1000 days of UDP amplification DDoS attacks

Daniel R. Thomas,
Richard Clayton,
Alastair R. Beresford

Firstname.Lastname@cl.cam.ac.uk
UDP scanning

Reflector
8.8.8.8

big.gov IN TXT " Extremely long response................
........................
........................
........................"
src: 8.8.8.8
dst: 192.168.25.4

Attacker
192.168.25.4

big.gov IN TXT
src: 192.168.25.4
dst: 8.8.8.8

(1)

(2)
UDP reflection DDoS attacks

big.gov IN TXT "Extremely long response"..........................
src: 8.8.8.8
dst: 172.16.6.2

big.gov IN TXT
src: 172.16.6.2
dst: 8.8.8.8

Reflector
8.8.8.8

Victim
172.16.6.2

Attacker
192.168.25.4
We run lots of UDP honeypots

- Median 65 nodes since 2014
- Hopscotch emulates abused protocols
  - QOTD, CHARGEN, DNS, NTP, SSDP, SQLMon, Portmap, mDNS, LDAP
- Sniffer records all resulting UDP traffic
- (try to) Only reply to black hat scanners
Estimating total attacks using capture-recapture

A = 160

B = 200

Estimated population: 400 ± 62
The graph illustrates the number of honeypots in operation over time, with two categories labeled '# A+H' and '# A'. The x-axis represents the years from 2014 to 2017, with quarterly intervals, while the y-axis represents the number of honeypots in operation, ranging from 0 to 90.
NTP

Frequency of attacks (millions)

Duration of attack (minutes)
NTP

P(attack ends in <5min | duration)

Duration of attack (minutes)
Vdos coverage NTP

![Graph showing Vdos coverage NTP with seen and missing data over time from 2015-09 to 2016-09.](chart.png)
Vdos coverage SSDP

Number of attacks

- Seen
- Missing

Yearly timeline from 2015-09 to 2016-09 with data points indicating the number of attacks.
This was ethical

- We reduce harm by absorbing attack traffic
- We don’t reply to white hat scanners (no timewasting)
- We used leaked data for validation, this was necessary and did not increase harm.
- We have a paper under submission on the ethics of using leaked data for research.
Running a honeypot network is cheap (but we do it for you)

- Median of 65 nodes.
- 200GB/month inbound per node.
- Hosting costs of $170/month (+staff costs)
- Need 10 to 100 sensors depending on protocol.
- Our collection is ongoing and you can use our data. You can also contribute.
This is a solvable problem

- BCP38/SAVE
- Follow the money
- Enforce the law
- Warn customers it is illegal
Ongoing work

● Selective reply (like Krupp et al. 2016)
● More cross validation
● Estimate attack volume
● Collaboration
  – What do you want to do with this data?
  – You can run our code.
  – Do you have ground truth for attack volumes?
Data is available through the Cambridge Cybercrime Centre

https://cambridgecybercrime.uk/

Daniel R. Thomas
Richard Clayton
Alastair R. Beresford

Firstname.Lastname@cl.cam.ac.uk