DNS Abuse in Africa

What is DNS Abuse? One persons terrorist is another's freedom fighter

results of 3 day survey

Consensus is that little to none is seen coming from hosts in KE or the region

ZA reports a little but “under the radar”

Some port scanning/auto querying coming from Eastern Europe and China seen by registries and operators

DNSSEC planning going on, but no deployments

regional carrier NS log snippet

Mar 7 23:37:42 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:42 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:43 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:43 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:43 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:44 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:44 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:45 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:45 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:45 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:45 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:46 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:46 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:55 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:56 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:56 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:37:57 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:37:59 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:38:00 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53
Mar 7 23:38:00 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 195.24.78.112#53
Mar 7 23:38:01 ns0 named[3804]: lame server resolving 'www.duhi-darom.ru' (in 'duhi-darom.ru'?): 89.108.118.75#53

89.108.118.75 is a nameserver in RU

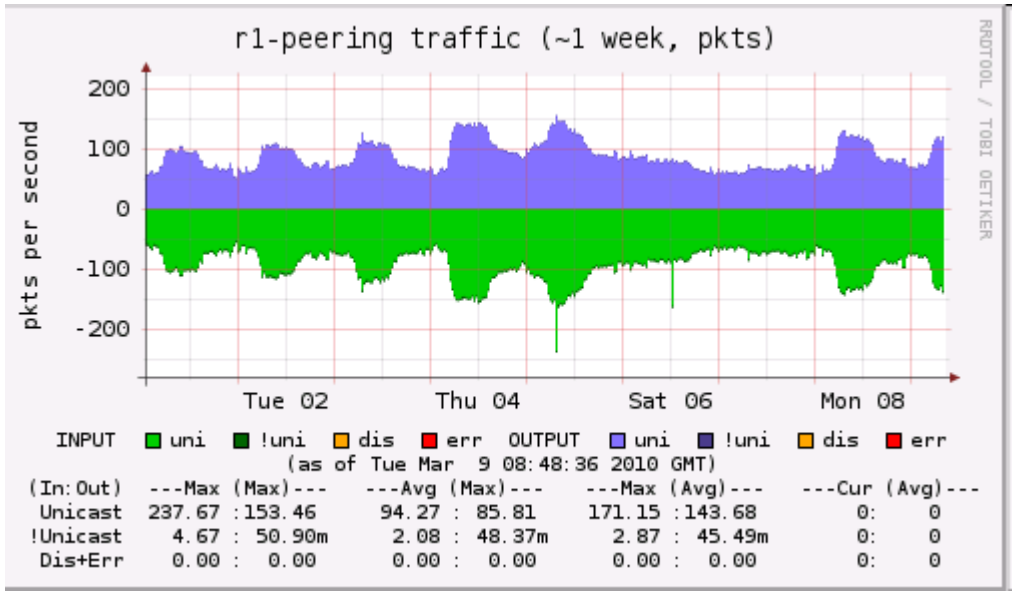
195.24.78.112 is a NS in Luxembourg

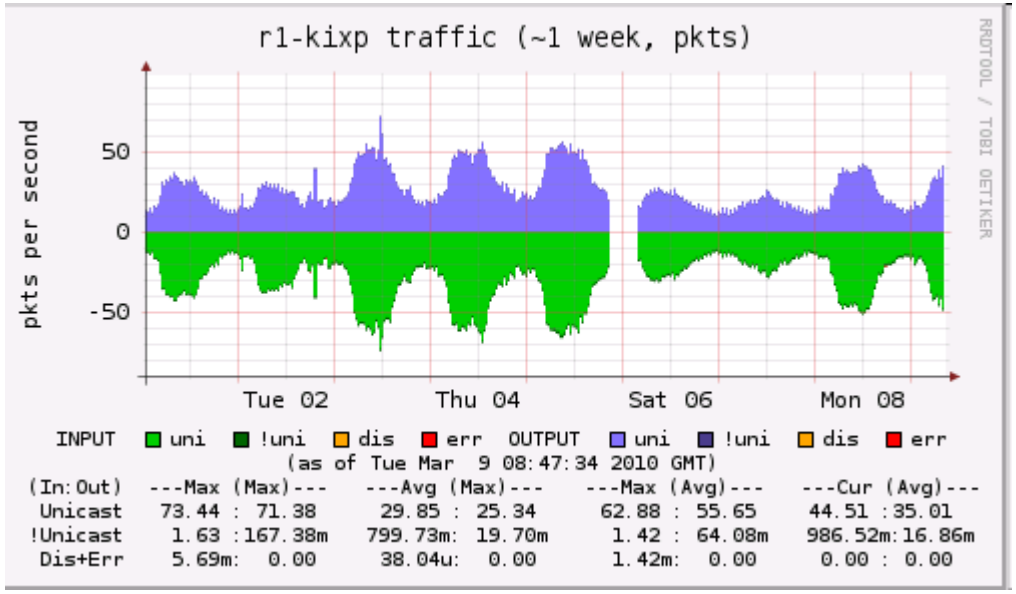
Non-DNS attacks on DNS orgs

- .UG, .TN, .MW, and .MA had records altered last year by SQL injection attacks
- KE, ZM, others reporting brute force login attempts on registry interface
- DNSCurve/DNSSEC does not prevent this type of behavior

root servers in the region

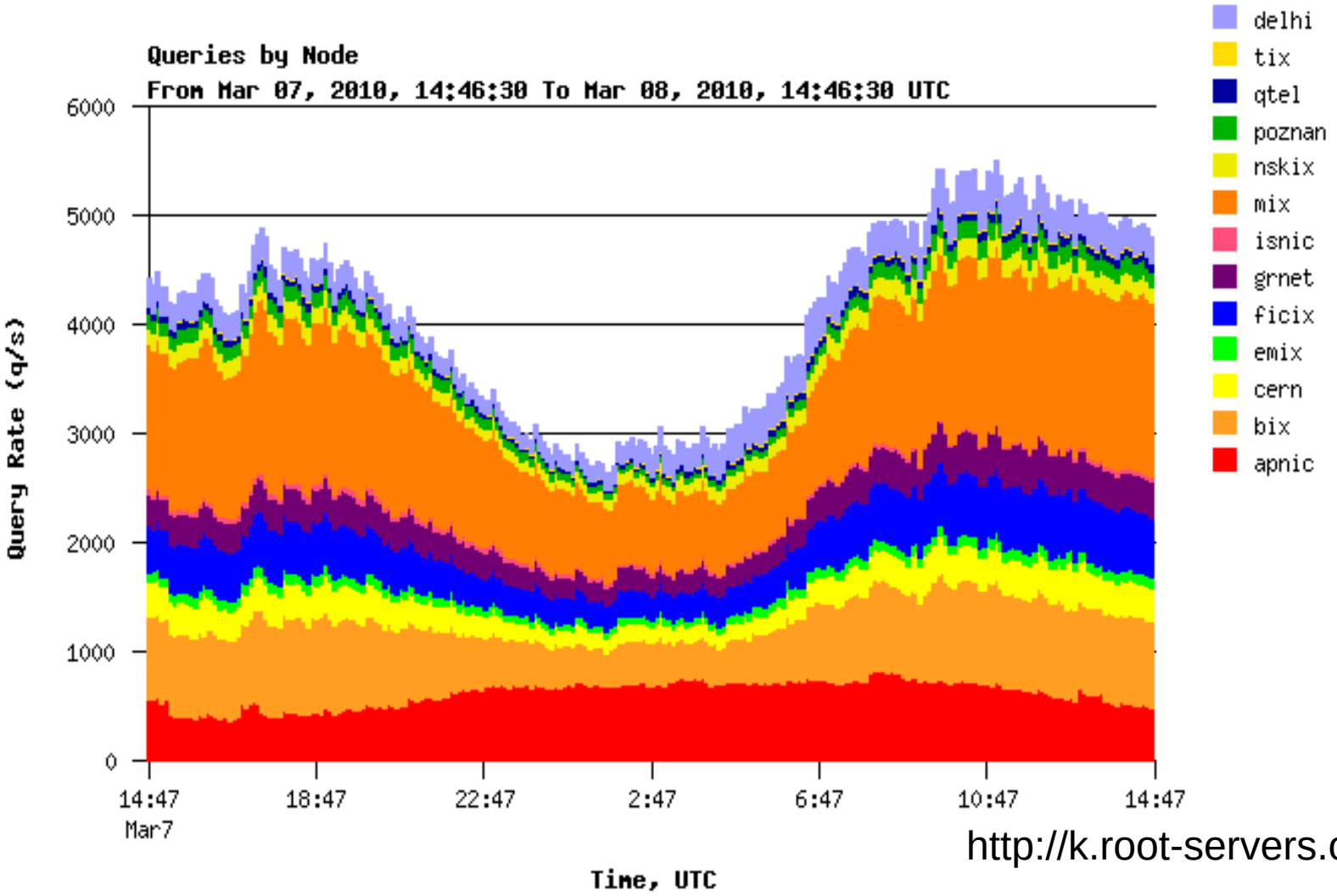
- F-root node in Nairobi is a quiet one, localised to KE ISPs, working well
- most non-pertinent traffic blocked, rate limited incoming traffic, no packet storms as seen elsewhere
- SSH scans seen, as everywhere else
- node is Jo'burg sees more than double the traffic of the one in Nairobi





Source: J. Damas ISC

K-root in TZ
local node so less traffic, but same pattern as other nodes



http://k.root-servers.org/

cybercrime does affect us

- Cybercafes running “XP” other holes
- Conficker hit cafes fairly hard
- Banks and other financial services also targets

- “True that - Mozilla flags www.births.go.ke as a reported attack site - meaning bad boys and girls are using it to launch cyberattacks...

  funny, just sitting at KICC (ICANN Meeting) listening to the Director General, CCK boasting of our East African Cyber Security Task Force…

Mitigation

- .ke, others looking at DNSSEC
- CERTs & CSIRTs being created, many folk inspired by Team Cymru!
- AfNOG/AfriNIC/ISOC/NSRC trainings
- East African Cyber Security Task Force
- Awareness increasing

food for thought

- Do we in the region lack the capacity to launch sophisticated attacks?
- Do we lack capacity to detect attacks?
- Do we not (yet) have the mindset to launch attacks via DNS (softer targets, e.g. mobile money, identity theft)?
- Are botnets in Africa less useful to miscreants due to outgoing bandwidth constraints?
- Is it just a question of scale?
- Do we not do enough log monitoring?
- Fiber to the world means we will be botnet herder target?