IPv6 Background

Radiation

Geoff Huston

APNIC R&D
IPv4 Background Radiation

• We understand that the IPv4 address space is now heavily polluted with toxic background traffic
  – Most of this traffic is directly attributable to infected hosts performing address and port scanning over the entire IPv4 address range
  – Average background traffic level in IPv4 is ~5.5Gbps across the Internet, or around 300 – 600 bps per /24, or an average of 1 packet every 2 seconds
    – There is a “heavy tail” to this distribution, with some /24s attracting well in excess of 1Mbps of continuous traffic
    – The “hottest” point in the IPv4 network is 1.1.1.0/24. This prefix attracts some 100Mbps as a constant incoming traffic load
IPv4 vs IPv6

• Darknets in IPv4 have been the subject of numerous studies for many years
• What about IPv6?
• Does IPv6 glow in the dark with toxic radiation yet?
2400::/12

Allocated to APNIC on 3 October 2006

Currently 2400::/12 has:

- 709 address allocations, spanning a total of:
  - 16,629 /32’s
  - 71,463,960,838,144 /64’s
  - 1.59% of the total block

- 323 route advertisements, spanning a total of:
  - 9,584 /32’s
  - 41,164,971,903,233 /64’s
  - 0.91% of the /12 block

- 0.91% of the block is covered by existing more specific advertisements
- 0.68% of the block is unadvertised allocated address space
- 98.41% of the block is unadvertised and unallocated
Advertising 2400::/12

Darknet experiment performed between 19\textsuperscript{th} June 2010 – 27\textsuperscript{th} June 2010

– Advertised by AS7575 (AARNet)

– Passive data collection (no responses generated by the measurement equipment)
Total Traffic Profile

Traffic Log for 2400::1/12 (KBps)

- Peak Rate = 3.5Mbps
- Average Traffic Rate = 407Kbps

ICMP, UDP, TCP, and Total Traffic Graphs over 24 Hours.
Traffic Profile

Average Traffic Rate: 407 Kbps (726 packets per second)
  ICMP: 323 Kbps (611 pps)
  UDP: 54 Kbps (68 pps)
  TCP: 30 Kbps (45 pps)

This is predominately ICMP traffic (destination unreachables being sent to dud addresses – i.e. a double misconfig of both source AND destination).
Destination Address Distribution
Destination Address Distribution

Traffic Distribution in 2400 /12 per /20

Average bps (log scale)

AVG Load
PEAK Minute Load
Top 5 /20s in 2400::/12

<table>
<thead>
<tr>
<th>IP Block</th>
<th>Bandwidth</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2408:0000::/20</td>
<td>197Kbps</td>
<td>Allocated: 2408::/22 – NTT East, JP</td>
</tr>
<tr>
<td>2401:d000::/20</td>
<td>7Kbps</td>
<td>8 x /32 allocations in this block</td>
</tr>
<tr>
<td>2403:8000::/20</td>
<td>4Kbps</td>
<td>4 x /32 allocations in this block</td>
</tr>
<tr>
<td>2404:0000::/20</td>
<td>1Kbps</td>
<td>29 allocations in this block</td>
</tr>
<tr>
<td>2405:b000::/20</td>
<td>0.3Kbps</td>
<td>4 x /32 allocations in this block</td>
</tr>
</tbody>
</table>
Is This Leakage or Probing?

- There is no direct equivalent of RFC1918 private use addresses in IPv6
  
  (well, there are ULAs, but they are slightly different!)
- In IPv6 it’s conventional to use public IPv6 addresses in private contexts
  
  How much of this “dark” IPv6 traffic is a result of “leakage” from private contexts into the public network?
  
  Filter the captured packets using the address allocation data
Allocated vs Unallocated Dark Traffic

Leaked IPv6 traffic

Dark IPv6 Traffic

Traffic Profile for 2400:7/12

Time

Kbps
Dark IPv6 Traffic

Yes, that’s a pattern of 16 UDP packets per second every 24 hours for 5 seconds.

less than 1 packet per second of ICMP
Dark IPv6 Traffic Profile

Average Packet Rate:
1 packet per 36.8 seconds for the entire /12

Packet Count: 21,166

ICMP: 7881 (37%)
TCP: 7660 (36%)
UDP: 5609 (26%)
TCP Profile

SYN packets: (possibly probe / scanning traffic)
  1126

SYN+ACK packets: (wrong source, local config errors?)
  6392

Others (Data packets!):
  141
TCP Oddities

Stateless TCP in the DNS?
(no opening handshake visible in the data collection – just the TCP response data!)

DNS TCP Response:
04:47:06.962808 IP6 (hlim 51, next-header TCP (6) payload length: 1351)
Response: finlin.wharton.upenn.edu. A 128.91.91.59
TCP Probing?

Repeated TCP packets, same source addresses and ports, no preceding SYN/ACK TCP handshake, different addresses addresses, small dest port set (1158, 3113, 2273)
TCP Probing, or...?

Same Teredo source address, but varying destination addresses
A mail server at he.net is (correctly) responding to a mail client at the (invalid) address 2402:5000::250:56ff:feb0:11aa. There are sequences of 8 packets paced over ~90 seconds with doubling intervals – typical signature of a SYN handshake failure.

This single address pair generated a total of 6,284 packets over 9 days (corresponding to 780 sendmail attempts!)
Dark DNS

Queries: 2,892 queries over 7 days from just 4 source addresses!
Backscattered Responses: 30

All of these look a lot like configuration errors in dual stack environments. These errors go largely unnoticed because of the fallback to V4 in dual stack.
Dark ICMP

- echo request packets (ping) – 7,802 packets
- 93 others – destination unreachable, and malformed packet headers
IPv6 Dark Traffic

• Most of the traffic in the dark space is leakage from private use contexts
  – There is a message here to all “private” networks: they really aren’t necessarily all that private!

• And a we’ve seen a small amount of traffic that appears to be a result of poor transcription of IPv6 addresses into system configs and into DNS zone files

• And the use of dual stack makes most of these IPv6 config stuffups go completely unnoticed!
IPv6 Scanning?

• What happens in IPv4 does not translate into IPv6.
• There is no visible evidence of virus scanners attempting to probe into private use and dark address blocks in IPv6.
• The nature of IPv6 is such that address scanning as a means of virus propagation is highly impractical.
  – That does not mean that IPv6 is magically “secure” – far from it – it just means that virus propagation via address scanning does not translate from IPv4 into IPv6.
Thank You