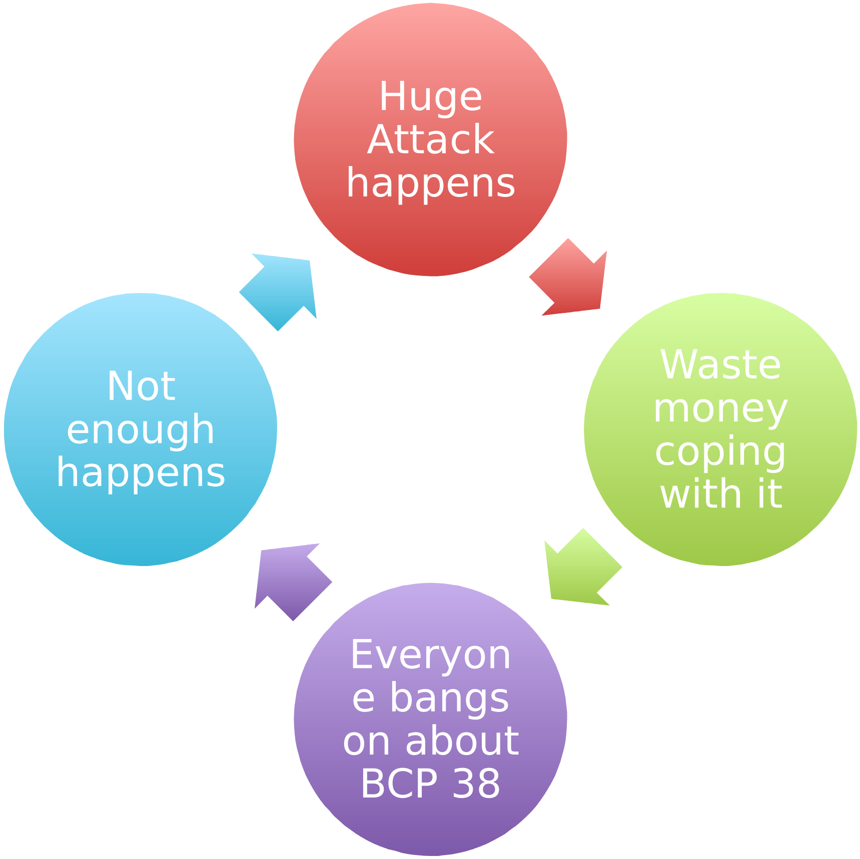
BCP38 - UKNOF

Neil McRae and others

(names omitted to protect the guilty^w innocent).

Big Network Attack Cycle


Huge Attack happens

Waste money coping with it

Everyone bangs on about BCP 38

Not enough happens

BCP38 - what is it?

- Denying access to the network to traffic with spoofed addresses from _your_ customers.
- Helping to ensure that traffic is traceable to its correct source network.
- Stops your customers driving cost in your network.
- Stops our industry costs increasing and government intervention.
- Other good things…

Filtering your customer FOONET

- access-list 199 remark **All acceptable prefixes from FOONET**
- access-list 199 permit ip host 194.8.68.130 any
- access-list 199 permit ip host 193.112.33.4 any
- access-list 199 permit ip host 193.112.33.34 any
- access-list 199 permit ip 195.151.3.0 0.0.0.7 any
- access-list 199 permit ip 195.151.6.0 0.0.0.7 any
- access-list 199 permit ip 195.21.70.0 0.0.0.255 any

- And attach to an interface

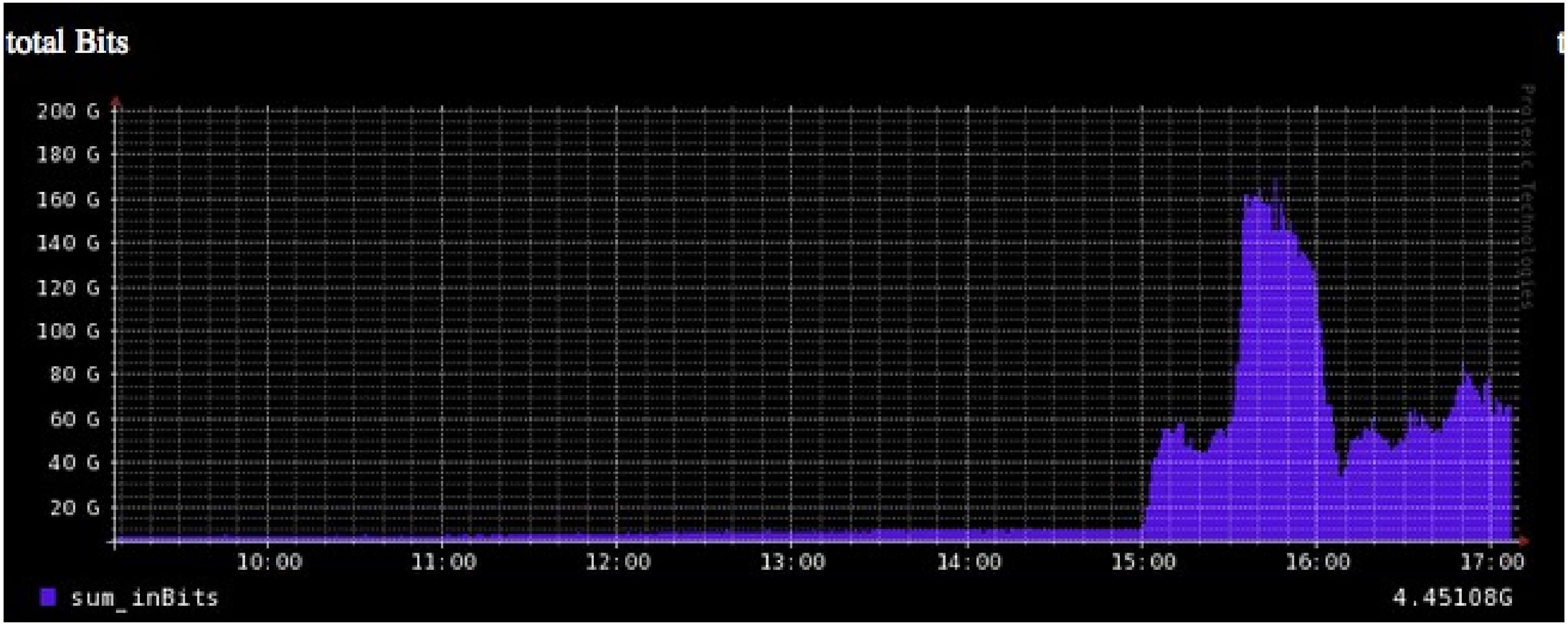
- If you need to log
- access-list 199 deny ip any any log

- But you need a pretty good logging setup as the volume is significant.

Where to do it?

- Deploy filters on your customer edge
  - PE / Access Device / BRAS
  - Datacentre edge gateway (more and more attacks from here) – Cloud providers are a real issue here.
  - Standardisation in cloud makes firing up instant VM based botnets
  - Be wary if you have a customer who sells transit via BGP – you may consider building filter list from your prefix list (you do have prefix lists on your customers right?!)
  - Make deploying BCP38 a T&C issue. (this is a plus point with big corporates!).

About the recent issues…



Spend the time now on network hygiene rather than spend a lot more dealing with an issue.

Wider Network Hygene

- Open resolvers – see:

- http://openresolverproject.org

Further reading

- MIT - http://spoofer.cmand.org/papers.php
- Nico @ COLT NGN Securite http://securite.org/
- RIPE 432 – Benefits of BCP38
- Openresolver - http://openresolverproject.org