Tracking Address Spoofing Through Triangulation

John Kristoff  jtk@cymru.com
Reflection / Amplification

Question: What is π?

Answer:
3.1415926535897932384
62643383279502884197
16939937510582097494
45923078164062862089
98628034825342117067
98214808651328230664
7093844609550582231...
Spoofed Packet DoS Observations

• Anti-spoofing is about as deployed as it will get
• Not all source address spoofing can be prevented
• Current Internet is ill designed to eliminate spoofing
• Spoofed DoS origination highly concentrated
• Victim nets ill equipped to withstand spoof attacks
• Attack originating network often lacks white hat(s)
• Intermediate nets caught in the uninspired middle
Current, Popular Spoofed Packet DoS Threat Vectors

- DNS amplification / reflection
- SNMP
- NTP
- chargen
- RIP
- COD (Call of Duty server)
Motivations

• Many victims are game servers or other gamers
• Variety of server ops also targeted
• Most traffic originates from hosting providers
• We see some recon scanning from there too
Traditional Mitigation

- Filters
- Increased capacity
- Source address validation
- Rate limits
- Path pruning and isolation
- Service distribution and replication (e.g. anycast)
- Protocol / Application protections (e.g. DNS RRL)
- Law enforcement
Getting Aggressive with Enablers

• De-peering
• Financial incentives
• Route Poisoning
• TCP-only filters
• Outreach campaign / public shaming / SpoofBL
Total BGP Table Growth

From NANOG 27, February 2003
Spoof Detection and Monitoring

- Spoofer project [http://spoofer.cmand.org](http://spoofer.cmand.org)
- Jared Mauch's openresolver tests?
- Possible future DRG Distro module
TTL Sonar

IP y, TTL = 128
IP x, TTL = 255
IP z, TTL = 64

Varying Number of Router Hops

IP x, TTL - x₁
IP y, TTL - y₁
IP z, TTL - z₁
http://www.cymru.com/jtk/code/ttlmon.pl

```
$ sudo ./ttlmon.pl
2013-08-30 18:31:21 |  64 | 192.0.2.2/32
2013-08-30 18:31:21 |  64 | 192.0.2.3/32
2013-08-30 18:31:21 |   1 | 192.0.2.1/32
[...]
2013-08-30 18:35:19 |  51 | 198.51.100.1/32
2013-08-30 18:35:19 |  49 | 198.51.100.1/32
2013-08-30 18:35:19 |  53 | 198.51.100.1/32
[...]
2013-08-30 18:42:08 | 115 | 192.0.2.4/32
2013-08-30 18:42:08 | 115 | 198.51.100.5/32
2013-08-30 18:42:08 | 115 | 203.0.113.6/32
```
TTL Sonar Use Cases

• Real-time path change detection
• Early warning spoofing detector
• Fun anomaly detection?

```sql
select distinct ttl from ttlmon where \prefix = '8.8.8.0/24';
```

<table>
<thead>
<tr>
<th>ttl</th>
<th>datasrc</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>AS 23028</td>
</tr>
<tr>
<td>17</td>
<td>AS 23028</td>
</tr>
<tr>
<td>54</td>
<td>AS 23028</td>
</tr>
<tr>
<td>45</td>
<td>AS 23028</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
Regional Route Steering

- Proposition: Get targets close to the source
- Goal: Keep friends close, enemies closer
- Gather hard evidence on suspect network
- Build justification for action
For More Information

jtk@cymru.com
PGP key 0xFFE85F5D
http://www.cymru.com/jtk/