Measuring and reporting on unauthorized use of IPv4 address space

APNIC 31, Hong Kong
February 2011
Agenda

• There’s a problem
• Investigate
• Investigate more
• Share the results
• And now...
We were told about ‘hijackings’

Over five years ago we were told about the Hamachi/Logmein service using 5.0.0.0/8 without authorization.

5.0.0.0/8 was allocated to RIPE NCC in November 2010.
Poorly designed config defaults

Many commercial WiFi hotspots use 1.1.1.1. Users can only access the Internet after visiting a portal and registering or paying.
We researched other prefixes that had been used without authorization and published our findings in IPJ.

We were asked for more specifics. Data not anecdotes.

http://cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/
We had an idea...

We decided to look for DNS queries for unallocated IPv4 addresses.

We knew that this research would only find evidence of usage on poorly managed networks. Well managed networks would not leak these queries.

Let’s remove the allocated /8s and look at the mean QPS last Thursday 10 January.
Then we sponsored research

Duane Wessels (CAIDA/TMF) used DITL data to do a more thorough study which looked at the queries in more detail.

He identified which parts of /8s saw most activity as well as which /8s the activity was in.

But nothing’s unallocated now

The central pool of IPv4 address space is now fully allocated. It is time for any ‘bogon’ filters for previously unallocated /8s to be removed.

All we are left with is the ‘martian’ filters for address space reserved by various RFCs.

http://tools.ietf.org/id/draft-vegoda-no-more-unallocated-slash8s-00.txt
But nothing’s unallocated now

The central pool of IPv4 address space is now fully allocated. It is time for any ‘bogon’ filters for previously unallocated /8s to be removed.

All we are left with is the ‘martian’ filters for address space reserved by various RFCs.
Thank you