Track: DNS

Comcast DNS

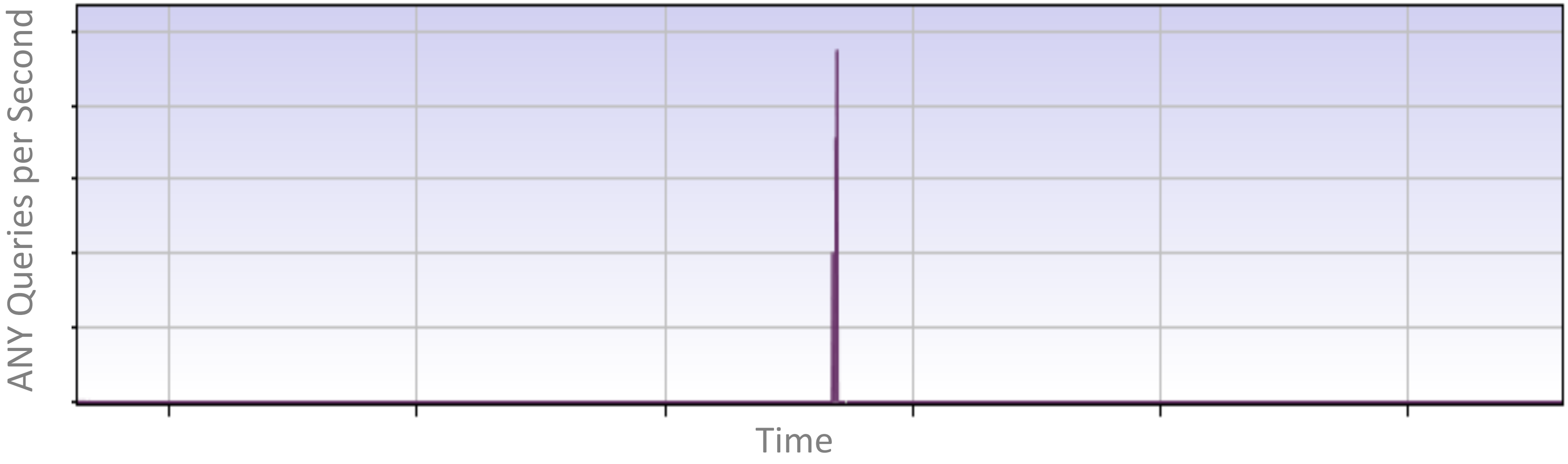
Monday, October 22, 2012

NATIONAL ENGINEERING & TECHNICAL OPERATIONS

DNS Amplification Attack – Application View

We recently identified an amplification attack attempt on one of our authoritative name server complexes.

- Details of Attack
  - ANY queries for a limited group of DNSSEC signed domains.
  - Queries contained spoofed source IPs.
  - Gradual increase in queries for more than 2 weeks.
  - Exponential spike in ANY queries lasting for 12 hours.
  - Attack subsided and traffic normalized.
  - No customer impact experienced for Comcast resolution.

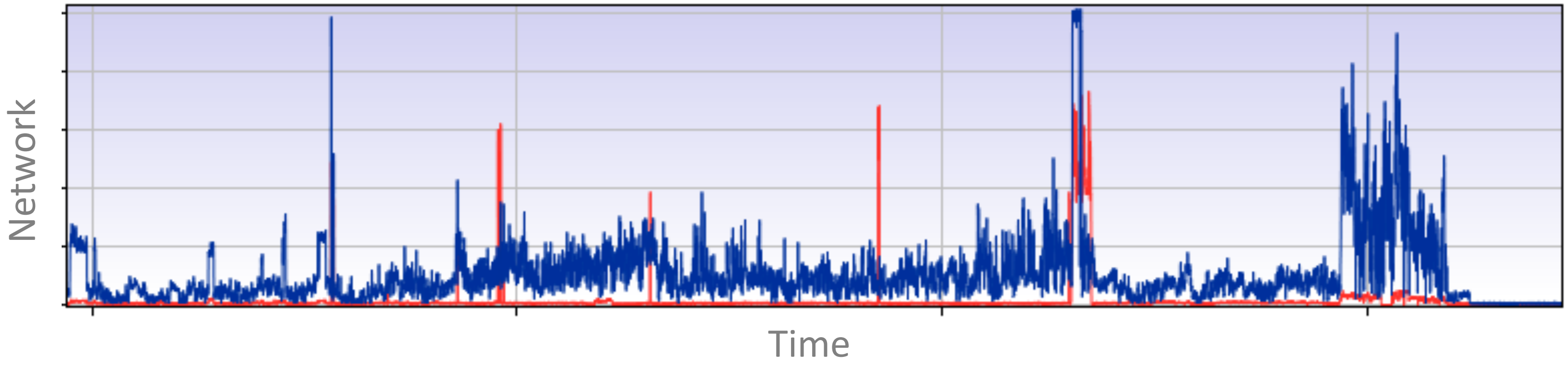


DNS Amplification Attack – Network View

Requests for an ANY query type for a DNSSEC signed domain versus a request for an A record request increased the amount of outbound traffic significantly. This is indicative of these types of attacks.

Red – Inbound Traffic

Blue – Outbound Traffic



DiG Example (ANY vs. A)

```
@dns101.comcast.net comcast.net +norecurse +dnssec ANY
;; MSG SIZE  rcvd: 4023 bytes

@dns101.comcast.net comcast.net +norecurse +dnssec A
;; MSG SIZE  rcvd: 2481 bytes
```

DNS Amplification Attack – Mitigation

We are faced with following questions:

- "What is the most efficient way to mitigate attacks without impacting time to service a query?"
- "How do we avoid blocking legitimate users when the source IP is spoofed?"
- "What is the appropriate query rate per query type per second per source IP?"

Mitigation

- Analyze normal peak query metrics and attack patterns.
- Review the capabilities of different rate limiting mechanisms.
  - Example: DNS Response Rate Limiting (RRL)

Thank You!

xfinity™

For more information on the Comcast DNS and IPv6 deployments:

http://dns.comcast.net
http://www.comcast6.net

Chris Ganster
chris_ganster@cable.comcast.com

Comcast®
NATIONAL ENGINEERING & TECHNICAL OPERATIONS