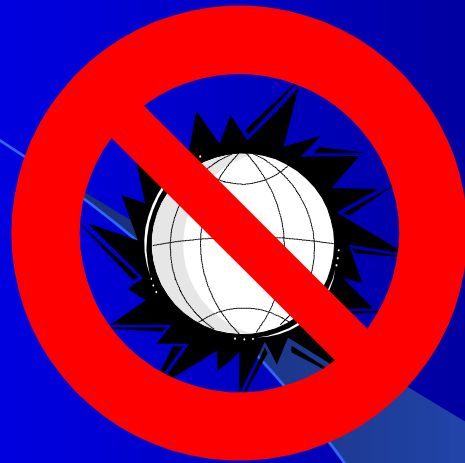


Geo-IP Blocking: A sometimes effective Mal-ware deterrent



DEFCON 13

Presentation

July 30, 2005

Agenda

- What is Geo-IP Blocking?
- Why Geo-IP Block?
- Why not to Geo-IP Block
- How Geo-IP Blocking works
- Regional Internet Registries (RIRs)
- Different Geo-IP Blocking strategies
- Automation
- Caveats

Presenter AKA Shameless Personal Plug

Tony Howlett

- President of Network Security Services, Inc.
- CISSP, GSNA, CNA, CSSA
- Author of “Open Source Security Tools”
- 17 years of experience building and managing networks

What is Geo-IP Blocking?

- Indiscriminately blocking entire sections of IP addresses related to geographical areas at your firewall or router

Spam Statistics



A recent study show that the following countries were the leaders in originating spam

USA	42%
South Korea	13%
China	8%

Blocking those two countries alone would take care of 21% of your spam

Source: SpamHaus 2005

Why Geo-IP Block?

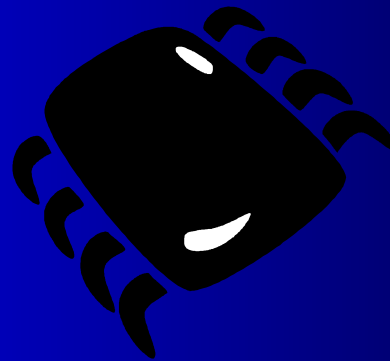
- **Quick (within minutes)**
- **No Cost (just entries in a router)**
- **Avoids almost ALL types of attacks including zero day and unreported exploits (at least those originating from the blocked countries)**
- **Easily reversible**
- **Users can still access blocked sites outbound**
- **Most companies don't need to give the ENTIRE world access to their network.**
- **Even Fortune 500 companies can use this for some parts of their network.**

More Reasons to Geo-IP Block

- **May become more effective over time as more spam / malware moves offshore**
- **May force “bad actor” countries to crack down on spam / malware**
- **China recently announced a crackdown on spam partially due to pressure from ISPs blocking their IP space**

Types of malware Geo-IP can stop

- Spam
- Email Fraud
- Phishing
- Viruses
- Worms
- Automated hacking tools
- Manual hacking (script kiddies)
- Prohibited website hosted offshore (porn, gambling, etc)



Reasons NOT to Geo-IP block

- Not 100% effective (what is?)
- Goes against the idea of global access to the Internet
- Large multinational corporation (may still work in some limited instances)
- Doing business overseas (may still work for some areas)
- Will block all emails from that part of the world (unless you except mail traffic from your rules)

How Geo-IP Blocking Works

- IANA assigns address blocks out to the Regional Internet Registries (RIRs) for local assignment
- American Registry for Internet Numbers (ARIN) handles North America

Other RIRs

- **APNIC (Asia)**
- **RIPE (Europe, Middle East and Central Asia)**
- **LACNIC (Latin America)**
- **AfriNIC (new RIR for Africa)**

APNIC (Asia)

- Asia Pacific Network Information Centre
- Takes in many of the bad actor countries (the #2 and #3 spammers in our example)
- Just blocking APNIC could lower your malware hits by 20-30%
- Be careful; also cover Japan where a lot of westerners do business

APNIC IPs to block*

58.0.0.0/8

61.0.0.0/8

124.0.0.0/8

126.0.0.0/8

168.208.0.0/16

196.192.0.0/16

202.0.0.0/8

210.0.0.0/8

218.0.0.0/8

220.0.0.0/8

222.0.0.0/8

*List not guaranteed to be complete or accurate, caveat emptor

China Only (with APNIC and ARIN IP space)*

*List not guaranteed to be complete or accurate, caveat emptor

159.226.0.0 - 159.226.255.255

161.207.0.0 - 161.207.255.255

162.105.0.0 - 162.105.255.255

166.111.0.0 - 166.111.255.255

167.139.0.0 - 167.139.255.255

168.160.0.0 - 168.160.255.255

192.124.154.0 - 192.124.154.255

192.188.170.0 - 192.188.170.255

192.83.122.0 - 192.83.122.255

198.17.7.0 - 198.17.7.255

198.97.132.0 - 198.97.132.255

202.0.110.0 - 202.0.110.255

202.0.160.0 - 202.0.179.255

202.122.128.0 - 202.122.128.255

202.127.0.0 - 202.127.63.255

202.127.128.0 - 202.127.255.255

202.130.0.0 - 202.130.31.255

202.130.224.0 - 202.130.255.255

202.131.208.0 - 202.131.223.255

202.136.252.0 - 202.136.255.255

202.14.235.0 - 202.14.238.255

202.14.88.0 - 202.14.88.255

202.192.0.0 - 202.207.255.255

202.20.120.0 - 202.20.120.255

202.22.248.0 - 202.22.255.255

202.38.0.0 - 202.38.15.255

202.38.140.0 - 202.38.156.255

202.38.158.0 - 202.38.161.255

202.38.164.0 - 202.38.176.255

202.38.184.0 - 202.38.255.255

202.38.32.0 - 202.38.47.255

202.38.64.0 - 202.38.138.255

202.4.128.0 - 202.4.159.255

202.4.252.0 - 202.4.255.255

202.90.0.0 - 202.90.3.255

202.90.252.0 - 202.91.3.255

202.91.128.0 - 202.91.131.255

202.92.0.0 - 202.92.3.255

202.92.252.0 - 202.93.3.255

202.93.252.0 - 202.93.255.255

202.94.0.0 - 202.94.31.255

202.95.0.0 - 202.95.31.255

202.95.252.0 - 202.122.39.255

203.128.128.0 - 203.128.159.255

203.184.0.0 - 203.184.3.255

203.192.0.0 - 203.192.31.255

203.196.0.0 - 203.196.3.255

203.207.64.0 - 203.208.19.255

203.212.0.0 - 203.212.15.255

203.222.192.0 - 203.222.207.255

203.223.0.0 - 203.223.15.255

203.81.16.0 - 203.81.31.255

203.87.224.0 - 203.88.3.255

203.89.0.0 - 203.89.3.255

203.90.0.0 - 203.90.3.255

203.91.0.0 - 203.91.3.255

203.92.0.0 - 203.92.3.255

203.93.0.0 - 203.94.31.255

203.95.0.0 - 203.95.7.255

210.12.0.0 - 210.13.255.255

210.14.160.0 - 210.15.191.255

210.192.96.0 - 210.192.127.255

210.21.0.0 - 210.22.255.255

210.211.0.0 - 210.211.15.255

210.25.0.0 - 210.47.255.255

210.5.0.0 - 210.5.31.255

210.5.128.0 - 210.5.143.255

210.51.0.0 - 210.53.255.255

210.72.0.0 - 210.78.255.255

210.79.224.0 - 210.79.255.255

210.82.0.0 - 210.83.255.255

211.136.0.0 - 211.167.255.255

211.64.0.0 - 211.71.255.255

211.80.0.0 - 211.103.255.255

Korea Only (with APNIC and
ARIN IP space)*

*List not guaranteed to be complete or accurate, caveat emptor

128.134.0.0 - 128.134.255.255
129.254.0.0 - 129.254.255.255
132.16.0.0 - 132.16.255.255
134.75.0.0 - 134.75.255.255
137.68.0.0 - 137.68.255.255
141.223.0.0 - 141.223.255.255
143.248.0.0 - 143.248.255.255
147.43.0.0 - 147.43.255.255
147.46.0.0 - 147.47.255.255
147.6.0.0 - 147.6.255.255
150.150.0.0 - 150.150.255.255
150.183.0.0 - 150.183.255.255
150.197.0.0 - 150.197.255.255
152.149.0.0 - 152.149.255.255
152.99.0.0 - 152.99.255.255
154.10.0.0 - 154.10.255.255
155.230.0.0 - 155.230.255.255
156.147.0.0 - 156.147.255.255
157.197.0.0 - 157.197.255.255
158.44.0.0 - 158.44.255.255
161.122.0.0 - 161.122.255.255
163.152.0.0 - 163.152.255.255
163.180.0.0 - 163.180.255.255
163.239.0.0 - 163.239.255.255
164.124.0.0 - 164.125.255.255
165.132.0.0 - 165.133.255.255
165.141.0.0 - 165.141.255.255
165.186.0.0 - 165.186.255.255

165.194.0.0 - 165.194.255.255
165.213.0.0 - 165.213.255.255
165.229.0.0 - 165.229.255.255
165.243.0.0 - 165.244.255.255
165.246.0.0 - 165.246.255.255
166.103.0.0 - 166.104.255.255
166.125.0.0 - 166.125.255.255
166.79.0.0 - 166.79.255.255
168.115.0.0 - 168.115.255.255
168.126.0.0 - 168.126.255.255
168.131.0.0 - 168.131.255.255
168.154.0.0 - 168.154.255.255
168.188.0.0 - 168.188.255.255
168.219.0.0 - 168.219.255.255
168.248.0.0 - 168.249.255.255
168.78.0.0 - 168.78.255.255
169.140.0.0 - 169.140.255.255
192.100.2.0 - 192.100.2.255
192.104.15.0 - 192.104.15.255
192.132.15.0 - 192.132.15.255
192.132.247.0 - 192.132.251.255
192.195.39.0 - 192.195.40.255
192.203.138.0 - 192.203.146.255
192.245.249.0 - 192.245.251.255
192.249.16.0 - 192.249.31.255
192.5.90.0 - 192.5.90.255
198.178.187.0 - 198.178.187.255
202.14.103.0 - 202.14.103.255

202.14.165.0 - 202.14.165.255
202.189.128.0 - 202.189.191.255
202.20.119.0 - 202.20.119.255
202.20.128.0 - 202.20.255.255
202.20.82.0 - 202.20.86.255
202.20.99.0 - 202.20.99.255
202.21.0.0 - 202.21.7.255
202.30.0.0 - 202.31.255.255
202.6.95.0 - 202.6.95.255
203.224.0.0 - 203.255.255.255
210.178.0.0 - 210.183.255.255
210.204.0.0 - 210.207.255.255
210.216.0.0 - 210.223.255.255
210.80.96.0 - 210.80.111.255
210.90.0.0 - 210.127.255.255
211.104.0.0 - 211.119.255.255
211.168.0.0 - 211.255.255.255
211.32.0.0 - 211.63.255.255
218.144.0.0 - 218.159.255.255
218.232.0.0 - 218.239.255.255
218.36.0.0 - 218.39.255.255
218.48.0.0 - 218.55.255.255
219.240.0.0 - 219.241.255.255
219.248.0.0 - 219.255.255.255
220.64.0.0 - 220.92.255.255
61.248.0.0 - 61.255.255.255
61.32.0.0 - 61.43.255.255
61.72.0.0 - 61.87.255.255

Riseaux IP Europeens (RIPE)

- **Covers Europe, the Middle East and Central Asia**
- **Not as effective to block country by country as many blocks cover multiple countries (Multinational ISPs, companies, etc)**
- **Also hard to block wholesale as a lot of global companies based in Europe**
- **There are a few troublesome countries worth blocking (Russia, Bulgaria, Romania)**

RIPE IPs to block*

80.0.0.0/8

81.0.0.0/8

82.0.0.0/8

83.0.0.0/8

84.0.0.0/8

85.0.0.0/8

86.0.0.0/8

87.0.0.0/8

88.0.0.0/8

89.0.0.0/8

90.0.0.0/8

91.0.0.0/8

193.0.0.0/8

194.0.0.0/8

195.0.0.0/8

212.0.0.0/8

213.0.0.0/8

217.0.0.0/8

*List not guaranteed to be complete or accurate, caveat emptor

LACNIC

- Latin America and Caribbean
- Many organizations / entities may still use ARIN addresses
- Brazil and Argentina are worst offenders
- Border companies may want to leave in Mexico

LACNIC IPs to block*

189.0.0.0/8

190.0.0.0/8

200.0.0.0/8

201.0.0.0/8

*List not guaranteed to be complete or accurate, caveat emptor

Complete Brazilian List with ARIN assignments

139.82.0.0/16
143.54.0.0/16
143.106.0.0/15
143.108.0.0/16
144.23.0.0/16
146.134.0.0/16
146.164.0.0/16
147.65.0.0/16
150.161.0.0/16
150.162.0.0/15
150.164.0.0/15
152.84.0.0/16
152.92.0.0/16
155.211.0.0/16
157.86.0.0/16
161.24.0.0/16
161.79.0.0/16
161.148.0.0/16
164.41.0.0/16
164.85.0.0/16
170.66.0.0/16
192.80.209.0/24
192.111.229.0/24
192.111.230.0/24
192.132.35.0/24
192.146.157.0/24

192.146.229.0/24
192.147.210.0/24
192.147.218.0/24
192.153.88.0/24
192.153.120.0/24
192.153.155.0/24
192.159.116.0/23
192.160.45.0/24
192.160.50.0/24
192.160.111.0/24
192.160.128.0/24
192.160.188.0/24
192.188.11.0/24
192.190.30.0/23
192.195.237.0/24
192.198.8.0/21
192.207.194.0/23
192.207.200.0/22
192.207.204.0/23
192.207.206.0/24
192.223.64.0/18
192.231.114.0/23
192.231.116.0/22
192.231.120.0/23
192.231.175.0/24
192.231.176.0/24

198.17.120.0/23
198.17.231.0/24
198.17.232.0/24
198.49.128.0/22
198.49.132.0/23
198.50.16.0/21
198.58.8.0/22
198.58.12.0/24
198.184.161.0/24
200.0.8.0/21
200.0.0.0/16
200.3.0.0/16
200.5.0.0/16
200.6.0.0/16
200.7.0.0/16
200.9.0.0/16
200.10.0.0/16
200.11.0.0/16
200.12.0.0/16
200.12.0.0/16
200.13.0.0/16
200.14.0.0/16
200.17.0.0/16
201.0.0.0/11
201.32.0.0/12
206.221.80.0/20

AfriNIC

- A lot of fraud and phishing based here
- Not much legitimate commerce (except for energy companies)
- Since this is new, many assignments still come from RIPE address space

AfriNIC IPs to Block

- 41.0.0.0/8

Geo-IP Blocking Strategies

- The Shotgun Approach
- Block Entire RIR address space
- Pros: Easy and Quick
- Cons: Might block some countries or areas you want.
- Example: Australian and New Zealand sites use APNIC address space

Geo-IP Blocking Strategies

- The Rifle Approach
- Block by specific country assignments
- Pros: Less likely to block wanted traffic
- Cons: Time consuming, have to keep configs up to date, some assignments not country specific

Limited Geo-IP Blocking Strategies

- Block all protocols but mail (no spam benefit)
- Block all except web server and mail
- Block on all private LAN segments but not DMZ (no spam or public server exploits benefits)

More Limited Geo-IP Blocking

- Block only interactive services (Telnet, SSH, VNC, Terminal services)
- Block only on specialized servers (VPN, database)
- Block RIR but allow certain ISP and hotel webspace (to allow for VPN access)

IP Chains Geo IP Blocking Example

```
ipchains -I input -s 58.0.0.0/8 -j DENY
```

Cisco Geo IP Blocking Example

```
access-list 101 deny ip 58.0.0.0 0.0.0.255 any
```

SonicWall Geo IP Blocking Example

General

Advanced

Bandwidth

Action: Allow Deny

Service:

Ethernet: Address Range Begin: Address Range End:

Source:

Destination:

Comment

Comment:

Ready

OK

Cancel

Help

Geo-IP Blocking Automation

- Ip.ludost.net has a script that will generate country specific lists for importing into a IP Tables format
- There are companies now that will do this work for you, producing a file for importing into your configs
- Used by large websites, search engines, some ISPs

Resources

Bob's IP blocking list

(<http://www.unixhub.com/block>)

IP to Country Database at Ludost.net

(<http://ip.ludost.net>)

Questions / Comments / Abuse?

- Email me at thowlett@netsecuritysvcs.com
- The presentation will be posted to :
www.netsecuritysvcs.com/defcon13/