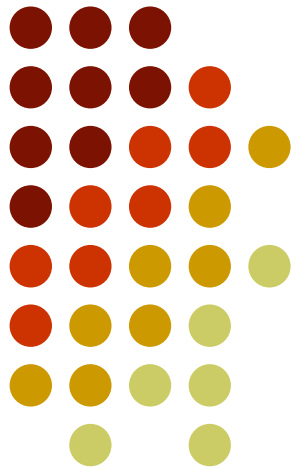
Automated Bogon Filtering

Dave Deitrich

Team Cymru Inc.
team-cymru@cymru.com



ARIN XVII - 10 April 2006

What's a Bogon?

- A BOGON is a prefix that should never appear in the Internet routing table
- Different types of bogons
  - MARTIANS - private (RFC 1918) and reserved (RFC 3330) addresses
  - UNALLOCATED - address space that has not yet been assigned to an RIR by IANA

http://www.iana.org/assignments/ipv4-address-space

Why Filter Bogons?

- Prevent private address space in your network from leaking out into the Internet
- Sometimes used in Spam and DDoS
  - In 2001 roughly 60% of attacks came from bogon source addresses (1)
  - In Jan 2005 during one DDoS attack 12% of incoming traffic was sourced from bogons

(1) http://www.cymru.com/Presentations/60Days.ppt

Why Filter Bogons?

- Bogons seen in the past 30 days
  - 87 distinct prefixes
  - Ranged in size from /32 to /13
  - 6 prefixes seen on >25 peers

Netblock	Src ASN	First Seen	Last Seen	Duration
183.206.196.0/24	2188	3/25/06 12:41	Still Present	2w 1d 14h
2.0.0.0/24	15967	3/29/06 13:12	3/29/06 13:27	14m
1.1.1.0/24	8764	3/28/06 14:16	3/29/06 5:06	14h 49m
1.1.1.0/24	1257	3/23/06 10:06	3/23/06 10:41	35m
101.76.76.0/24	8764	3/20/06 8:06	3/20/06 8:16	10m
42.138.81.0/24	7908	3/7/06 21:06	3/7/06 21:41	35m

Perils of Bogon Filtering

- Bogon filters regularly need to be updated
  - Unallocated space eventually gets allocated

January 2006	121/8 thru 123/8 allocated to APNIC
June 2005	89/8 thru 91/8 allocated to RIPE
June 2005	74/8 thru 76/8 allocated to ARIN
June 2005	189/8 and 190/8 allocated to LACNIC
April 2005	41/8 allocated to AfriNIC
Mar 2005	73/8 allocated to ARIN
January 2005	124/8 thru 126/8 allocated to APNIC
April 2003	223/8 DE-ALLOCATED from APNIC

Perils of Bogon Filtering

- Actual email received by Team Cymru on December 2nd, 2004:

```
I am the Director of Network Services at
[University]. We just changed our ISP and
in the change received a new set of IP
numbers (70.[xxx.xxx.xxx]/25). In the
first three days we were on the new IP
range, we encountered 6 places that seem
to be using your "bogon" list and have not
updated it since 70/8 was taken off in
January of this year.
```

Perils of Bogon Filtering

- Martians occasionally change as well
  - RFC 3068: 192.88.99.0/24 allocated for use by 6to4 relays (June 01)
- For best results use an automated method to keep your bogon filters up-to-date
- Know your network! Don’t block “bogons” by accident!
  - Example: Internal SMTP Relays

Perils of Bogon Filtering

```
Delivered-To: person@example.org
Received: by server.example.org (Postfix, from userid 123456)
     id 741C32442; Wed,  7 Sep 2005 08:24:55 -0500 (CDT)
Received: from relay.example.org (64.1.1.1)
     by server.example.org (Postfix) with ESMTP id B37CE243F
     for <person@server.example.org>; Wed,  7 Sep 2005 08:24:51 -
     0500 (CDT)
Received: from smtp.some.site (70.1.1.1)
     by relay.example.org (Postfix) with ESMTP id 5648EC916
     for <person@example.org>; Wed,  7 Sep 2005 08:24:51 -0500
     (CDT)
Received: from workstation.some.site (192.0.2.1) by
     smtp.some.site (Sendmail)
     id 42F22E990020F370; Wed, 7 Sep 2005 15:24:49 +0200
```

Bogon Route Server Project

- Advertises bogon prefixes via eBGP
- Peers configure routers to automatically filter bogons based on prefixes received
- BGP advertisements are updated as netblocks become bogon/non-bogon
  - Filtering updates are automatic!

http://www.cymru.com/BGP/bogon-rs.html

Bogon Route Server Project

- Currently 16 route servers online
  - 6 in ARIN, 7 in RIPE, 2 in APNIC, 1 in AfriNIC
- 866 peering sessions across 374 ASNs
- All route servers use Secure IOS and BGP templates for configs
  - http://www.cymru.com/Documents

IOS Config Example

```
ip bgp-community new-format
!
ip route 192.0.2.1 255.255.255.255 null0
!
ip community-list 10 permit 65333:888
!
route-map CYMRUBOGONS permit 10
  match community 10
  set ip next-hop 192.0.2.1
```

JunOS Config Example

```
routing-options {
    static {
        route 192.0.2.1/32 {
            discard; no-readvertise; retain;
        }}}

policy-options {
    community CYMRU-bogon-community members
       [ no-export 65333:888 ];
    as-path CYMRU-private-asn 65333;
```

JunOS Config Example (Cont)

```
policy-statement CYMRU-bogons-in {
    term 1 {
        from {
            protocol bgp;
            as-path CYMRU-private-asn;
            community CYMRU-bogon-community;
        } then {
            next-hop 192.0.2.1;
            accept;
        }}
     then reject; }
```

More Config Examples

- Examples for Cisco IOS, Juniper JunOS and OpenBGP are available at: http://www.cymru.com/BGP/bogon-rs.html

- Use prefix lists to block announcements of bogons that you use internally

- Use Unicast RPF to block bogon traffic at ingress points

Other Methods

- Bogon lists are also available as:
  - Text lists (aggregated & unaggregated)
  - Prefix Lists (Juniper/Cisco)
  - BIND Templates
  - RADB, RIPE NCC, DNS
  - Mailing list for change announcements

- For more info visit http://www.cymru.com/Bogons/

Useful Links

http://www.iana.org/assignments/ipv4-address-space

http://www.cymru.com/Bogons/

http://www.completewhois.com/bogons/

http://www.sixxs.net/tools/grh/bogons/

http://www.cidr-report.org/#Bogons

Useful Links

ftp://ftp-eng.cisco.com/cons/isp/security/

- Remote-Triggered-Black-Hole-Filtering-02.pdf
- URPF-ISP.pdf
- Ingress-Prefix-Filter-Templates

http://www.cymru.com/gillsr/documents/

- junos-isp-prefix-filter-loose.htm
- junos-isp-prefix-filter-strict.htm

http://www.cymru.com/BGP/bogon-rs.html

THANK YOU!

If you have any comments or questions please feel free to contact us at:

team-cymru@cymru.com

http://www.cymru.com