Risky BIZness
Risks Derived from Registrar Name Management

Applied Networking Research Prize | IETF 115 London
9th November 2022

Gautam Akiwate, Stefan Savage, Geoffrey M. Voelker, KC Claffy
Story of how well-meaning standards can encourage operational practices that lead to issues.

Link to Risky BIZness Paper
Mystery #1: Nameserver Change Whodunnit?

White County, Georgia Official Domain: whitecounty.net

whitecounty.net

Parent Zone
- ns1.hemc.net
- ns2.internetemc.com

Child Zone
- ns1.hemc.net
- ns2.internetemc.com
Mystery #1: Nameserver Change Whodunnit?

White County, Georgia Official Domain: whitecounty.net

Parent Zone
ns1.hemc.net
ns2.internetemc.com

Child Zone
ns1.hemc.net
ns2.internetemc.com

Parent Zone
ns1.hemc.net
ns2.internetemc1aj2tkdy.biz

Child Zone
ns1.hemc.net
ns2.internetemc.com

July 01, 2019
Mystery #1: Nameserver Change Whodunnit?

**Why** did the nameserver change?

**Who** changed the nameserver?
Mystery #2: DROPTHISHOST Anomaly

33% of nameservers in the last 9 years ending in .biz are dropthishost-xxxx.biz
Mystery #2: DROPTHISHOST Anomaly

33% of nameservers in the last 9 years ending in .biz are dropthishost-xxxx.biz

yourgadgetnews.com

Parent Zone
ns1.knowanewbie.com
ns2.knowanewbie.com

Parent Zone
dropthishost-e06eed78-1098-41db-9964-f13d6f032d52.biz
dropthishost-e6a1816-88a8-455b-b20d-e4aeef79ed9e.biz

Jan 09, 2016
Mystery #2: DROPTHISHOST Anomaly

Why did the nameservers change?

Who changed the nameservers?
Mystery #2: DROPTHISHOST Anomaly

33% of nameservers in the last 9 years ending in .biz are dropthishost-xxxx.biz

yourgadgetnews.com

Parent Zone
ns1.knowanewbie.com
ns2.knowanewbie.com

Jan 09, 2016

Parent Zone
dropthishost-e06eed78-1098-41db-9964-f13d6f032d52.biz
dropthishost-e6a1816-88a8-455b-b20d-e4aeef79ed9e.biz

Large numbers indicate systemic issue.
Changes to DNS Configuration: Behind the Scenes

How do updates to DNS Configuration propagate?

Parent Zone

Registry
Registrar

Child Zone
Registrant
Changes to DNS Configuration: Behind the Scenes

How do updates to DNS Configuration propagate?

Parent Zone

Registry

Registrar

Registrant

Child Zone

Web Portal / API

Registrar
Changes to DNS Configuration: Behind the Scenes

How do updates to DNS Configuration propagate?

Parent Zone

Registry → Registrar → Registrant

EPP

Child Zone

Web Portal / API
Changes to DNS Configuration: Behind the Scenes

How do updates to DNS Configuration propagate?

Parent Zone

Registry

Registrar

EPP

Child Zone

Registrar

Registrant

Web Portal / API
Extensible Provisioning Protocol: Mental Model

Registry TLD DNS Configuration == Database

RFC 5730, RFC 5731
Extensible Provisioning Protocol: Mental Model

Registry TLD DNS Configuration == Database

TLD DNS Configuration

foo.com → Domain Object

ns1.foo.com

ns1.foo.com is *subordinate host object* of foo.com

ns1.foo.com → Host Object
Extensible Provisioning Protocol: Mental Model

Registry TLD DNS Configuration == Database

EPP as the specification on how this database can be modified.

foo.com → Domain Object
ns1.foo.com is subordinate host object of foo.com
ns1.foo.com → Host Object

RFC 5730, RFC 5731
EPP Mental Model

foo.com

bar.com

Registrar A  Registrar B
EPP Mental Model
EPP Mental Model

foo.com expires.

Registrar A  Registrar B

Subordinate Relationship  Delegated Nameserver

Host Object  Domain Object  Host Object
EPP Mental Model

foo.com expires.

ns1.f*com

ns2.foo.com

ns1.bar.com

foo.com

bar.com

Registrar A

Registrar B

Subordinate Relationship

Delegated Nameserver

Host Object

Domain Object

Host Object
**EPP Mental Model**

**EPP Constraint:** host object referenced by another domain object cannot be deleted.
EPP Mental Model

**EPP Constraint:** host object referenced by another domain object cannot be deleted.

**EPP Workaround:** Rename host object.
Host Object Renaming Constraints

- If renamed within the same TLD, EPP requires the domain object must exist.
  - \texttt{ns2.foo.com} \textbf{CANNOT} be renamed to \texttt{dropthishost-xxxx.com}
    - if \texttt{dropthishost-xxxx.com} does NOT exist

- EPP cannot check references to external TLDs.
  - \texttt{ns2.foo.com} \textbf{CAN} be renamed to \texttt{dropthishost-xxxx.biz}
    - even if \texttt{dropthishost-xxxx.biz} does NOT exist
Host Object Renaming Constraints

- If renamed within the same TLD, EPP requires the domain object must exist.
  - \texttt{ns2.foo.com} CANNOT be renamed to \texttt{dropthishost-xxxx.com}
    if \texttt{dropthishost-xxxx.com} does NOT exist.

- EPP cannot check references to external TLDs.
  - \texttt{ns2.foo.com} CAN be renamed to \texttt{dropthishost-xxxx.biz}
    even if \texttt{dropthishost-xxxx.biz} does NOT exist.

- Drop \texttt{ns2.foo.com} altogether.
Host Object Renaming Constraints

- If renamed within the same TLD, EPP requires the domain object must exist.
  - ns2.foo.com CANNOT be renamed to dropthishost-xxxx.com
    if dropthishost-xxxx.com does NOT exist

- EPP cannot check references to external TLDs.
  - ns2.foo.com CAN be renamed to dropthishost-xxxx.biz
    even if dropthishost-xxxx.biz does NOT exist

- Drop ns2.foo.com altogether.
Registrar Renaming Options

Registrar A Options

1. Rename NS to a “sink” domain owned by Registrar A
   a. Internet.bs used dummyns.com
   b. Registrar A is responsible for queries and upkeep of sink domain.

2. Rename NS to a “random” domain in a different TLD
   a. Different TLD bypasses EPP check.
   b. Registrar does not have to handle queries or upkeep any domains.
   c. Potential security risk.
EPP Mental Model
EPP Mental Model
EPP Mental Model

sacrificial nameserver

Registrar A Registrar B

Subordinate Relationship

Delegated Nameserver

Host Object Domain Object Host Object
Renaming Effects Across TLDs
Renaming Effects Across TLDs

Verisign EPP Repository

Afilias EPP Repository

foo.com

ns2.foo.com

ns1.qux.gov

ns1.baz.org

baz.org

qux.gov

ns1.com

ns2.com

foo.com expires.

ns1.com

ns2.com

-
Renaming Effects Across TLDs
EPP Renaming Summary

- EPP consistency constraints lead to unintuitive consequences on domain deletion
- Security risk without any action from domain owner
  - Opaque to the domain owner and even its own registrar
  - Re-registering the expired domain “foo.com” does not fix the issue
- Affects domains even in “restricted” TLDs like .gov and .edu
  - Even though no registrars in “restricted” TLDs
Identifying Sacrificial Nameservers
Identifying Sacrificial Nameservers: Longitudinal Analysis

- Three properties of sacrificial nameservers
  - Sacrificial nameservers only exist in the TLD zone files (parent zone)
  - Good renaming idioms use non-existent domain names i.e., lame delegated on creation
  - EPP renamings affect domains within a single database
Identifying Sacrificial Nameservers: Longitudinal Analysis

● Three properties of sacrificial nameservers
  ○ Sacrificial nameservers only exist in the TLD zone files (parent zone)
  ○ Good renaming idioms use non-existent domain names i.e., lame delegated on creation
  ○ EPP renamings affect domains within a single database

● Use 9 years of zone files spanning 1250 TLDs (CAIDA-DZDB)

● Modify methodology used to identify lame delegations
  ○ Unresolved Issues - IMC’ 20

● Apply methodology to ~20M nameservers in the zone files.
  ○ Details in paper.
# Hijackable Renaming Idioms

<table>
<thead>
<tr>
<th>Renaming Idiom Sink Domain</th>
<th>Registrar</th>
<th># of Sacrificial Nameservers</th>
<th># of Affected Domains</th>
<th>Example Renaming ns1.foo.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLEASEDROPTHISHOST</td>
<td>GoDaddy</td>
<td>75,030</td>
<td>217,952</td>
<td>pleasedroptthishostxxxxx.foo.biz</td>
</tr>
<tr>
<td>DROPTHISHOST</td>
<td>GoDaddy</td>
<td>40,374</td>
<td>109,478</td>
<td>dropthishost-xxxxx.biz</td>
</tr>
<tr>
<td>DELETED-DROP</td>
<td>Internet.bs</td>
<td>3,511</td>
<td>9,289</td>
<td>deleted-xxxxx.drop-xxxxxx.biz</td>
</tr>
<tr>
<td>123.BIZ</td>
<td>Enom</td>
<td>5,799</td>
<td>7,157</td>
<td>ns1.foo123.biz</td>
</tr>
<tr>
<td>xxxxx.{BIZ, COM}</td>
<td>Enom</td>
<td>54,752</td>
<td>164,264</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td>xxxxx.BIZ</td>
<td>DomainPeople</td>
<td>654</td>
<td>3,304</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td>xxxxx.BIZ</td>
<td>Fabulous.com</td>
<td>334</td>
<td>1,223</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td>xxxxx.BIZ</td>
<td>Register.com</td>
<td>388</td>
<td>1,570</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>180,842</strong></td>
<td><strong>512,715</strong></td>
<td></td>
</tr>
</tbody>
</table>
Hijackable Renaming Idioms

<table>
<thead>
<tr>
<th>Renaming Idiom Sink Domain</th>
<th>Registrar</th>
<th># of Sacrificial Nameservers</th>
<th># of Affected Domains</th>
<th>Example Renaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLEASEDROPTHISHOST</td>
<td>GoDaddy</td>
<td>75,030</td>
<td>217,952</td>
<td>pleasedropthishostxxxxx.foo.biz</td>
</tr>
<tr>
<td>DROPTHISHOST</td>
<td>GoDaddy</td>
<td>40,374</td>
<td>109,478</td>
<td>dropthishost-xxxxx.biz</td>
</tr>
<tr>
<td>DELETED-DROP</td>
<td>Internet.bs</td>
<td>3,511</td>
<td>9,289</td>
<td>deleted-xxxxx.drop-xxxxx.biz</td>
</tr>
<tr>
<td>123.BIZ</td>
<td>Enom</td>
<td>5,799</td>
<td>7,157</td>
<td>ns1.foo123.biz</td>
</tr>
<tr>
<td>xxxxx.{BIZ, COM}</td>
<td>Enom</td>
<td>54,752</td>
<td>164,264</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td>xxxxx.BIZ</td>
<td>DomainPeople</td>
<td>654</td>
<td>3,304</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td>xxxxx.BIZ</td>
<td>Fabulous.com</td>
<td>334</td>
<td>1,223</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td>xxxxx.BIZ</td>
<td>Register.com</td>
<td>388</td>
<td>1,570</td>
<td>ns1.fooxxxxx.biz</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>180,842</strong></td>
<td><strong>512,715</strong></td>
<td></td>
</tr>
</tbody>
</table>

32% of affected domains were hijacked by registering the sacrificial nameserver domain
Hijacked Domains

- Hijackers seem to have two main uses
  - Ads
  - Search Engine Optimization
- Opportunistic hijacks!
Prevent Creation of New Sacrificial Nameservers

- Worked with the three registrars with largest impact to prevent creation of new sacrificial nameservers using “sink” domains.
  - Prevented ~30K domains from being hijackable.

- New Renaming Idioms
  - GoDaddy - droptthishost-xxxx.as112.arpa
  - Enom - xxxx.delete-registration.com
  - Internet.bs - xxxx.notaplaceto.be
Remediate Currently Hijacked Domains

- Created per registrar lists of affected domains.
  - Make available lists to registrar community to address currently affected domains.
- Notable remediation efforts by GoDaddy, and MarkMonitor.
Need for Long Term Solutions

● “Sink” domains not a good long term solution.
  ○ Multiple instances of “sink” domains becoming available for registration.
  ○ Single registration gets all domains.

● Potential Solutions
  ○ Use .alt TLD --- RFC Draft
  ○ Delete NS without renaming
Changes to EPP?

Any long term solution needs to be codified as a change to EPP!

Prevent relapse to old renaming idioms.

Not all EPP instances support proposed solutions.
Zooming Out: The Larger Picture

Infrastructure Hijacks

Opportunistic Hijacks

Targeted Hijacks

Risky BIZness: IMC 2021
Zooming Out: The Larger Picture

Infrastructure Hijacks

Opportunistic Hijacks
- Risky BI/Zness: IMC 2021

Targeted Hijacks
- Retroactive Identification: IMC 2022
Emergency Directive 19-01

Original Release Date: January 22, 2019

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM: Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CC: Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT: Mitigate DNS Infrastructure Tampering
Widespread DNS Hijacking Activity Targets Multiple Sectors

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale
Safran Aircraft Engine Company (Circa 2014)

Safran Aircraft Engine Company (previously Snecma) a French aerospace company
Client Logging Into “Secure” Network...

Client Stub Resolver -> Recursive Resolver

You are entering a restricted area
Please enter your userid and password

User id
Password

Unauthorized access is prohibited and may result in prosecution under French law.
(Loi du 5 janvier 1998 art. 321-1)
Normal Resolution

Client Stub Resolver

Recursive Resolver

secure.sneema.fr

217.108.170.196

secure.sneema.fr

Ask fr Auth NS

secure.sneema.fr

Ask ns[1,2].sneema.fr

Root Authoritative NS

TLD Authoritative NS

Domain Authoritative NS
Normal Resolution

Client Stub Resolver

Recursive Resolver

secure.snehma.fr

217.108.170.196

secure.snehma.fr

Ask fr Auth NS

secure.snehma.fr

Ask ns[1,2].snehma.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

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

Ask ns[1,2].acfine.net
67.198.195.126

Attacker controlled NS
67.198.195.126

Root Authoritative NS
TLD Authoritative NS
Attackers Redirect All Users

Client Stub Resolver

Recursive Resolver

secure.sncema.fr

Ask ns[1,2].acfine.net

67.198.195.126

secure.sncema.fr

Ask ns[1,2].acfine.net

Root Authoritative NS

TLD Authoritative NS

attacker controlled NS

Registry

Database

EPP Server

Updates

EPP

Registrar

Web/API

Registrant
What about TLS Certificates?

Your connection is not private

Attacks 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 Infrastructure Hijack

- Acquire ability to control DNS delegations
  - Hijacks characterized by multiple brief updates to evade detection
  - Attacker can bypass protections

- Attacker infrastructure to mimic target domain
  - Responds with maliciously obtained TLS certificate
  - Cannot be distinguished from legitimate infrastructure

- Harvest credentials or compromise redirected users to infiltrate target organization
The Goal

Construct a methodology to retroactively identify targeted domain hijacks in the wild as an independent third-party.
Hijacked Domains

Identified 41 domains as hijacked

- 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>
<tr>
<td>Type</td>
<td>Hij.</td>
<td>Targeted Domain Information</td>
<td>Cross Ref</td>
<td>Attacker Infra. (Transient)</td>
<td>Legitimate Infra. (Stable)</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-----------------------------</td>
<td>-----------</td>
<td>----------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CC Domain</td>
<td>Sub.</td>
<td>pDNS</td>
<td>cert</td>
<td>IP</td>
</tr>
<tr>
<td>T1</td>
<td>May’18</td>
<td>AE</td>
<td>sofagovae</td>
<td>webmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Sep’18</td>
<td>AE</td>
<td>police.govae</td>
<td>advpm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1*</td>
<td>Sep’18</td>
<td>AE</td>
<td>apcgovae</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>Sep’18</td>
<td>AE</td>
<td>mgovae</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Jan’18</td>
<td>AL</td>
<td>e-albaniaal</td>
<td>ova</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>Nov’18</td>
<td>AL</td>
<td>sep.goval</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Nov’18</td>
<td>AL</td>
<td>shishциальн</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Dec’18</td>
<td>CY</td>
<td>govcn1</td>
<td>personal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Dec’18</td>
<td>CY</td>
<td>ova.govcy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Dec’18</td>
<td>CY</td>
<td>webmail.govcy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Jan’19</td>
<td>CY</td>
<td>cyta.comcy</td>
<td>xbox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Jan’19</td>
<td>CY</td>
<td>selvpn.govcy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Feb’19</td>
<td>CY</td>
<td>defa.comcy</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Nov’18</td>
<td>EG</td>
<td>nsgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>Nov’18</td>
<td>EG</td>
<td>nodgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>Nov’18</td>
<td>EG</td>
<td>nmgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Nov’18</td>
<td>EG</td>
<td>petroleumgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Apr’19</td>
<td>GR</td>
<td>kyvernisi</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Apr’19</td>
<td>GR</td>
<td>nsgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>Sep’18</td>
<td>IQ</td>
<td>nsgov.</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Nov’18</td>
<td>IQ</td>
<td>ircvrdil</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-NS</td>
<td>Dec’18</td>
<td>JO</td>
<td>gid.govjo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-NS</td>
<td>Dec’20</td>
<td>KG</td>
<td>ftagov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Dec’20</td>
<td>KG</td>
<td>investgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Dec’20</td>
<td>KG</td>
<td>nsgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-NS</td>
<td>Jan’21</td>
<td>KG</td>
<td>infoconn</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Dec’17</td>
<td>KW</td>
<td>ckgov</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Dec’18</td>
<td>KW</td>
<td>dgsagovkw</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1*</td>
<td>Apr’19</td>
<td>KW</td>
<td>泃govkw</td>
<td>webmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td>May’18</td>
<td>KW</td>
<td>kotc.comkw</td>
<td>mail2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Nov’18</td>
<td>LB</td>
<td>financegov</td>
<td>webmail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Nov’18</td>
<td>LB</td>
<td>nes.com</td>
<td>memail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Nov’18</td>
<td>LB</td>
<td>medgulf.con</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Nov’18</td>
<td>LB</td>
<td>pcm.gov</td>
<td>mail1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-IP</td>
<td>Oct’18</td>
<td>LY</td>
<td>embassyy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-NS</td>
<td>Oct’18</td>
<td>LY</td>
<td>foreigny</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Oct’18</td>
<td>LY</td>
<td>socly</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Jan’18</td>
<td>NL</td>
<td>ocom.com</td>
<td>connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-NS</td>
<td>Jan’19</td>
<td>SE</td>
<td>netnoodse</td>
<td>dsnodeapi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td>Mar’19</td>
<td>SY</td>
<td>syyristelsy</td>
<td>mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P-NS</td>
<td>Dec’18</td>
<td>US</td>
<td>pchnet</td>
<td>kerrionail</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Targeted Hijacks Summary

- Traditional mechanisms not effective against DNS infrastructure hijacks
  - Attackers can bypass DNSSEC and TLS since they control DNS Infrastructure
- Need for more transparency and proactive measurements to understand how to mitigate future hijacks
Christmas RFC Wishlist
Christmas RFC Wishlist

EPP Updates

DNS Transparency

Certificate Transparency ++
EPP Updates

- Codify changes to EPP to prevent creation of sacrificial nameservers
  - .alt TLD
  - Drop NS without renaming
- Consistency across TLDs?
  - Different registries communicate domain deletions.
DNS Transparency

- Organizations cannot tell if their nameservers ever changed!
  - Have ietf.org nameservers changed recently? [No, as per zone file data...]
  - But hijacks last for as little as 15 minutes and zone files updated daily.
  - Think “supply chain attacks”
  - Continuous monitoring?

- Certificate Transparency like transparency with DNS
  - Append only changes to domain nameservers at TLDs?
Certificate Transparency ++

- Certificate Transparency has been a great resource to identify bad actors.
- Certificate Authorities (CAs) do a lot of work to issue certificates
- ACME Transaction Information
  - DNS queries from multiple vantage points
  - IP which initiated the certificate request
Collaborators

Geoffrey Voelker
Ian Foster
KC Claffy
Mattijs Jonker
Raffaele Sommese
Stefan Savage
Zakir Durumeric
Questions?

gakiwate -- at -- cs.stanford.edu
Backup
<table>
<thead>
<tr>
<th>Tar. Date</th>
<th>CC</th>
<th>Targeted Domain</th>
<th>Sub</th>
<th>Cross Ref.</th>
<th>Attacker Infra. (Transient)</th>
<th>Legit. Infra. (Stable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Domain</td>
<td></td>
<td>pDNS</td>
<td>IP</td>
<td>ASN</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>cert</td>
<td>194.152.42.16</td>
<td>47220</td>
</tr>
<tr>
<td>Apr’20</td>
<td>AE</td>
<td>milmail.ae</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Apr’20</td>
<td>AE</td>
<td>mocaf.gov.ae</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Apr’20</td>
<td>AE</td>
<td>moi.gov.ae</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dec’20</td>
<td>AE</td>
<td>epg.gov.ae</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Jun’20</td>
<td>CH</td>
<td>parlament.ch</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Nov’20</td>
<td>GH</td>
<td>nita.gov.gu</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sep’17</td>
<td>JO</td>
<td>psd.gov.jo</td>
<td>mail</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Jun’20</td>
<td>KZ</td>
<td>zerde.gov.kz</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Nov’20</td>
<td>LT</td>
<td>stat.gov.lt</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Jul’20</td>
<td>LV</td>
<td>iem.gov.lv</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Nov’20</td>
<td>LV</td>
<td>zva.gov.lv</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Apr’18</td>
<td>MA</td>
<td>justice.gov.ma</td>
<td>micj</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Apr’20</td>
<td>MA</td>
<td>mem.gov.ma</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Oct’20</td>
<td>MM</td>
<td>mofa.gov.mm</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Nov’20</td>
<td>PL</td>
<td>knf.gov.pl</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>May’20</td>
<td>SA</td>
<td>cnmail.sa</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sep’20</td>
<td>TM</td>
<td>turkmenpost.gov.tm</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Aug’20</td>
<td>US</td>
<td>manchesternh.gov</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dec’20</td>
<td>US</td>
<td>batesvillearkansas.gov</td>
<td>host</td>
<td>X</td>
<td>188.166.160.110</td>
<td>14061</td>
</tr>
<tr>
<td>Apr’19</td>
<td>VN</td>
<td>ais.gov.vn</td>
<td>intranet</td>
<td>X</td>
<td>45.77.45.193</td>
<td>20473</td>
</tr>
<tr>
<td>Dec’20</td>
<td>VN</td>
<td>mofa.gov.vn</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mar’20</td>
<td>VN</td>
<td>cpt.gov.vn</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mar’20</td>
<td>VN</td>
<td>most.gov.vn</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sep’20</td>
<td>VN</td>
<td>vass.gov.vn</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
To continue using the email service, you must install the security update:
Download Update
Focus on Operational Requirements of Hijack

**Requirement #1:** Update DNS resolutions to malicious IP for the duration of hijack

**Requirement #2:** Obtain new TLS certificate to prevent warnings

**Requirement #3:** Attacker Infrastructure set up to use maliciously obtained new TLS certificate at a malicious IP address which the target domain resolves to intermittently

**Key Insight**
Attacker infrastructure will appear in global IP scans looking for certificates.
Identifying Targeted DNS Infrastructure Hijacks: Intuition

- **Global IP Scans**
  - Identify Attacker Infrastructure. $IP_A + Cert_A$

- **Passive DNS**
  - Corroborate target domain was redirected to $IP_A$

- **CT Logs**
  - Corroborate $Cert_A$ was issued during redirection

**Hijack Evidence**
- DNS Redirection + New Certificate + Use of New Certificate at Redirected IP
How to Identify Attacker Infrastructure?
Map Observable Infrastructure

“Observable Infrastructure for a domain”

*IP addresses and certificates that secure and serve the domain*
Observable Infrastructure

**IP**: 217.108.170.196
**Port**: 443
**Certificate**: <A>
**SANs**: [secure.snecma.fr]
Observable Infrastructure

IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.sneecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True
Scan #1

- **IP:** 217.108.170.196
- **Port:** 443
- **Certificate:** <A>
- **SANs:** [secure.snecma.fr]
- **Geolocation:** France
- **AS:** 3215
- **Browser Trusted:** True
- **Issuing CA:** Let's Encrypt
- **Sensitive:** True

Deployment #1
Scan #2

IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.sneecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

Deployment #1
Scan #3

Deployment #1
- **IP**: 217.108.170.196
- **Port**: 443
- **Certificate**: <A>
- **SANs**: [secure.snecma.fr]
- **Geolocation**: France
- **AS**: 3215
- **Browser Trusted**: True
- **Issuing CA**: Let's Encrypt
- **Sensitive**: True

Deployment #2
- **IP**: 67.198.195.126
- **Port**: 443
- **Certificate**: <B>
- **SANs**: [secure.snecma.fr]
- **Geolocation**: US
- **AS**: 35908
- **Browser Trusted**: True
- **Issuing CA**: Comodo
- **Sensitive**: True
Scan #3

**Deployment #1**
- **IP**: 217.108.170.196
- **Port**: 443
- **Certificate**: <A>
- **SANs**: [secure.snecma.fr]
- **Geolocation**: France
- **AS**: 3215
- **Browser Trusted**: True
- **Issuing CA**: Let's Encrypt
- **Sensitive**: True

**Deployment #2**
- **IP**: 67.198.195.126
- **Port**: 443
- **Certificate**: <B>
- **SANs**: [secure.snecma.fr]
- **Geolocation**: US
- **AS**: 35908
- **Browser Trusted**: True
- **Issuing CA**: Comodo
- **Sensitive**: True

Legitimate or Malicious?
Scan #4

IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.snecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

Deployment #1
### Longitudinal View: Deployment Maps

<table>
<thead>
<tr>
<th>Date</th>
<th>Stable Deployment</th>
<th>Transient Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan #1</td>
<td>AS3215 [FR]</td>
<td>certs [A]</td>
</tr>
<tr>
<td>Scan #2</td>
<td>AS3215 [FR]</td>
<td>certs [A]</td>
</tr>
<tr>
<td>Scan #3</td>
<td>AS3215 [FR]</td>
<td>AS35908 [US]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>certs [B]</td>
</tr>
<tr>
<td>Scan #4</td>
<td>AS3215 [FR]</td>
<td>certs [A]</td>
</tr>
</tbody>
</table>
Suspicious Deployments → Potential Attacker Infrastructure

**Deployment #1**
- **IP**: 217.108.170.196
- **Port**: 443
- **Certificate**: <A>
- **SANs**: secure.snecma.fr
- **Geolocation**: France
- **AS**: 3215
- **Browser Trusted**: True
- **Issuing CA**: Let's Encrypt
- **Sensitive**: True

**Deployment #2**
- **IP**: 67.198.195.126
- **Port**: 443
- **Certificate**: <B>
- **SANs**: secure.snecma.fr
- **Geolocation**: US
- **AS**: 35908
- **Browser Trusted**: True
- **Issuing CA**: Comodo
- **Sensitive**: True
Suspicious Deployments → Potential Attacker Infrastructure

Deployment #1
- **IP**: 217.108.170.196
- **Port**: 443
- **Certificate**: <A>
- **SANs**: [secure.snecma.fr]
- **Geolocation**: France
- **AS**: 3215
- **Browser Trusted**: True
- **Issuing CA**: Let's Encrypt
- **Sensitive**: True

Deployment #2
- **IP**: 67.198.195.126
- **Port**: 443
- **Certificate**: <B>
- **SANs**: [secure.snecma.fr]
- **Geolocation**: US
- **AS**: 35908
- **Browser Trusted**: True
- **Issuing CA**: Comodo
- **Sensitive**: True

#1: Check Passive DNS if secure.snecma.fr was redirected to 67.198.195.126
#2: Check CT Log to see if Cert <B> was issued during redirection