The Domain Name System

Part Two

•••

CS 249i : The Modern Internet

Winter 2024 | 29th January 2024

Gautam Akiwate

Goal

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

Terminology Revision

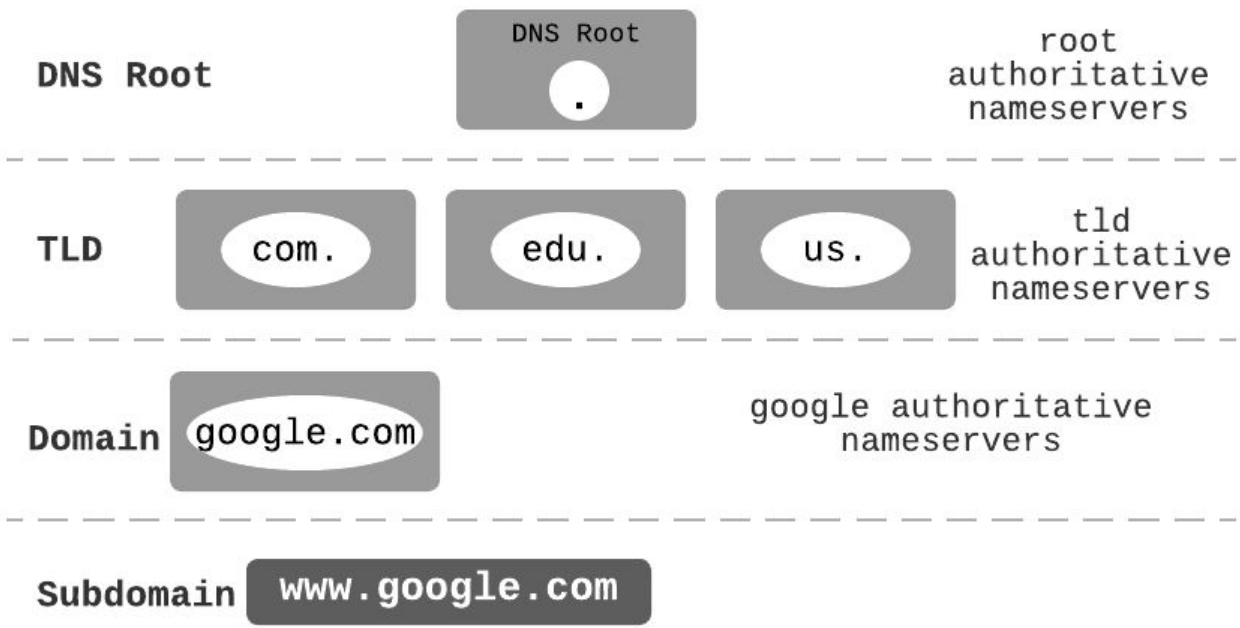
TLDs / ccTLDs / gTLDs

Zone / Zone files

Recursive Resolver / Authoritative Nameserver

Anycast

DNS Hierarchical Namespace



ICANN

VERISIGN

Google

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

Who Controls the Internet Address Book? ICANN, NTIA and IANA

Paul Rosenzweig | Saturday, March 15, 2014, 3:10 PM

LAWFARE

DNS Stakeholders

DNS Stakeholders

Registrant

Registrant is the domain owner.

DNS Stakeholders

Registrar

Registrar handles registration of domains.

Registrant

Registrant is the domain owner.

DNS Stakeholders

Registry

Registry handles operations

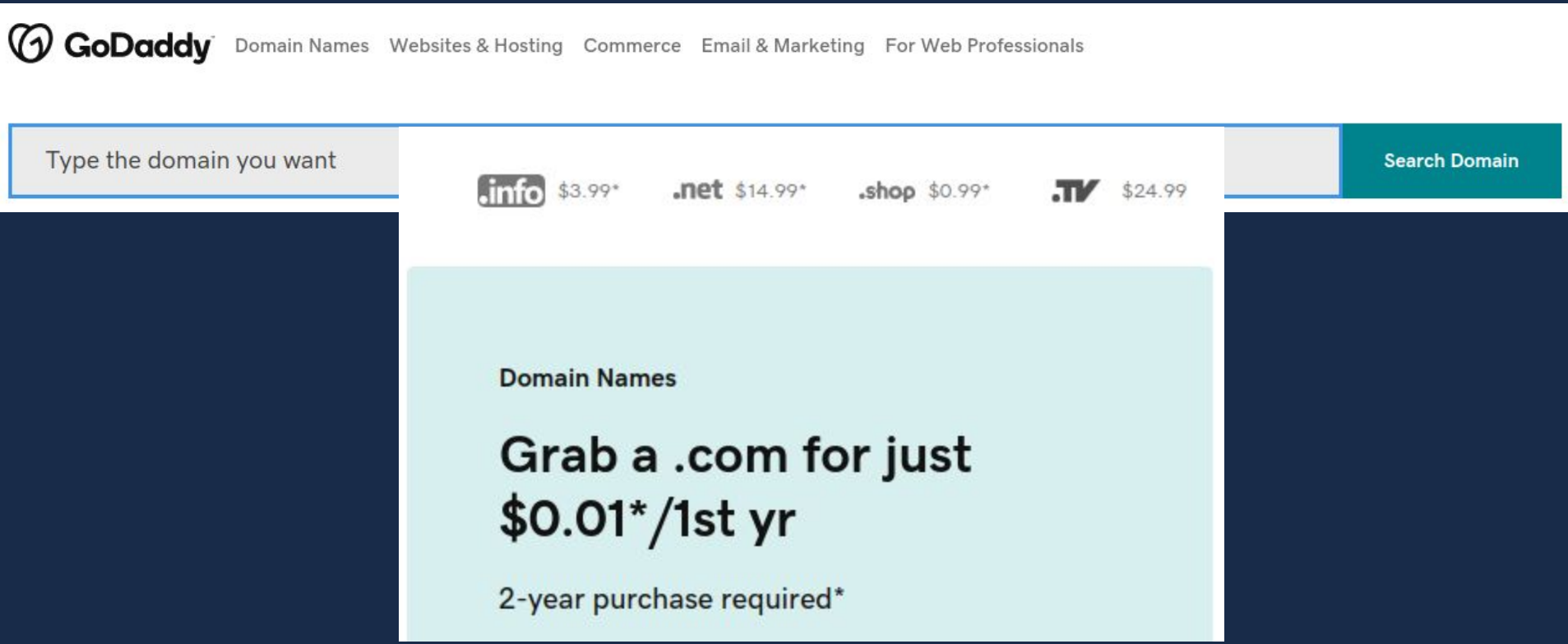
Registrar

Registrar handles registration of domains.

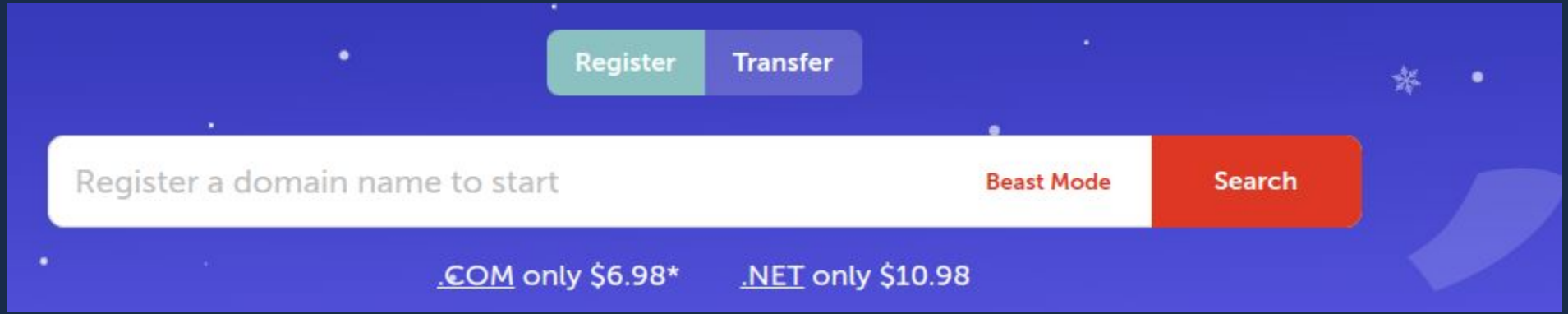
Registrant

Registrant is the domain owner.

How to Get a Domain?



How to Get a Domain?



How to get your own TLD?

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

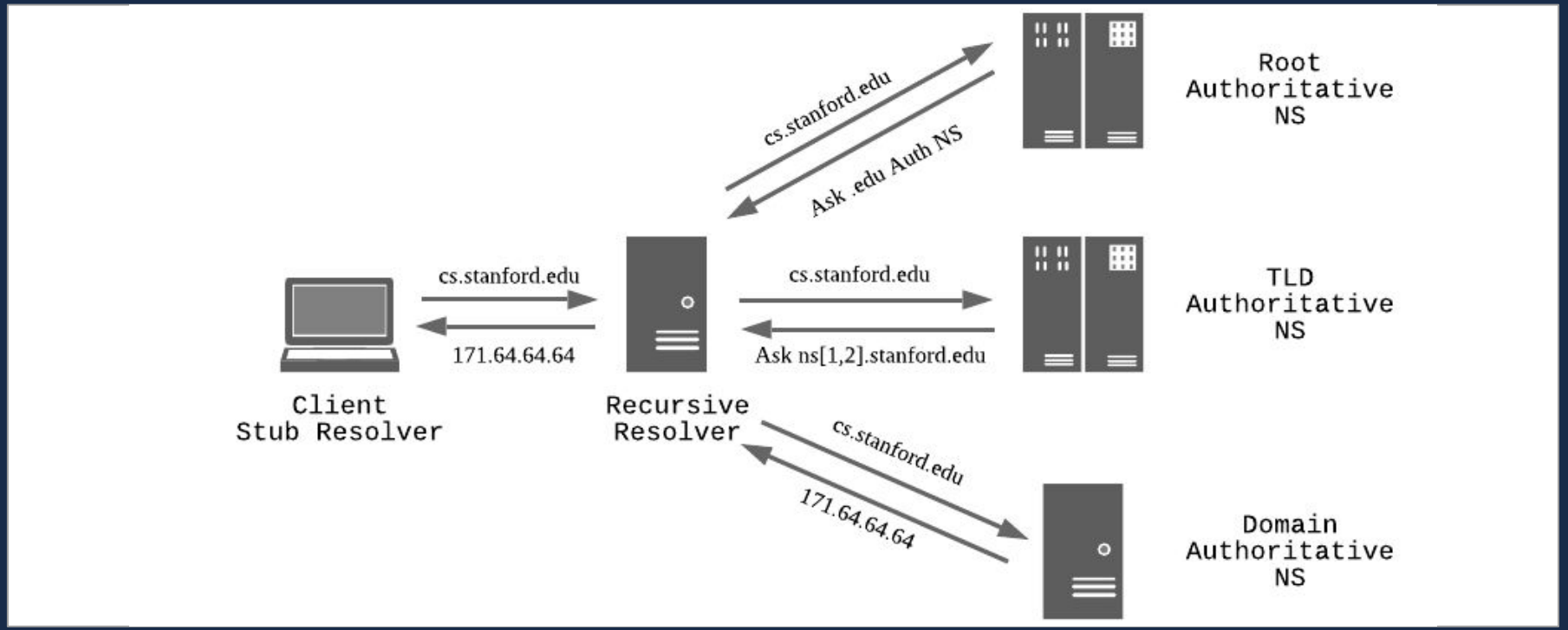
Blockchain DNS? Not official.

No guarantees about future namespace collisions.

Discussion

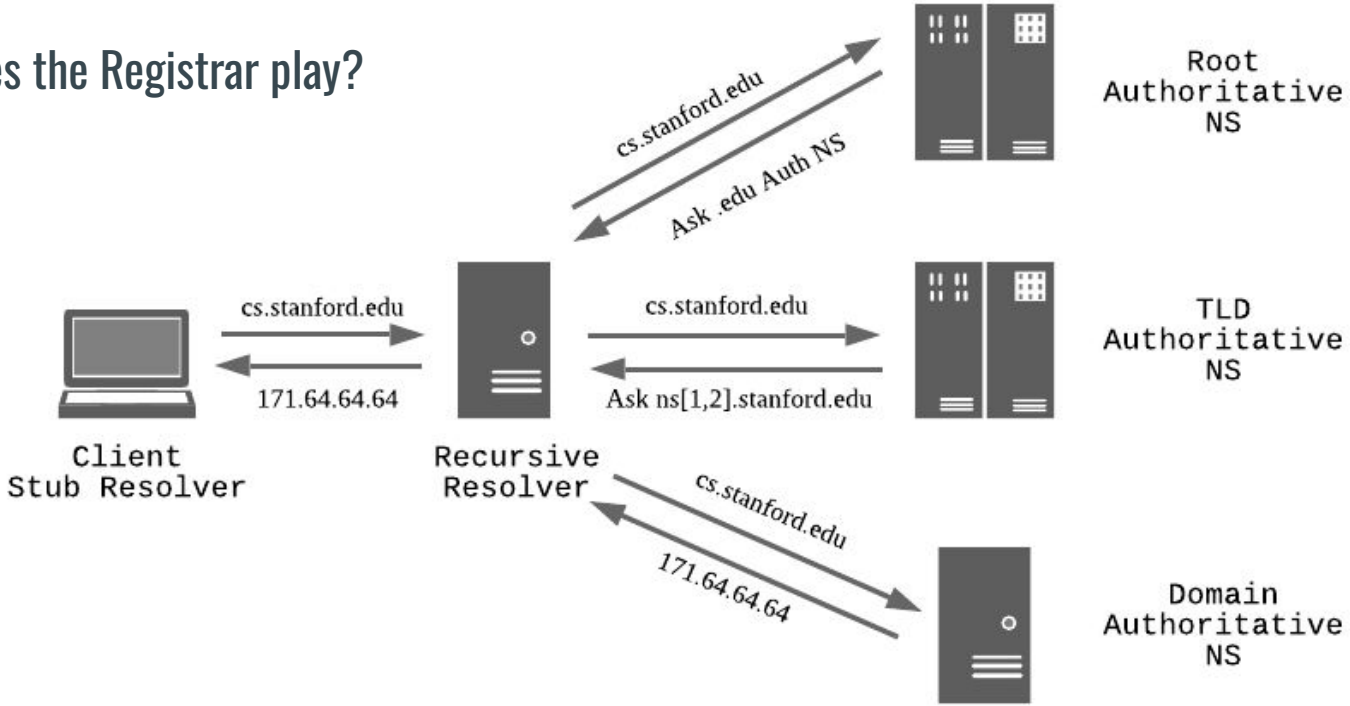
Why have separate registrars and registries?

Life of a DNS Query

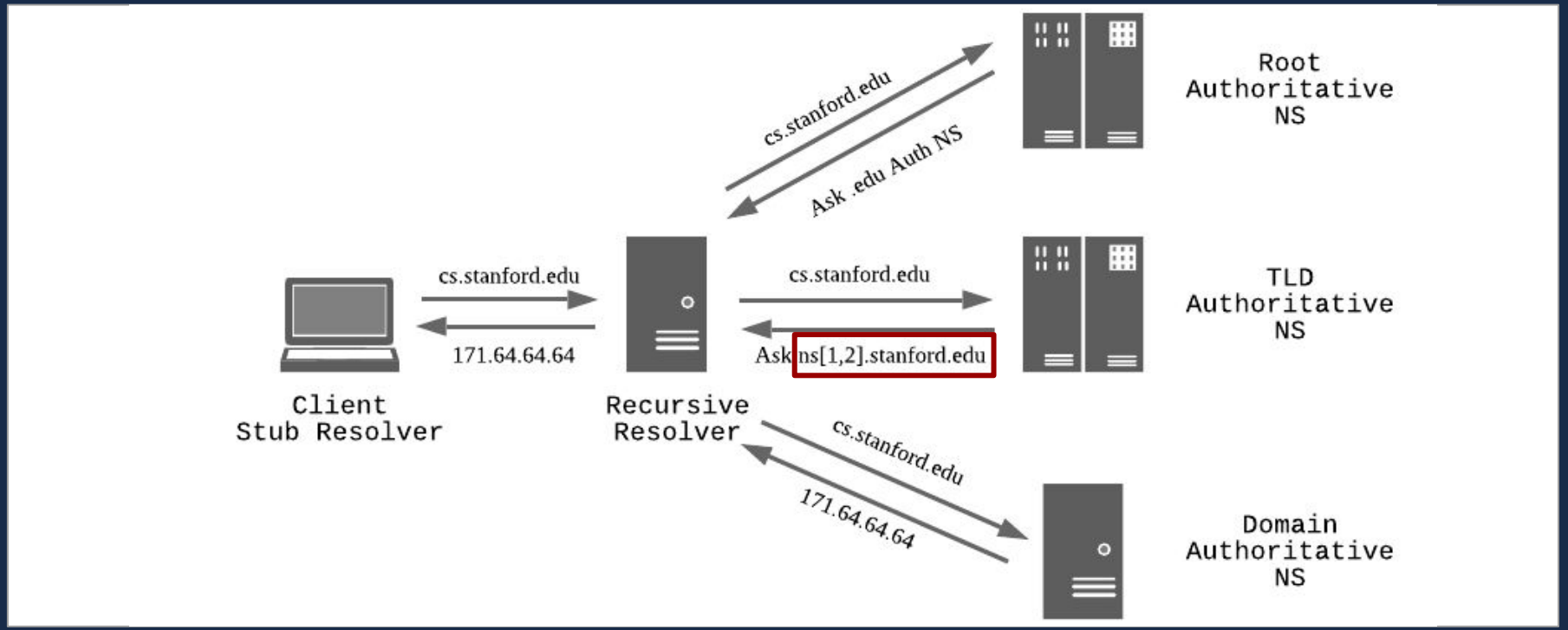


Life of a DNS Query

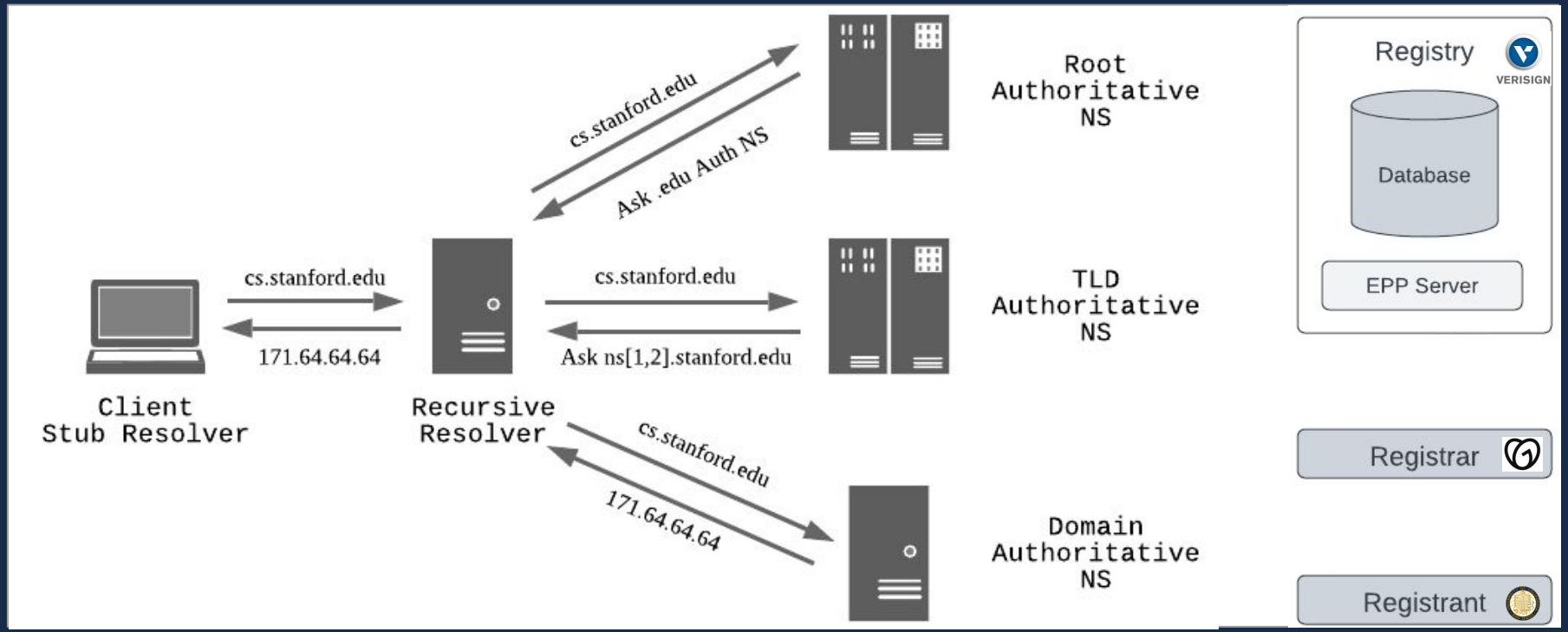
What role does the Registrar play?



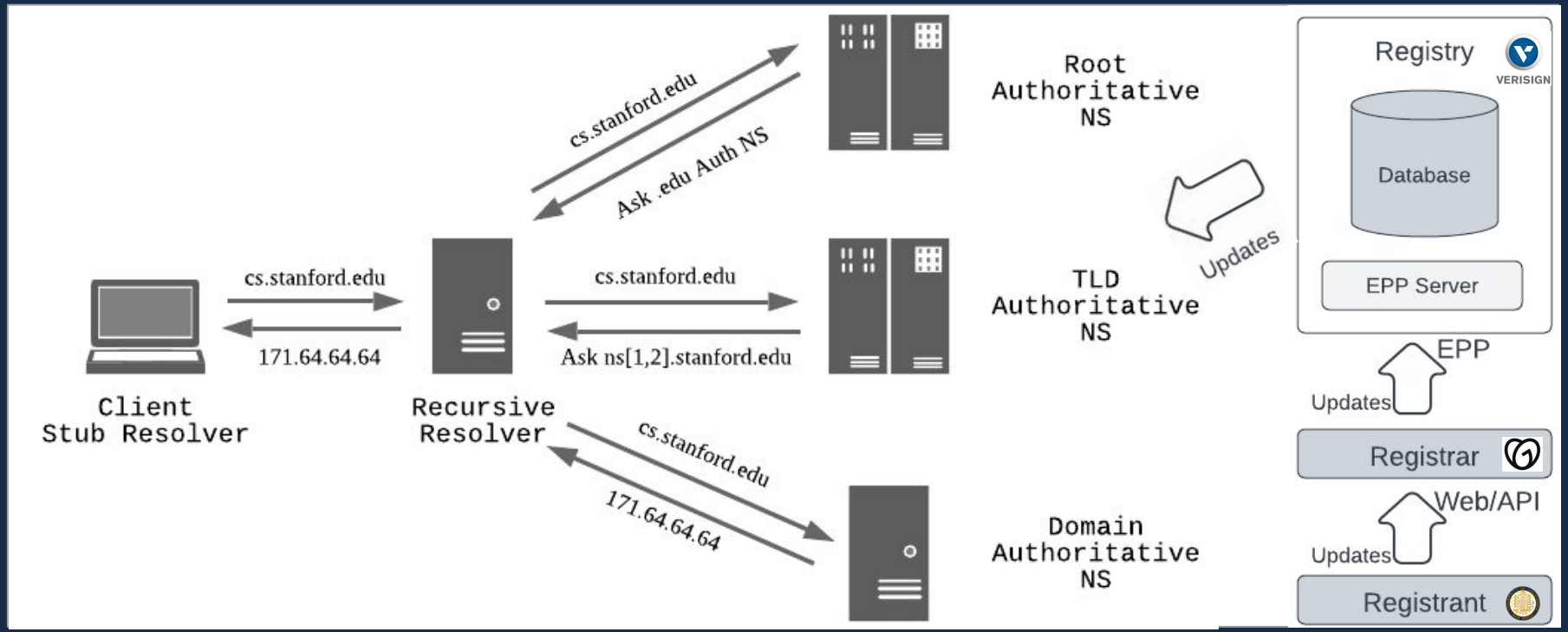
Life of a DNS Query



Configuration Updates

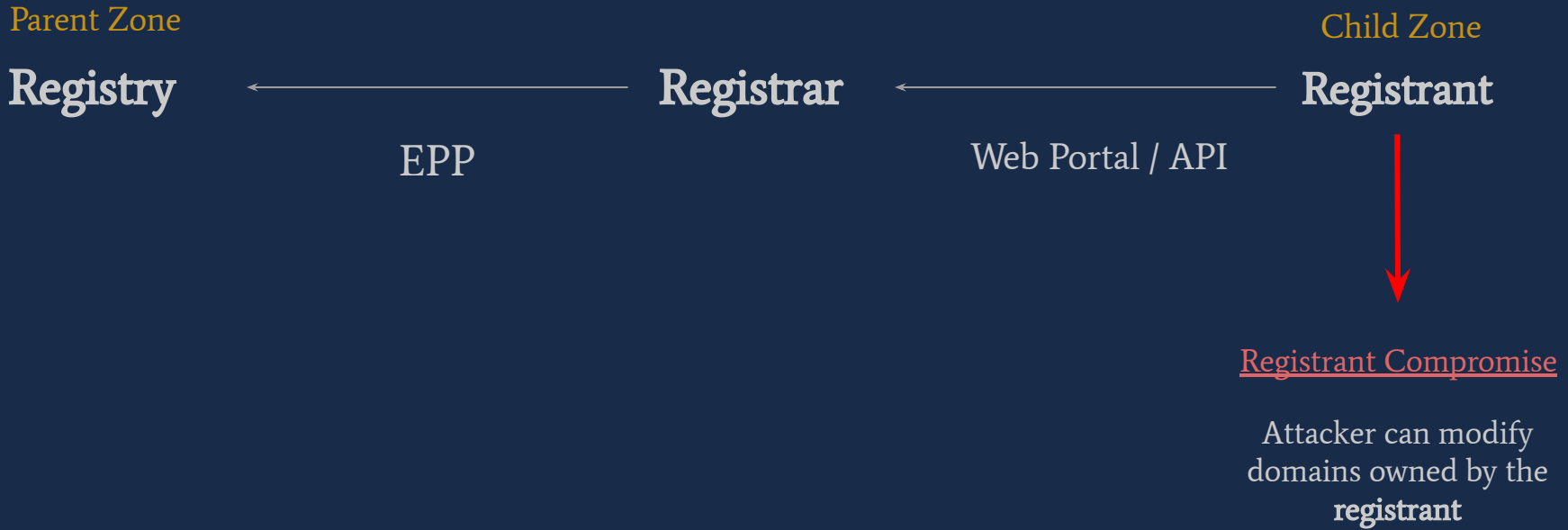


Configuration Updates



Ecosystem Threat Model

Ecosystem Threat Model



Ecosystem Threat Model

Registrar Compromise

Attackers typically compromise EPP credentials.

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

Registrant Compromise

Attacker can modify domains owned by the **registrant**

Ecosystem Threat Model

Registry Compromise

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

Registrar Compromise

Attackers typically compromise EPP credentials.

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

Registrant Compromise

Attacker can modify domains owned by the **registrant**

The Problem: Attackers Targeting DNS Infrastructure

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

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

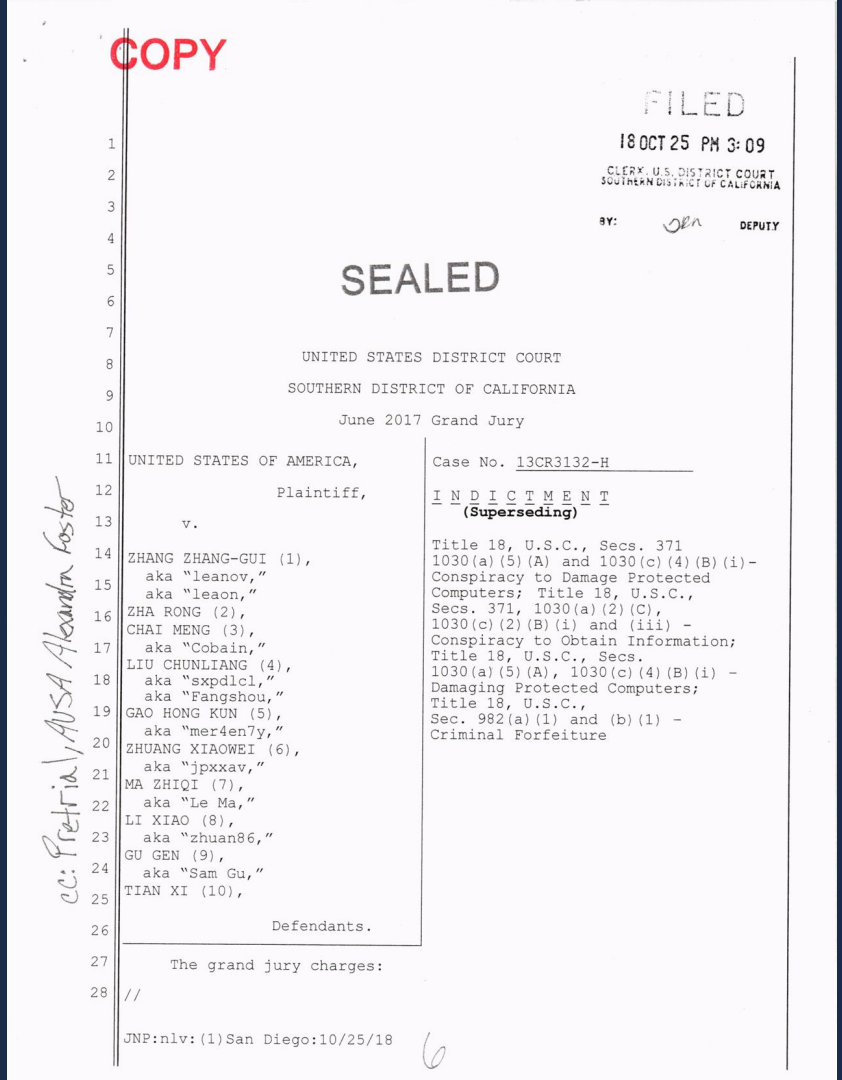
BUSINESS NEWS

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

Exclusive: France's Snecma targeted by hackers - researcher

Broader Context

- Part of a larger coordinated attack against ***aerospace*** companies.



COPY

FILED
18 OCT 25 PM 3:09
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY: DEPUTY

SEALED

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

June 2017 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

ZHANG ZHANG-GUI (1),
aka "leanov,"
aka "leaon,"
ZHA RONG (2),
CHAI MENG (3),
aka "Cobain,"
LIU CHUNLIANG (4),
aka "sxpdlcl,"
aka "Fangshou,"
GAO HONG KUN (5),
aka "mer4en7y,"
ZHUANG XIAOWEI (6),
aka "jpxxav,"
MA ZHIQI (7),
aka "Le Ma,"
LI XIAO (8),
aka "zhuan86,"
GU GEN (9),
aka "Sam Gu,"
TIAN XI (10),

Defendants.

Case No. 13CR3132-H

INDICTMENT
(Superseding)

Title 18, U.S.C., Secs. 371 1030(a)(5)(A) and 1030(c)(4)(B)(i)- Conspiracy to Damage Protected Computers; Title 18, U.S.C., Secs. 371, 1030(a)(2)(C), 1030(c)(2)(B)(i) and (iii) - Conspiracy to Obtain Information; Title 18, U.S.C., Secs. 1030(a)(5)(A), 1030(c)(4)(B)(i) - Damaging Protected Computers; Title 18, U.S.C., Sec. 982(a)(1) and (b)(1) - Criminal Forfeiture

The grand jury charges:

//

JNP:nlv:(1)San Diego:10/25/18

cc: Fedrin, AUSA Alexandra Foster

Broader Context

- Part of a larger coordinated attack against ***aerospace*** companies.
- Use of many known tactics
  - Spear phishing
  - Malware
  - Doppelganger Domains

c. Members of the conspiracy used a variety of computer intrusion tactics, alone or in combination, including but not limited to:

i. Spear phishing, the use of fictitious emails embedded with malicious code (malware) that facilitated access to the email recipient's computer and connected network,

ii. Malware, including but not limited to certain malware, such as Sakula and IsSpace, that was uniquely used by members of the conspiracy during the period of the conspiracy,

iii. Doppelganger Domain Names, the creation and use of domain names that closely resemble legitimate domain names to trick unwitting recipients of spear phishing emails,

iv. Dynamic Domain Name Service (DNS) Accounts, a service of DNS providers that allows users, including members of the conspiracy, to register one or more domain names under a single account and frequently change the Internet Protocol (IP) address assigned to a registered domain name.

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,

vi. Watering Hole Attacks, the installation of malware on legitimate web pages of victim companies to facilitate intrusions of computers that visited those pages, and

vii. Co-Opting Victim Company Employees, the use of insiders at victim companies to facilitate computer intrusions or monitor investigations of computer intrusion activity.

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,

c. Members of the conspiracy used a variety of computer intrusion tactics, alone or in combination, including but not limited to:

i. Spear phishing, the use of fictitious emails embedded with malicious code (malware) that facilitated access to the email recipient's computer and connected network,

ii. Malware, including but not limited to certain malware, such as Sakula and IsSpace, that was

uniquely used by members of the conspiracy

racy,

creation and use

emble legitimate

g recipients of

NS) Accounts, a

allows users,

acy, to register

single account

et Protocol (IP)

domain name.

nise of domain

members of the

company's domain

a malicious IP

address in order to facilitate computer

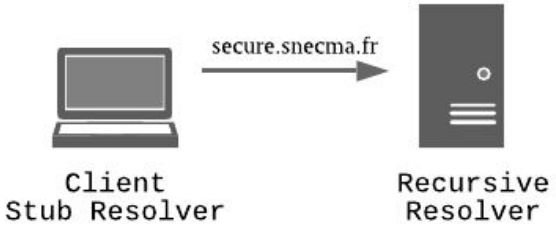
intrusions,

vi. Watering Hole Attacks, the installation of malware on legitimate web pages of victim companies to facilitate intrusions of computers that visited those pages, and

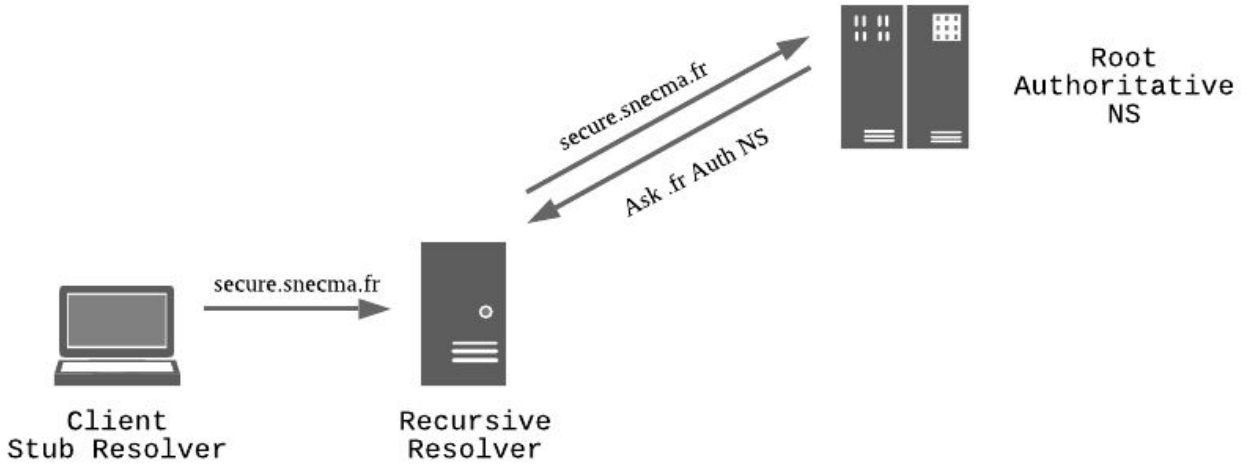
vii. Co-Opting Victim Company Employees, the use of insiders at victim companies to facilitate computer intrusions or monitor investigations of computer intrusion activity.

Domain Hijack In Practice

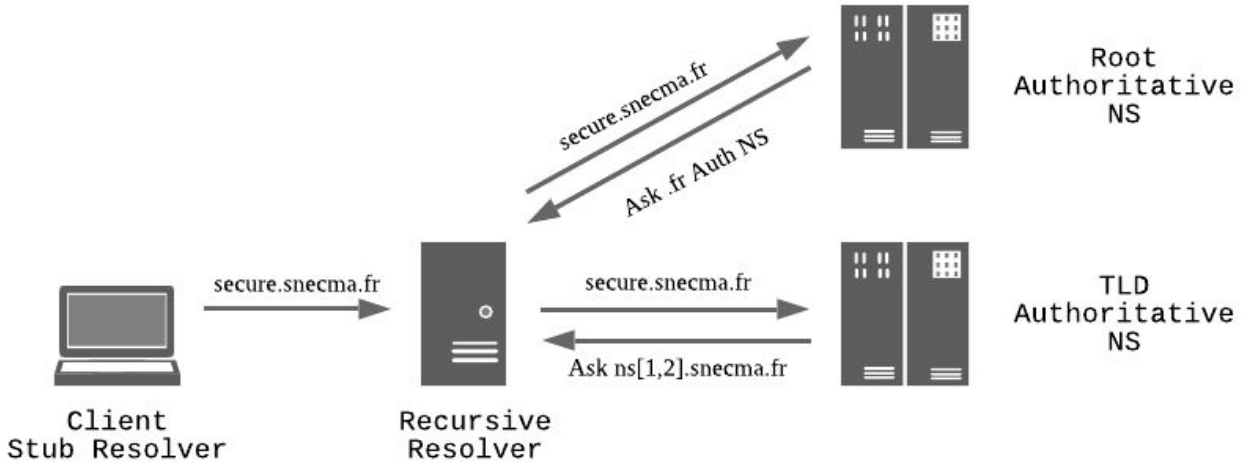
Client Logging Into “Secure” Network...



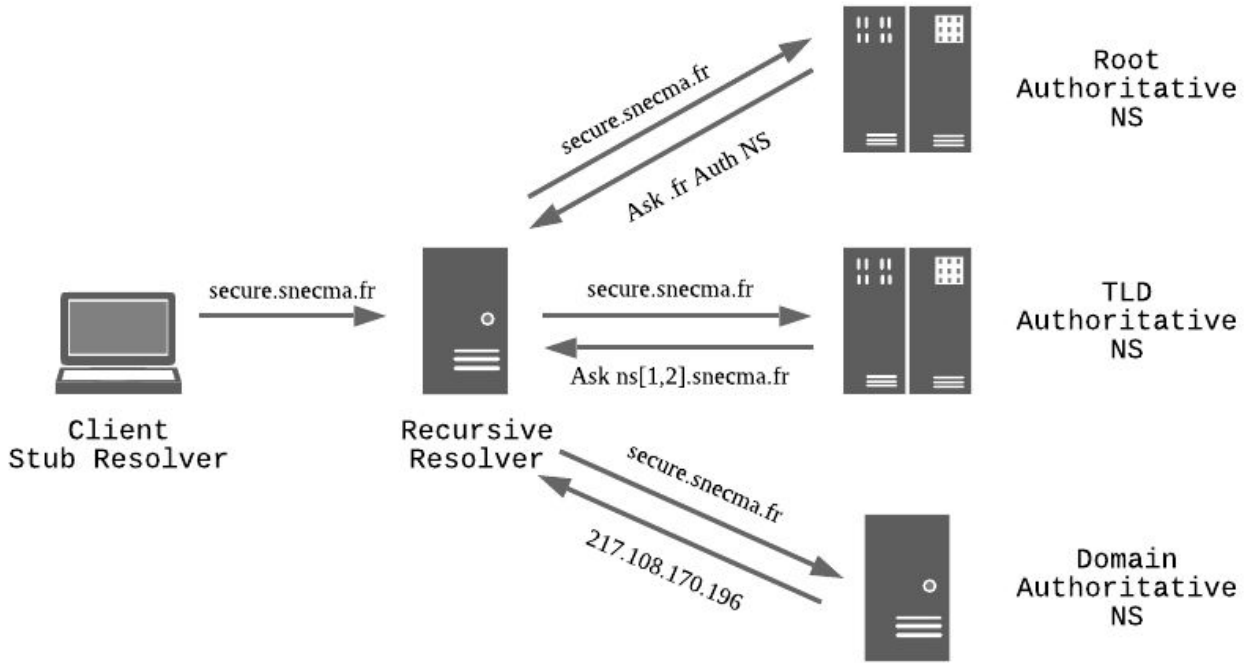
Normal Resolution



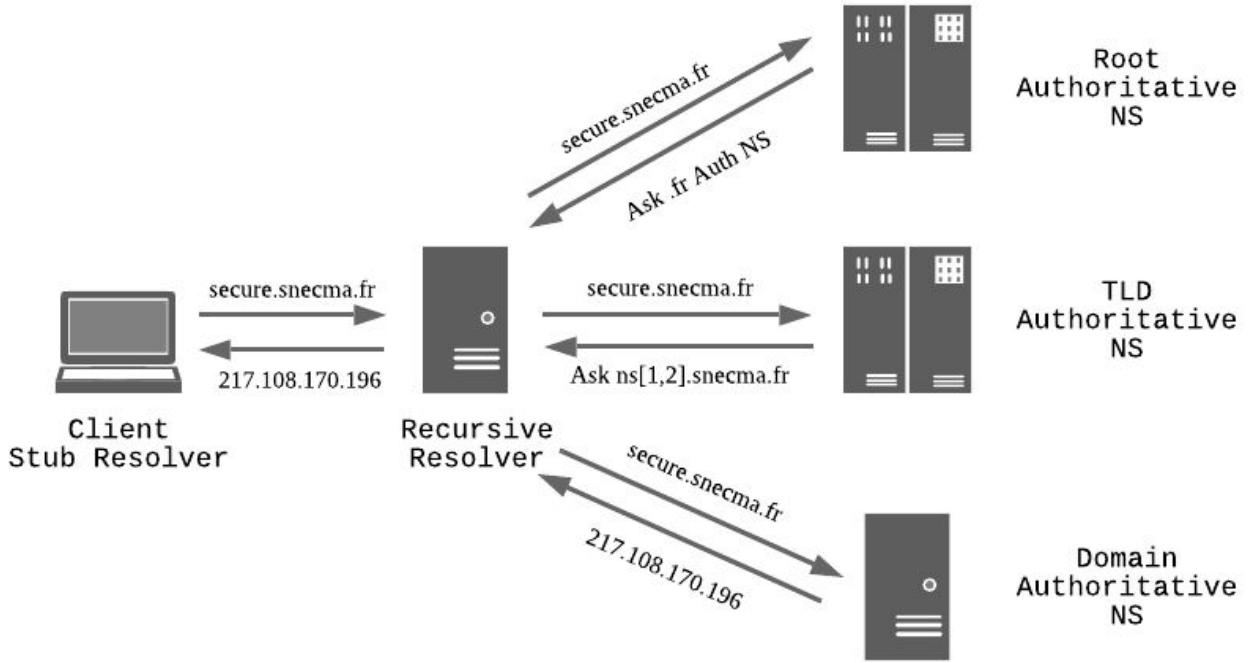
Normal Resolution



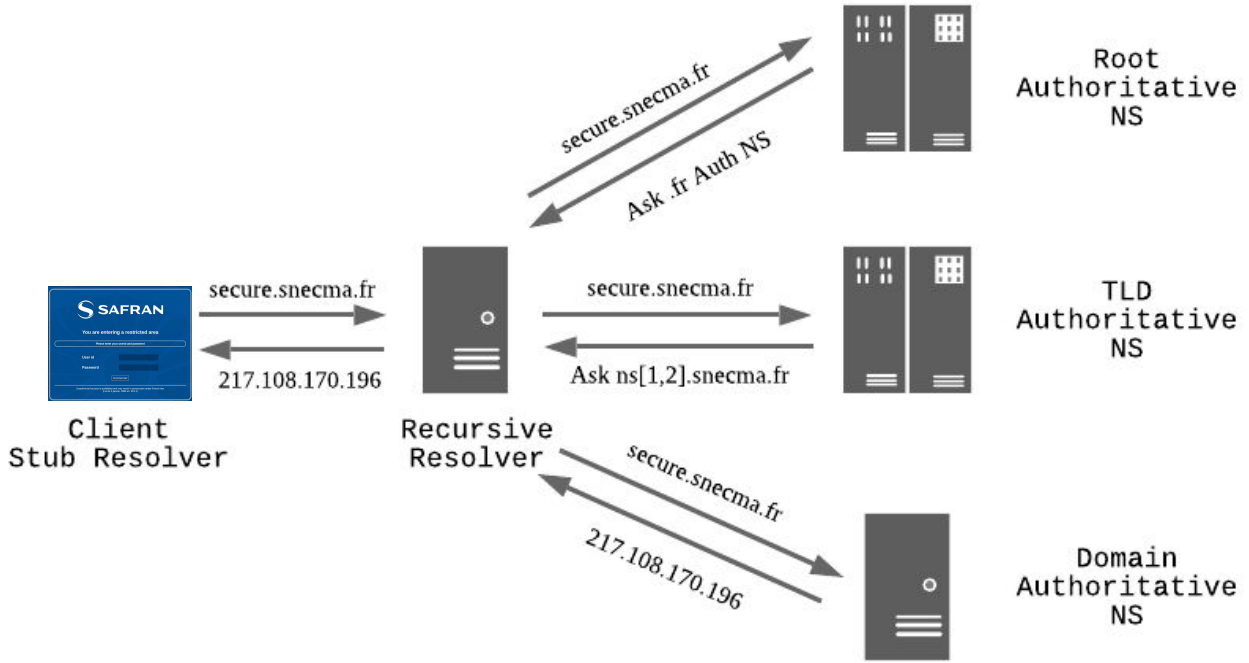
Normal Resolution



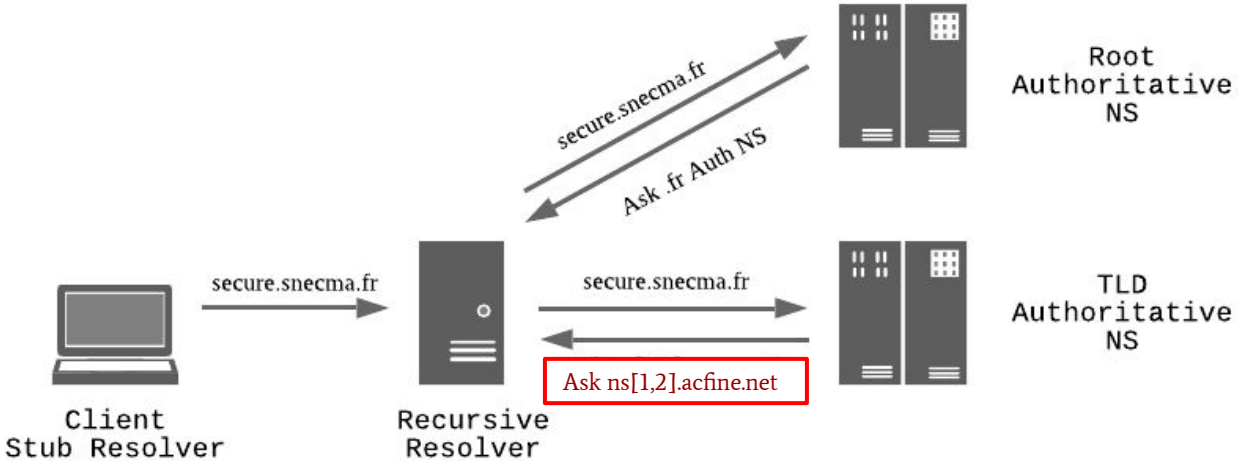
Normal Resolution



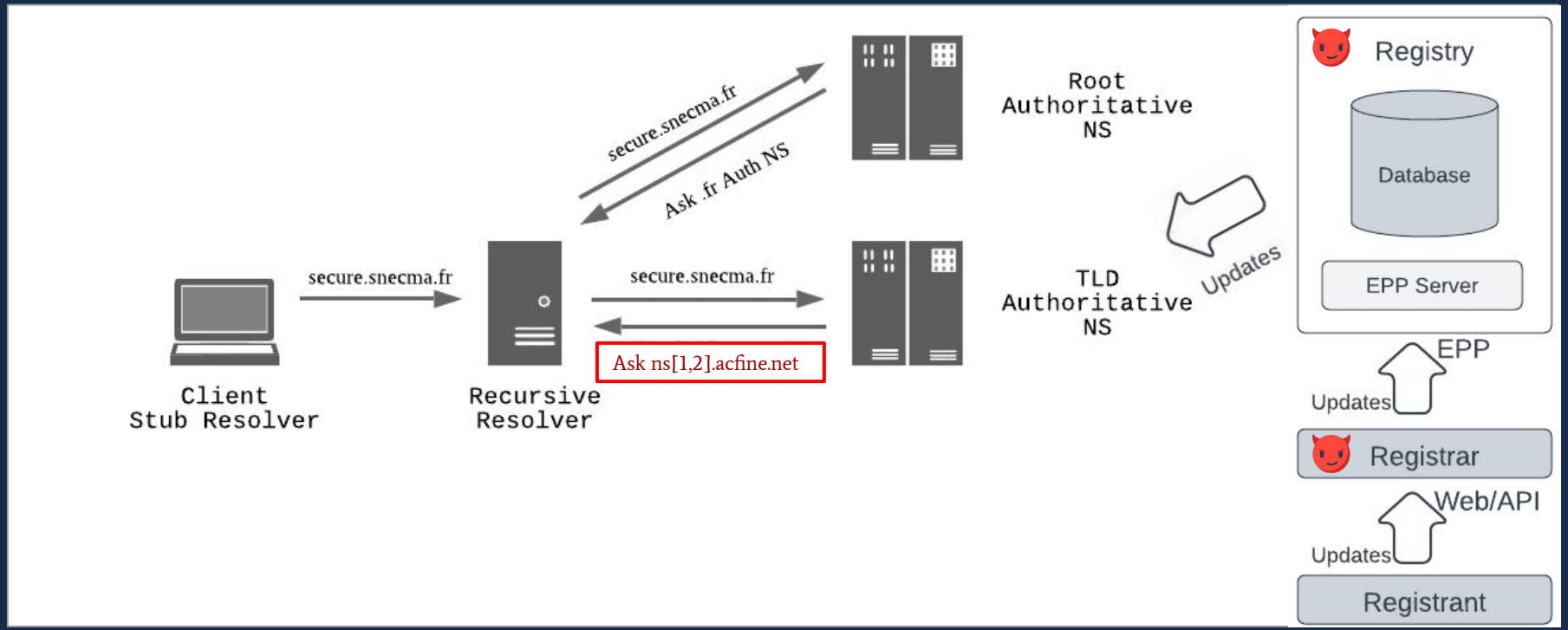
Normal Resolution



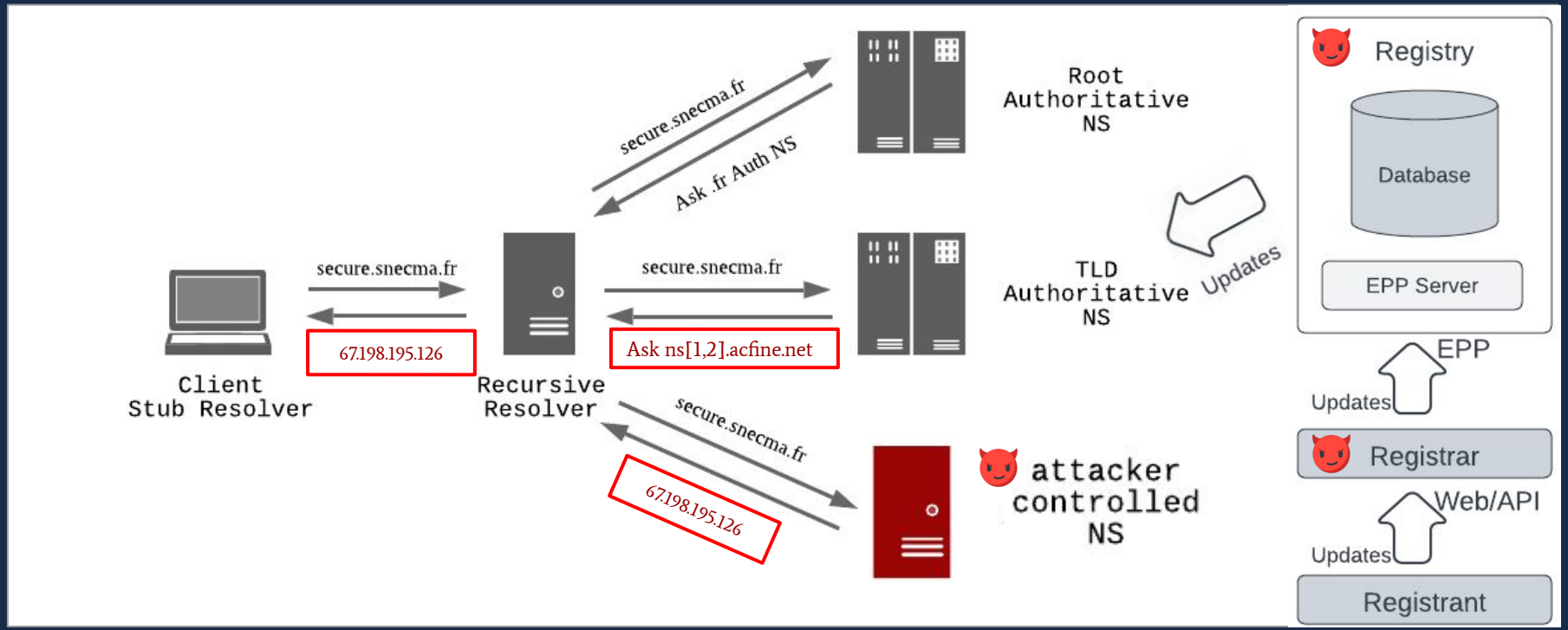
Malicious DNS Delegation Update (Circa 2014)



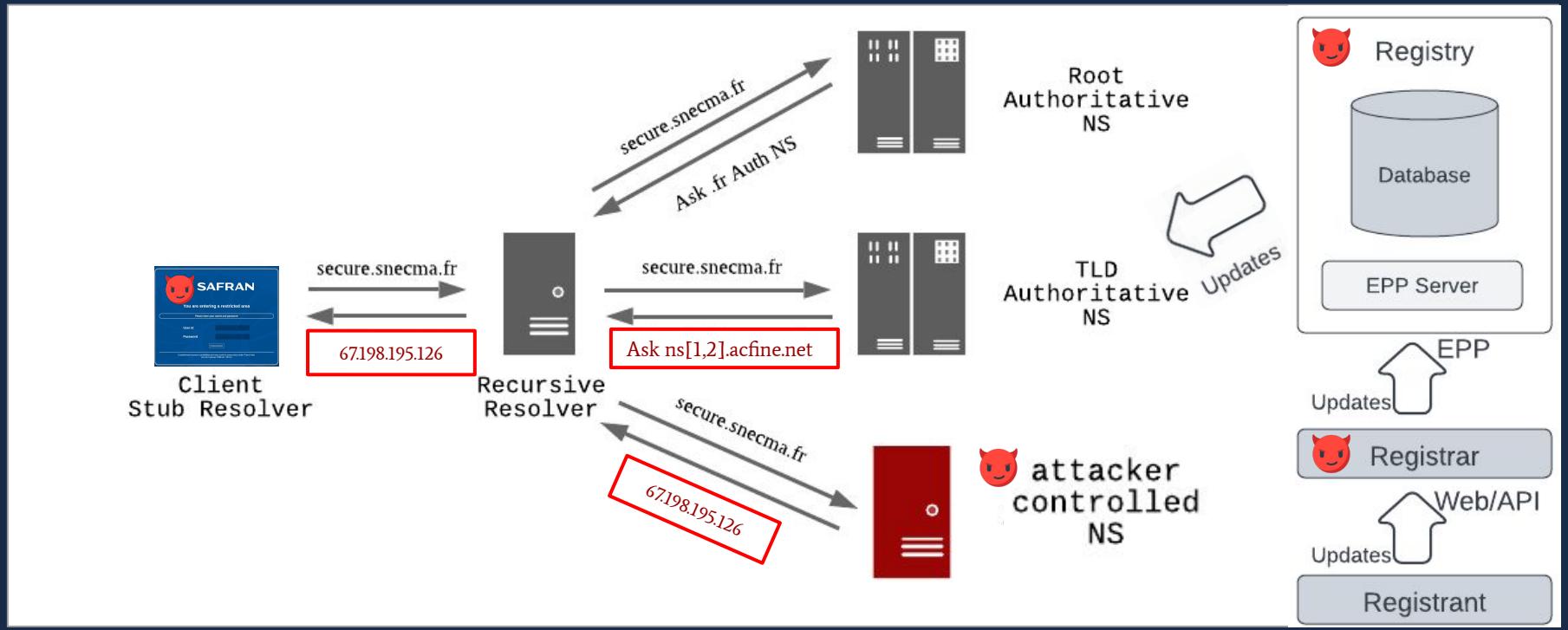
Attackers Target DNS Delegation Update Mechanism



Attackers Redirect All Users



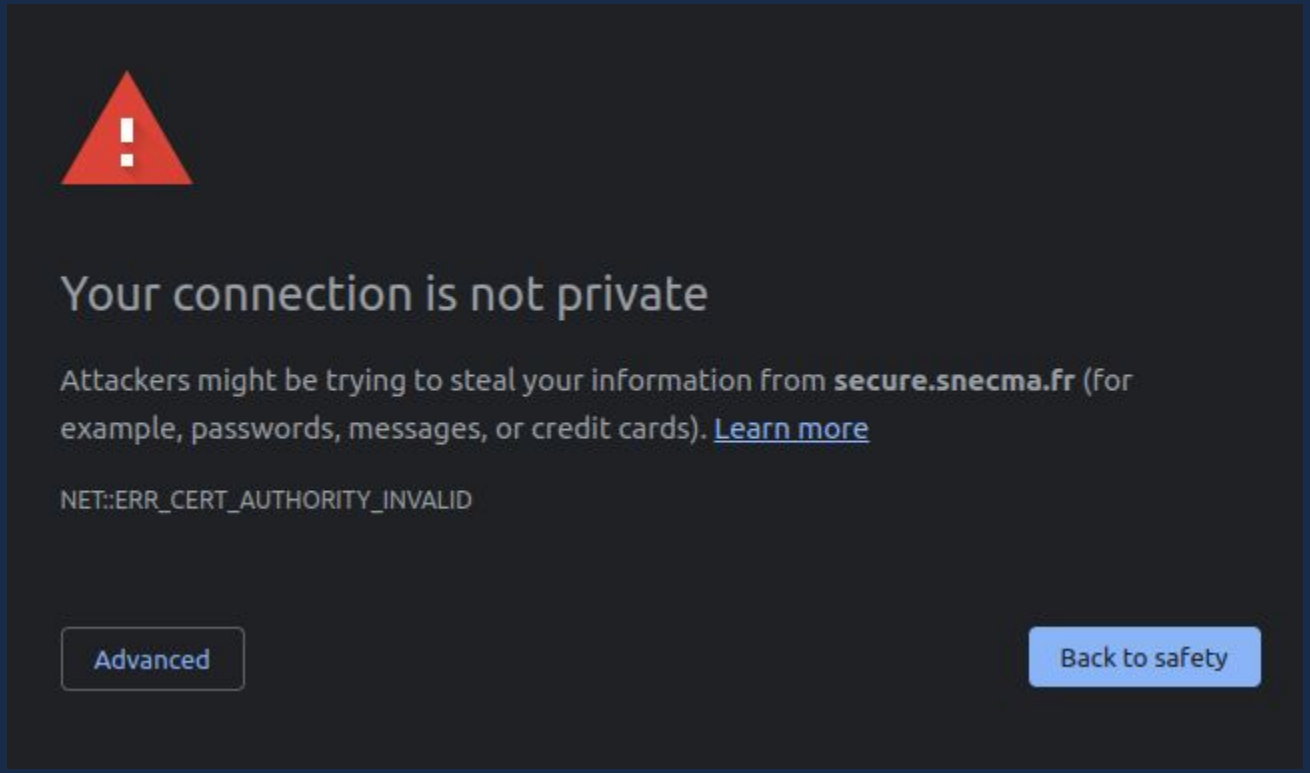
Attackers Redirect All Users



Next Stage of Attack

- Prompt malicious downloads
- Mimic webpage to harvest credentials

What about TLS Certificates?

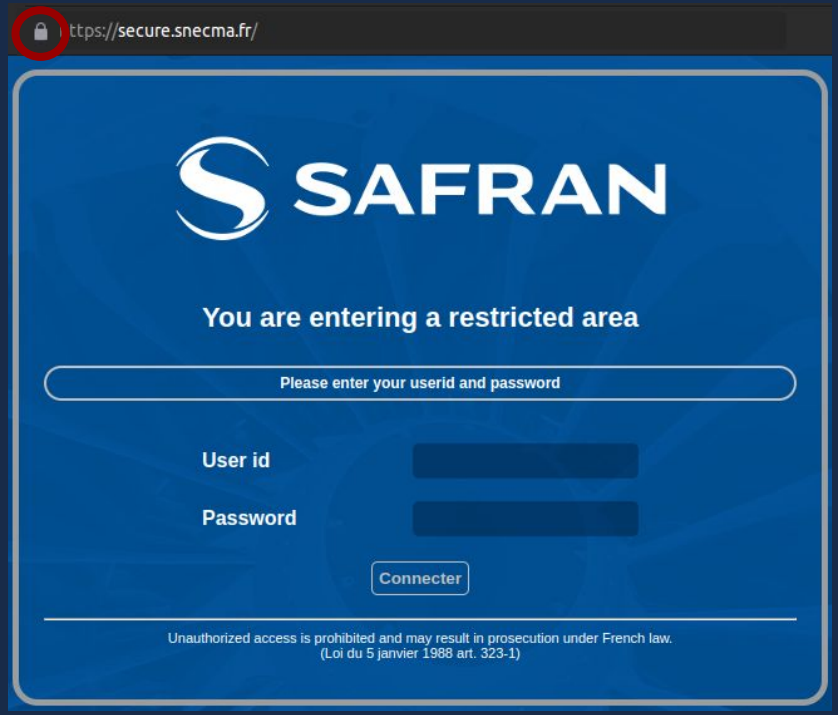


Implicit Trust Dependence

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

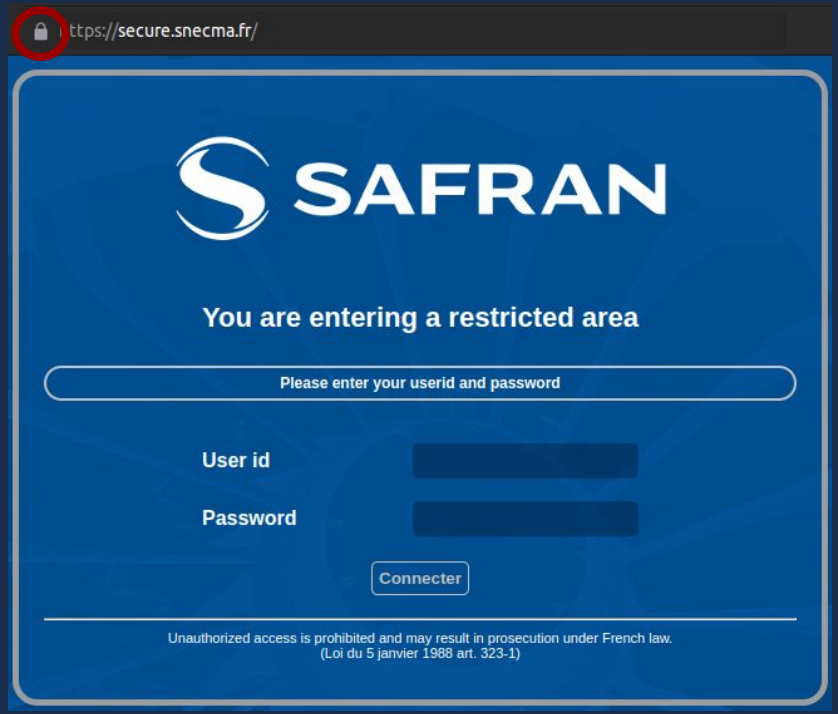
Implicit Trust Dependence

- 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 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.

y. On August 28, 2013, LIU sent MA a link to a news article that explained how the Syrian Electronic Army (SEA) had hacked into the computer systems of Company L, a domain registrar, in order to facilitate intrusions.

z. On December 3, 2013, members of the conspiracy used the same method as the SEA to hack into the computer systems of Company L and hijack domain names of Company H, which were hosted by Company L.

aa. On December 3, 2013, a member of the conspiracy installed Sakula malware on Company H's computer network and caused the malware to send a beacon to a doppelganger domain name under the control of one or more members of the conspiracy. Notably, the doppelganger domain name was designed to resemble the real domain of Company A, which had previously been hacked by members of the conspiracy.

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

Hijacked Domains (Retroactive Identification)

Identified 41 domains as hijacked (between 2017-2020)

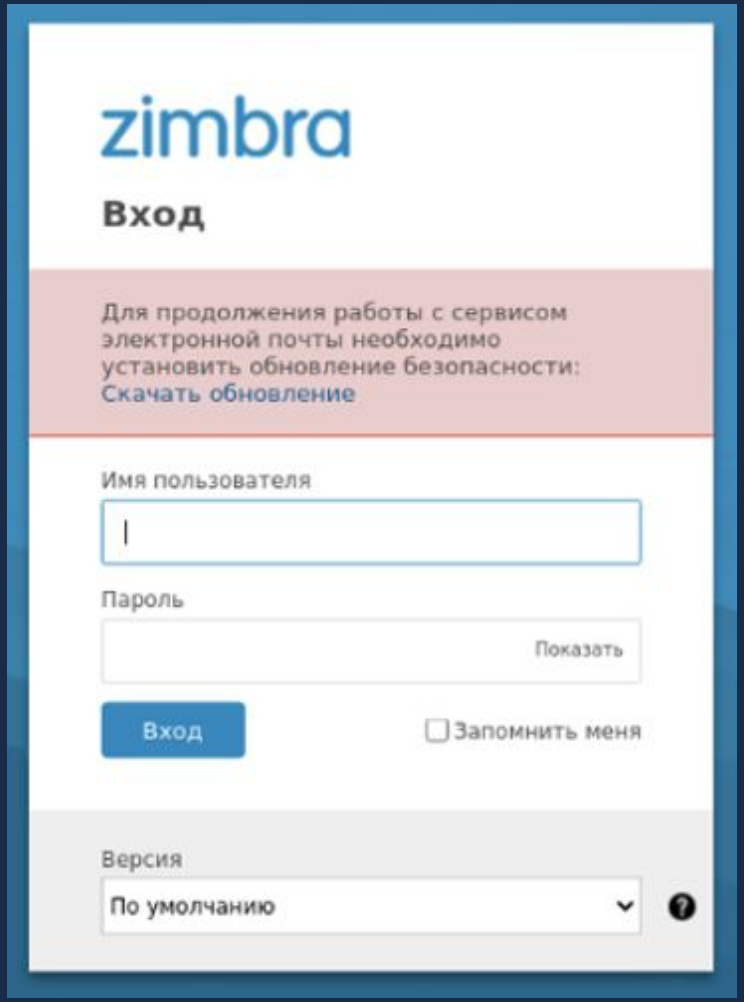
- 33 domains re-identified and verified from previous reports
- 8 domains not previously identified

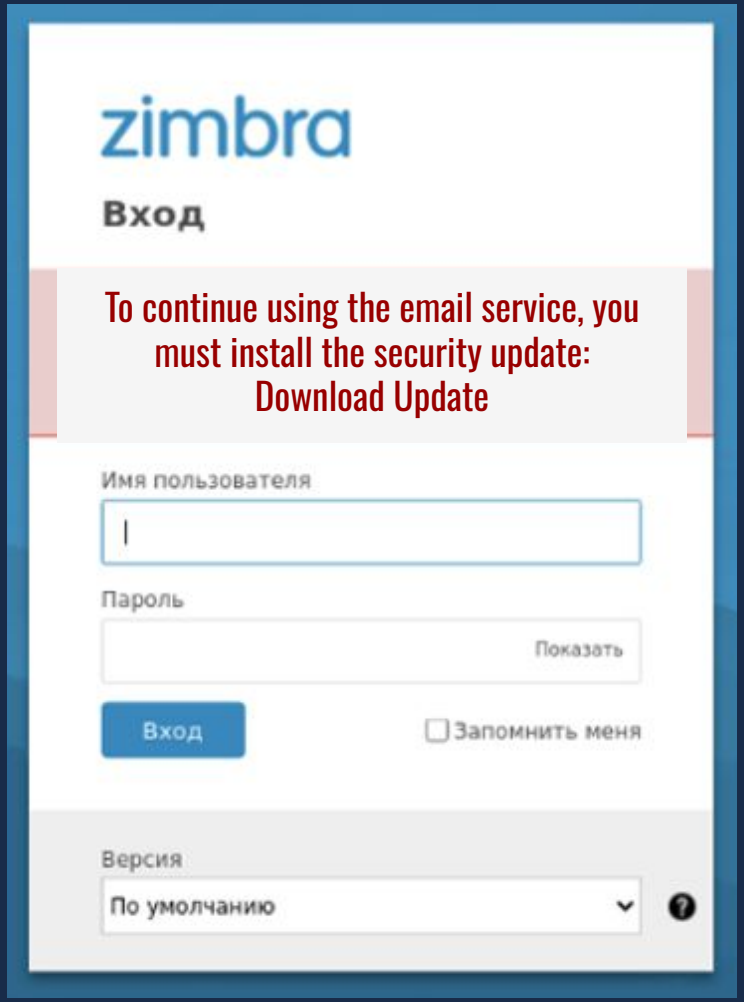
High confidence manually evaluated hijacks!

Many many more domains where there is circumstantial evidence

Kyrgyzstan Hijacks

	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





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

Type	Hij.	Targeted Domain Information			Cross Ref		Attacker Infra. (Transient)			Legitimate Infra. (Stable)	
		CC	Domain	Sub.	pDNS	crt	IP	ASN	CC	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	–	–


THE DNS
1-603-532-6088
1-800-382-0204
1-603-532-6088
1-800-382-0204
IS DARK AND FULL OF TERRORS
imgflip.com

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?

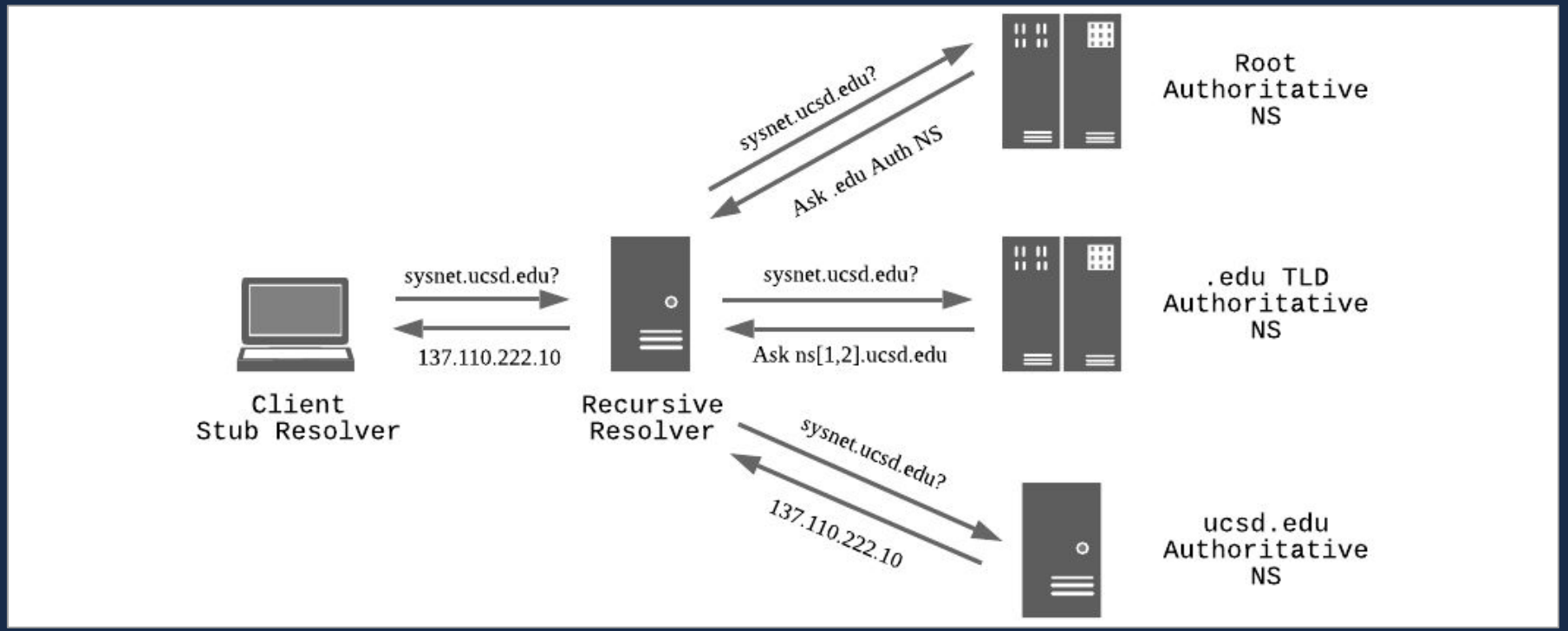
Does it matter if they are modified?

SSL Certificates to the rescue(?) !

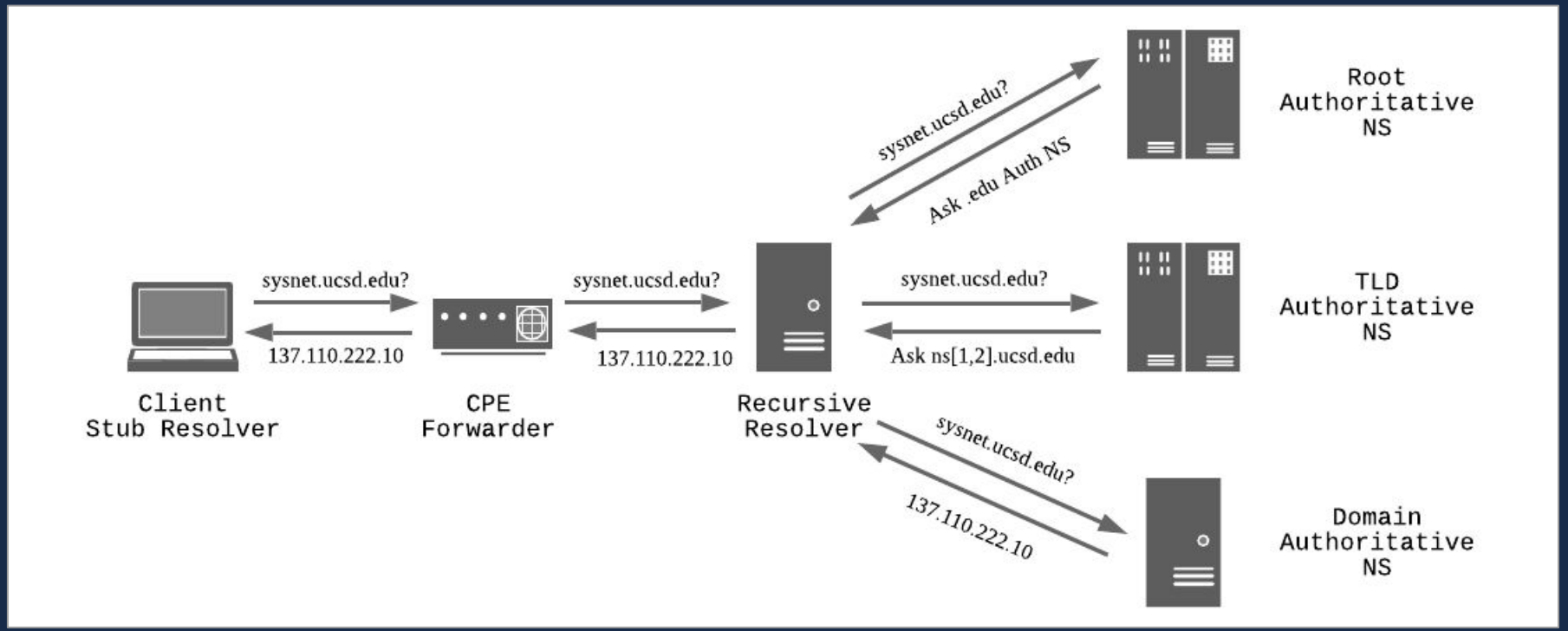
DNS Interception

- Intercept DNS Queries
  - Exploit lack of integrity check on DNS responses
- Interception by whom?
  - ISPs
  - Governments
  - Companies
- Interception where?

Where can Interception occur?



Where can Interception occur?



DNS Interception: Why?

- Censorship
- Parental Controls/Firewalls/Security
- Advertising
    - Take over NXDOMAIN queries.

Discussion

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*.

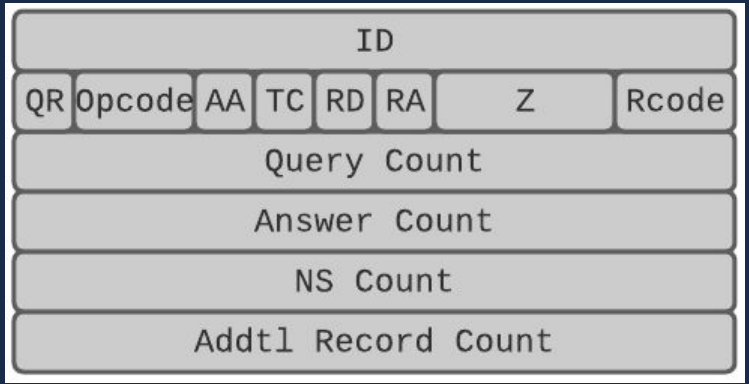
- Webpage on www.example.com does not load
- You see your mail at you@example.com stop.

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 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?

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!

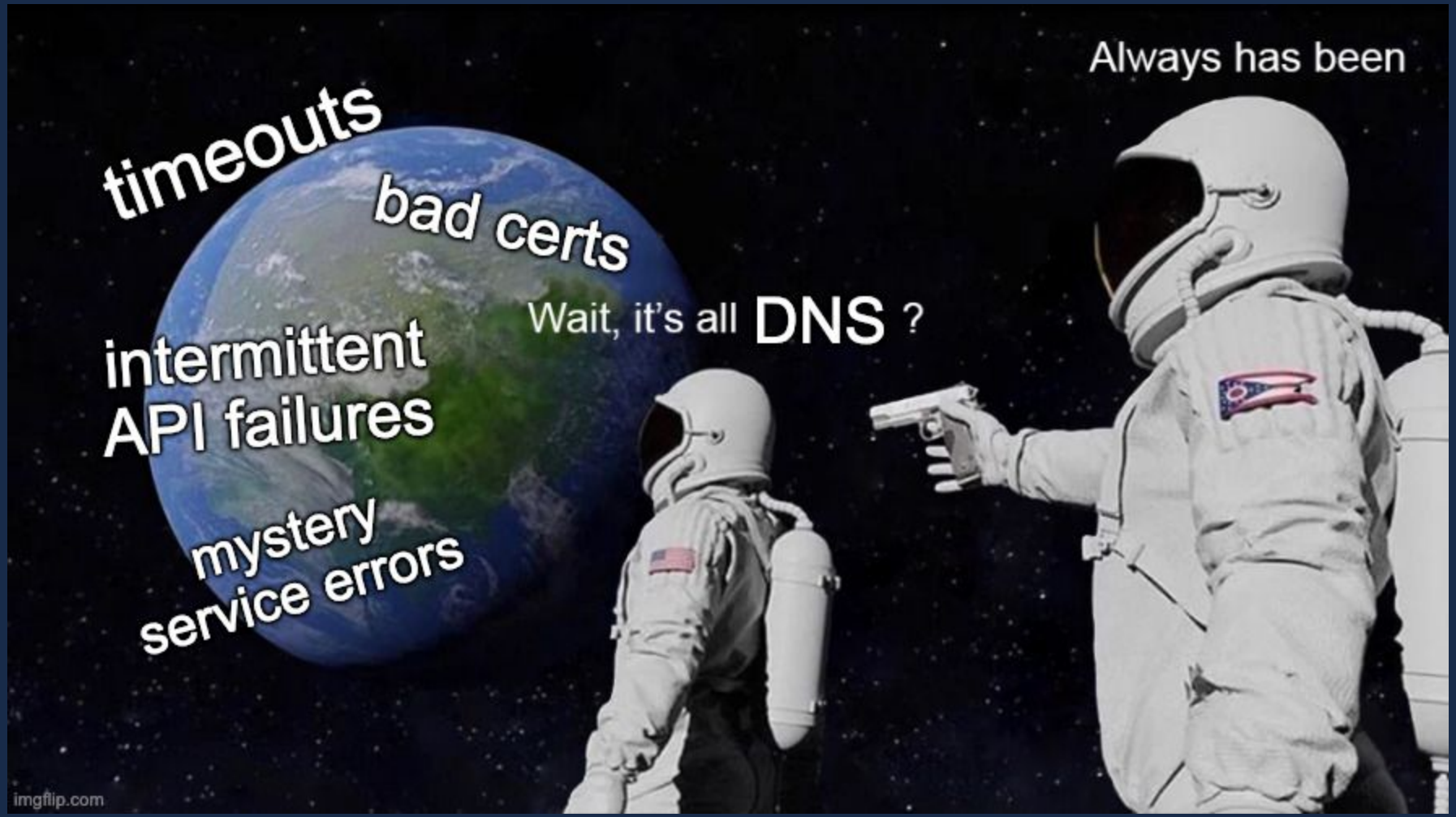
Discussion

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
imgflip.com

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