Retroactive Identification of Targeted Domain Hijacks

•••

NANOG 87 | Atlanta, Georgia
14th February 2023

Gautam Akiwate, Raffaele Sommese, Mattijs Jonker, Zakir Durumeric, KC Claffy, Geoffrey M. Voelker, Stefan Savage

About Me

UC San Diego

Stanford University

- Postdoctoral Researcher @ Stanford University
- Recent PhD @ UC San Diego
- Work in “Empirical Security”
  - Build systems to collect, and analyze data
  - Use insights to build better protocols, and systems
- Focus on the core Internet Infrastructure
  - DNS, BGP, and TLS (CAs)

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

REUTERS

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 I N D I C T M E N T (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: Pretrial, AUSA Alexandra Foster

6

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.

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

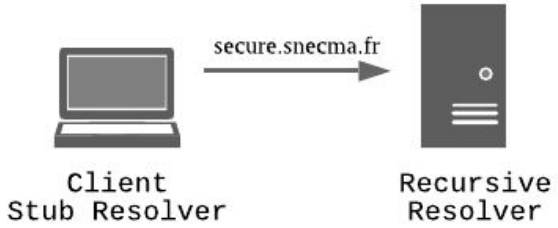
v. Domain Hijacking, the compromise of domain registrars in which one or more members of the conspiracy redirected a victim company's domain name at a domain registrar to a malicious IP address in order to facilitate computer intrusions,

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

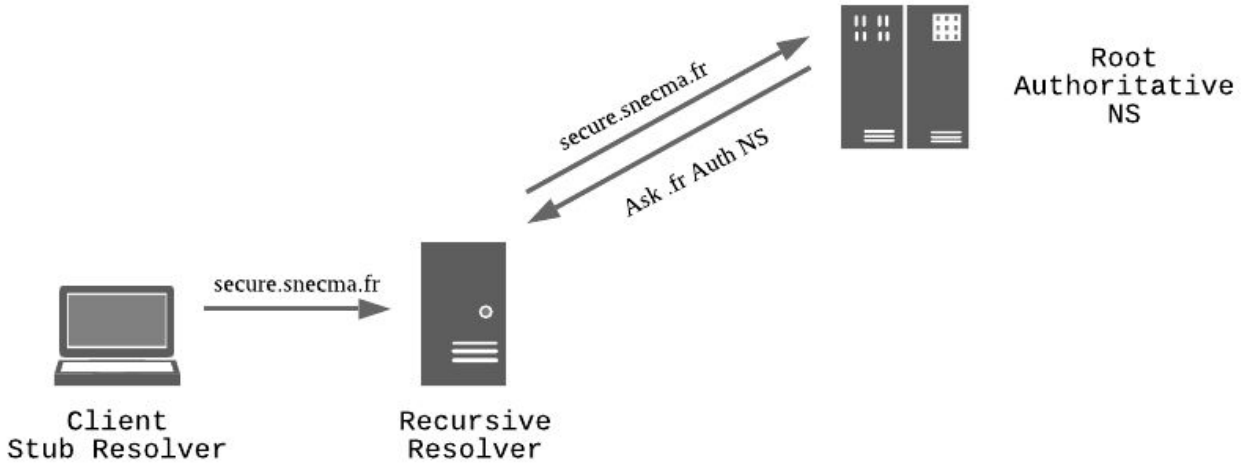
vii. Co-Opting Victim Company Employees, the use of insiders at victim companies to facilitate computer intrusions or monitor investigations of computer intrusion activity.

Domain Hijack In Practice

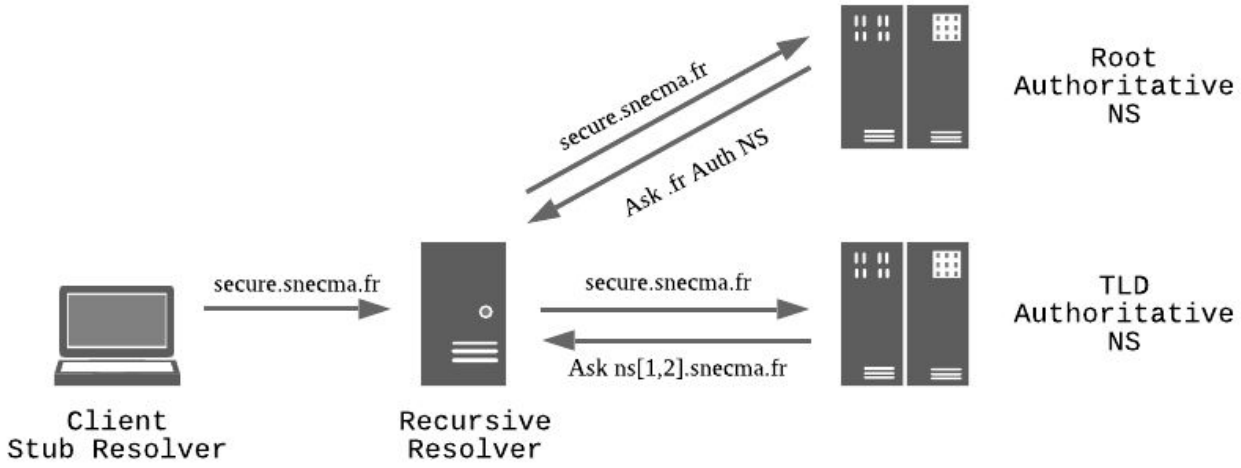
Client Logging Into “Secure” Network...



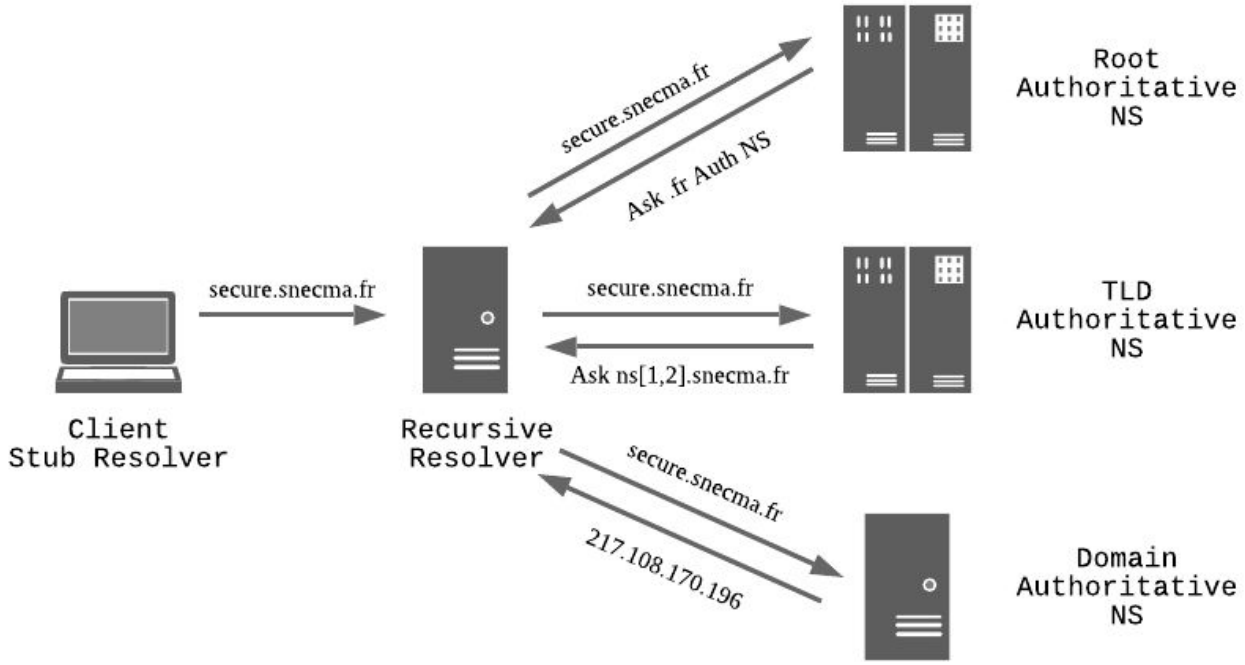
Normal Resolution



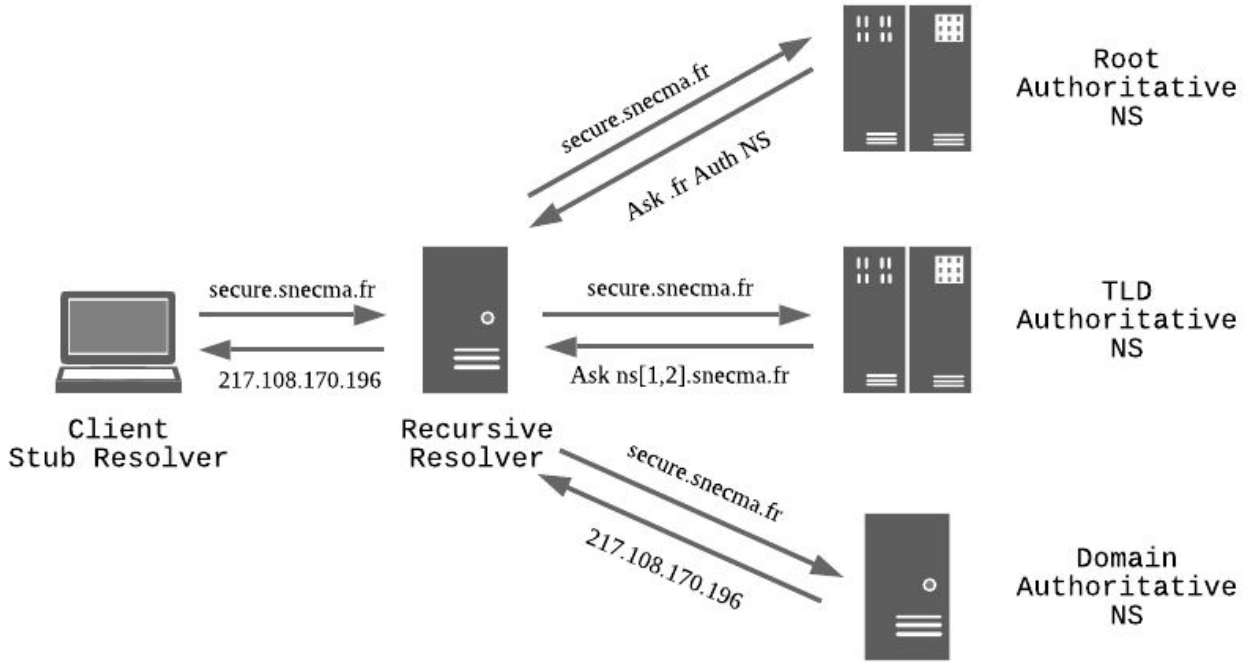
Normal Resolution



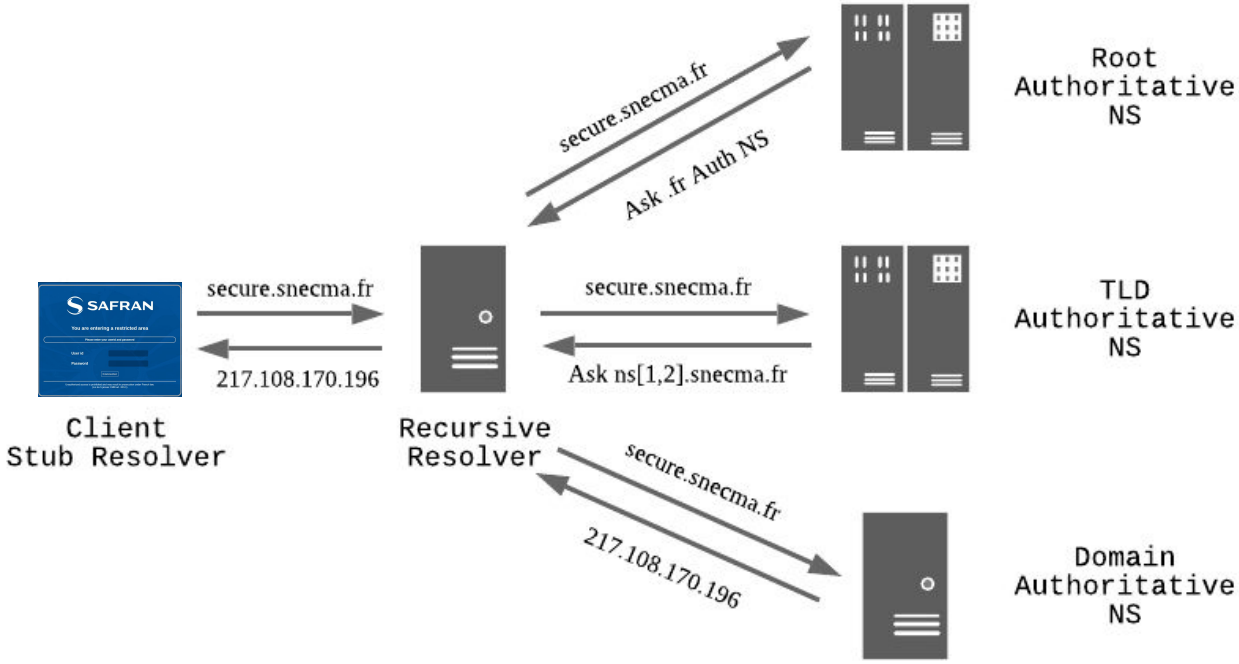
Normal Resolution



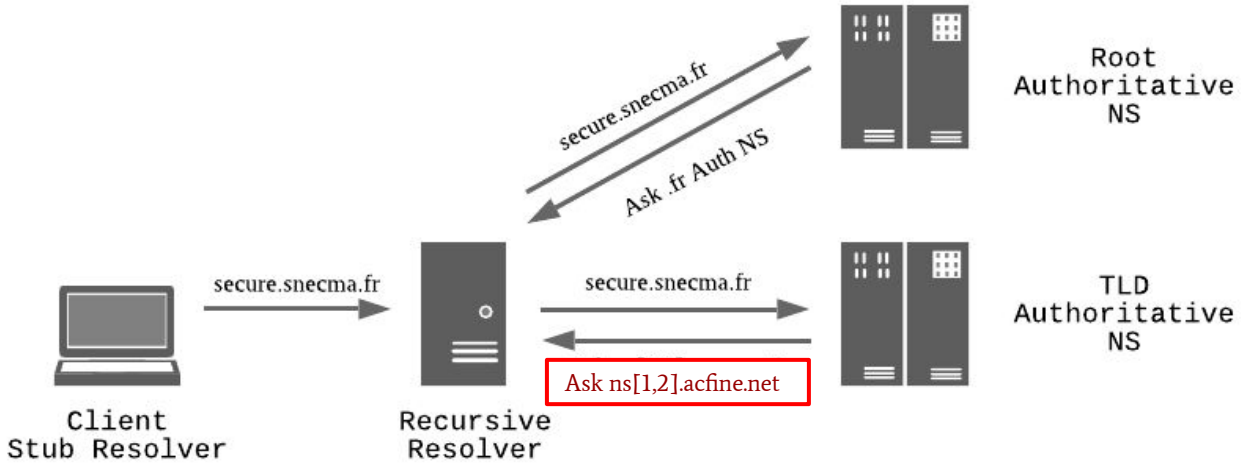
Normal Resolution



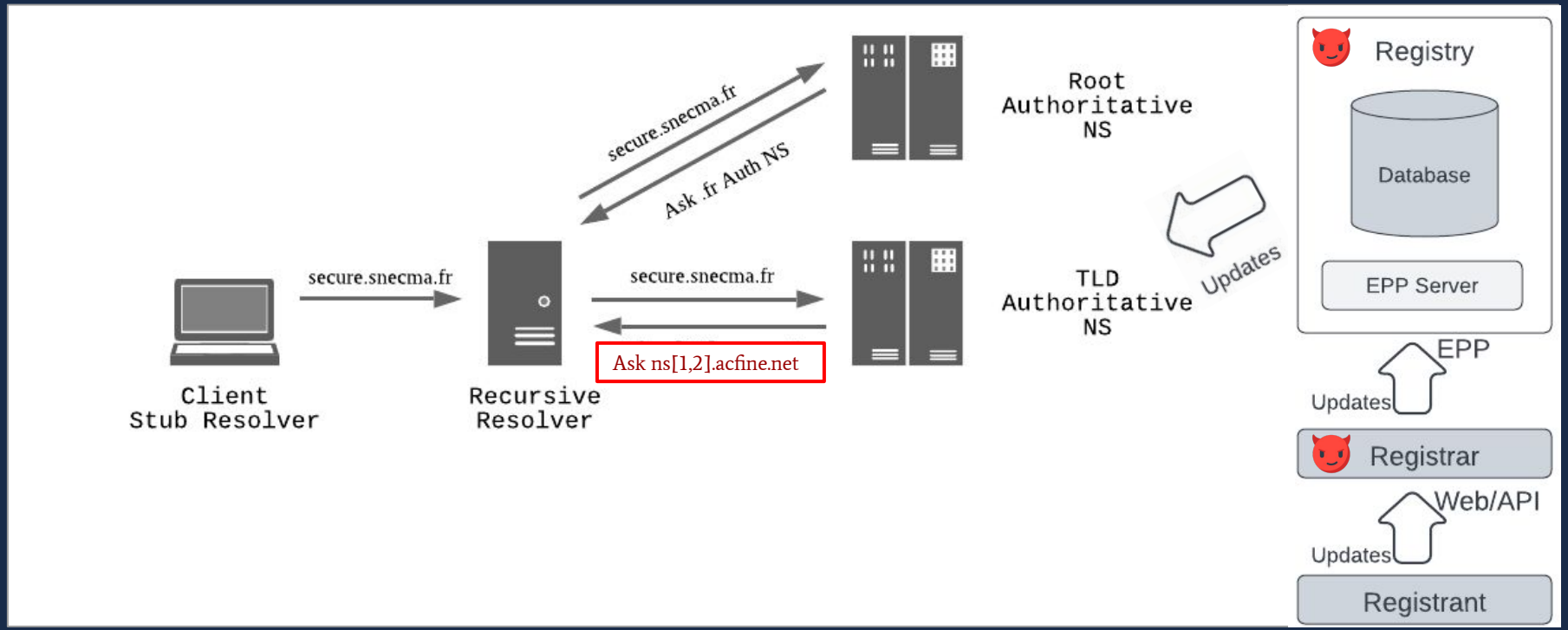
Normal Resolution



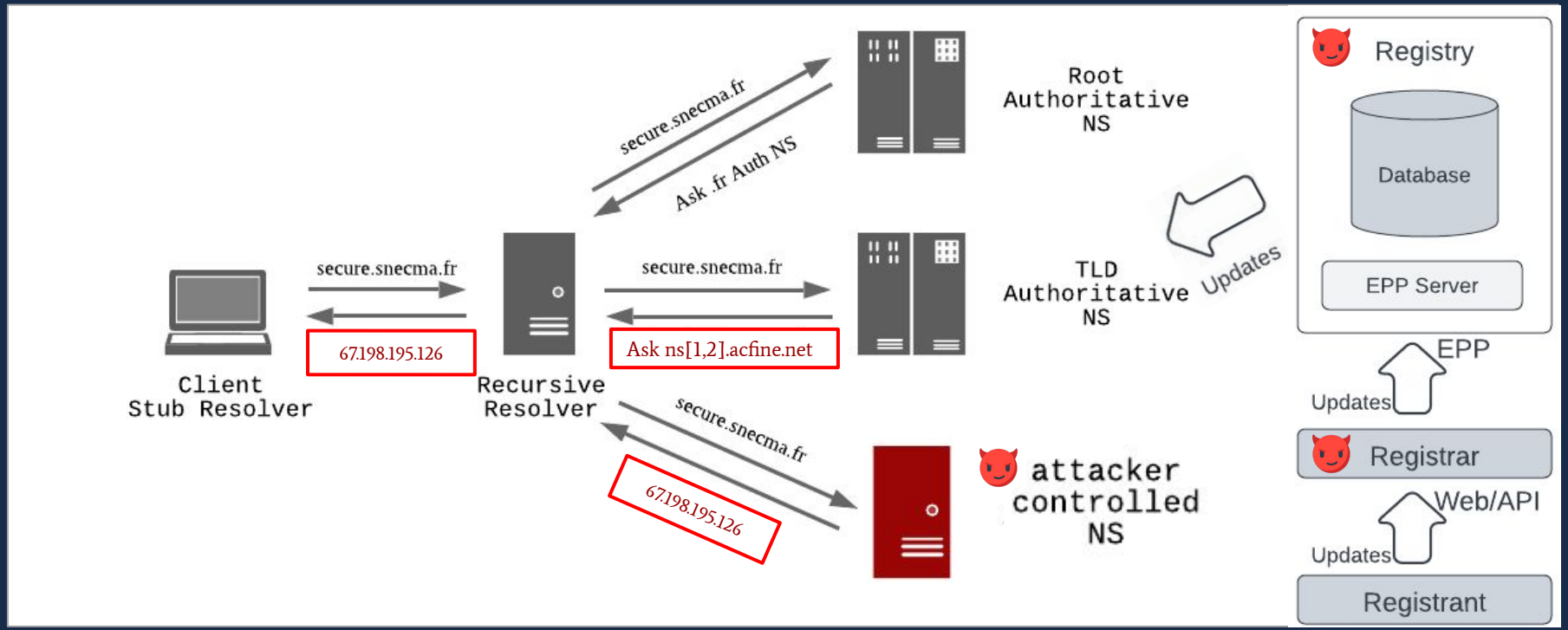
Malicious DNS Delegation Update (Circa 2014)



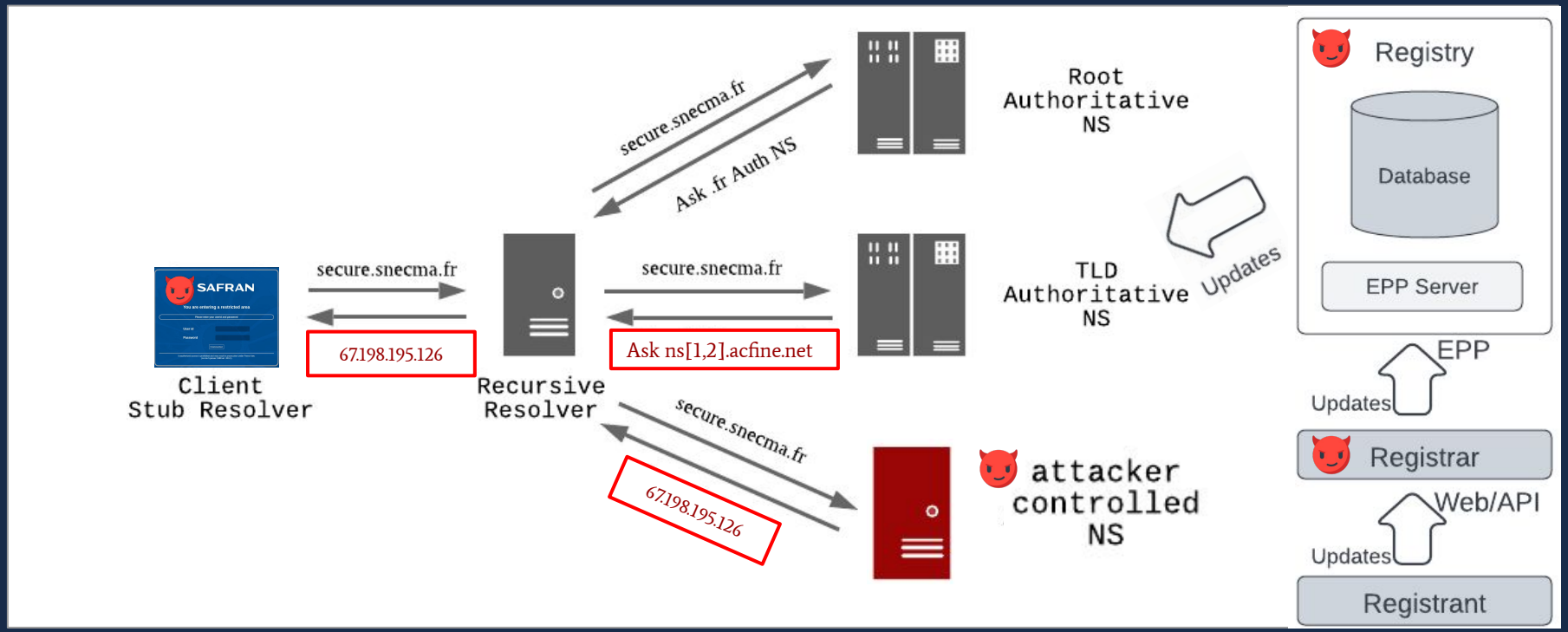
Attackers Target Registrars and Registries



Attackers Redirect All Users



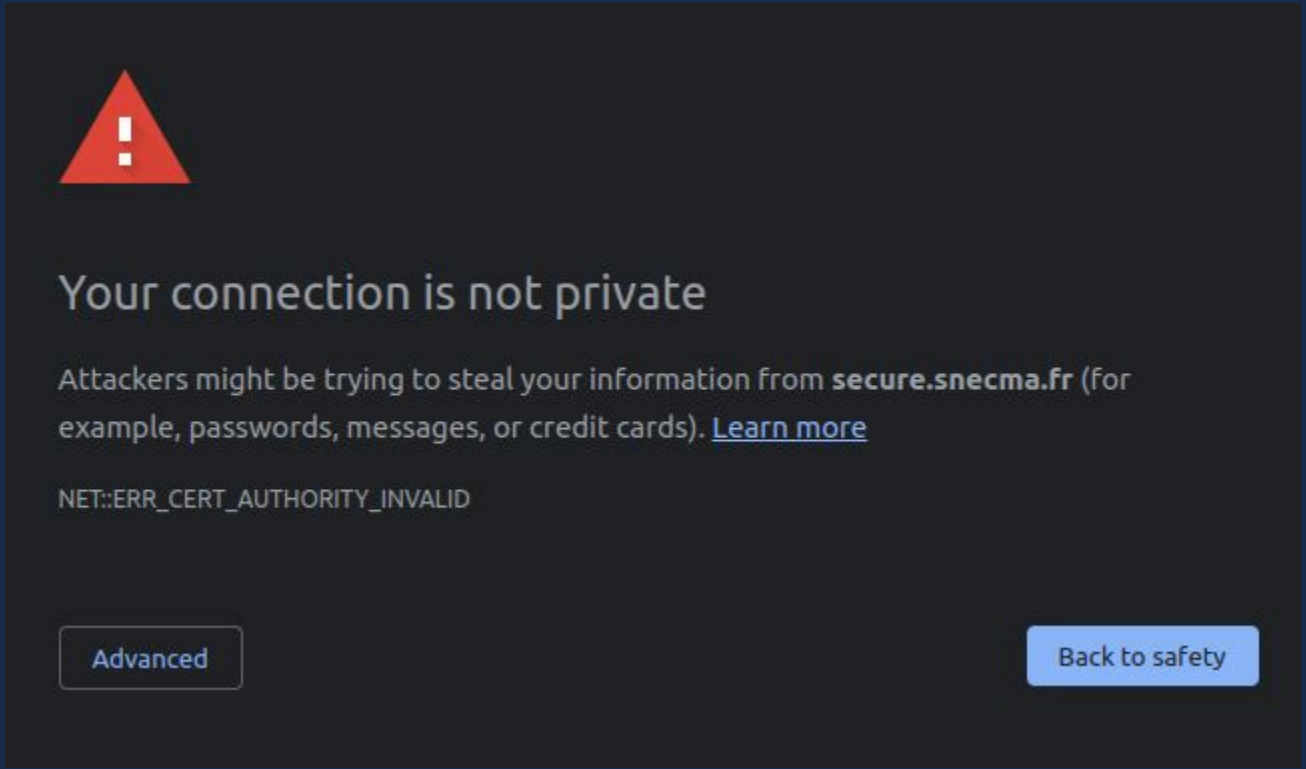
Attackers Redirect All Users



Next Stage of Attack

- Prompt malicious downloads
- Mimic webpage to harvest credentials

What about TLS Certificates?

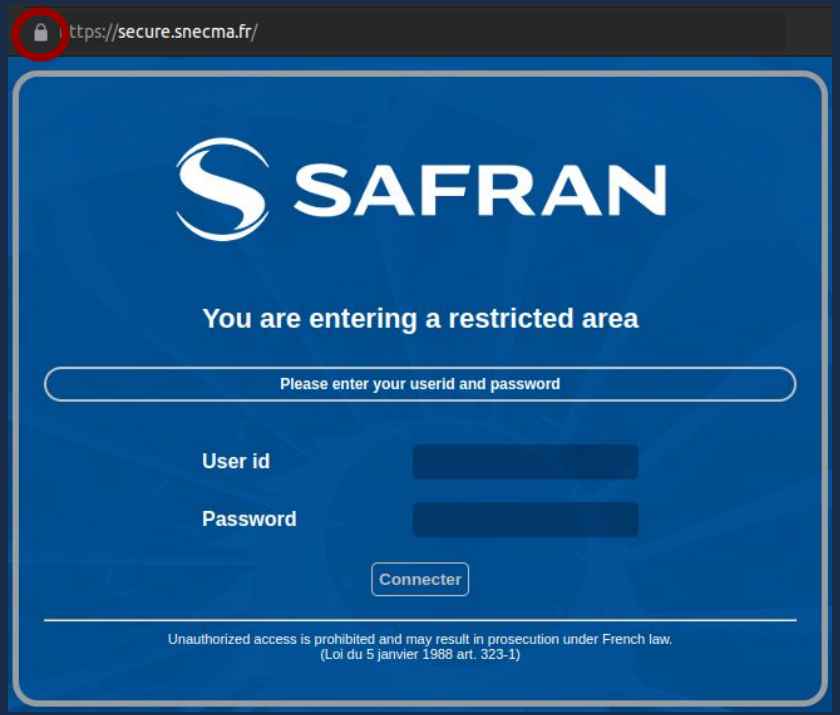


Implicit Trust Dependence

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

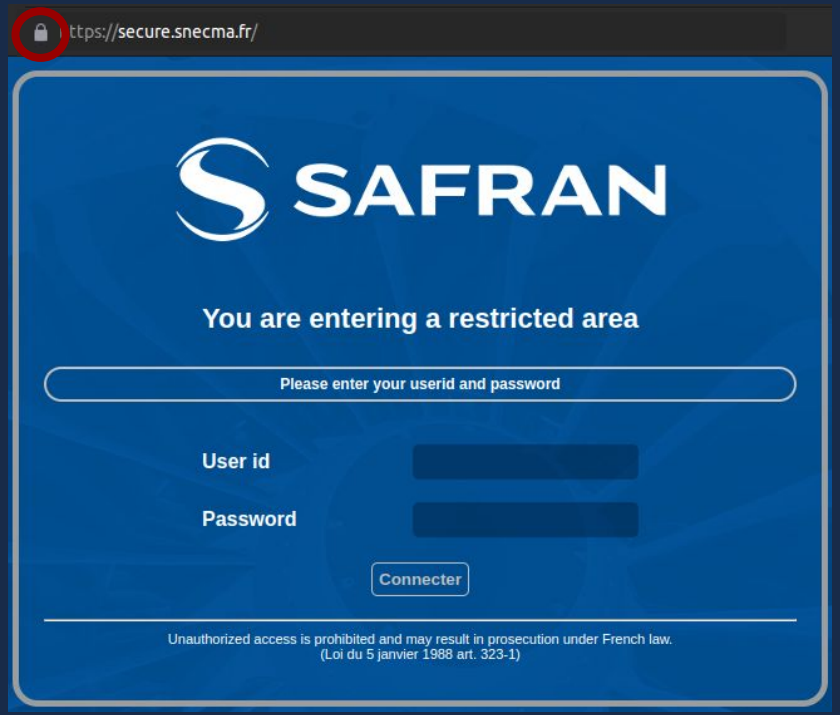
Implicit Trust Dependence

- 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.

The Washington Post

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

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**

The Goal

Construct a methodology to
retroactively identify targeted DNS infrastructure hijacks
as a third-party.

Challenges in Identifying Targeted Hijacks

Challenge #1: Delineating malicious updates from legitimate updates is hard

Malicious but looks Legitimate...

stlouisfed.org

Nameservers
ns-533.awsdns-02.net
ns-482.awsdns-60.com

→

Nameservers
ns1.stlouisfed.org
ns2.stlouisfed.org

St. Louis Federal Reserve Suffers DNS Breach

May 18, 2015

KrebsonSecurity
In-depth security news and investigation

Challenges in Identifying Targeted Hijacks

Challenge #1: Delineating malicious updates from legitimate updates is hard

Challenge #2: Malicious updates to DNS are short-lived

Challenges in Identifying Targeted Hijacks

Challenge #1: Delineating malicious updates from legitimate updates is hard

Challenge #2: Malicious updates to DNS are short-lived

—

Lesson #1: Cannot solely rely on DNS to determine hijacks

Lesson #2: Need multiple data sets to corroborate hijacks

Focus on Operational Requirements of Hijack

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

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

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

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

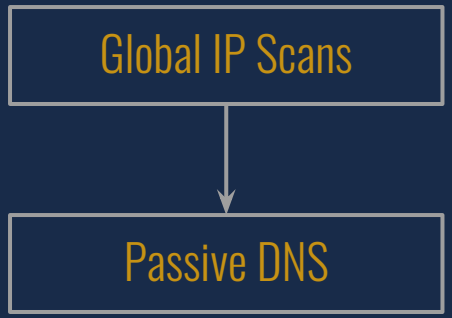
Attacker infrastructure will appear in global IP scans looking for certificates.

Identifying Targeted DNS Infrastructure Hijacks: Intuition

Global IP Scans

Identify Attacker Infrastructure. IP_A + $Cert_A$

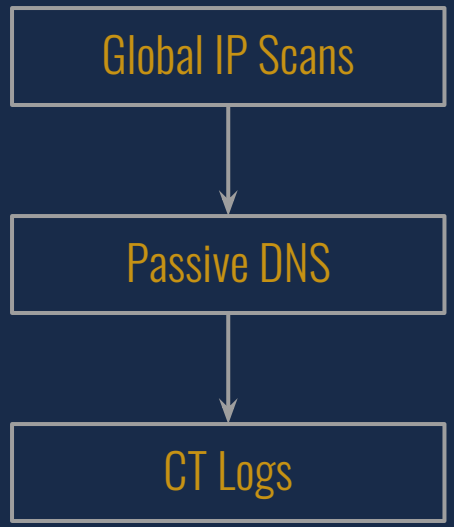
Identifying Targeted DNS Infrastructure Hijacks: Intuition



Identify Attacker Infrastructure. IP_A + $Cert_A$

Corroborate target domain was redirected to IP_A

Identifying Targeted DNS Infrastructure Hijacks: Intuition

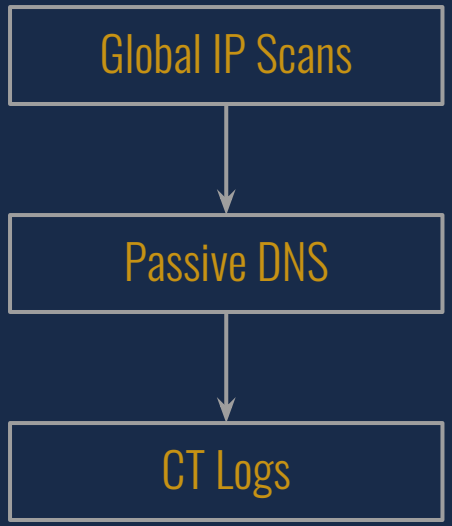


Identify Attacker Infrastructure. IP_A + $Cert_A$

Corroborate target domain was redirected to IP_A

Corroborate $Cert_A$ was issued during redirection

Identifying Targeted DNS Infrastructure Hijacks: Intuition



Identify Attacker Infrastructure. IP_A + $Cert_A$

Corroborate target domain was redirected to IP_A

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: 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

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

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

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

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

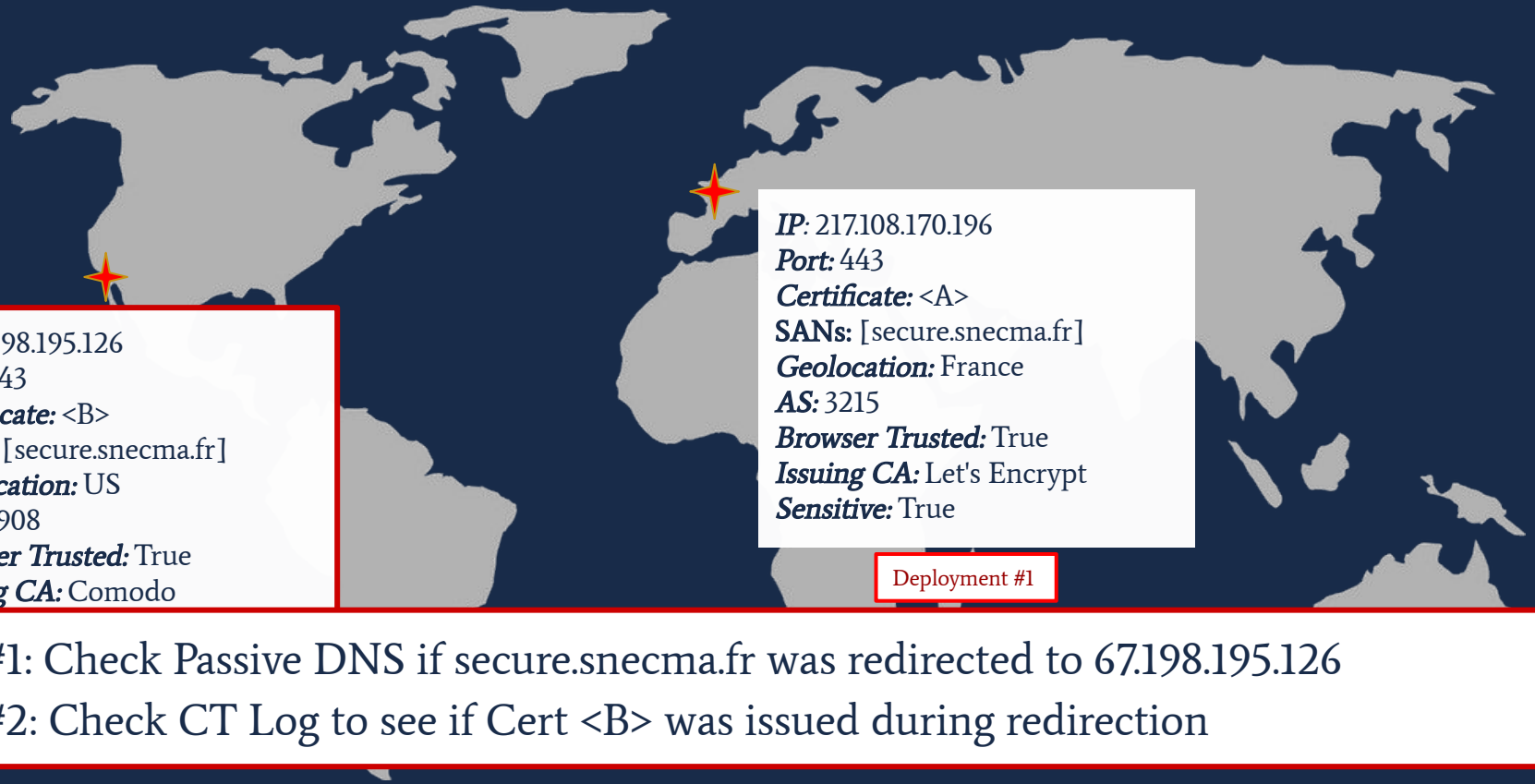
IP: 67.198.195.126
Port: 443
Certificate: <B>
SANs: [secure.snecma.fr]
Geolocation: US
AS: 35908
Browser Trusted: True
Issuing CA: Comodo
Sensitive: True

Deployment #2

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

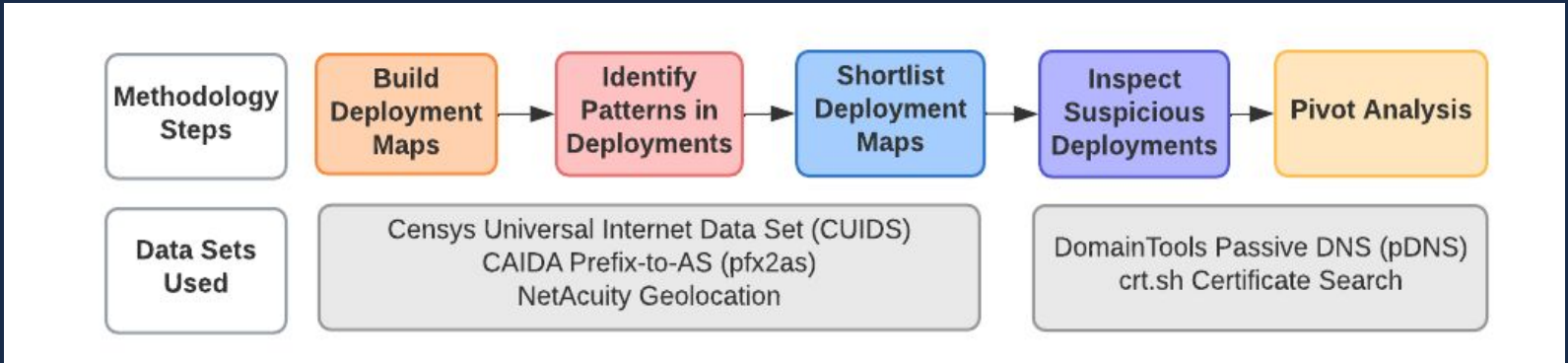
Suspicious Deployments → Potential Attacker Infrastructure



#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

Methodology Summary



Results

Identified 41 domains as hijacked

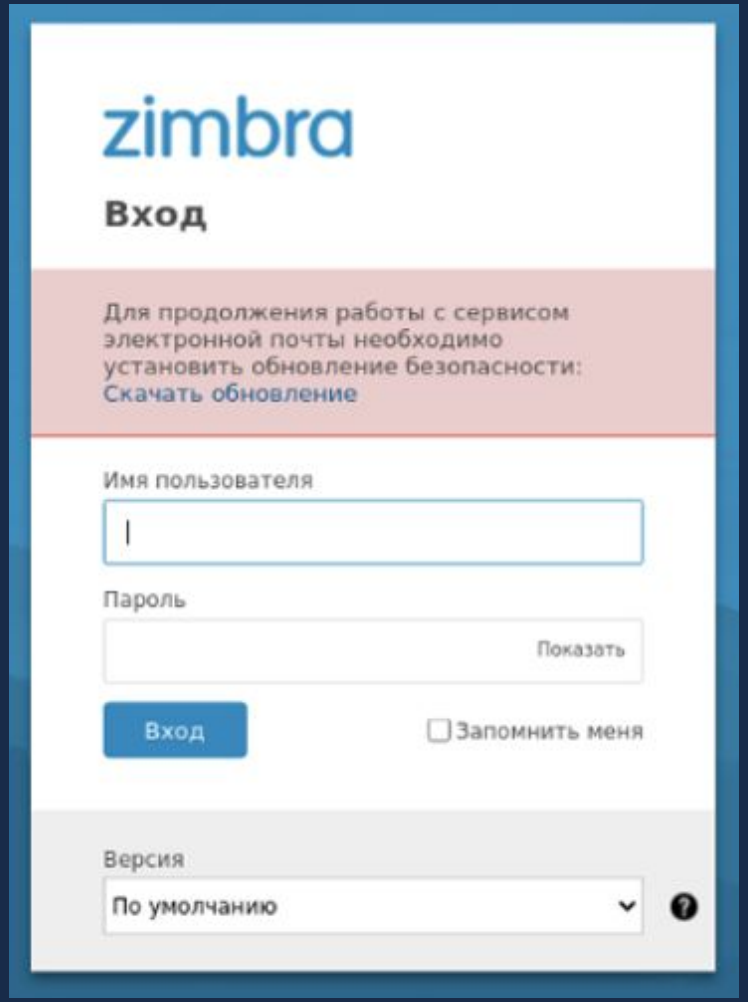
- 33 domains re-identified and verified from previous reports
- 8 domains not previously identified

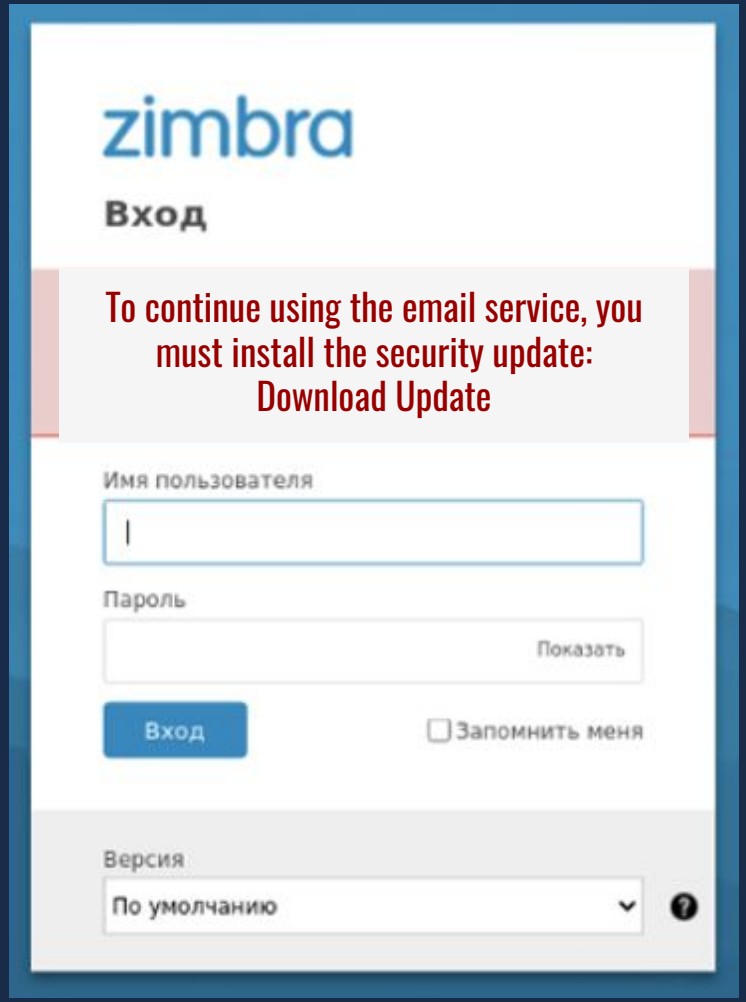
High confidence hijacks!

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	—	—

Organizations Hijacked

Domain Organization Type	Hijacked Domains
Government Ministry	12
Government Organization	4
Government Services	7
Infrastructure Provider	6
Law Enforcement	3
Energy Company	3
Intelligence Services	3
Civil Aviation	2
Insurance	1

Organizations Hijacked

Domain Organization Type	Hijacked Domains
Government Ministry	12
Government Organization	4
Government Services	7
Infrastructure Provider	6
Law Enforcement	3
Energy Company	3
Intelligence Services	3
Civil Aviation	2
Insurance	1

Summary

- Possible to identify targeted DNS infrastructure hijacks as a third-party
  - Analyzing DNS delegations alone does not work
  - Focus on operational requirements of attacks
  - Need to use a combination of data sources to build confidence in results
- 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 hijacks

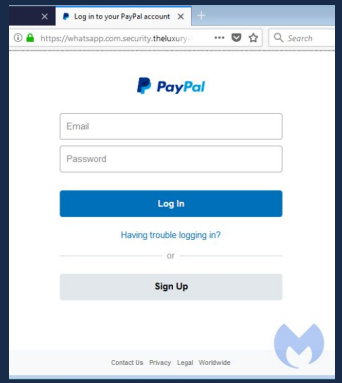
Parting Thoughts

Thought #1

DNS introduces *dependency* on external entities (registrar, registry) allowing for a “supply chain attack”.

Not a hypothetical risk. Operators are prime targets.

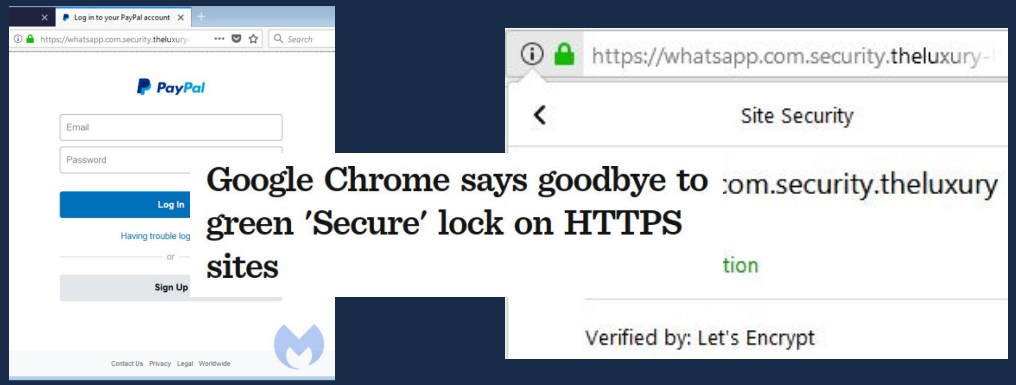
Thought #2



Secure protocols do not *always* mean secure.

Malwarebytes Labs | HTTPS: why the green padlock is not enough

Thought #2



Secure protocols do not *always* mean secure.

Malwarebytes Labs | HTTPS: why the green padlock is not enough

Thought #3

Monitoring and Transparency are important

or

“You cannot secure what you cannot measure!”

DNS Transparency

- Organizations cannot tell if their nameservers ever changed!
  - Have nanog.org nameservers changed recently? [No, as per zone file data...]
  - But hijacks last for as little as 15 minutes and zone files updated daily.
  - Continuous monitoring?
- Certificate Transparency like transparency with DNS
  - Append only changes to domain nameservers at TLDs?

Thanks

Questions?

gakiwate -- at -- cs.stanford.edu