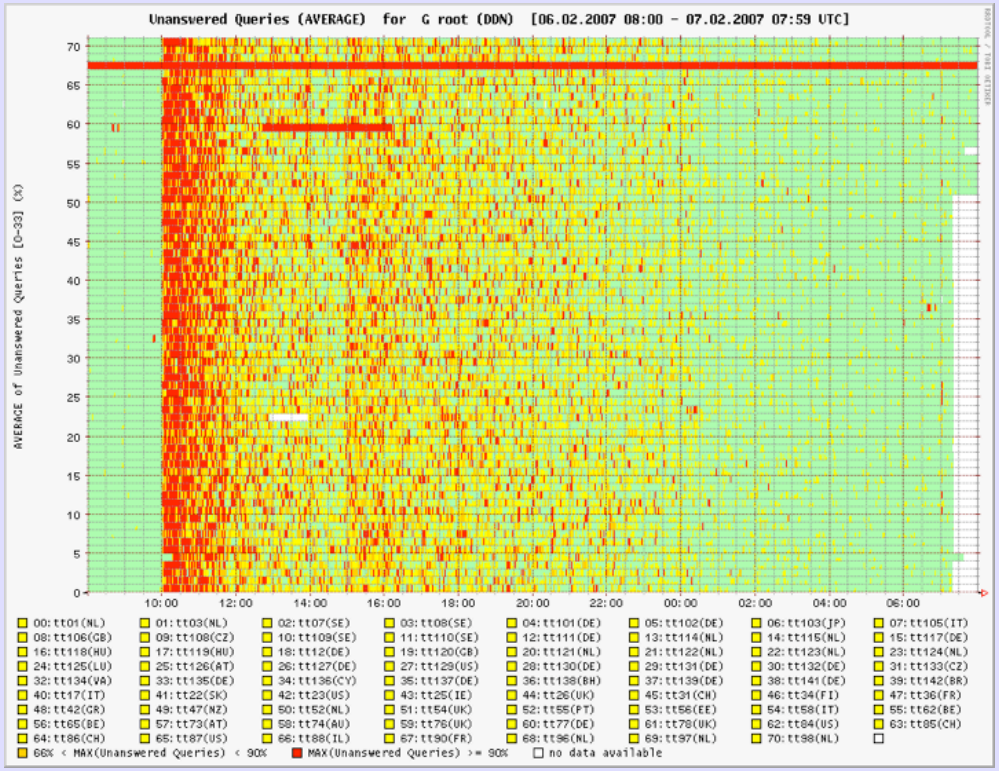
Attacks against DNS root nameservers

Johan Ihrén, Autonomica AB

i.root-servers.net

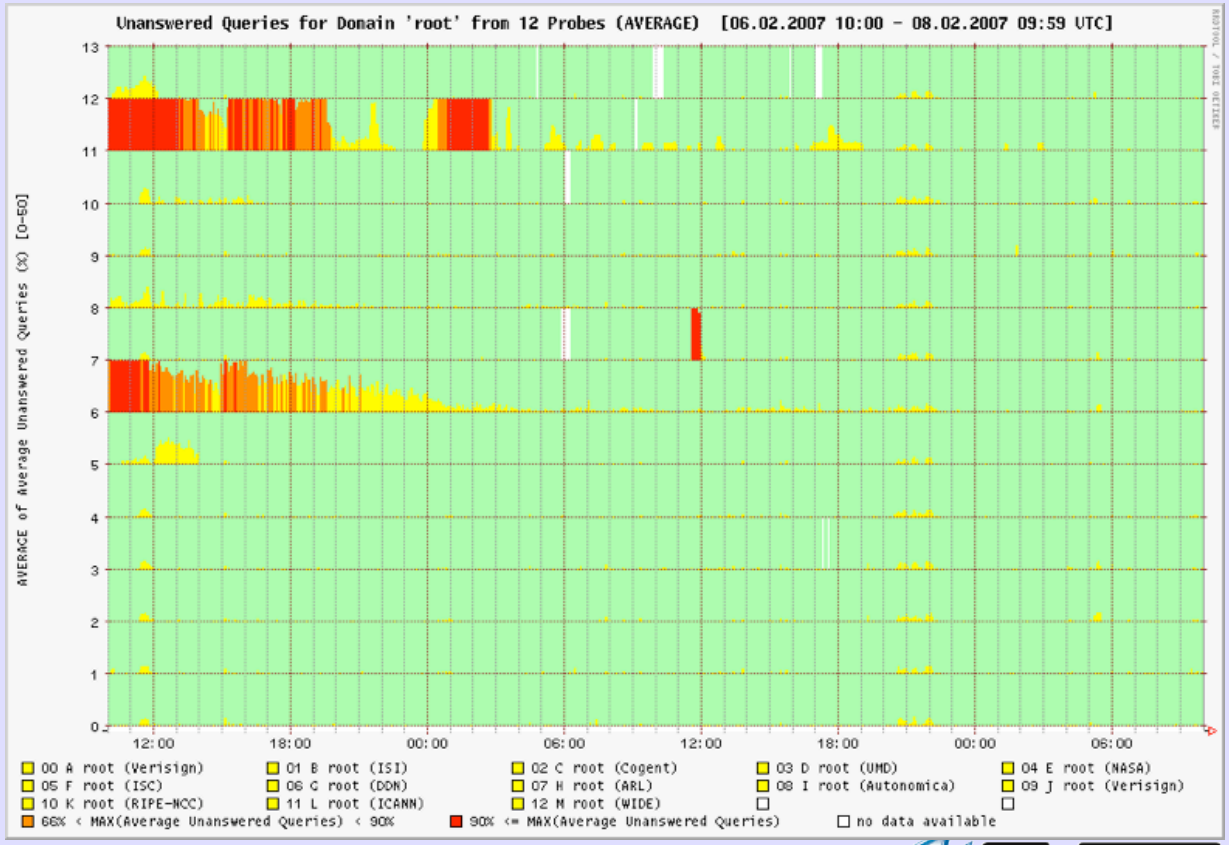
In spite of...



- this was not really an attack on the root server system

because...

- ...most of the roots were just fine:



What is was:

- An attack on certain IP addresses, some of which (but not all) were root nameservers
- The cause is unknown, but it seems likely to be some sort of vanity attack or display of ability
  - the more we talk about this the greater the success was...

“Botnets” and DDOS

- No one should make the claim that they are invincible against large scale DDOS attacks
- This is true also for the root nameservers
- However, while we’re not invincible, the root nameservers are really not where the problem is

“Botnets” and DDOS, cont’d

- The root nameservers are widely anycast
  - in more than 100 locations
- They are (in spite of all our efforts) really only used very rarely by individual resolvers for the Internet to work just fine
  - one root server is really sufficient
  - this was true also this time
- Others don’t have the same luxury

The Consequences

- There are organizations that would go out of business if they were hit by a large scale attack
- ...or at least suffer considerable harm

- Without having to look for the really speculative it is obvious that there are examples all over the map of services that have bad DDOS resilience

“Botnets” and DDOS

- “Botnets” are a term frequently used for farms of remotely controlled hosts
- The owners are unaware that their hardware is being used maliciously
- The hosts are infected via all the traditional means of malware propagation (viruses, email, cooked web sites, etc)

The Tragedy of The Commons

- The Tragedy of The Commons is a metaphor for a shared resource with a value greater than its individual parts failing due to some people systematically extracting more from the shared resource than they contribute
- Thereby the continued existence of the resource is threatened

The Tragedy of The Commons

- Common Internet-related examples include spam, phishing and DDOS
- In this case it was the latter

- The problem is not only one of defending against the attack (important as that is)
- it is also about gradually decreasing the overall value of the network

The Questions

- So what happens to the victims of attacks that do not reach the headlines?
- Is the Internet turning into a vehicle for blackmail and extortion?
- How did we get here?
- How do we get out of here?

Other Questions?

johani@autonomica.se