1000 days of UDP amplification DDoS attacks

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

Firstname.Lastname@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Daniel: 5017 A1EC 0B29 08E3 CF64 7CCD 5514 35D5 D749 33D9
Richard: 899A 94CE BFCE CCE2 5744 5ACE 3BBC CF52 A8B9 ECFB
Alastair: 9217 482D D647 8641 44BA 10D8 83F4 9FBF 1144 D9B3
UDP scanning

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

(1)

big.gov IN TXT
src: 192.168.25.4
dst: 8.8.8.8

(2)

Attacker
192.168.25.4
UDP reflection DDoS attacks

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

Reflector
8.8.8.8

big.gov IN TXT
src: 172.16.6.2
dst: 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
This is ethical

- We reduce harm by absorbing attack traffic
- We don’t reply to white hat scanners (no timewasting)
Estimating total attacks using capture-recapture

A=160

B=200

Estimated population: 400 ± 62
NTP

Duration of attack (minutes)

Frequency of attacks (millions)
NTP

$p(\text{attack ends in } <5\text{min} | \text{duration})$

Duration of attack (minutes)
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

Daniel:  5017 A1EC 0B29 08E3 CF64 7CCD 5514 35D5 D749 33D9
Richard:  899A 94CE BFCE CCE2 5744 5ACE 3BBC CF52 A8B9 ECFB
Alastair:  9217 482D D647 8641 44BA 10D8 83F4 9FBF 1144 D9B3