Goal

Understand the history, actors, and issues in the DNS Ecosystem.
Terminology Revision

TLDs / ccTLDs / gTLDs

Zone / Zone files

Recursive Resolver / Authoritative Nameserver

Anycast
DNS Hierarchical Namespace

- **DNS Root**: .
- **TLD**: com., edu., us.
- **Domain**: google.com
- **Subdomain**: www.google.com
DNS Administration: A Simplified History

- Before 1999, Department of Commerce, SRI-NIC, Network Solutions
- After 1999, Department of Commerce identified *Internet Corporation for Assigned Names and Numbers (ICANN)* to administer the DNS
  - gTLDs have to obey rules set forth by ICANN
  - ccTLD rules are determined by each country
- Department of Commerce NTIA gave up final control to ICANN in 2016
DNS Stakeholders

Registrant

Registrant is the domain owner.

Google
DNS Stakeholders

Registrar
Registrar handles registration of domains.

Registrant
Registrant is the domain owner.
DNS Stakeholders

**Registry**
Registry handles operations

**Registrar**
Registrar handles registration of domains.

**Registrant**
Registrant is the domain owner.
How to Get a Domain?

GoDaddy

Type the domain you want

Search Domain

Domain Names

Grab a .com for just $0.01*/1st yr

2-year purchase required*
How to Get a Domain?

Register a domain name to start

.COM only $6.98* .NET only $10.98
How to get your own TLD?

Apply for one [icann-newgtlds]! In 2012 it cost $185,000.

Blockchain DNS? Not official.

   No guarantees about future namespace collisions.
Discussion

Why have separate registrars and registries?
Life of a DNS Query

Client Stub Resolver

Recursive Resolver

Root Authoritative NS

TLD Authoritative NS

Domain Authoritative NS

cs.stanford.edu

Ask _edu Auth NS

cs.stanford.edu

Ask ns[1,2].stanford.edu

171.64.64.64

171.64.64.64

14
What role does the Registrar play?
Life of a DNS Query

Client Stub Resolver
171.64.64.64
cs.stanford.edu

Recursive Resolver
Ask ns[1,2].stanford.edu
cs.stanford.edu

Root Authoritative NS
Ask .edu Auth NS
cs.stanford.edu

TLD Authoritative NS

Domain Authoritative NS
Configuration Updates

- Client Stub Resolver
- Recursive Resolver
- Root Authoritative NS
- TLD Authoritative NS
- Domain Authoritative NS
- cs.stanford.edu
- 171.64.64.64
- Ask edu Auth NS
- Ask ns[1,2].stanford.edu
- Registry
- EPP Server
- Registrar
- Registrant
Ecosystem Threat Model

Parent Zone

Registry → Registrar

EPP

Registrar → Registrant

Web Portal / API

Child Zone
Ecosystem Threat Model

Parent Zone

Registry

Registrar

EPP

Child Zone

Registrar

Registrant

Web Portal / API

Registrant Compromise

Attacker can modify domains owned by the registrant
Ecosystem Threat Model

Parent Zone

Registry → Registrar

EPP

Registrar Compromise

Attackers typically compromise EPP credentials.

Attacker can modify *all* domains managed by the registrar.

Registrar → Registrant

Web Portal / API

Registrant Compromise

Attacker can modify domains owned by the registrant.

Child Zone
Ecosystem Threat Model

Parent Zone

Registry

Registrar Compromise
Attacker can modify *all* domains managed by the registrar.

Registrar

EPP

Web Portal / API

Registrar Compromise
Attacker can modify *all* domains managed by the registrar.

Registrant

Child Zone

Attacker can modify domains owned by the registrant.

Registry

Registry Compromise
Attacker can modify *all* domains in the TLDs managed by the registry.

Child Zone
The Problem: Attackers Targeting DNS Infrastructure

In 2014, Snecma (now Safran Aircraft Engine Company) targeted by attackers
Broader Context

- Part of a larger coordinated attack against aerospace companies.
Broader Context

- Part of a larger coordinated attack against aerospace companies.
- Use of many known tactics
  - Spear phishing
  - Malware
  - Doppelganger Domains
v. Domain Hijacking, the compromise of domain registrars in which one or more members of the conspiracy redirected a victim company’s domain name at a domain registrar to a malicious IP address in order to facilitate computer intrusions,
Domain Hijack In Practice

Client Logging Into “Secure” Network...

Client Stub Resolver → Recursive Resolver → secure.sneecma.fr

You are entering a restricted area

Please enter your userid and password

User id

Password

Connecter

Unauthorized access is prohibited and may result in prosecution under French law.
(Loi du 5 janvier 1988 art. 323-1)
Normal Resolution

Client Stub Resolver

Recursive Resolver

secure.sneccma.fr

secure.sneccma.fr

Root Authoritative NS

Ask for Auth NS
Normal Resolution

Client Stub Resolver → Recursive Resolver

Recursive Resolver → secure.sneecma.fr

Secure.sneecma.fr → Ask ns[1,2].sneecma.fr

Ask ns[1,2].sneecma.fr → Root Authoritative NS

Root Authoritative NS → TLD Authoritative NS

TLD Authoritative NS → secure.sneecma.fr

Secure.sneecma.fr → Ask fr Auth NS

Ask fr Auth NS → Root Authoritative NS
Normal Resolution
Normal Resolution

Client Stub Resolver

217.108.170.196

Recursive Resolver

secure.sneecma.fr

Ask fr Auth NS

secure.sneecma.fr

Ask ns[1,2].sneecma.fr

Root Authoritative NS

secure.sneecma.fr

TLD Authoritative NS

secure.sneecma.fr

Domain Authoritative NS

217.108.170.196
Normal Resolution

Client Stub Resolver

Recursive Resolver

217.108.170.196

secure.sneicma.fr

Ask fr Auth NS

secure.sneicma.fr

Root Authoritative NS

TLD Authoritative NS

Domain Authoritative NS
Malicious DNS Delegation Update (Circa 2014)
Attackers Target DNS Delegation Update Mechanism
Attackers Redirect All Users

- Attackers redirect all users to ns[1,2].acfine.net.
- Recursive Resolver contacts ns[1,2].acfine.net.
- Client Stub Resolver contacts secure.sneema.fr.
- Root Authoritative NS updates TLD Authoritative NS.
- Updates from Registrar to Registrant via EPP Server.
Attackers Redirect All Users

Client Stub Resolver

Recursive Resolver

secure.sneema.fr

Ask ns[1,2].acfine.net

67.198.195.126

Attacker controlled NS
Next Stage of Attack

- Prompt malicious downloads
- Mimic webpage to harvest credentials
What about TLS Certificates?

Your connection is not private

Attackers might be trying to steal your information from secure.snecma.fr (for example, passwords, messages, or credit cards). Learn more

NET:ERR_CERT_AUTHORITY_INVALID

Advanced

Back to safety
Implicit Trust Dependence

- TLS protects against AiTM (adversary-in-the-middle) attacks
- Automated TLS Certificate Issuance using “Domain Validation” uses DNS to authenticate domain “ownership”
Implicit Trust Dependence

- TLS protects against AiTM (adversary-in-the-middle) attacks
- Automated TLS Certificate Issuance using “Domain Validation” uses DNS to authenticate domain “ownership”
- Attacker controls DNS → can obtain TLS certificates for the domain
  - Malicious but legitimate!
**Implicit Trust Dependence**

- TLS protects against AiTM (adversary-in-the-middle) attacks
- Automated TLS Certificate Issuance using “Domain Validation” uses DNS to authenticate domain “ownership”
- Attacker controls DNS → can obtain TLS certificates for the domain
- Malicious but legitimate!

CT Logs allow for auditing!
Anatomy of a Targeted Domain Hijack

- Acquire ability to control DNS delegations
  - Hijacks characterized by multiple brief updates to evade detection
  - Attacker can bypass TLS, and DNSSEC protections
Anatomy of a Targeted Domain Hijack

- Acquire ability to control DNS delegations
  - Hijacks characterized by multiple brief updates to evade detection
  - Attacker can bypass TLS, and DNSSEC protections
- Set up infrastructure to mimic target domain
  - Infrastructure uses maliciously obtained TLS certificate
  - Practically, indistinguishable from legitimate infrastructure
Anatomy of a Targeted Domain Hijack

- Acquire ability to control DNS delegations
  - Hijacks characterized by multiple brief updates to evade detection
  - Attacker can bypass TLS, and DNSSEC protections
- Set up infrastructure to mimic target domain
  - Infrastructure uses maliciously obtained TLS certificate
  - Practically, indistinguishable from legitimate infrastructure
- Harvest credentials or compromise redirected users to infiltrate target organization
Learning New Tactics...

- Attack adapted from a previous attack targeting NYTimes.
- Attack targets the same registrar three months later.

The New York Times Web site was taken down by DNS hijacking. Here’s what that means.
Widespread DNS Hijacking Activity Targets Multiple Sectors

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale
Hijacked Domains (Retroactive Identification)

Identified 41 domains as hijacked (between 2017-2020)

- 33 domains re-identified and verified from previous reports
- 8 domains not previously identified

High confidence manually evaluated hijacks!

Many many more domains where there is circumstantial evidence
## Kyrgyzstan Hijacks

<table>
<thead>
<tr>
<th>Date</th>
<th>Domain</th>
<th>Target</th>
<th>Organization</th>
<th>Malicious IP</th>
<th>Malicious ASN</th>
<th>Geo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec'20</td>
<td>fiu.gov.kg</td>
<td>mail</td>
<td>Financial Intelligence Service</td>
<td>178.20.41.140</td>
<td>AS 48282</td>
<td>Russia</td>
</tr>
<tr>
<td>Dec'20</td>
<td>invest.gov.kg</td>
<td>mail</td>
<td>Investment Portal</td>
<td>94.103.90.182</td>
<td>AS 48282</td>
<td>Russia</td>
</tr>
<tr>
<td>Dec'20</td>
<td>mfa.gov.kg</td>
<td>mail</td>
<td>Ministry of Foreign Affairs</td>
<td>94.103.91.159</td>
<td>AS 48282</td>
<td>Russia</td>
</tr>
<tr>
<td>Jan'21</td>
<td>infocom.kg</td>
<td>mail</td>
<td>Internet Services Provider</td>
<td>195.2.84.10</td>
<td>AS 48282</td>
<td>Russia</td>
</tr>
</tbody>
</table>
To continue using the email service, you must install the security update:
Download Update
<table>
<thead>
<tr>
<th>Type</th>
<th>Hij.</th>
<th>Targeted Domain Information</th>
<th>Domain</th>
<th>Sub.</th>
<th>Cross Ref</th>
<th>Attacker Infra. (Transient)</th>
<th>Legitimate Infra. (Stable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>May'18</td>
<td>AE</td>
<td>nofa.gov.ac</td>
<td>webmail</td>
<td>146.185.143.158</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Sep'18</td>
<td>AE</td>
<td>adspice.gov.ac</td>
<td>advpm</td>
<td>185.20.187.8</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>T1*</td>
<td>Sep'18</td>
<td>AE</td>
<td>apc.gov.ac</td>
<td>mail</td>
<td>185.20.187.8</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>T2</td>
<td>Sep'18</td>
<td>AE</td>
<td>ngov.ac</td>
<td>mail</td>
<td>185.20.187.8</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Jan'18</td>
<td>AL</td>
<td>e-albania.al</td>
<td>ova</td>
<td>185.15.247.140</td>
<td>24961</td>
<td>DE</td>
</tr>
<tr>
<td>T2</td>
<td>Nov'18</td>
<td>AL</td>
<td>nsp.gov.ac</td>
<td>mail</td>
<td>199.247.3.191</td>
<td>20473</td>
<td>DE</td>
</tr>
<tr>
<td>T1</td>
<td>Nov'18</td>
<td>AL</td>
<td>shish.gov.ac</td>
<td>mail</td>
<td>37.139.11.155</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Dec'18</td>
<td>CY</td>
<td>govcld.gov.cy</td>
<td>personal</td>
<td>178.62.218.244</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>P-IP</td>
<td>Dec'18</td>
<td>CY</td>
<td>ova.gov.cy</td>
<td></td>
<td>178.62.218.244</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Dec'18</td>
<td>CY</td>
<td>webmail.gov.cy</td>
<td></td>
<td>178.62.218.244</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>P-IP</td>
<td>Jan'19</td>
<td>CY</td>
<td>cyta.com.cy</td>
<td>xbox</td>
<td>178.62.218.244</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Jan'19</td>
<td>CY</td>
<td>selvpm.gov.cy</td>
<td></td>
<td>178.62.218.244</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Feb'19</td>
<td>CY</td>
<td>defa.com.cy</td>
<td>mail</td>
<td>108.61.123.149</td>
<td>20473</td>
<td>FR</td>
</tr>
<tr>
<td>T1</td>
<td>Nov'18</td>
<td>EG</td>
<td>nsf.gov.ee</td>
<td>mail</td>
<td>188.166.119.57</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T2</td>
<td>Nov'18</td>
<td>EG</td>
<td>nod.gov.ee</td>
<td>mail</td>
<td>188.166.119.57</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T2</td>
<td>Nov'18</td>
<td>EG</td>
<td>nni.gov.ee</td>
<td>mail</td>
<td>188.166.119.57</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Nov'18</td>
<td>EG</td>
<td>petroleum.gov.ee</td>
<td>mail</td>
<td>206.221.184.133</td>
<td>20473</td>
<td>US</td>
</tr>
<tr>
<td>T1</td>
<td>Apr'19</td>
<td>GR</td>
<td>kyvernisi.gr</td>
<td></td>
<td>95.179.131.225</td>
<td>20473</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Apr'19</td>
<td>GR</td>
<td>nfa.gr</td>
<td>pop3</td>
<td>95.179.131.225</td>
<td>20473</td>
<td>NL</td>
</tr>
<tr>
<td>T2</td>
<td>Sep'18</td>
<td>IQ</td>
<td>nofs.gov.iq</td>
<td>mail</td>
<td>82.196.9.10</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>P-IP</td>
<td>Nov'18</td>
<td>IQ</td>
<td>inc-vrdl.iq</td>
<td></td>
<td>199.247.3.191</td>
<td>20473</td>
<td>DE</td>
</tr>
<tr>
<td>P-NS</td>
<td>Dec'18</td>
<td>JO</td>
<td>gid.gov.jo</td>
<td></td>
<td>139.162.144.139</td>
<td>63949</td>
<td>DE</td>
</tr>
<tr>
<td>P-NS</td>
<td>Dec'20</td>
<td>KG</td>
<td>fti.gov.kg</td>
<td>mail</td>
<td>178.20.41.140</td>
<td>48282</td>
<td>RU</td>
</tr>
<tr>
<td>T1</td>
<td>Dec'20</td>
<td>KG</td>
<td>invest.gov.kg</td>
<td></td>
<td>94.103.90.182</td>
<td>48282</td>
<td>RU</td>
</tr>
<tr>
<td>T1</td>
<td>Dec'20</td>
<td>KG</td>
<td>nfa.gov.kg</td>
<td>mail</td>
<td>94.103.91.159</td>
<td>48282</td>
<td>RU</td>
</tr>
<tr>
<td>P-NS</td>
<td>Jan'21</td>
<td>KG</td>
<td>infocon.kg</td>
<td></td>
<td>195.2.84.10</td>
<td>48282</td>
<td>RU</td>
</tr>
<tr>
<td>T1</td>
<td>Dec'17</td>
<td>KW</td>
<td>cab.gov.kw</td>
<td>mail</td>
<td>82.102.14.232</td>
<td>20860</td>
<td>GB</td>
</tr>
<tr>
<td>P-IP</td>
<td>Dec'18</td>
<td>KW</td>
<td>dgos.gov.kw</td>
<td>mail</td>
<td>185.15.247.140</td>
<td>24961</td>
<td>DE</td>
</tr>
<tr>
<td>T1*</td>
<td>Apr'19</td>
<td>KW</td>
<td>moh.gov.kw</td>
<td>webmail</td>
<td>91.132.139.200</td>
<td>9009</td>
<td>AT</td>
</tr>
<tr>
<td>T2</td>
<td>May'19</td>
<td>KW</td>
<td>kicok.com.kw</td>
<td>mail2010</td>
<td>91.132.139.200</td>
<td>9009</td>
<td>US</td>
</tr>
<tr>
<td>P-IP</td>
<td>Nov'18</td>
<td>LB</td>
<td>finance.gov.lb</td>
<td>webmail</td>
<td>185.20.187.8</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>P-IP</td>
<td>Nov'18</td>
<td>LB</td>
<td>nes.com.lb</td>
<td>news</td>
<td>185.20.187.8</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Nov'18</td>
<td>LB</td>
<td>medgulf.com.lb</td>
<td>mail</td>
<td>185.161.209.147</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Nov'18</td>
<td>LB</td>
<td>pcm.gov.lb</td>
<td>mail</td>
<td>185.20.187.8</td>
<td>50673</td>
<td>NL</td>
</tr>
<tr>
<td>P-IP</td>
<td>Oct'18</td>
<td>LY</td>
<td>embassy.ly</td>
<td></td>
<td>188.166.119.57</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>P-NS</td>
<td>Oct'18</td>
<td>LY</td>
<td>foreign.ly</td>
<td></td>
<td>188.166.119.57</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Oct'18</td>
<td>LY</td>
<td>soc.ly</td>
<td>mail</td>
<td>188.166.119.57</td>
<td>14061</td>
<td>NL</td>
</tr>
<tr>
<td>T1</td>
<td>Jan'18</td>
<td>NL</td>
<td>ocom.com</td>
<td>connect</td>
<td>147.75.205.145</td>
<td>54825</td>
<td>US</td>
</tr>
<tr>
<td>P-NS</td>
<td>Jan'19</td>
<td>SE</td>
<td>netnod.se</td>
<td>dnsnodeapi</td>
<td>139.59.134.216</td>
<td>14061</td>
<td>DE</td>
</tr>
<tr>
<td>T1</td>
<td>Mar'19</td>
<td>SY</td>
<td>syrjistel.sy</td>
<td>mail</td>
<td>45.77.137.65</td>
<td>20473</td>
<td>NL</td>
</tr>
<tr>
<td>P-NS</td>
<td>Dec'18</td>
<td>US</td>
<td>pch.net</td>
<td>kerio2mail</td>
<td>159.89.101.204</td>
<td>14061</td>
<td>DE</td>
</tr>
</tbody>
</table>
THE DNS

IS DARK AND FULL OF TERRORS
Discussion: Integrity

Can DNS responses be modified?
Can one tell if the responses are modified?
Does it matter if they are modified?
Discussion: Integrity

Can DNS responses be modified?
Can one tell if the responses are modified?
Does it matter if they are modified?
SSL Certificates to the rescue(?)!
DNS Interception

● Intercept DNS Queries
  ○ Exploit lack of integrity check on DNS responses

● Interception by whom?
  ○ ISPs
  ○ Governments
  ○ Companies

● Interception where?
Where can Interception occur?

Client Stub Resolver

Recursive Resolver

Root Authoritative NS

.edu TLD Authoritative NS

UCSD Authoritative NS

sysnet.ucsd.edu?

Ask edu Auth NS

sysnet.ucsd.edu?

Ask ns[1,2]ucsd.edu

137.110.222.10
Where can Interception occur?
DNS Interception: Why?

- Censorship
- Parental Controls/Firewalls/Security
- Advertising
  - Take over NXDOMAIN queries.
You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.

What are potential root causes?
It's not DNS
There's no way it's DNS
It was DNS
Discussion

You own a domain *example.com*.

- Webpage on [www.example.com](http://www.example.com) does not load
- You see your mail at [you@example.com](mailto:you@example.com) stop.

What are potential root causes?

- **Lame Delegation**
  - Typo in A/NS Records
  - Misconfiguration
  - example.com NS not working
  - IP addresses unreachable
- **Domain expired?**
- **Hijack?**
DNS Cache Poisoning

- Attack that exploits implementation
- Vulnerability in old implementations
  - Client used same UDP Port
  - If attacker guessed 16 bit ID then they could poison cache.
  - “Fixed” by randomizing UDP source port.
Discussion

You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.
- The authoritative nameservers have changed.

Potential root causes?
Discussion

You own a domain *example.com*.

- **Webpage on** [www.example.com](http://www.example.com) **does not load**
- You see your mail at *[you@example.com](mailto:you@example.com)* stop.
- The authoritative nameservers have changed.
- You cannot log into your registrar account.

How did the hijackers hijack it?
Discussion

You own a domain *example.com*.

- Webpage on [www.example.com](http://www.example.com) does not load
- You see your mail at [you@example.com](mailto:you@example.com) stop.
- The authoritative nameservers have changed.
- You cannot log into your registrar account.

How did the hijackers hijack it? -- Registrars!
Discussion

You own a domain example.com.

- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.
- The authoritative nameservers have changed.
- You cannot log into your registrar account.

How did the hijackers hijack it? -- Registrars!

What do attackers do to offload the domain?
timeouts
bad certs
intermittent API failures
mystery service errors
Wait, it's all DNS?
Always has been
More DNS
DNS Tunneling

- DNS is typically not blocked at organizational firewall
- Some organizations block .xyz TLD
  - But do not block DNS queries
- Can use DNS queries to exfiltrate data!
Alternative Root
Blockchain DNS