

country2ip

mapping entire
country netblocks

Done already publicly?

- Probably not (according to Google)
- We found many “ip2country” services, but NOT “country2ip”

Registry DBs (whois)

- Interesting fields
 - "country:"
 - "inetnum:"
 - "NetRange:"

Mapping Methodology

- Generate random IP address every X seconds (bash bots?)
- Make whois lookup to random IP address
- Grab netblock and country code and write to a database
- Simply query a geoip DB

Problems

- Country to which a netblock is registered is NOT necessarily the location of the servers using IP addresses in that netblock
- Many others!!!

Applications for this data

- Electronic warfare
- Legal port-scanning
- Exploitation of international politics for crackers when breaking into computers (finding hopping point in Cuba to attack a machine in the US?)
- Any other ideas? 😊

Open source geoip DBs

- <http://www.maxmind.com/download>,
- <http://tqmcube.com/worldcidr.php>

Lame PoC

- <http://ikwt.com/projects/country2ip>
- Security monkeys that researched this topic:
 - pdp [<http://gnucitizen.org/>]
 - pagvac [<http://ikwt.com/>]