Open resolvers

IEPG Meeting July 2007

John Kristoff
jtk@ultradns.net
Rodney Joffe
rodney.joffe@neustar.com

Open DNS resolvers

- Well known threat for a long time
- Very public DNS amp/reflection attacks in 2006
- In one attack we saw ~52,000 sources
- These were open resolvers, many home nat/proxies
- Attack traffic aggregate was measured in Gb/s
- A few weeks ago, more than 40% were still open
- What is the entire Internet resolver population?

Open resolver studies

- Duane Wessels has performed a sample
- Dan Kaminsky has done an all-Internet probe
- We did an all-Internet probe
  - And are doing continuous monitoring/analysis

The numbers

- We have sent at least one A query to 2,884,370,176 addresses at least once
- We have seen 16,696,502 unique addresses test as open resolvers
- At any one instant, about half of those are active
- Most of them are forwarders
- We have seen only 853,935 unique addresses query our authoritative server
- We've had about 6 email inquires on the probes

Who are the forwarders?

Configuration defaults

Vigor 2600 Highlights

- Built-in ADSL modem - plugs directly into your ADSL-enabled line
- Universal Plug'n'Play (uPnP) Support
- Comprehensive Firewall - with keepstate facility, DoS/DDoS protection, IP anti-spoofing and user-configurable packet-filtering.
- Built-in native VPN facility with PPTP, L2TP, 3DES IPSec and MPPE encryption
- NAT Port redirection, forwarding and DMZ
- Multi-NAT facility - enables a one-to-one mapping of public to private IP addresses, with individual DMZ and port-formwarding.
- LAN-to-LAN linking via ISDN or VPN
- VPN routing for multiple remote private subnets (between two Vigors)
- VPN Passthrough for VPN client/server running behind the router
- 4-Port 10/100BaseT Ethernet Switch (with automatic uplink detection) for PC/Mac connection
- NAT port forwarding (For individual ports, ranges and DMZ)
- Support for non-NAT public subnets (multiple public IP addresses)
- WAN-Side IP address is selectable from all available addresses
- LAN Side IP address range fully configurable
- SNMP & Syslog control/logging/monitoring
- Dynamic DNS Posting, compatible with popular services
- Easy configuration, monitoring & control from web-interface
- Wireless Access Point (802.11b Ethernet) for wireless LAN (Vigor 2600We/W only)
- DNS Proxy/Cache & DHCP Server (with ability to fix allocations)
- ISDN Interface for dial-up access and ISP backup for ADSL (Vigor2600W/X only)

A BCP won't change this

- Some routed netblocks are full of them
  - e.g. 62261 unique addrs from one /16 alone
- Over 16,000 unique ASNs represented
- Over 100,000 unique routed netblocks represented
- Work in DNS-OARC continuing to analyze further
- IETF to help pressure vendors for saner defaults?