DVMRP Ask Neighbors2: an IGMP-based DDoS/leak threat

John Kristoff
jtk@cymru.com
Internet Group Multicast Protocol (IGMP)

- End hosts signal interest in a group
- Routers (and often switches) maintain membership
- No real reason for IGMP to leave local subnet
Distance Vector Multicast Routing Protocol (DVMRP)

- Long obsolete IP multicast routing protocol
- Runs (ran) over IGMP
- Details relatively unimportant for our purposes
- Never got out of experimental (v1) or draft (v3)
- v3 draft added “tracing and troubleshooting” messages
  - Ask Neighbors2 – yay, a use for forwarding IGMP?
  - implemented in mrinfo (see the mrouted package)
  - widely implemented by Cisco & Juniper
Ask Neighbors2

“[...] a unicast request packet directed at a DVMRP router. The destination should respond with a unicast Neighbors2 message back to the sender of the Ask Neighbors2 message”

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0x13)</td>
<td>(0x5)</td>
<td></td>
</tr>
</tbody>
</table>

+-------------------+----------+---------+
| Reserved           | Minor    | Major   |
|                    | Version  | Version |

0         8          16              31
Neighbors2 Response

• “[...] a common header at the top followed by the routers capabilities. One or more sections follow that contain an entry for each logical interface. The interface parameters are listed along with a variable list of neighbors learned on each interface.”
# Neighbors2 Response

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>(0x13)</td>
</tr>
<tr>
<td>Code</td>
<td>(0x6)</td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Capabilities</td>
<td>Minor</td>
</tr>
<tr>
<td>Version</td>
<td>Major</td>
</tr>
<tr>
<td>Local Addr</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td></td>
</tr>
<tr>
<td>Threshold</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td></td>
</tr>
<tr>
<td>Nbr Count</td>
<td></td>
</tr>
<tr>
<td>Nbr</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Nbr m</td>
<td></td>
</tr>
<tr>
<td>Local Addr</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

The Neighbors2 Response is a protocol used for neighbor discovery. The response message contains information about neighbors, including their local addresses, metrics, thresholds, flags, and neighbor counts. The structure of the response includes fields for the type, code, and checksum, followed by fields for reserved, capabilities, minor and major versions, and local addresses. Each neighbor is represented by a series of fields including metric, threshold, flags, and neighbor count.
Notes on Ask Neighbors2

• Some responses can be very large (long interface list)
  • Cisco will send multiple 576 byte responses
  • Note: there is no sequence ID, can't guarantee order
  • Juniper will perform IP fragmentation
• Spec says put 0x3, 0xff in the major/minor version fields
  • Cisco fills these with their IOS major/minor version
The Bad News

- DVMRP doesn't need to be activated
  - e.g. Cisco "ip pim sparse mode" on any interface
  - e.g. Juniper "protocols { igmp; }" globally
  - many publicly accessible routers in this state
- The response packets can be big and numerous
- The content of the responses can be interesting
  - e.g. interface list and neighbor addresses
  - e.g. IOS major/minor version (in Cisco responses)
- IGMP responses are not rate limited like ICMP
The Good News

• Relatively easy to mitigate
• Some networks/gear will not forward IGMP messages
• Vendors removing associated code in future releases
• No IGMP in IPv6, at least none of this legacy stuff there
• Doesn't appear to be “millions” of potential reflectors
Pretty Picture (well kinda)
28 bytes $\rightarrow$ 340 bytes (common)
How Much Packet Potential?

- Work in progress
- Accurate numbers require anti-aliasing analysis
- Approximately 3-5% Internet routers seem to respond
  - I've not scanned all of IPv4, but from a “router set”
    - I've seen approximately 20,000 – 25,000 routers
  - I've seen some routers send **thousands** of responses
    - Appears to be just a rare bug or configuration oddity
    - 2,235,623:1 packet amplification anyone?
Cisco Mitigation

• See:

http://www.cisco.com/web/about/security/intelligence/multicast_toolkit.html#20

ip multicast mrinfo-filter 52
access-list 52 deny any
Juniper Mitigation

```plaintext
filter igmp {
    term igmp_accept {
        from {
            destination-address {
                224.0.0.0/4;
            }
            protocol igmp;
        }
        then accept;
    }
    term igmp_drop {
        from {
            protocol igmp;
        }
        then {
            discard;
        }
    }
}
```
What Else is Happening?

• Kudos to Cisco PSIRT and Juniper SIRT!
  • Ask Neighbors2 functionality being removed
  • Vendor bulletins should be published around now
  • NOTE: there is intentionally no CVE for this
• Conducting research with ICSI (Vern Paxson's group)
• Limited heads up given to nsp-security / REN-ISAC
• And not happening: ongoing data feed of AN2 routers
  • Our infrastructure will not transit IGMP probes :-(/
References

- Internet Group Multicast Protocol (IGMP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- This slide deck and a blog post
  https://www.cymru.com/jtk/blog/2014/10/06#an2