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

10000ft Summary

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*

whitecounty.net

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

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

July 01, 2019

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

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

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		Parent Zone
ns1.knowanewbie.com ns2.knowanewbie.com	→ *Jan 09, 2016*	dropthishost-e06eed78-1098-41db-9964-f13d6f032d52.biz dropthishost-e6a1816-88a8-455b-b20d-e4aeef79ed9e.biz

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		Parent Zone
ns1.knowanewbie.com ns2.knowanewbie.com	→ *Jan 09, 2016*	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

Child Zone

Registry | **Registrar** ← **Registrant**

Web Portal / API

Changes to DNS Configuration: Behind the Scenes

How do updates to DNS Configuration propagate?

Parent Zone

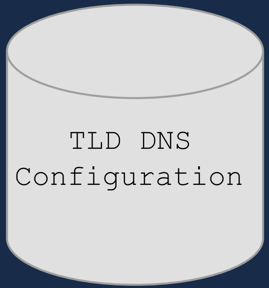
Child Zone

Registry $\xleftarrow{\text{EPP}}$ **Registrar** $\xleftarrow{\text{Web Portal / API}}$ **Registrant**

Changes to DNS Configuration: Behind the Scenes

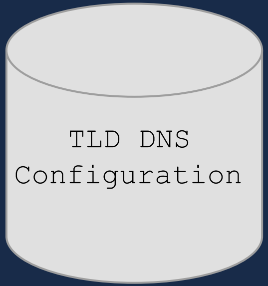
How do updates to DNS Configuration propagate?

Extensible Provisioning Protocol: Mental Model



Registry TLD DNS Configuration == Database

Extensible Provisioning Protocol: Mental Model



Registry TLD DNS Configuration == Database

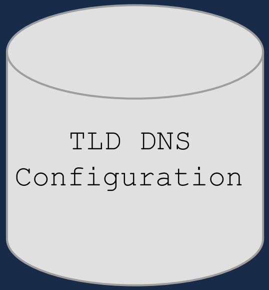
foo.com → Domain Object

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

nsl.foo.com → Host Object

RFC 5730, RFC 5731

Extensible Provisioning Protocol: Mental Model



Registry TLD DNS Configuration == Database

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

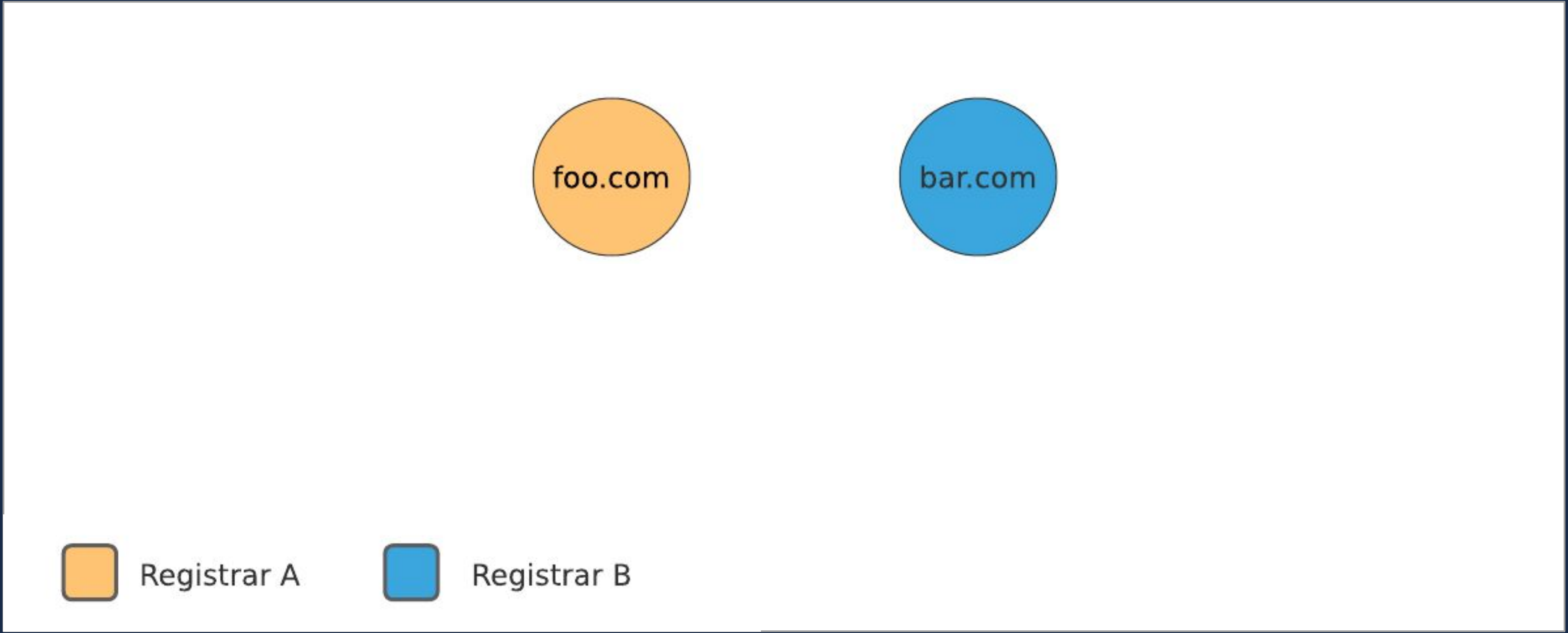
foo.com → Domain Object

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

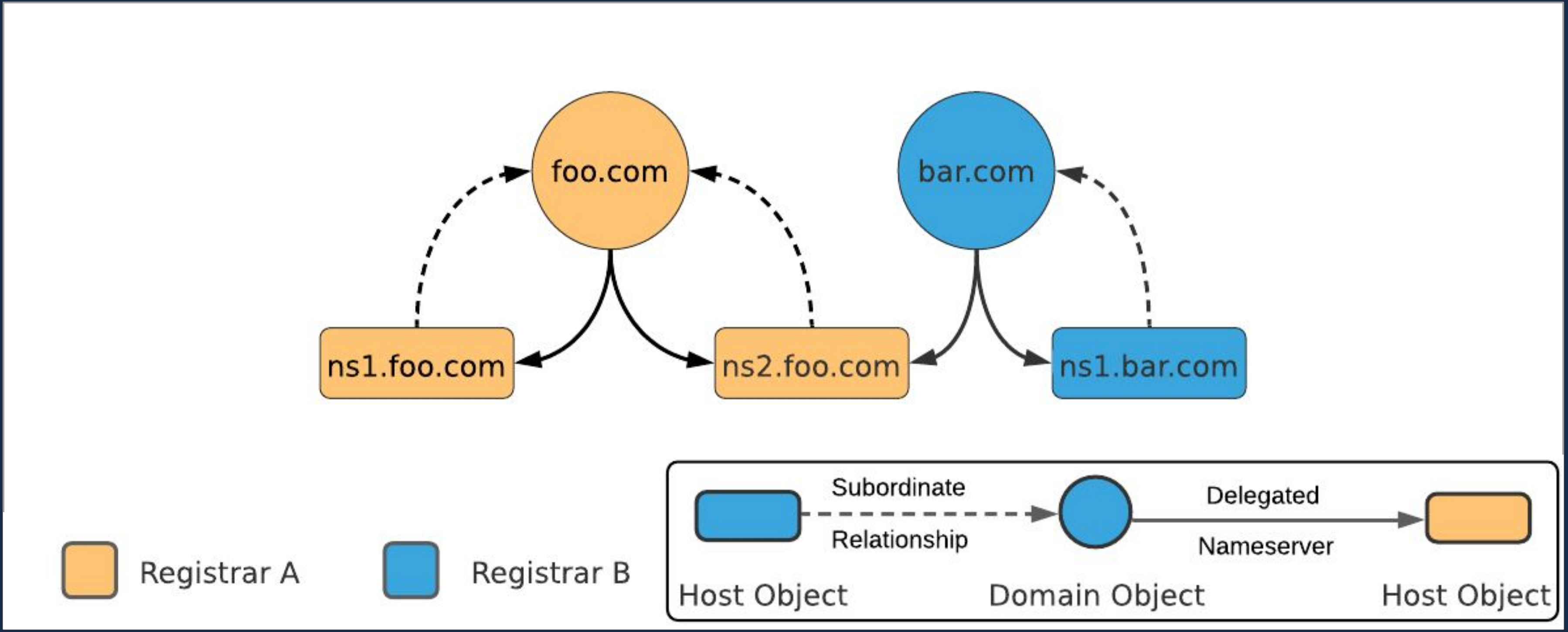
ns1.foo.com → Host Object

RFC 5730, RFC 5731

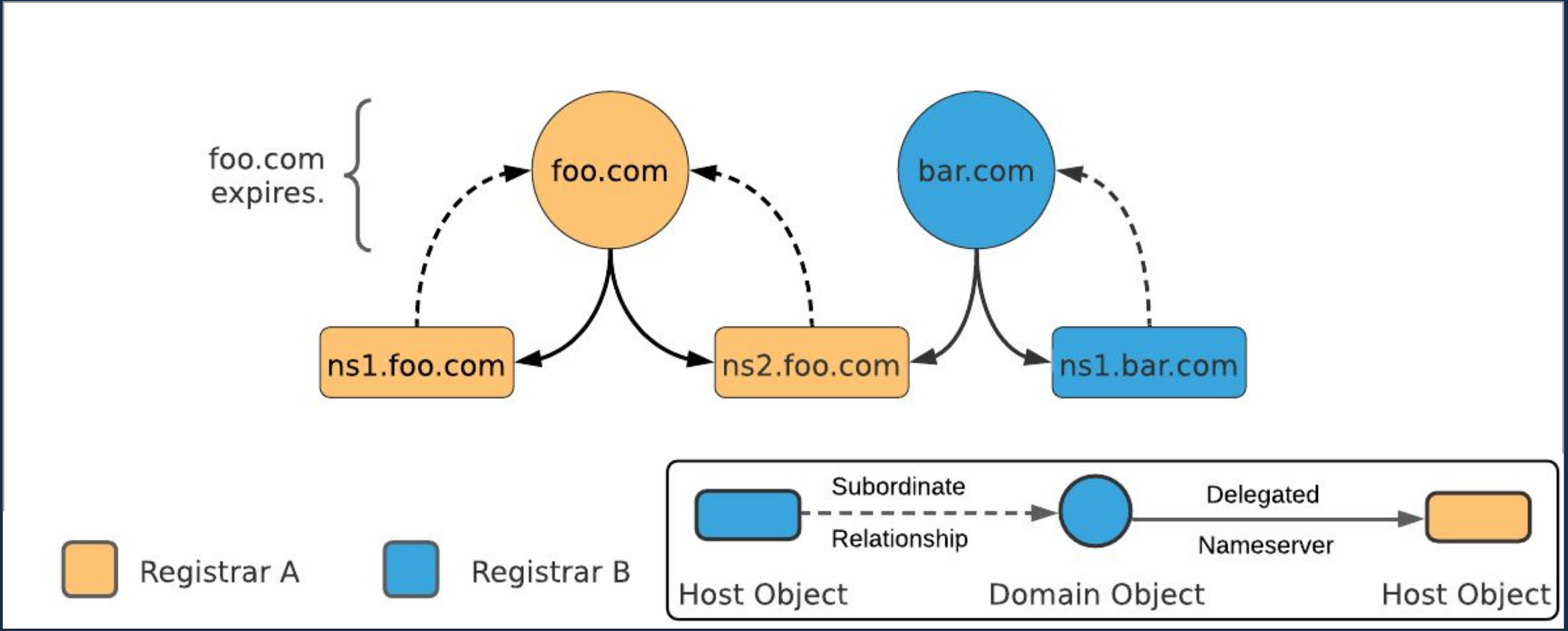
EPP Mental Model



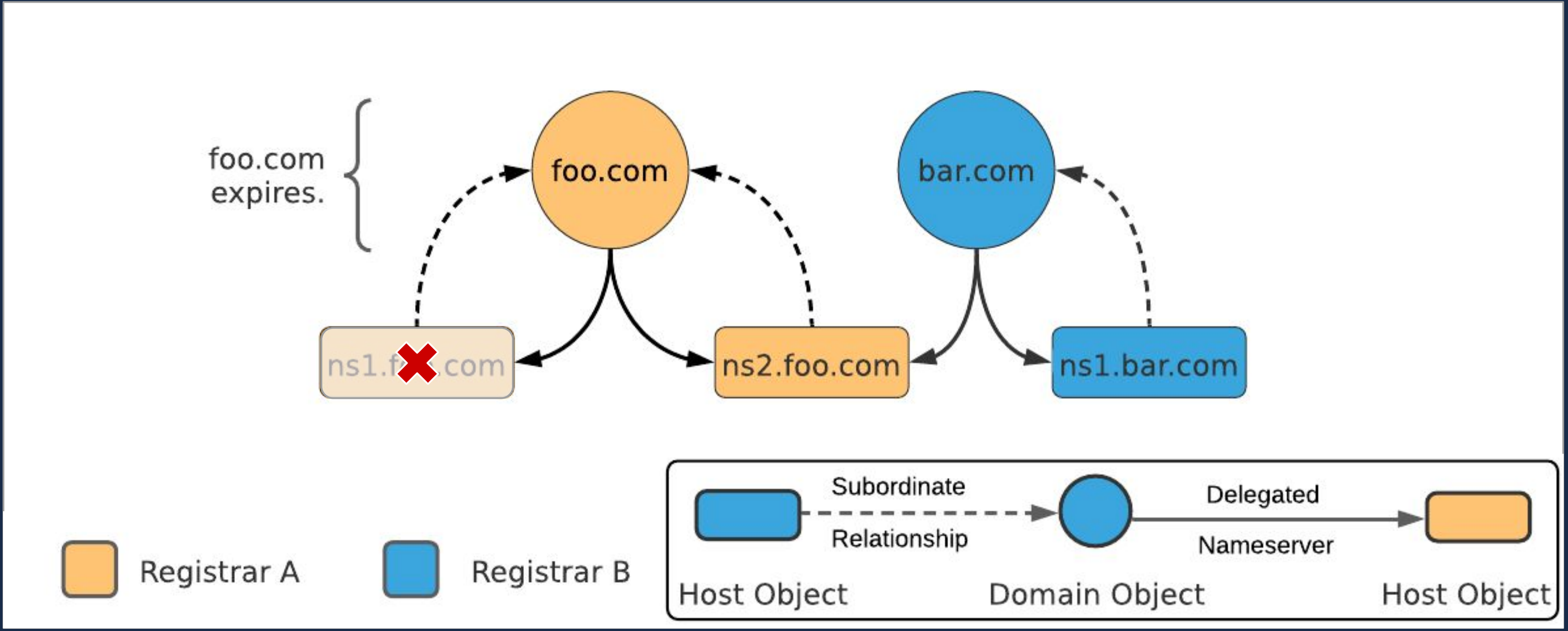
EPP Mental Model



EPP Mental Model

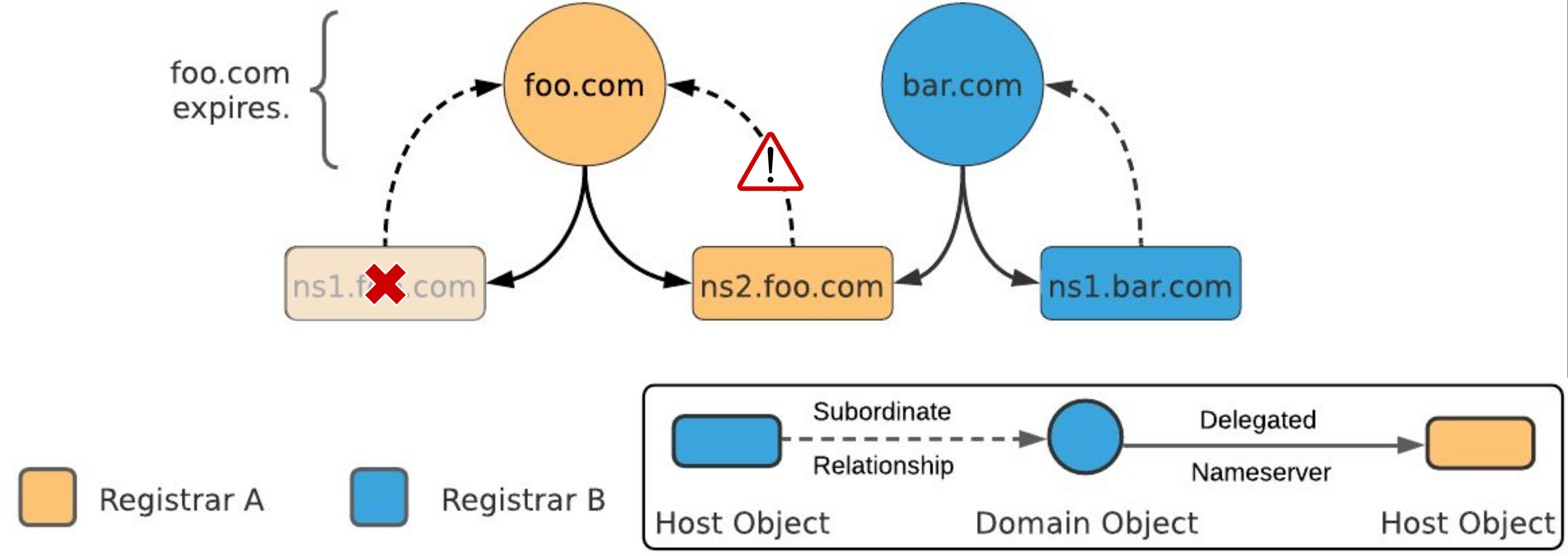


EPP Mental Model



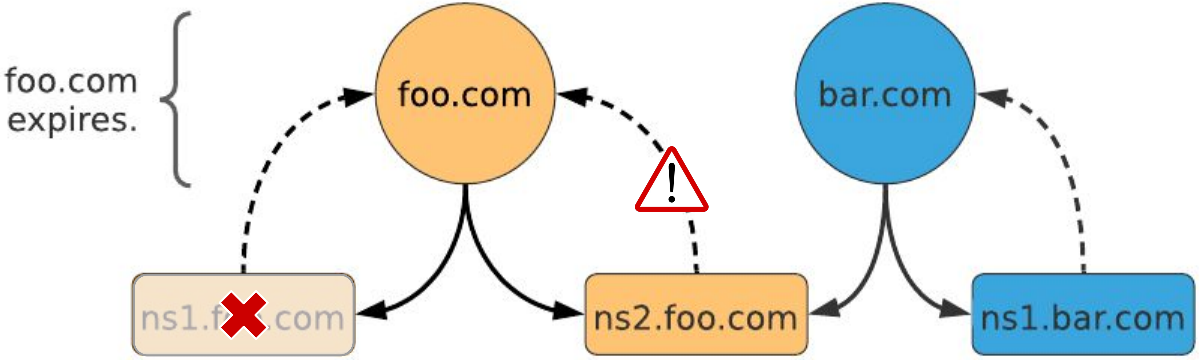
EPP Mental Model

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

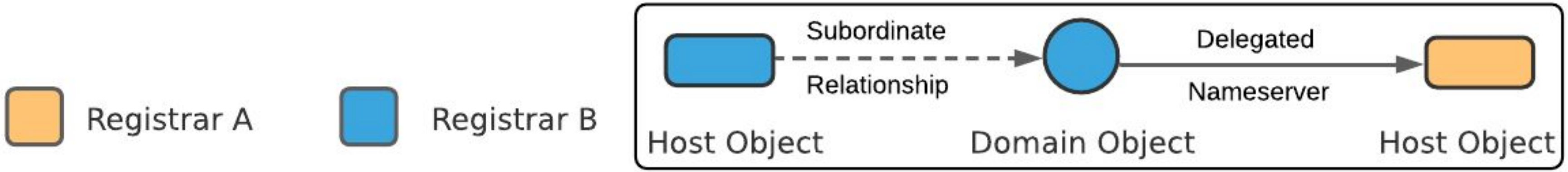


EPP Mental Model

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.
  - 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

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.

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

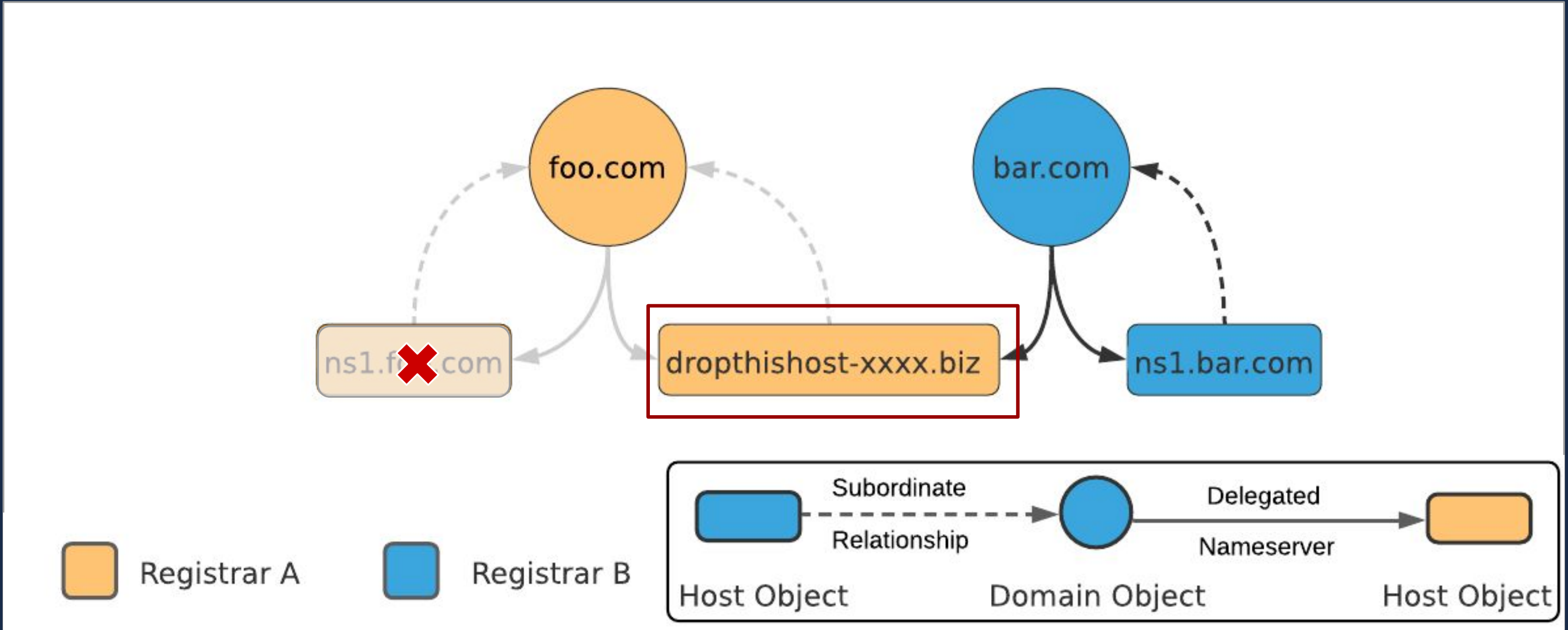
- ~~Drop ns2.foo.com altogether.~~

Registrar Renaming Options

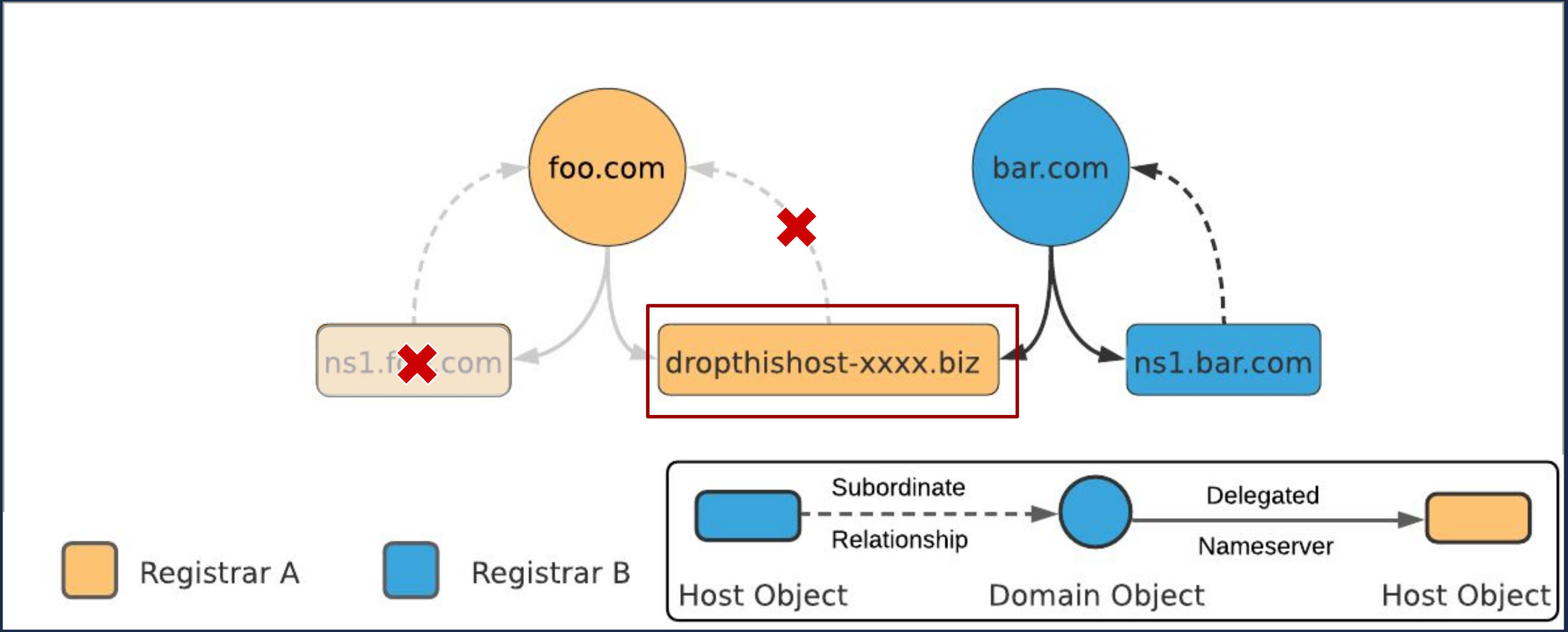
Registrar A Options

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.

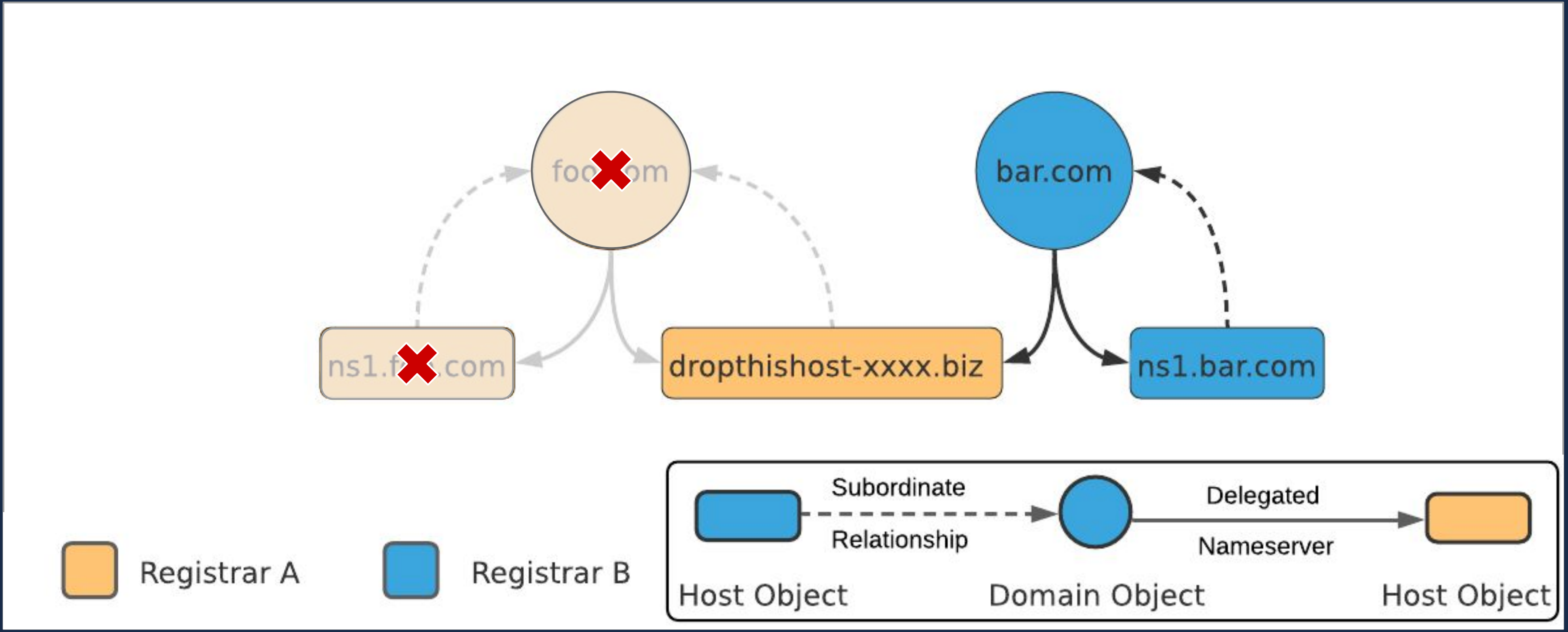
EPP Mental Model



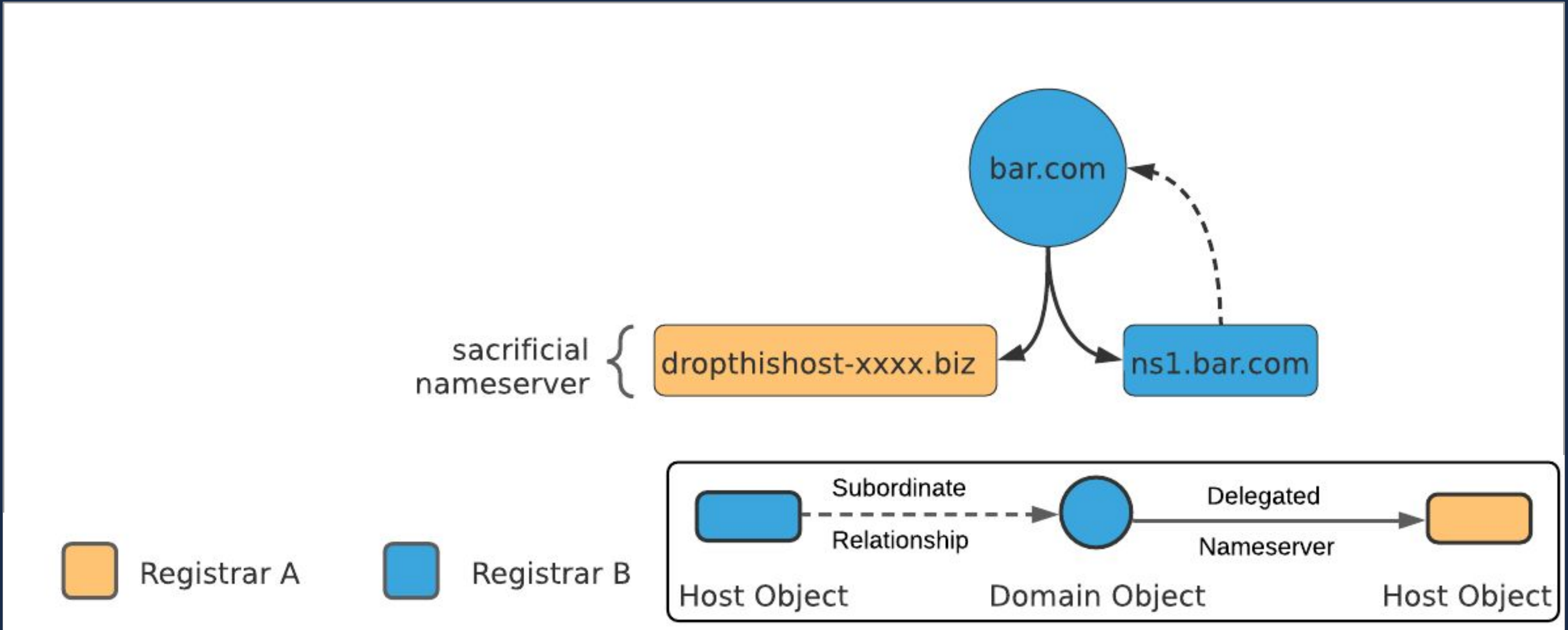
EPP Mental Model



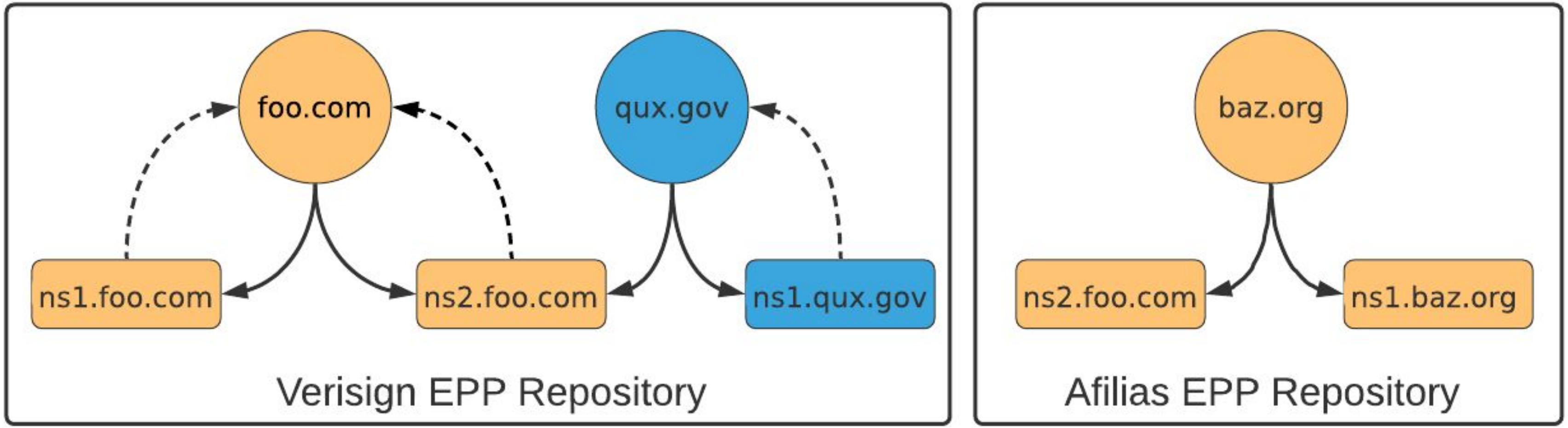
EPP Mental Model



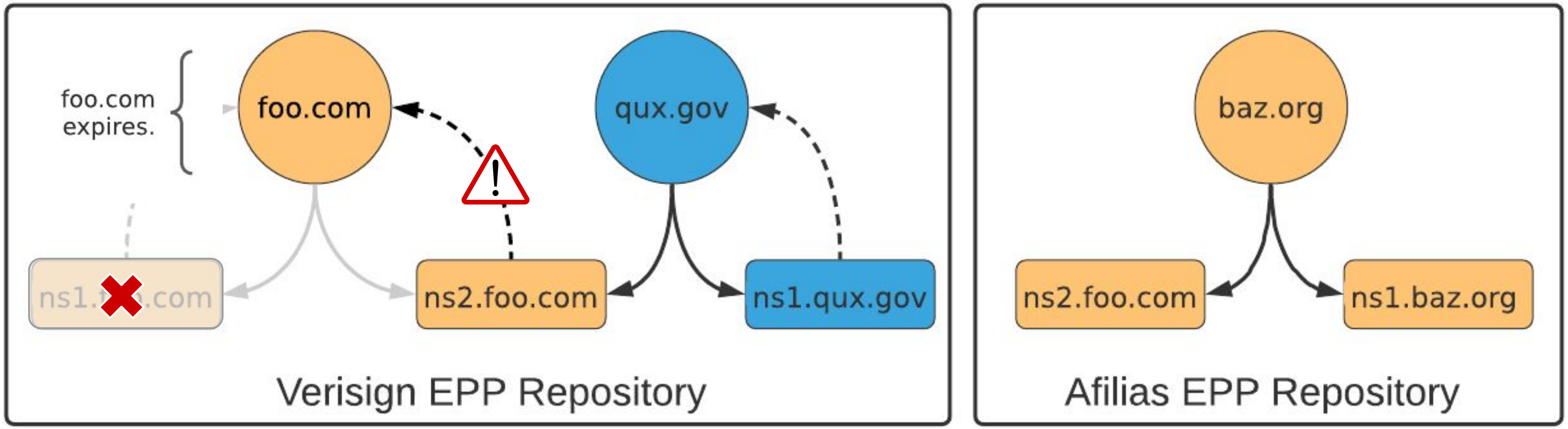
EPP Mental Model



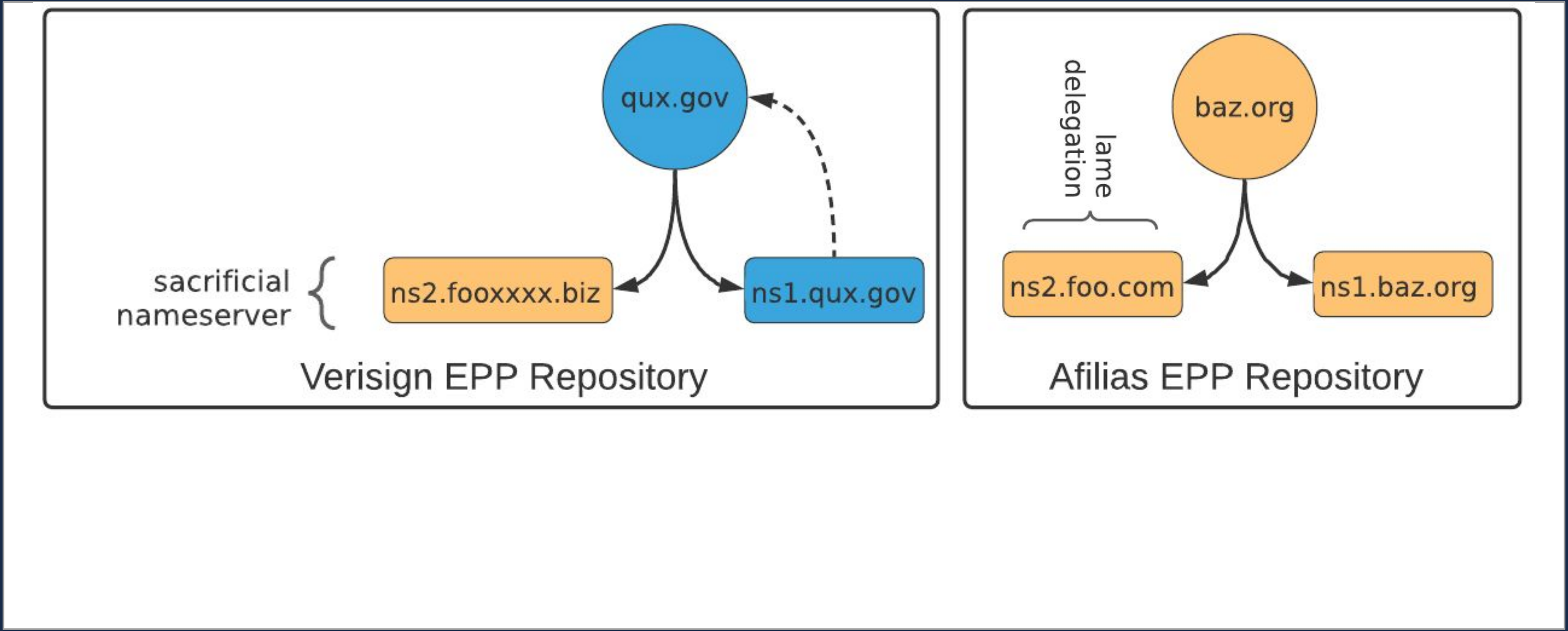
Renaming Effects Across TLDs



Renaming Effects Across TLDs



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 it's 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

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

Hijackable Renaming Idioms

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

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!

Remediation

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 - dropthishost-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

Targeted Hijacks

Risky BIZness: IMC 2021

Retroactive Identification: IMC 2022

U.S. Department of Homeland Security
Washington, DC 20528

CISA
CYBER+INFRASTRUCTURE

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**

DNS Hijacking Abuses Trust In Core Internet Service

Widespread DNS Hijacking Activity Targets Multiple Sectors

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

DNSpionage Campaign Targets Middle East

Safran Aircraft Engine Company (Circa 2014)

Safran Aircraft Engine Company (previously Snecma) a French aerospace company

The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity

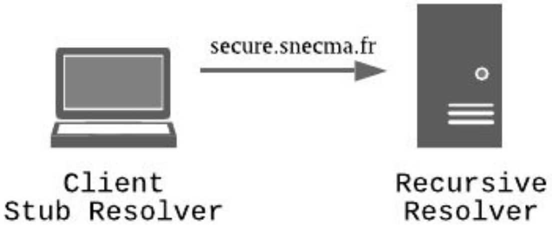
REUTERS

BUSINESS NEWS

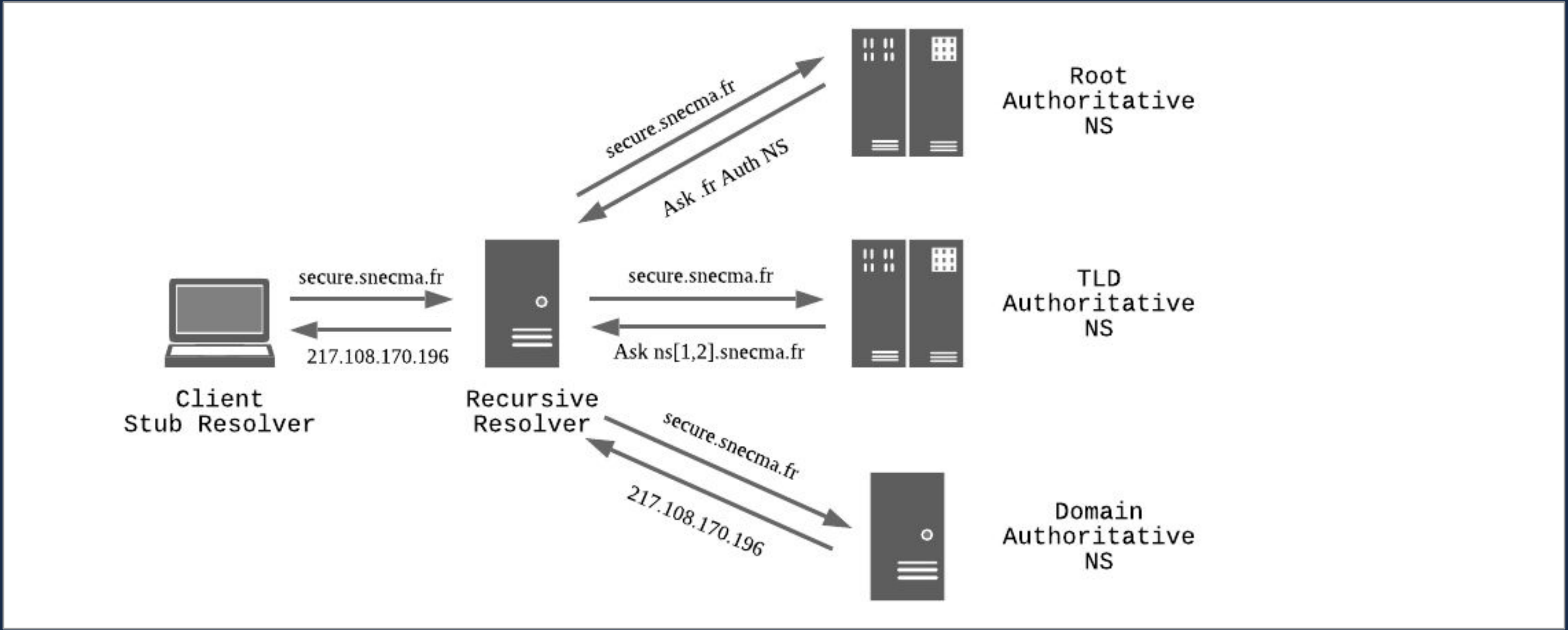
FEBRUARY 18, 2014 / 12:29 PM / UPDATED 9 YEARS AGO

Exclusive: France's Snecma targeted by hackers - researcher

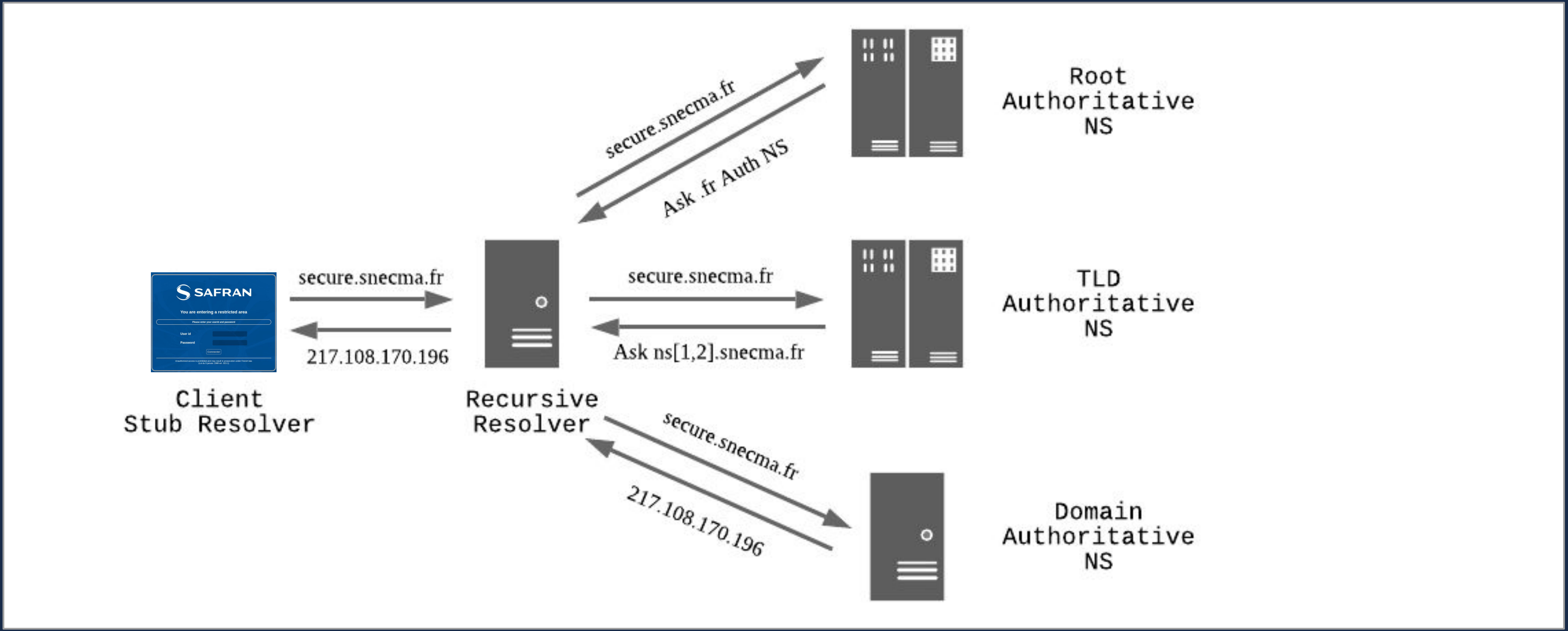
Client Logging Into “Secure” Network...



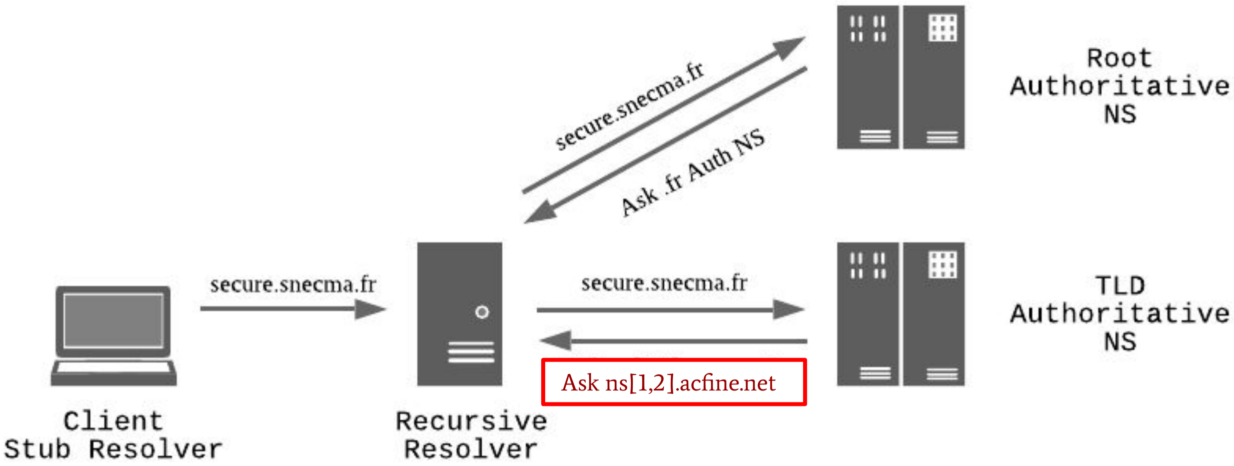
Normal Resolution



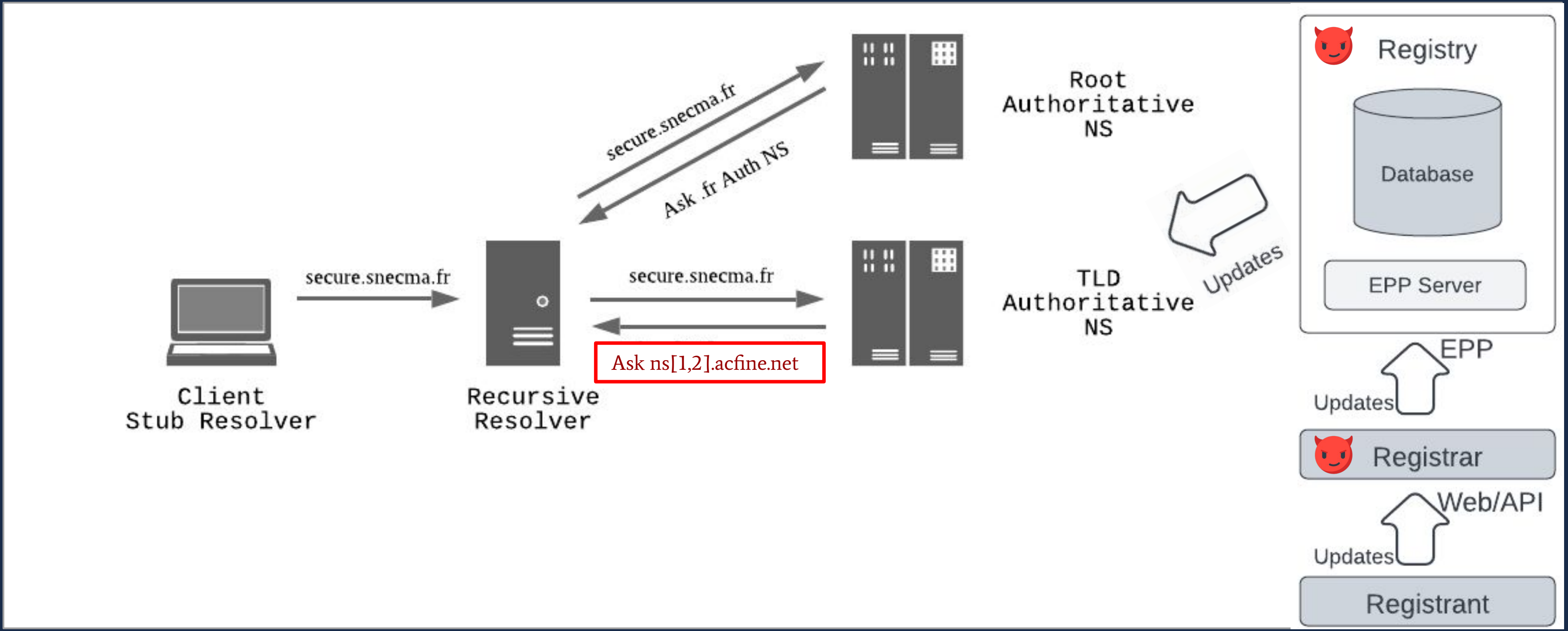
Normal Resolution



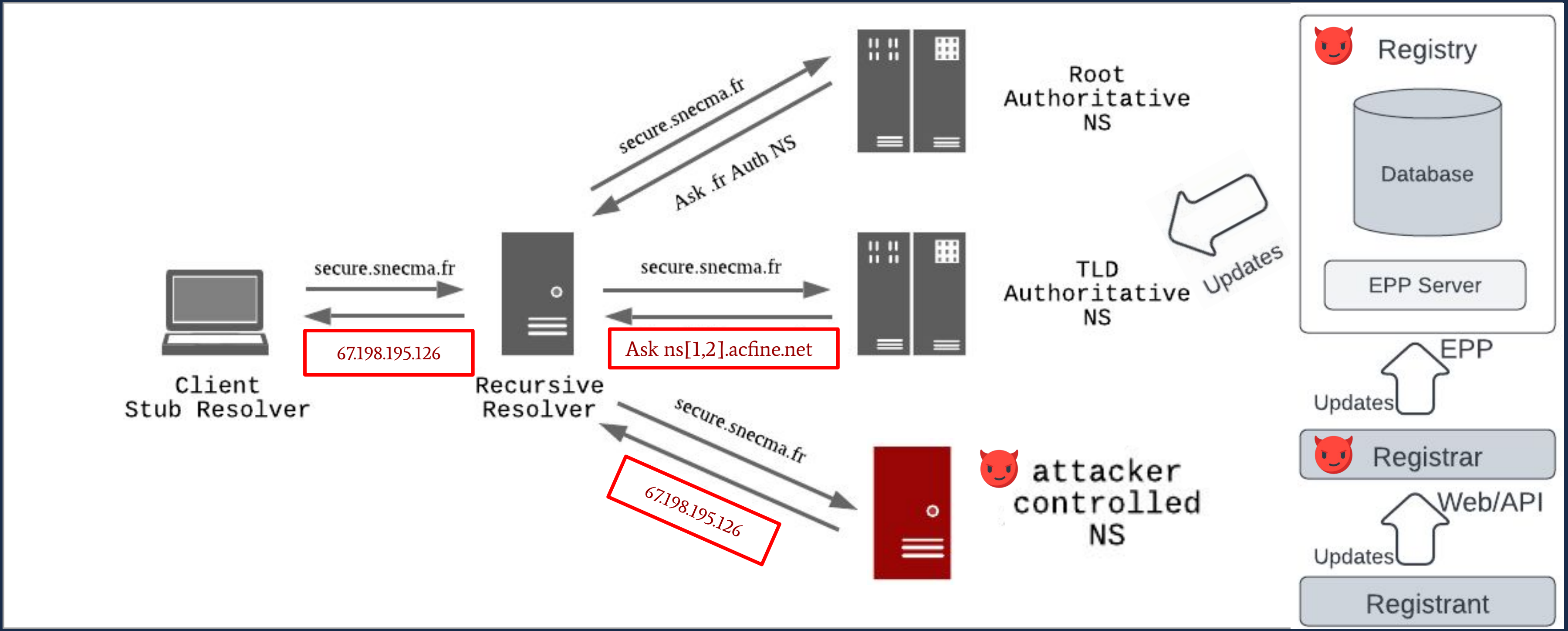
Malicious DNS Delegation Update (Circa 2014)



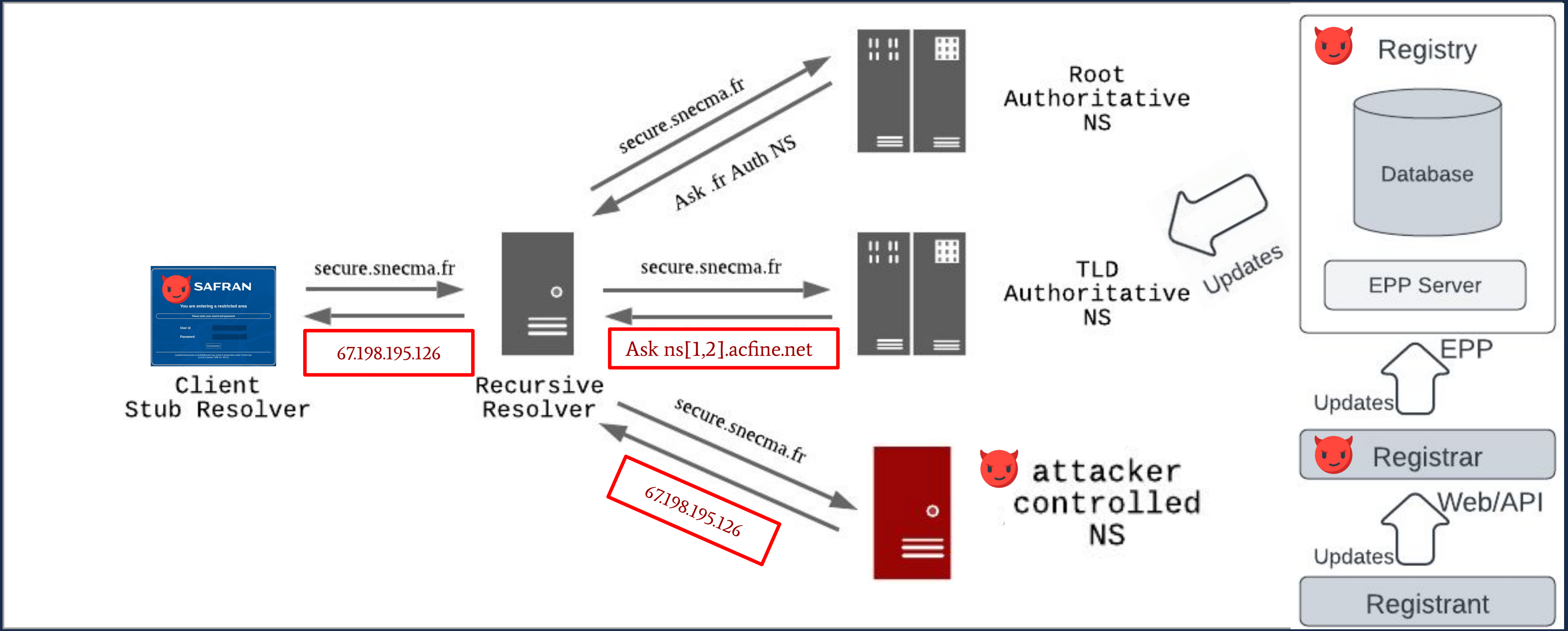
Attackers Target DNS Delegation Update Mechanism



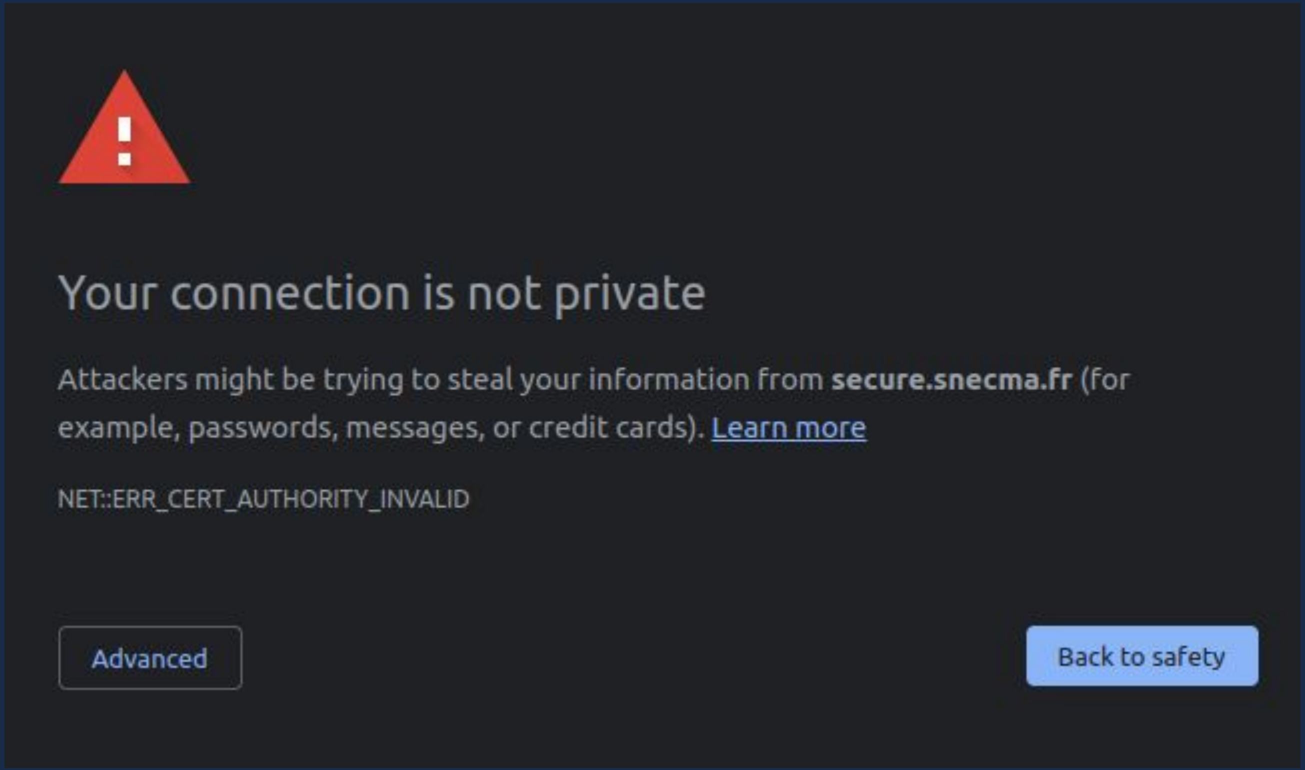
Attackers Redirect All Users



Attackers Redirect All Users



What about TLS Certificates?

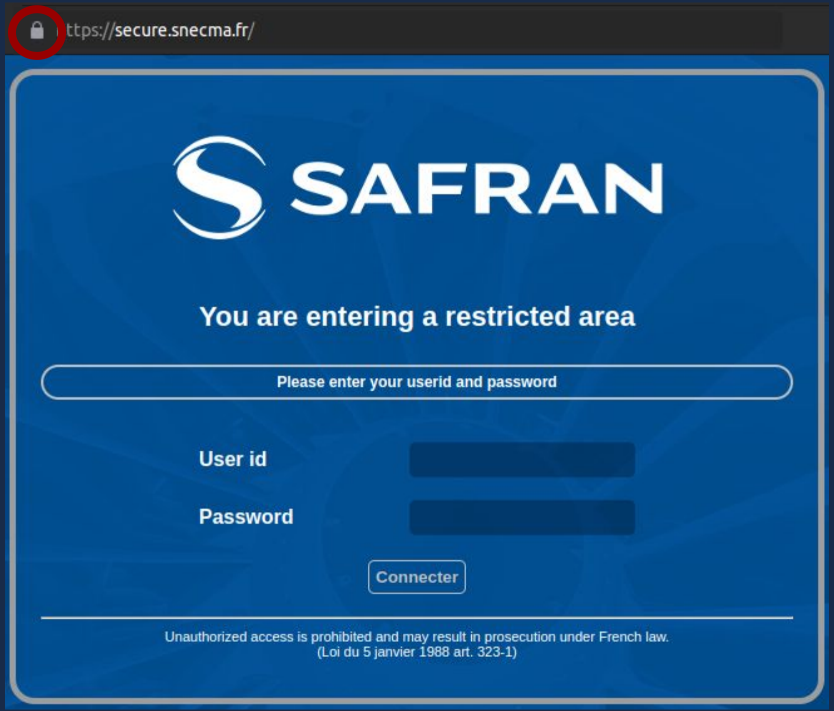


Implicit Trust Dependence

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

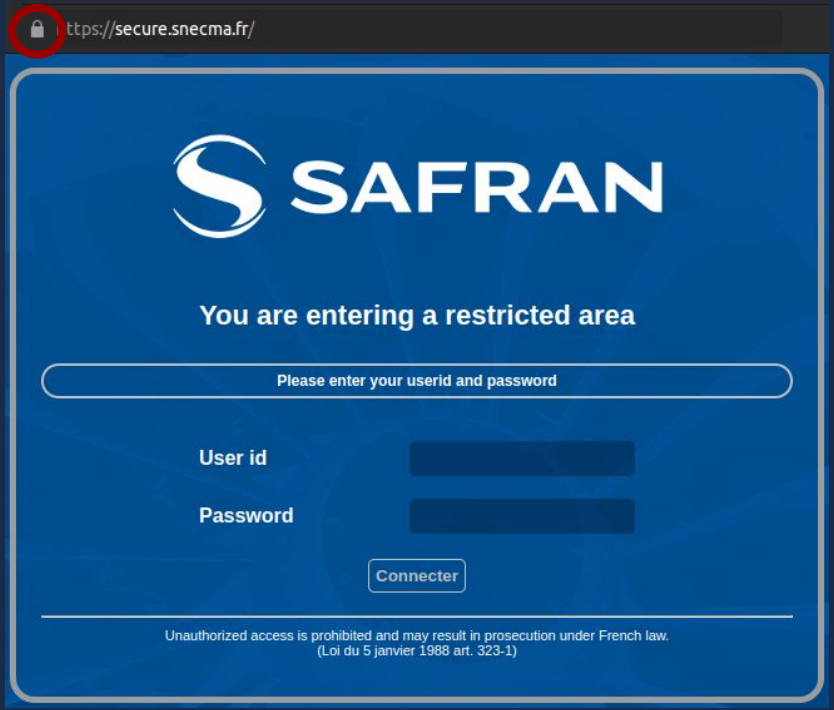
Implicit Trust Dependence

- 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

	Hijacked Domains			Attacker Infrastructure		
Date	Domain	Target	Organization	Malicious IP	Malicious ASN	Geo
Dec'20	fiu.gov.kg	mail	Financial Intelligence Service	178.20.41.140	AS 48282	Russia
Dec'20	invest.gov.kg	mail	Investment Portal	94.103.90.182	AS 48282	Russia
Dec'20	mfa.gov.kg	mail	Ministry of Foreign Affairs	94.103.91.159	AS 48282	Russia
Jan'21	infocom.kg	mail	Internet Services Provider	195.2.84.10	AS 48282	Russia

Type	Hij.	Targeted Domain Information CC	Domain	Sub.	Cross Ref pDNS	crt	Attacker Infra. (Transient) IP	ASN	CC	Legitimate Infra. (Stable) ASNs	CCs
T1	May'18	AE	mofa.gov.ae	webmail	✔	✔	146.185.143.158	14061	NL	[5384,202024]	[AE]
T1	Sep'18	AE	adpolice.gov.ae	advpn	✔	✔	185.20.187.8	50673	NL	[5384]	[AE]
T1*	Sep'18	AE	apc.gov.ae	mail	✖	✔	185.20.187.8	50673	NL	[5384]	[AE]
T2	Sep'18	AE	mgov.ae	mail	✔	✔	185.20.187.8	50673	NL	[202024]	[AE]
T1	Jan'18	AL	e-albania.al	owa	✔	✔	185.15.247.140	24961	DE	[5576]	[AL]
T2	Nov'18	AL	asp.gov.al	mail	✔	✔	199.247.3.191	20473	DE	[201524]	[AL]
T1	Nov'18	AL	shish.gov.al	mail	✔	✔	37.139.11.155	14061	NL	[5576]	[AL]
T1	Dec'18	CY	govcloud.gov.cy	personal	✔	✔	178.62.218.244	14061	NL	[50233]	[CY]
P-IP	Dec'18	CY	owa.gov.cy	.	✔	✔	178.62.218.244	14061	NL	[50233]	[CY]
T1	Dec'18	CY	webmail.gov.cy	.	✔	✔	178.62.218.244	14061	NL	[50233]	[CY]
P-IP	Jan'19	CY	cyta.com.cy	mbox	✔	✔	178.62.218.244	14061	NL	—	—
T1	Jan'19	CY	sslvpn.gov.cy	.	✔	✔	178.62.218.244	14061	NL	[50233]	[CY]
T1	Feb'19	CY	defa.com.cy	mail	✔	✔	108.61.123.149	20473	FR	[35432]	[CY]
T1	Nov'18	EG	mfa.gov.eg	mail	✔	✔	188.166.119.57	14061	NL	[37066]	[EG]
T2	Nov'18	EG	mod.gov.eg	mail	✔	✔	188.166.119.57	14061	NL	[25576]	[EG]
T2	Nov'18	EG	nmi.gov.eg	mail	✔	✔	188.166.119.57	14061	NL	[31065]	[EG]
T1	Nov'18	EG	petroleum.gov.eg	mail	✔	✔	206.221.184.133	20473	US	[24835,37191]	[EG]
T1	Apr'19	GR	kyvernisi.gr	mail	✔	✔	95.179.131.225	20473	NL	[35506]	[GR]
T1	Apr'19	GR	mfa.gr	pop3	✔	✔	95.179.131.225	20473	NL	[35506,6799]	[GR]
T2	Sep'18	IQ	mofa.gov.iq	mail	✔	✔	82.196.9.10	14061	NL	[50710]	[IQ]
P-IP	Nov'18	IQ	inc-vrdl.iq	.	✔	✔	199.247.3.191	20473	DE	[50710]	[IQ]
P-NS	Dec'18	JO	gid.gov.jo	.	✔	✔	139.162.144.139	63949	DE	—	—
P-NS	Dec'20	KG	fiu.gov.kg	mail	✔	✔	178.20.41.140	48282	RU	—	—
T1	Dec'20	KG	invest.gov.kg	mail	✔	✔	94.103.90.182	48282	RU	[39659]	[KG]
T1	Dec'20	KG	mfa.gov.kg	mail	✔	✔	94.103.91.159	48282	RU	[39659]	[KG]
P-NS	Jan'21	KG	infocom.kg	mail	✔	✔	195.2.84.10	48282	RU	—	—
T1	Dec'17	KW	csb.gov.kw	mail	✔	✔	82.102.14.232	20860	GB	[6412]	[KW]
P-IP	Dec'18	KW	dgca.gov.kw	mail	✔	✔	185.15.247.140	24961	DE	—	—
T1*	Apr'19	KW	moh.gov.kw	webmail	✖	✔	91.132.139.200	9009	AT	[21050]	[KW]
T2	May'19	KW	kotc.com.kw	mail2010	✔	✔	91.132.139.200	9009	US	[57719]	[KW]
P-IP	Nov'18	LB	finance.gov.lb	webmail	✔	✔	185.20.187.8	50673	NL	—	—
P-IP	Nov'18	LB	mea.com.lb	memail	✔	✔	185.20.187.8	50673	NL	—	—
T1	Nov'18	LB	medgulf.com.lb	mail	✔	✔	185.161.209.147	50673	NL	[31126]	[LB]
T1	Nov'18	LB	pcm.gov.lb	mail1	✔	✔	185.20.187.8	50673	NL	[51167]	[DE]
P-IP	Oct'18	LY	embassy.ly	.	✔	✖	188.166.119.57	14061	NL	—	—
P-NS	Oct'18	LY	foreign.ly	.	✔	✔	188.166.119.57	14061	NL	—	—
T1	Oct'18	LY	noc.ly	mail	✔	✔	188.166.119.57	14061	NL	[37284]	[LY]
T1	Jan'18	NL	ocom.com	connect	✔	✔	147.75.205.145	54825	US	[60781]	[NL]
P-NS	Jan'19	SE	netnod.se	dnsnodeapi	✔	✔	139.59.134.216	14061	DE	—	—
T1	Mar'19	SY	syriatel.sy	mail	✔	✔	45.77.137.65	20473	NL	[29256]	[SY]
P-NS	Dec'18	US	pch.net	keriomail	✔	✔	159.89.101.204	14061	DE	—	—

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

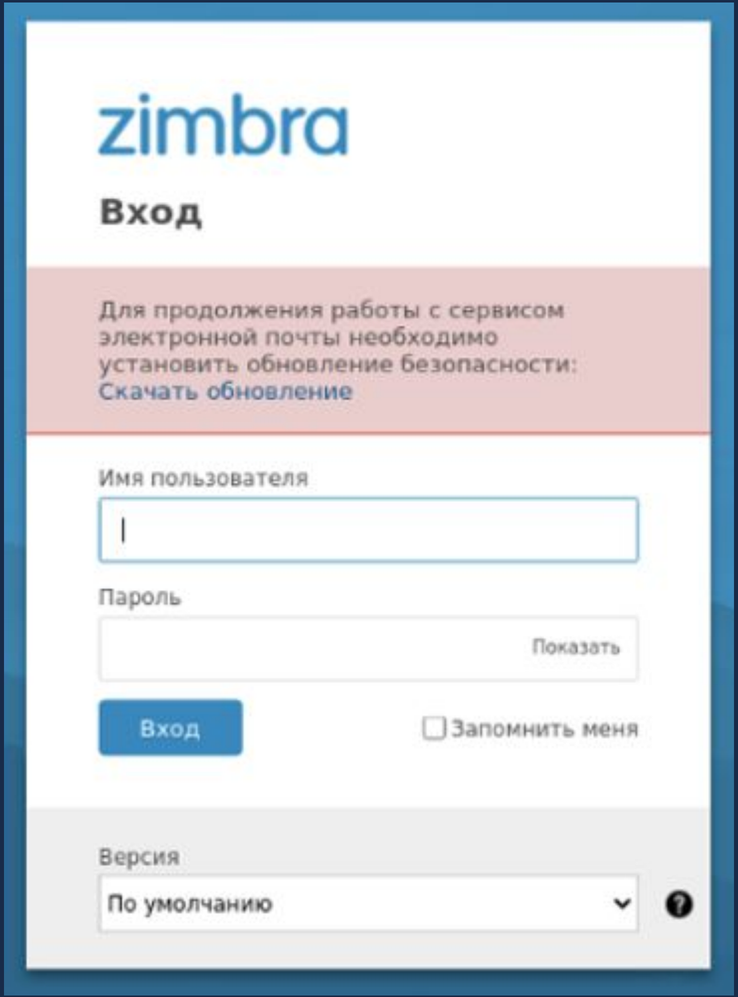
Zakir Durumeric

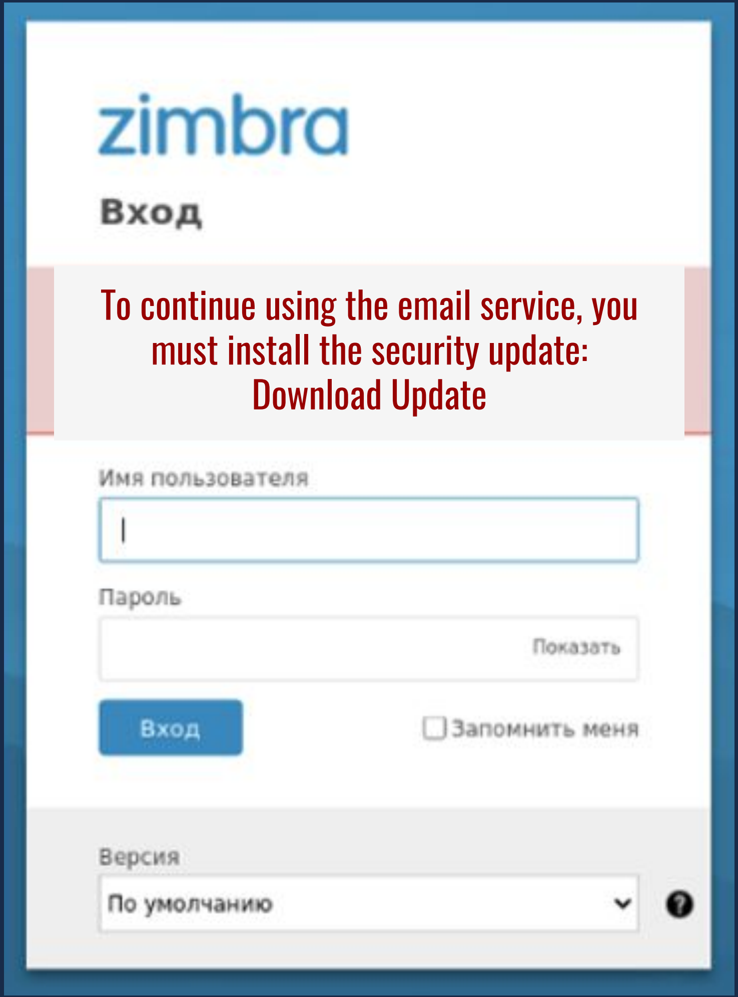
Questions?

gakiwate -- at -- cs.stanford.edu

Backup

	Targeted Domain			Cross Ref.		Attacker Infra. (Transient)			Legit. Infra. (Stable)	
Tar. Date	CC	Domain	Sub	pDNS	crt	IP	ASN	CC	ASNs	CCs
Apr'20	AE	milmail.ae	–	✗	✗	194.152.42.16	47220	RO	[5384]	[AE]
Apr'20	AE	mocaf.gov.ae	–	✗	✗	194.152.42.16	47220	RO	[5384]	[AE]
Apr'20	AE	moi.gov.ae	–	✗	✗	194.152.42.16	47220	RO	[5384]	[AE]
Dec'20	AE	epg.gov.ae	–	✗	✗	159.69.193.152	24940	DE	[202024]	[AE]
Jun'20	CH	parlament.ch	–	✗	✗	8.210.146.182	45102	SG	[61098,3303]	[CH]
Nov'20	GH	nita.gov.gh	–	✗	✗	78.141.218.158	20473	NL	[37313]	[GH]
Sep'17	JO	psd.gov.jo	mail	✗	✗	185.162.235.106	50673	NL	[8934]	[JO]
Jun'20	KZ	zerde.gov.kz	–	✗	✗	8.210.190.81	45102	SG	[48716,15549]	[KZ]
Nov'20	LT	stat.gov.lt	–	✗	✗	8.210.190.214	45102	SG	[6769]	[LT]
Jul'20	LV	iem.gov.lv	–	✗	✗	8.210.199.85	45102	SG	[8194, 25241]	[LV]
Nov'20	LV	zva.gov.lv	–	✗	✗	8.210.36.66	45102	SG	[8194, 199300]	[LV]
Apr'18	MA	justice.gov.ma	micj	✓	✗	188.166.160.110	14061	DE	[6713]	[MA]
Apr'20	MA	mem.gov.ma	–	✗	✗	47.75.34.153	45102	HK	[6713]	[MA]
Oct'20	MM	mofa.gov.mm	–	✗	✗	47.242.150.18	45102	US	[136465]	[MM]
Nov'20	PL	knf.gov.pl	–	✗	✗	103.195.6.231	64022	HK	[34986]	[PL]
May'20	SA	cmail.sa	–	✗	✗	194.152.42.16	47220	RO	[49474]	[SA]
Sep'20	TM	turkmenpost.gov.tm	–	✗	✗	185.229.225.228	41436	NL	[20661]	[TM]
Aug'20	US	manchesternh.gov	–	✗	✗	8.210.210.235	45102	SG	[13977]	[US]
Dec'20	US	batesvillearkansas.gov	host	✗	✗	95.179.153.176	20473	NL	[32244]	[US]
Apr'19	VN	ais.gov.vn	intranet	✓	✗	45.77.45.193	20473	SG	[131375,63748]	[VN]
Dec'20	VN	mofa.gov.vn	–	✗	✗	45.77.27.9	20473	JP	[24035]	[VN]
Mar'20	VN	cpt.gov.vn	–	✗	✗	103.213.244.205	136574	JP	[63747]	[VN]
Mar'20	VN	most.gov.vn	–	✗	✗	103.213.244.205	136574	JP	[38731,131373]	[VN]
Sep'20	VN	vass.gov.vn	–	✗	✗	47.74.3.121	45102	JP	[18403]	[VN]





https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/

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

Observable Infrastructure

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

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.snecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

Deployment #1

Scan #3

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

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

Deployment #2

Scan #3

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?

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 #4

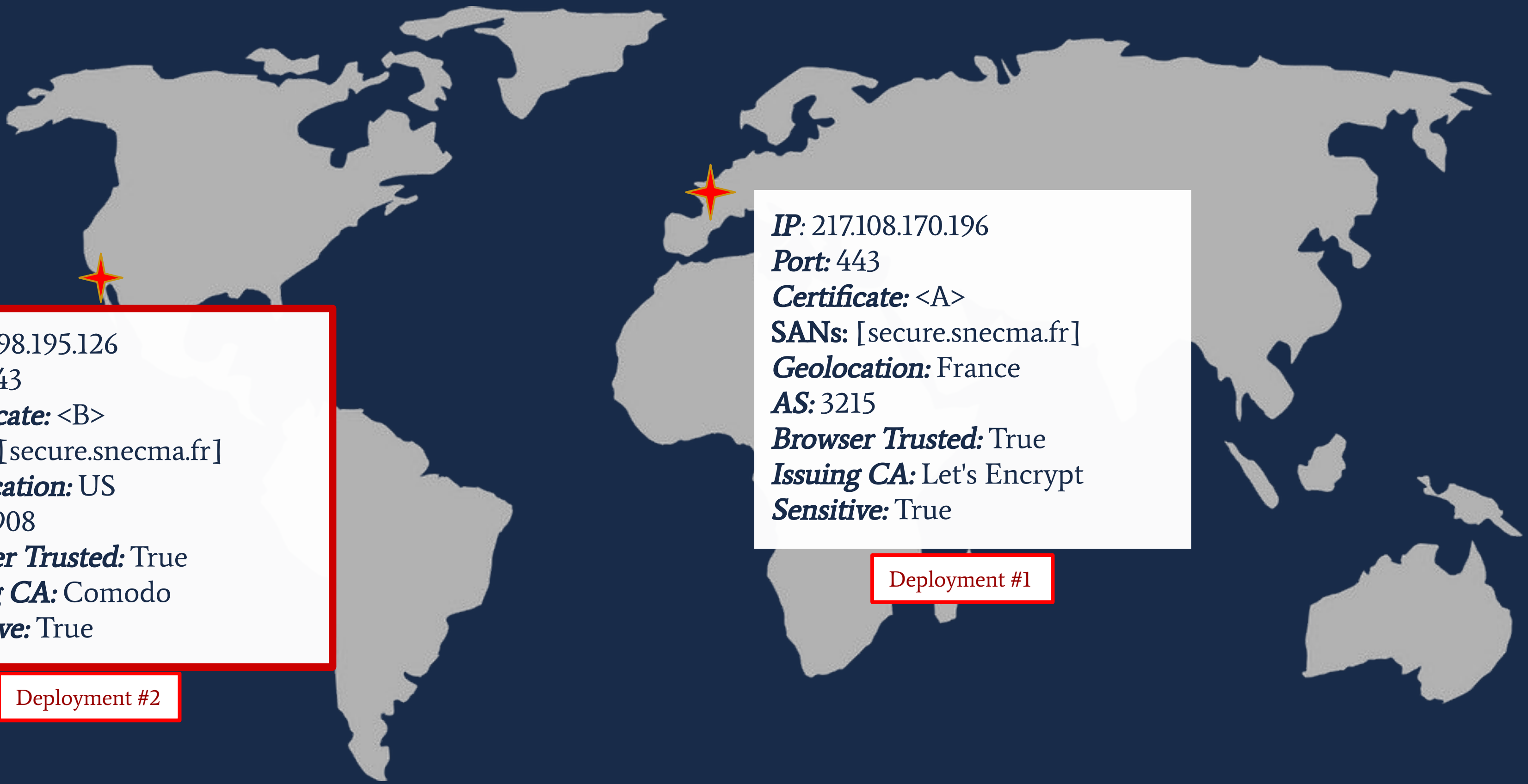
IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.snecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

Deployment #1

Longitudinal View: Deployment Maps

Date	*Stable Deployment*		*Transient Deployment*	
Scan #1	AS3215 [FR]	certs [A]		
Scan #2	AS3215 [FR]	certs [A]		
Scan #3	AS3215 [FR]	certs [A]	AS35908 [US]	certs [B]
Scan #4	AS3215 [FR]	certs [A]		

Suspicious Deployments → Potential Attacker Infrastructure



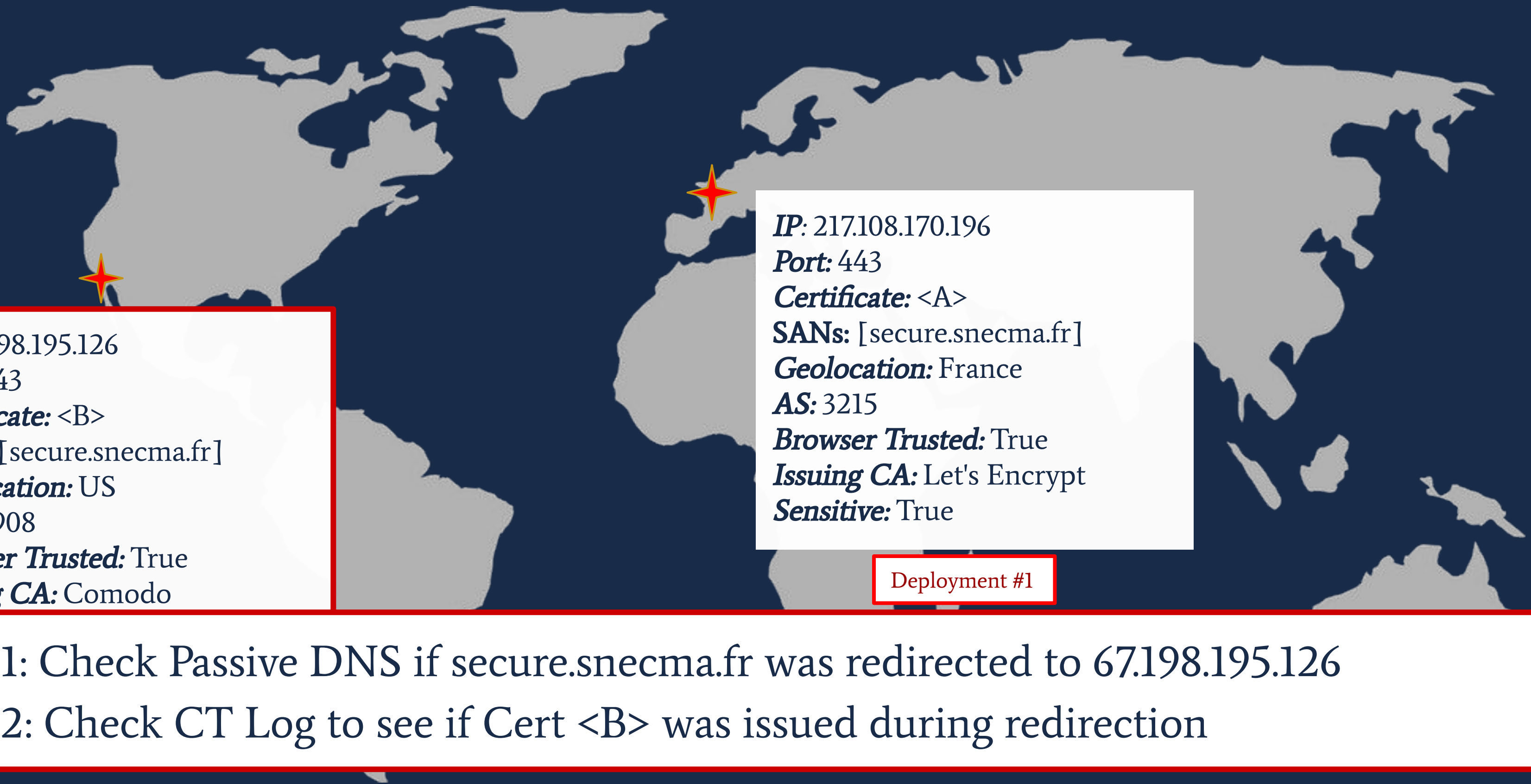
IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.snecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

Deployment #1

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

Deployment #2

Suspicious Deployments → Potential Attacker Infrastructure



IP: 67.198.195.126
Port: 443
Certificate: <B>
SANs: [secure.snecma.fr]
Geolocation: US
AS: 35908
Browser Trusted: True
Issuing CA: Comodo
Sen

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

#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