Bogon IP addresses

November, 2006
RoN Autumn 2006 Meeting,
SURFnet, Utrecht

Andree Toonk
Andree@sara.nl
Research and Engineering
SARA - High Performance Networking
Amsterdam, The Netherlands

Outline

- What is a Bogon?
- Purpose of this project
- Data sources
- Results

What is a Bogon?

- The use of an address or, more generally a route object, that is not authorized by the entity to which the address, or resource, was originally assigned to:

  - The resource has never been allocated (still in the IANA pool)
  - The resource has been hijacked
  - Incorrect use of special/reserved addresses (RFC 1918 / 3330)

  - Resource can be an IP address or an IP range
  - Resource can be an AS number

What is a Bogon?

- A few examples :
  - 108.8.180.1 (whois-info: IANA Reserved)
  - 0.66.154.180 (whois-info: IANA Special Use, Please see RFC 3330)
  - 248.4.49.192 (whois-info: IANA Special Use, Please see RFC 3330)
  - 94.39.203.54 (whois-info: IANA Reserved)

- A few examples of bogons in the global routing table (as seen from as1103):
  - 192.168.100.0/24 (whois-info: IANA Special Use, Please see RFC 1918)
  - 198.18.0.0/15 (whois-info: IANA Special Use, Please see RFC 2544)

Purpose of this project

- Try to get an understanding of bogon traffic in SURFnet6
- What kind of traffic is this?
- Why is it out there?
- Are there specific trends?
- What's the impact?

Data sources

- **Netflow data**

  • FLOW recv_time 2006-10-25T01:32:37.462073 proto 17 tcpflags 10 tos 00 agent [127.0.0.1] src [**37.119.130.130**]:30734 dst [x.x.x.x]:1026 packets 1 octets 533

- **IP routing tables**

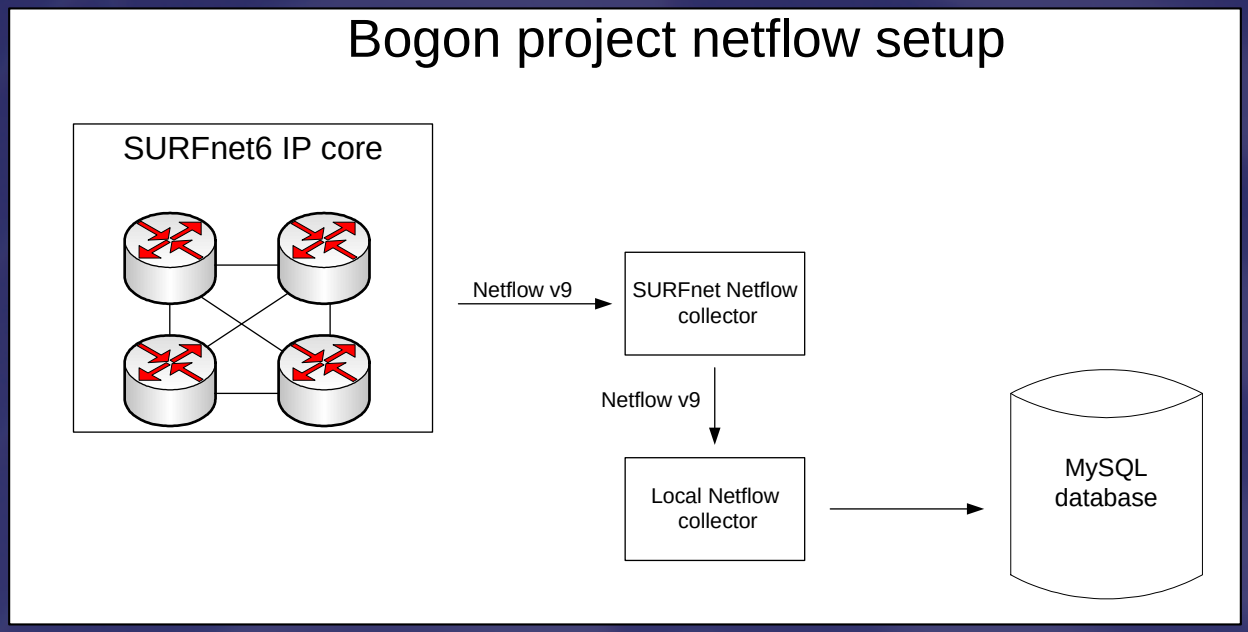
```
Asd001A-XSR03[Ford]#show ip route
<SNIP>
B      198.18.0.0/15          via 67.17.162.205 [d:20 m:2503]
                              and 208.49.125.49
                              and 208.49.224.21
```

- **Email**

  • Received: from craftsperson.conceptiongalen@anjungcafe.net ([**248.168.128.16**]) by iu6-f00.conceptiongalen@anjungcafe.net with Microsoft SMTPSVC(5.0.1397.2276)

Netflow data

- **Netflow setup:**

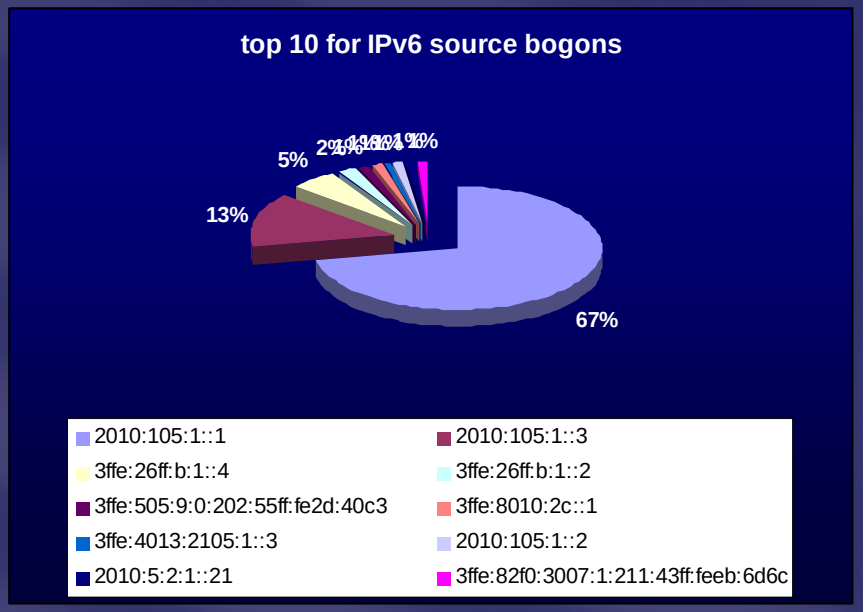


- **86.271.118 flows in the database**
  - **2869 IPv6 flows**

Data analysis

IPV6 SOURCE BOGONS:

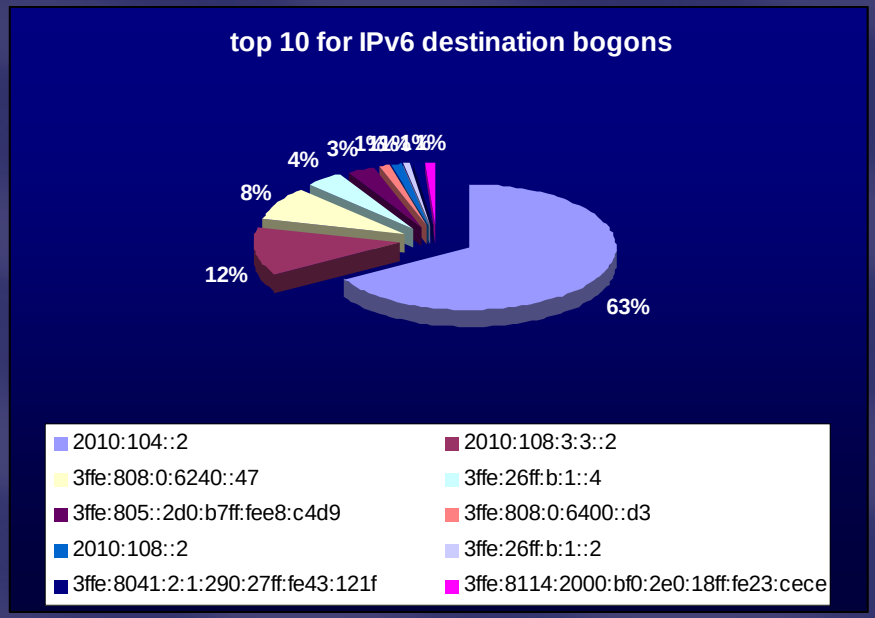
total inet6 src bogons	331	
2010:105:1::1	222	67%
2010:105:1::3	42	13%
3ffe:26ff:b:1::4	16	5%
3ffe:26ff:b:1::2	8	2%
3ffe:505:9:0:202:55ff:fe2d:40c3	4	1%
3ffe:8010:2c::1	4	1%
3ffe:4013:2105:1::3	4	1%
2010:105:1::2	4	1%
2010:5:2:1::21	3	1%
3ffe:82f0:3007:1:211:43ff:feeb:6d6c	3	1%



Data analysis

IPV6 DESTINATION BOGONS:

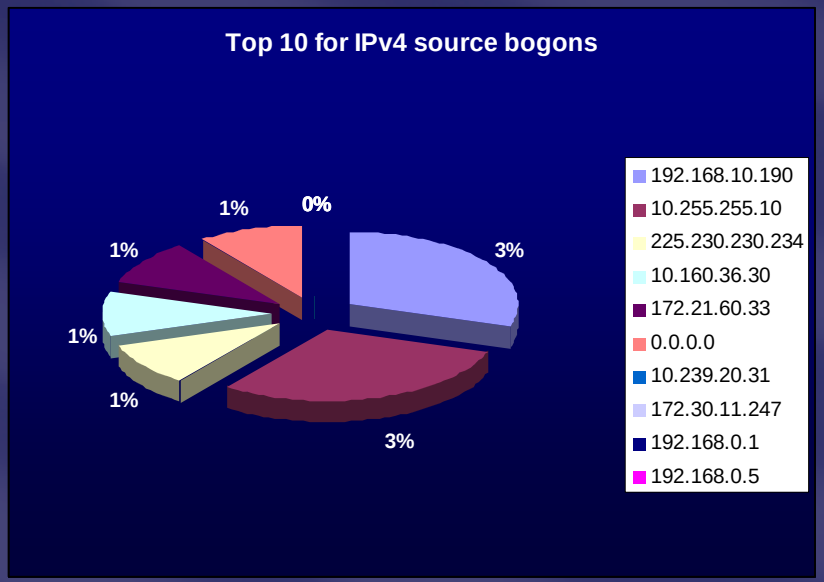
total inet6 dst bogons	354	
2010:104::2	222	63%
2010:108:3:3::2	42	12%
3ffe:808:0:6240::47	29	8%
3ffe:26ff:b:1::4	15	4%
3ffe:805::2d0:b7ff:fee8:c4d9	11	3%
3ffe:808:0:6400::d3	4	1%
2010:108::2	4	1%
3ffe:26ff:b:1::2	2	1%
3ffe:8041:2:1:290:27ff:fe43:121f	2	1%
3ffe:8114:2000:bf0:2e0:18ff:fe23:cece	2	1%



Data analysis

IPV4 SOURCE BOGONS:

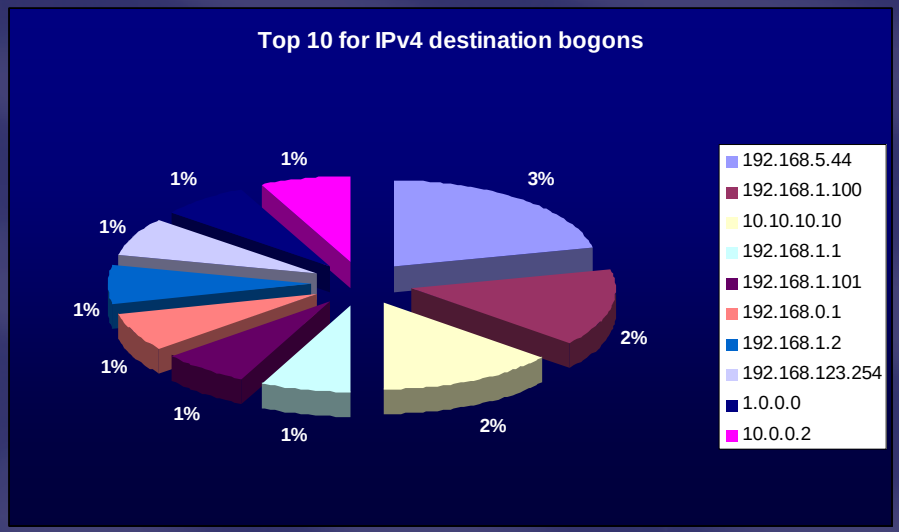
total inet4 src bogons	879346	
192.168.10.190	28496	3%
10.255.255.10	24742	3%
225.230.230.234	11283	1%
10.160.36.30	9303	1%
172.21.60.33	8935	1%
0.0.0.0	5629	1%
10.239.20.31	3453	0%
172.30.11.247	3436	0%
192.168.0.1	3436	0%
192.168.0.5	3189	0%



Data analysis

IPv4 destination bogons:

total inet4 dst bogons	8810639	
192.168.5.44	295952	3%
192.168.1.100	185604	2%
10.10.10.10	132595	2%
192.168.1.1	128589	1%
192.168.1.101	121880	1%
192.168.0.1	104168	1%
192.168.1.2	102536	1%
192.168.123.254	93804	1%
1.0.0.0	86757	1%
10.0.0.2	74964	1%



Data analysis

EXCLUDE RFC1918 SPACE

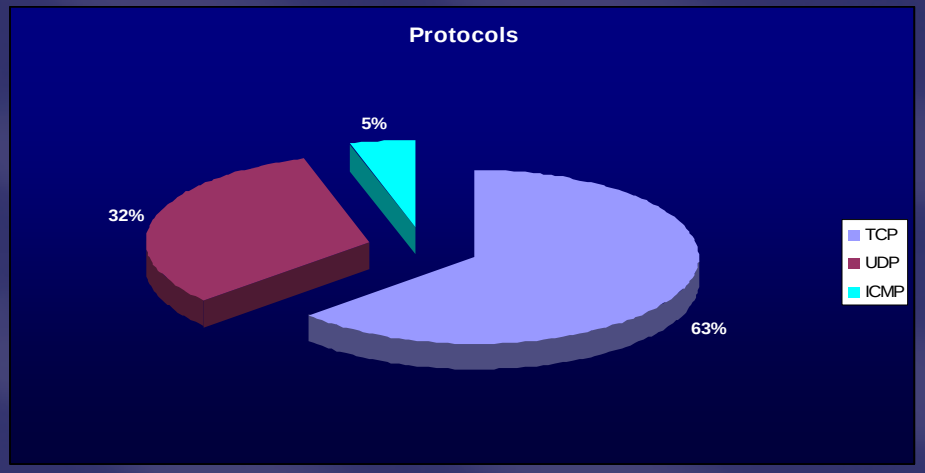
total inet4 source bogons	609983	
225.230.230.234	11283	1,8497%
0.0.0.0	5629	0.9221%
102.139.220.86	2532	0.4150%
103.98.49.43	2082	0.3413%
169.254.25.129	724	0.1186%
95.15.183.16	512	0.0839%
113.243.164.146	480	0.0786%
187.158.237.73	479	0.07852%
95.228.151.137	468	0.07672%
169.254.27.20	370	0.06065%

total inet4 destination bogons	4628675	
1.0.0.0	116469	2,5162%
1.1.1.2	65501	1,4151%
112.5.145.124	61854	1,3363%
1.1.1.1	58585	1,2656%
169.254.2.2	36909	0,7974%
234.5.6.7	32904	0,7109%
112.5.144.124	18576	0,4013%
39.123.0.0	17519	0,3785%
169.254.254.229	16962	0,3665%

Data analysis

Protocol analysis

protocol	count	Percentage (%)
TCP	15286587	63,31844
UDP	7698538	31,88805
ICMP	1151370	4,76908
IPv6 Hop-by-Hop	2958	0,01225
PIM	1342	0,00556
IPv6	994	0,00412
GRE	307	0,00127
ESP	256	0,00106
IPv6-ICMP	25	0,00010
RSVP	9	0,00004
IGMP	6	0,00002
OSPF	1	0,00000



Data analysis

Protocol analysis

- Protocol ‘0’ is IPv6 Hop-by-Hop Option [RFC1883]
- However, these are not Ipv6 addresses 

proto	srcip	dstip	count
0	IPv4 unicast address 1	108.122.0.0	2948
0	IPv4 unicast address 2	97.87.6.0	5
0	IPv4 unicast address 3	94.157.6.0	2
0	IPv4 unicast address 4	109.171.6.0	1
0	192.168.0.2	IPv4 unicast address 5	1

Data analysis

Protocol analysis

- Observed more interesting things:

1. Packets with protocol number 4 > IP in IP (encapsulation) [RFC2003]
   - However these had IPv6 addresses in the outer IP header, RFC explicitly says: Version 4

2 Multiple packets with protocol numbers that are not assigned yet:

Protocol: 201

Protocol: 207

Protocol: 242

Routing table analysis

Checked global routing tables for bogons:

- Checked on the SURFnet border routers
- Checked on route-views.routeviews.org

Result: there are always a few bogons in the routing table

Let's look at an example:

```
andree@kahn:~/projects$ perl bogon-routing-table.pl SN6routing-table-23-nov-ford.txt
0.0.0.0/0                                0.0.0.0/8
127.0.0.0/8                              127.0.0.0/8
192.168.100.0/24                         192.168.0.0/16
198.18.0.0/15                            198.18.0.0/15
number of prefixes =  203799
number of prefixes with bogon = 4
percentage of prefixes with bogon = 0.002%
```

Routing table analysis

Closer look at: 192.168.100.0/24

```
BOFH:~# fping -g 192.168.100.0/24
192.168.100.1 is alive
192.168.100.2 is alive
```

```
•BOFH:~# traceroute-nanog -A -I icmp -n 192.168.100.1
•traceroute to 192.168.100.1 (192.168.100.1), 64 hops max, 28 byte packets
• 1  145.89.193.250 [AS1103]  0 ms  0 ms  0 ms
• 2  145.89.1.41 [AS1103]  1 ms  1 ms  1 ms
• 3  145.145.16.5 [AS1103]  2 ms  2 ms  3 ms
• 4  145.145.80.10 [AS1103]  2 ms  2 ms  3 ms
• 5  195.69.144.94 [AS1200]  2 ms  2 ms  2 ms
• 6  63.223.28.161 [AS19151]  91 ms  91 ms  91 ms
• 7  63.223.28.201 [AS19151]  91 ms  91 ms  91 ms
• 8  63.223.28.141 [AS19151]  94 ms  94 ms  95 ms
• 9  63.223.0.65 [AS19151]  123 ms  121 ms  124 ms
•10  63.223.20.53 [AS19151]  173 ms  173 ms  173 ms
•11  66.186.192.94 [AS19654]  173 ms  173 ms  174 ms
•12  63.223.30.134 [AS19151]  165 ms  165 ms  165 ms
•13  192.168.100.1 [<NONE>]  165 ms  165 ms  165 ms
```

Email analysis

- Idea: Bogons and spammers…
  1. Advertise a bogon prefix with BGP
  2. Send spam email
  3. Withdraw prefix

Result: Difficult to find the spammer afterwards.

The Question is:

"is this really happening..?"

- The Answer is:

minimal proof found in the netflow data.

Email analysis

- Found exactly 12 flows in the 86 million flows.
- Source IP is bogon, destination TCP port 25
- These flows had only rst or syn flags set

- However, these packets should not be seen.

Email analysis

- Scan “received from” lines in email headers for bogon IP addresses
  1. Spam
  2. Non spam

	Non spam email	*Spam email*
total email scanned	31502	53195
emails with bogon	7	2438
email with bogon %	0,02%	4,5%
total bogons	7	2762

*** non spam email = Not marked as spam by mailserver. In this case email from NANOG and IETF mailing lists**

**** Spam email = email marked as spam by mail server (SpamAssassin)**

•Although the headers might be forged it’s an indication that this is spam mail.

Email analysis

- A SpamAssassin plugin has been written
  - Authors:
    - Bas Toonk (bas@toonk.nl)
    - Andree Toonk (andree@sara.nl)
- Will check email headers for bogon IP addresses

```
Received: from smtp.spam.nl ([198.18.0.26]) by localserver with
Microsoft SMTPSVC(6.0.3790.1830); Wed, 22 Nov 2006 16:45:03 +0100
```

<snip>

```
X-Virus-Scanned: by amavisd-new-20030616-p10 at toonk.nl
X-Spam-Status: No, hits=1.8 tagged_above=1.0 required=3.0 tests=AWL,
BAYES_05, BOGONRECEIVEDLINE, HTML_50_60, HTML_MESSAGE
X-Spam-Level: *
```

Some conclusions (1)

- In the netflow data we found a lot of flows with Bogon addresses.
- Majority is RFC1918 (private space) addresses.
- For IPv6 a lot of 6bone (3ffe::)
- Lot of traffic (scans) towards ‘notorious’ Windows services (1025,1026,1027, 135/139)
- Some flows were identified as configuration errors.
- some flows were identified as DOS attacks (spoofed bogon source address)
- Weird things, such as:
  - Traffic to TCP and UDP port 0
  - Protocol numbers that do not exist
  - Protocol number and Inet family mismatch

Some conclusions (2)

- Bogons were found in routing table.
  - On purpose or configuration error?
  - Typically between 1 and 5 bogons in the routing table
- 5% of the SPAM mail has a bogon address in header
- 0,02% of non SPAM mail has a bogon header
  - SpamAssassin plugin will be available soon
- A few flows to TCP port 25 (smtp) had bogon source address
  - Spammer?

Questions

- Report will soon be available on:
  http://nrg.sara.nl/

  Email: nrg@sara.nl

Questions?