Community tools to fight against DDoS

Fakrul Alam
Senior Training Officer

SANOG 27 & APNIC Regional Meeting, Kathmandu, Nepal
25 Jan - 01 Feb, 2016
DDoS

- Denial of Service (DoS) / Distributed Denial of Service (DDoS) is the act of
  - performing an attack which prevents the system from providing services to legitimate users
- Denial of Service attacks take many forms, and utilize many attack vectors
- Used to cover up other attack vectors
Types of Attacks

- Volume Based Attacks
- Application Layer Attacks

http://thehackernews.com/2016/01/biggest-ddos-attack.html
Addressing DDoS attacks

• Preparation
  – Deploy necessary tools and grab list

• Detection
  – Detect incoming fake requests

• Mitigation
  – Diversion: Send traffic to a specialized device that removes the fake packets from the traffic stream while retaining the legitimate packets
  – Return: Send back the clean traffic to the server
3 Community tools

• Bogon Filter

• Flow Sonar
  – https://www.team-cymru.org/Flow-Sonar.html

• UTRS (Unwanted Traffic Removal Service)
1. Bogon Filter
A bogon prefix is a route that should never appear in the Internet routing table

- Bogons are defined as Martians (private and reserved addresses defined by RFC 1918, RFC 5735, and RFC 6598) and netblocks that have not been allocated to a RIR by the IANA

These are commonly found as the source addresses of DDoS attacks

Study shows 60% of the naughty packets were obvious bogons

Bogon and fullbogon lists are NOT static lists
Bogon Filter: Configuration IPv4

```
router bgp 17821
  neighbor 38.229.xxx.xxx remote-as 65332
  neighbor 38.229.xxx.xxx description CYMRUBOGONS
  neighbor 38.229.xxx.xxx ebgp-multihop 255
  neighbor 38.229.xxx.xxx password 7 070C134D575F0A5116
  neighbor 38.229.xxx.xxx update-source Loopback0

  address-family ipv4
    neighbor 38.229.xxx.xxx activate
    neighbor 38.229.xxx.xxx soft-reconfiguration inbound
    neighbor 38.229.xxx.xxx prefix-list CYMRU-OUT-V4 out
    neighbor 38.229.xxx.xxx route-map CYMRUBOGONS-V4 in

! configure community list to accept the bogon prefixes into the route-map
ip community-list 100 permit 65332:17821

! configure route-map. Remember to apply it to the proper peering sessions.
route-map CYMRUBOGONS-V4 permit 10
  description IPv4 Filter bogons learned from cymru.com bogon route-servers
  match community 100
  set ip next-hop 192.0.2.1

! set a bogon next-hop on all routers that receive the bogons
ip route 192.0.2.1 255.255.255.255 Null0

ip prefix-list CYMRU-OUT-V4 seq 5 deny 0.0.0.0/0 le 32
```
Bogon Filter: Configuration IPv6

```
router bgp 17821
  neighbor 2620:0:6B0::xxxx:xxxx remote-as 65332
  neighbor 2620:0:6B0::xxxx:xxxx description CYMRUBOGONS
  neighbor 2620:0:6B0::xxxx:xxxx ebgp-multihop 255
  neighbor 2620:0:6B0::xxxx:xxxx password 7 0458390716775F1A08
  neighbor 2620:0:6B0::xxxx:xxxx update-source Loopback0

! address-family ipv6
  neighbor 2620:0:6B0::xxxx:xxxx activate
  neighbor 2620:0:6B0::xxxx:xxxx soft-reconfiguration inbound
  neighbor 2620:0:6B0::xxxx:xxxx prefix-list CYMRU-OUT-V6 out
  neighbor 2620:0:6B0::xxxx:xxxx route-map CYMRUBOGONS-V6 in

! configure community list to accept the bogon prefixes into the route-map
ip community-list 100 permit 65332:17821

! configure route-map. Remember to apply it to the proper peering sessions.
route-map CYMRUBOGONS-V6 permit 10
  description IPv6 Filter bogons learned from cymru.com bogon route-servers
  match community 100
  set ipv6 next-hop 2001:DB8:0:DEAD:BEEF::1

! set a bogon next-hop on all routers that receive the bogons
ipv6 route 2001:DB8:0:DEAD:BEEF::1/128 Null0

ipv6 prefix-list CYMRU-OUT-V6 seq 5 deny ::/0 le 128
```
Bogon Filter : Output

APNIC-Training-Lab01#show ip bgp 31.22.8.0/21
BGP routing table entry for 31.22.8.0/21, version 175332535
Paths: (1 available, best #1, table default, not advertised to EBGP peer)
   Advertised to update-groups:
      1
   Refresh Epoch 1
65332, (received & used)
   192.0.2.1 from 38.229.66.20 (38.229.66.20)
      Origin IGP, localpref 100, valid, external, best
      Community: 65332:17821 no-export
      rx pathid: 0, tx pathid: 0x0
Bogon Filter : Status

• The IPv4 fullbogons list is approximately 3,714 prefixes.
  – [date : 26th January, 2016]

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.229.xxx.xxx</td>
<td>4</td>
<td>65332</td>
<td>12017</td>
<td>12017</td>
<td>186072391</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0 1w0d</td>
<td>3733</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• The IPv6 fullbogons list is approximately 65,788 prefixes.
  – [date : 26th January, 2016]

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>2404:A800:xxxx:xx::xxxx</td>
<td>4</td>
<td>9498</td>
<td>3239994</td>
<td>72131</td>
<td>40075514</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3w1d</td>
<td>65788</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bogon Filter : Peering

• Contact bogonrs@cymru.com
  1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
  2. Your AS number
  3. The IP address(es) you want us to peer with
  4. Does your equipment support MD5 passwords for BGP sessions?
  5. Optional: your GPG/PGP public key

• https://www.team-cymru.org/bogon-reference-bgp.html
2. Flow Sonar
Flow Sonar

• The Team Cymru Flow Sonar system is a powerful tool for network managers to visually identify and understand what is happening on their network at any given time
• Leveraging the free and open-source framework provided by Peter Haag of SWITCH
• Special plugins "dosrannu" developed by Team Cymru to track malicious activity on your network
• Unique dosrannu feeds alerted to DDoS attacks, compromised machines, and the presence of connections to C&C hosts
Flow Sonar

Flow Stats

icmp trend is 99.87% (down) | tcp trend is 95.71% (down) | udp trend is 97.85% (down)

<table>
<thead>
<tr>
<th>timestamp</th>
<th>icmp flows</th>
<th>icmp % diff</th>
<th>tcp flows</th>
<th>tcp % diff</th>
<th>udp flows</th>
<th>udp % diff</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-04-09 20:35:01</td>
<td>1040153</td>
<td>95.12%</td>
<td>3813482</td>
<td>94.06%</td>
<td>122602785</td>
<td>97.82%</td>
</tr>
<tr>
<td>2015-04-09 20:36:01</td>
<td>1661393</td>
<td>99.1%</td>
<td>4028783</td>
<td>95.49%</td>
<td>125343851</td>
<td>94.89%</td>
</tr>
<tr>
<td>2015-04-09 20:35:01</td>
<td>1676511</td>
<td>97.2%</td>
<td>42190036</td>
<td>94.08%</td>
<td>13069615</td>
<td>95.85%</td>
</tr>
<tr>
<td>2015-04-09 20:35:01</td>
<td>1724813</td>
<td>100.45%</td>
<td>44845318</td>
<td>96.22%</td>
<td>13696839</td>
<td>99.02%</td>
</tr>
<tr>
<td>2015-04-09 20:35:01</td>
<td>1717072</td>
<td>104.76%</td>
<td>46666550</td>
<td>97.78%</td>
<td>13775167</td>
<td>102.24%</td>
</tr>
<tr>
<td>2015-04-09 20:35:01</td>
<td>1699111</td>
<td>98.02%</td>
<td>46768743</td>
<td>94.93%</td>
<td>13472789</td>
<td>96.29%</td>
</tr>
</tbody>
</table>

Latest Flow Alerts

<table>
<thead>
<tr>
<th>timestamp</th>
<th>count</th>
<th>src ip</th>
<th>src port</th>
<th>dst ip</th>
<th>dst port</th>
<th>protocol</th>
<th>alert source</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>*202.59.132.4</td>
<td>33356</td>
<td>113.107.239.158</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>*116.193.217.35</td>
<td>8080</td>
<td>100.140.100.132</td>
<td>1423</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>8</td>
<td>103.231.222.100</td>
<td>80</td>
<td>*116.193.217.35</td>
<td>60589</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>113.107.239.158</td>
<td>8081</td>
<td>*202.59.132.4</td>
<td>45278</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>183.61.179.151</td>
<td>8081</td>
<td>*202.59.132.4</td>
<td>46173</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>100.43.169.4</td>
<td>3619</td>
<td>*116.193.217.35</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>8</td>
<td>61.160.207.170</td>
<td>55142</td>
<td>*202.59.132.4</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>100.43.132.148</td>
<td>2076</td>
<td>*116.193.217.35</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>*116.193.217.35</td>
<td>8080</td>
<td>100.43.161.12</td>
<td>1079</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>*116.68.199.110</td>
<td>36293</td>
<td>122.225.38.197</td>
<td>81</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>60.169.77.106</td>
<td>62030</td>
<td>*116.127.26.1</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>12</td>
<td>61.160.207.204</td>
<td>16302</td>
<td>*116.127.26.3</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>8</td>
<td>61.160.6.105</td>
<td>16991</td>
<td>*202.59.132.4</td>
<td>8080</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>8</td>
<td>*202.59.132.4</td>
<td>8080</td>
<td>60.169.77.116</td>
<td>16040</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>*202.59.132.4</td>
<td>8080</td>
<td>222.186.26.34</td>
<td>58493</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
<tr>
<td>2015-04-09 20:55:01</td>
<td>4</td>
<td>120.195.155.69</td>
<td>801</td>
<td>*202.59.132.4</td>
<td>48362</td>
<td>6</td>
<td>ip reputation</td>
<td>proxy</td>
</tr>
</tbody>
</table>
Flow Sonar : Get It

• Contact outreach@cymru.com
  1. Team Cymru will send hardware
     • 1 Server
     • 1 Router

• https://www.team-cymru.org/Flow-Sonar.html
3. UTRS (Unwanted Traffic Removal Service)
RTBH 101

Customer Infra

IP: 203.0.113.114

Website

BGP: 203.0.113.0/24

CE

Provider Infra

Transit I

PE

Transit II

BGP: 203.0.113.0/24

Internet

Website
RTBH 101

Customer Infra

- IP: 203.0.113.114
- Website
- DDoS Traffic
- BGP: 203.0.113.0/24

Provider Infra

- PE
- Transit I
- DDoS Traffic
- DDoS Traffic
- Transit II
- Internet
- BGP: 1.2.3.0/24
RTBH 101
RTBH 101
RTBH Upstream

- Check whether your upstream provider support RTBH
- Configure & Test RTBH before incident
- Only announce IPv4 /32's from address space you originate or your customer
UTRS

• It’s based on the basic principle of DDoS filtering; Remotely Triggered Black Hole Filtering

• UTRS is a system that helps mitigate large infrastructure attacks by leveraging:
  – an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions
  – that automatically distributes verified BGP-based filter rules from victim to cooperating networks
UTRS : Configuration

router bgp 17821
neighbor 154.35.xxx.xxx remote-as 64496
neighbor 154.35.xxx.xxx description CYMRUBOGONS-UTRS
neighbor 154.35.xxx.xxx ebgp-multihop 255
neighbor 154.35.xxx.xxx transport connection-mode passive
neighbor 154.35.xxx.xxx password 7 xxxxxxxxxxxxxxxxxxxxxxxx
neighbor 154.35.xxx.xxx update-source Loopback0
!
address-family ipv4
    neighbor 154.35.xxx.xxx activate
    neighbor 154.35.xxx.xxx send-community
    neighbor 154.35.xxx.xxx soft-reconfiguration inbound
    neighbor 154.35.xxx.xxx route-map UTRS-OUT out
    neighbor 154.35.xxx.xxx route-map UTRS-IN in
!
access-list 1 remark utility ACL to deny everything
access-list 1 deny any
!
ip prefix-list 32-only permit 0.0.0.0/0 ge 32
ip community-list standard RTBH permit 17821:0
!
route-map UTRS-IN permit 10
    match ip address prefix-list 32-only
route-map UTRS-IN deny 100
    match ip address 1
!
route-map UTRS-OUT permit 10
    match ip address prefix-list 32-only
    match community RTBH
route-map UTRS-OUT deny 100
    match ip address 1
!
ip route 203.176.189.10 255.255.255.255 null0
UTRS : Apply

• Newly launched service
  – Quite picky to choose whom to peer
  – Do organization verification

• https://www.team-cymru.org/UTRS/index.html

• FAQ:
  – https://www.cymru.com/jtk/misc/utrs.html
How UTRS varies from RTBH with upstream!
Other Efforts

• NANOG BCOP : DDoS-DoS-attack-BCOP

• Routing Resilience Manifesto
  – Mutually Agreed Norms for Routing Security (MANRS)
  – https://www.routingmanifesto.org/manrs/
Questions!