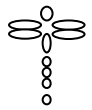


ルートDNSへの攻撃
～その時キャッシュサーバは見た ～

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

attack on root dns

- 2007年2月6日 19:00JST頃～
- 複数のroot dnsと、一部tldのdnsにDDoS
  - UDP/53宛に大量パケット
  - パケットサイズは大き目
  - dnsではないパケットフォーマットなど
  - 攻撃の送信元は主にアジア地域
- rootやISPのオペレータ達が協力して対応

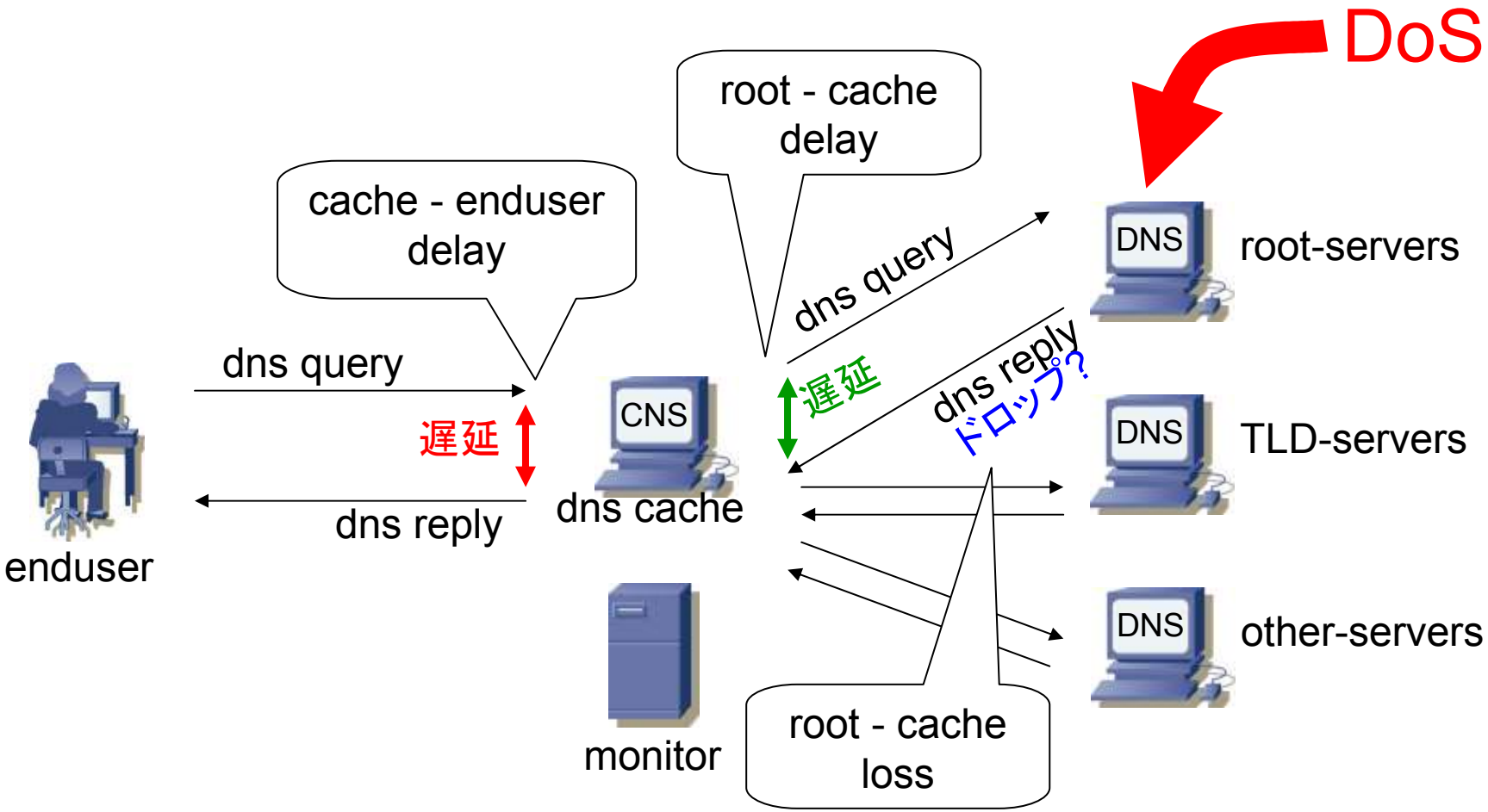
攻撃に関するレポート

- 既に多くの組織から攻撃に関するレポートが出ている
  - http://www.nanog.org/mtg-0702/presentations/knight.pdf
  - www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf
- anycastの効果や攻撃に関する調査など
  - 主にroot側でのレポート

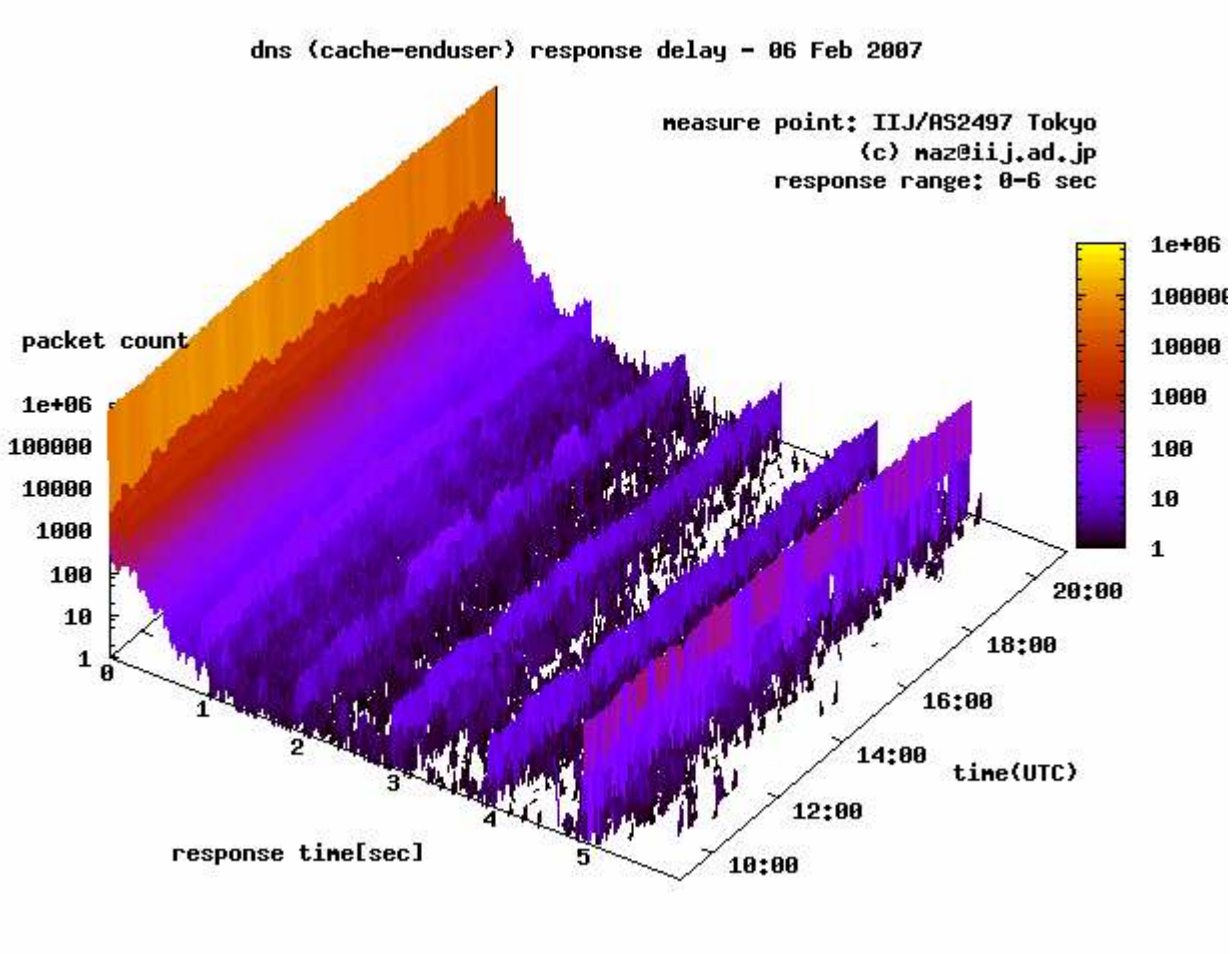
キャッシュdnsでの状況

- IIJで運用するキャッシュdnsで、攻撃発生時の応答遅延などを調査
  - サーバはCNSで稼働中
  - グラフの時刻はUTC

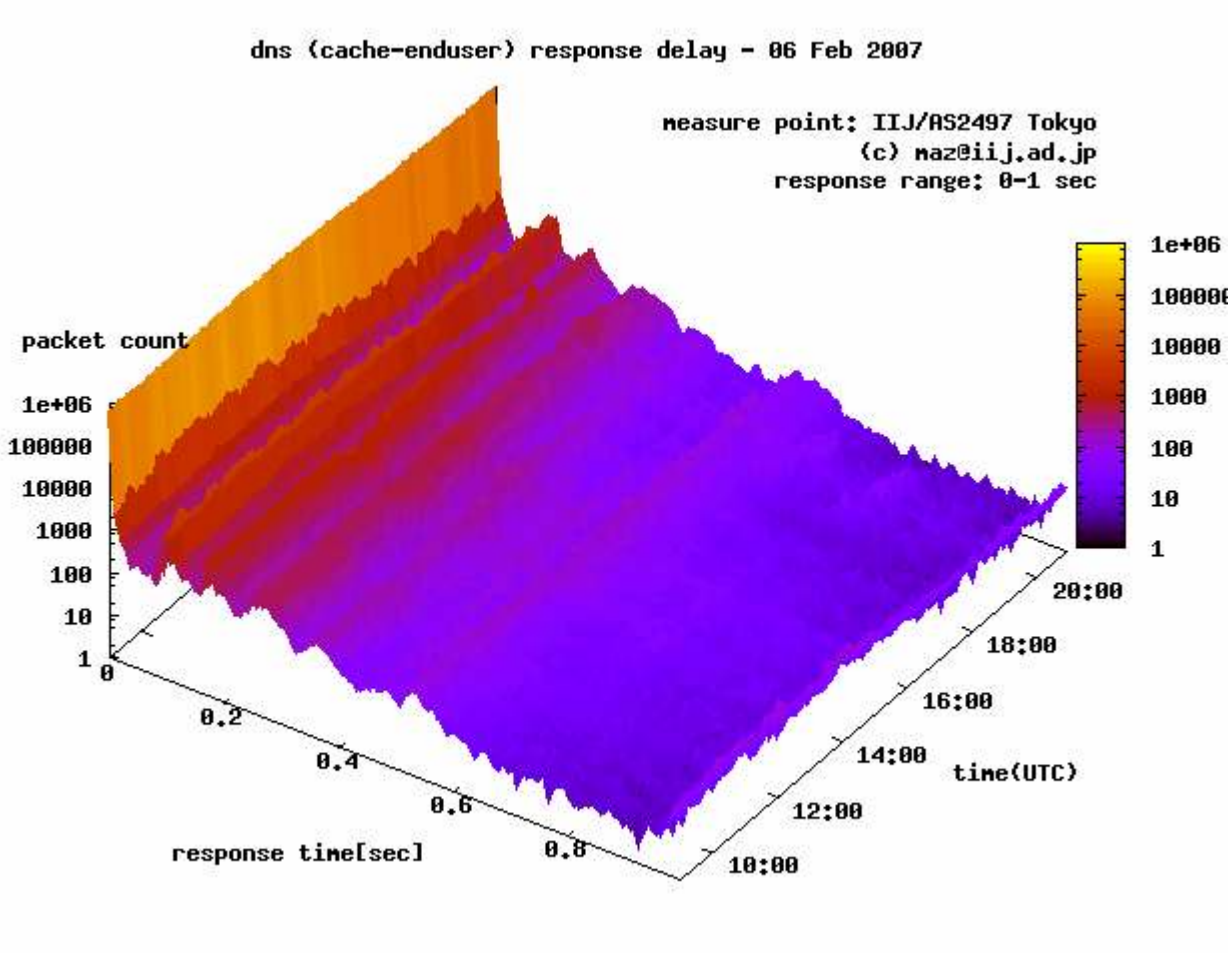
調査



応答遅延概要

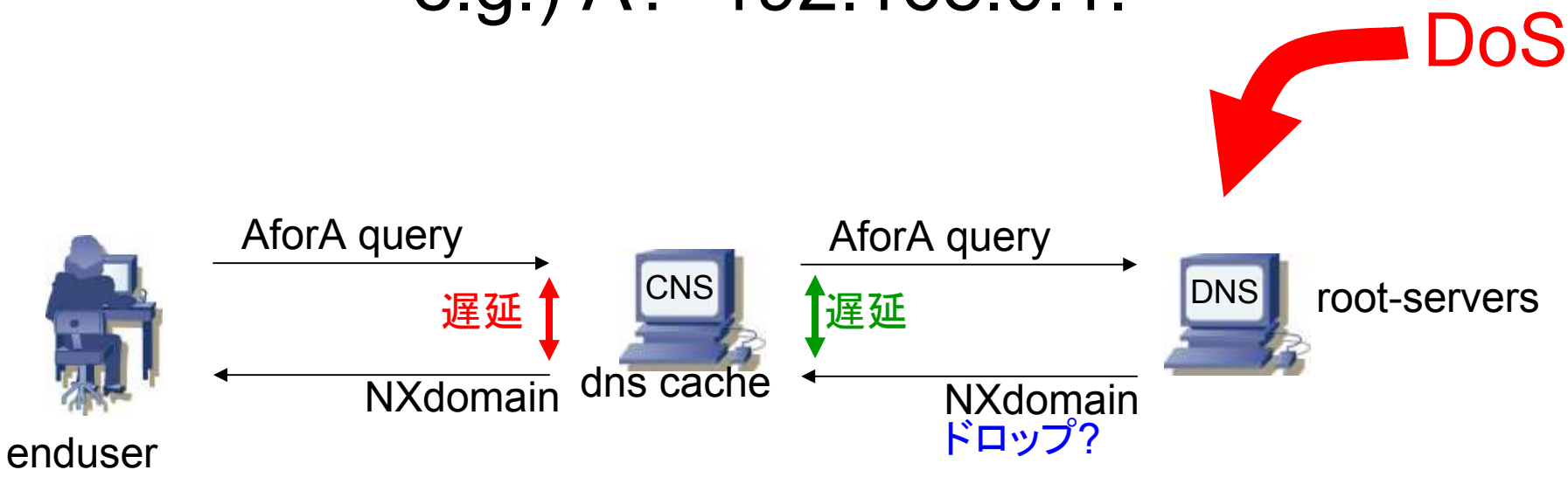


遅延1秒までを拡大



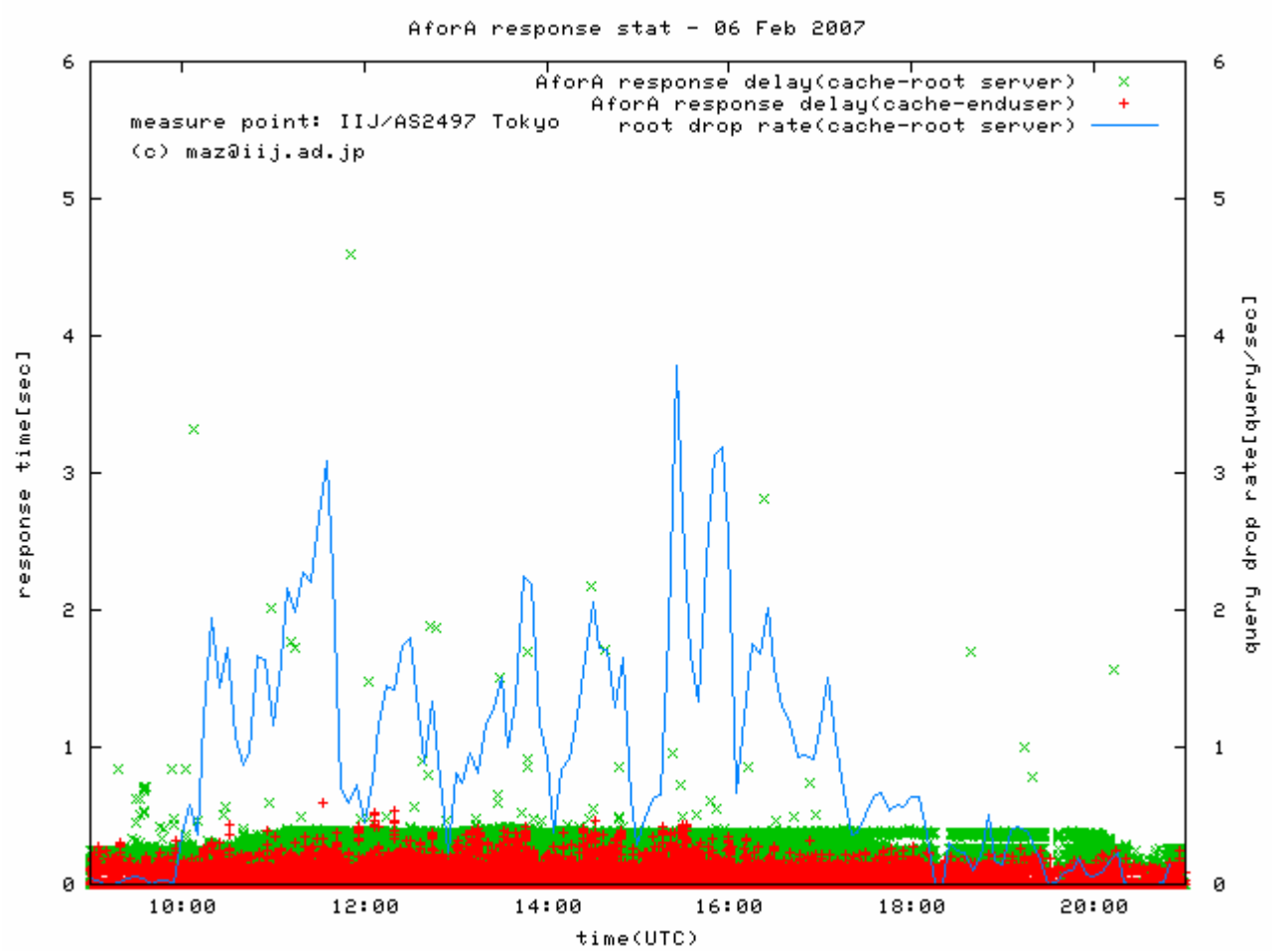
AforA

e.g.) A? 192.168.0.1.

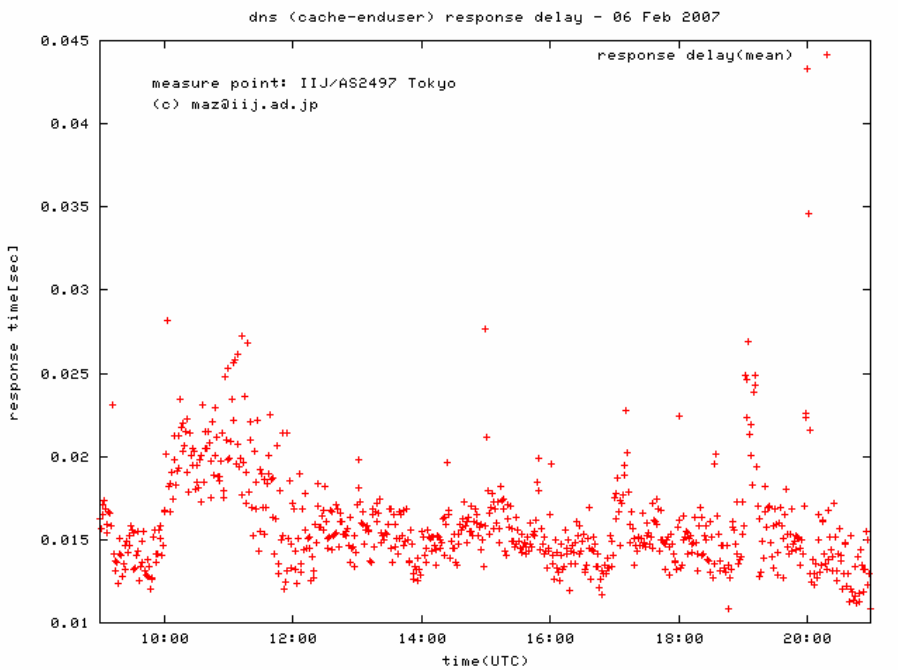


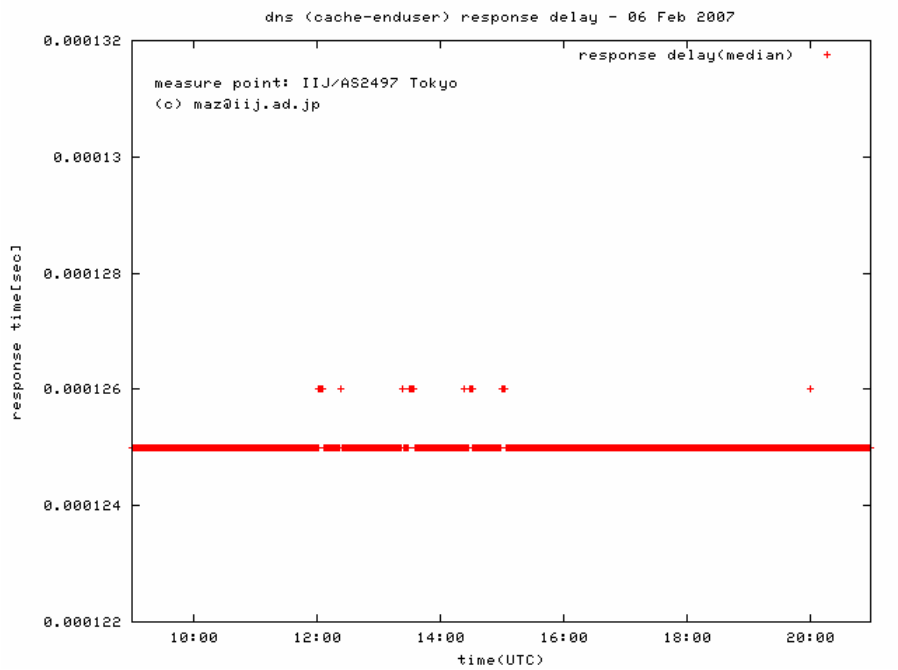
- AforAを計測すれば、rootの性能評価ができるかも

AforA query stat

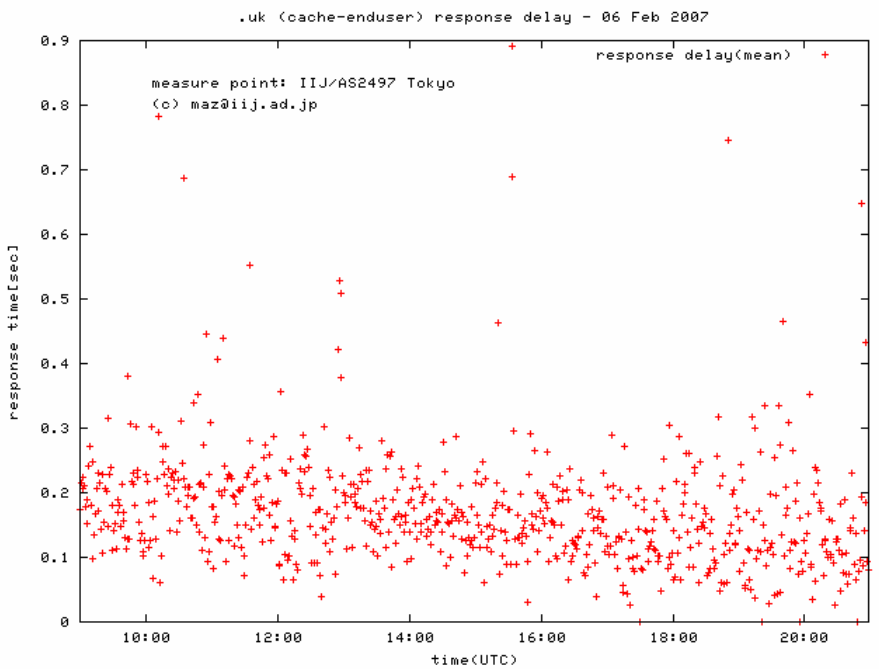


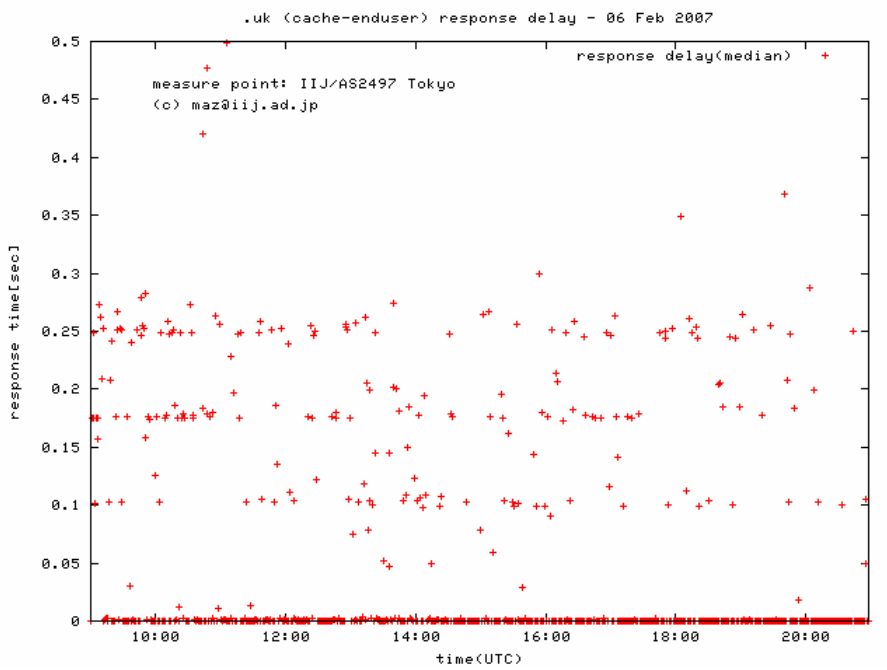
response delay - all recursive query



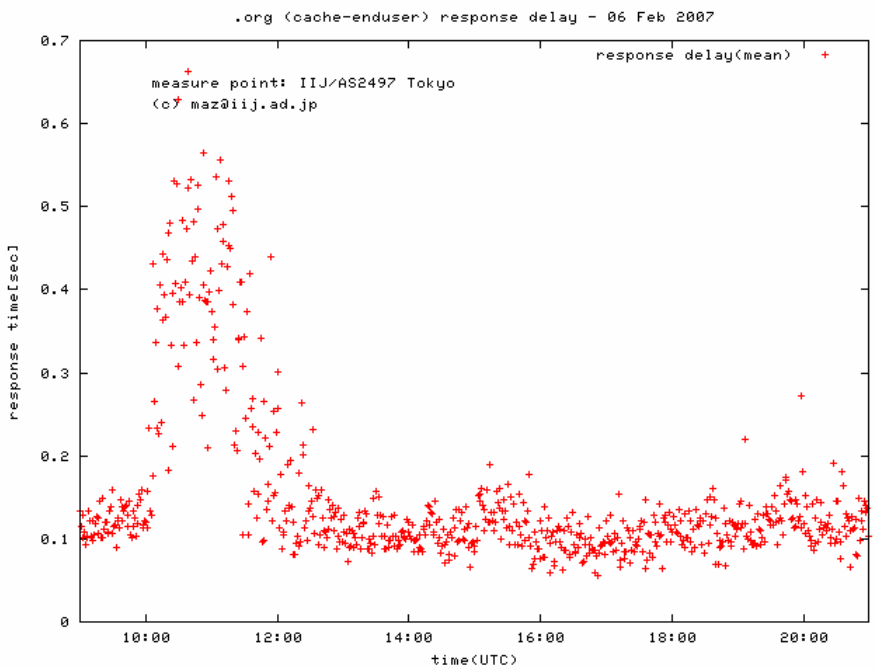


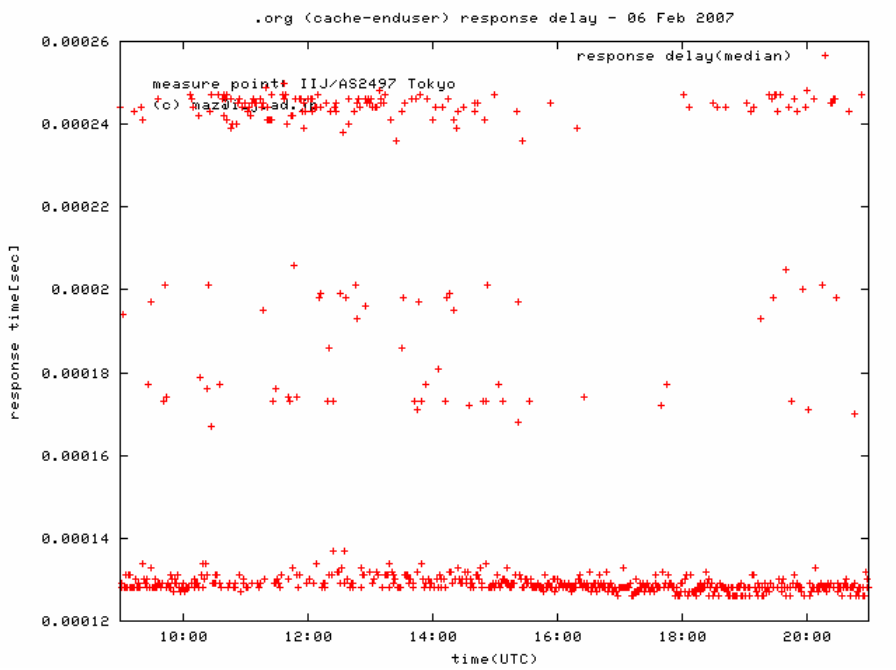
response delay - .uk query only



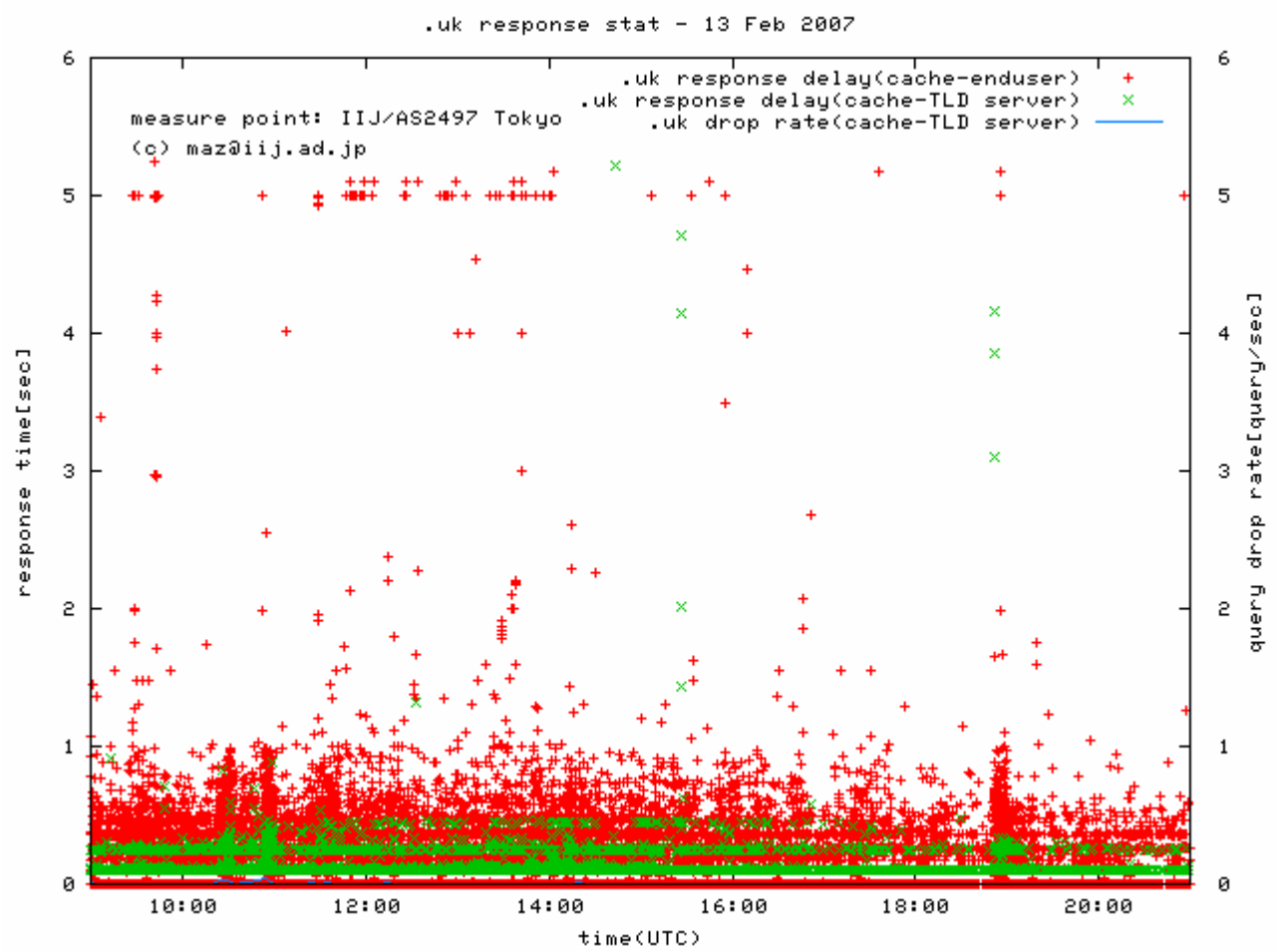


response delay - .org query only

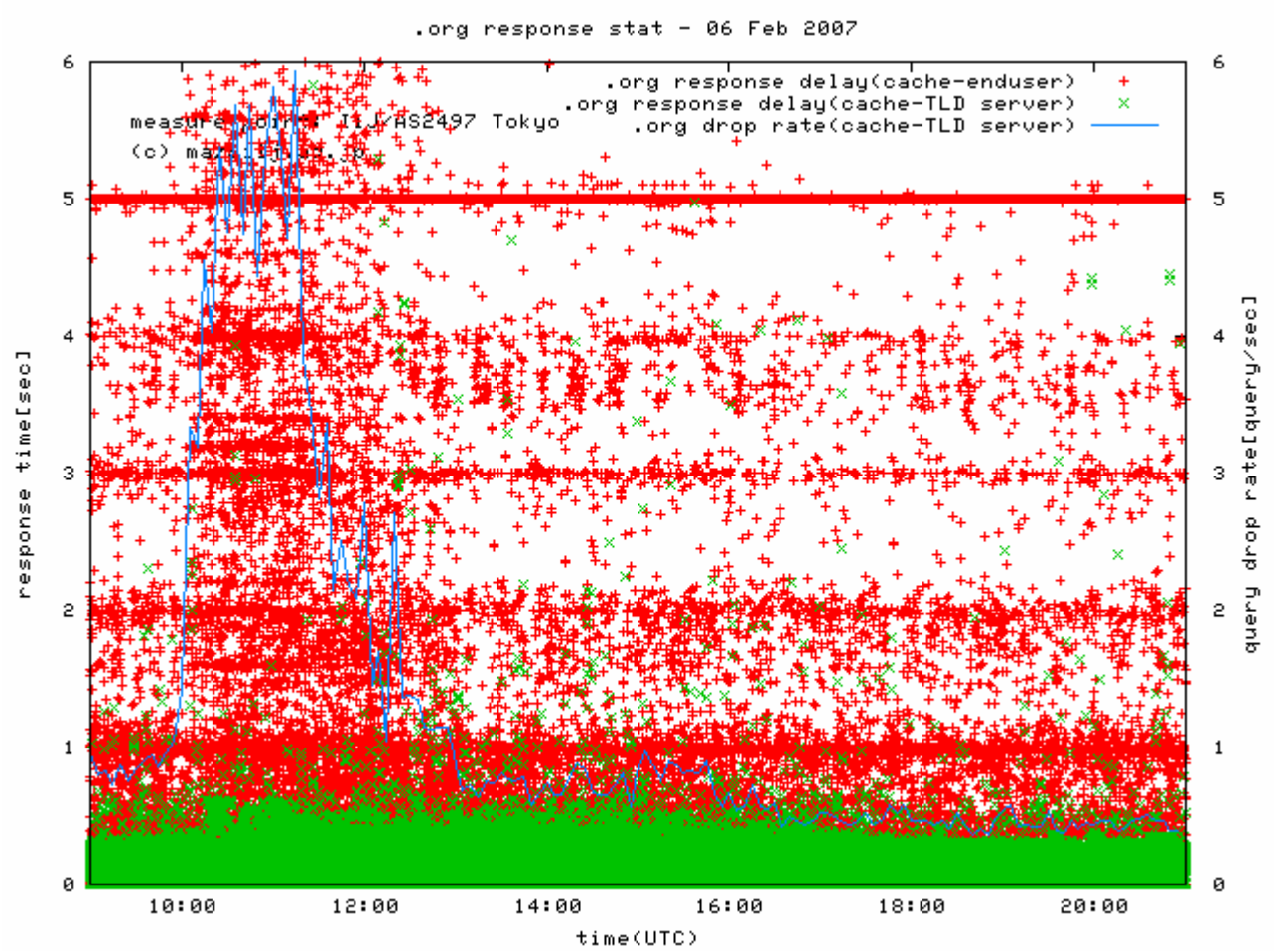




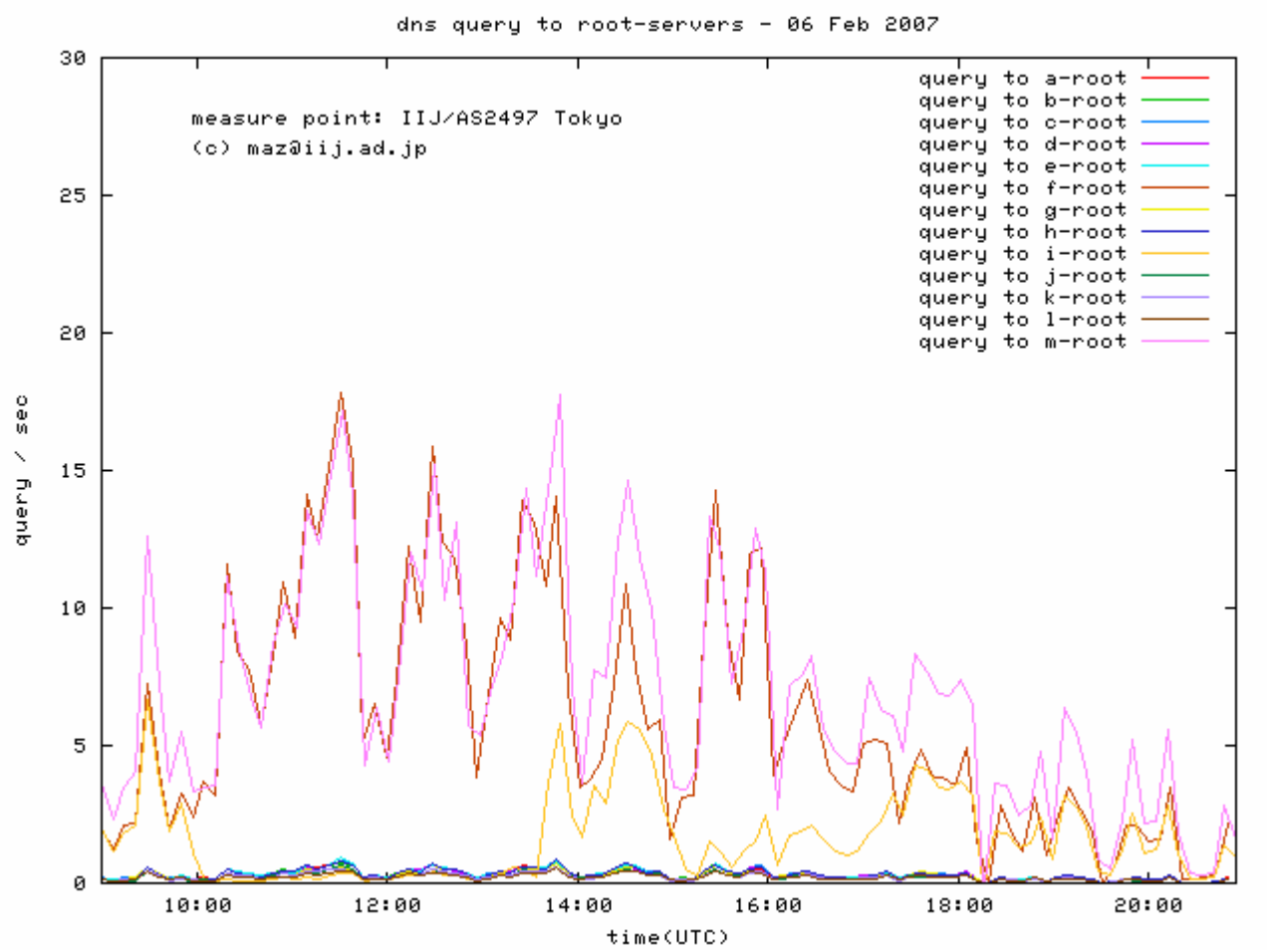
.uk query stat



.org query stat



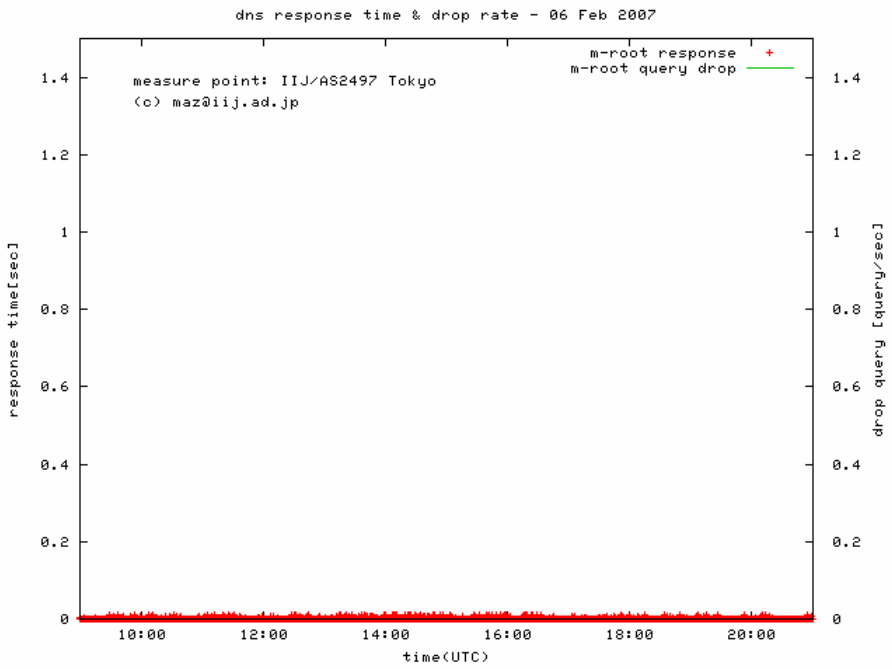
query to root-servers



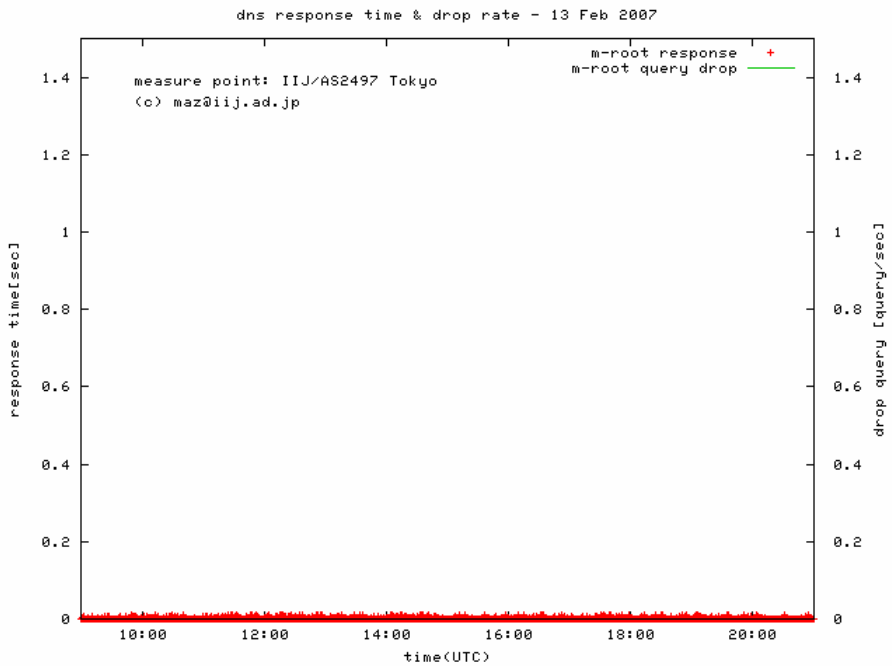
response delay of m.root

hostname.bind. - "M-NRT-JPNAP-3"

during attack

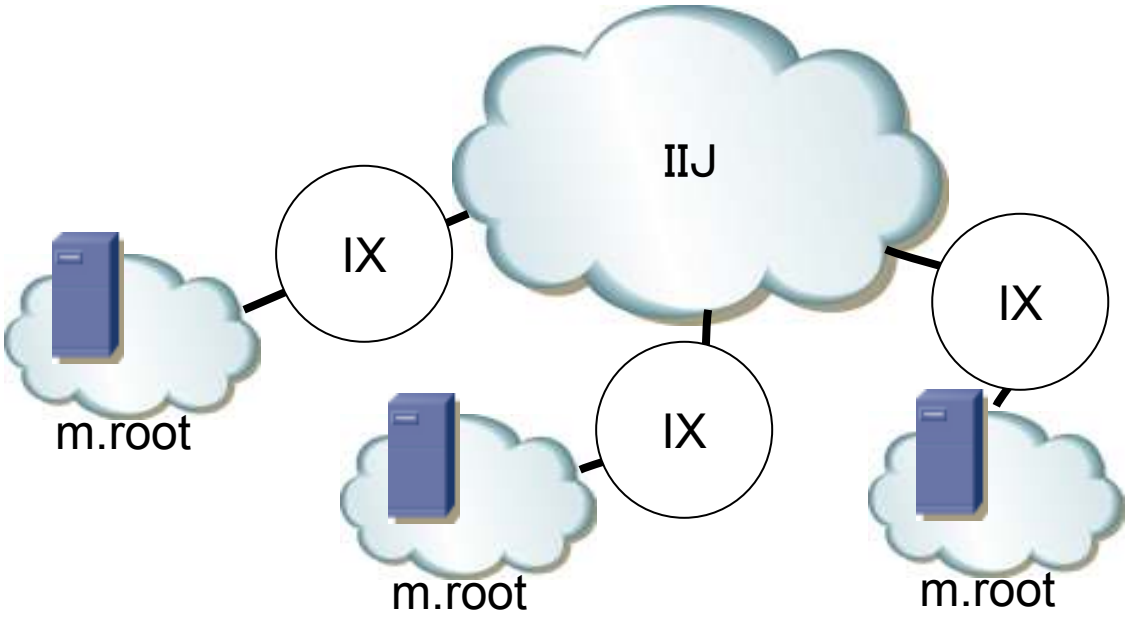


1 week later



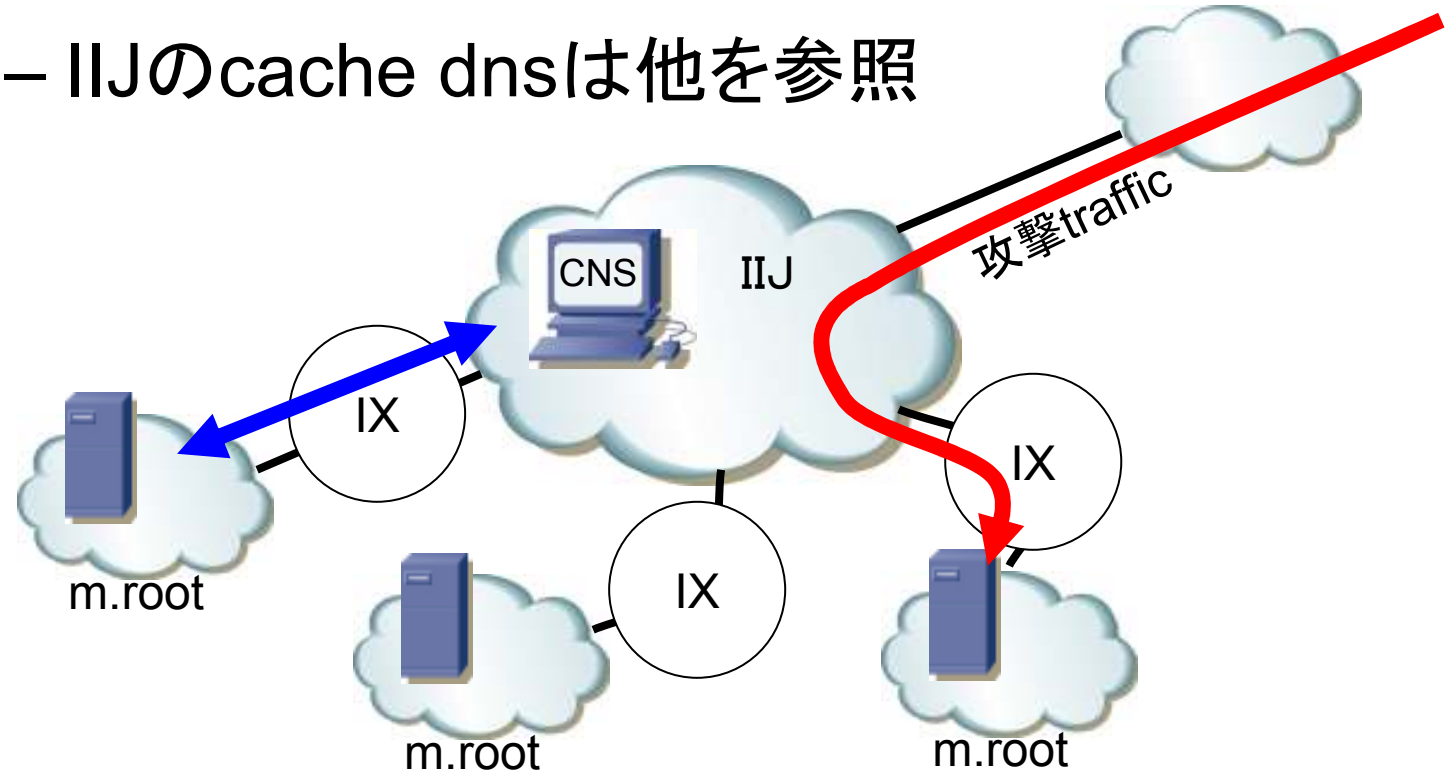
IIJとm.root

- m.rootのanycastサイトと複数接続
  - transitも提供してます



攻撃中

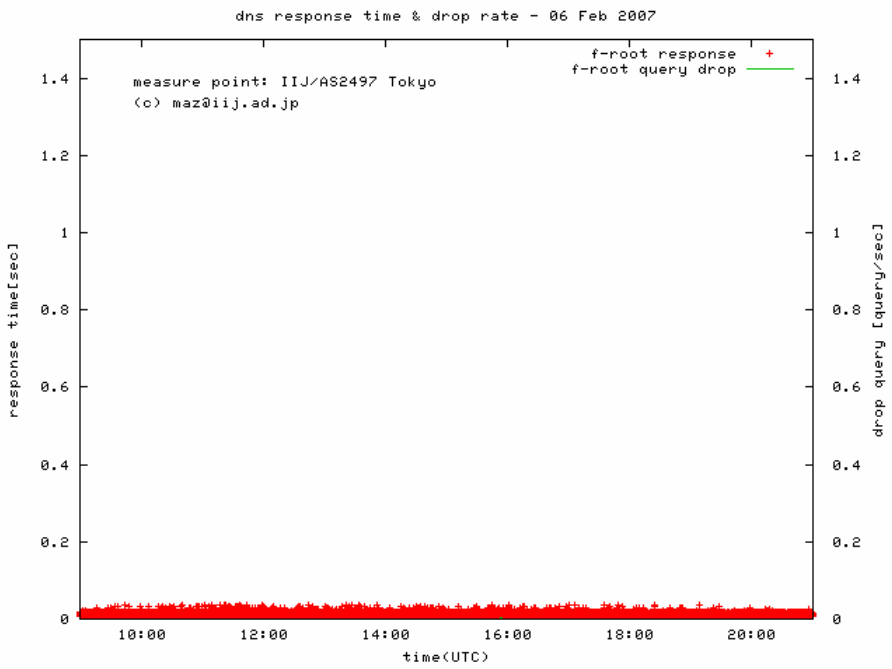
- 攻撃trafficもばっちりtransit
  - IIJのcache dnsは他を参照



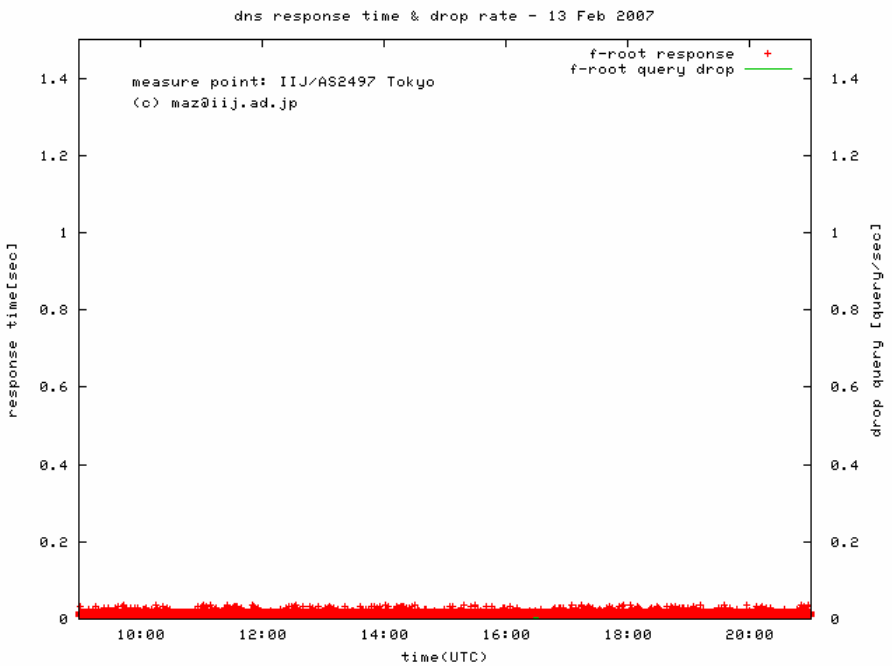
response delay of f.root

hostname.bind. - "kix1b.f.root-servers.org"

during attack



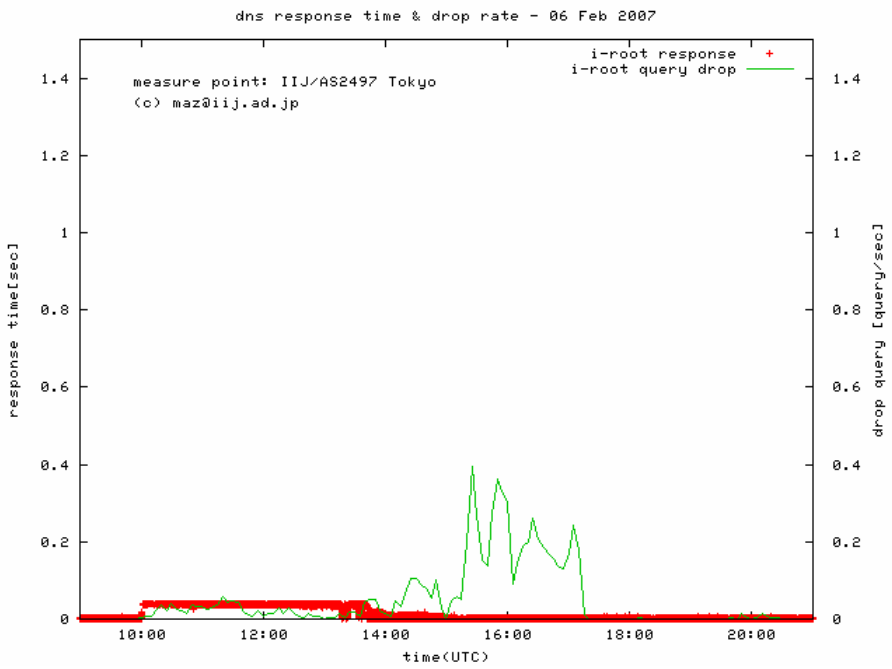
1 week later



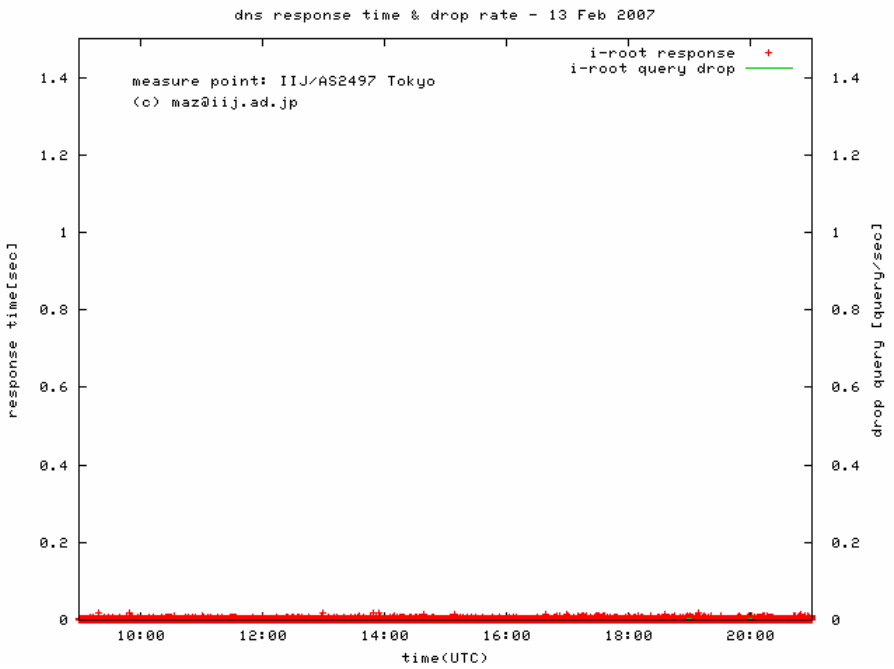
response delay of i.root

hostname.bind. - "s1.tok"

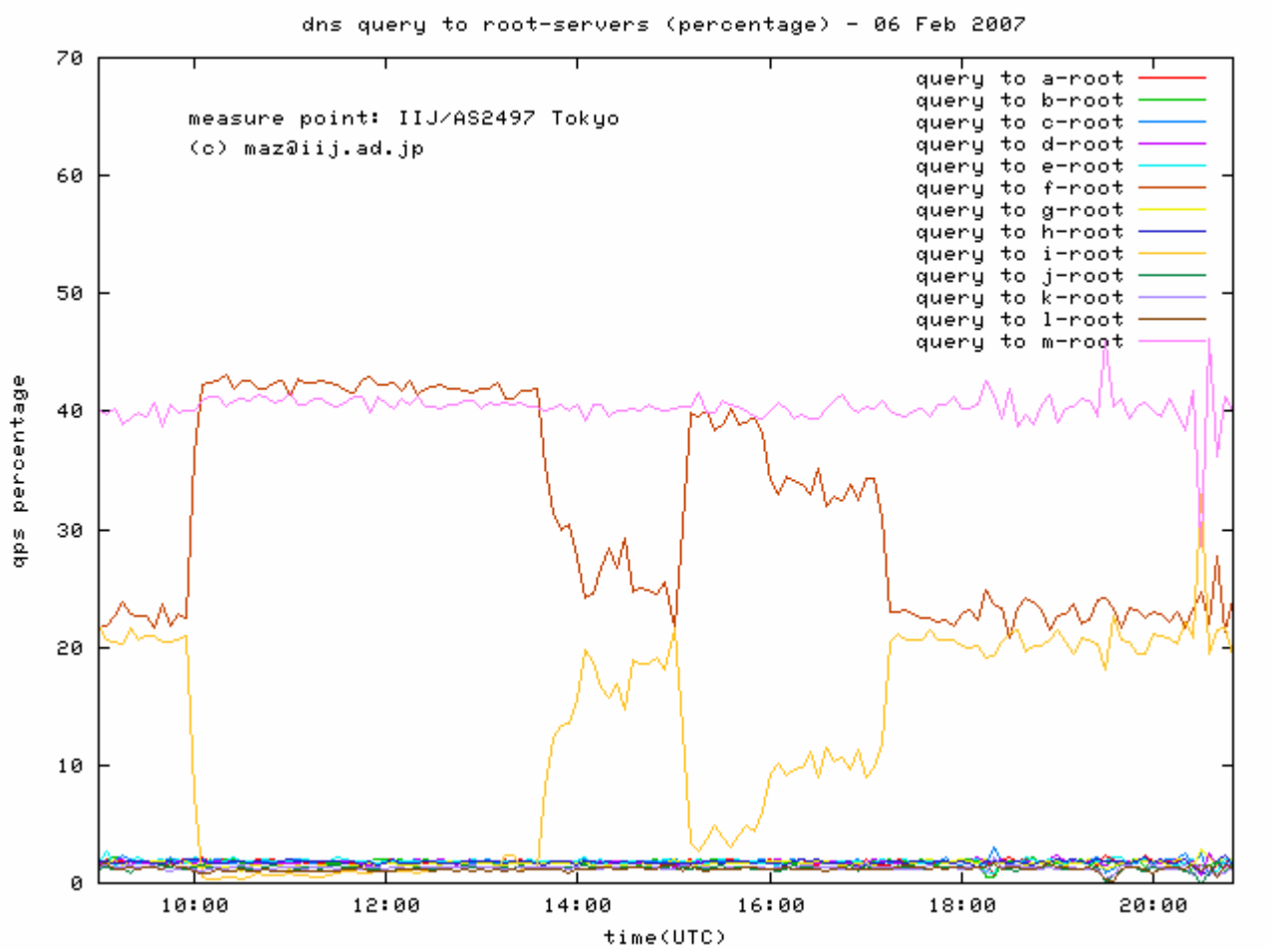
during attack



1 week later

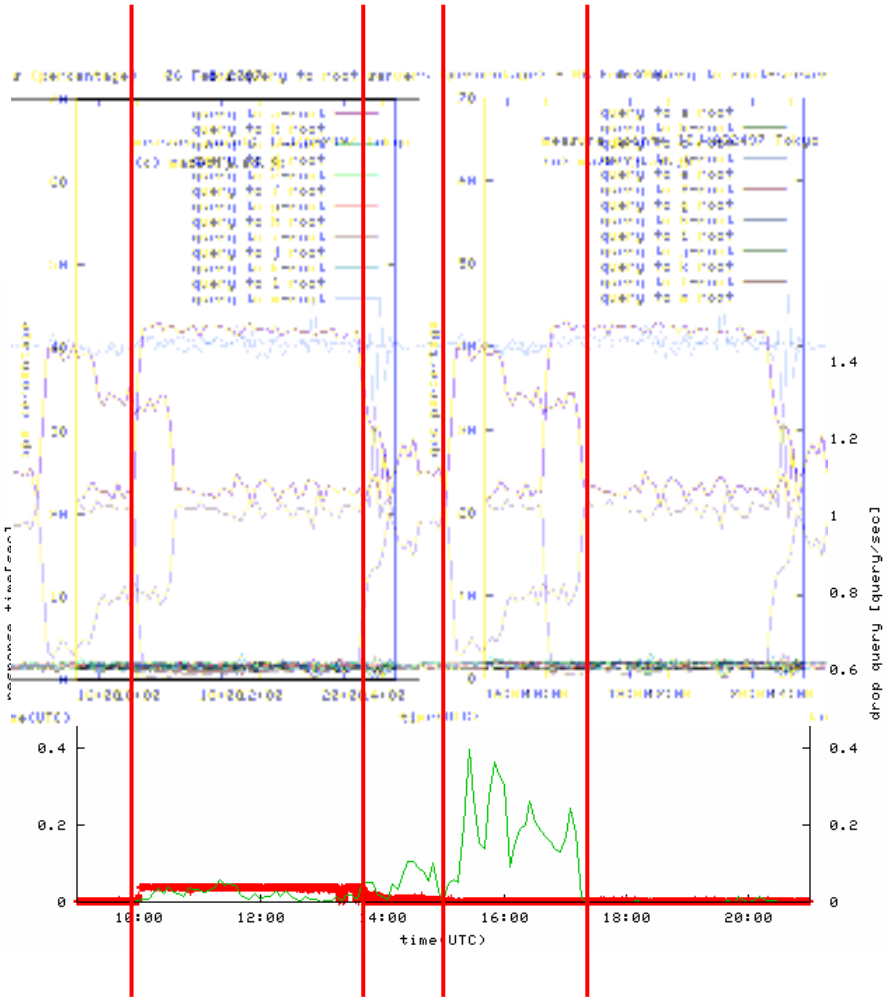


server selection



アプリケーションでの回復

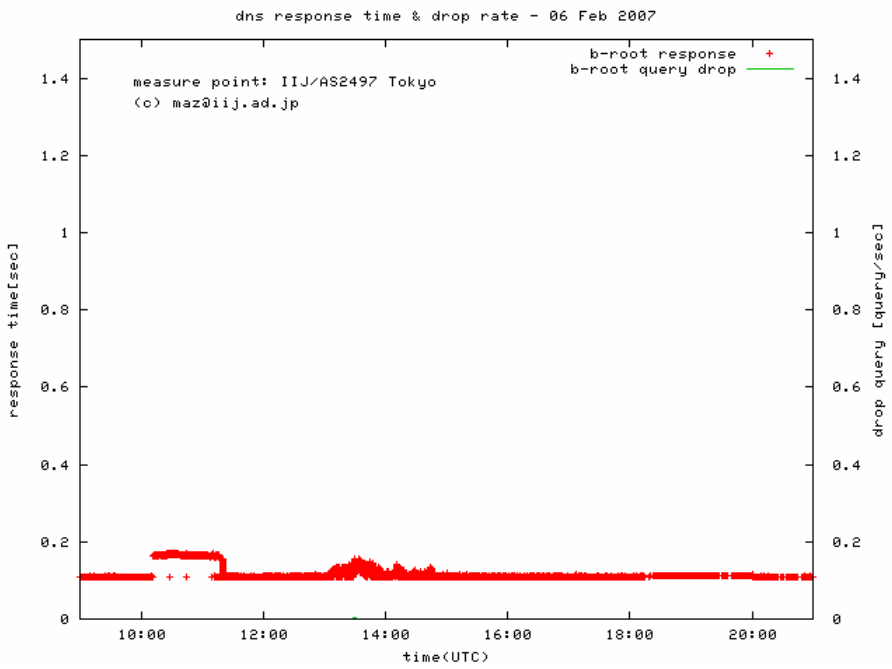
- 遅延/ロスが発生したサーバを回避して、大丈夫な人にqueryを向けちゃう
- 実装依存
  - BIND9では遅延を評価しているみたい
  - CNSでは、もうちょっと頑張っているらしい



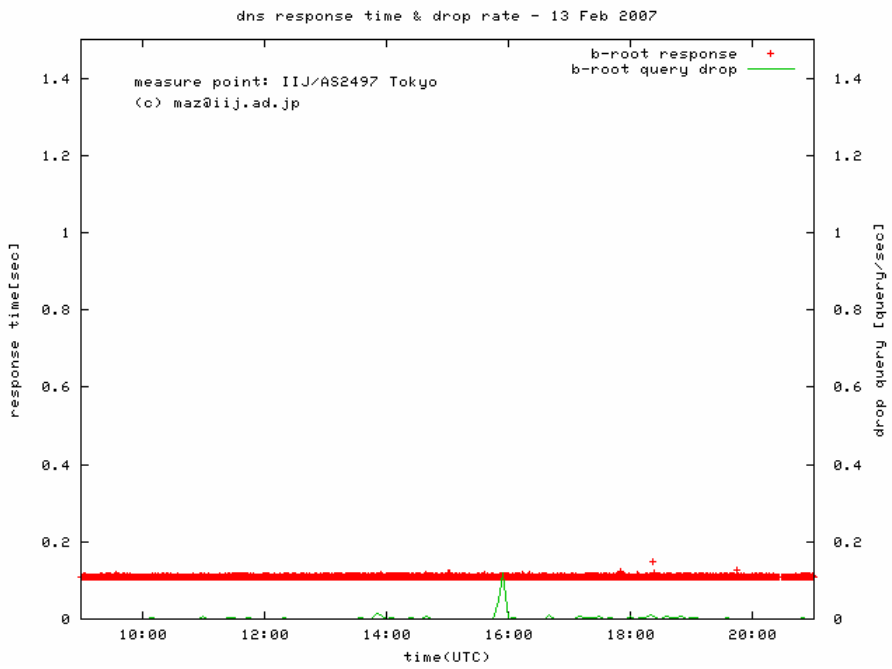
response delay of b.root

hostname.bind. - "b2"

during attack



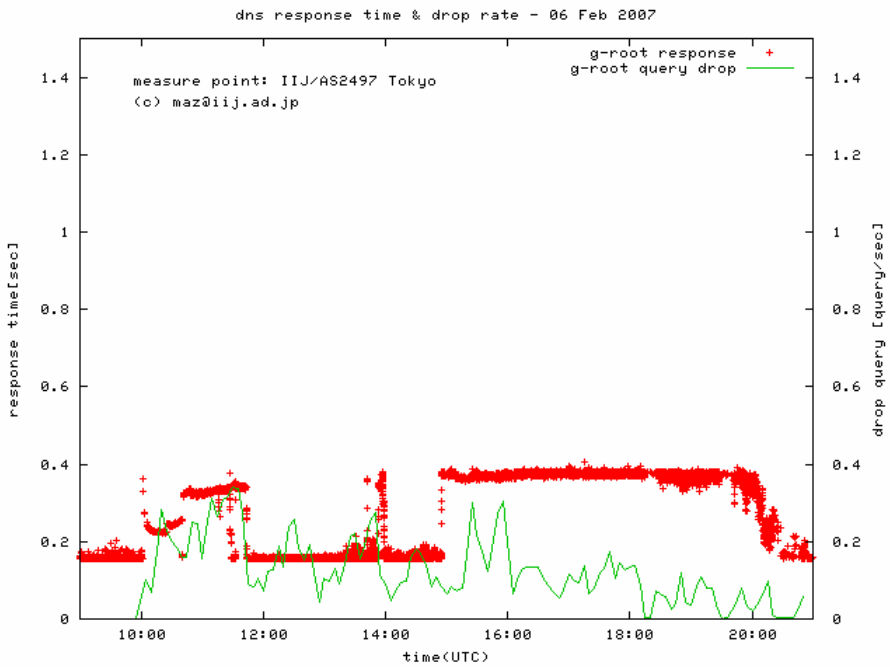
1 week later



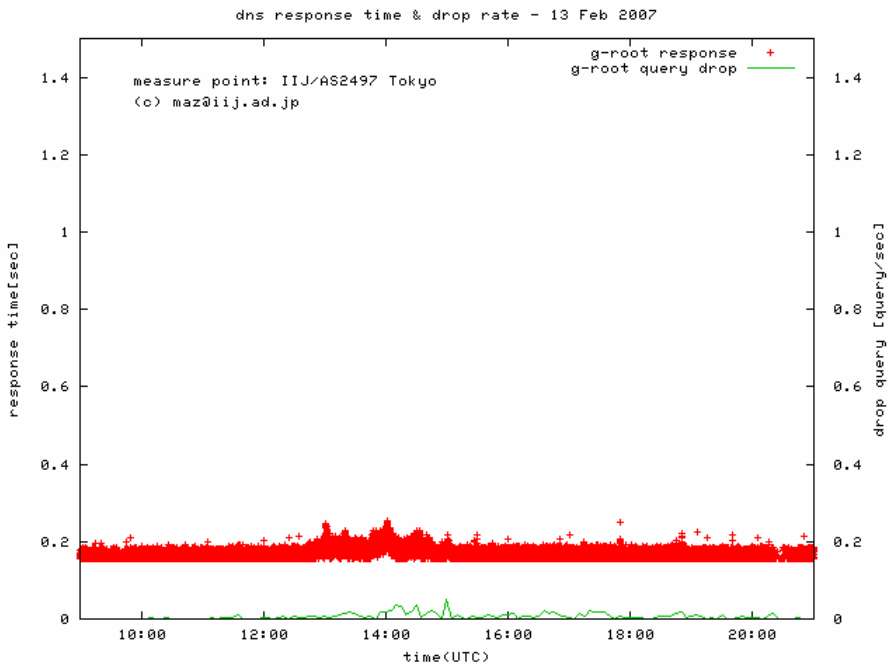
response delay of g.root

hostname.bind. - "g.root-servers2.net"

during attack



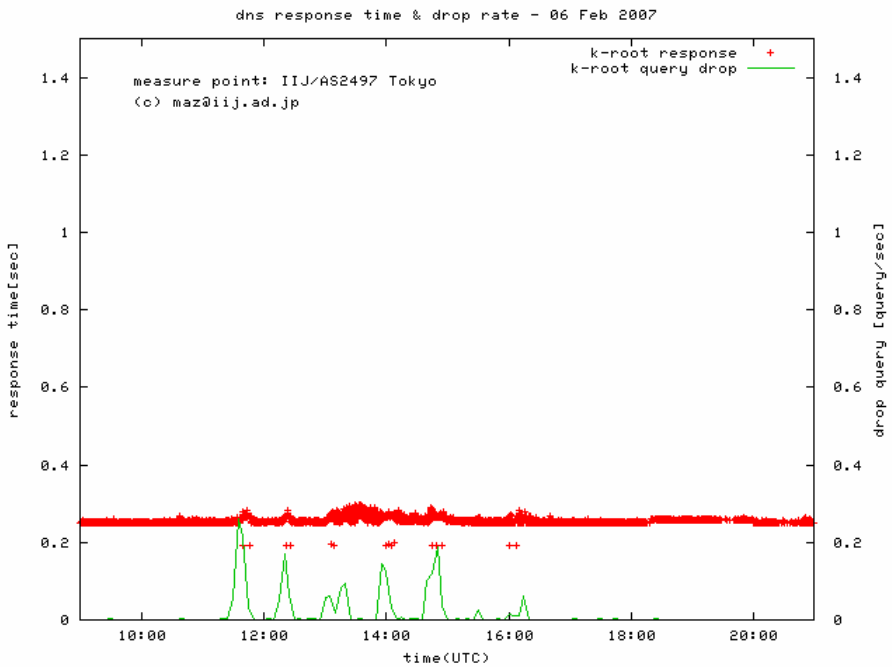
1 week later



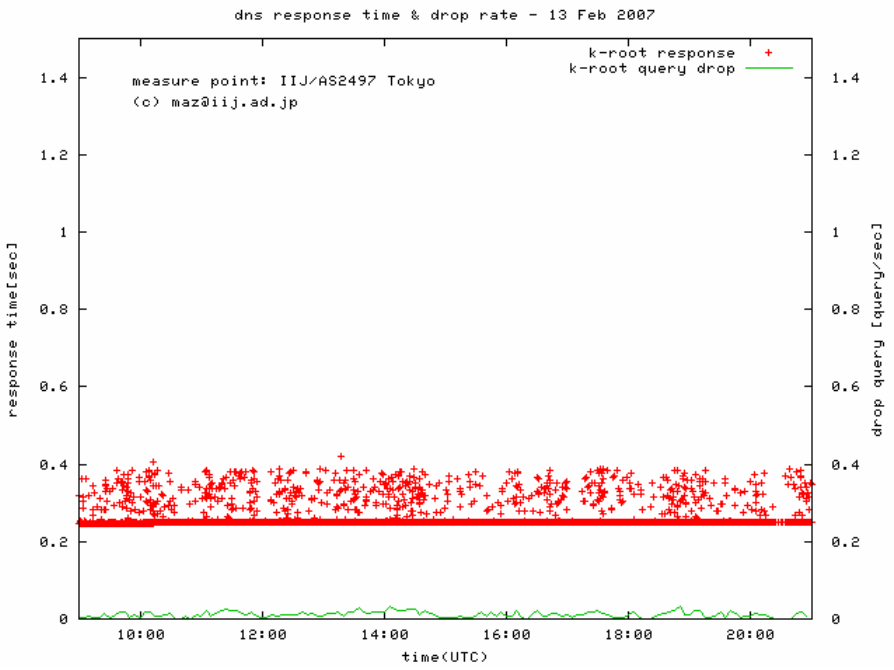
response delay of k.root

hostname.bind. - "k1.linx"

during attack



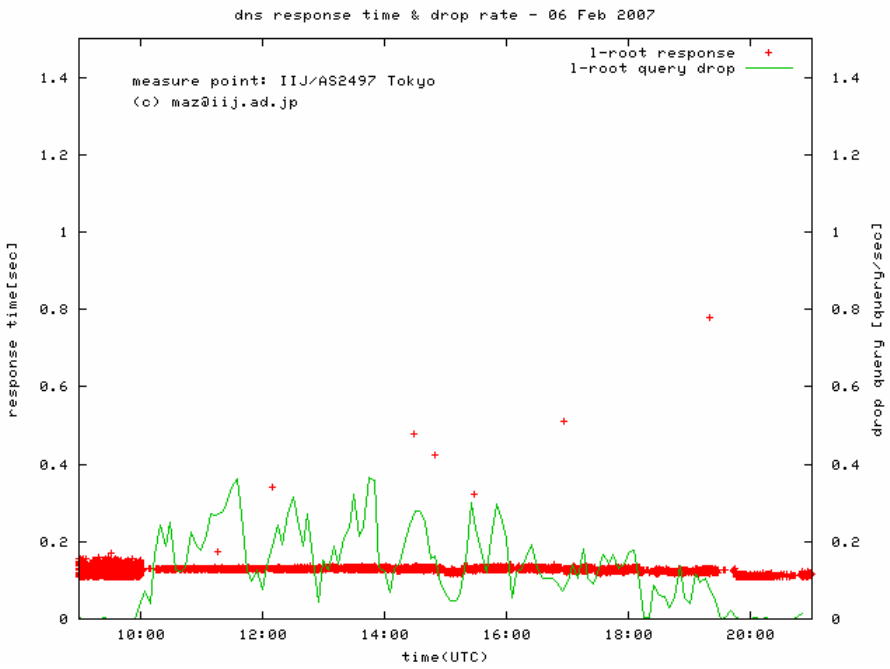
1 week later



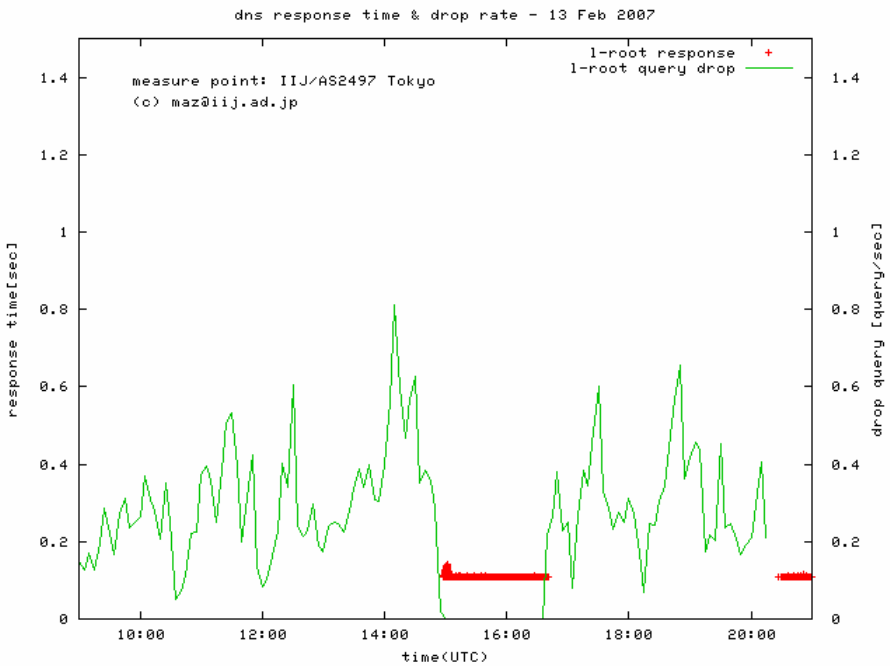
response delay of l.root...?

hostname.bind. - "lax-25"

during attack



1 week later



root-serversへのquery数・・・

- 1229097 total queries
  - 1223957 invalid_TLD (99.5%)
    - 1110543 AforA (90.3%)
    - 113414 other invalid_TLD (9.2%)
  - 5140 valid_TLD(0.4%)
    - 4787 .arpa (0.3%)
    - 353 other valid_TLD(0.02%)

期間 08 Feb 2007 09:00UTC-21:00UTC

まとめると

- root dnsへの攻撃がありましたが、影響は無視できるor影響があったとしても極軽微
  - anycastはうまく動いてた ☺
  - cacheサーバでのserver selectionはきちんと動いていて、自動的に影響の無いサーバを選択できた ☺
  - そもそも、キャッシュサーバがrootに対してqueryを投げるのはまれ

おわり