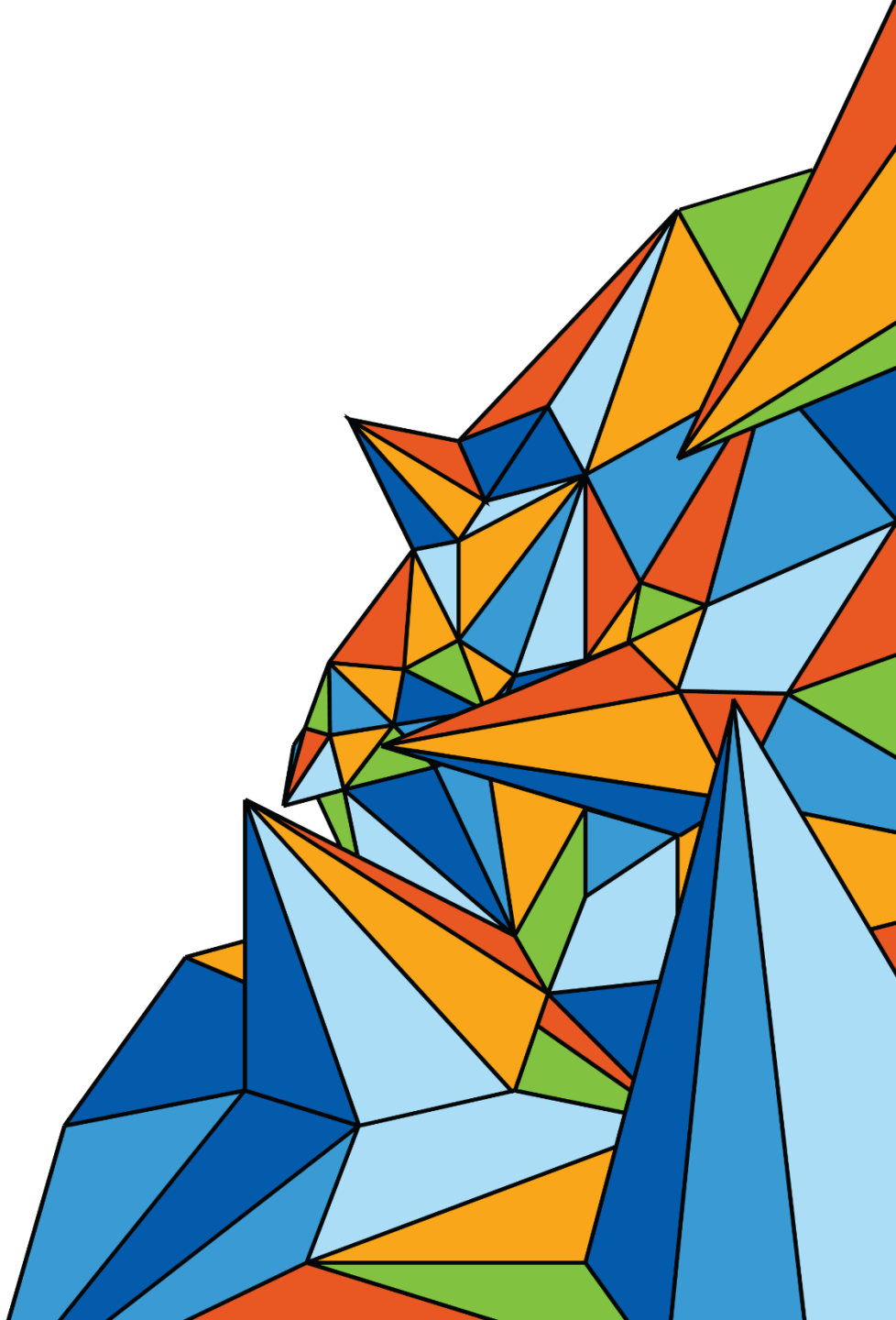
2015 UNITED
RAPID7 SECURITY SUMMIT

RAPID7 RESEARCH

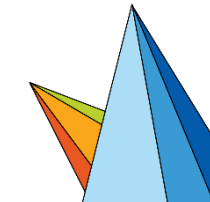
PROJECT SONAR

HD Moore



Agenda

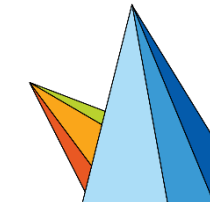
- Internet Scanning
- Global Overview
- Exposure Trends



What this talk is NOT about

- Making fun of technology users due to product flaws
- Image galleries of open industrial systems
- Snapshots of baby monitor cameras
- Shaming product vendors
- ShellHeartPoodleBleed
- Pew Pew Attack Maps

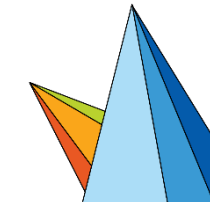
Internet Scanning



RAPID7

Why Scan the Internet?

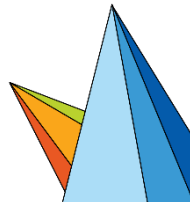
- Improve security decision making with real-world data
- Fix endemic security flaws before they get exploited
- Prioritize vulnerability research according to impact
- Improve open source security tools
- Hold vendors accountable
- Make the Internet safer
- The kids are doing it



Why You Shouldn’t Scan the Internet

- Network administrators see scans as attacks
- Scanning the internet is resource-intensive
- Lots of complaints (legal & physical)
- IP addresses constantly shuffle
- Processing can be difficult

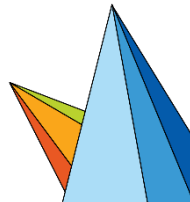
- **Skip all of this and use publicly available data!**



Internet Scanning with Project Sonar

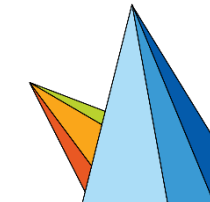
- Focused entirely on IPv4 and public DNS records
  - 1.0.0.0 to 223.255.255.255
  - Exclude reserved & private ranges
  - Exclude our opt-out list
- Scan about 3.7 billion IPv4 addresses
  - Scans run sequentially, from a single server
  - Typically span Monday - Friday

* Unless you opted out, see https://sonar.labs.rapid7.com/



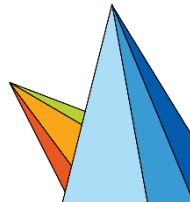
TCP & UDP Scanning

- Use Zmap to scan all of IPv4, except for opt-out ranges
- UDP scans are throttled to 180,000 pps on average
- TCP scans only send the SYN packet
- AWS nodes used to grab banners
- Data is deduplicated & decoded
- Uploaded to https://scans.io/



Project Sonar TCP & UDP Services

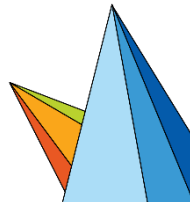
UDP	UDP	SSL	TCP
53	1900	25	22*
111	5060	143	80*
123	5351	443	445*
137	5353	993	
623	17185	995	
1434	47808		



RAPID7

Reverse DNS Enumeration

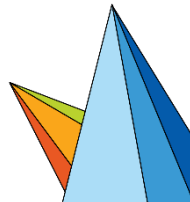
- Reverse DNS lookup of 0.0.0.0/0 every two weeks
  - Use dozens of cloud nodes to balance the load
  - Accidentally melted a few Tier-1 ISPs*
- 1.2 billion PTR records on average



Forward DNS Enumeration

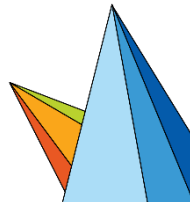
- Forward DNS is driven by a giant list of hostnames
  - Pulled from TLD/gTLD zone files
  - Extracted form SSL certificates (SAN/CN)
  - Extracted from HTTP scan HTML references
  - Extracted from PTR records

- 1.4 billion records on average



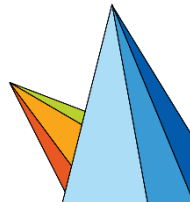
Data, Tools, and Documentation

- Public Datasets
  - https://scans.io/
- Open Source Tools
  - https://zmap.io/
  - https://nmap.org/
  - https://github.com/rapid7/dap/ && https://github.com/rapid7/recog/
- Documentation
  - https://github.com/rapid7/sonar/wiki

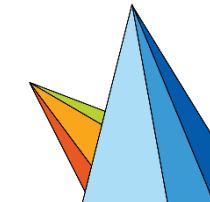


Other Projects & Data Sources

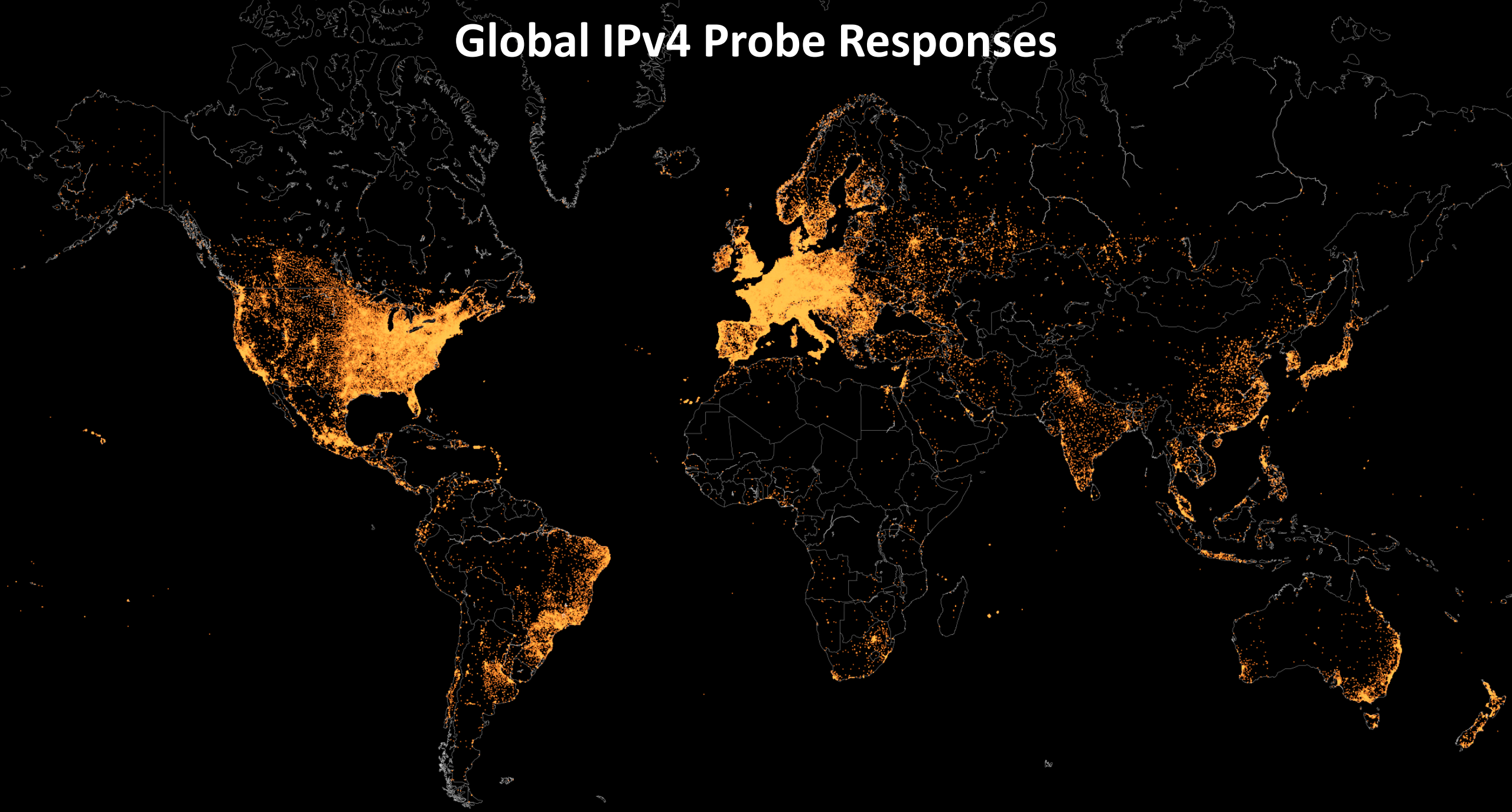
- Active scanning projects with public data
  - University of Michigan: https://scans.io/
  - Shodan: https://shodan.io/
- Older scanning projects with public data
  - http://internetcensus2012.bitbucket.org/ (2012)
- Previous scanning projects
  - Critical.IO (2012-2013)
  - PTCoreSec (2012+)
  - Metlstorm: “Low Hanging Kiwi Fruit” (2009+)
  - Nmap: Scanning the Internet (2008)
  - BASS (1998)



Global Overview

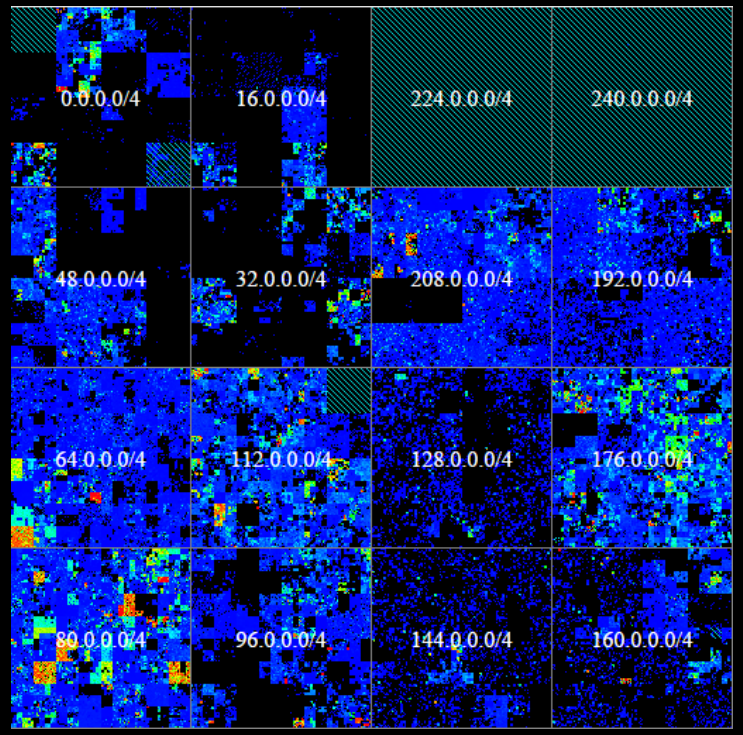


Global IPv4 Probe Responses

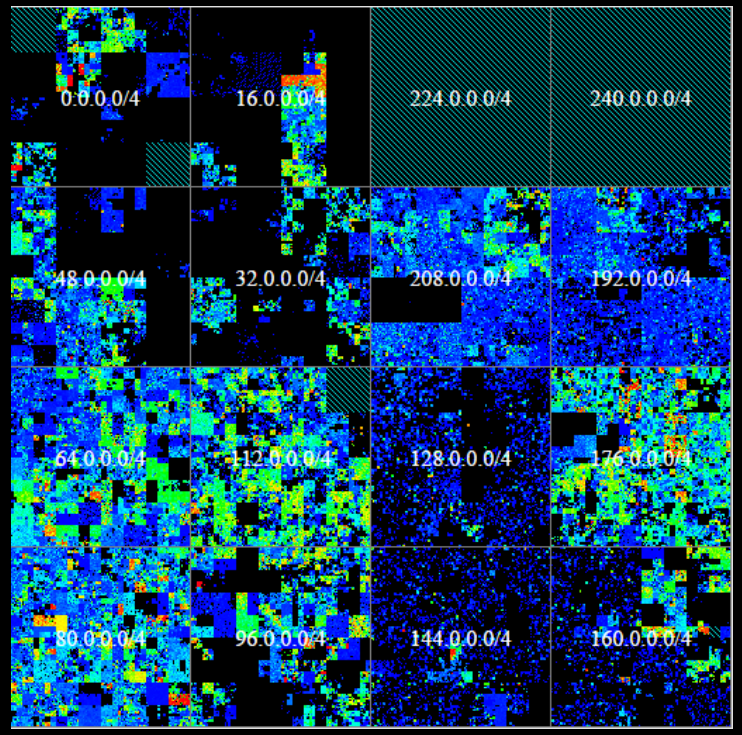


Source: 2015-04-06 Shodan ICMP scan + Project Sonar UDP & TCP scans

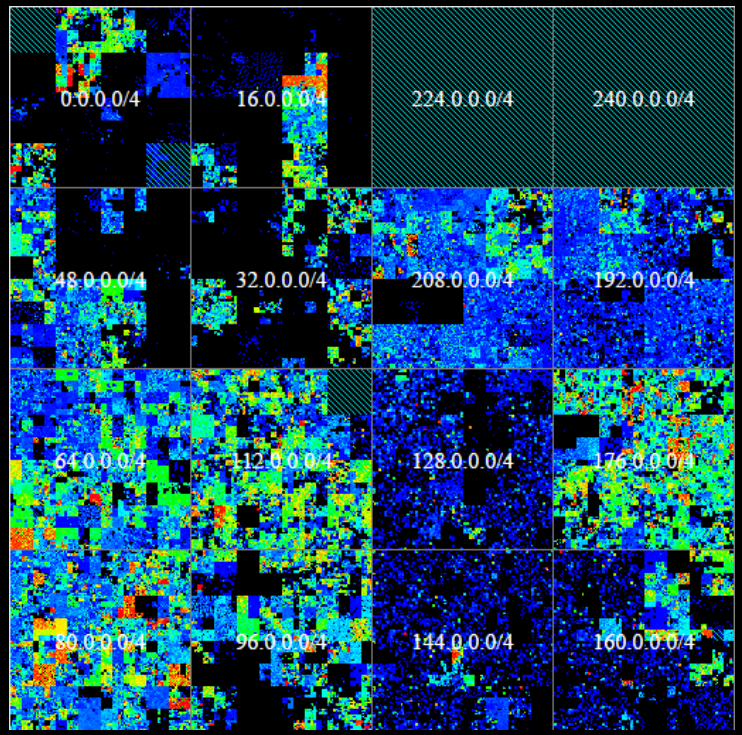
UDP Only



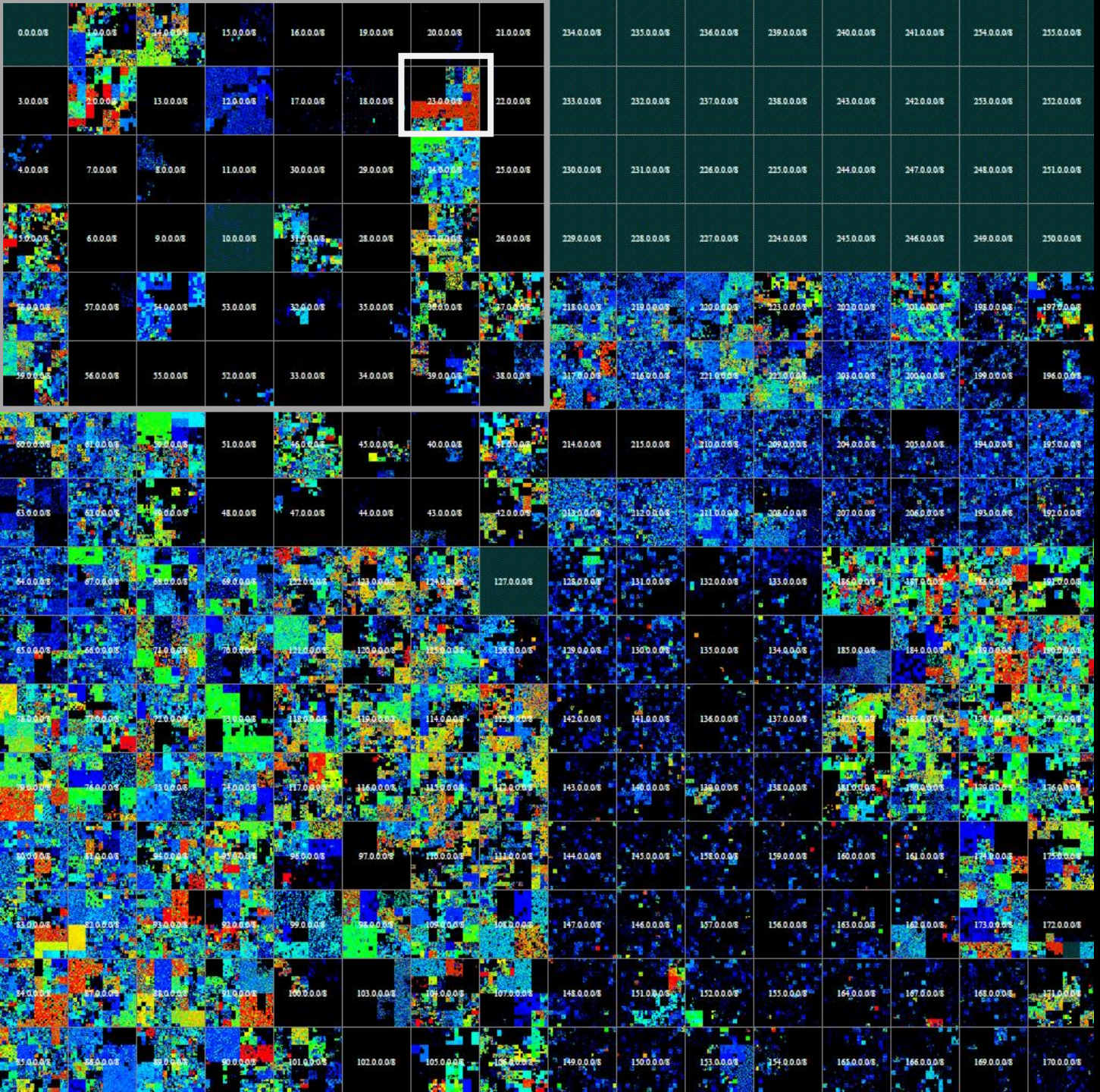
ICMP Only

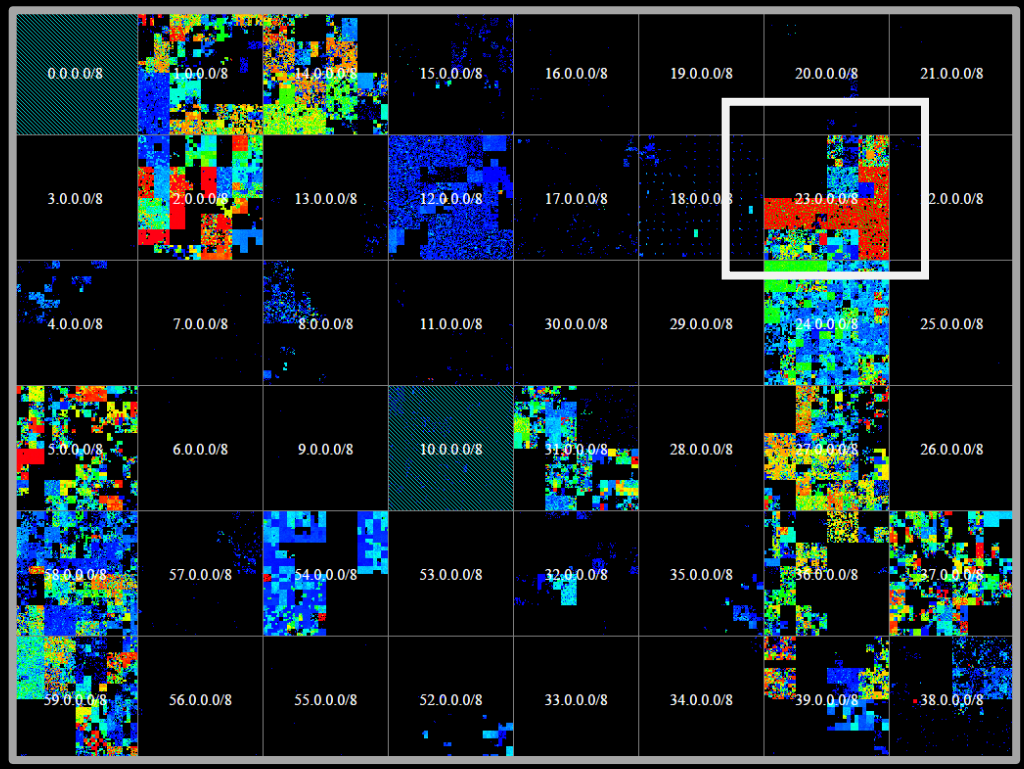


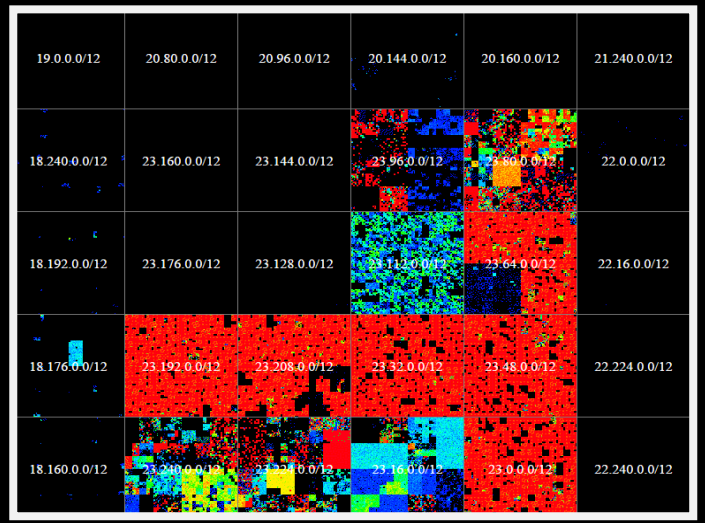
Combined



Source: 2015-04-06 Shodan ICMP scan + Project Sonar UDP & TCP scans

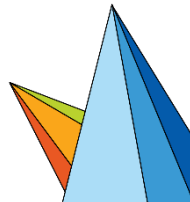

0.0.0.0/8
1.0.0.0/8
14.0.0.0/8
15.0.0.0/8
16.0.0.0/8
19.0.0.0/8
20.0.0.0/8
21.0.0.0/8
3.0.0.0/8
2.0.0.0/8
13.0.0.0/8
12.0.0.0/8
17.0.0.0/8
18.0.0.0/8
23.0.0.0/8
22.0.0.0/8
4.0.0.0/8
7.0.0.0/8
8.0.0.0/8
11.0.0.0/8
30.0.0.0/8
29.0.0.0/8
24.0.0.0/8
25.0.0.0/8
5.0.0.0/8
6.0.0.0/8
9.0.0.0/8
10.0.0.0/8
31.0.0.0/8
28.0.0.0/8
27.0.0.0/8
26.0.0.0/8
58.0.0.0/8
57.0.0.0/8
54.0.0.0/8
53.0.0.0/8
32.0.0.0/8
35.0.0.0/8
36.0.0.0/8
37.0.0.0/8
59.0.0.0/8
56.0.0.0/8
55.0.0.0/8
52.0.0.0/8
33.0.0.0/8
34.0.0.0/8
39.0.0.0/8
38.0.0.0/8
60.0.0.0/8
61.0.0.0/8
62.0.0.0/8
51.0.0.0/8
50.0.0.0/8
45.0.0.0/8
40.0.0.0/8
41.0.0.0/8
63.0.0.0/8
64.0.0.0/8
67.0.0.0/8
68.0.0.0/8
69.0.0.0/8
122.0.0.0/8
123.0.0.0/8
124.0.0.0/8
127.0.0.0/8
65.0.0.0/8
66.0.0.0/8
71.0.0.0/8
70.0.0.0/8
121.0.0.0/8
120.0.0.0/8
125.0.0.0/8
126.0.0.0/8
72.0.0.0/8
77.0.0.0/8
73.0.0.0/8
118.0.0.0/8
119.0.0.0/8
114.0.0.0/8
74.0.0.0/8
75.0.0.0/8
117.0.0.0/8
116.0.0.0/8
115.0.0.0/8
80.0.0.0/8
81.0.0.0/8
84.0.0.0/8
85.0.0.0/8
96.0.0.0/8
97.0.0.0/8
110.0.0.0/8
111.0.0.0/8
83.0.0.0/8
82.0.0.0/8
93.0.0.0/8
92.0.0.0/8
99.0.0.0/8
98.0.0.0/8
109.0.0.0/8
108.0.0.0/8
86.0.0.0/8
87.0.0.0/8
88.0.0.0/8
91.0.0.0/8
100.0.0.0/8
103.0.0.0/8
104.0.0.0/8
107.0.0.0/8
95.0.0.0/8
94.0.0.0/8
89.0.0.0/8
90.0.0.0/8
101.0.0.0/8
102.0.0.0/8
105.0.0.0/8
106.0.0.0/8
234.0.0.0/8
235.0.0.0/8
236.0.0.0/8
239.0.0.0/8
240.0.0.0/8
241.0.0.0/8
254.0.0.0/8
255.0.0.0/8
233.0.0.0/8
232.0.0.0/8
237.0.0.0/8
238.0.0.0/8
243.0.0.0/8
242.0.0.0/8
253.0.0.0/8
252.0.0.0/8
230.0.0.0/8
231.0.0.0/8
226.0.0.0/8
225.0.0.0/8
244.0.0.0/8
247.0.0.0/8
248.0.0.0/8
251.0.0.0/8
229.0.0.0/8
228.0.0.0/8
227.0.0.0/8
224.0.0.0/8
245.0.0.0/8
246.0.0.0/8
249.0.0.0/8
250.0.0.0/8
218.0.0.0/8
219.0.0.0/8
220.0.0.0/8
223.0.0.0/8
202.0.0.0/8
201.0.0.0/8
198.0.0.0/8
197.0.0.0/8
217.0.0.0/8
216.0.0.0/8
221.0.0.0/8
222.0.0.0/8
203.0.0.0/8
200.0.0.0/8
199.0.0.0/8
196.0.0.0/8
214.0.0.0/8
215.0.0.0/8
210.0.0.0/8
209.0.0.0/8
204.0.0.0/8
205.0.0.0/8
194.0.0.0/8
195.0.0.0/8
213.0.0.0/8
212.0.0.0/8
211.0.0.0/8
208.0.0.0/8
207.0.0.0/8
206.0.0.0/8
193.0.0.0/8
192.0.0.0/8
128.0.0.0/8
131.0.0.0/8
132.0.0.0/8
133.0.0.0/8
184.0.0.0/8
187.0.0.0/8
183.0.0.0/8
191.0.0.0/8
129.0.0.0/8
130.0.0.0/8
135.0.0.0/8
134.0.0.0/8
185.0.0.0/8
182.0.0.0/8
189.0.0.0/8
190.0.0.0/8
142.0.0.0/8
141.0.0.0/8
136.0.0.0/8
137.0.0.0/8
143.0.0.0/8
140.0.0.0/8
139.0.0.0/8
138.0.0.0/8
181.0.0.0/8
180.0.0.0/8
179.0.0.0/8
176.0.0.0/8
144.0.0.0/8
145.0.0.0/8
158.0.0.0/8
159.0.0.0/8
160.0.0.0/8
161.0.0.0/8
174.0.0.0/8
175.0.0.0/8
147.0.0.0/8
146.0.0.0/8
157.0.0.0/8
156.0.0.0/8
163.0.0.0/8
162.0.0.0/8
173.0.0.0/8
172.0.0.0/8
148.0.0.0/8
151.0.0.0/8
152.0.0.0/8
155.0.0.0/8
164.0.0.0/8
167.0.0.0/8
168.0.0.0/8
171.0.0.0/8
149.0.0.0/8
150.0.0.0/8
153.0.0.0/8
154.0.0.0/8
165.0.0.0/8
166.0.0.0/8
169.0.0.0/8
170.0.0.0/8


0.0.0.0/8
1.0.0.0/8
14.0.0.0/8
15.0.0.0/8
16.0.0.0/8
19.0.0.0/8
20.0.0.0/8
21.0.0.0/8
3.0.0.0/8
2.0.0.0/8
13.0.0.0/8
12.0.0.0/8
17.0.0.0/8
18.0.0.0/8
23.0.0.0/8
22.0.0.0/8
4.0.0.0/8
7.0.0.0/8
8.0.0.0/8
11.0.0.0/8
30.0.0.0/8
29.0.0.0/8
24.0.0.0/8
25.0.0.0/8
5.0.0.0/8
6.0.0.0/8
9.0.0.0/8
10.0.0.0/8
31.0.0.0/8
28.0.0.0/8
27.0.0.0/8
26.0.0.0/8
58.0.0.0/8
57.0.0.0/8
54.0.0.0/8
53.0.0.0/8
32.0.0.0/8
35.0.0.0/8
36.0.0.0/8
37.0.0.0/8
59.0.0.0/8
56.0.0.0/8
55.0.0.0/8
52.0.0.0/8
33.0.0.0/8
34.0.0.0/8
39.0.0.0/8
38.0.0.0/8


19.0.0.0/12
20.80.0.0/12
20.96.0.0/12
20.144.0.0/12
20.160.0.0/12
21.240.0.0/12
18.240.0.0/12
23.160.0.0/12
23.144.0.0/12
23.96.0.0/12
23.80.0.0/12
22.0.0.0/12
18.192.0.0/12
23.176.0.0/12
23.128.0.0/12
23.112.0.0/12
23.64.0.0/12
22.16.0.0/12
18.176.0.0/12
23.192.0.0/12
23.208.0.0/12
23.32.0.0/12
23.48.0.0/12
22.224.0.0/12
18.160.0.0/12
23.240.0.0/12
23.224.0.0/12
23.16.0.0/12
23.0.0.0/12
22.240.0.0/12

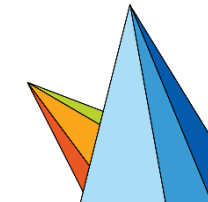
What is the internet?

- In terms of unique systems? Nobody really knows
  - Cisco claimed **8.7 billion** in 2012, predicted **15 billion** in 2015
  - Carrier NAT hides a millions of connected nodes
  - Firewalls and traditional NAT hide the rest
  - Over 7 billion active mobile phones
  - IPv6 gateways also do IPv4 NAT



What is directly exposed on the IPv4 internet?

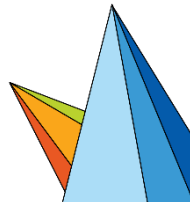
- Approximately 1 billion IPv4 systems are directly connected
  - ~500 million broadband clients and gateways
  - ~200 million servers (web, email, database, VPN)
  - ~200 million mobile devices (phones, tablets)
  - ~100 million devices (routers, printers, cameras)



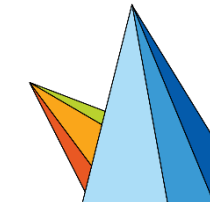
What about IPv6?

- Somewhere between 10-20 million IPv6 global unicast nodes
  - 97.6% of top-level domains have an IPv6 DNS record*
  - 6.7 million domain names with a top-level AAAA record*
  - RIPE has issued over 8000 network blocks
  - HE.net TunnelBroker alone serves 562,000 users

*** 2015-04-19 Hurricane Electric IPv6 Progress Report http://bgp.he.net/ipv6-progress-report.cgi**

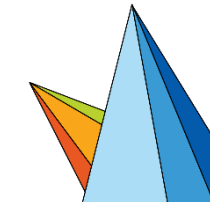


Exposure Trends

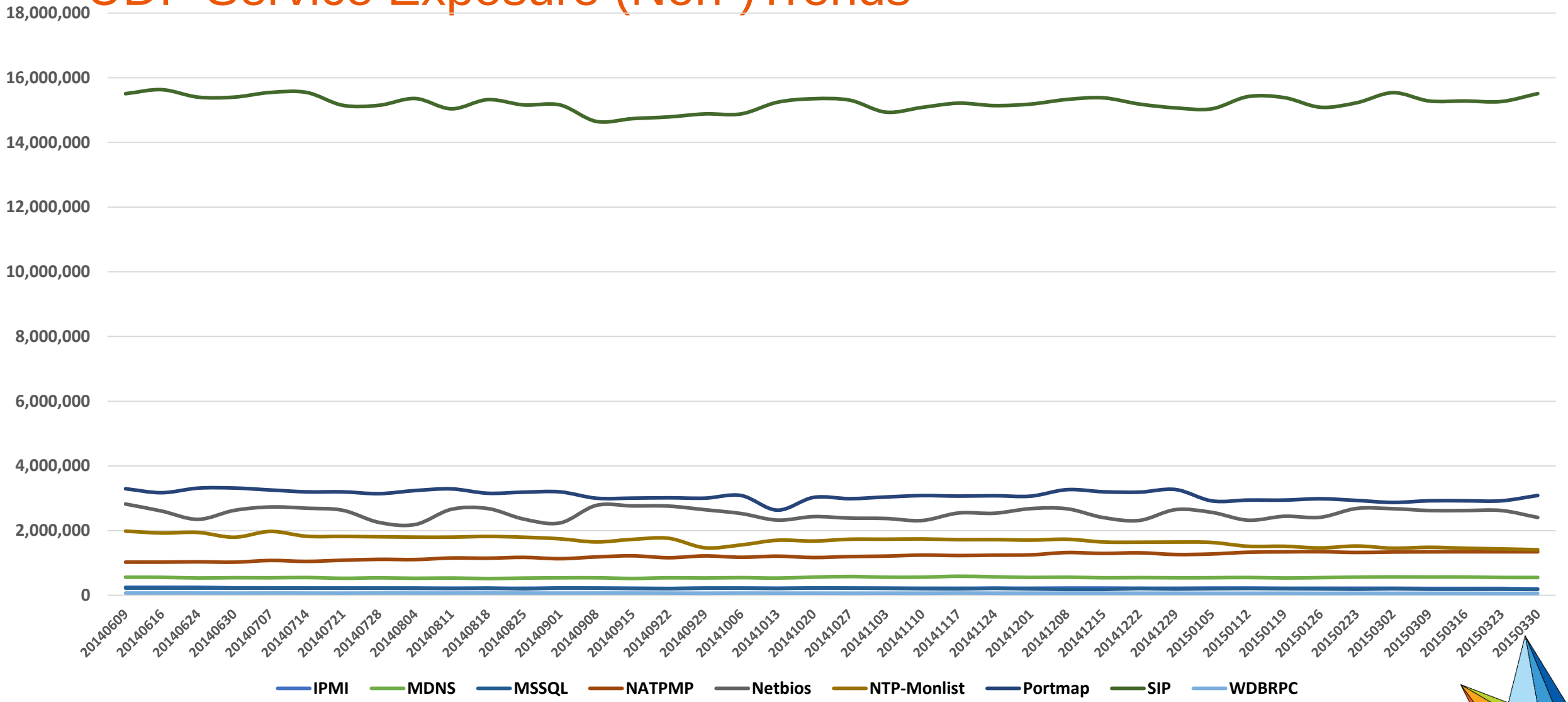


Service Trends

- Project Sonar scans 12 unique UDP services each week
- Most should never be exposed to the internet
- Many can lead to a direct compromise
- How have exposure levels changed?



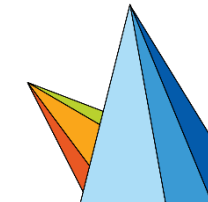
UDP Service Exposure (Non-)Trends



RAPID7

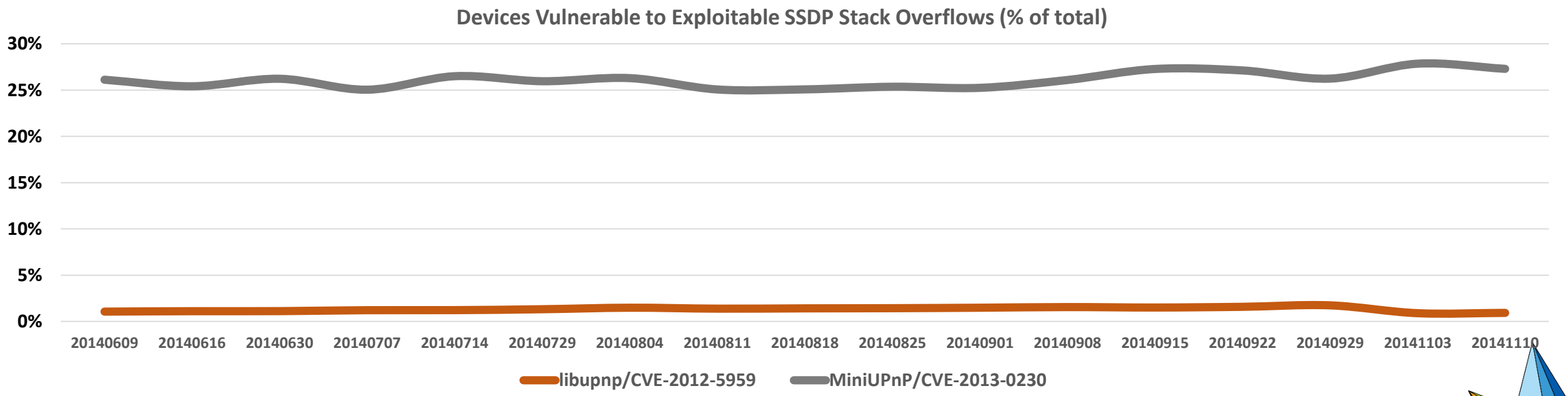
Vulnerability Trends

- Instead of service trends, how about vulnerability trends?
- Are known vulnerabilities getting patched?
- How quickly are patches being applied?



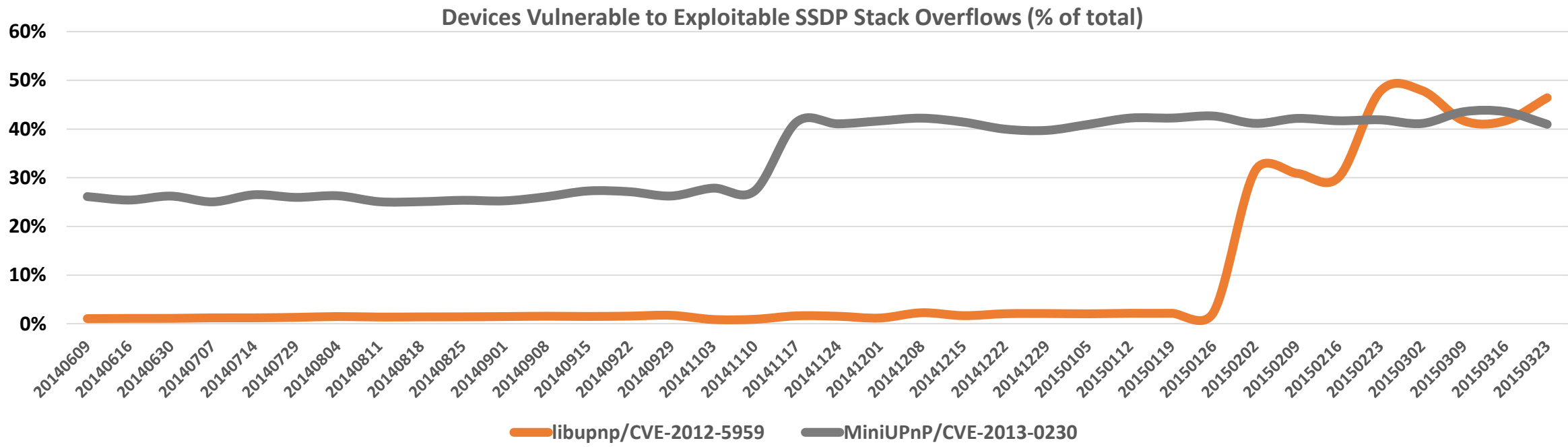
UPnP SSDP Vulnerabilities (1900/udp)

- Monitored two UPnP SSDP vulnerabilities that have public exploits
- We tracked the % of vulnerable services for libupnp & miniupnp
- June 2014 to November 2014 is basically flat…



UPnP SSDP Vulnerabilities (1900/udp)

- In late 2014, both of these issues spiked dramatically
- Likely the result of a new broadband ISP deployment
- Vulnerability ratio is higher in 2015 than 2014!



RAPID7

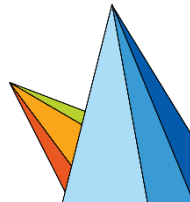
SSDP Distributed Reflective Denial of Service

- SSDP should never be internet-facing in the first place
- DrDoS capabilities in addition to exploits
- 15+ million SSDP services
- Massive amplification
- Live stats at SS
  - https://ssdpscan.shadowserver.org/

RAPID7

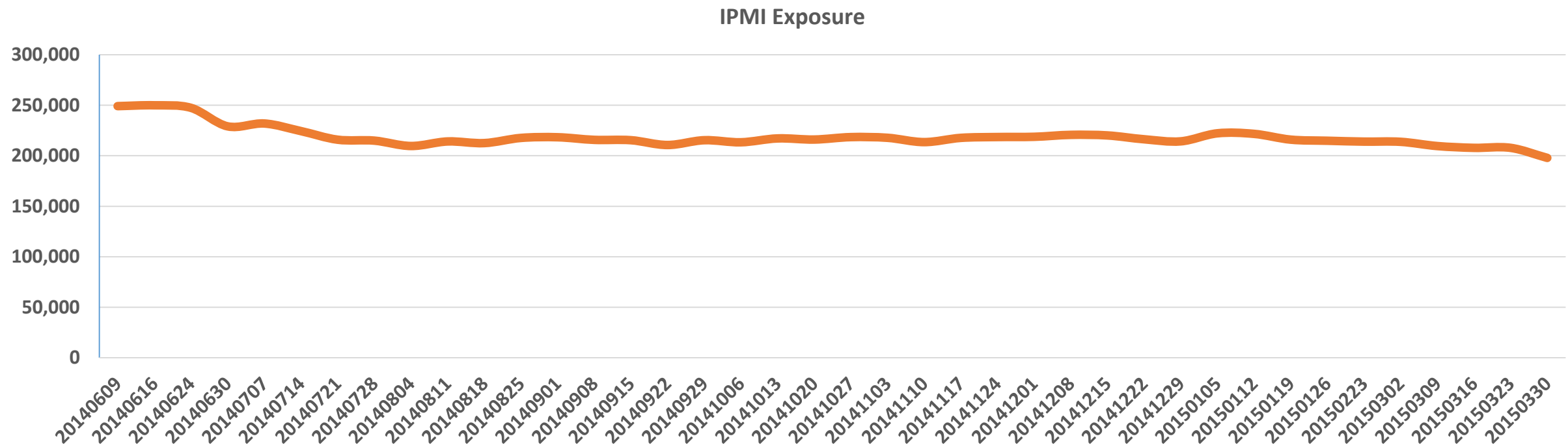
IPMI: The Server Backdoor (623/udp)

- IPMI is used for OOB server management (iDRAC, iLO, SMC IPMI)
- Almost the equivalent of physical access
  - Keyboard, video, mouse, ISO boot, I2C bus access
- Typically Linux running on ARM or MIPS SoCs
- Enabled by default on major server brands
- Dan Farmer broke the IPMI protocol
  - http://fish2.org/ipmi/



IPMI Exposure (623/udp)

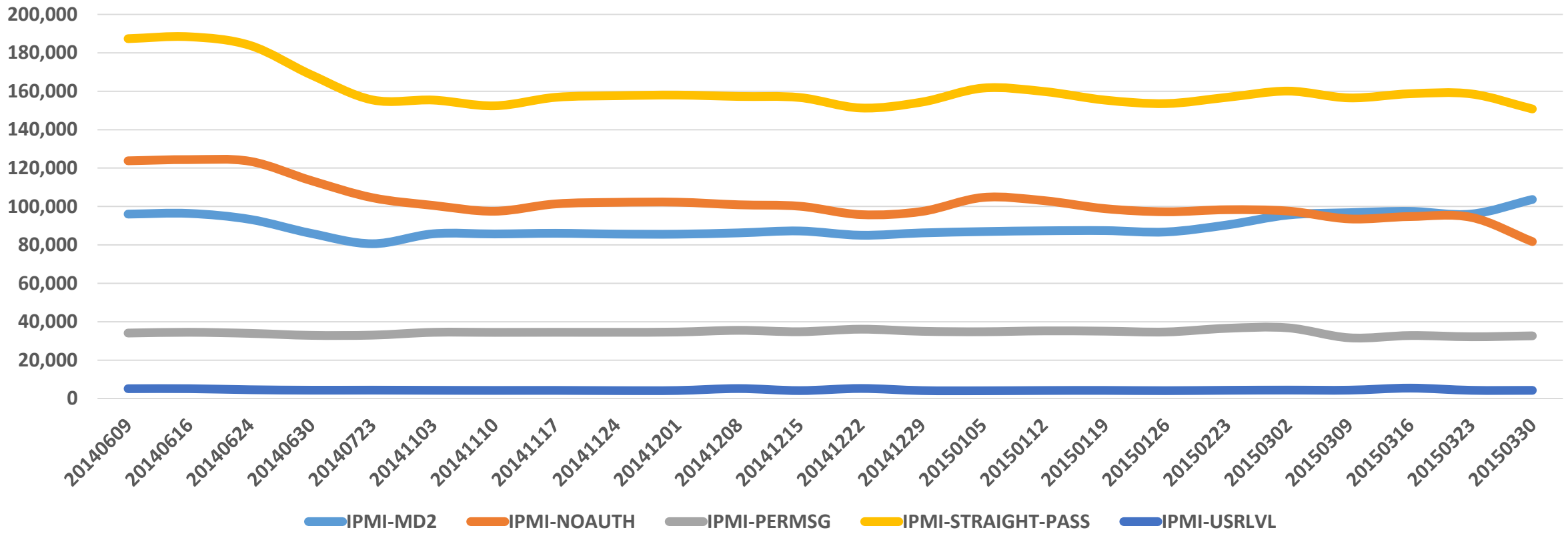
- We identified ~300,000 exposed instances in 2013
- This dropped down to ~250,000 as of June 2014
- Leveled off at ~210,000 in January 2015



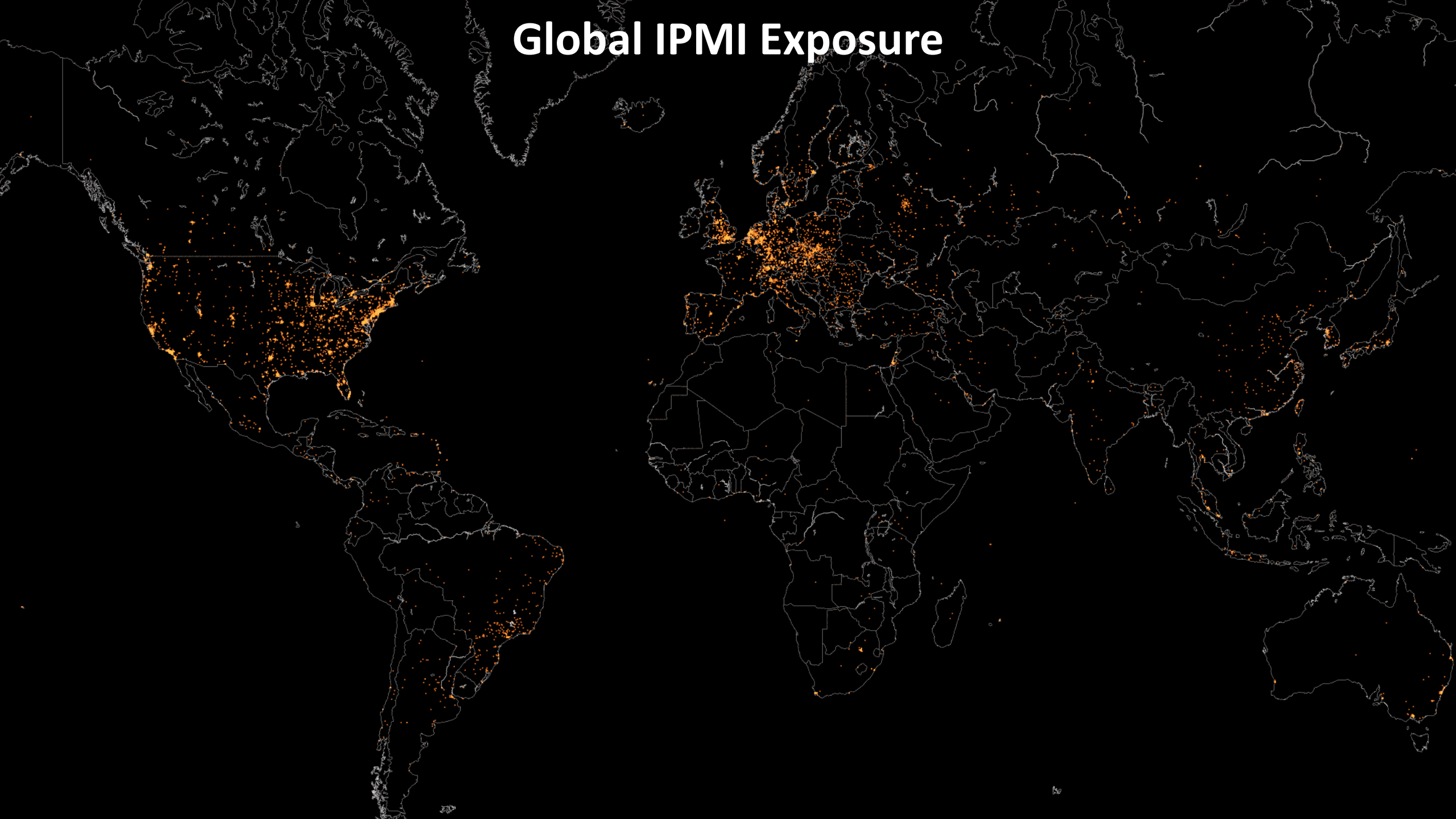
RAPID7

IPMI Capabilities

- The IPMI probe response includes a list of capabilities
- 50% support anonymous authentication!

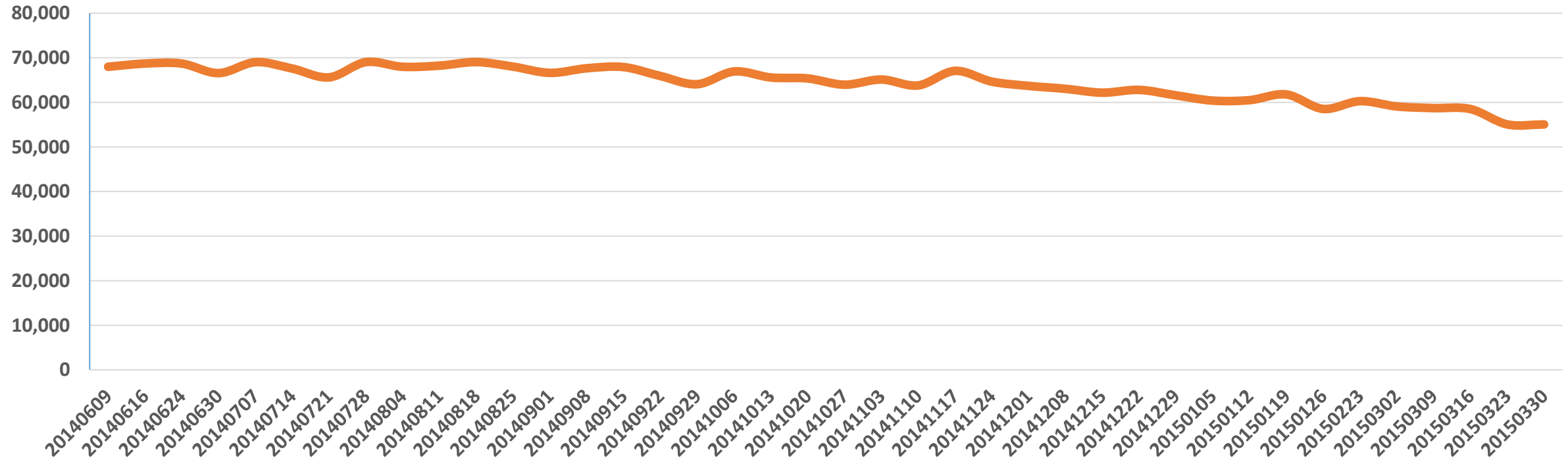


Global IPMI Exposure



Vxworks 5.x Debugger Exposure (17185/udp)

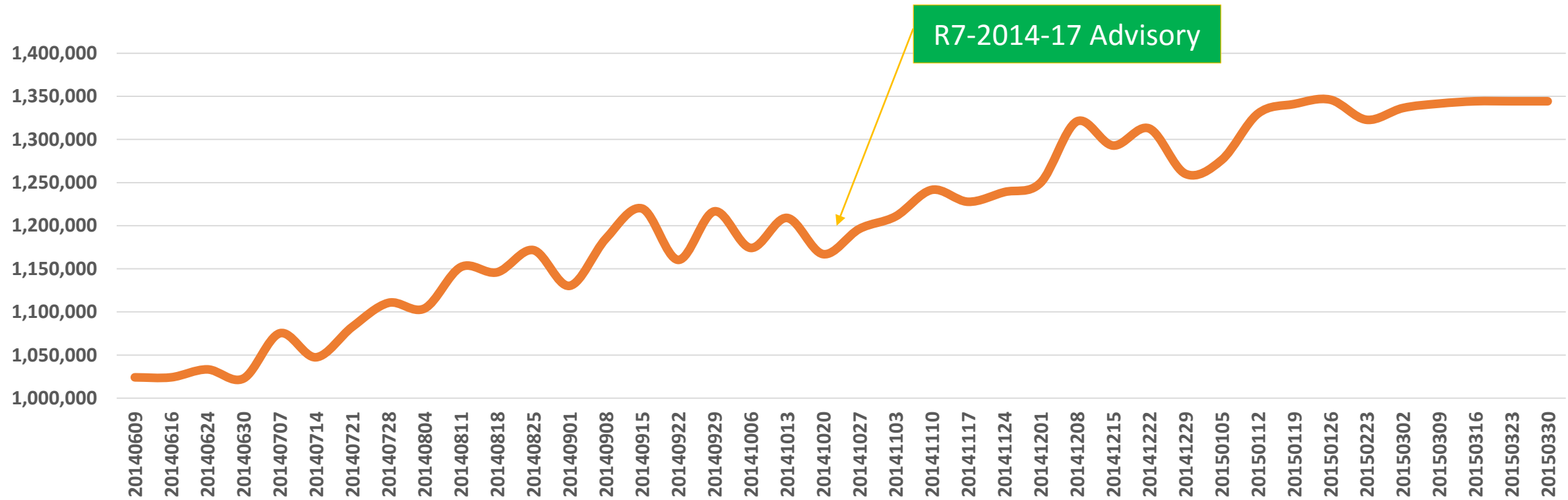
- WDBRPC has dropped from 300k to about 65k since 2010
- Provides remote memory access and OS control
- Relatively flat exposure level for the last year



RAPID7

NAT-PMP Exposure (5351/udp)

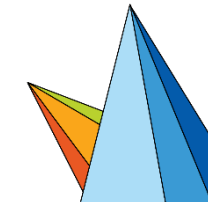
- This service should never be on the internet by definition (RFC)
- Increasing exposure, even after CERT/CC advisory



RAPID7

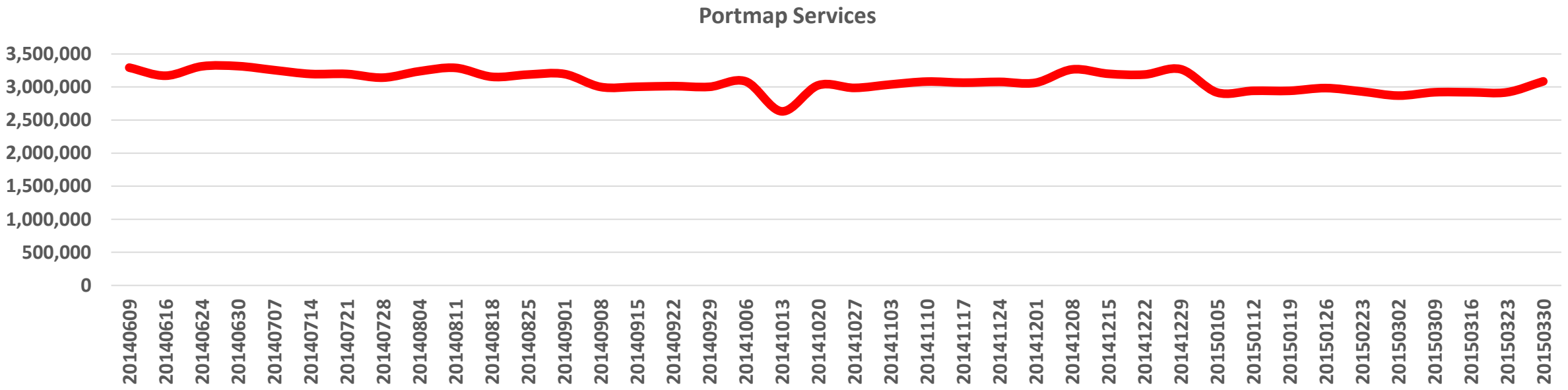
Vulnerability Trend Summary

- Vulnerability trends don’t follow the expected decreasing pattern
- Some flaws issues got worse after the advisory (NATPMP)
- Most things that Sonar measures are not improving
- We need vendors to take more responsibility



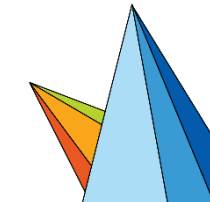
Portmap Exposure (111/udp)

- Portmap (SunRPC) is a discovery mechanism for other services
- Not commonly used in new application development
- Commonly open on Linux servers, not much of a risk

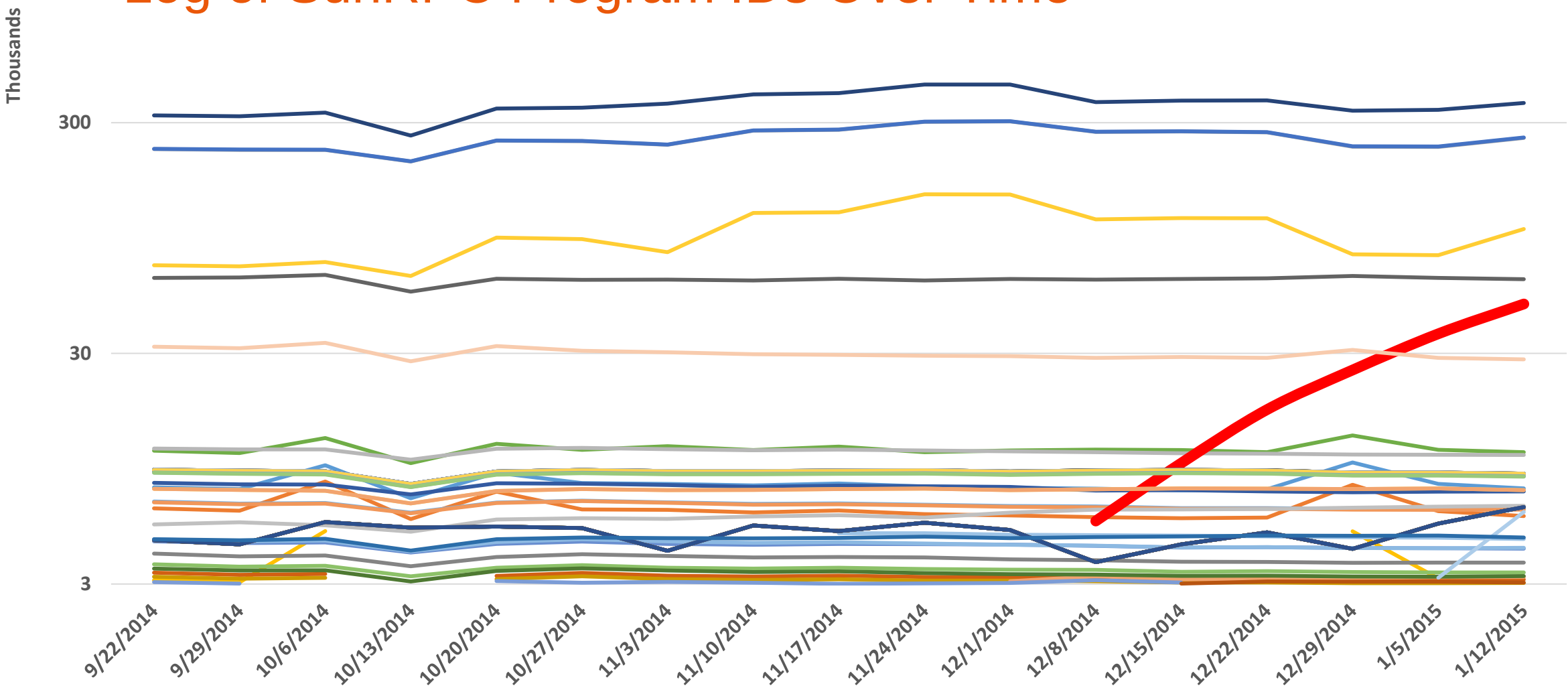


SunRPC Program Trends

- Analyzing SunRPC program IDs from portmap “dump” scans
- These provide a list of all registered programs
- Vendors often create proprietary program IDs
- These can be used for precise fingerprints



Log of SunRPC Program IDs Over Time

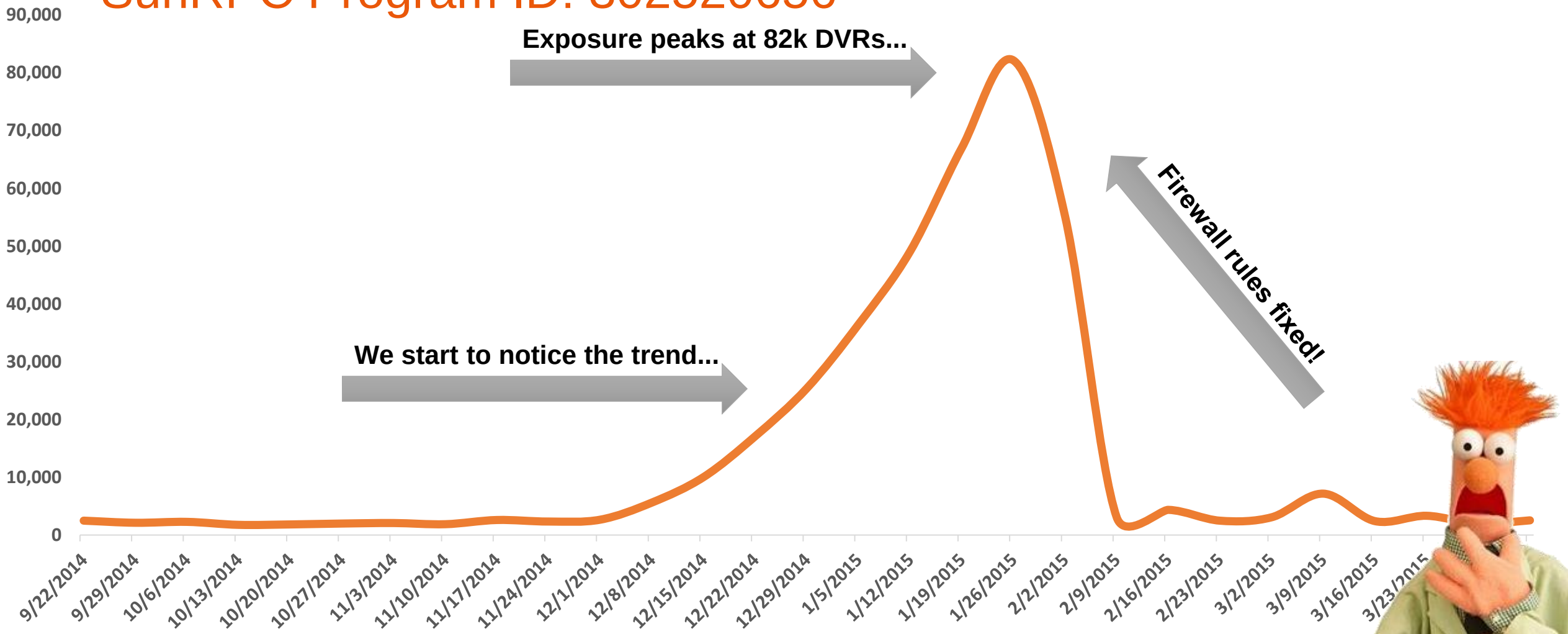


RAPID7

SunRPC Program ID: 302520656

- Zero to substantial in just a few months
- Seems to be a Samsung TV Set-Top Box DVR
- 80% of these show up on Comcast ranges...
- This is their 4K TV rollout!
- With no firewall?

SunRPC Program ID: 302520656

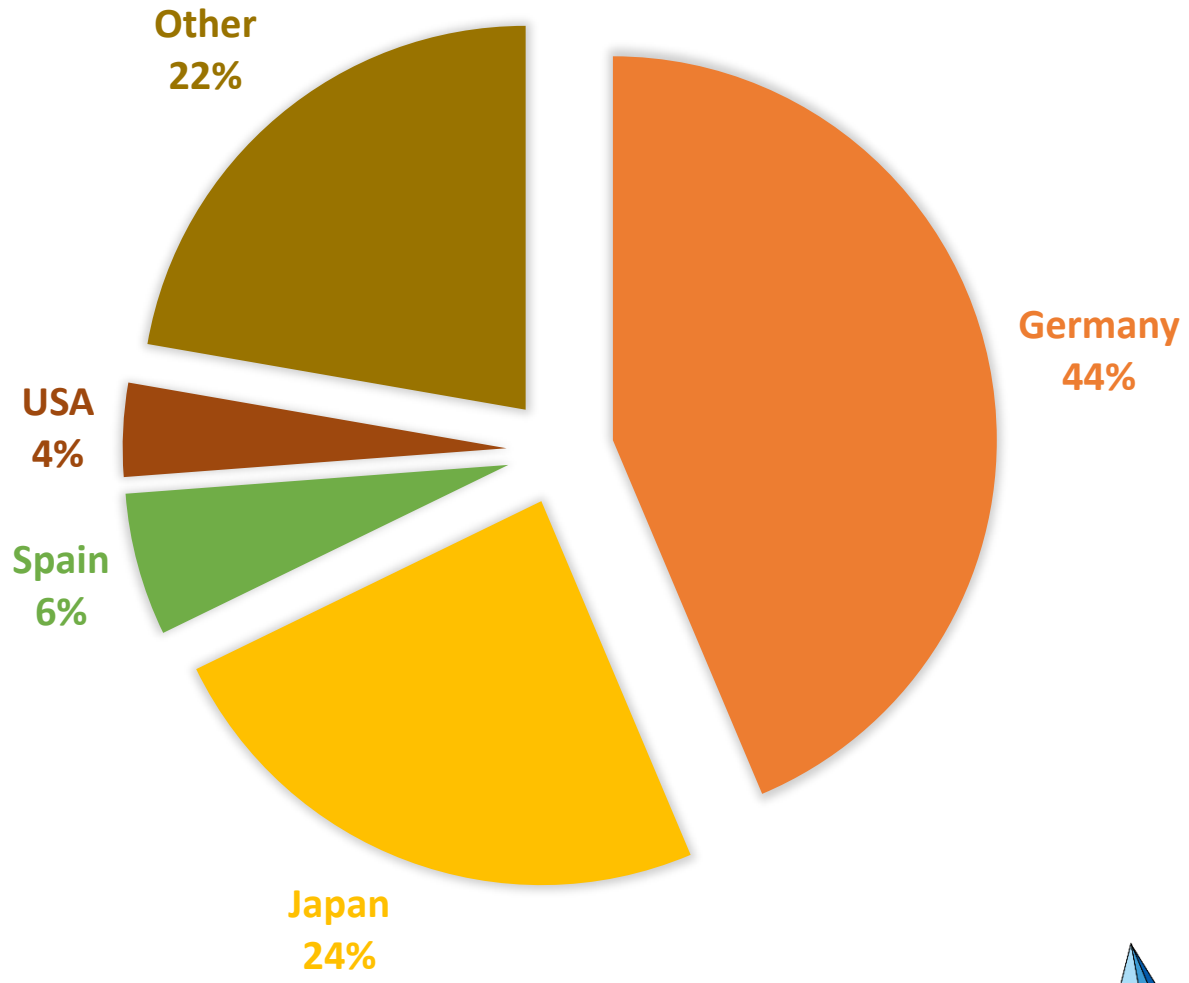


RAPID7

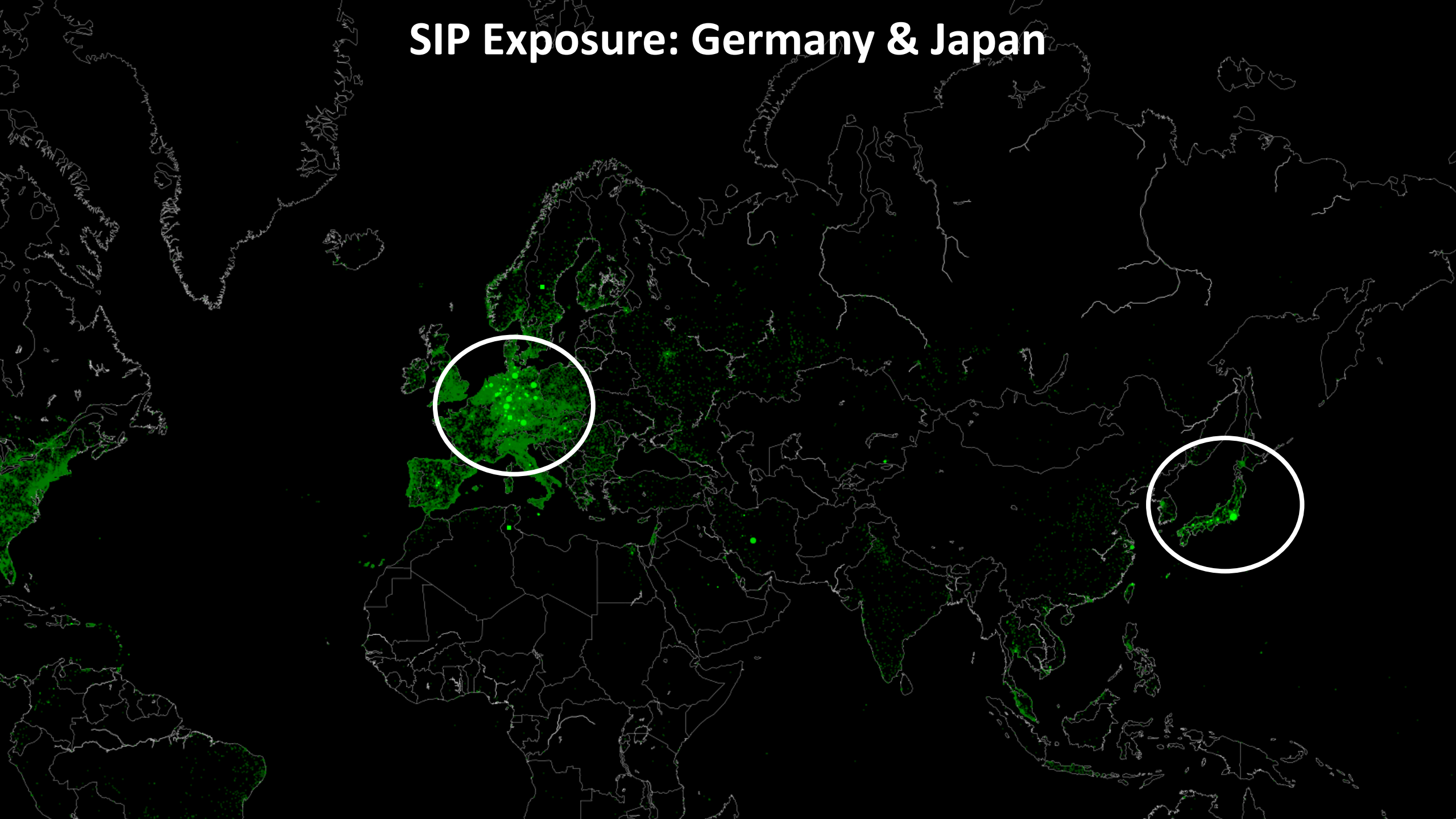
VoIP Session Initiation Protocol (5060/udp)

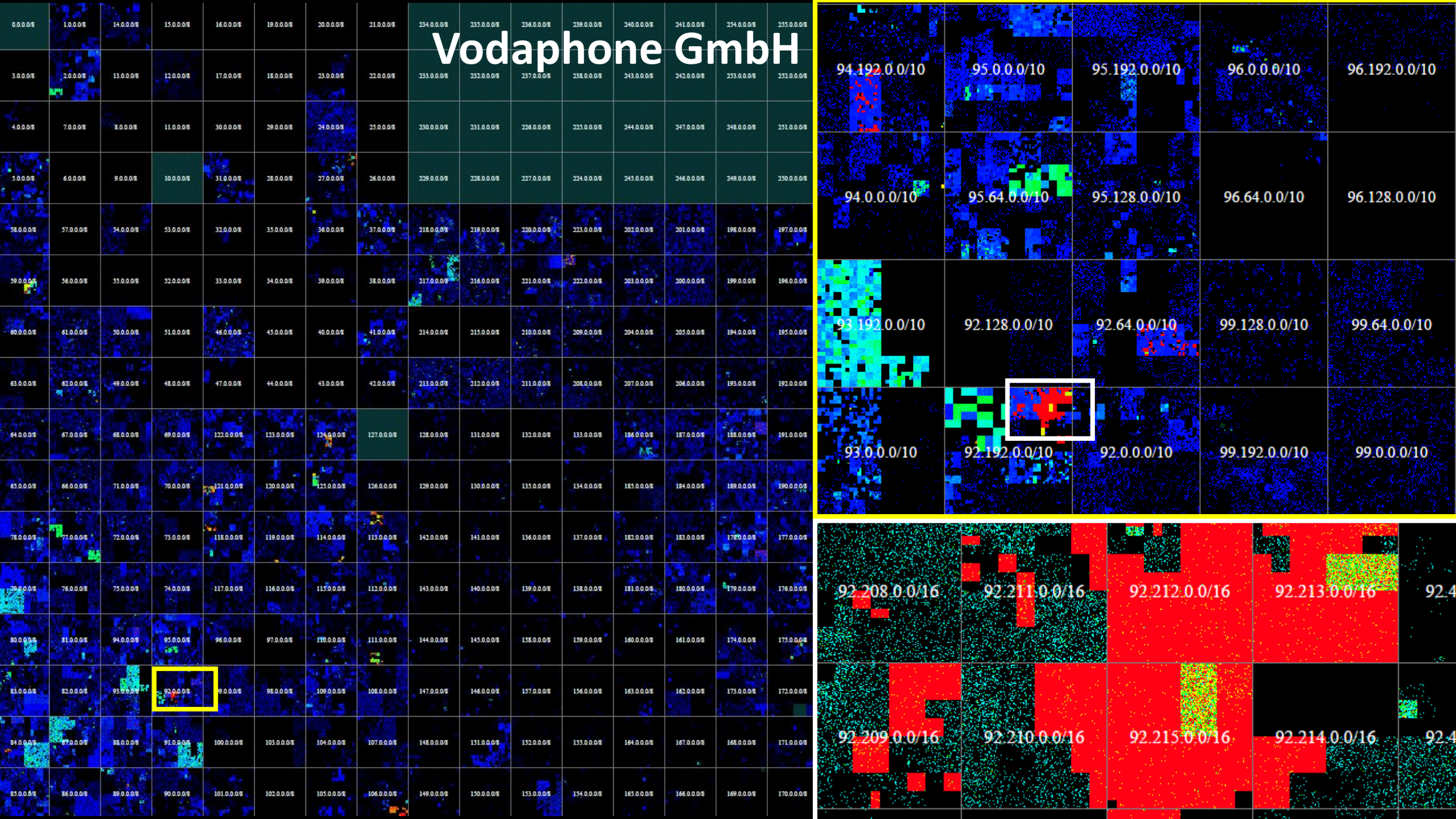
Internet-exposed SIP telephones

- 15 million exposed SIP endpoints
- 44% of these are in Germany
- 24% of these are in Japan
- Digging deeper…



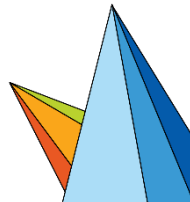
SIP Exposure: Germany & Japan




Vodaphone GmbH
94.192.0.0/10
95.0.0.0/10
95.192.0.0/10
96.0.0.0/10
96.192.0.0/10
94.0.0.0/10
95.64.0.0/10
95.128.0.0/10
96.64.0.0/10
96.128.0.0/10
93.192.0.0/10
92.128.0.0/10
92.64.0.0/10
99.128.0.0/10
99.64.0.0/10
93.0.0.0/10
92.192.0.0/10
92.0.0.0/10
99.192.0.0/10
99.0.0.0/10
92.208.0.0/16
92.211.0.0/16
92.212.0.0/16
92.213.0.0/16
92.209.0.0/16
92.210.0.0/16
92.215.0.0/16
92.214.0.0/16

SIP: Hallo from Germany

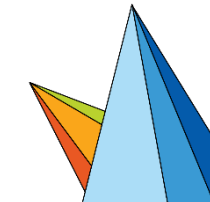
- 5.5 million devices over three primary ISPs
  - All based on the FRITZ!BOX sold by AVM.de
  - All running variants of the same firmware
  - Not the best security record
  - At the least, DDoS potential
  - At the worst, shells!
- 2014 RCE flaw abused for fraud
- Likely more bugs...



RAPID7

Conclusions

- Internet-wide scanning highlights global security challenges
- ISPs have far too much control over internet security
- Vulnerabilities have an incredibly long half-life
- Public data is driving security improvements



Thanks!

hdm@rapid7.com

@hdmoore