


# Examining the Internet's Pollution

Karyn Benson


[kbenson@cs.ucsd.edu](mailto:kbenson@cs.ucsd.edu)






# askreddit


COMMENTS



This is an archived post. You won't be able to vote or comment.



4332



## Garbage men of Reddit, what's the most illegal, strange or valuable thing you have seen while gathering people's trash? (self.AskReddit)

submitted 1 year ago by [eat\\_me\\_now](#)

**4911 comments** [share](#)

# People throw out interesting and valuable items

---



This talk: what sort of interesting and valuable information can we find in the Internet's “trash?”



# About me

---

- I studied Internet “trash” for the last 4 years of my PhD
- Before grad school: wrote intrusion detection software

# Outline

---

- What is Internet “trash?”
- How can we collect “trash?”
- Data for this presentation
- Interesting and valuable items found in “trash”
- Conclusion

# What is Internet “trash?”

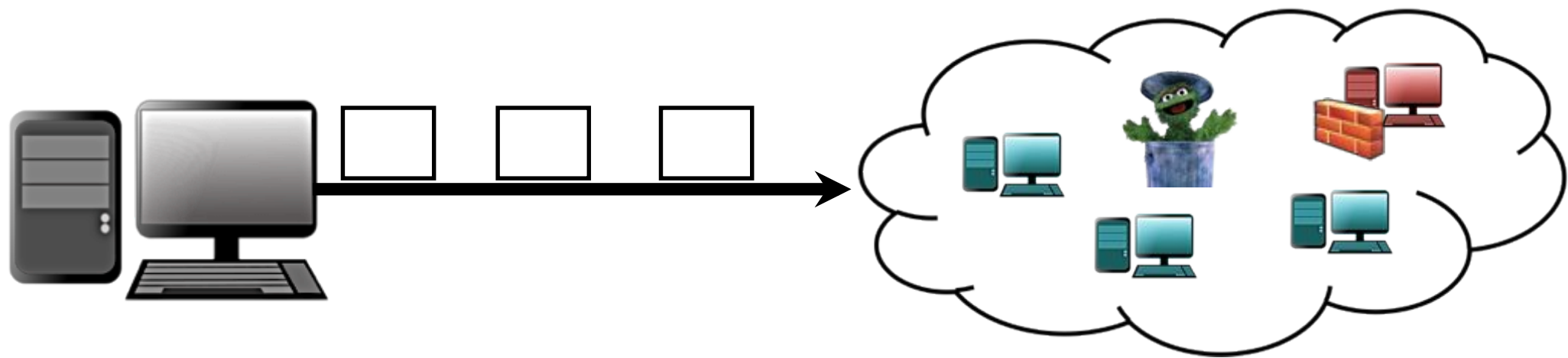
---

- Unsolicited packets
- Passively captured
- Also called Internet Background Radiation (IBR)

# Traffic: Scanning

---

- Searching for hosts that run a service

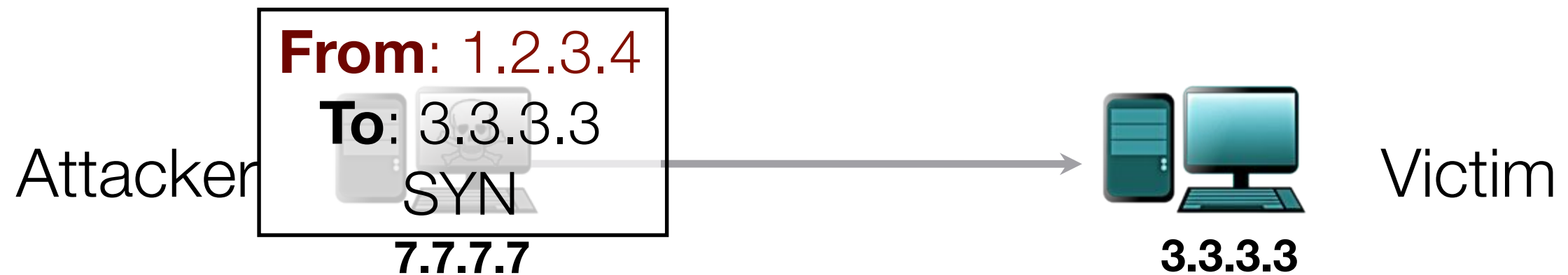




# Traffic: Backscatter

---

- Host responds to forged packets

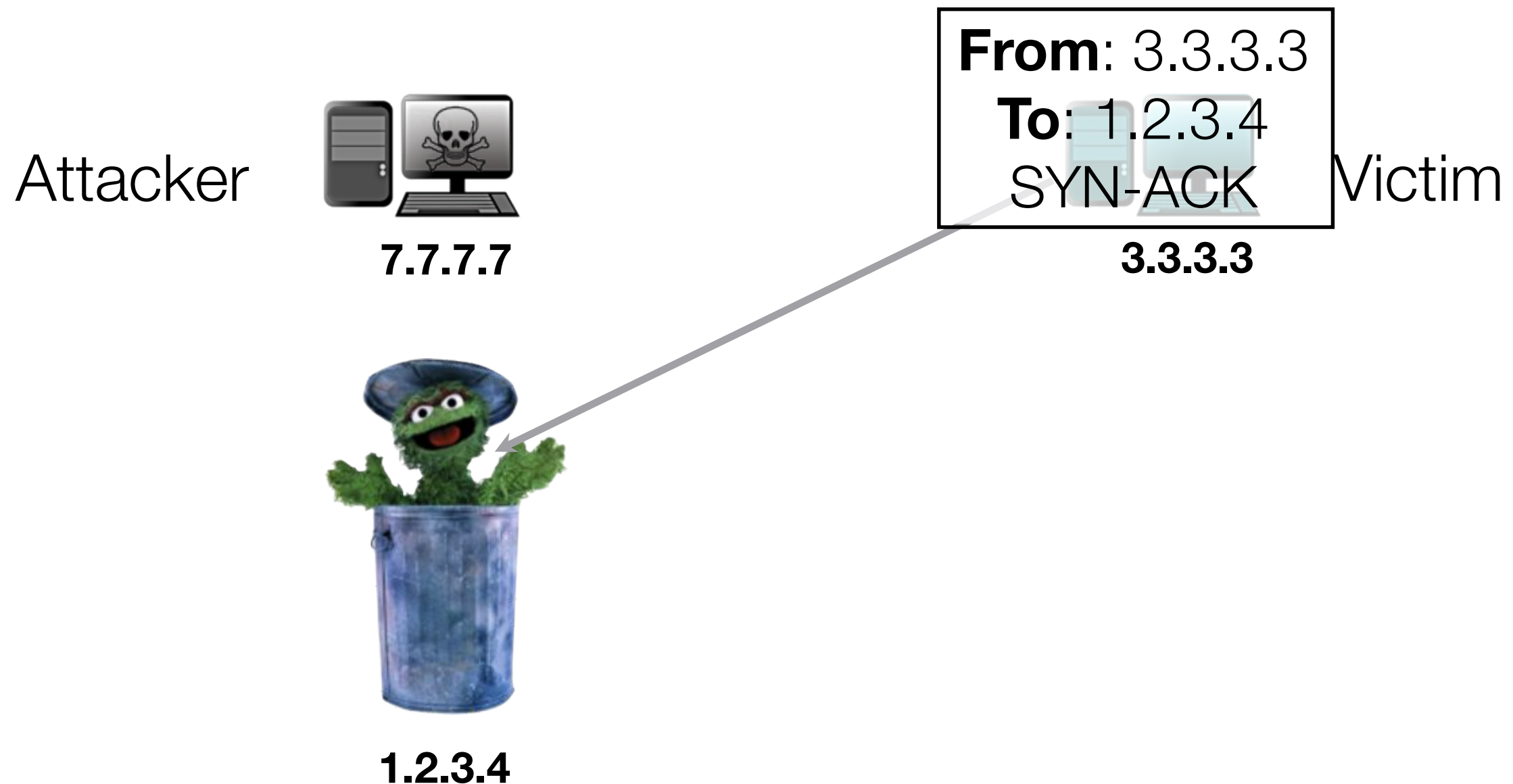


1.2.3.4

# Traffic: Backscatter

---

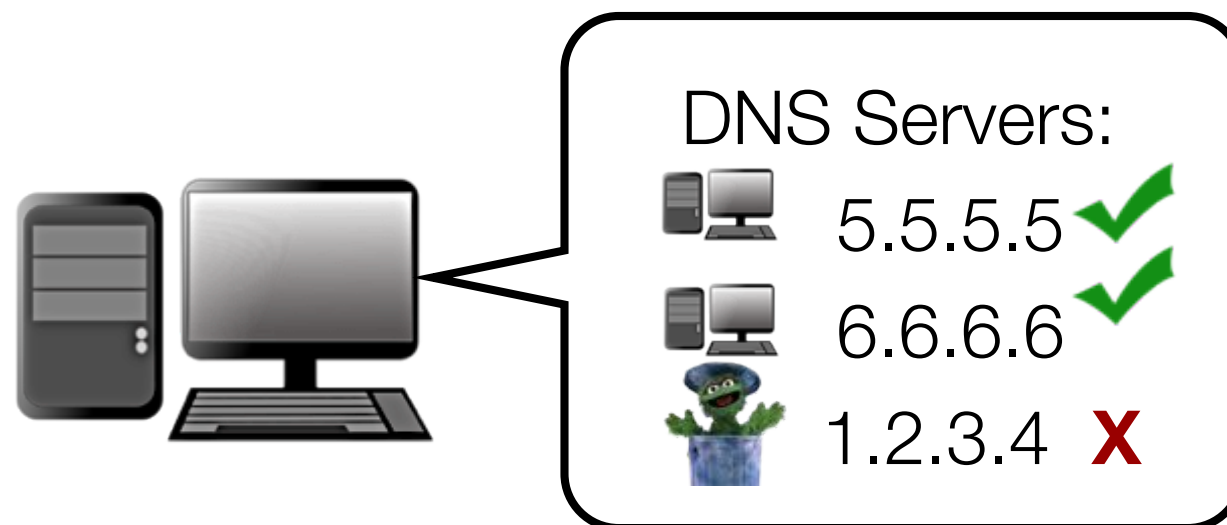
- Host responds to forged packets



# Traffic: Misconfiguration

---

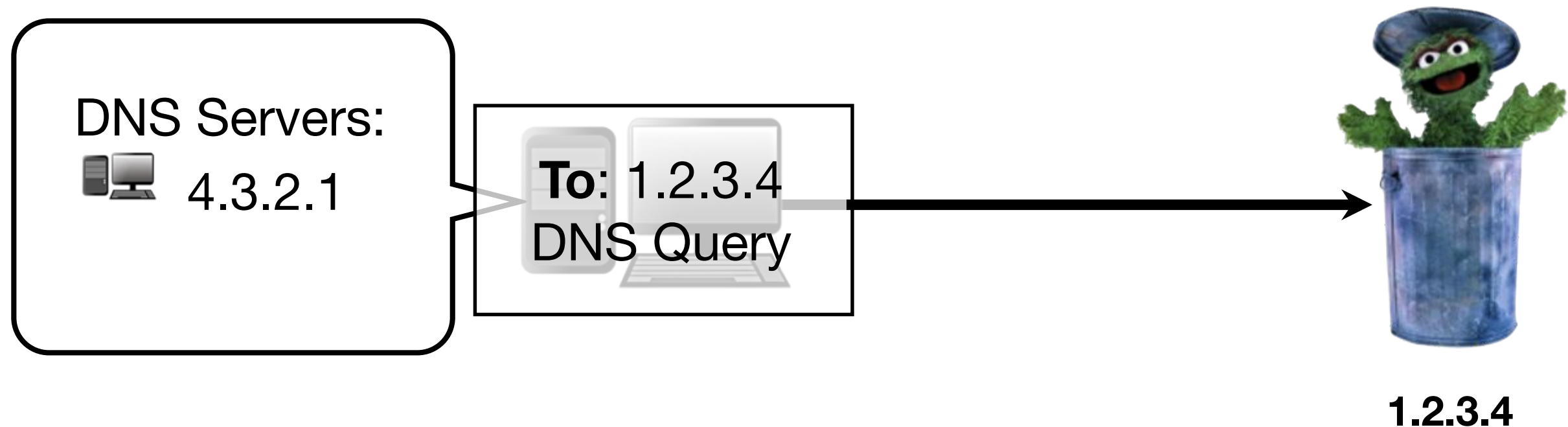
- Host erroneously believes that a machine is hosting a service



# Traffic: Bugs

---

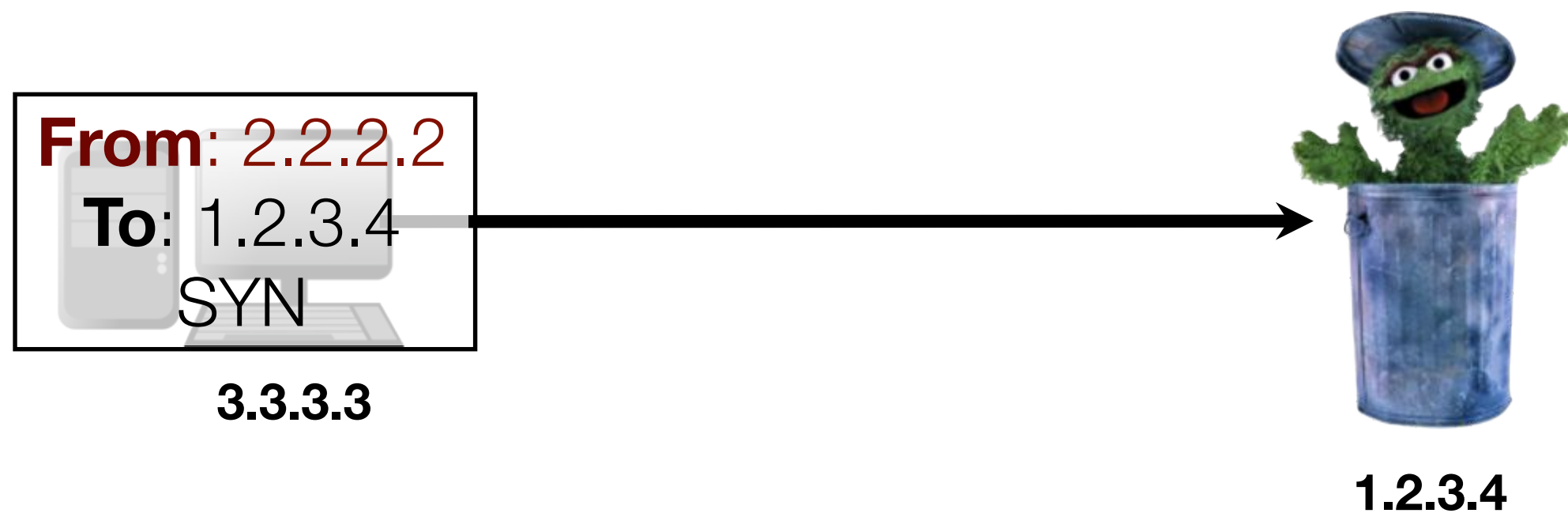
- Software errors cause packets to reach unintended destinations



# Traffic: Spoofed

---

- Hosts forge their IP address to make it appear as though it originates from a different source



# Traffic: Unknown

---

- Traffic produced for an unknown purpose
  - TCP SYN to non-standard port
  - Encrypted UDP packets
  - UDP with unknown payload

```
6:00:06.000065 IP 111.248.55.49.51956 > 1.16.56.246.7605: UDP, length 19
  0x0000:  4500 002f 6c48 0000 7011 ---- 6ff8 3731  E../lH..p..Fo.71
  0x0010:  0110 38f6 caf4 1db5 001b 8298 7133 0f00  ,.8.....q3..
  0x0020:  643e c2d4 2cf5 42b5 810f 7f01 5344 1e    d>...,.B.....SD.
```

# How can we collect “trash?”

---

# How to collect unsolicited traffic

---

- Honeypots: Setting up machines that are purposefully infected with malware

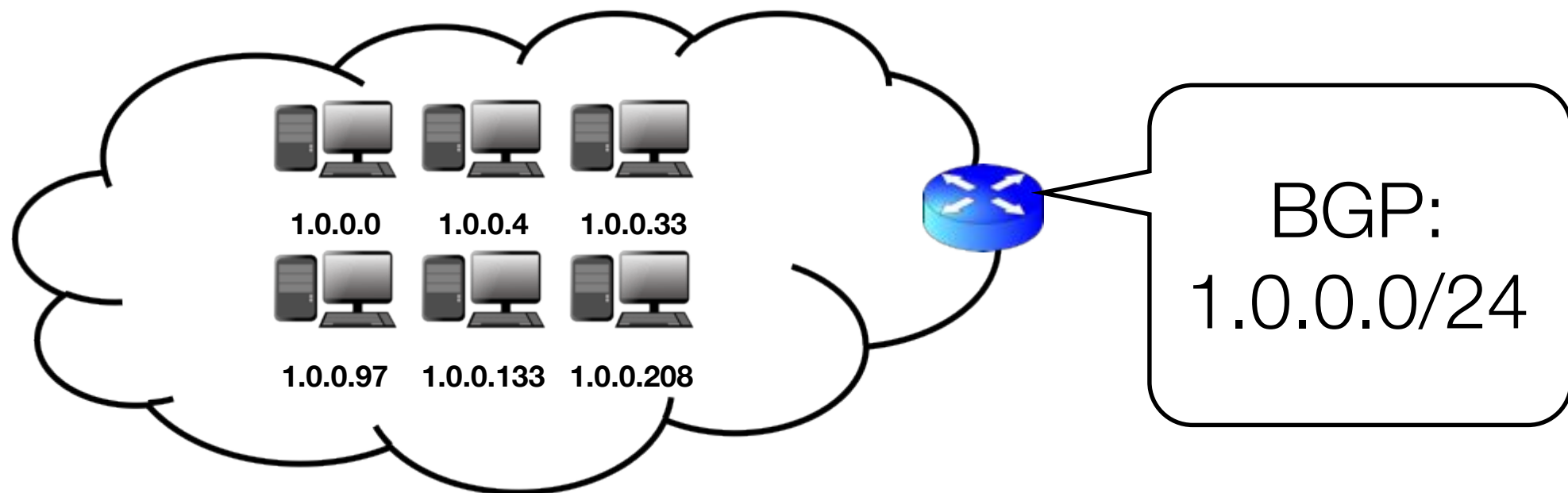


**1.0.0.0**



# How to collect unsolicited traffic

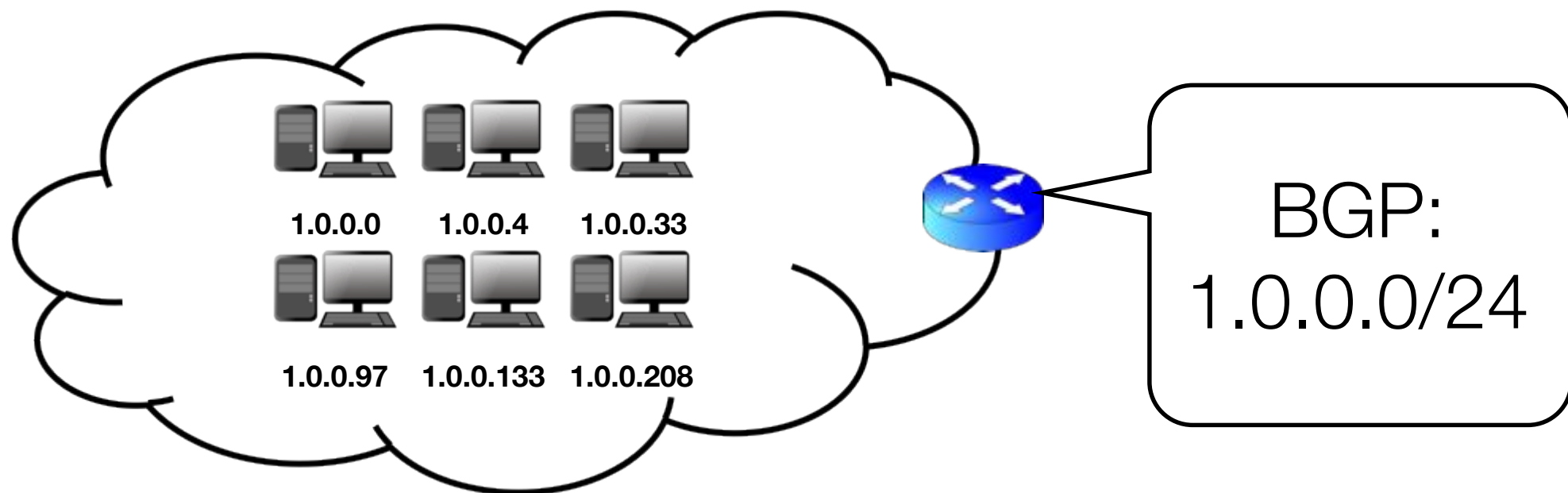
- One-way traffic: Record any packet without a response



Destination	Rule
Any without response	Write packet to storage

# How to collect unsolicited traffic

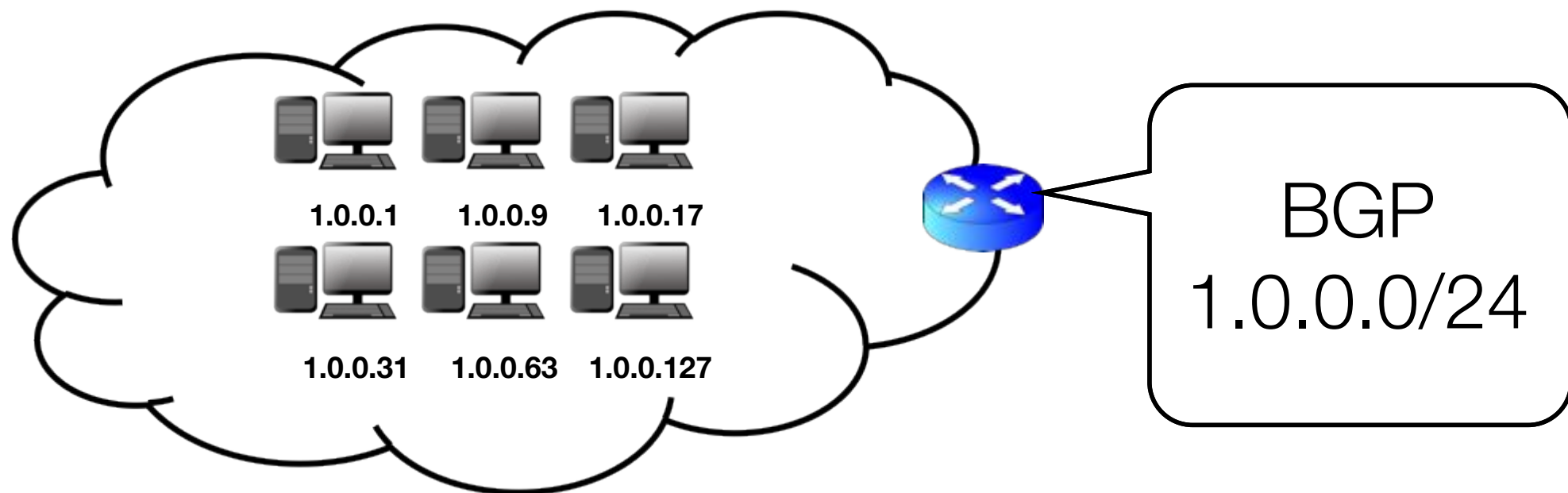
- Greynet: Record traffic destined to any unused IP address



Destination	Rule
1.0.0.[0,4,33,97,133, 208]	Route to destination
All others in 1.0.0.0/24	Write packet to storage

# How to collect unsolicited traffic

- Covering prefix: Record any packet destined to an unused subnet

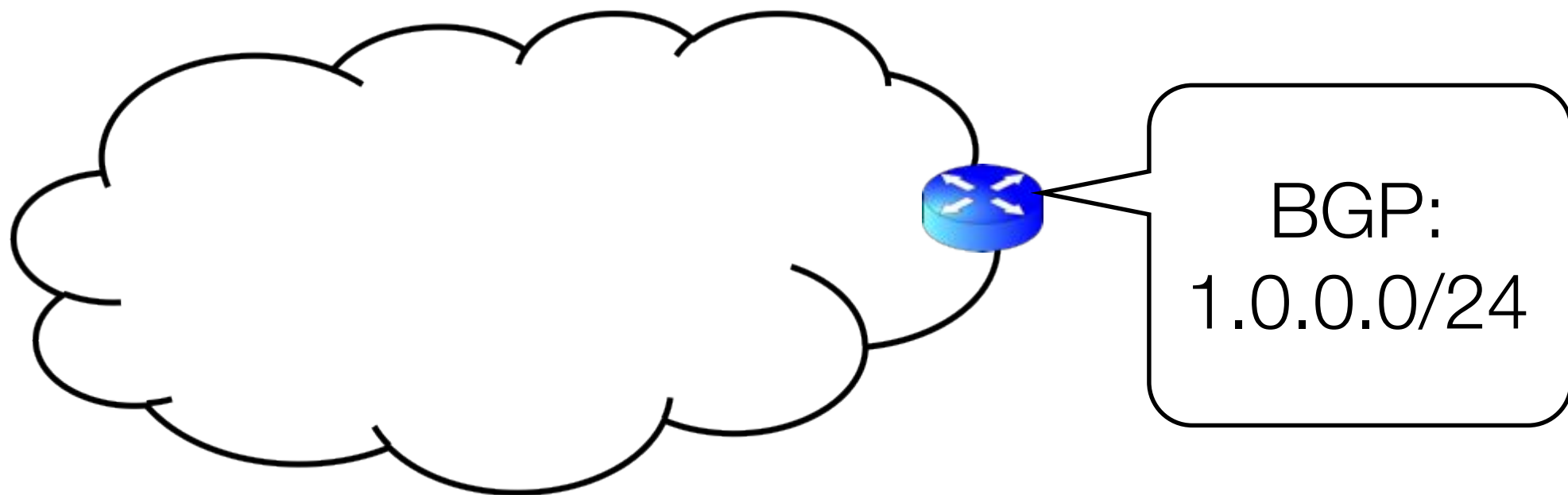


Destination	Rule
1.0.0.0/25	Route to destination
1.0.0.128/25	Write packet to storage

# How to collect unsolicited traffic

---

- Network telescope: Announce unused addresses and record all traffic



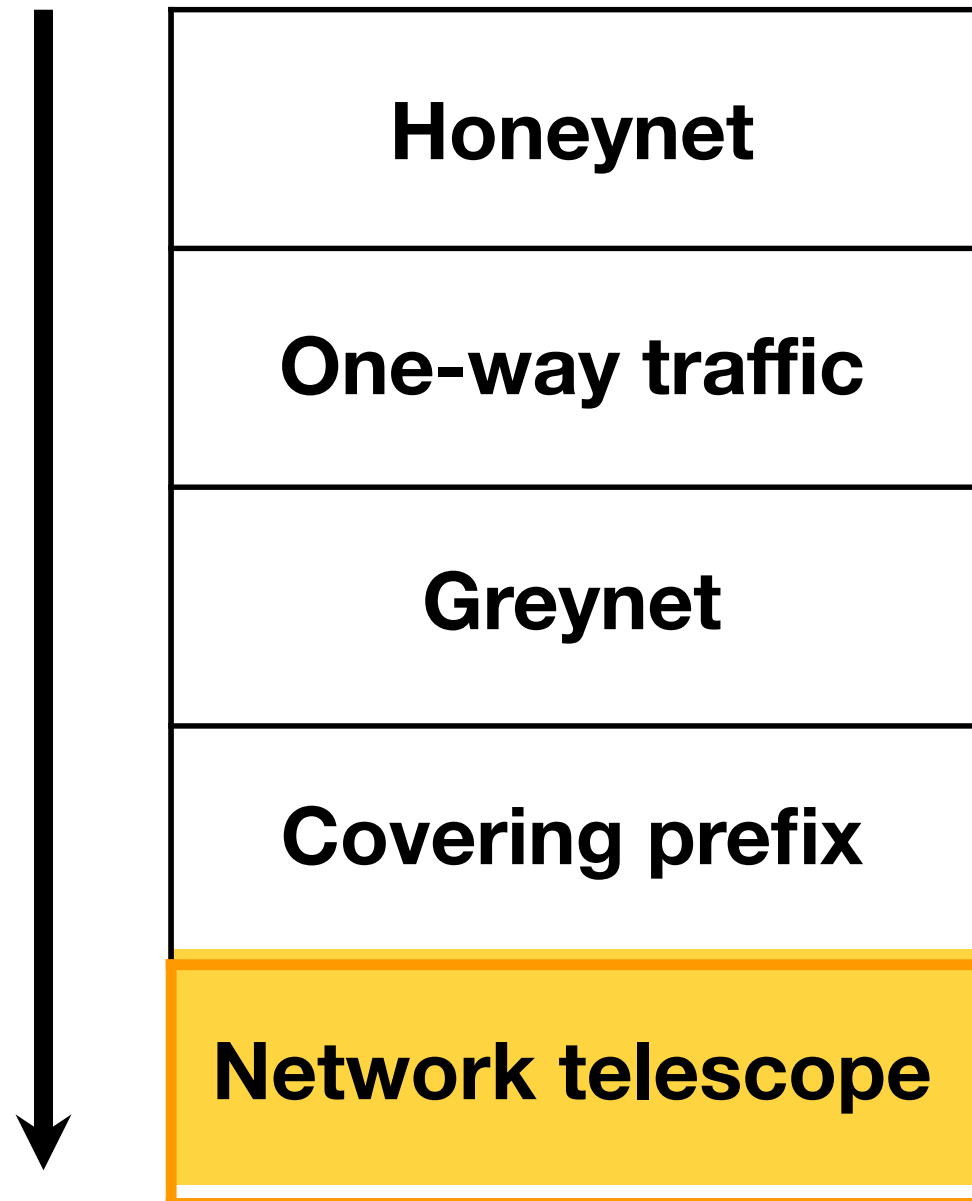
Destination	Rule
1.0.0.0/24	Write packet to storage

# We use network telescopes to easily study macroscopic behaviors

---

**Pros:**  
Scalability  
Ease of implementation  
Fewer privacy concerns

**Cons:**  
Lack of in-depth details  
Avoidability

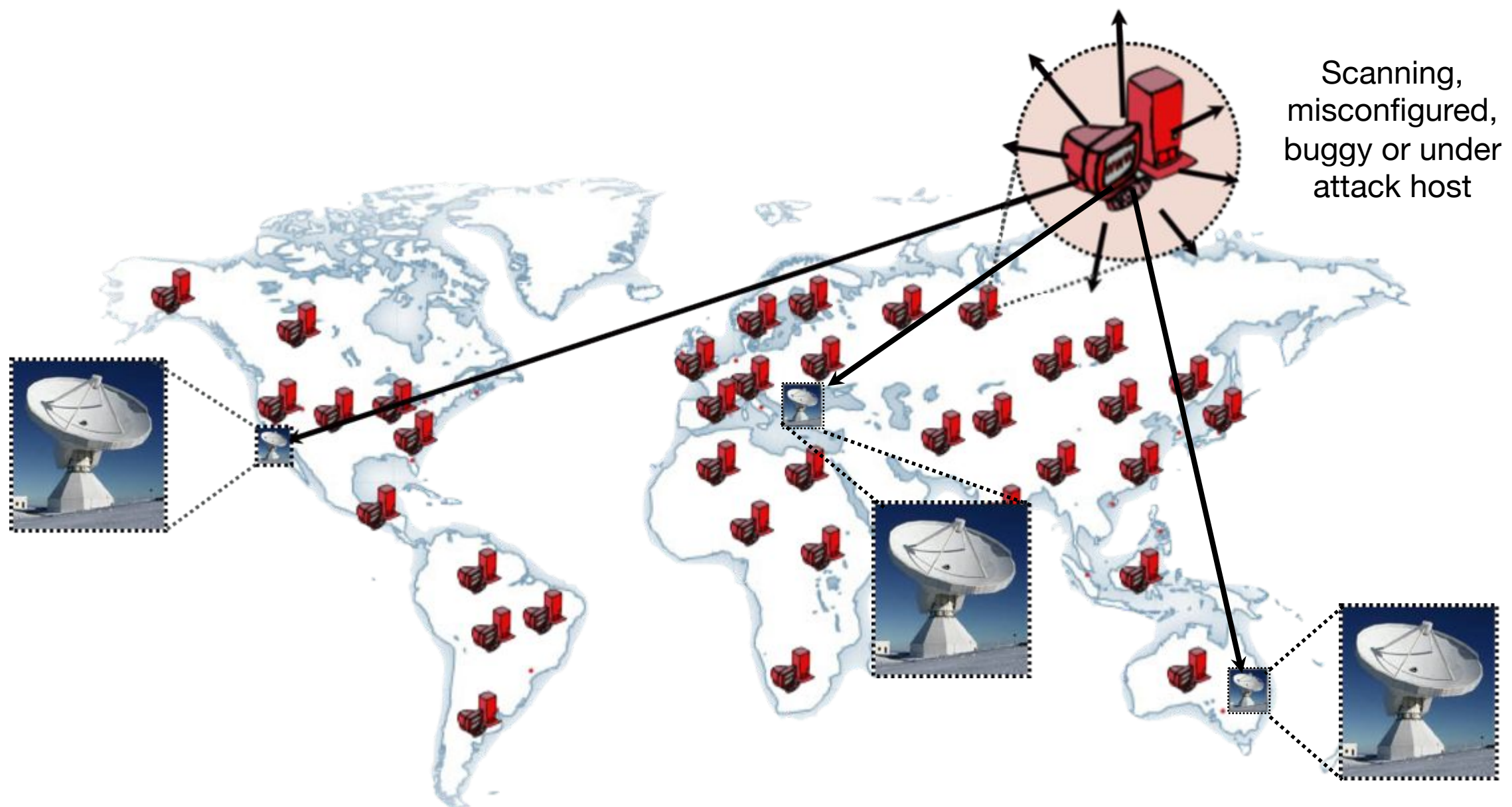


# Data used in this presentation

---

# Our method of obtaining “trash”: Network telescopes

- Multiple large (academic) network telescopes
  - Currently capturing ~5TB compressed pcap per week
  - Historical: traffic since 2008



# IBR is pervasive: We observe traffic from many diverse sources

---

- Removed spoofed traffic. Method: [CCR '13]

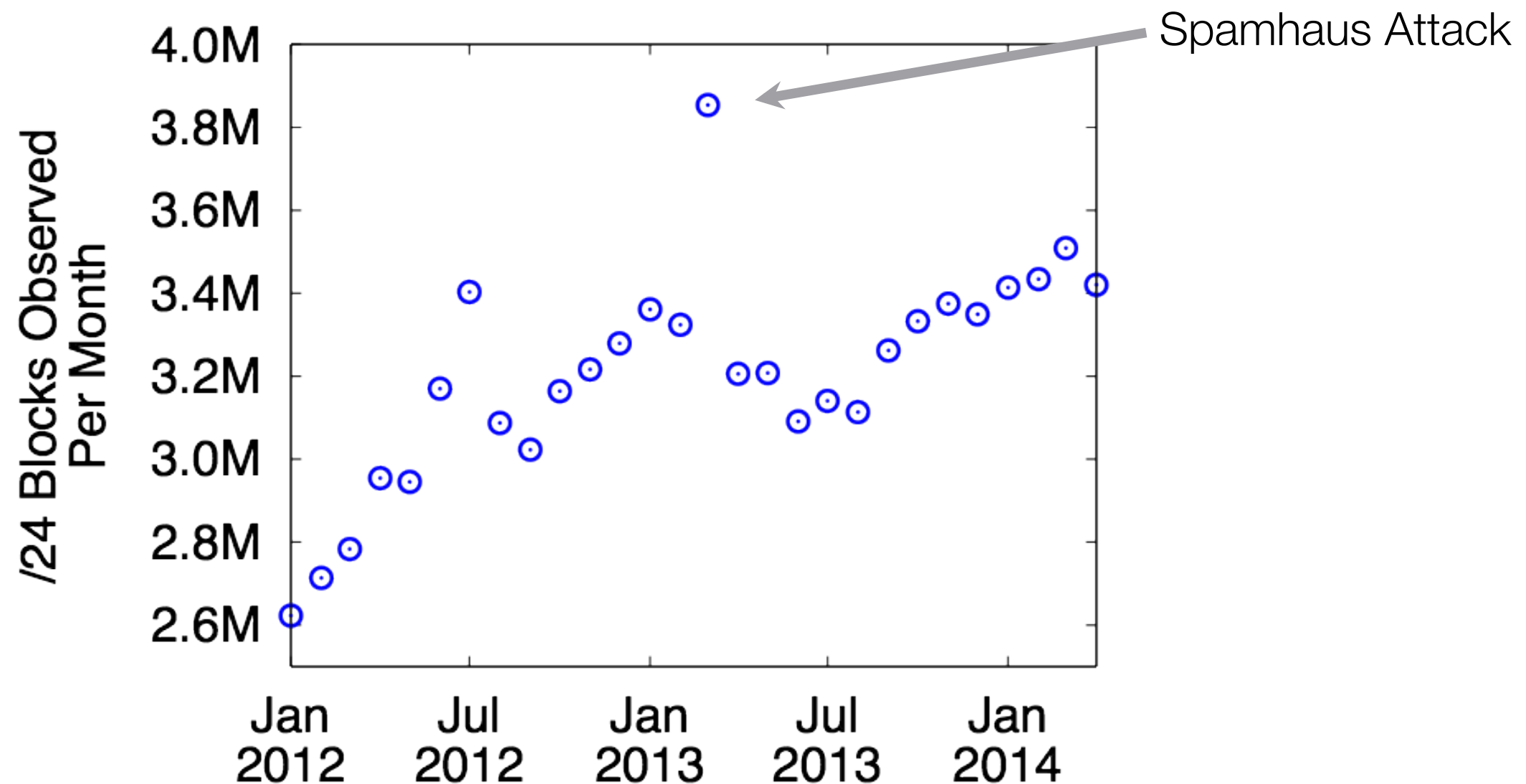
	Total ~July 2013	Percent BGP Announced
IP addresses	133M	5%
/24 blocks	3.15M	30%
Prefixes	205k	45%
ASes	24.2k	54%
Countries	233	99%



# IBR is persistent: We observe a large number of sources over time

---

- Removed spoofed traffic. Method: [CCR '13]



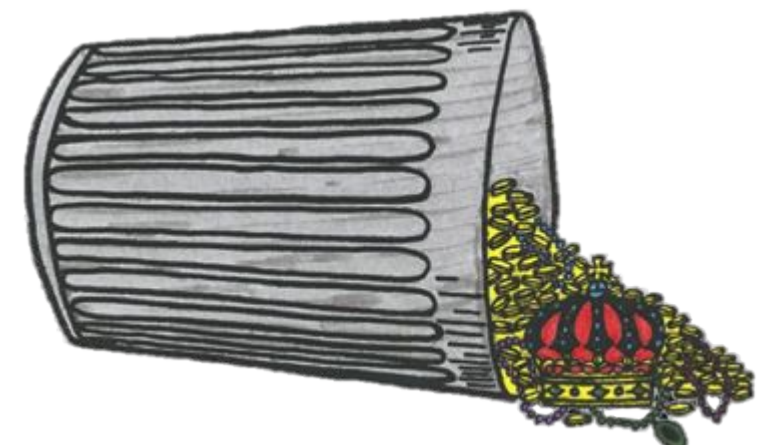
Interesting and valuable items found in Internet  
“trash”

---

# Network telescopes capture a wealth of security-related data

---

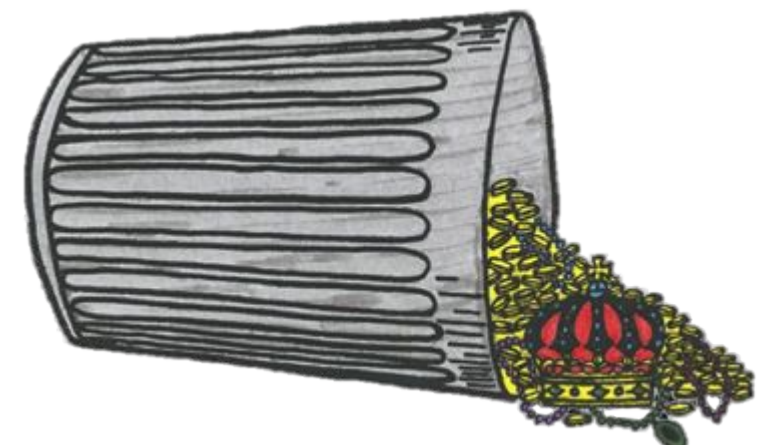
- Scanning: Trends and relation to vulnerability announcements
- Backscatter: Attacks on authoritative name servers
- Misconfigurations: BitTorrent index poisoning attacks
- Bugs: Byte order bug in security software
- Unknown: Encryption vs. obfuscation



# Network telescopes capture a wealth of security-related data

---

- **Scanning: Trends and relation to vulnerability announcements**
- Backscatter: Attacks on authoritative name servers
- Misconfigurations: BitTorrent index poisoning attacks
- Bugs: Byte order bug in security software
- Unknown: Encryption vs. obfuscation



# Methodology

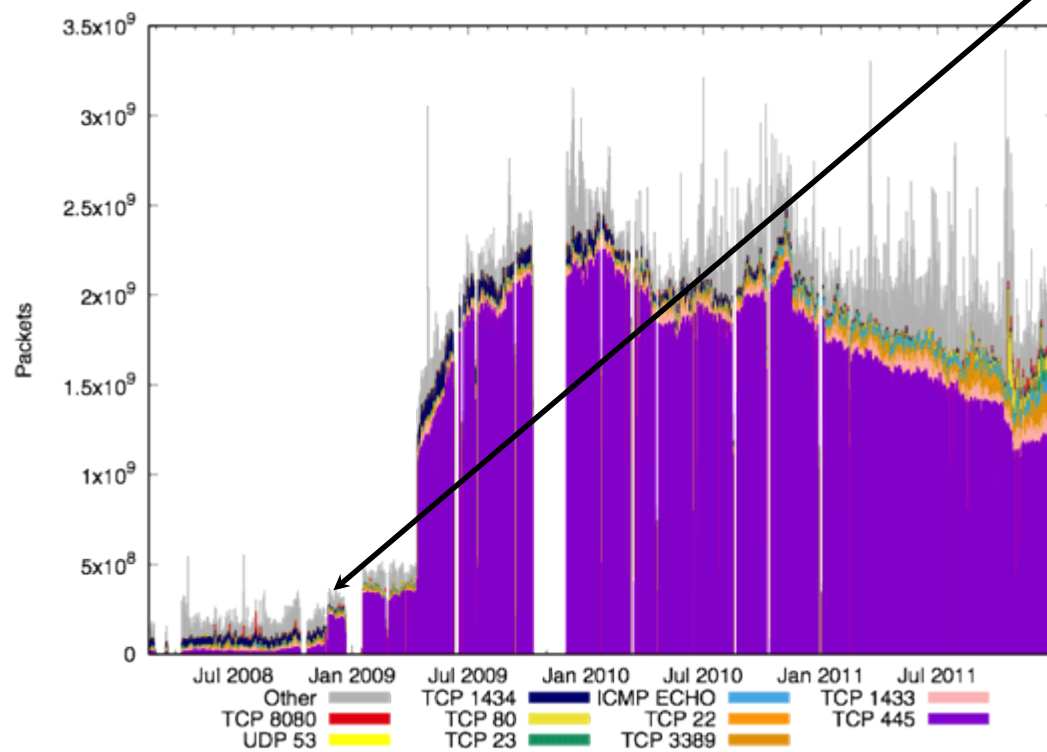
---

- Used Bro's parameters: IP is considered a scanner if it sends:
  - Packets to 25 different network telescope IP addresses
  - Same protocol/port
  - Within 5 minutes
- Results depend on size of network telescope
- Doesn't capture super stealthy scanners (e.g., [Dainotti et al. IMC '12])

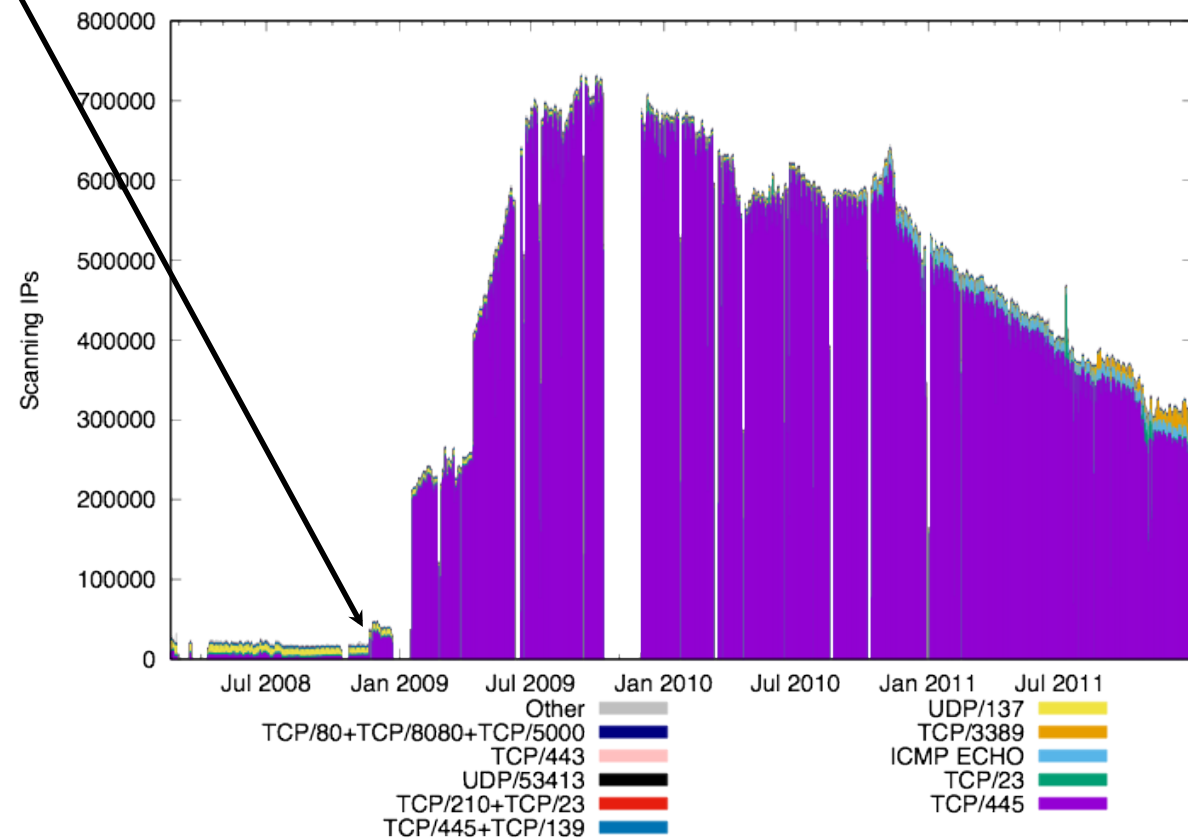
# Scanning: 2008-2012

- Conficker dominates

Conficker Outbreak



Packets

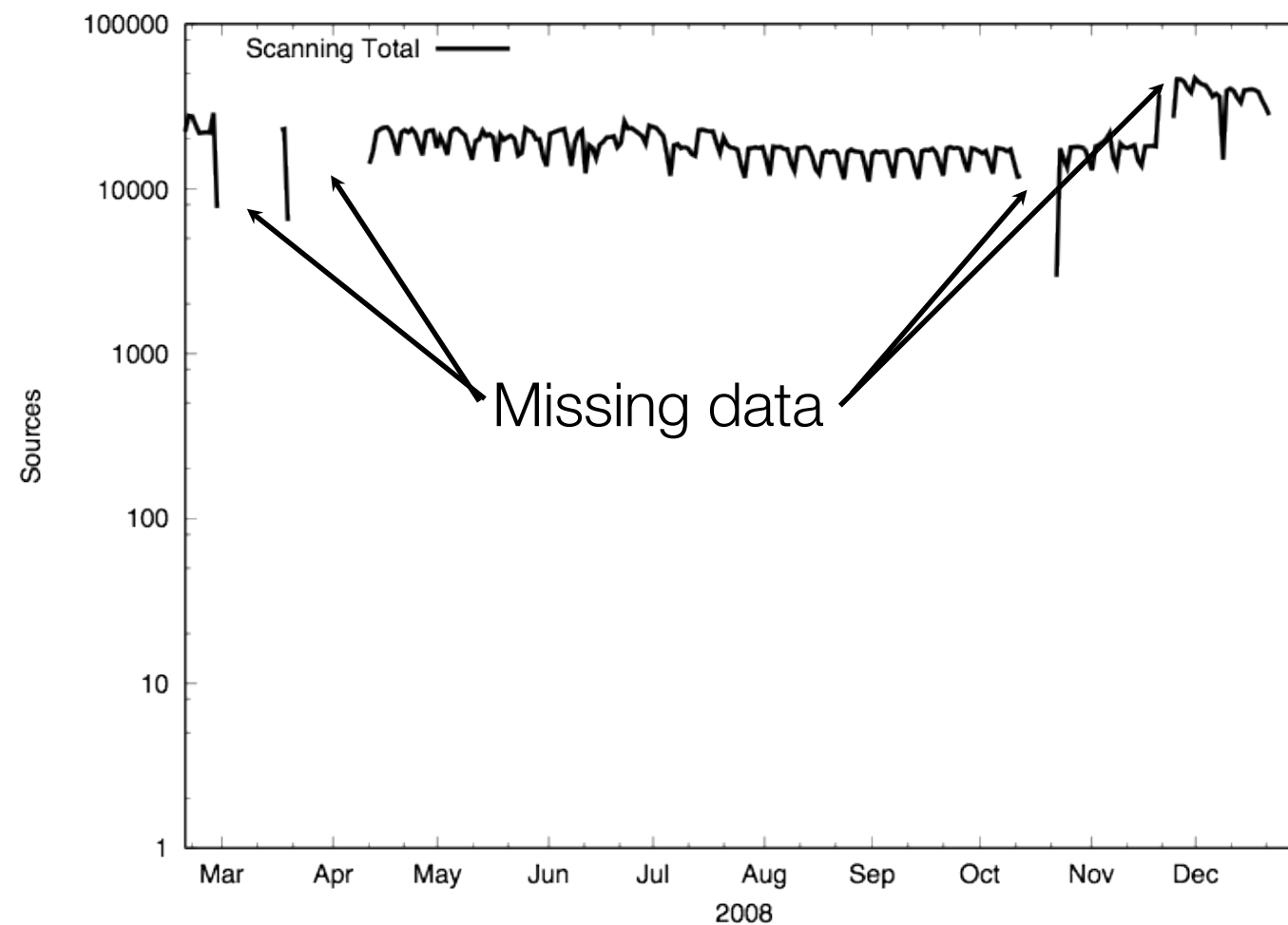


IPs

# How do we know which packets originate from Conficker?

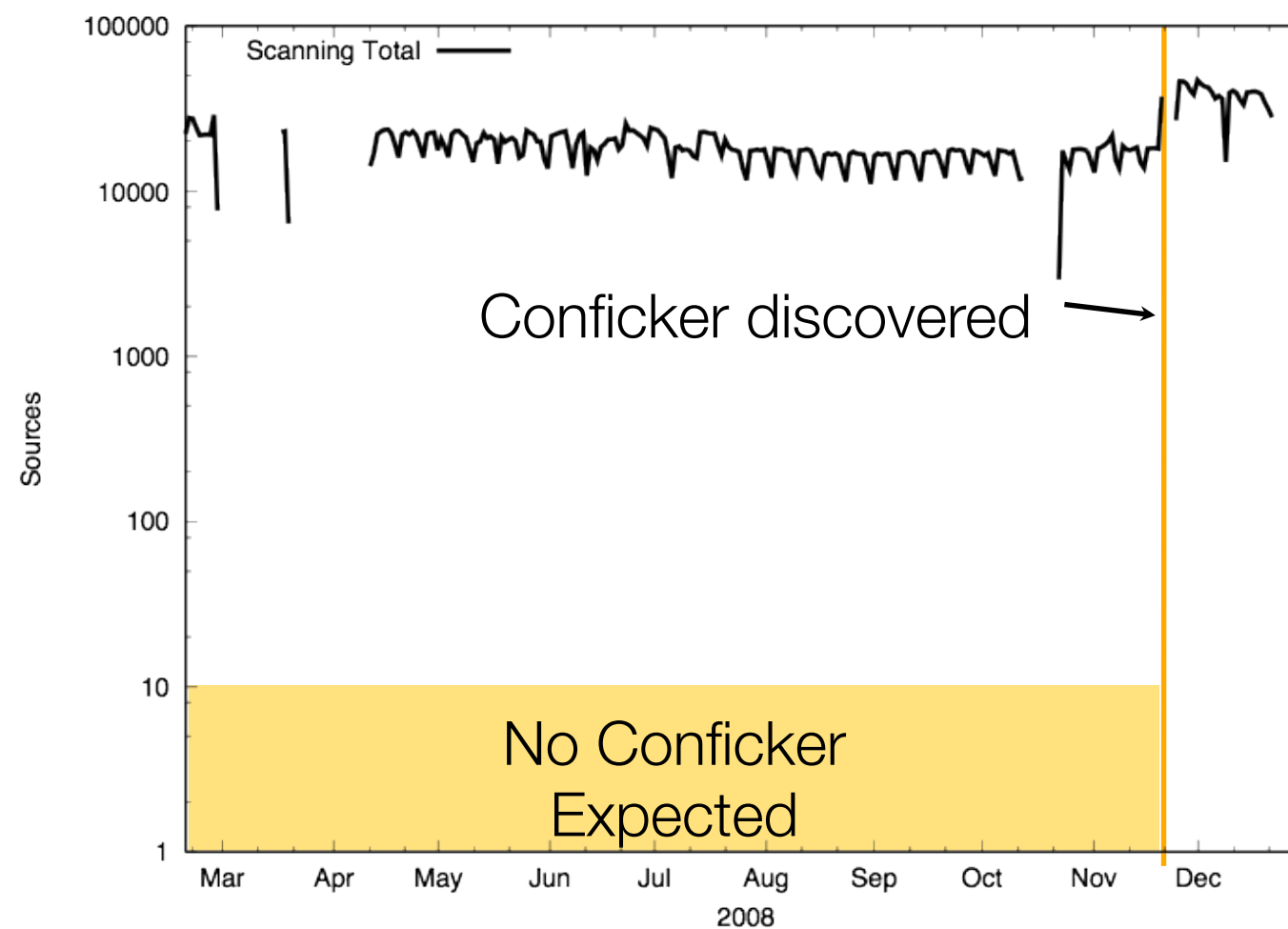
---

- Bug in PRNG: primarily targets IP addresses  $\{A.B.C.D \mid B < 128 \text{ \& } D < 128\}$ 
  - Developed heuristic to identify sources randomly scanning with this bug



# How do we know which packets originate from Conficker?

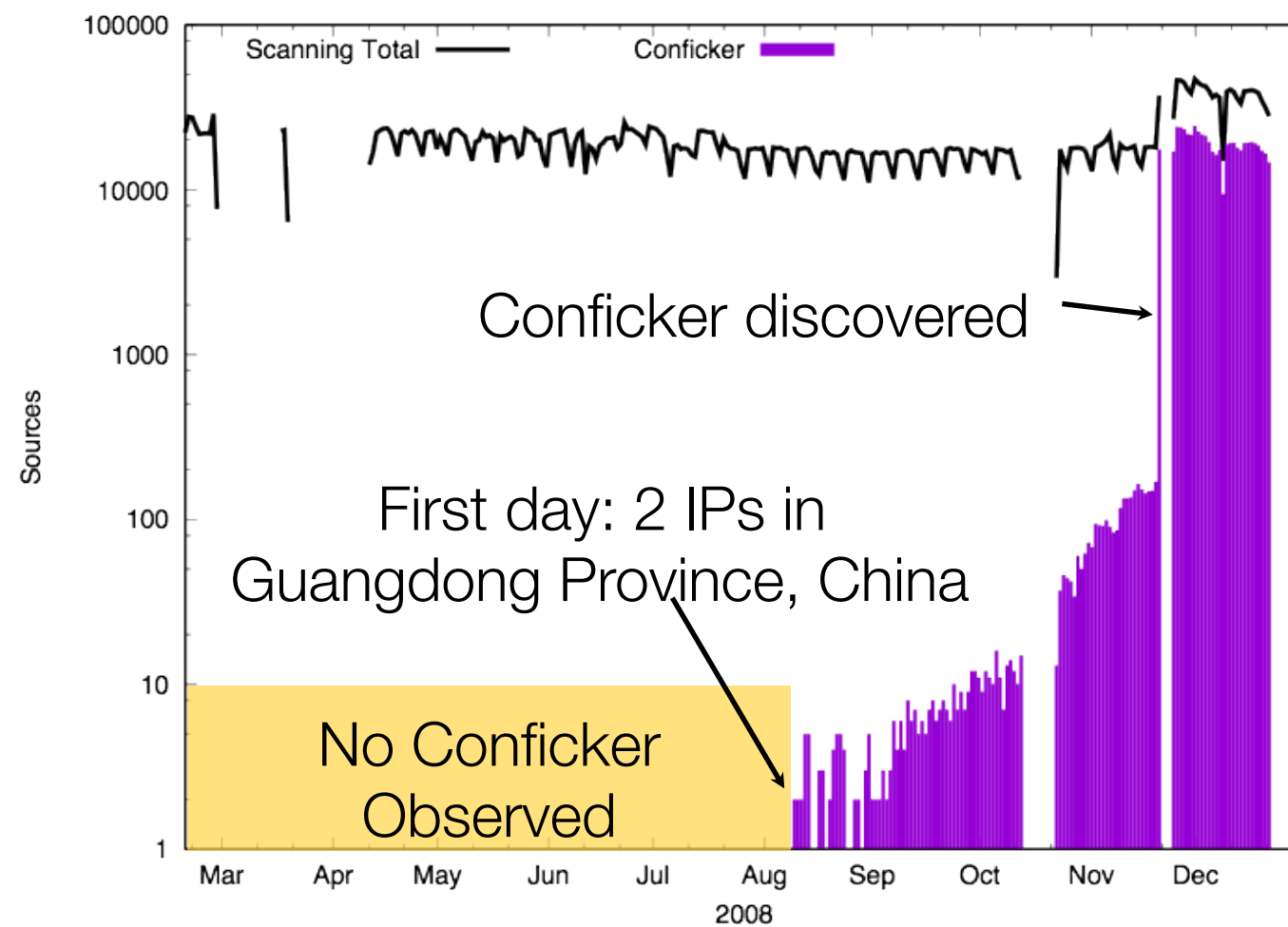
- Bug in PRNG: primarily targets IP addresses  $\{A.B.C.D \mid B < 128 \text{ \& } D < 128\}$ 
  - Developed heuristic to identify sources randomly scanning with this bug





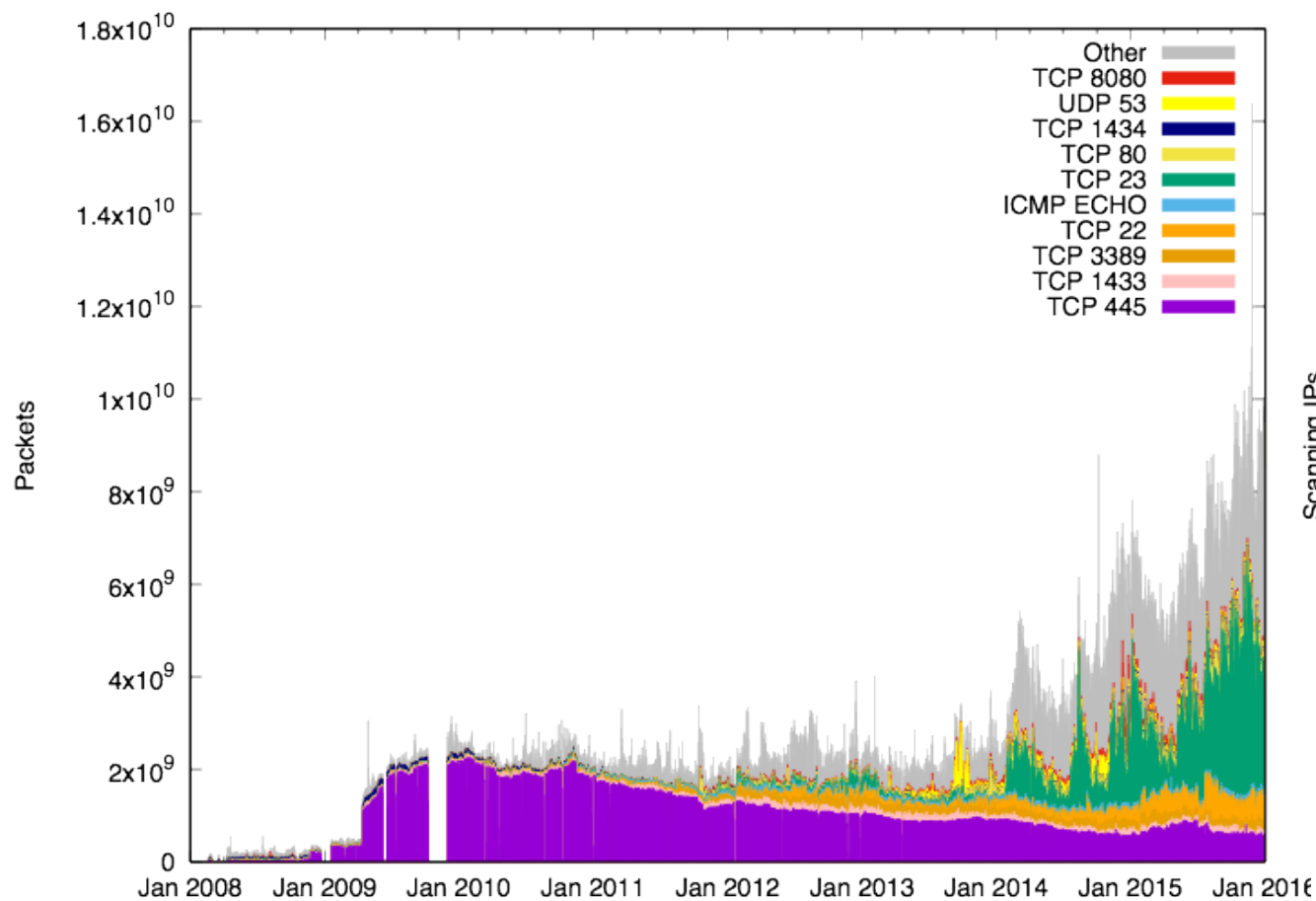
# How do we know which packets originate from Conficker?

- Bug in PRNG: primarily targets IP addresses  $\{A.B.C.D \mid B < 128 \text{ \& } D < 128\}$ 
  - Developed heuristic to identify sources randomly scanning with this bug
- Some evidence of a testing phase prior to discovery

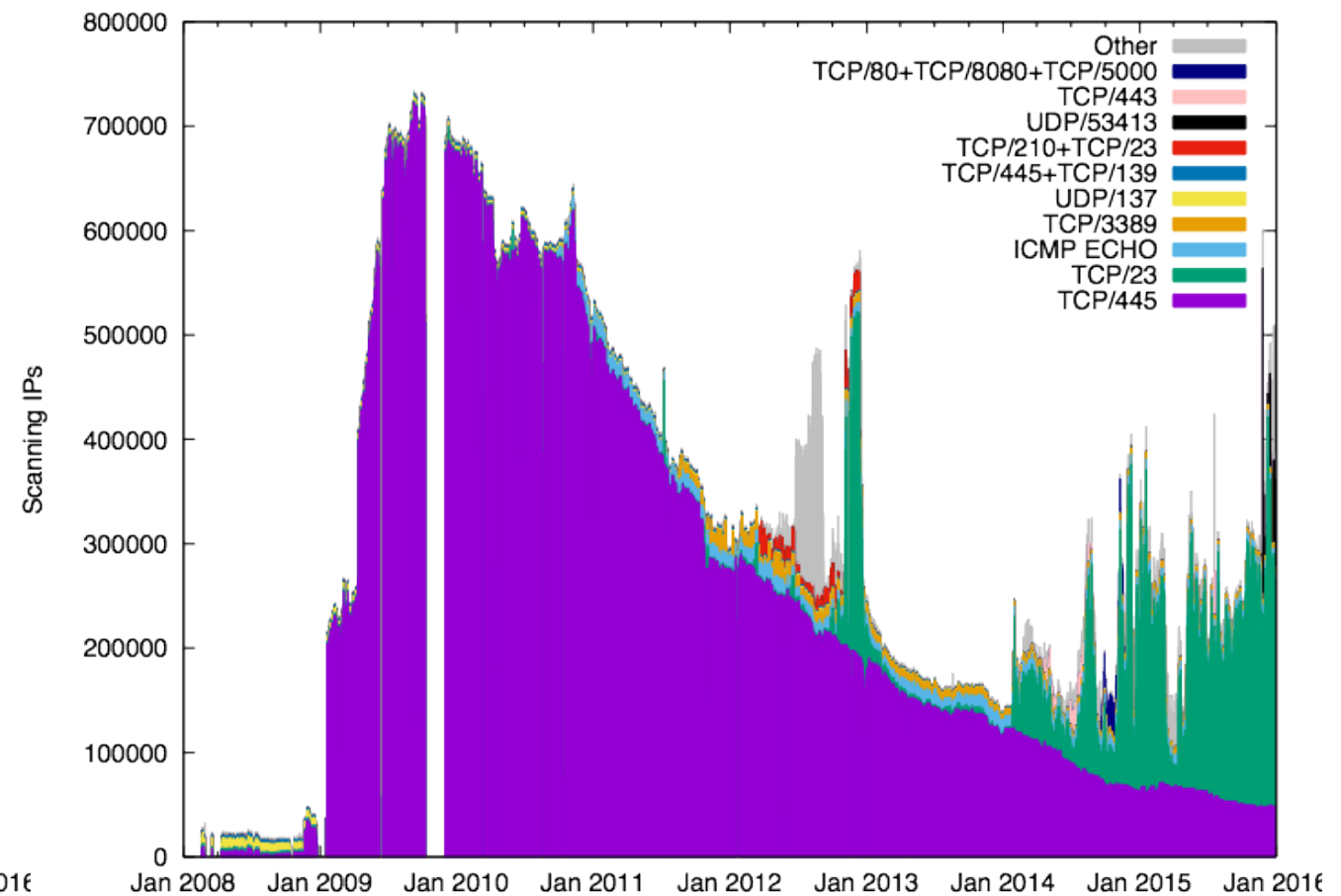


# Scanning Post 2012

- Conficker is dying out
- Port 23 (telnet) is popular



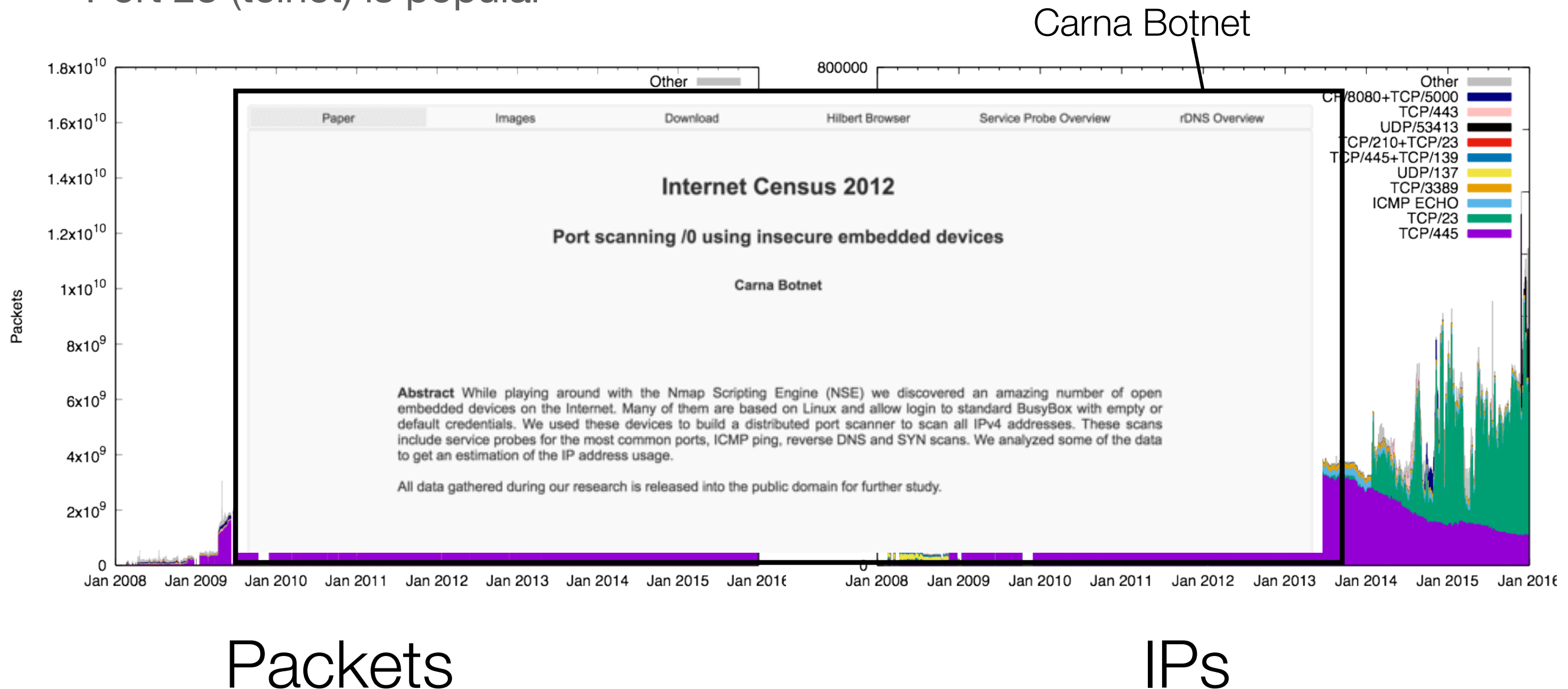
Packets



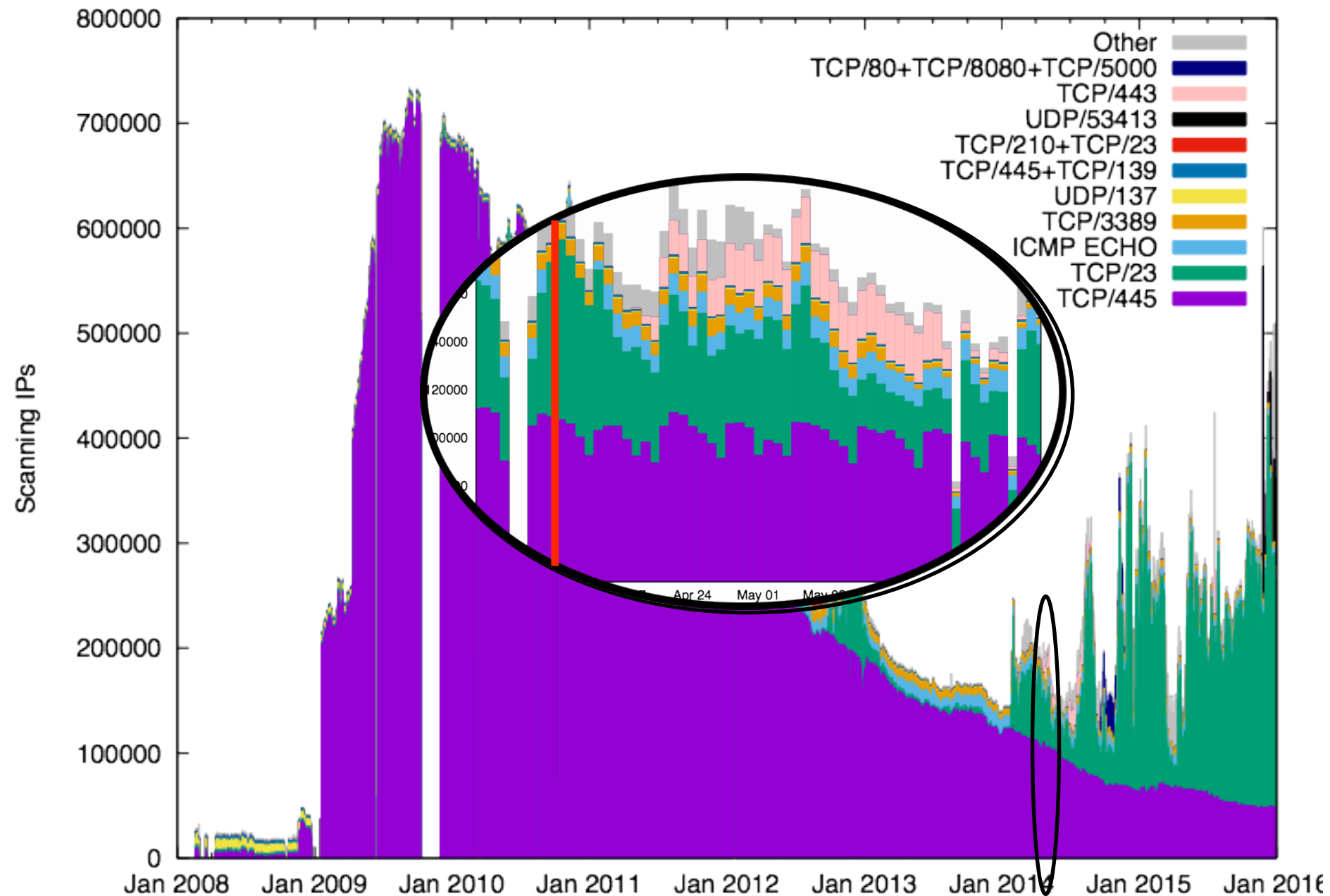
IPs

# Scanning Post 2012

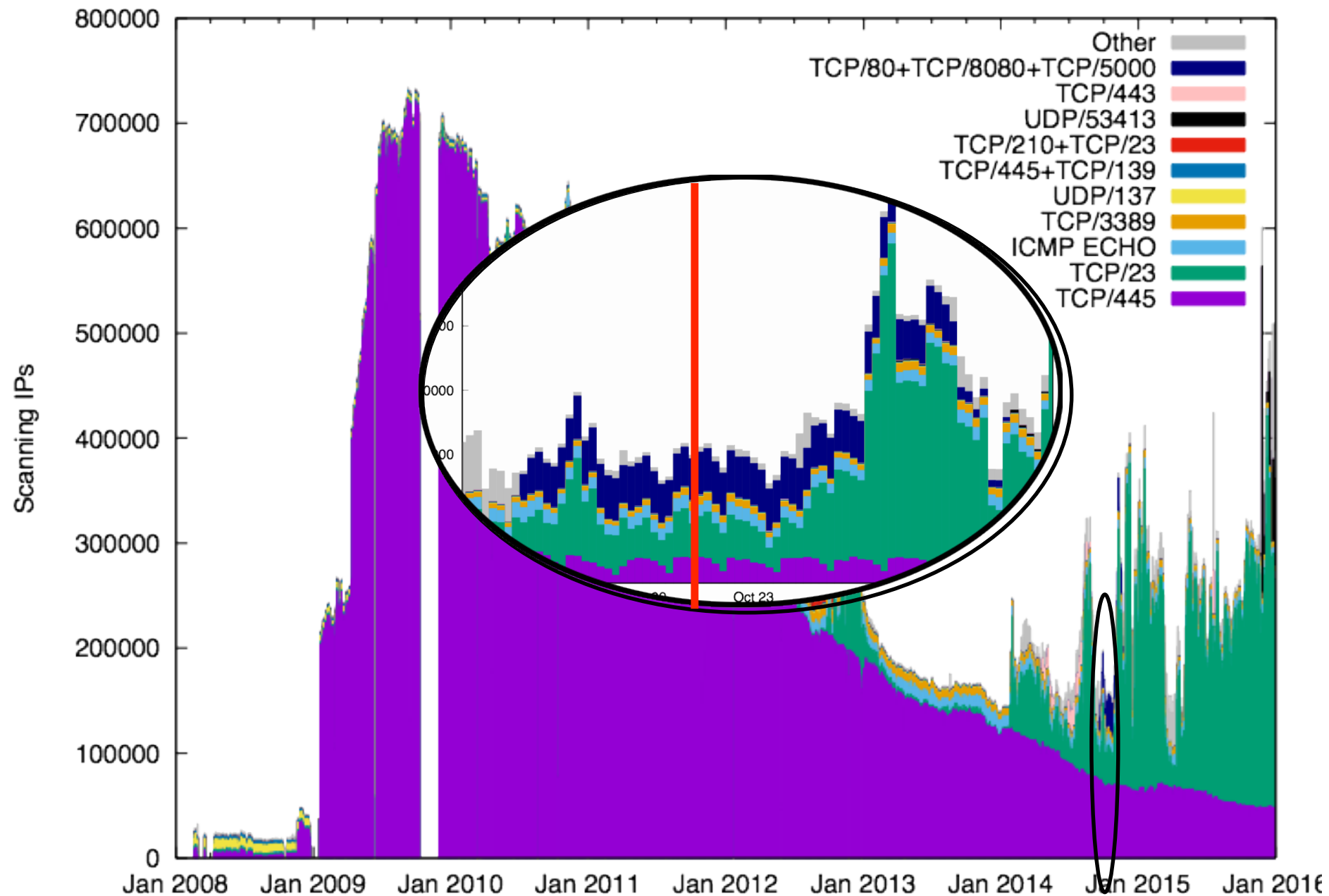
- Conficker is dying out
- Port 23 (telnet) is popular



# Scanning Post 2012: Scans of TCP/443 following Heartbleed vulnerability announcement



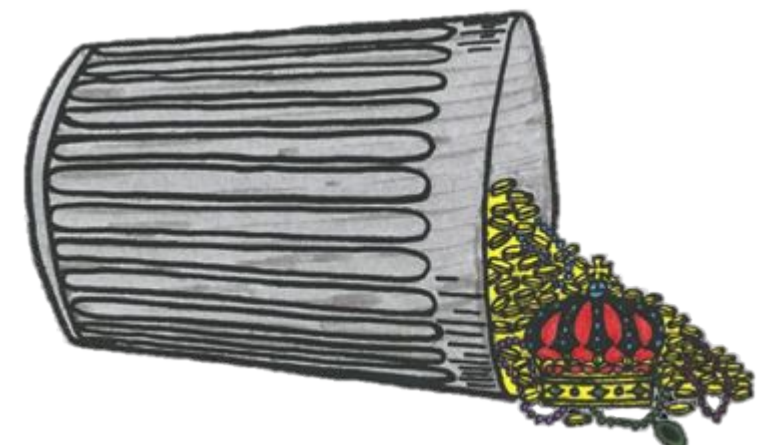
# Scanning Post 2012: Scans of TCP/5000 prior to Akamai report of UPnP used for DDoS attacks



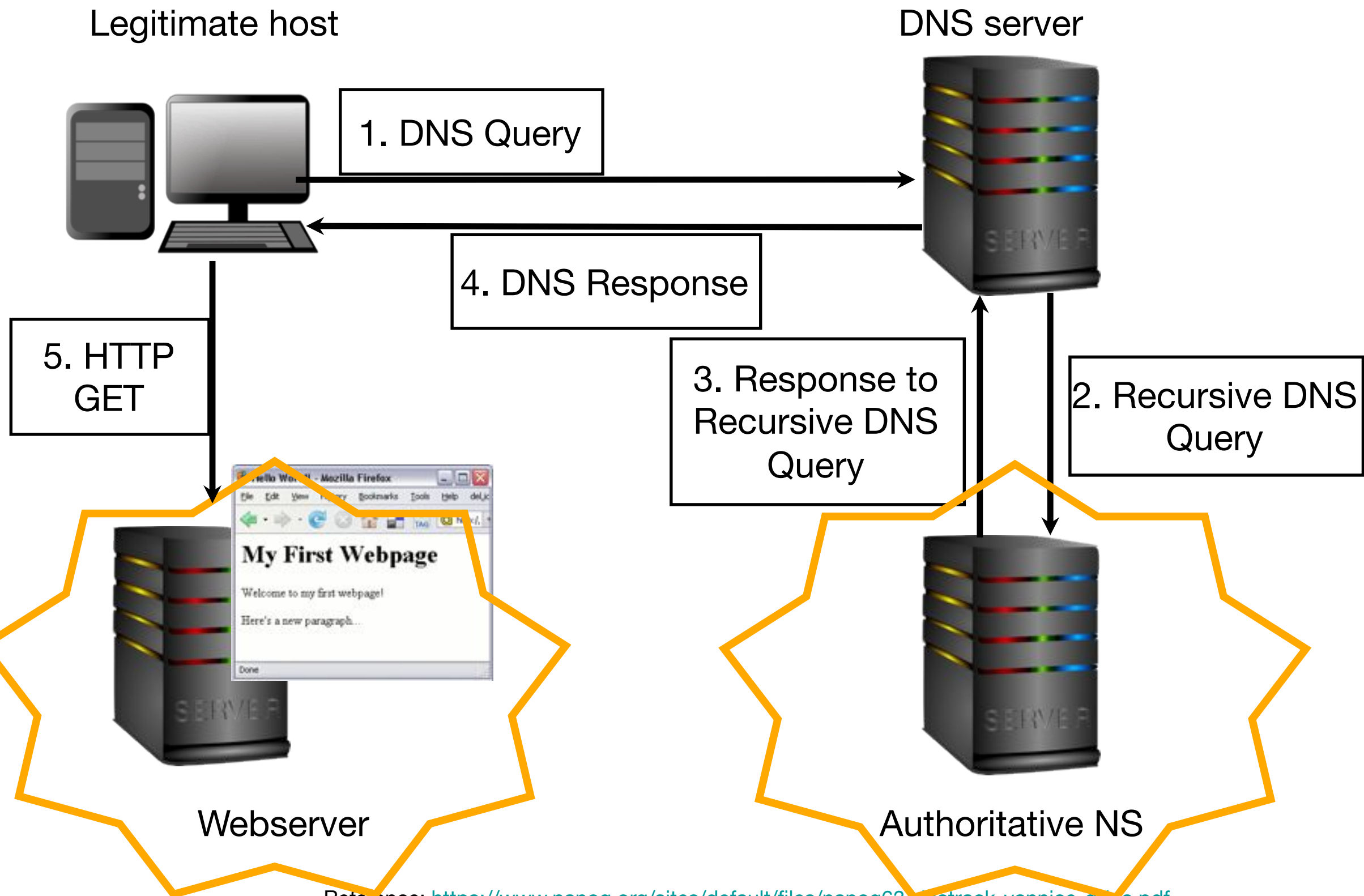
# Network telescopes capture a wealth of security-related data

---

- Scanning: Trends and relation to vulnerability announcements
- **Backscatter: Attacks on authoritative name servers**
- Misconfigurations: BitTorrent index poisoning attacks
- Bugs: Byte order bug in security software
- Unknown: Encryption vs. obfuscation



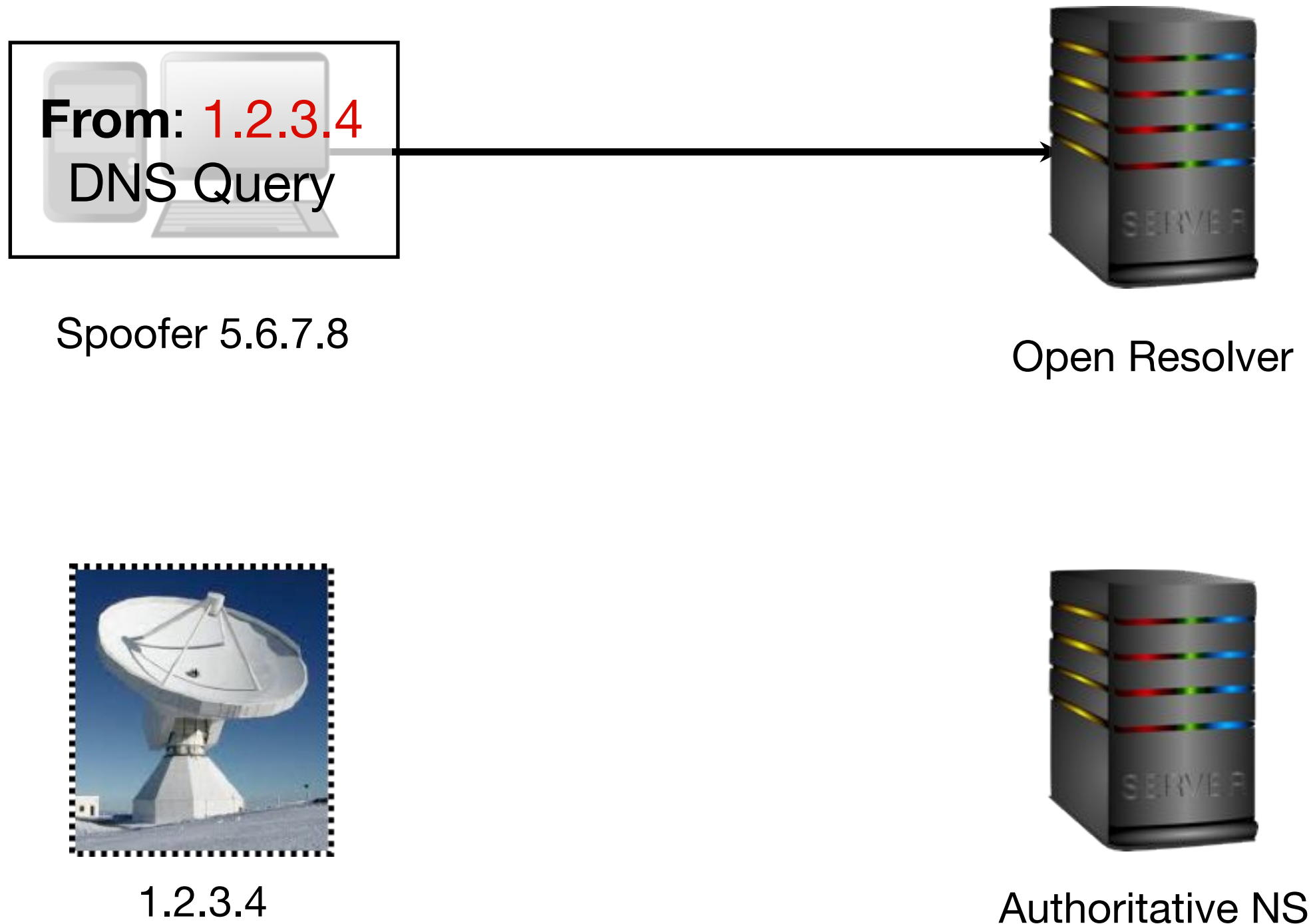
# Preventing access to websites via attacks on authoritative name servers





# Why we see some of these attacks: open resolvers

---





# Why we see some of these attacks: open resolvers

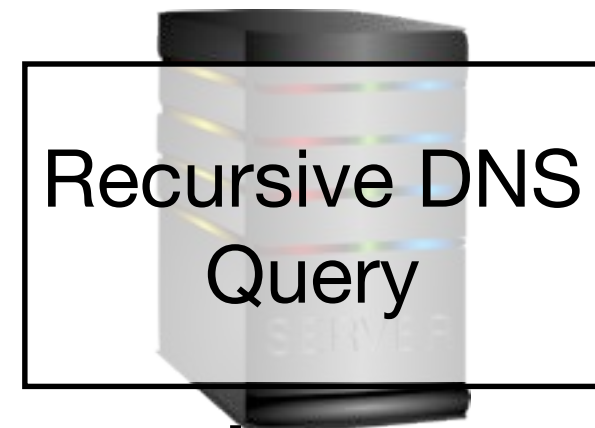
---



Spoofers 5.6.7.8



1.2.3.4



Open Resolver



Authoritative NS

# Why we see some of these attacks: open resolvers

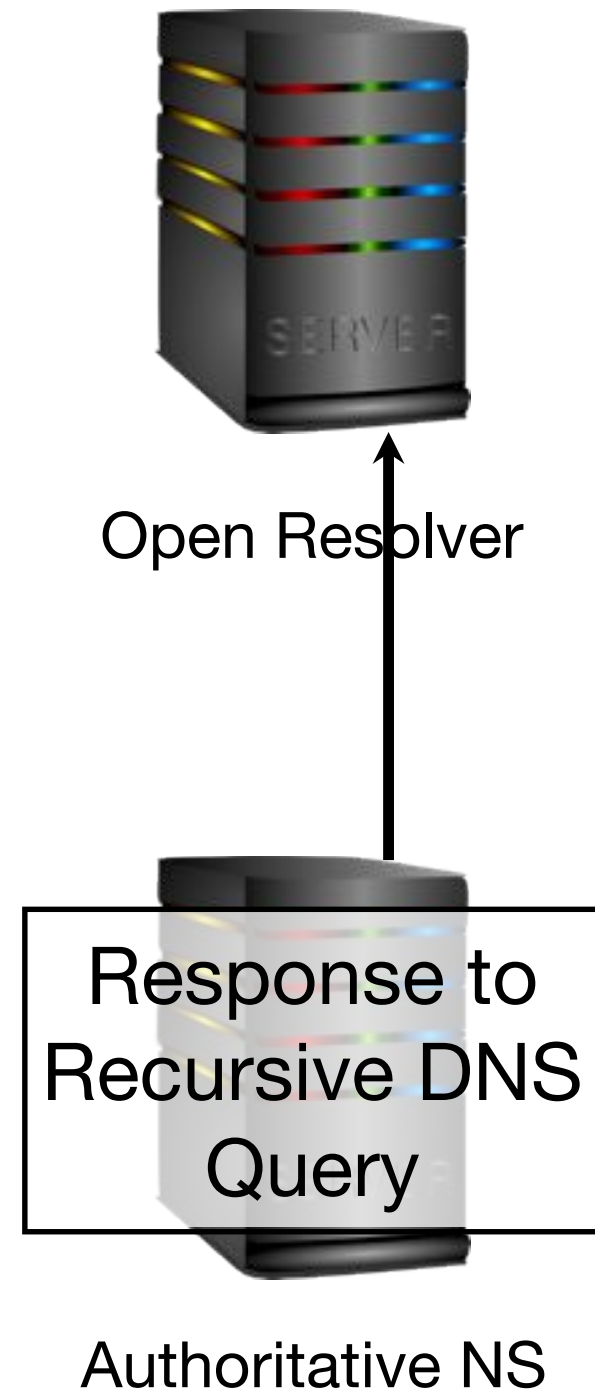
---



Spoofers 5.6.7.8



1.2.3.4

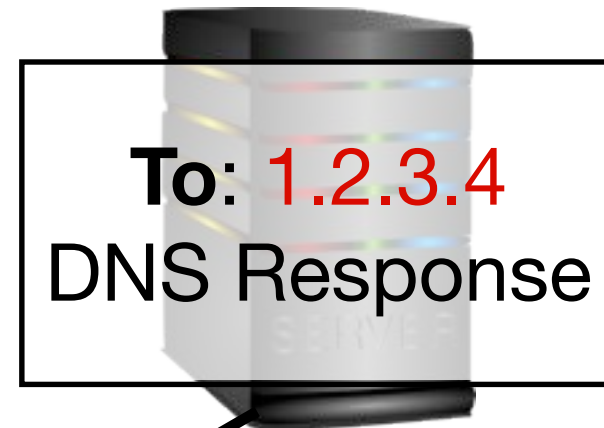


# Why we see some of these attacks: open resolvers

---



Spoofed 5.6.7.8



Open Resolver



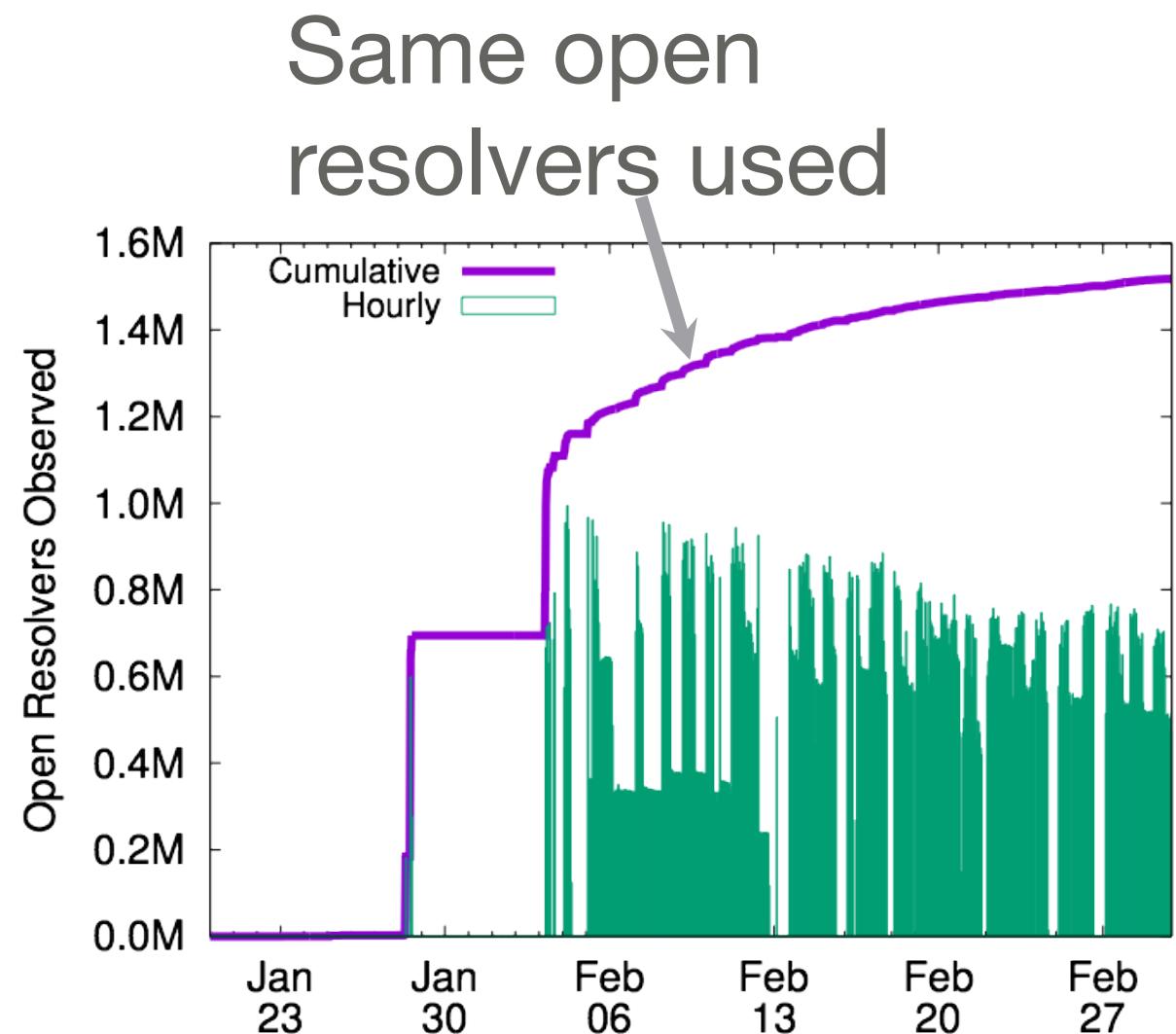
1.2.3.4



Authoritative NS

# We infer more open resolvers as a result of an increase in DNS traffic

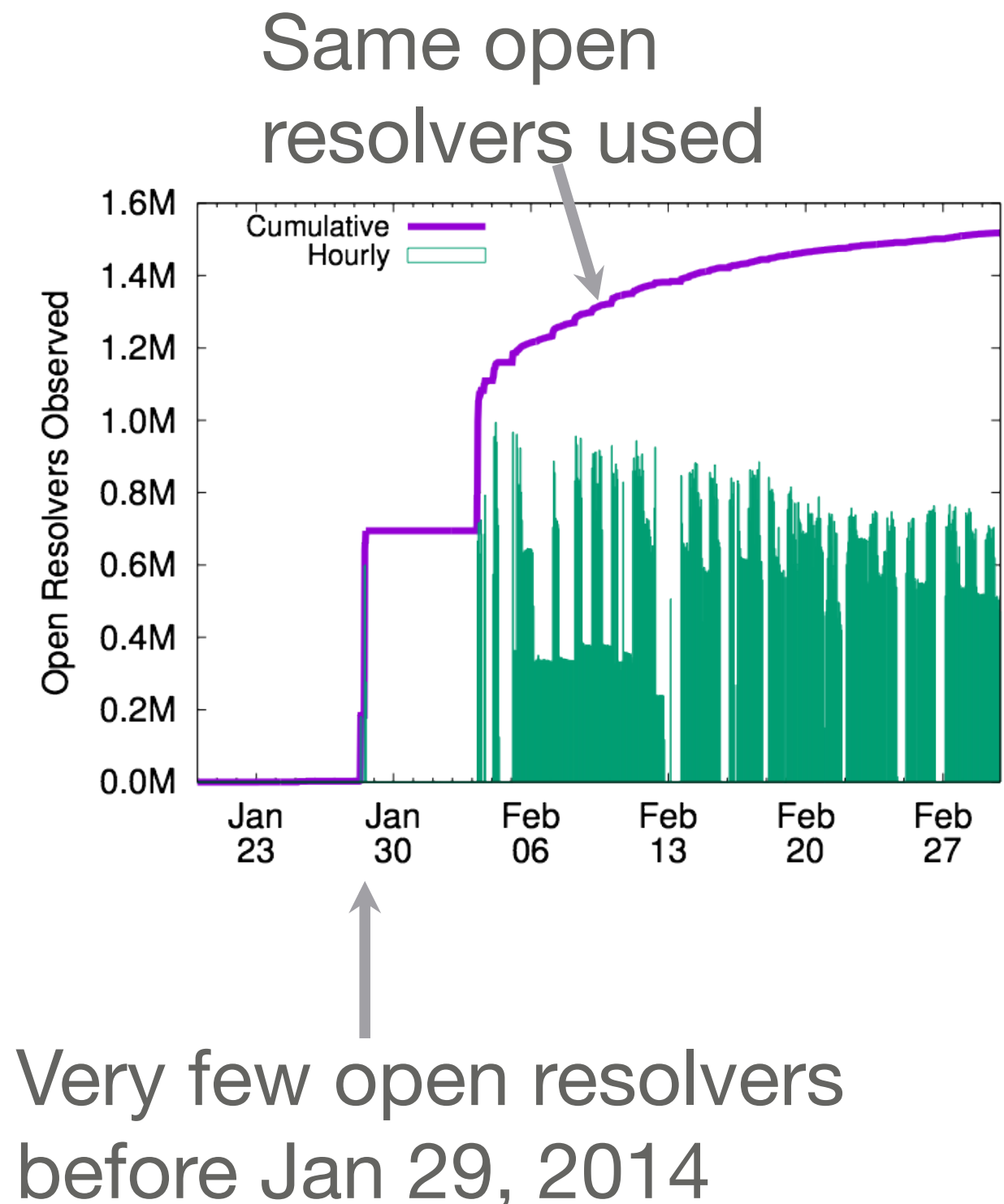
	IPs
IBR ~July 2013	3.4k
IBR ~Feb. 2014	1.56M



Very few open resolvers  
before Jan 29, 2014

But the number of open resolvers we see is much less than active probing

	IPs
IBR ~July 2013	3.4k
IBR ~Feb. 2014	1.56M
Open Resolver Project ~Feb. 2014	37.6M



# The open resolvers we observe are used in DoS attacks... and it's working

---

	IPs	OPCODE: OK	OPCODE: SERVFAIL	Problem with the (authoritative) NS
IBR ~July 2013	3.4k	3.0k	148	
IBR ~Feb. 2014	1.56M	1.44M	1.45M	High number of errors
Open Resolver Project ~Feb. 2014	37.6M	32.6M	0.92M	Low number of errors

# Queried domains

- First day: queries for baidu.com --- likely testing phase
- Data from first month of activity. We still observe the attack.

020sf.com 024web.net 027dz.com 028xkj.com 029sms.com 02gd.com 0319pk.com 03lcq.com 052000.com 0538hj.com 0571video.com 059sem.com  
0769cg.com 0769ff.com 08ws.com 111da.com 1188008.com 1234176.com 139hg.com 167uc.com 16888china.com 173pk.com 176cc.com 176dd.com  
176gj.com 176kw.com 176l.com 176mm.com 176xq.com 17c.cc 180xp.com 184sf.com 185jxcq.com 191cq.com 19jy.com 201314baidu.com 202aaa.com  
236899.com 24ribi.com 250hj.com 266mi.com 269sf.com 2kkx.com 3000sy.com 300eeee.com 300lll.com 300ssss.com 303aaa.com 303bbb.com 30gg.com  
316ms.com 321xy.com 360362.com 365ddos.cn 369df.com 38db.com 38za.com 3gabn.com 3kkx.com 3q518.com 3t33.com 4000123046.com 40cqcq.com  
442ko.com 4z1s.info 500sf.com 512312.com 513wt.com 515kkk.com 51aidi.com 51rebeng.com 51yjs.com 520898.com 520sfyx.com 525mk.com 52ccx.com  
52ssff.com 531gou.com 555fz.com 567uu.com 56bj56.com 5ipop.net 5kkx.com 600ddd.com 60sf.com 616162.com 63fy.com 666hf.com 68yb.com 6ee.com  
6g5b.info 6kkx.com 6ksf.com 700rrrr.com 72play.com 72sm.com 74486.com 76489.com 766mi.com 767hh.com 76wzw.com 76yxw.com 775gg.com  
778ff.com 787ok.com 799mi.com 7afa.com 7s7ss.com 800liao.net 800nnnn.com 83uc.cn 83wy.com 84822258.com 85191.com 87145.com 87xn.com 885jj.com  
911gan.com 911ii.com 911mimi.com 911sepian.com 911xi.com 911xu.com 940945.net 97pc.net 980311.net 981118.com 98989833.com 991816.com  
9aq.com 9kanwo.com 9kf.com 9zny.com a6c5.com akadns.net aliyuncs.com atnext.com aws520.com b166.com badong123.com bbidda.com bbjck.com  
bettykid.com bjts168.com boeeo.com boooooook.com bw176.com byfire.com cdxgy.com cg1314.com cgxin.com chinahjfu.com chuansf-1.com chuansf.com  
cp375.com cq520.com cqqhjgj.com cs912.com ct0553.com ct176.com ctysy.com dt176.com dudu176.com dw173.com dytt8.net e0993.com e5e566.com edge  
fw10000.com fzl4.com gbdzd.com gegegan1.com gegequ.com go176.com hao9458.com haocq99.com haosf3165.com haosf86.net hcemba.com hcq  
hi0762.com hi182.com hj19.com hj321.com hkdns-vip.com hl176.com hltbdcn.com huaxia76.com hw166.com hyh588.com hz96.com icheren.net  
jdyw.com jeeweb.net jf086.com jh219.com jiaduolu.net jiayun588.com jk5888.com kp811.com kr5b.com kx2014.com laocq.com laocq180.com  
like400.com lmh176.com love303.com lpp176.com lsr176.com luse0.com luse8.com luse9.com lwfb800.com lxt998.com lygfp.com lyxyqp.com lz9999.com  
miryy.com mly555.com mm5ii.com ncmir.com net0335.com nextmedia.com pkxf08.com puhup.com purednsd.com purevm.com px518.com q1.com qf  
rp1704.com rq180.com s6s5.com salangane-books.com scktsj.com sdcsnk.com sf665.com sf717.com sg500.com sh1099.com sheshows.com sinaapp.com  
tangdefenghuang.com tg180.com tianmao76.com tjldktv.com txj880.com wanfuyou.com wb123.com wfbaby.net wn176.com wotebang.com wsn88.com  
xhzssj.com xia00.com xiaolongcq.com xiaoyx123.com xie139.com xin2003.com yeyelu9.com yg521.com yh996.com yifeng2012.com yinquanxuan.com  
yuhuakonggu.com yw110.com yw119.com yx5881.com yy188.com yy698.com zhaoil.com zhaoqjs.com zhizunfugu.com zinearts.com zongzi0898.com zst05  
5rxe.info 999.net.ru baidu.com bb0575.com gb41.com geigan.org lhy

## Example Registration Info:

Domain Name:029sms.com

Updated Date:2014-02-14 14:55:38

Creation Date:2014-02-14 14:55:38

Registrant

Street:hkjhhkjhhkjhhkjRegistrant

City:Beijing ShiRegistrant State/

Province:Beijing ShiRegistrant Postal

Code:333333Registrant

Country:ChinaRegistrant Phone:

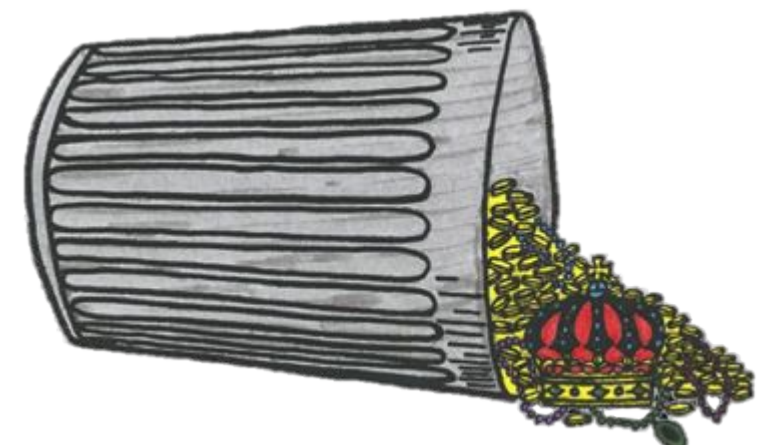
11111111Registrant Phone

Ext:Registrant Fax:11111111

# Network telescopes capture a wealth of security-related data

---

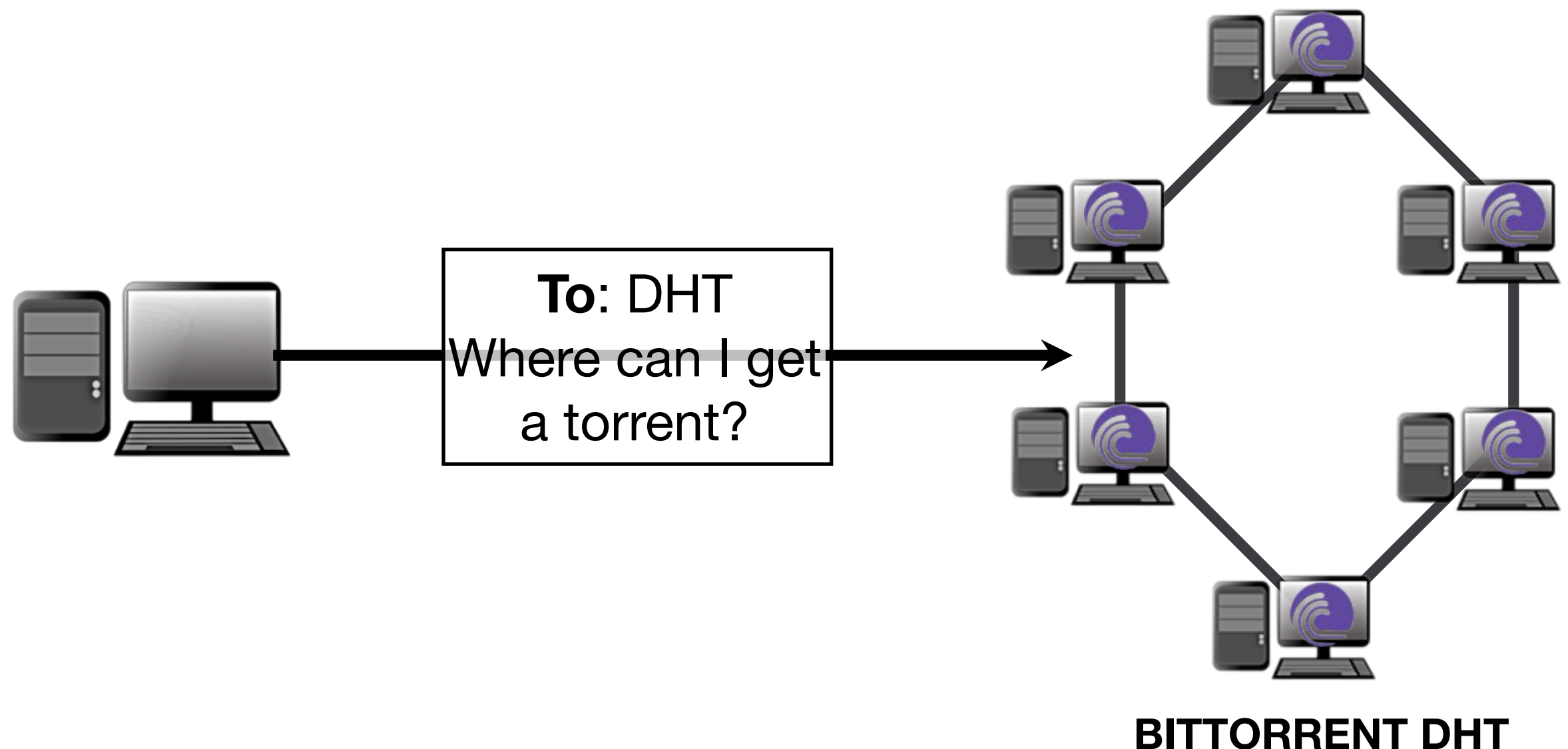
- Scanning: Trends and relation to vulnerability announcements
- Backscatter: Attacks on authoritative name servers
- **Misconfigurations: BitTorrent index poisoning attacks**
- Bugs: Byte order bug in security software
- Unknown: Encryption vs. obfuscation





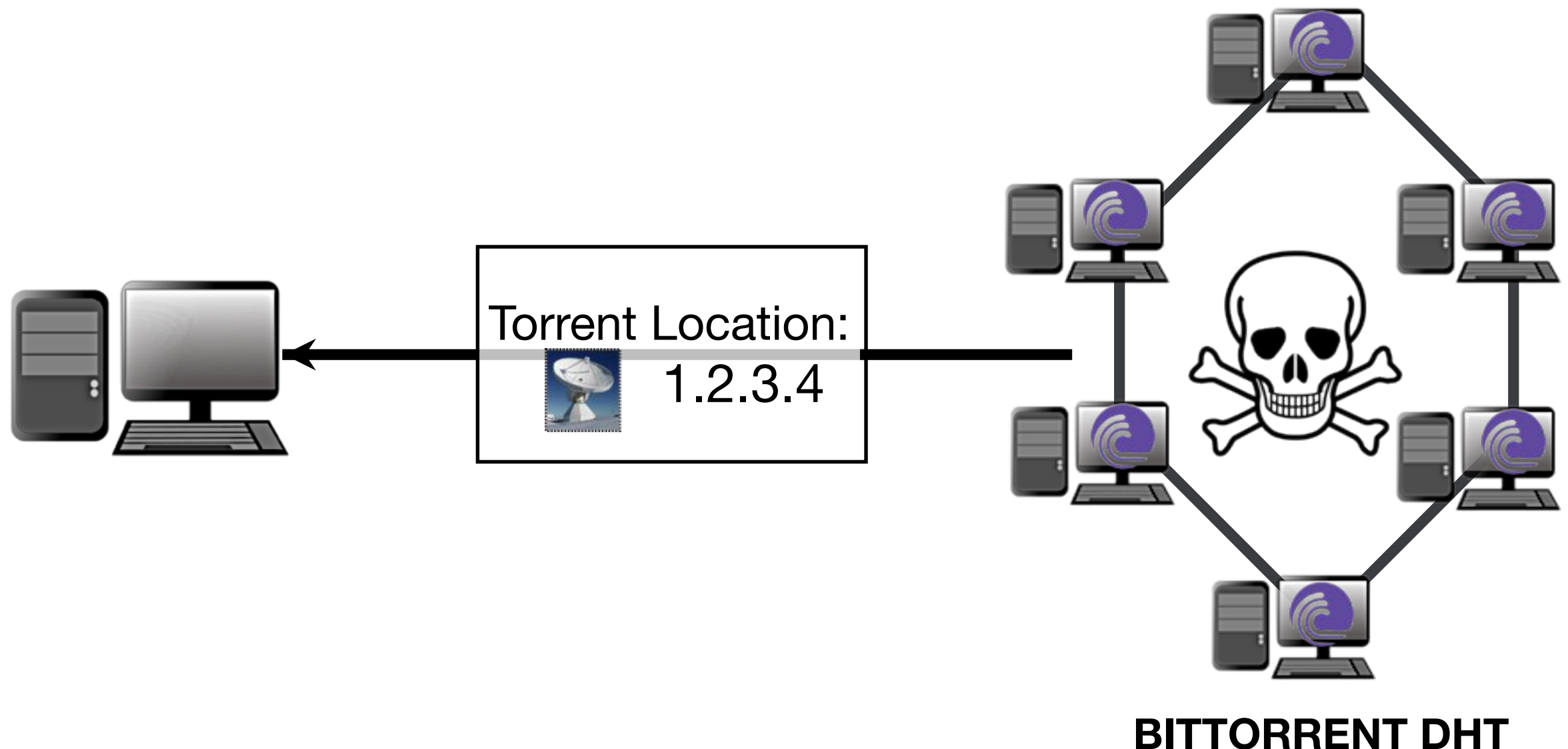
# BitTorrent index poisoning attacks induce many hosts to send IBR

- Index poisoning: purposefully inserting fake information into the DHT



# BitTorrent index poisoning attacks induce many hosts to send IBR

- Index poisoning: purposefully inserting fake information into the DHT



# Popular Torrents in IBR - July 2012

hash	Torrent	Packets
48484fab5754055fc530fcb5de556 4651c4ef28f	Grand Theft Auto - Chinatown Wars	450k
5b5e1ffa9390fff13f4af2aef9f58 61c4fbf46eb	Modern Family S3E22	398k
d90c1110a5812d9a4bf3c28e27 9653a5c4f78dd1	CSI S12E22	204k
2ecce214e48feca39e32bb50df cf8151c1b166cc	Coldplay Ft. Rhianna Princess of China	187k
79f771ec436f09982fc345015fa 1c1d0d8c38b48	???	129k
b9be9fc1db584145407422b09 07d6a09b734a206	Parks and Recreation S4E22	127k
99a837efde41d35c283e2d9d7 e0a1d4a7cd996dd	Missing 2012 S1E9	106k
7b05b6b6db6c66e7bb8fa5aa7 0a185c7cfcd3d07	???	104k
c0841cf3196a83d1d08ae4a9e af10fcfc6c7ba66	Big Trouble Little China	99k
99dfae74641d0ca29ef5238607 13a6270daefc6e	36 China Town	91k

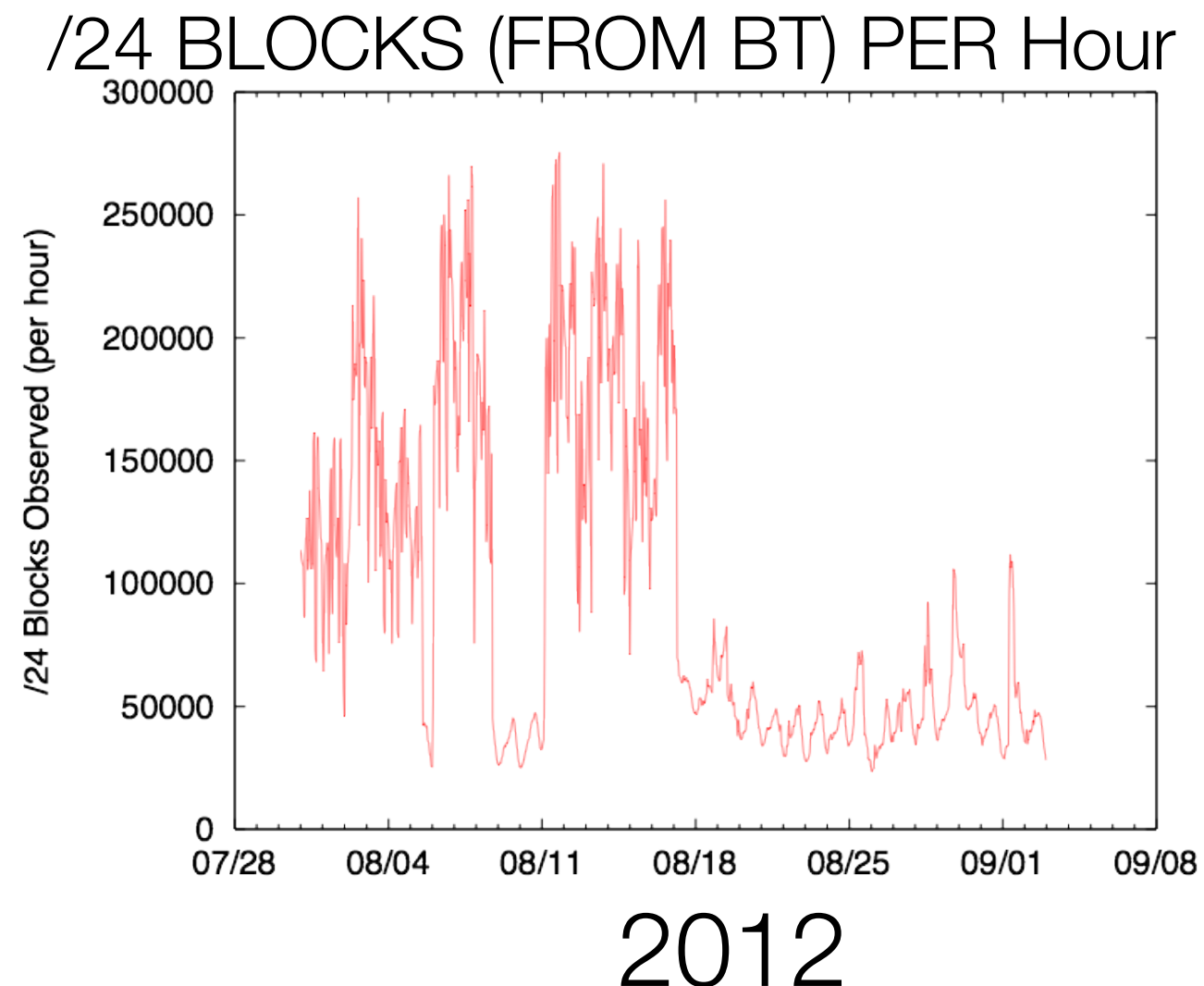
# Popular Torrents in IBR - July 2013

hash	Torrent	Packets
f7eb38b830ec749f43cf3df20dbc2bf2c99fad97	Sette Anni in Tibet	2,356k
6ec64cb88937418d6af29fca6d017e0c658654b7	高清蓝光720P版BD-RMVB.中字	912k
f90cb027174c2af3c5b838be09a62ff16d6c2ef5	美丽生灵 TC英语中字.rmvb	845k
fedcf797109c7929558d069602ac6fab0b46e814	Halo 4 Until Dawn	735k
3b508d09e9c4677b2f67683a9dde2d5ce0b2aa24	soh 360	580k
1254bb23d1a04447cb67bc0479549a504d083c31	Her Sweet Hand China Lost Treasure	539k
48484fab5754055fc530fcb5de5564651c4ef28f	Grand Theft Auto - Chinatown Wars	489k
b9be9fc1db584145407422b0907d6a09b734a206	Parks and Rec S4E22	482k
93efed3aa07e7523d5c4e42f0257f9aa8d5011c3	Dajiyun	431k
039a07b38de4529c477f3b75698937e9c5d4acd6	ntdvt news	325k

# BitTorrent: Temporal aspect

---

- Unclear why fewer /24 blocks are observed
- But pausing attack is a possible explanation



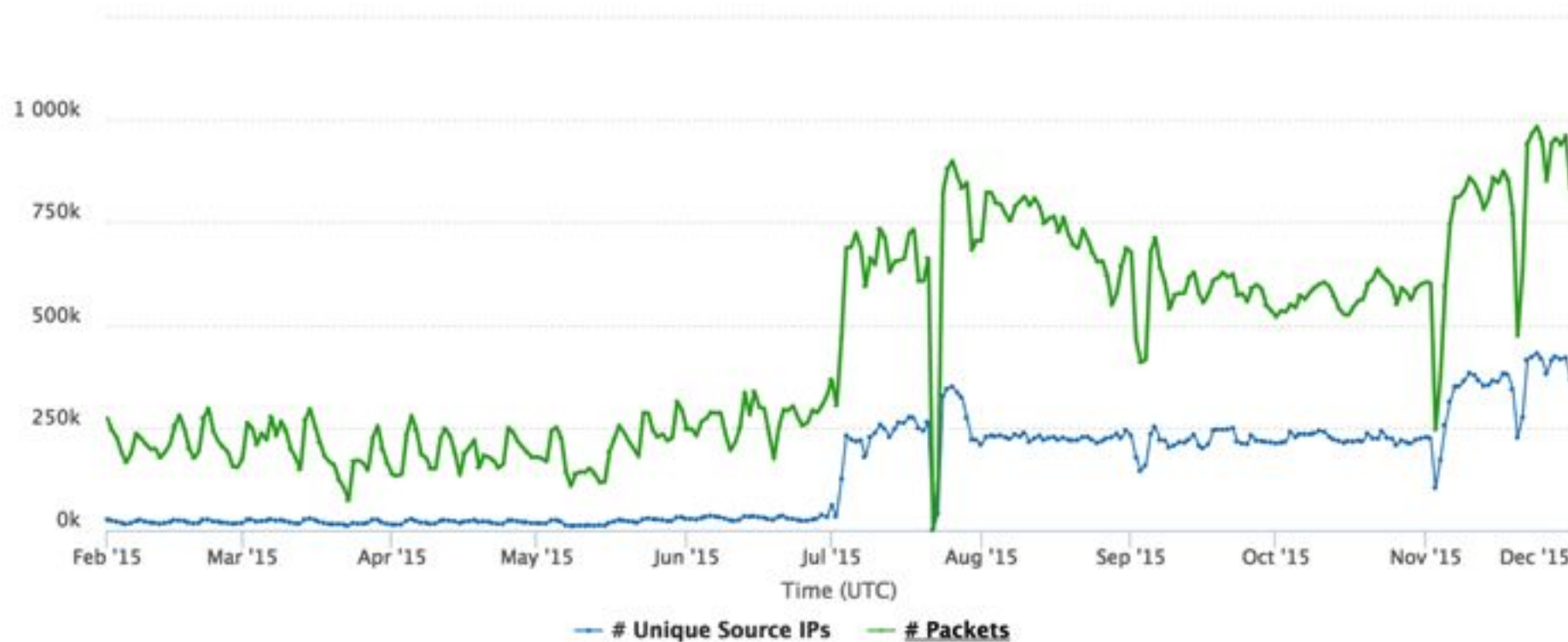
# BitTorrent: Spatial aspect

---

- /24 blocks sending BitTorrent KRPC packets are more likely to be observed by certain destination IPs and ports
  - get\_peers and find\_node packets: certain IP addresses more likely to be targeted :  $\{X.B.C.D \mid B \ \& \ 0x88 = 0x00 \text{ and } D \ \& \ 0x09 = 0x01\}$
- A bug in PRNG for generating IP addresses is a plausible explanation

# July 2015: Huge increase in BitTorrent traffic

---



- Graph: BitTorrent KRPC packets
- Increase is caused by traffic destined to 1 IP => traffic from over 3.7M /24s per month
- Still going on... not sure of all the details yet

# Investigating July 2015 increase in BitTorrent IBR

---

- Installed two BitTorrent clients on one machine (uTorrent, Deluged)
- Just joined DHT didn't download any torrents
- ~2.5 months: Nov. 15 2015 - Jan. 28 2016
  - uTorrent: 12 IPs sent 112 packets to a network telescope IP
  - Deluged: 51 IPs send 64 packets to a network telescope IP
- Who directed us to network telescope?
  - LibTorrent most popular client, but not used exclusively
  - China most popular geolocation, but not exclusively



# Suspicious BitTorrent behavior

---

- Most IDs associated with network telescope IP have their third byte equal to 0x04
- Other IP address in response packets occur frequently and have third-byte quirks

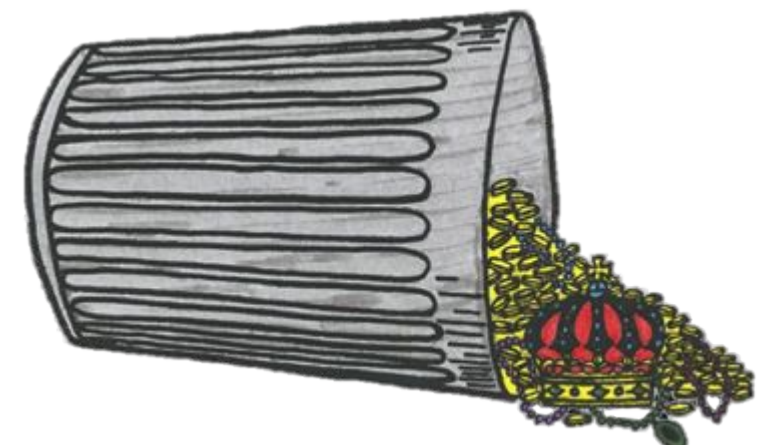
Sample node IDs
b8:1d:04:ef:96:18:e4:20:6b:c2:8d:1a:31:af:de:7a:81:66:02:56
bd:23:04:04:e9:5e:f5:a0:10:08:06:95:a3:ab:93:c7:74:f5:a6:58
52:b1:04:09:49:b4:91:f8:38:e6:c5:06:38:8d:04:8a:50:99:3f:50
05:b5:04:7e:6a:b8:96:1a:35:07:4e:ae:3e:d3:41:21:95:45:a8:81
13:28:04:d6:d3:2d:db:c5:07:79:7e:14:27:09:e1:37:e7:7e:25:2f
13:28:04:a9:5c:2d:82:2f:78:65:54:13:04:6d:b4:10:72:57:8d:5d

Other IP	Packets	3rd byte
157.144.153.163	76 from 6 IPs	0x05
177.123.230.26	55 from 7 IPs	0x00
212.246.161.63	64 from 7 IPs	0x06
217.123.247.72	87 from 4 IPs	0x03
27.171.198.228	55 from 8 IPs	0x07
90.122.90.178	4 from 3 IPs	0x01

# Network telescopes capture a wealth of security-related data

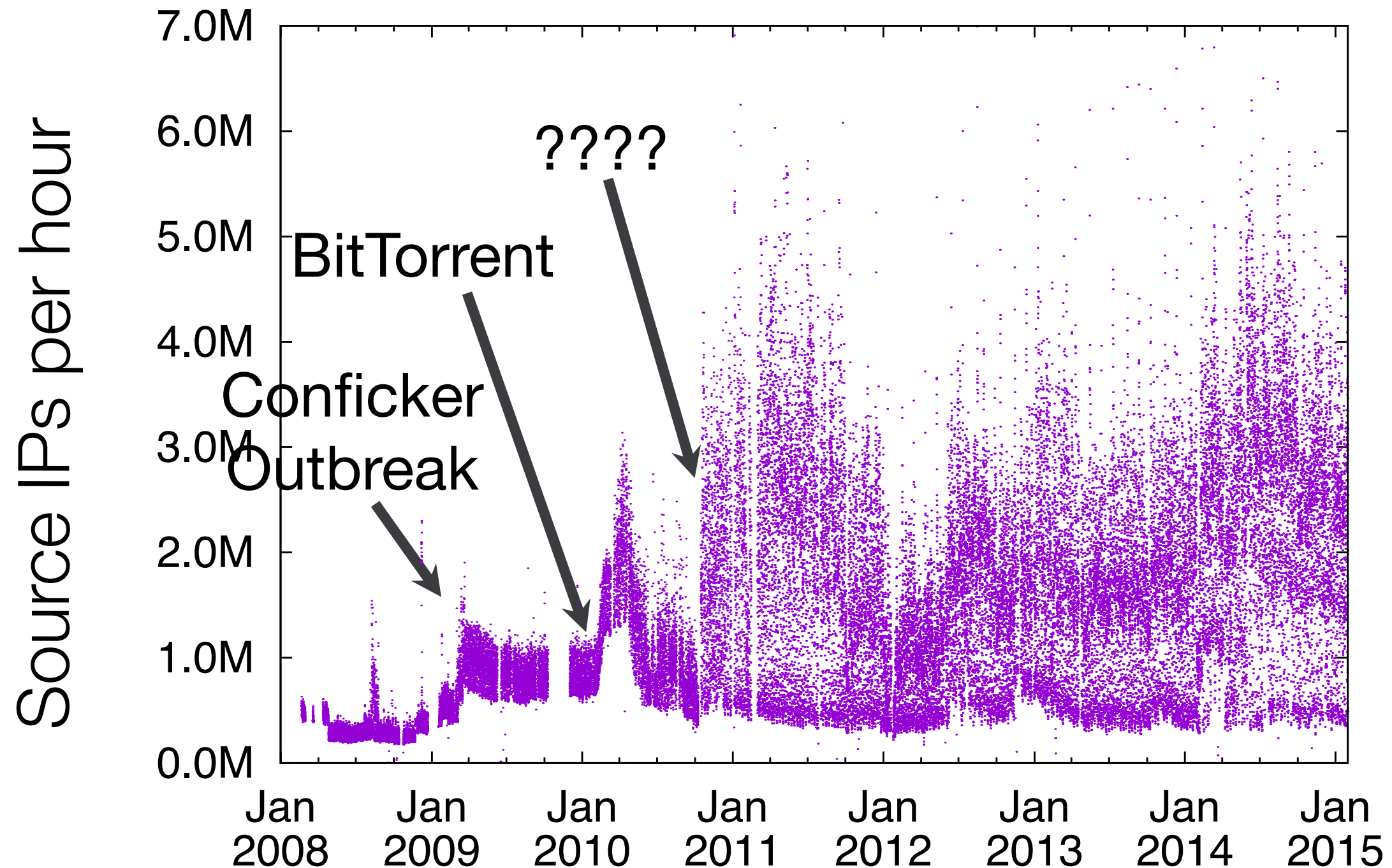
---

- Scanning: Trends and relation to vulnerability announcements
- Backscatter: Attacks on authoritative name servers
- Misconfigurations: BitTorrent index poisoning attacks
- **Bugs: Byte order bug in security software**
- Unknown: Encryption vs. obfuscation



# How many sources send us unsolicited traffic?

---



# Responsible payload

---

```
6:00:00.083796 IP 123.4.253.107.8090 > 1.179.58.115.42501: UDP, LENGTH 30
0X0000:  4500 003A DF4B 0000 2E11 ---- 7B04 FD6B  E...K.....{..K
0X0010:  01B3 3A73 1F9A A605 0026 C0CF 0000 0000  ...:S.....&.....
0X0020:  0000 0000 3100 3D57 0000 0000 0000 0000  ....1.=W.....
0X0030:  0000 0000 287E 02C7 0000
```

Fixed
Connection ID
Random
Counter

- 8090 is most popular source port
- 39455 is most popular destination port

# Lots of hosts from China

	IPs	% BGP Announced Address Space
China	101M	36.26%
Taiwan	505k	1.45%
Malaysia	442k	7.65%
USA	324k	0.03%
Hong Kong	10k	2.75%
Japan	186k	0.11%
Canada	129k	0.26%
Thailand	126k	1.55%
Australia	126k	0.31%
Singapore	116k	2.16%

4 IPs belonging to CS department!

- August 2013 data

# Monitoring CS department address space

---

- Capture 1: 36 hours of traffic in/out of CS department for this packet
  - CS address space also receives packets
  - 3 of 4 IPs from CS observed generating this traffic
- Capture 2: Monitor all traffic to/from these IPs on associated UDP ports

# Monitoring CS machines



- Packet 1: CS machines contact a common IP address: `tr-b.p.360.cn`

- Packet 2: CS machines receive a large packet

```
04:40:45.211649 IP 180.153.227.168.80 > 2.239.95.102.10102: UDP, length 1044
0x0000:  4500 0430 0100 0000 ed11 ---- b499 e3a8 E..0.....L%....
0x0010:  02ef 5f66 0050 2776 041c b5bd 0414 0350 .._f.P'v.....P
0x0020:  2c00 0000 e469 18ad ab70 9e6c dad1 d5fe ,....i...p.l....
0x0030:  c1c5 d3f7 e0cc 674d 0000 3200 0001 11d9 .....gM..2.....
0x0040:  0001 07ad 0000 0000 3538 3033 4443 3244 .....5803DC2D
0x0050:  4233 3937 3cf6 1925 1f9a 0044 3146 3443 B397<..%...D1F4C
0x0060:  3732 4334 3039 4232 7756 e0df 1f9a 0044 72C409B2wV.....D
0x0070:  3232 3134 4445 4133 4643 3138 dde8 a6ed 2214DEA3FC18....
0x0080:  6784 0044 3846 3731 4437 4342 3346 3833 g..D8F71D7CB3F83
0x0090:  7146 287a 153d 0144 3131 4545 3334 4443 qF(z.=.D11EE34DC
0x00a0:  4342 3035 718f 4da1 9d41 0144 4239 3631 CB05q.M..A.DB961
0x00b0:  3139 3441 4334 3645 73d7 4fdc 197a 0144 194AC46Es.O..z.D
0x00c0:  3131 3537 3736 3334 3946 4343 da17 0f23 115776349FCC...#
0x00d0:  2711 0144 4345 4539 3242 3938 3131 4639 '..DCEE92B9811F9
0x00e0:  b6f7 838b 2774 0144 4146 3546 4639 3333 ....'t.DAF5FF933
0x00f0:  4346 4541 b721 5ba8 2711 0144 3039 3738 CFEA.![.'...D0978
0x0100:  3030 4536 4643 4144 b622 bcb9 ace8 0144 00E6FCAD.".....D
0x0110:  3346 3935 3030 3736 3836 4342 7177 6c38 3F95007686CBqw18
0x0120:  9e52 0144 3946 3844 3139 3230 3941 4436 .R.D9F8D19209AD6
0x0130:  af0c 97d4 0845 0144 3545 4533 3335 4544 .....E.D5EE335ED
0x0140:  4642 4431 1b12 880f 1f9a 0044 3831 4230 FBD1.....D81B0
0x0150:  3542 3634 4441 4333 7075 6774 1f9a 0044 5B64DAC3pugt...D
0x0160:  3643 3146 4535 3832 3033 3330 deb4 5486 6C1FE5820330..T.
0x0170:  271c 0144 4234 4333 3130 4130 3243 3039 '..DB4C310A02C09
0x0180:  6a78 7c09 4f7b 0144 3130 3134 3044 3239 jx|.O{.D10140D29
0x0190:  4537 3234 b623 c1cc 157a 0144 4434 4430 E724.#...z.DD4D0
0x01a0:  3736 3634 4637 3042 0154 cc65 5c7e 0144 7664F70B.T.e\~.D
0x01b0:  4535 4137 3030 4330 3536 4137 6eb5 cd70 E5A700C056A7n..p
0x01c0:  2777 0144 4337 3037 3636 4233 3631 3338 'w.DC70766B36138
0x01d0:  71f9 2724 1f9a 0044 3832 3031 3232 3039 q.'$...D82012209
0x01e0:  3836 3431 dca2 f7ac 1f9a 0044 3941 4244 8641.....D9ABD
0x01f0:  4434 4437 3631 3742 2a5c 039e 0eca 0144 D4D7617B*\.....D
0x0200:  3137 3541 3834 4634 3844 3438 01cd 7bef 175A84F48D4863.{.
0x0210:  3b1a 0144 4130 3638 3042 3830 3335 3538 ;...DA0680B803558
0x0220:  ab53 1c9e ad82 0144 3841 3043 3430 3939 S      D8A0C4099
```

# Monitoring CS machines



- Packet 3-40: CS machines contact sources encoded in packet

04:40:45.211649 IP 180.153.227.168.80 > 2.239.95.102.10102: UDP, length 1044

```
0x0000: 4500 0430 0100 0000 ed11 ---- b499 e3a8 E..0.....L%....
0x0010: 02ef 5f66 0050 2776 041c b5bd 0414 0350 .._f.P'v.....P
0x0020: 2c00 0000 e469 18ad ab70 9e6c dad1 d5fe ,....i...p.l....
0x0030: c1c5 d3f7 e0cc 674d 0000 3200 0001 11d9 .....gM..2.....
0x0040: 0001 07ad 0000 0000 3538 3033 4443 3244 .....5803DC2D
0x0050: 4233 3937 3cf6 1925 1f9a 0044 3146 3443 B397<..%...D1F4C
0x0060: 3732 4334 3039 4232 7756 e0df 1f9a 0044 72C409B2wV.....D
0x0070: 3232 3134 4445 4133 4643 3138 dde8 a6ed 2214DEA3FC18....
0x0080: 6784 0044 3846 3731 4437 4342 3346 3833 g..D8F71D7CB3F83
0x0090: 7146 287a 153d 0144 3131 4545 3334 4443 qF(z'=.D11EE34DC
0x00a0: 4342 3035 718f 4da1 9d41 0144 4239 3631 CB05q.M..A.DB961
0x00b0: 3139 3441 4334 3645 73d7 4fdc 197a 0144 194AC46Es.O..z.D
0x00c0: 3131 3537 3736 3334 3946 4343 da17 0f23 115776349FCC...#
0x00d0: 2711 0144 4345 4539 3242 3938 3131 4639 '..DCEE92B9811F9
0x00e0: b6f7 838b 2774 0144 4146 3546 4639 3333 ....'t.DAF5FF933
```

04:40:45.215588 IP 2.239.95.102.10102 > 113.70.40.122.5437: UDP, length 72

```
0x0000: 4500 0064 536f 0000 3f11 ---- 02ef 5f66 E..dSo...?....._f
0x0010: 7146 287a 2776 153d 0050 1bff 0000 0000 qF(z'v'=.P.....
0x0020: f21e 9a42 4103 55e1 0000 0004 0000 0000 ...BA.U.....
0x0030: 0038 0000 0001 0000 0000 0028 e469 18ad .8.....(.i..
0x0040: ab70 9e6c dad1 d5fe c1c5 d3f7 e0cc 674d .p.l.....gM
0x0050: 3336 3050 3030 3638 3531 4534 4230 4442 360P006851E4B0DB
0x0060: 3433 3044 430D
```

```
0x0180: 6a78 7c09 4f7b 0144 3130 3134 3044 3239 jx|.O{.D10140D29
0x0190: 4537 3234 b623 c1cc 157a 0144 4434 4430 E724.#...z.DD4D0
0x01a0: 3736 3634 4637 3042 0154 cc65 5c7e 0144 7664F70B.T.e\~.D
0x01b0: 4535 4137 3030 4330 3536 4137 6eb5 cd70 E5A700C056A7n..p
0x01c0: 2777 0144 4337 3037 3636 4233 3631 3338 'w.DC70766B36138
0x01d0: 71f9 2724 1f9a 0044 3832 3031 3232 3039 q.'$...D82012209
0x01e0: 3836 3431 dca2 f7ac 1f9a 0044 3941 4244 8641.....D9ABD
0x01f0: 4434 4437 3631 3742 2a5c 039e 0eca 0144 D4D7617B*\.....D
0x0200: 3137 3541 3834 4634 3844 3438 01cd 7bef 175A84F48D4864.{.
0x0210: 3b1a 0144 4130 3638 3042 3830 3335 3538 ;...DA0680B803558
0x0220: ab53 1c9e ad82 0144 3841 3043 3430 3939 S D8A0C4099
```



# Monitoring CS machines

- More packets are exchanged...
- and sometimes there is a byte order bug!



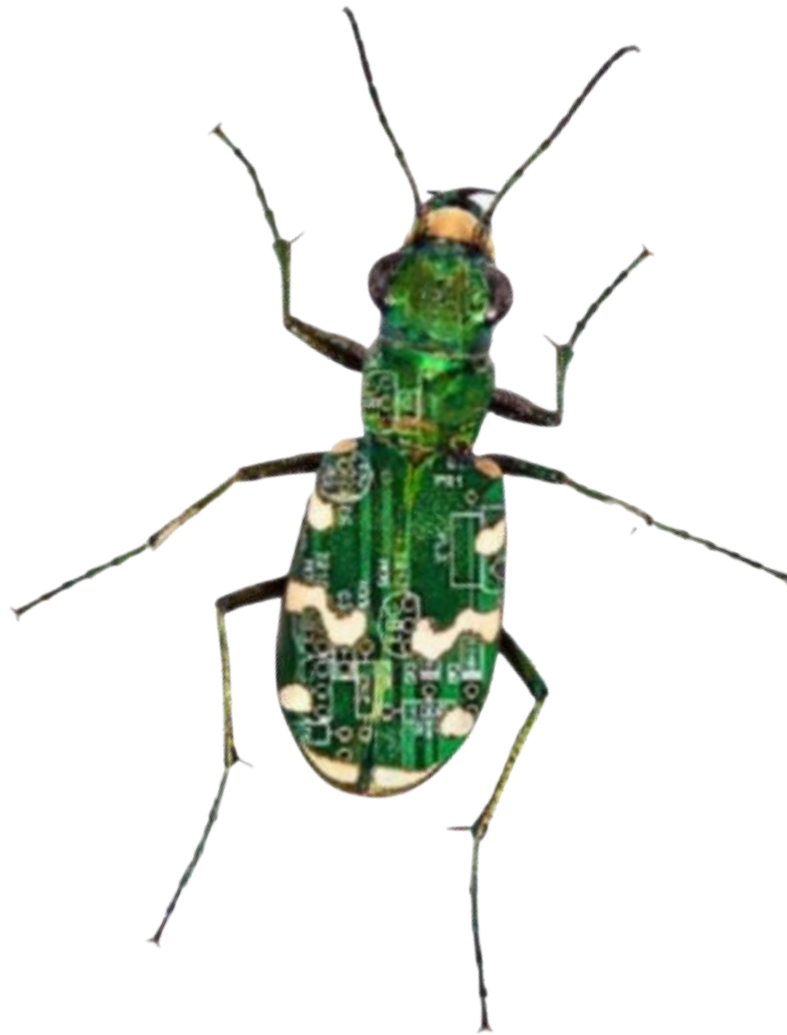
```
04:40:46.877858 IP 113.70.40.122.5437 > 2.239.95.102.10102: UDP, length 30
0x0000: 4500 003a 6213 0000 2f11 ---- 7146 287a E...b.../...qF(z
0x0010: 02ef 5f66 153d 2776 0026 8a67 0000 0000 .._f.='v.&.g....
0x0020: a800 0d13 2100 55e1 0149 f488 0134 9733 ....!.U..I...4.3
0x0030: 0038 0000 0005 0006 0000 .8.....
```

```
04:40:46.878016 IP 2.239.95.102.10102 > 122.40.70.113.15637: UDP, length 30
0x0000: 4500 003a 552d 0000 3f11 ---- 02ef 5f66 E...U-...?....._f
0x0010: 7a28 4671 2776 3d15 0026 2c6b 0000 0000 z(Fq'v=..&,k....
0x0020: 0000 0000 3100 55e1 0000 0000 0000 0000 ....1.U.....
0x0030: 0000 0000 42d6 0005 0000 ....B.....
```

- So 1.2.3.4 receives packets when intended recipient has IP address 4.3.2.1

# What software has this bug?

---



# Qihoo 360

---

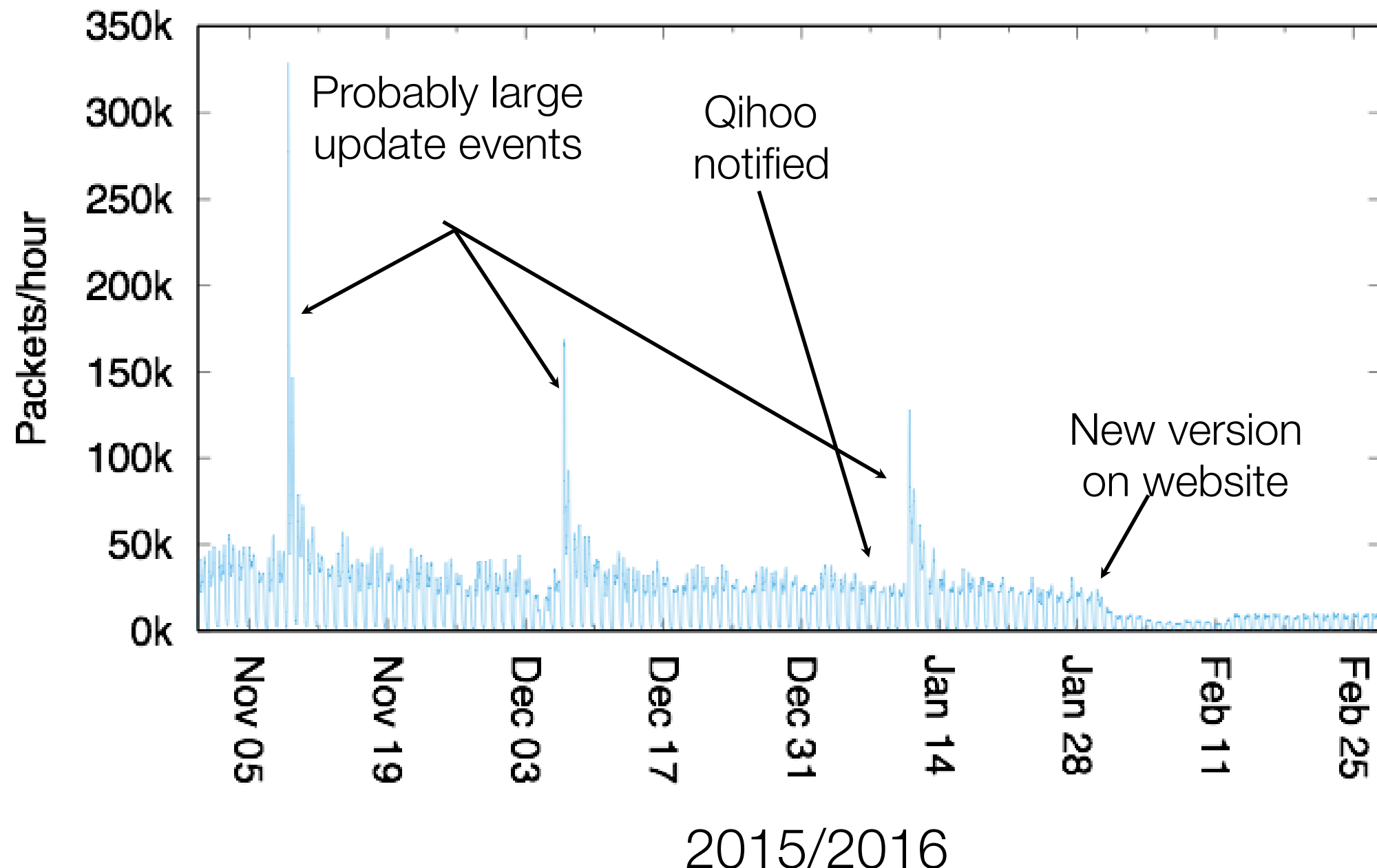


- Verified product usage with CS users
- 360 Total Security Software License and Service Agreement:

**iii) The Upgrade module of the Software uses peer-to-peer ("P2P") technology to improve upgrade speed and efficiency of your bandwidth usage. The P2P technology will cause data to be uploaded, including program modules and the Software's malware definition database, which are used as components of the Software. Your private data will not be uploaded.**

# Qihoo cleanup

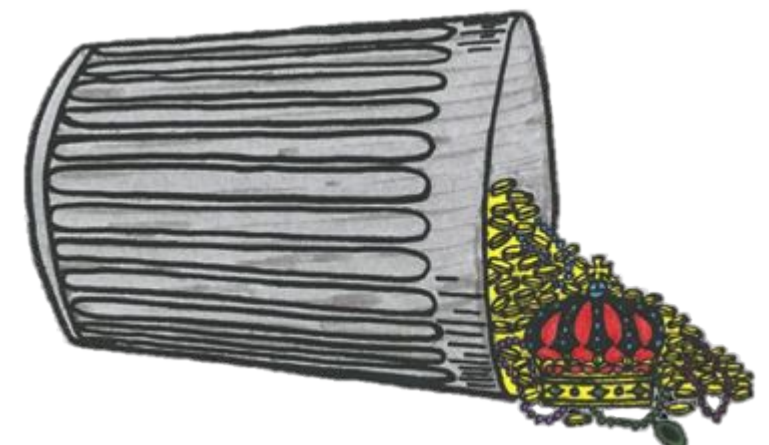
- It took about a month from notification for there to be a significant decrease in packets originating from bug



# Network telescopes capture a wealth of security-related data

---

- Scanning: Trends and relation to vulnerability announcements
- Backscatter: Attacks on authoritative name servers
- Misconfigurations: BitTorrent index poisoning attacks
- Bugs: Byte order bug in security software
- **Unknown: Encryption vs. obfuscation**



# Making the unknown traffic known

---

- Further investigation into “unknown” traffic can reveal source of traffic
- Recall packet that appeared to have encrypted payload
- Lots of traffic to 1 IP address + statistical analysis of bytes + white papers [1] => this packet is a Sality C&C

## Related packet length

```
6:00:06.000065 IP 111.248.55.49.51956 > 1.16.56.246.7605: UDP, length 19
0x0000:  4500 002f 6c48 0000 7011 ---- 6ff8 3731 E../lH..p..Fo.71
0x0010:  0110 38f6 caf4 1db5 001b 8298 7133 0f00 ,.8.....q3..
0x0020:  643e c2d4 2cf5 42b5 810f 7f01 5344 1e    d>...,.B.....SD.
```

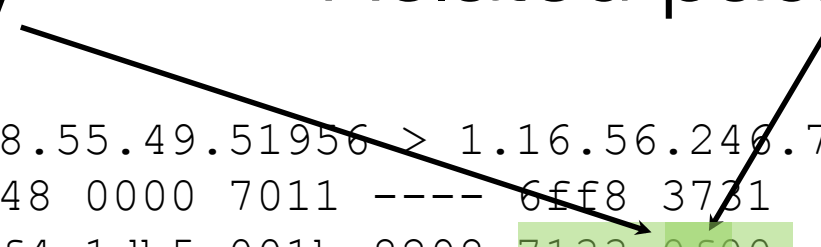
[1] Nicolas Falliere. Sality: Story of a Peer-to-Peer Viral Network.  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/sality\\_peer\\_to\\_peer\\_viral\\_network.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf), 2011.

# Making the unknown traffic known

---

- Further investigation into “unknown” traffic can reveal source of traffic
- Recall packet that appeared to have encrypted payload
- Lots of traffic to 1 IP address + statistical analysis of bytes + white papers [1] => this packet is a Sality C&C

RC4 Key                      Related packet length

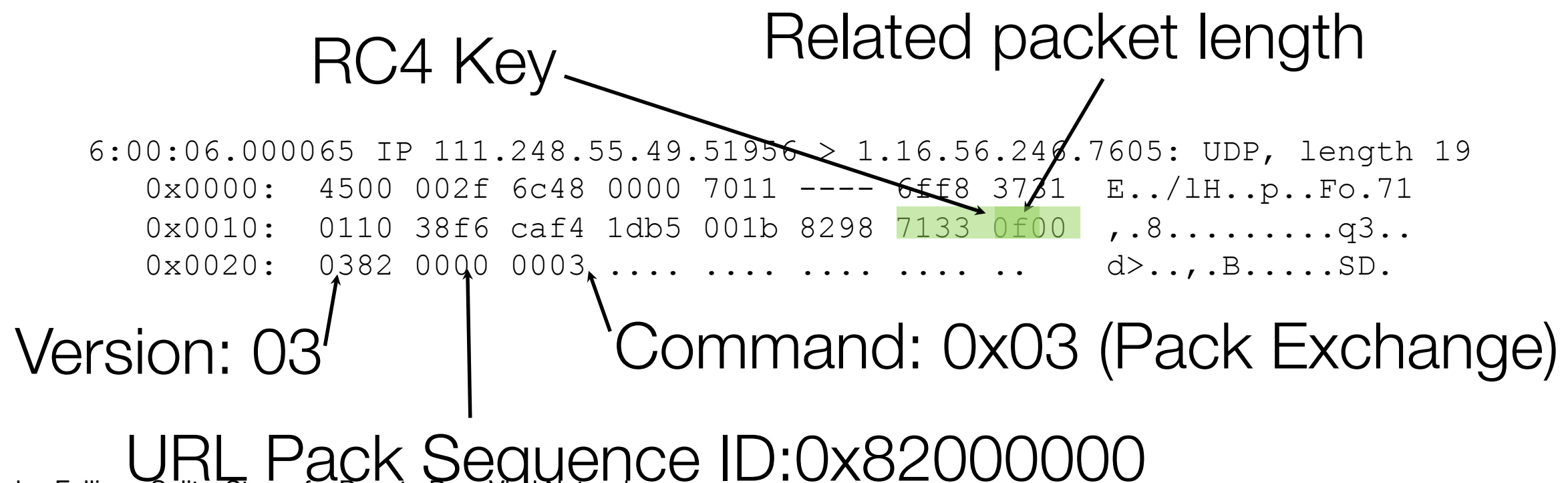


```
6:00:06.000065 IP 111.248.55.49.51956 > 1.16.56.246.7605: UDP, length 19
0x0000:  4500 002f 6c48 0000 7011 ---- 6ff8 3731  E../lH..p..Fo.71
0x0010:  0110 38f6 caf4 1db5 001b 8298 7133 0f00  ,.8.....q3..
0x0020:  643e c2d4 2cf5 42b5 810f 7f01 5344 1e    d>...,.B.....SD.
```

[1] Nicolas Falliere. Sality: Story of a Peer-to-Peer Viral Network.  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/sality\\_peer\\_to\\_peer\\_viral\\_network.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf), 2011.

# Making the unknown traffic known

- Further investigation into “unknown” traffic can reveal source of traffic
- Recall packet that appeared to have encrypted payload
- Lots of traffic to 1 IP address + statistical analysis of bytes + white papers [1] => this packet is a Sality C&C



[1] Nicolas Falliere. Sality: Story of a Peer-to-Peer Viral Network.  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/sality\\_peer\\_to\\_peer\\_viral\\_network.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf), 2011.



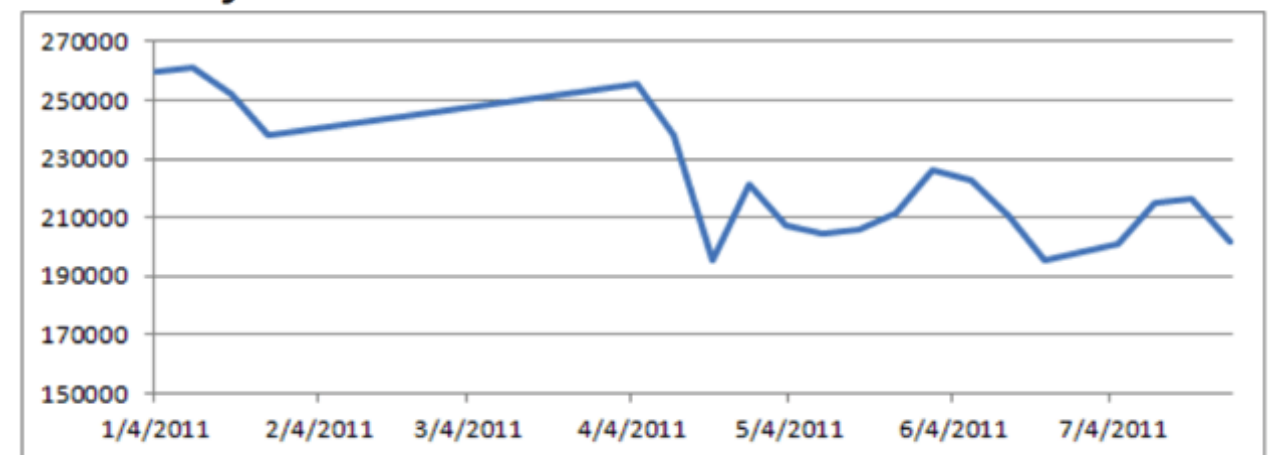
# Scale of misconfiguration

---

- Like BitTorrent, Sality can have bogus information in its hash table that results in many sources sending us packets
  - 34 days in 2012: 386k IPs
  - 34 days in 2013: 355k IPs
  - Symantec 2011:  
~300k infections

Figure 12

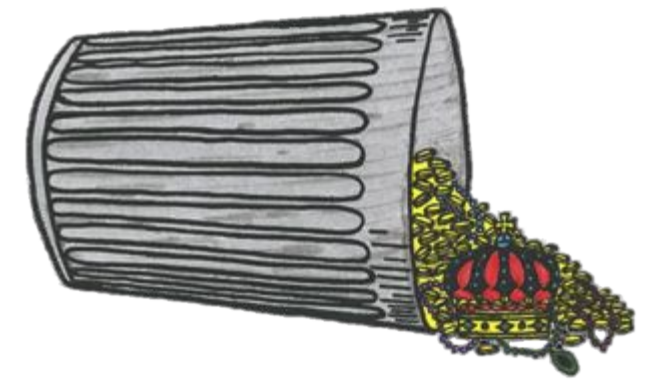
**W32.Sality.AE infection levels for 2011 to date**



[1] Nicolas Falliere. Sality: Story of a Peer-to-Peer Viral Network.  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/sality\\_peer\\_to\\_peer\\_viral\\_network.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf), 2011.

# Conclusion

---



- It's likely your machines transmit Internet background radiation
- Network telescopes capture a wealth of security-related data
  - Including somewhat complex attacks/bugs/misconfigurations
    - Scanning trends
    - Attacks on authoritative name servers
    - BitTorrent index poisoning
    - Qihoo 360 byte-order bug
    - Misconfigurations in Sality botnet