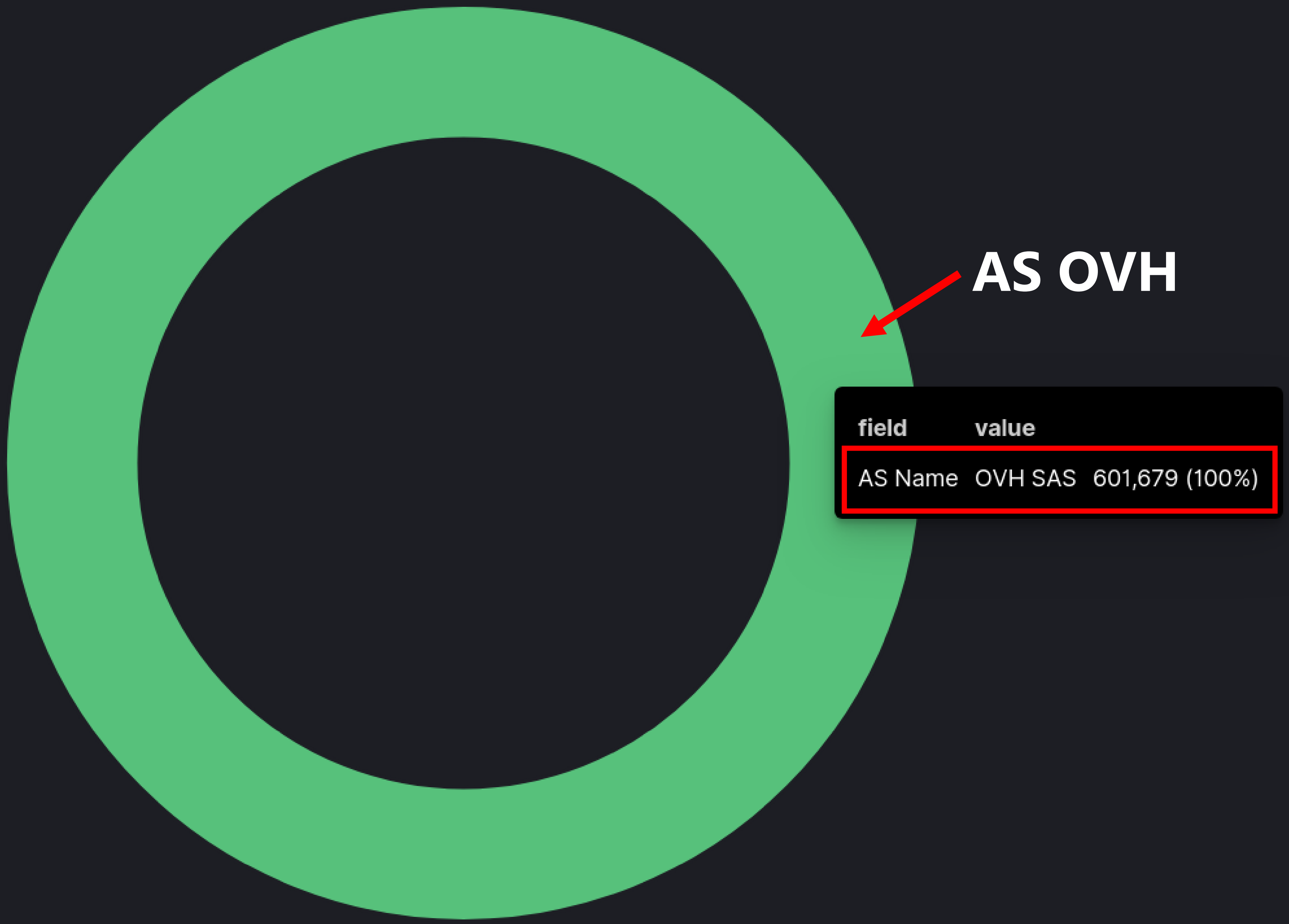


field	value	
AS Name	OVH SAS	601,679 (4.67%)



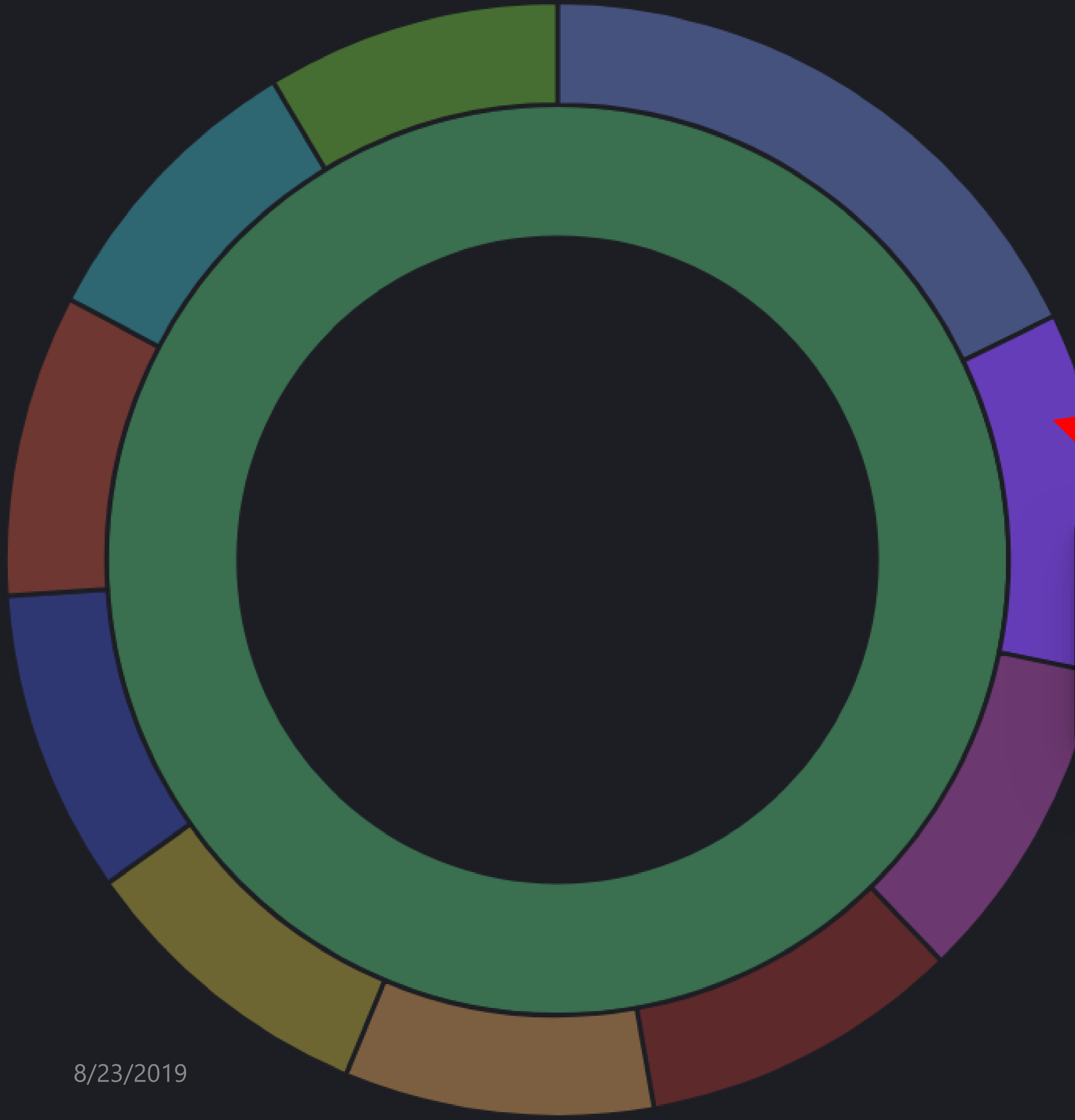
field	value	
AS Name	OVH SAS	601,679 (4.67%)
BGP Prefix	51.254.0.0/15	30,376 (17.8%)

HTTPS:
Top 10 AS +
Top 10 BGP Prefix

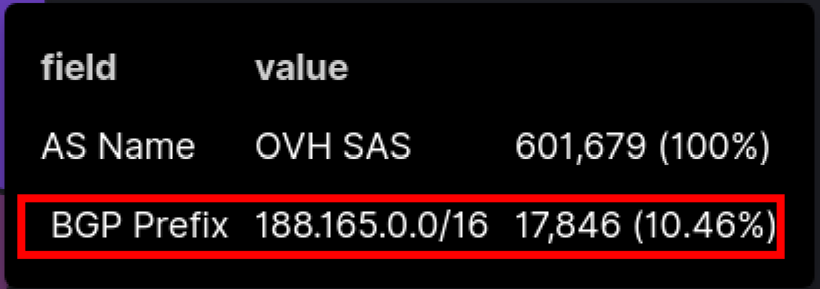


AS OVH

field	value	
AS Name	OVH SAS	601,679 (100%)

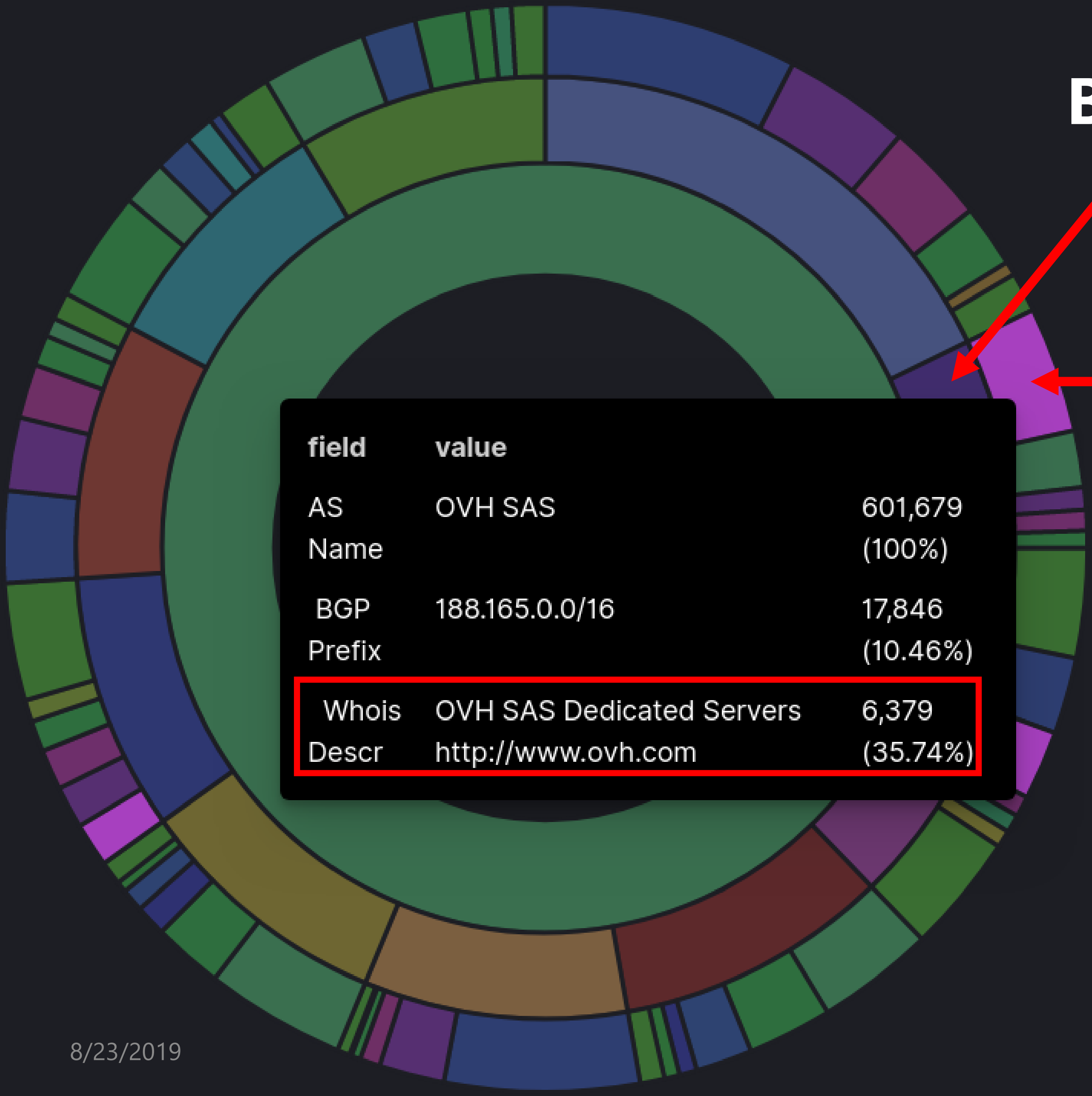


BGP Prefix



field	value	
AS Name	OVH SAS	601,679 (100%)
BGP Prefix	188.165.0.0/16	17,846 (10.46%)

HTTPS:
AS OVH+
Top 10 BGP Prefix

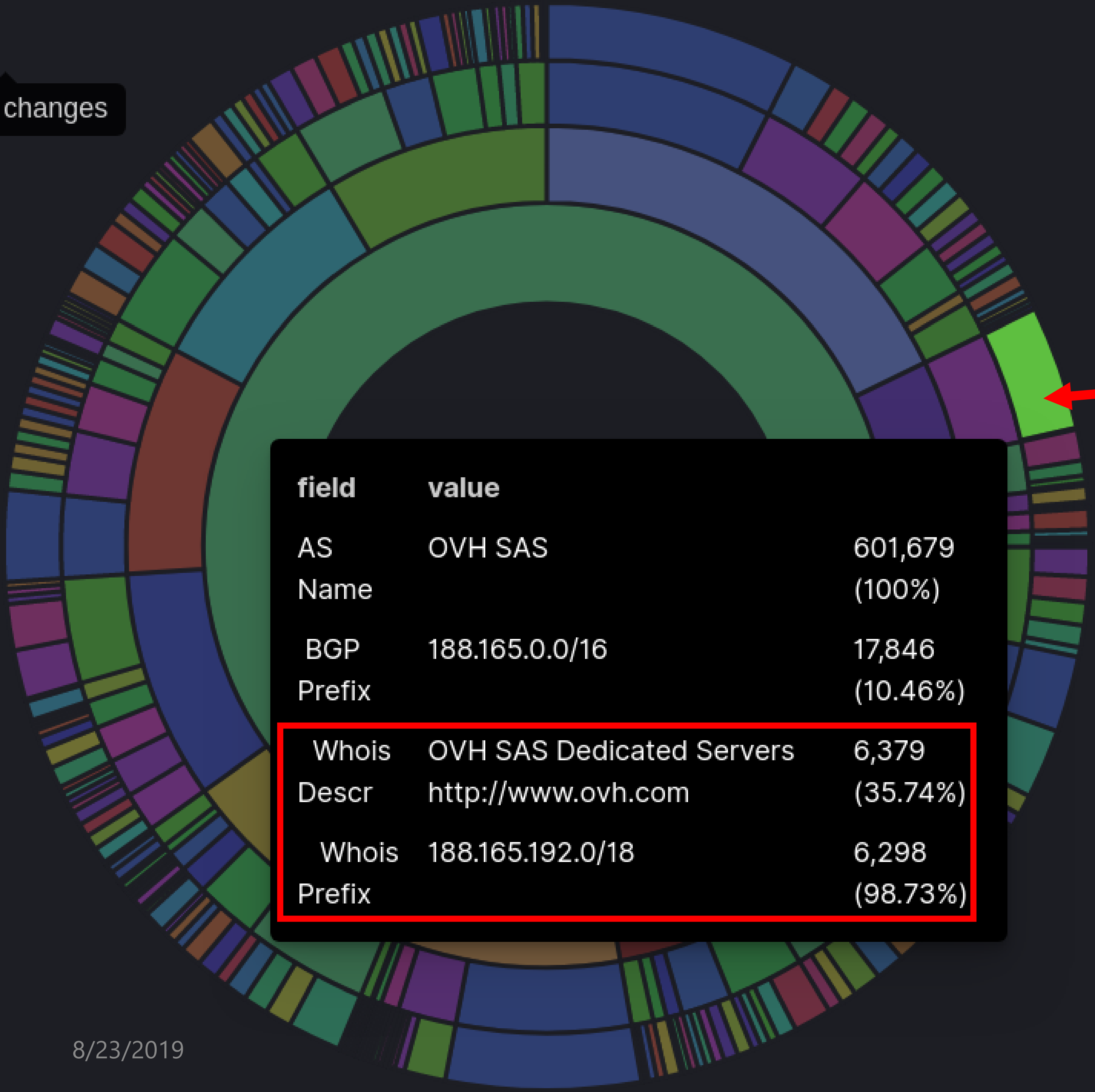


field	value	
AS Name	OVH SAS	601,679 (100%)
BGP Prefix	188.165.0.0/16	17,846 (10.46%)
Whois Descr	OVH SAS Dedicated Servers http://www.ovh.com	6,379 (35.74%)

BGP Prefix

Whois Descr.

HTTPS:
AS OVH+
Top 10 BGP Prefix+
Top 5 Whois Descr.

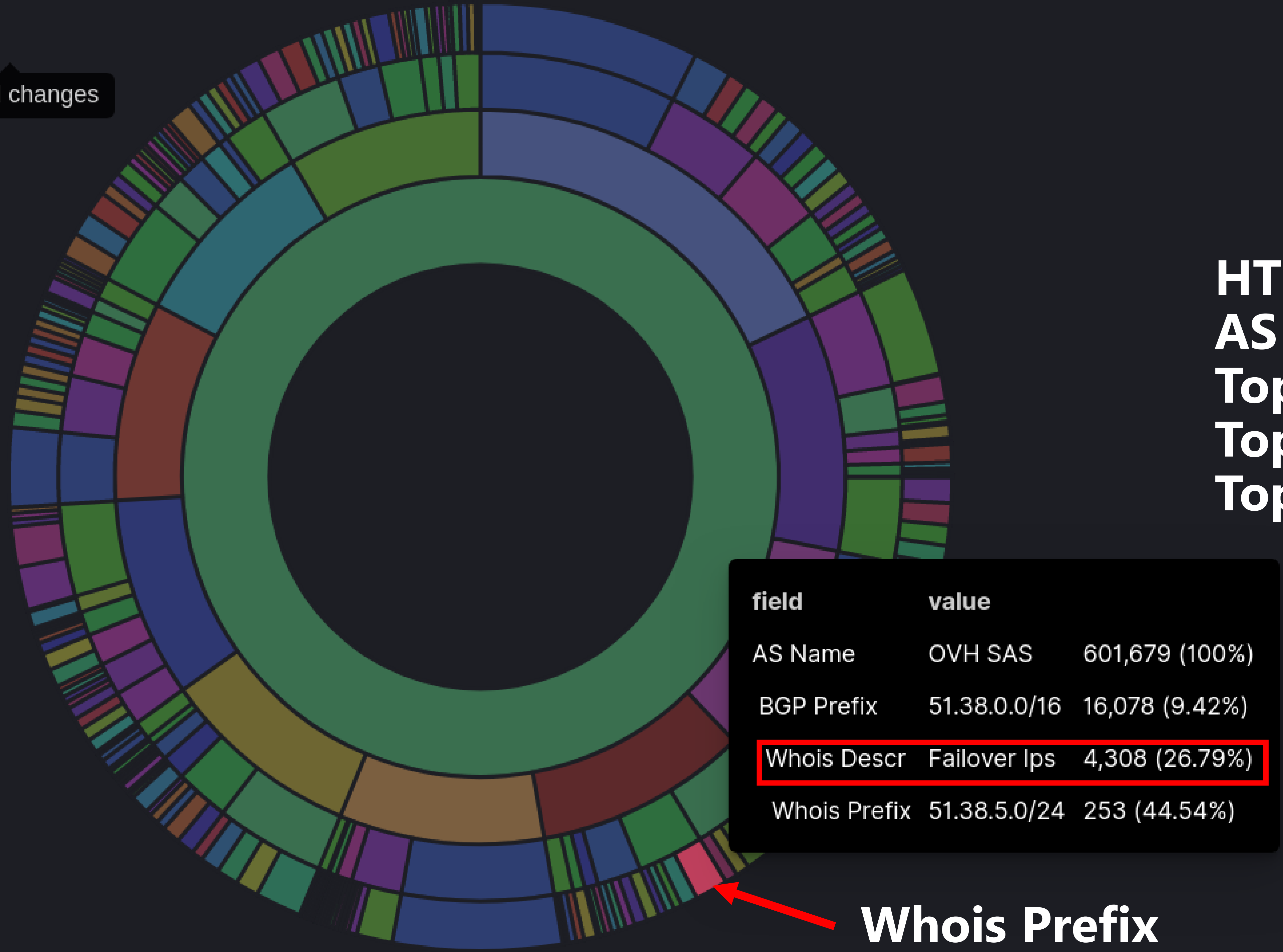


field	value	
AS Name	OVH SAS	601,679 (100%)
BGP Prefix	188.165.0.0/16	17,846 (10.46%)
Whois Descr	OVH SAS Dedicated Servers http://www.ovh.com	6,379 (35.74%)
Whois Prefix	188.165.192.0/18	6,298 (98.73%)

Whois Prefix

HTTPS:
AS OVH+
Top 10 BGP Prefix+
Top 5 Whois Descr.+
Top 5 Whois Prefix

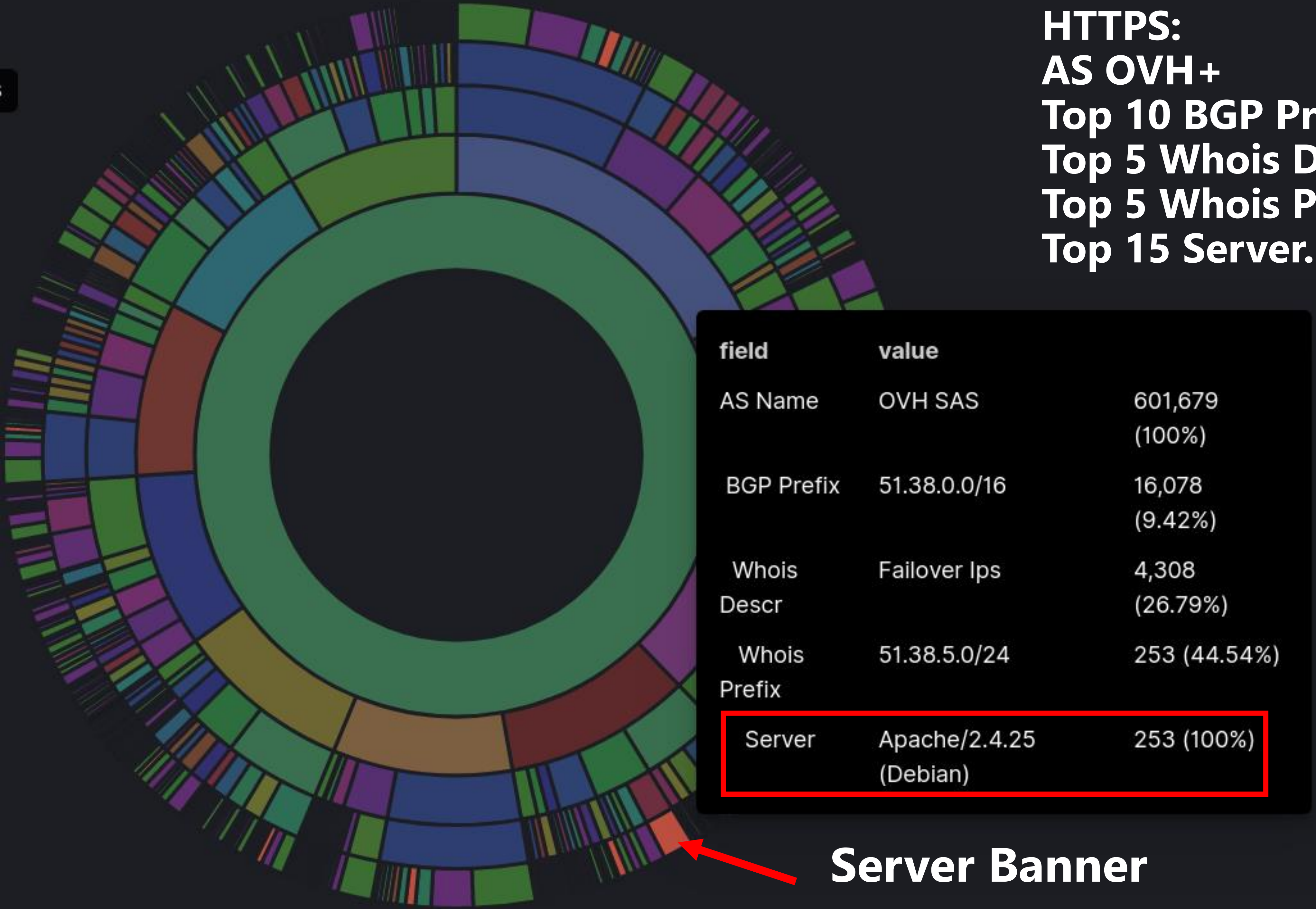
HTTPS:
AS OVH+
Top 10 BGP Prefix+
Top 5 Whois Descr.+
Top 5 Whois Prefix



field	value	
AS Name	OVH SAS	601,679 (100%)
BGP Prefix	51.38.0.0/16	16,078 (9.42%)
Whois Descr	Failover Ips	4,308 (26.79%)
Whois Prefix	51.38.5.0/24	253 (44.54%)

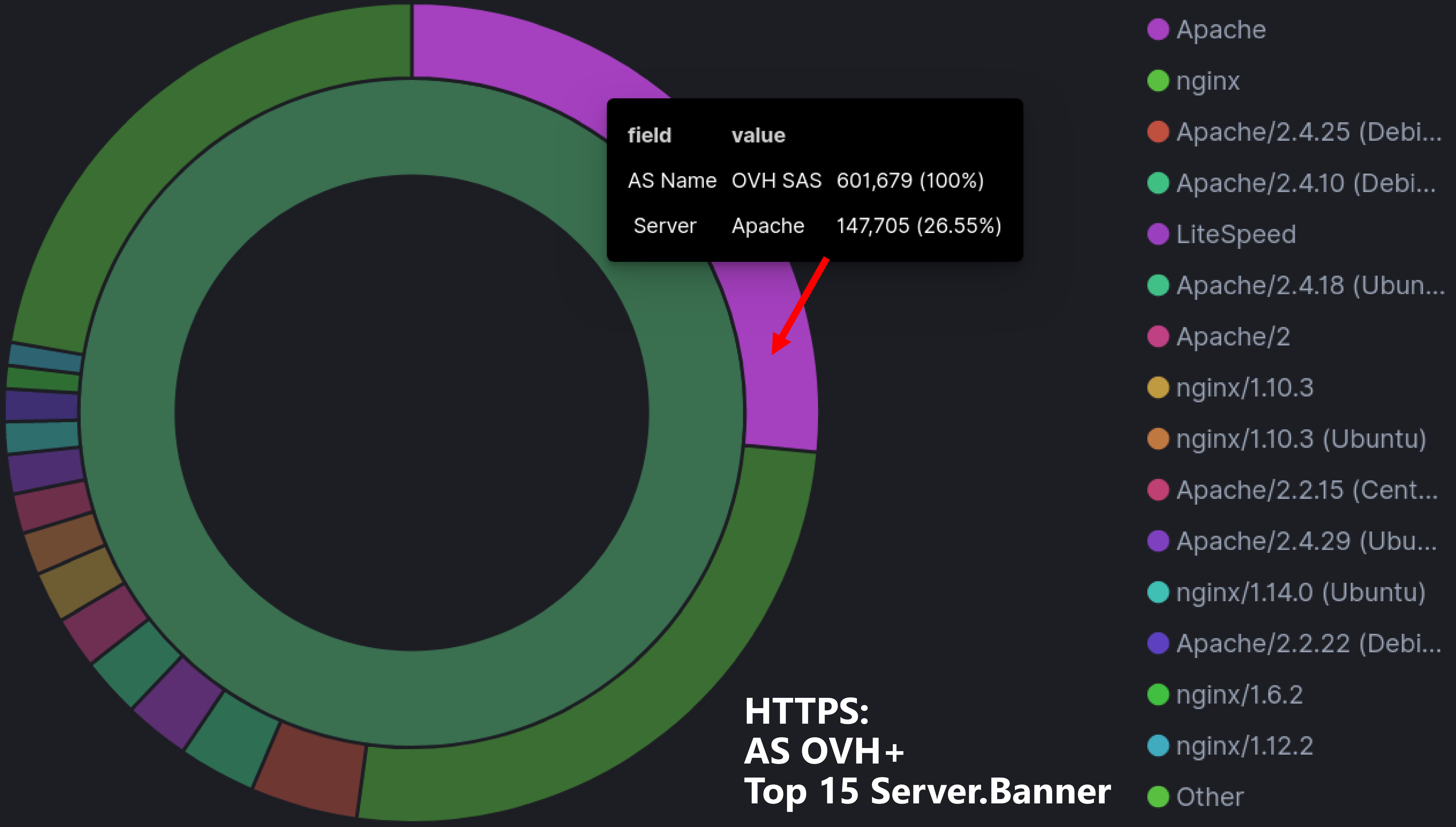
Whois Prefix

HTTPS:
AS OVH+
Top 10 BGP Prefix+
Top 5 Whois Descr.+
Top 5 Whois Prefix+
Top 15 Server.Banner



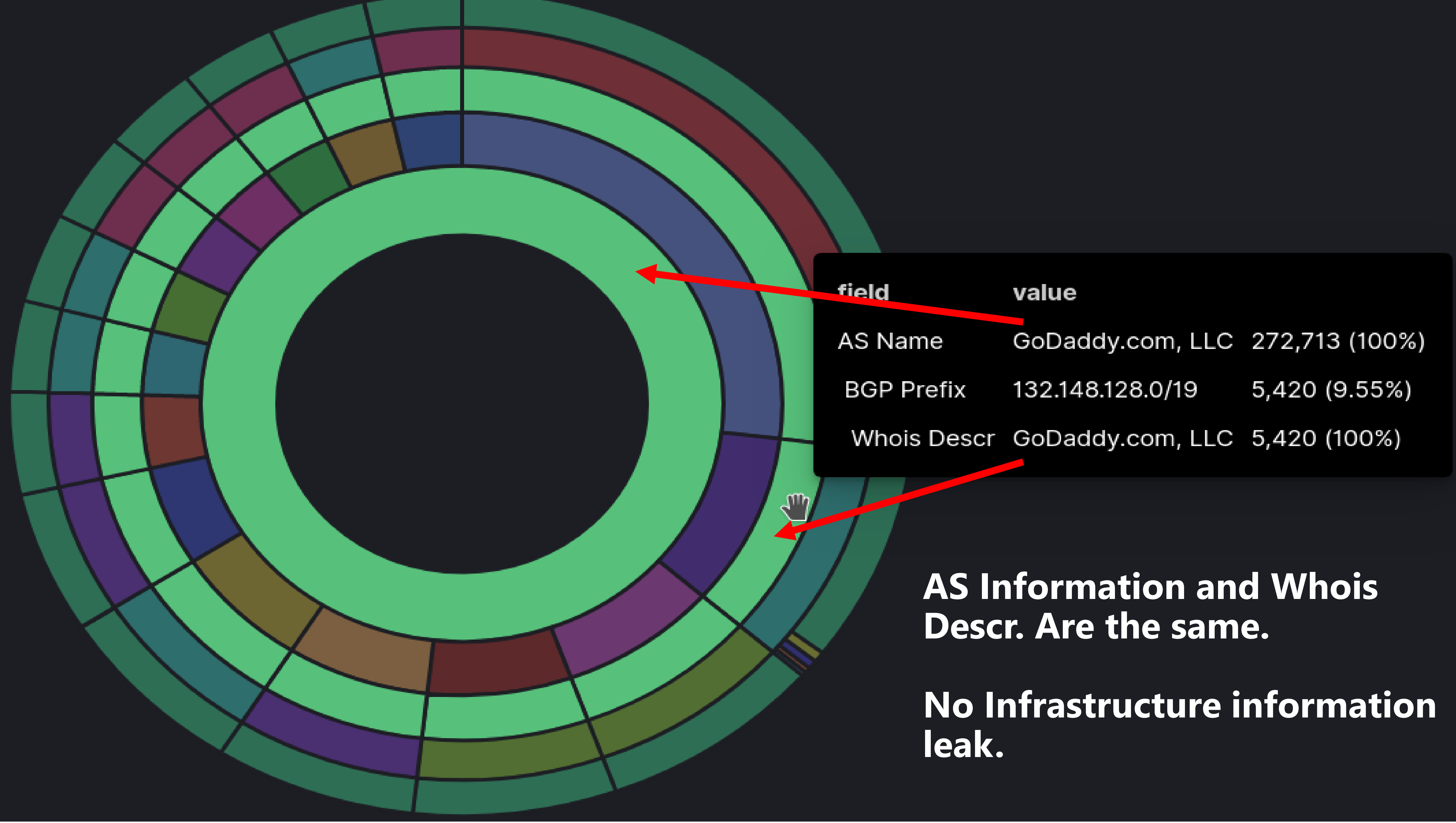
field	value	
AS Name	OVH SAS	601,679 (100%)
BGP Prefix	51.38.0.0/16	16,078 (9.42%)
Whois Descr	Failover Ips	4,308 (26.79%)
Whois Prefix	51.38.5.0/24	253 (44.54%)
Server	Apache/2.4.25 (Debian)	253 (100%)

Server Banner



field	value	
AS Name	OVH SAS	601,679 (100%)
Server	Apache	147,705 (26.55%)

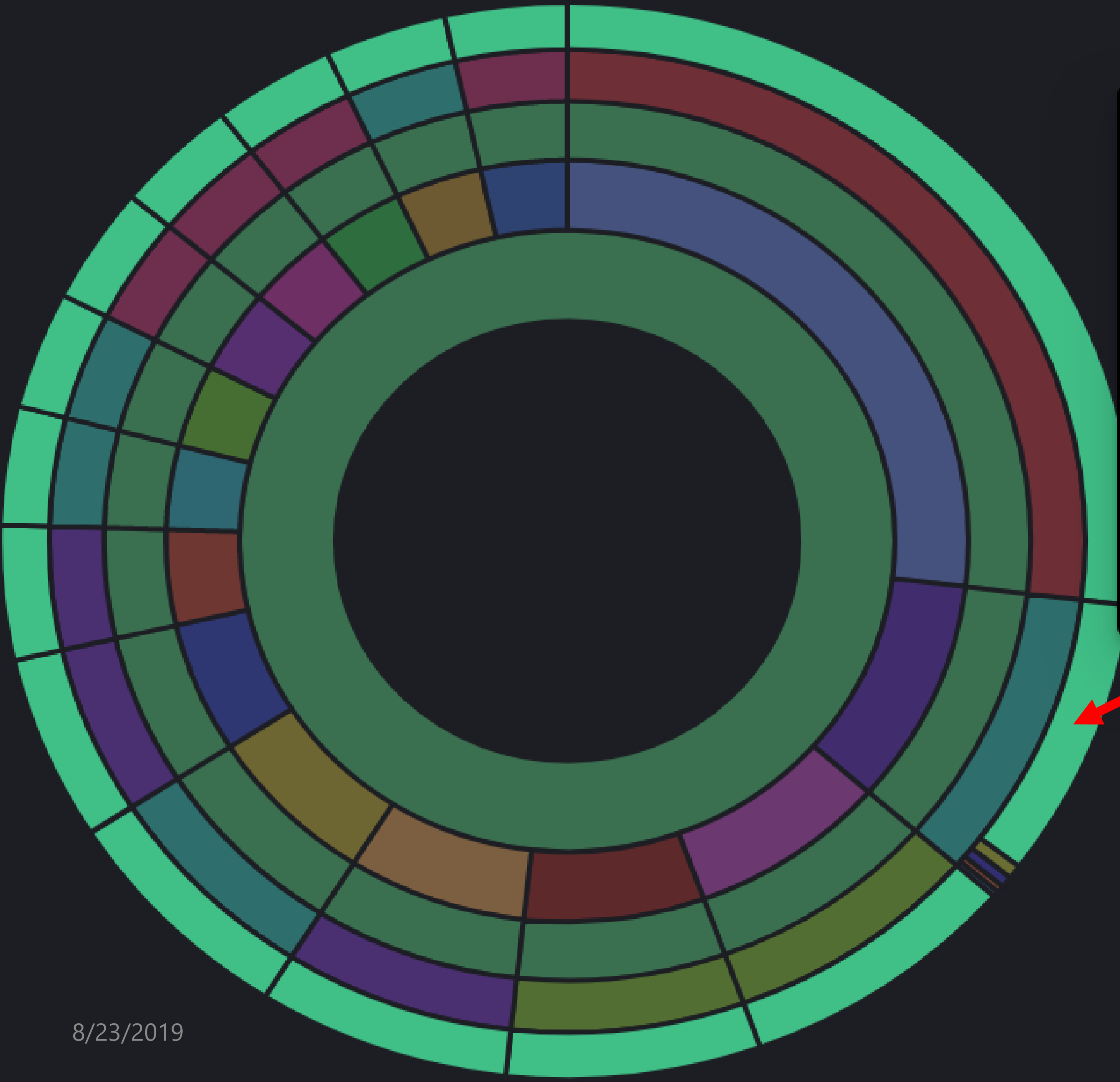
HTTPS:
AS OVH+
Top 15 Server.Banner

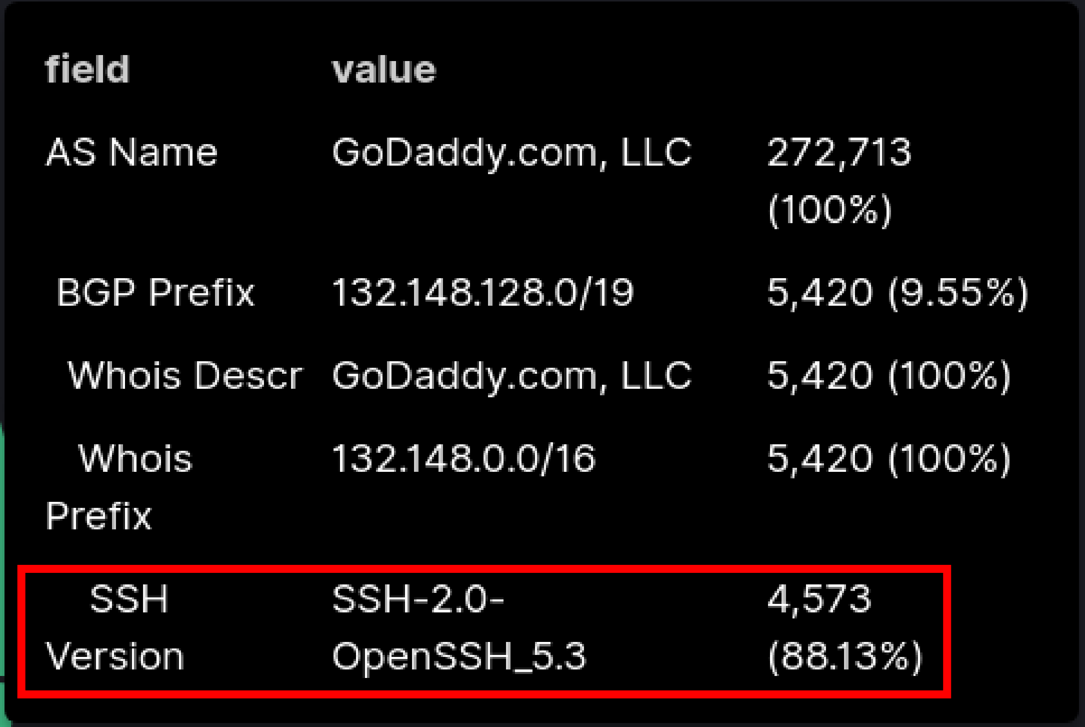


field	value	
AS Name	GoDaddy.com, LLC	272,713 (100%)
BGP Prefix	132.148.128.0/19	5,420 (9.55%)
Whois Descr	GoDaddy.com, LLC	5,420 (100%)

AS Information and Whois Descr. Are the same.

No Infrastructure information leak.



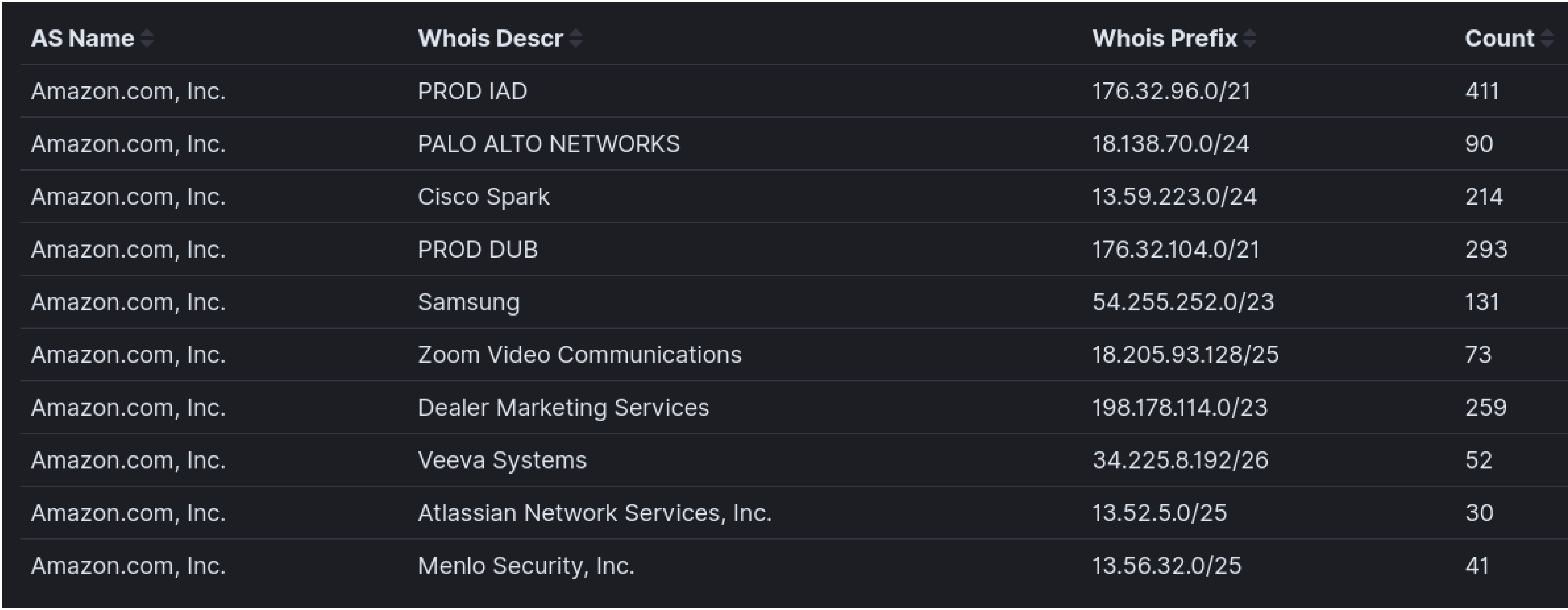


field	value	
AS Name	GoDaddy.com, LLC	272,713 (100%)
BGP Prefix	132.148.128.0/19	5,420 (9.55%)
Whois Descr	GoDaddy.com, LLC	5,420 (100%)
Whois Prefix	132.148.0.0/16	5,420 (100%)
SSH Version	SSH-2.0-OpenSSH_5.3	4,573 (88.13%)

GoDaddy is for

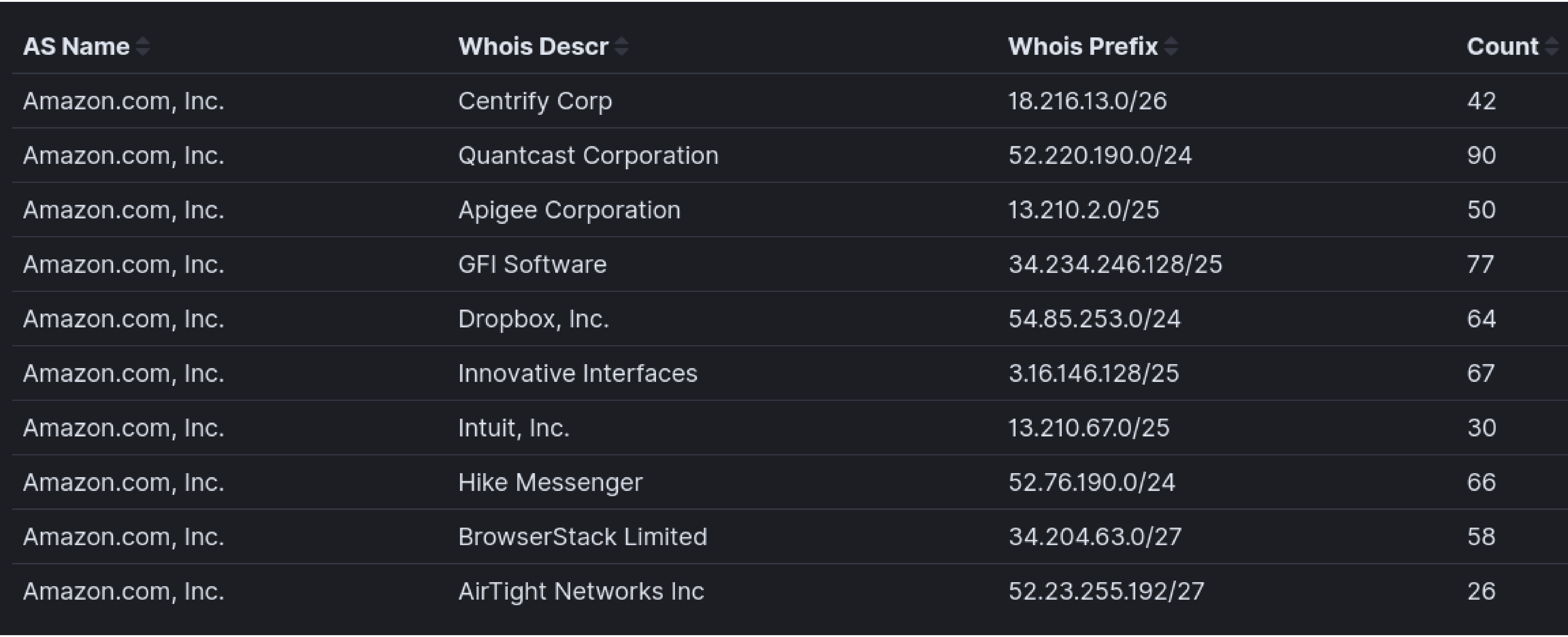
Amazon whois leaks reveals customer

Some Amazon Clients including Prefix



AS Name	Whois Descr	Whois Prefix	Count
Amazon.com, Inc.	PROD IAD	176.32.96.0/21	411
Amazon.com, Inc.	PALO ALTO NETWORKS	18.138.70.0/24	90
Amazon.com, Inc.	Cisco Spark	13.59.223.0/24	214
Amazon.com, Inc.	PROD DUB	176.32.104.0/21	293
Amazon.com, Inc.	Samsung	54.255.252.0/23	131
Amazon.com, Inc.	Zoom Video Communications	18.205.93.128/25	73
Amazon.com, Inc.	Dealer Marketing Services	198.178.114.0/23	259
Amazon.com, Inc.	Veeva Systems	34.225.8.192/26	52
Amazon.com, Inc.	Atlassian Network Services, Inc.	13.52.5.0/25	30
Amazon.com, Inc.	Menlo Security, Inc.	13.56.32.0/25	41

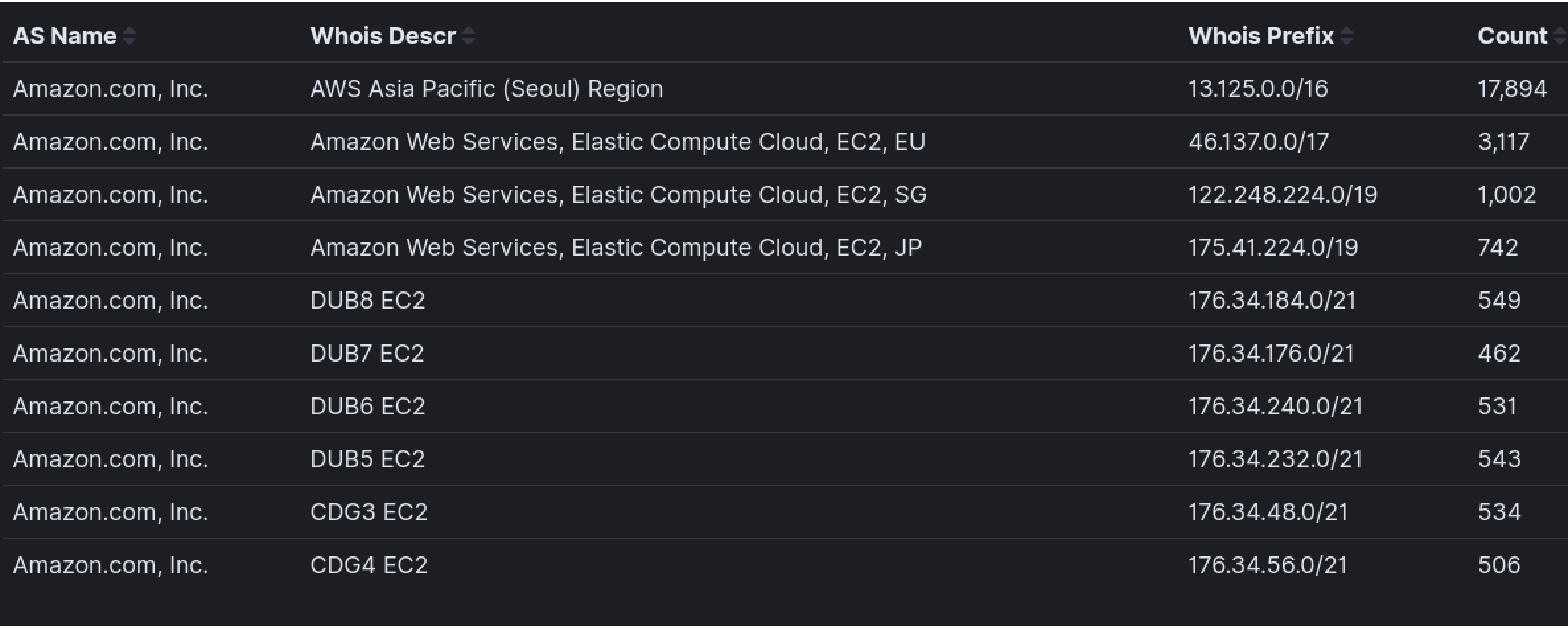
Some Amazon Clients including Prefix



AS Name	Whois Descr	Whois Prefix	Count
Amazon.com, Inc.	Centrify Corp	18.216.13.0/26	42
Amazon.com, Inc.	Quantcast Corporation	52.220.190.0/24	90
Amazon.com, Inc.	Apigee Corporation	13.210.2.0/25	50
Amazon.com, Inc.	GFI Software	34.234.246.128/25	77
Amazon.com, Inc.	Dropbox, Inc.	54.85.253.0/24	64
Amazon.com, Inc.	Innovative Interfaces	3.16.146.128/25	67
Amazon.com, Inc.	Intuit, Inc.	13.210.67.0/25	30
Amazon.com, Inc.	Hike Messenger	52.76.190.0/24	66
Amazon.com, Inc.	BrowserStack Limited	34.204.63.0/27	58
Amazon.com, Inc.	AirTight Networks Inc	52.23.255.192/27	26

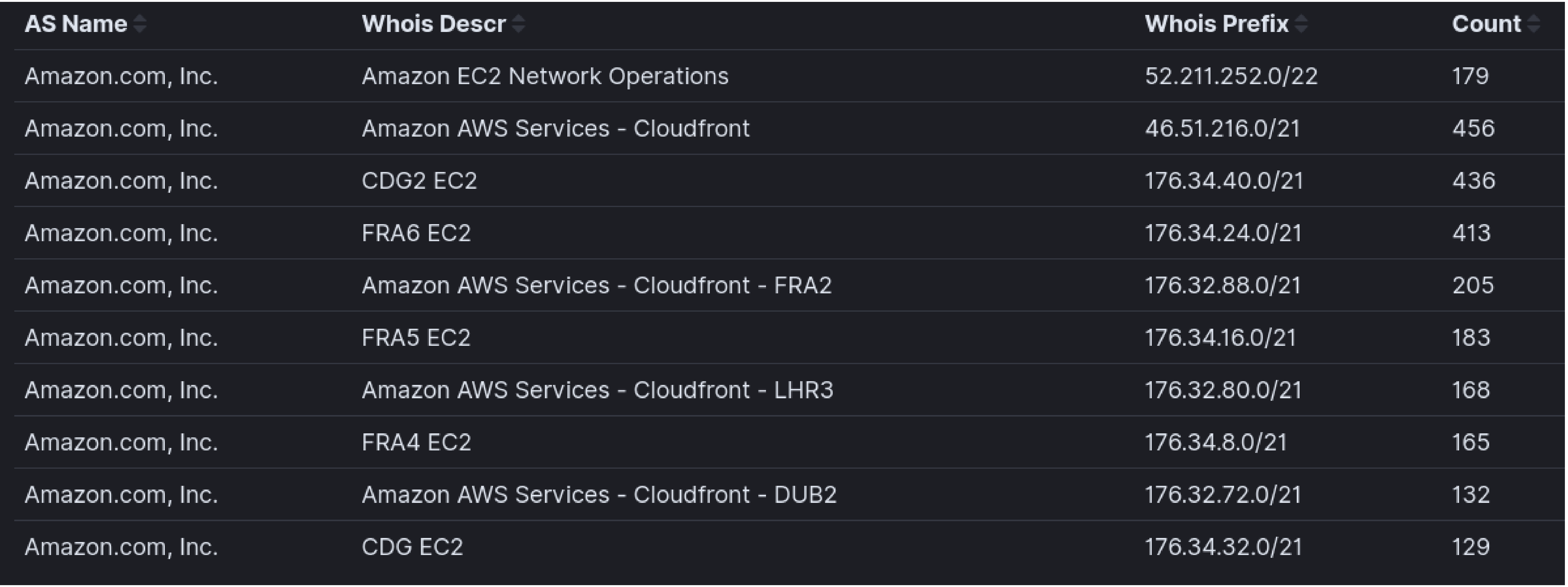
Amazon EC2 Infrastructure

Amazon AWS / EC2 Prefixes + Number HTTPS Server



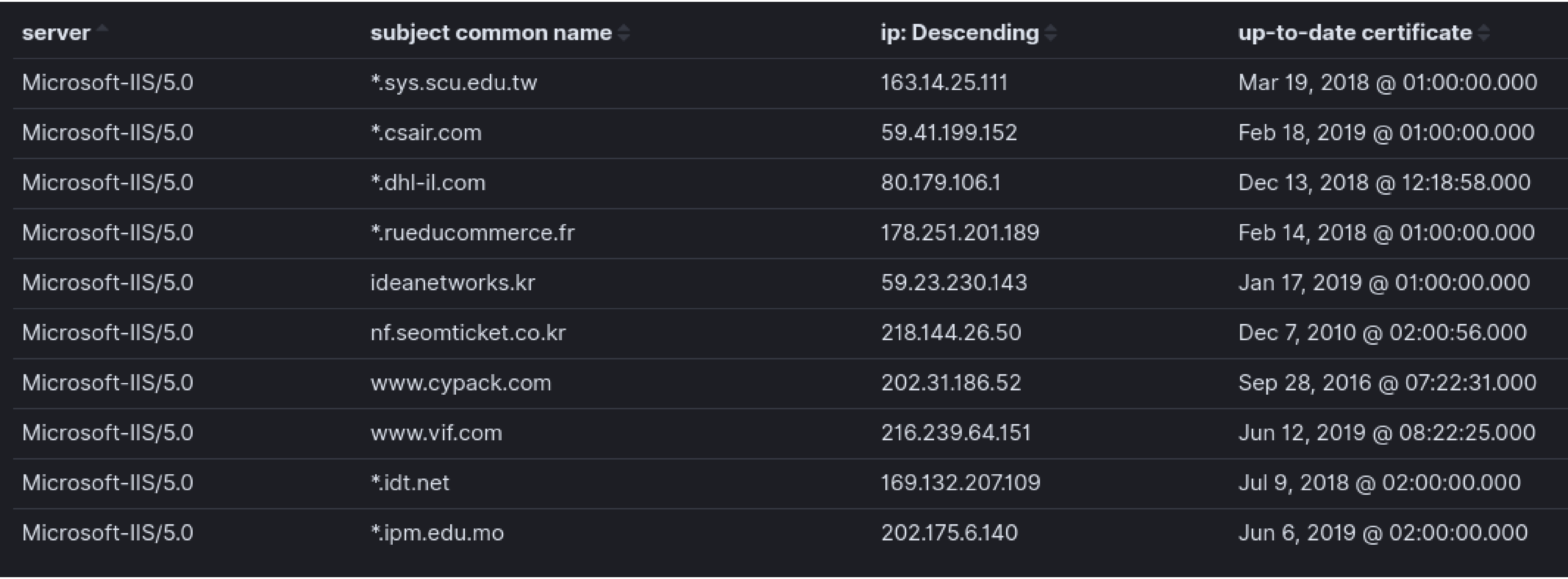
AS Name	Whois Descr	Whois Prefix	Count
Amazon.com, Inc.	AWS Asia Pacific (Seoul) Region	13.125.0.0/16	17,894
Amazon.com, Inc.	Amazon Web Services, Elastic Compute Cloud, EC2, EU	46.137.0.0/17	3,117
Amazon.com, Inc.	Amazon Web Services, Elastic Compute Cloud, EC2, SG	122.248.224.0/19	1,002
Amazon.com, Inc.	Amazon Web Services, Elastic Compute Cloud, EC2, JP	175.41.224.0/19	742
Amazon.com, Inc.	DUB8 EC2	176.34.184.0/21	549
Amazon.com, Inc.	DUB7 EC2	176.34.176.0/21	462
Amazon.com, Inc.	DUB6 EC2	176.34.240.0/21	531
Amazon.com, Inc.	DUB5 EC2	176.34.232.0/21	543
Amazon.com, Inc.	CDG3 EC2	176.34.48.0/21	534
Amazon.com, Inc.	CDG4 EC2	176.34.56.0/21	506

Amazon AWS / EC2 Prefixes + Number HTTPS Server



AS Name	Whois Descr	Whois Prefix	Count
Amazon.com, Inc.	Amazon EC2 Network Operations	52.211.252.0/22	179
Amazon.com, Inc.	Amazon AWS Services - Cloudfront	46.51.216.0/21	456
Amazon.com, Inc.	CDG2 EC2	176.34.40.0/21	436
Amazon.com, Inc.	FRA6 EC2	176.34.24.0/21	413
Amazon.com, Inc.	Amazon AWS Services - Cloudfront - FRA2	176.32.88.0/21	205
Amazon.com, Inc.	FRA5 EC2	176.34.16.0/21	183
Amazon.com, Inc.	Amazon AWS Services - Cloudfront - LHR3	176.32.80.0/21	168
Amazon.com, Inc.	FRA4 EC2	176.34.8.0/21	165
Amazon.com, Inc.	Amazon AWS Services - Cloudfront - DUB2	176.32.72.0/21	132
Amazon.com, Inc.	CDG EC2	176.34.32.0/21	129

Windows 2000 Server with fresh certificates



server	subject common name	ip: Descending	up-to-date certificate
Microsoft-IIS/5.0	*.sys.scu.edu.tw	163.14.25.111	Mar 19, 2018 @ 01:00:00.000
Microsoft-IIS/5.0	*.csair.com	59.41.199.152	Feb 18, 2019 @ 01:00:00.000
Microsoft-IIS/5.0	*.dhl-il.com	80.179.106.1	Dec 13, 2018 @ 12:18:58.000
Microsoft-IIS/5.0	*.rueducommerce.fr	178.251.201.189	Feb 14, 2018 @ 01:00:00.000
Microsoft-IIS/5.0	ideanetworks.kr	59.23.230.143	Jan 17, 2019 @ 01:00:00.000
Microsoft-IIS/5.0	nf.seomticket.co.kr	218.144.26.50	Dec 7, 2010 @ 02:00:56.000
Microsoft-IIS/5.0	www.cypack.com	202.31.186.52	Sep 28, 2016 @ 07:22:31.000
Microsoft-IIS/5.0	www.vif.com	216.239.64.151	Jun 12, 2019 @ 08:22:25.000
Microsoft-IIS/5.0	*.idt.net	169.132.207.109	Jul 9, 2018 @ 02:00:00.000
Microsoft-IIS/5.0	*.ipm.edu.mo	202.175.6.140	Jun 6, 2019 @ 02:00:00.000

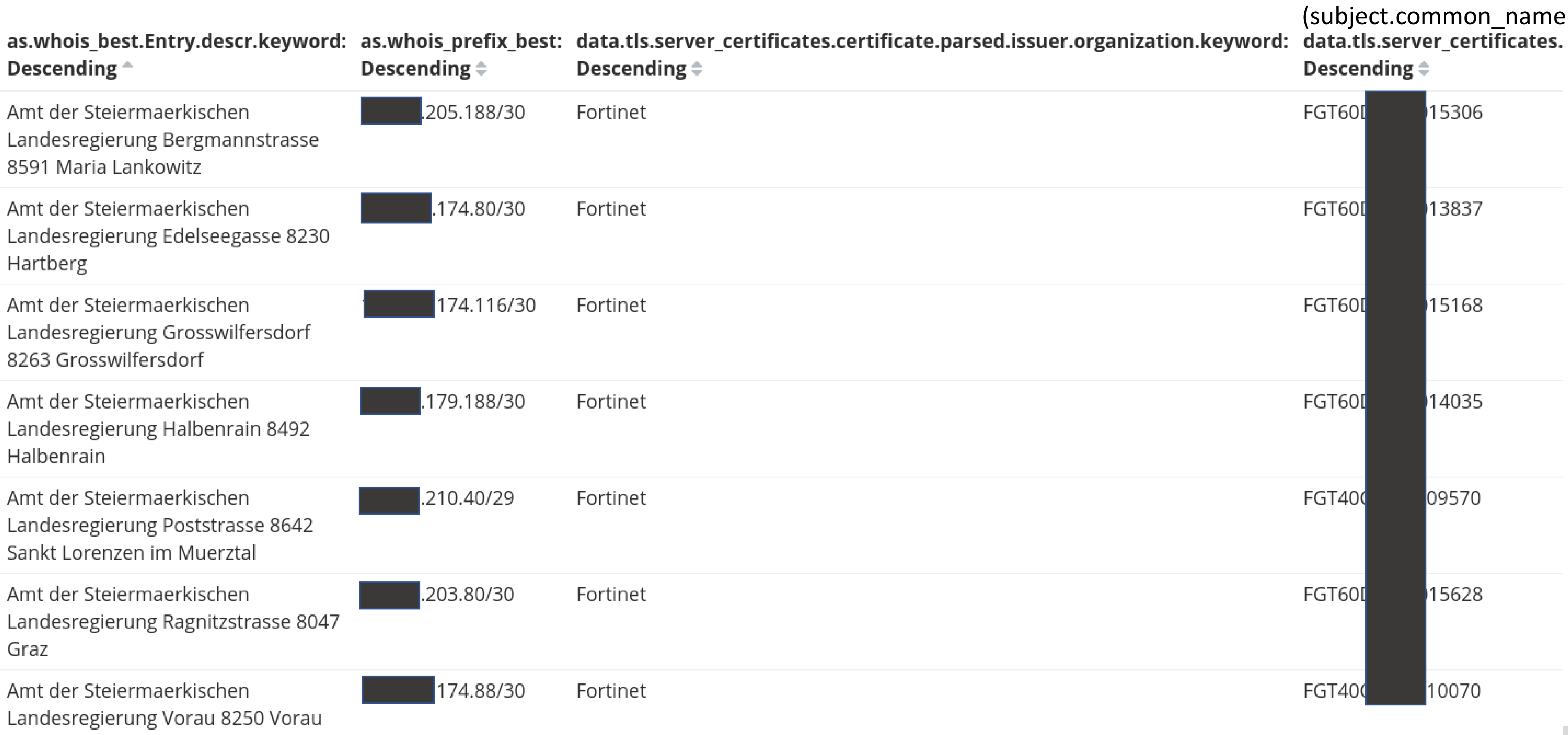
LET'S HAVE A LOOK AT
THE DARK SIDE OF THE INTERNET
imgflip.com

Combination Analysis with Heartbleed

- Query: as.whois_best.Entry.descr:Amt **AND** as.inetnum_best.CountryCode:AT **AND** data.heartbleed.heartbleed_vulnerable:true **AND** data.tls.server_certificates.certificate.parsed.issuer.organization: "Fortinet“

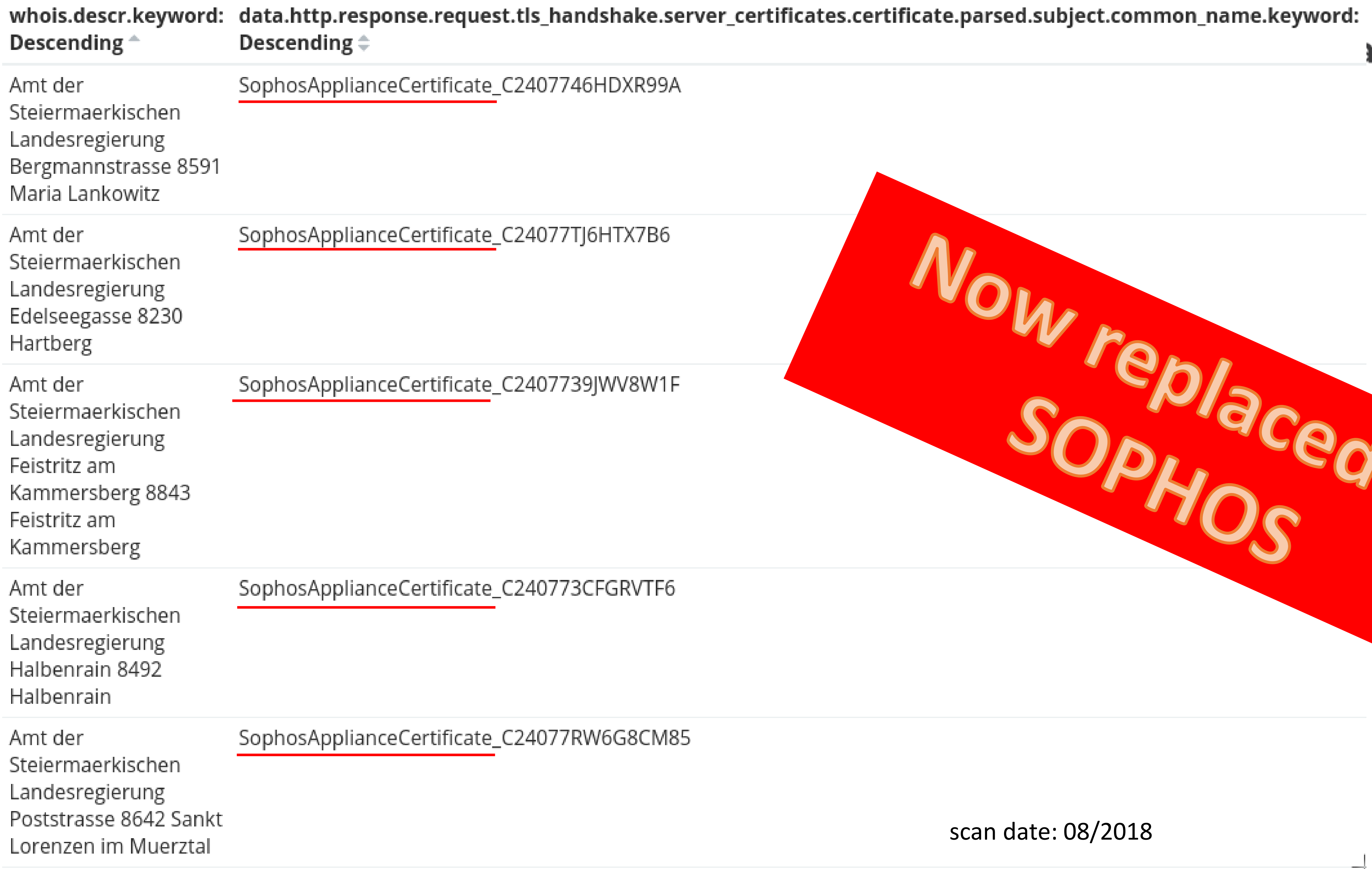
- Search for all devices on the net that are
  - in Austria contain the word "office" in the WHOIS
  - have a TLS certificate from "Fortinet
  - have a heartbleed vulnerability

Kombinationsanalysen mit Heartbleed



as.whois_best.Entry.descr.keyword: Descending	as.whois_prefix_best: Descending	data.tls.server_certificates.certificate.parsed.issuer.organization.keyword: Descending	(subject.common_name) data.tls.server_certificates. Descending
Amt der Steiermaerkischen Landesregierung Bergmannstrasse 8591 Maria Lankowitz	[redacted].205.188/30	Fortinet	FGT60[redacted]15306
Amt der Steiermaerkischen Landesregierung Edelseegasse 8230 Hartberg	[redacted].174.80/30	Fortinet	FGT60[redacted]13837
Amt der Steiermaerkischen Landesregierung Grosswilfersdorf 8263 Grosswilfersdorf	[redacted]174.116/30	Fortinet	FGT60[redacted]15168
Amt der Steiermaerkischen Landesregierung Halbenrain 8492 Halbenrain	[redacted].179.188/30	Fortinet	FGT60[redacted]14035
Amt der Steiermaerkischen Landesregierung Poststrasse 8642 Sankt Lorenzen im Muerztal	[redacted].210.40/29	Fortinet	FGT40[redacted]09570
Amt der Steiermaerkischen Landesregierung Ragnitzstrasse 8047 Graz	[redacted].203.80/30	Fortinet	FGT60[redacted]15628
Amt der Steiermaerkischen Landesregierung Vorau 8250 Vorau	[redacted]174.88/30	Fortinet	FGT40[redacted]10070

scan date: 04/2017

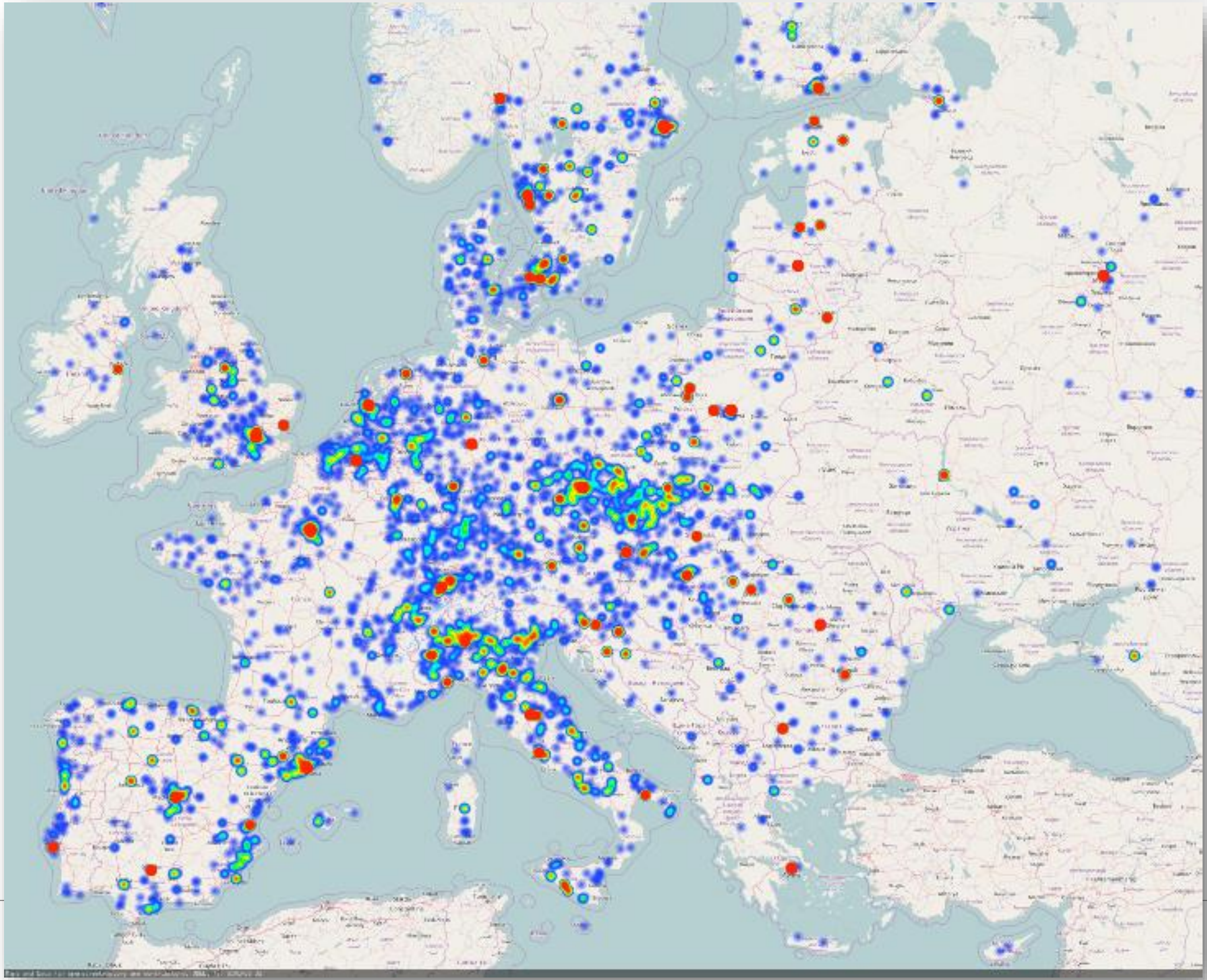


whois.descr.keyword: Descending	data.http.response.request.tls_handshake.server_certificates.certificate.parsed.subject.common_name.keyword: Descending
Amt der Steiermaerkischen Landesregierung Bergmannstrasse 8591 Maria Lankowitz	SophosApplianceCertificate_C2407746HDXR99A
Amt der Steiermaerkischen Landesregierung Edelseegasse 8230 Hartberg	SophosApplianceCertificate_C24077TJ6HTX7B6
Amt der Steiermaerkischen Landesregierung Feistritz am Kammersberg 8843 Feistritz am Kammersberg	SophosApplianceCertificate_C2407739JWV8W1F
Amt der Steiermaerkischen Landesregierung Halbenrain 8492 Halbenrain	SophosApplianceCertificate_C240773CFGRVTF6
Amt der Steiermaerkischen Landesregierung Poststrasse 8642 Sankt Lorenzen im Muerztal	SophosApplianceCertificate_C24077RW6G8CM85

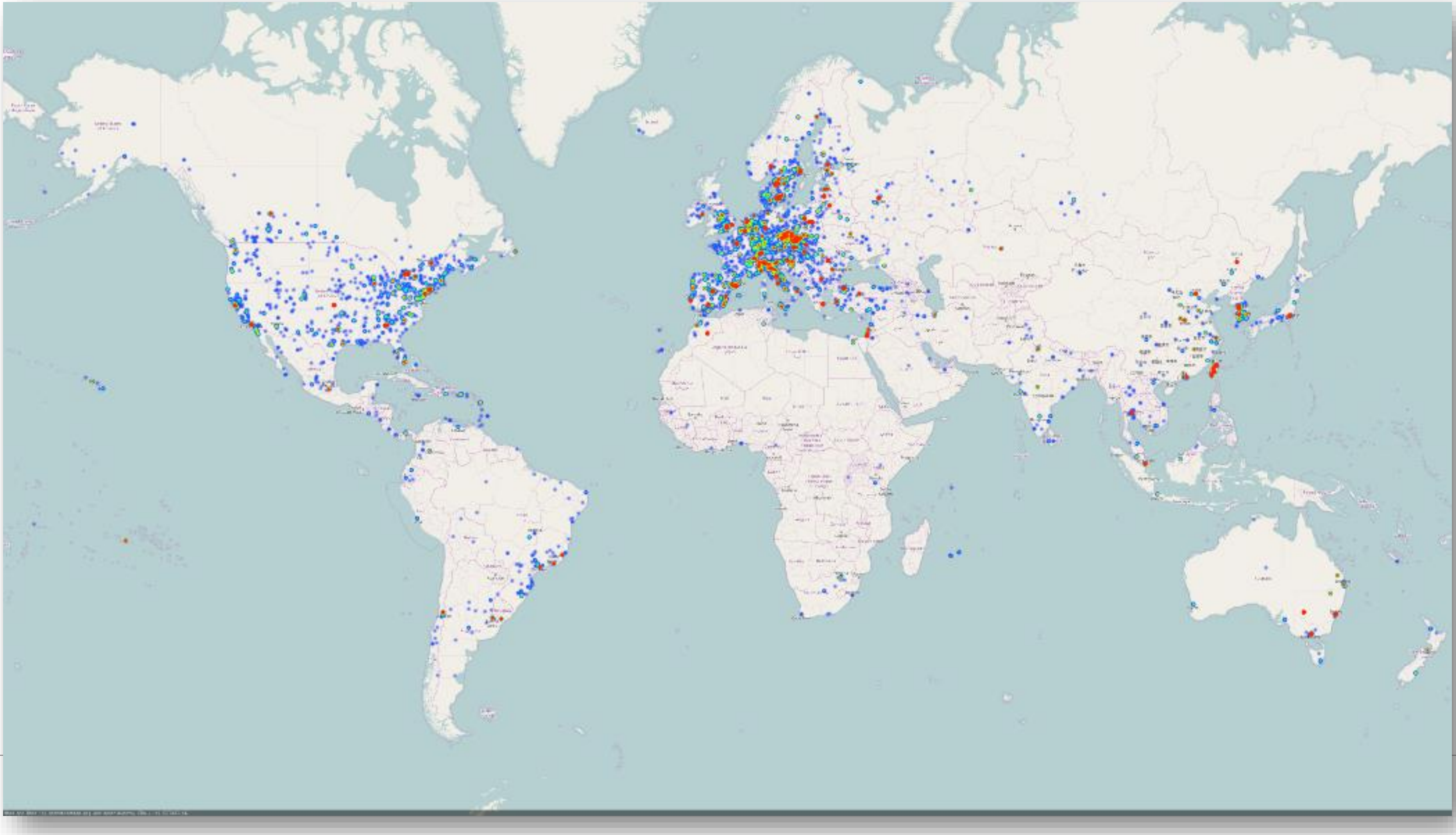
Now replaced by SOPHOS

scan date: 08/2018

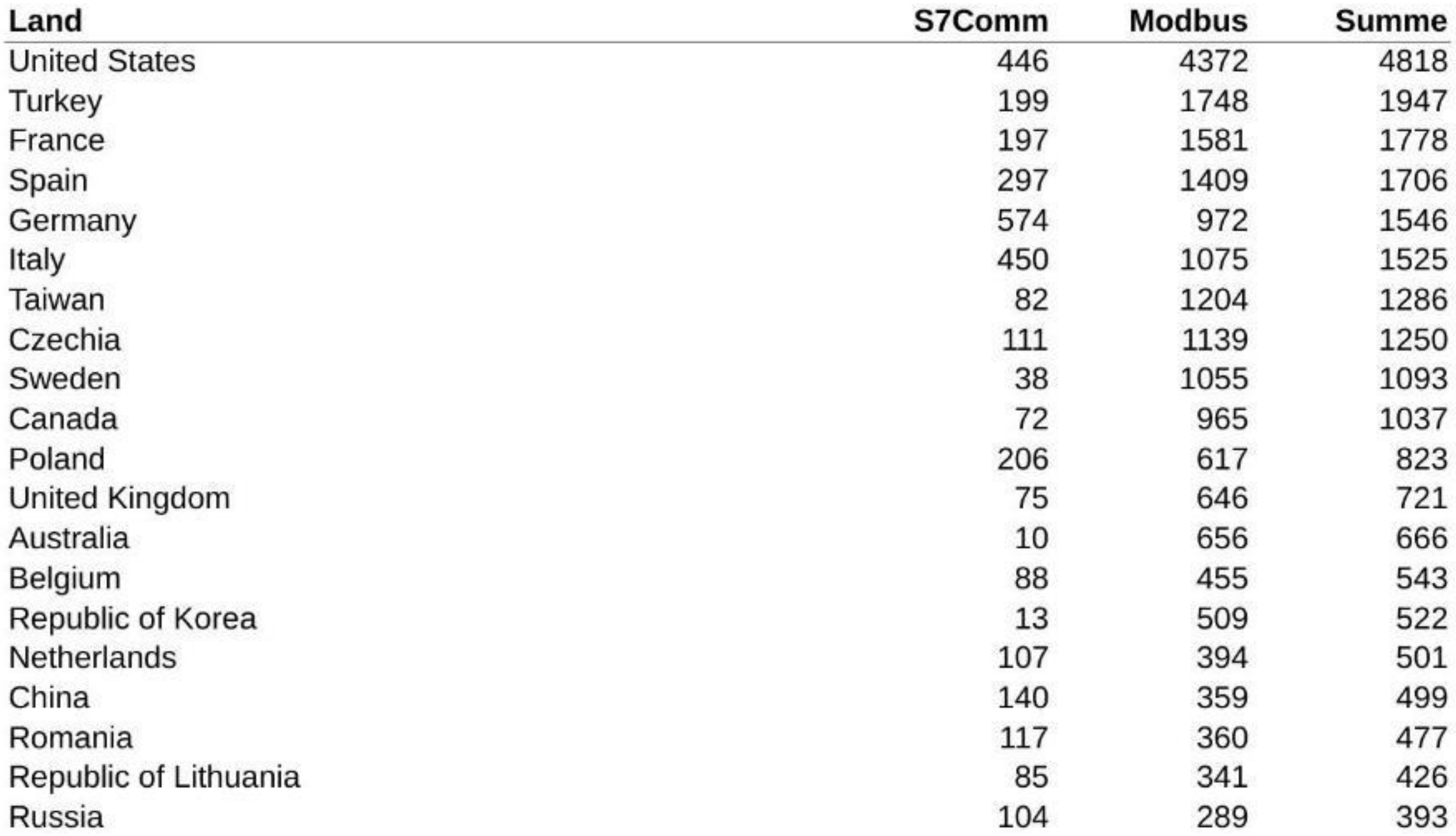
Public Accessible Industrial Control Systems



Public Accessible Industrial Control Systems

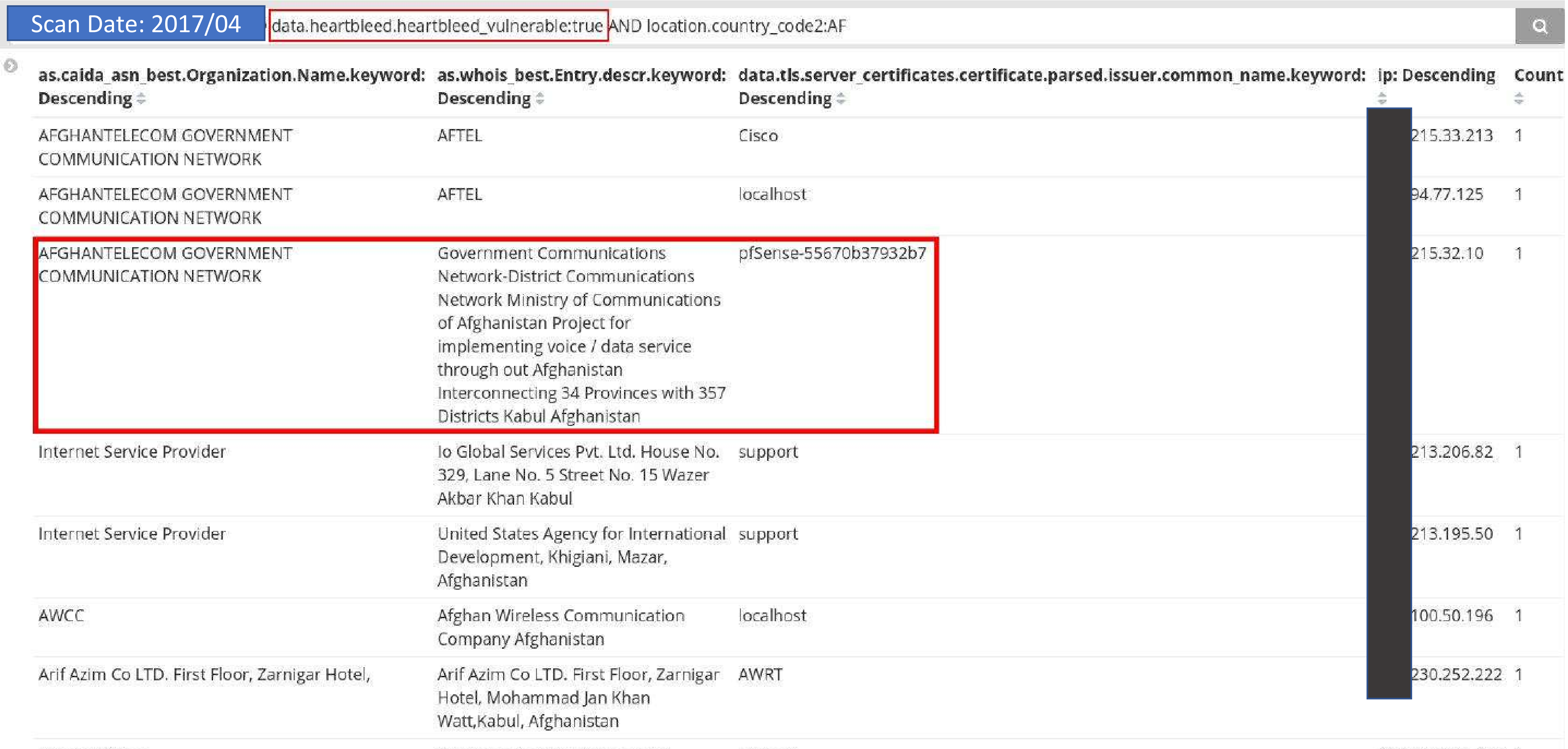


Public Accessible Industrial Control Systems



Land	S7Comm	Modbus	Summe
United States	446	4372	4818
Turkey	199	1748	1947
France	197	1581	1778
Spain	297	1409	1706
Germany	574	972	1546
Italy	450	1075	1525
Taiwan	82	1204	1286
Czechia	111	1139	1250
Sweden	38	1055	1093
Canada	72	965	1037
Poland	206	617	823
United Kingdom	75	646	721
Australia	10	656	666
Belgium	88	455	543
Republic of Korea	13	509	522
Netherlands	107	394	501
China	140	359	499
Romania	117	360	477
Republic of Lithuania	85	341	426
Russia	104	289	393

Heart-Bleed vulnerable pfSense FW detected in the Afghan Government communication Network

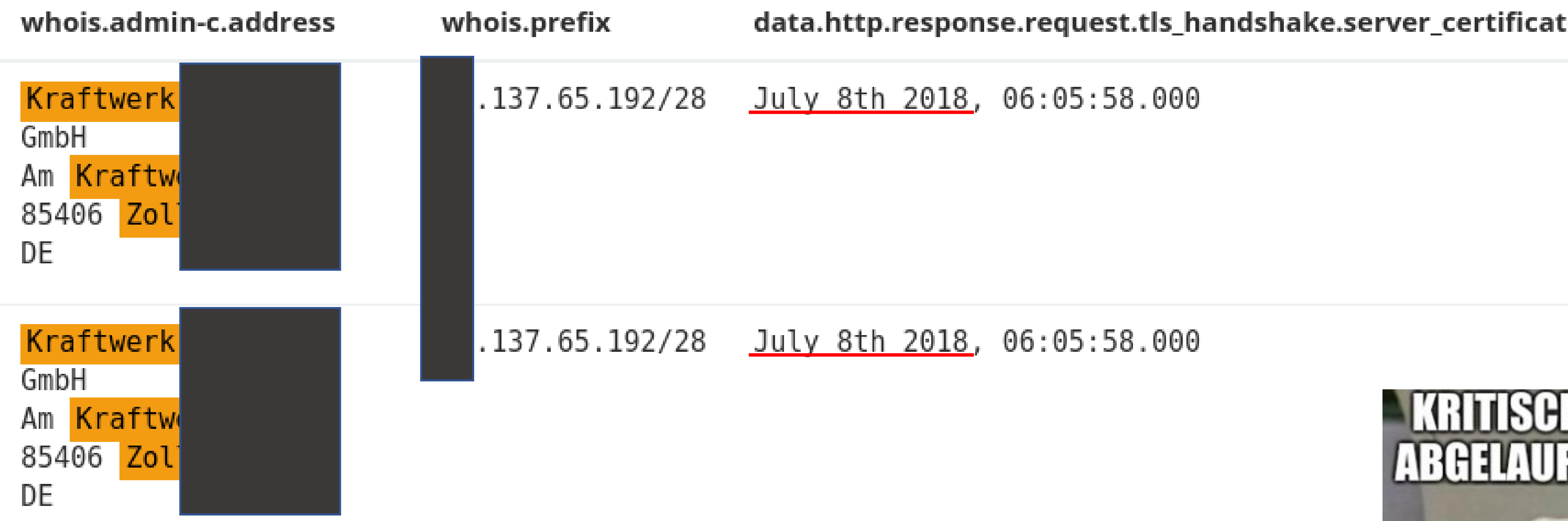


Scan Date: 2017/04

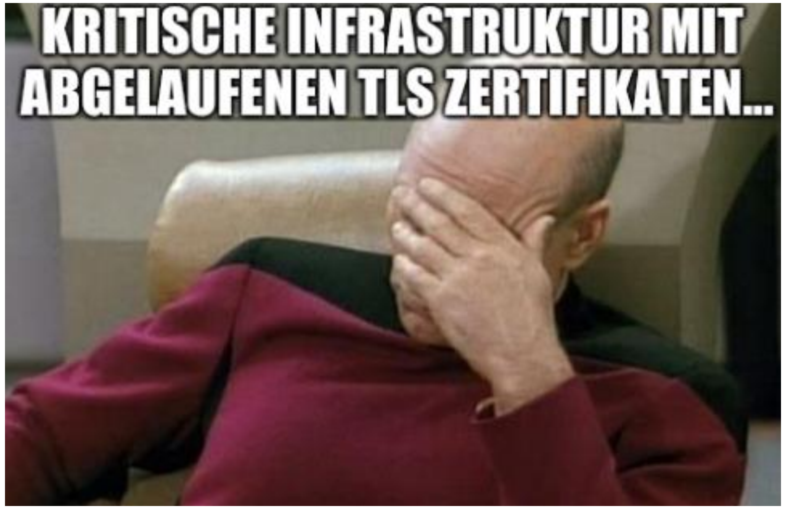
data.heartbleed.heartbleed_vulnerable:true AND location.country_code2:AF

as.caida_asn_best.Organization.Name.keyword: Descending	as.whois_best.Entry.descr.keyword: Descending	data.tls.server_certificates.certificate.parsed.issuer.common_name.keyword: Descending	ip: Descending	Count
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	AFTEL	Cisco	[redacted]215.33.213	1
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	AFTEL	localhost	[redacted]94.77.125	1
AFGHANTELECOM GOVERNMENT COMMUNICATION NETWORK	Government Communications Network-District Communications Network Ministry of Communications of Afghanistan Project for implementing voice / data service through out Afghanistan Interconnecting 34 Provinces with 357 Districts Kabul Afghanistan	pfSense-55670b37932b7	[redacted]215.32.10	1
Internet Service Provider	Io Global Services Pvt. Ltd. House No. 329, Lane No. 5 Street No. 15 Wazer Akbar Khan Kabul	support	[redacted]213.206.82	1
Internet Service Provider	United States Agency for International Development, Khigiani, Mazar, Afghanistan	support	[redacted]213.195.50	1
AWCC	Afghan Wireless Communication Company Afghanistan	localhost	[redacted]100.50.196	1
Arif Azim Co LTD. First Floor, Zarnigar Hotel,	Arif Azim Co LTD. First Floor, Zarnigar Hotel, Mohammad Jan Khan Watt,Kabul, Afghanistan	AWRT	[redacted]230.252.222	1

Critical Infrastructure



whois.admin-c.address	whois.prefix	data.http.response.request.tls_handshake.server_certificates.certificate.parsed.validity.end
Kraftwerk [redacted] GmbH Am Kraftw 85406 Zol DE	[redacted].137.65.192/28	July 8th 2018, 06:05:58.000
Kraftwerk [redacted] GmbH Am Kraftw 85406 Zol DE	[redacted].137.65.192/28	July 8th 2018, 06:05:58.000


KRITISCHE INFRASTRUKTUR MIT ABGELAUFENEN TLS ZERTIFIKATEN...

- It is a larger german coal-fired power plant and at least one VPN endpoint
- ~500 MW capacity, supplies ~1.5 million people

Scan date: 08/2018 - Status Update: 11/208 : still out of date (already contacted them) - New Certificate since 04/2019.

Summary

- Using raw data of scans with BGP, whois, and protocol specific information enables you to:
  - Identification of many external IP addresses, websites or vulnerabilities that may belong to a company, critical infrastructure or government agencies
  - Distribution analyses in which AS / prefix certain services are used most
  - Comprehensive topology / structural analysis of a specific network

Summary

- Get you own AS with 1024 IPv4 Addresses and a colocation space for scanning works very good
- Scanning with 70mbit/s (6-7h) works good
- 1 SYN / 2 SYNs makes no big difference
- Scanning the Internet in ~2 hours (ca. 200mbit/s) from a single IP decreases your results by 10-30%
- Scan only routed BGP-prefix will save ~35% of SYN traffic and time
- Using BGP-Prefix hitlists for fast intervall scanning can reduce the SYN traffic by further 25-50%

THE END

Contact:
garak-ccc@gmx.de

Twitter:
@AlphaStrikeLabs