Risky BIZness

Into the DNS Wilderness

•••

APRICOT 2023 | Keynote | APOPS1

Manila, Philippines

27th February 2023

Gautam Akiwate

Stanford University

About Me

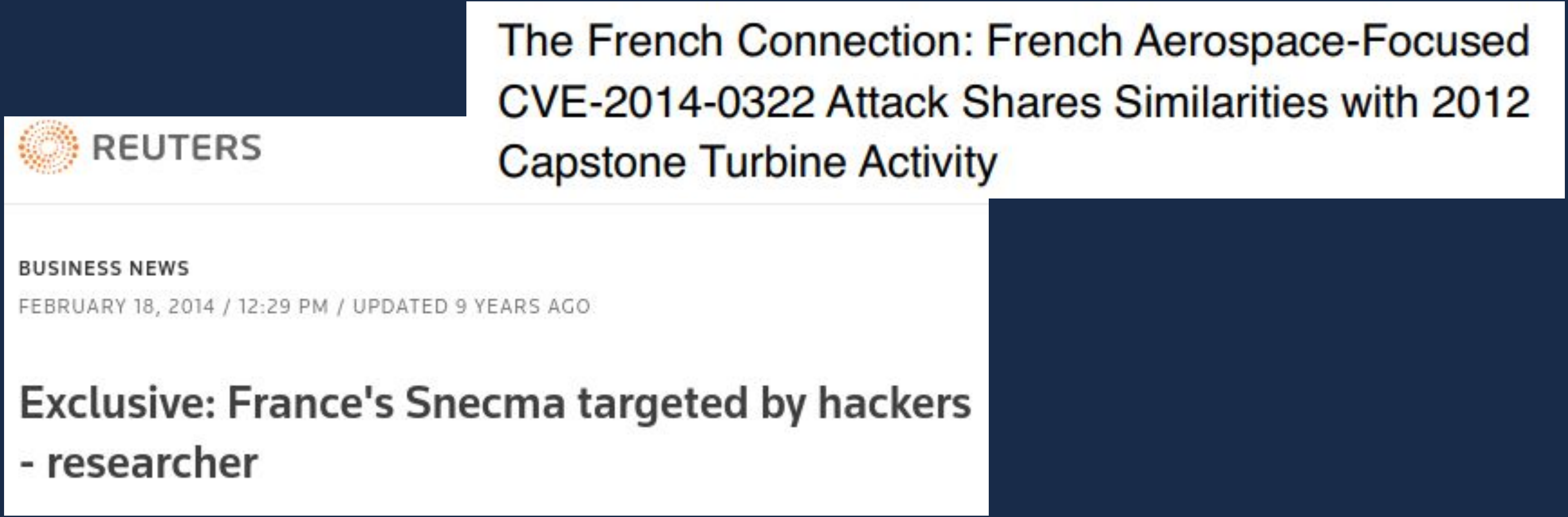
UC San Diego

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 Target DNS Infrastructure to Hijack Domains

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

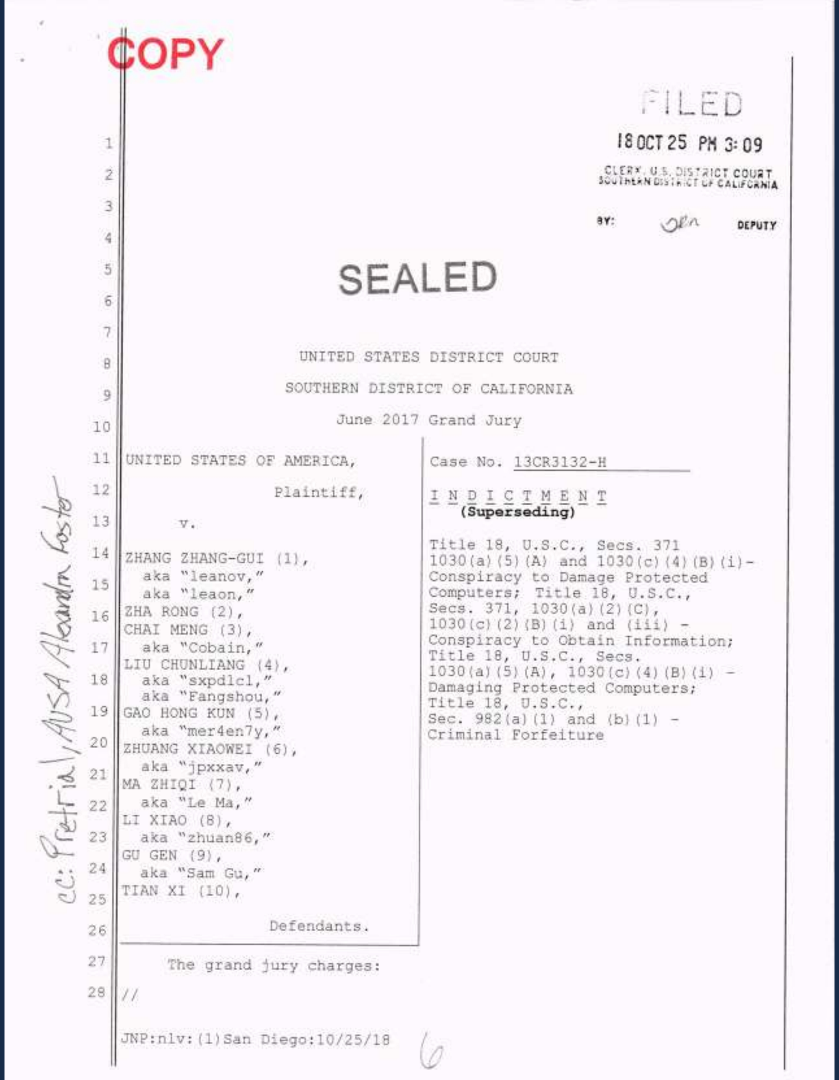
BUSINESS NEWS

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 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:

//

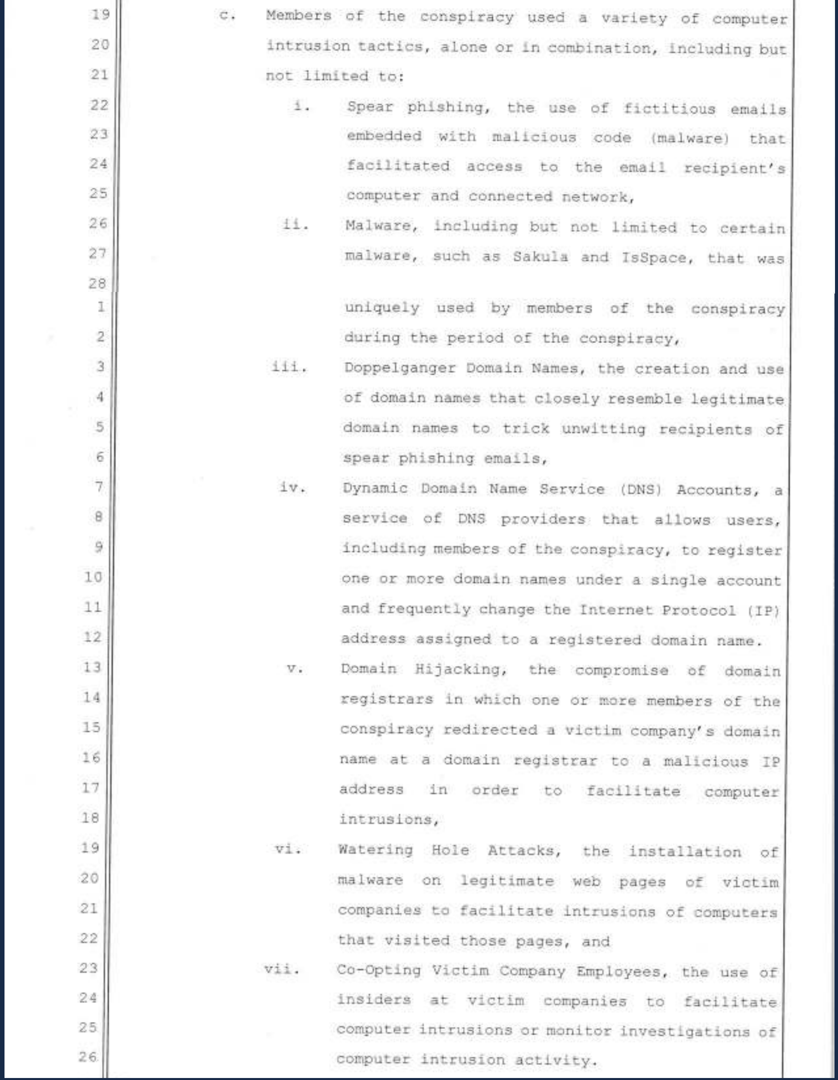
JNP:nlv:(1)San Diego:10/25/18

6

cc: Pretrial / 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,

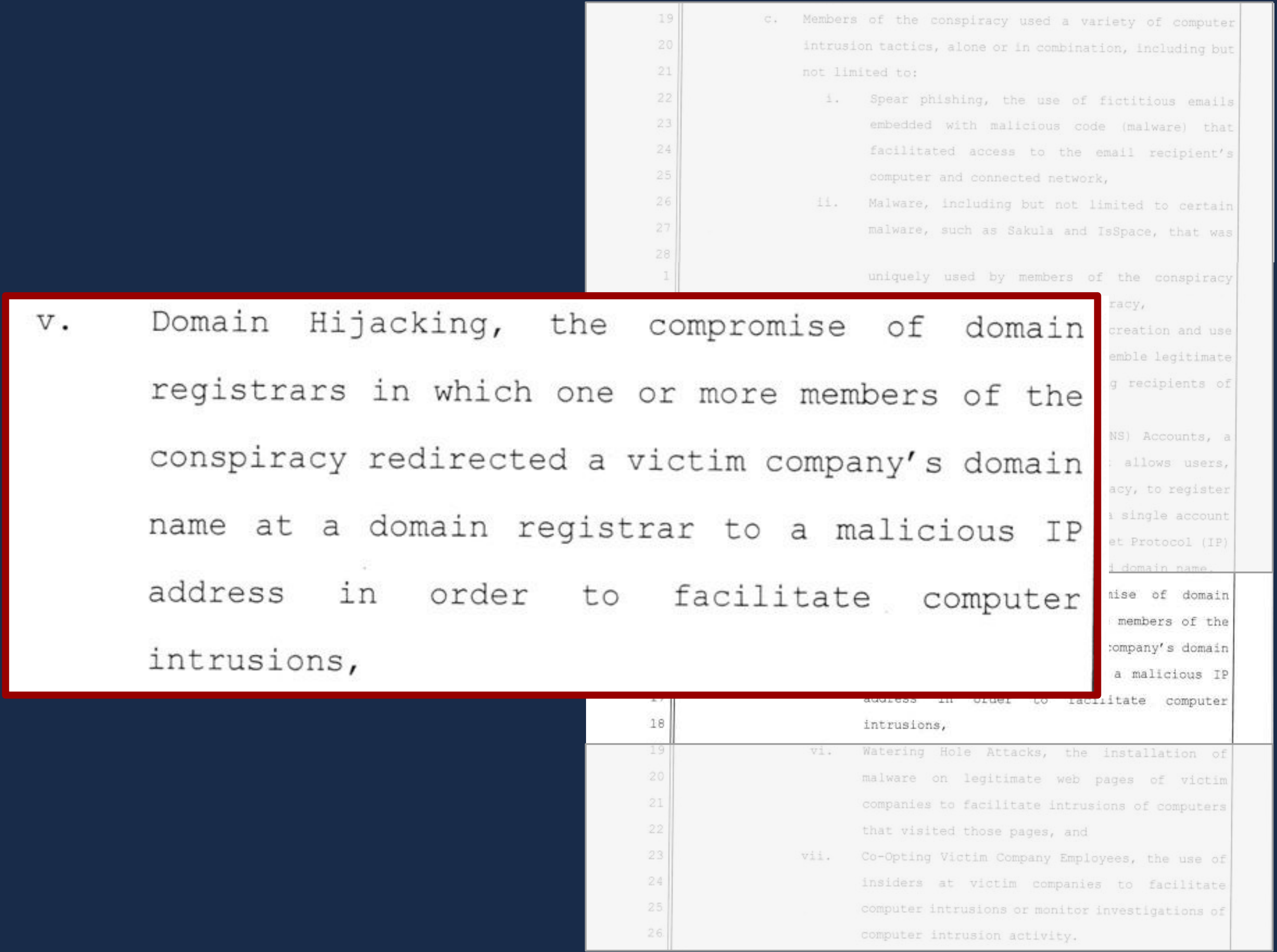
iii. Doppelganger Domain Names, the creation and use of domain names that closely resemble legitimate domain names to trick unwitting recipients of spear phishing emails,

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.



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

a single account

et Protocol (IP)

d domain name.

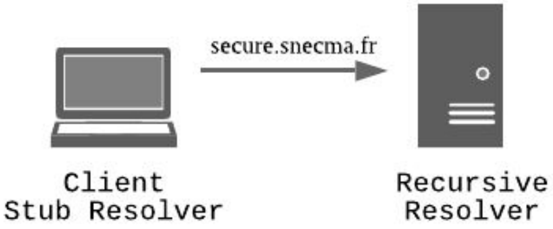
v. Domain Hijacking, the compromise of domain registrars in which one or more members of the conspiracy redirected a victim company's domain name at a domain registrar to a malicious IP address in order to facilitate computer intrusions,

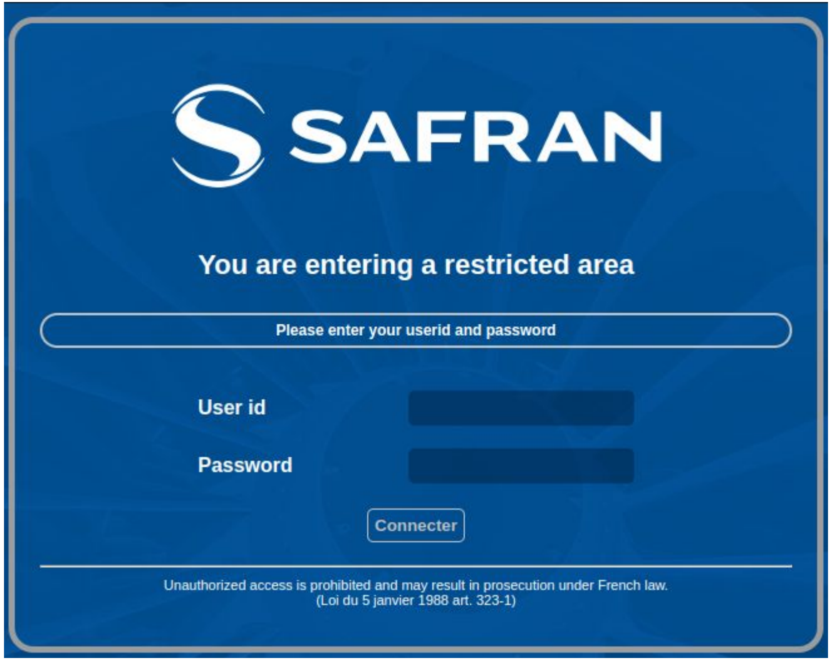
vi. Watering Hole Attacks, the installation of malware on legitimate web pages of victim companies to facilitate intrusions of computers that visited those pages, and

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

Domain Hijack In Practice

Client Logging Into “Secure” Network...





You are entering a restricted area

Please enter your userid and password

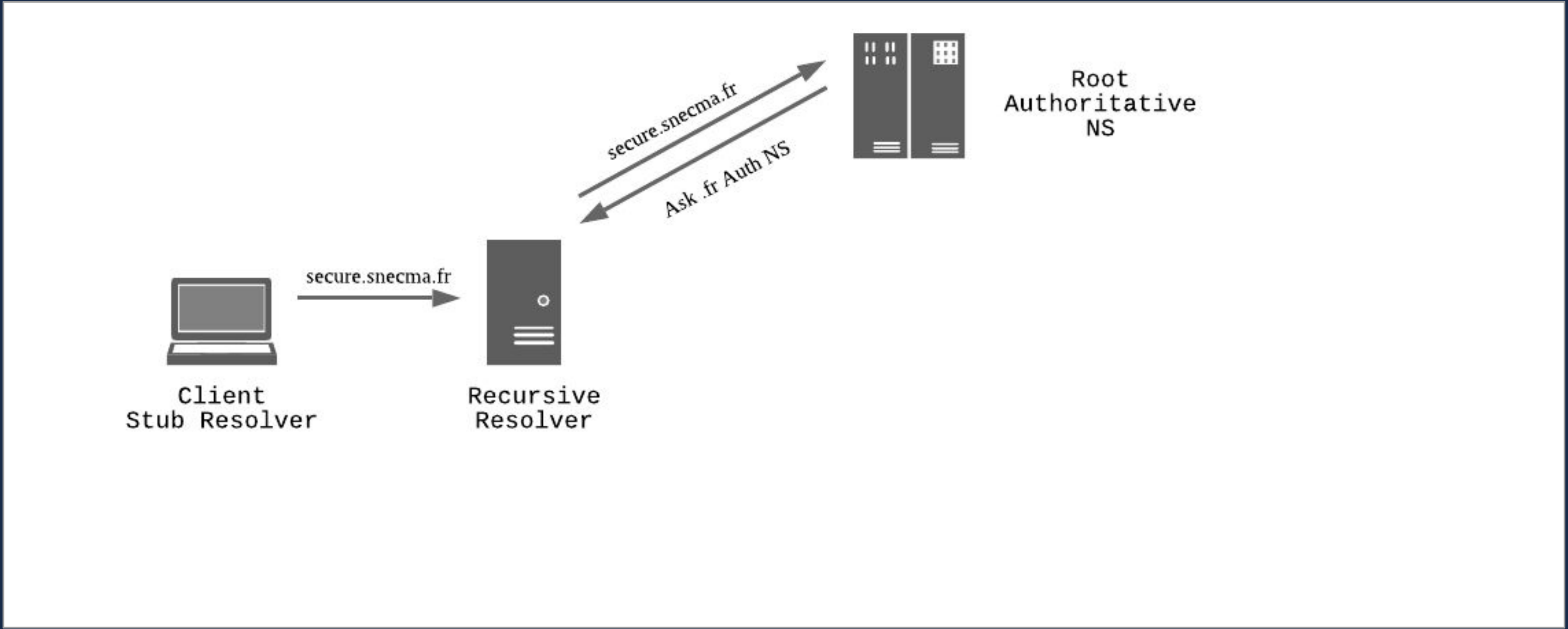
User id

Password

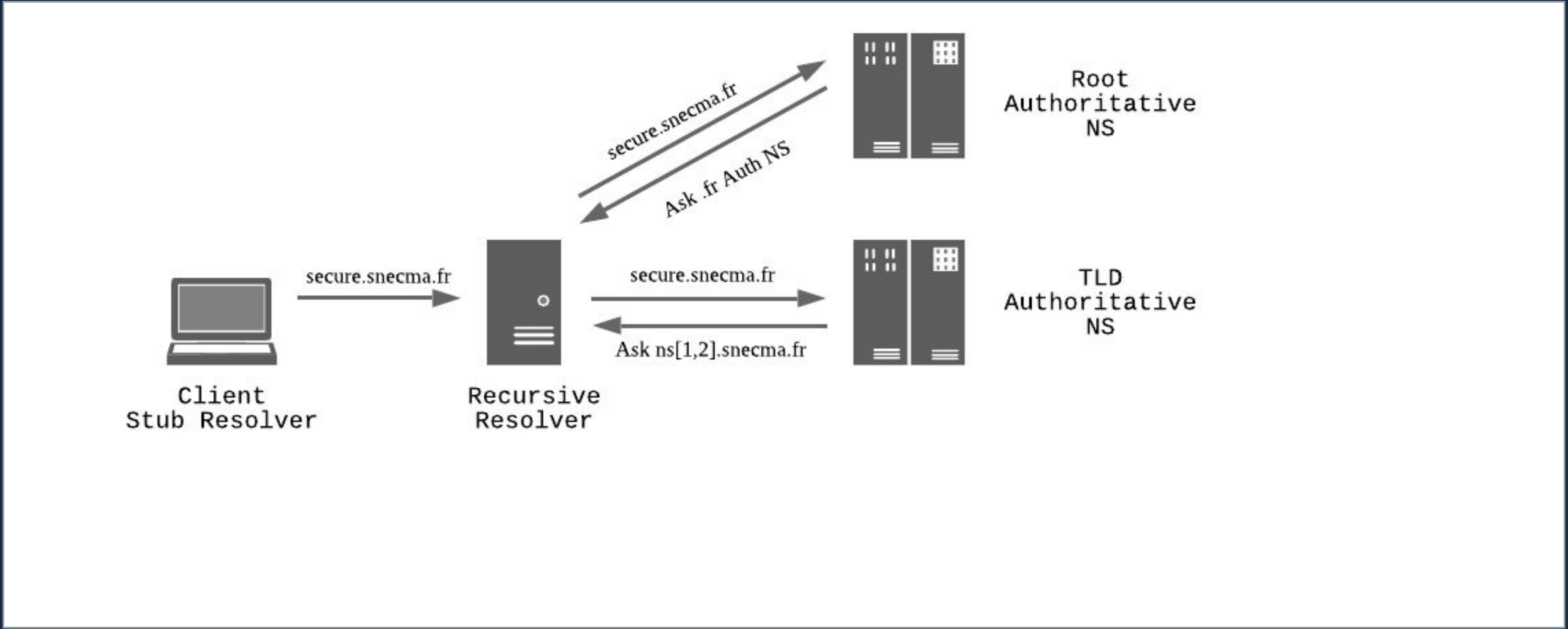
Connecter

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

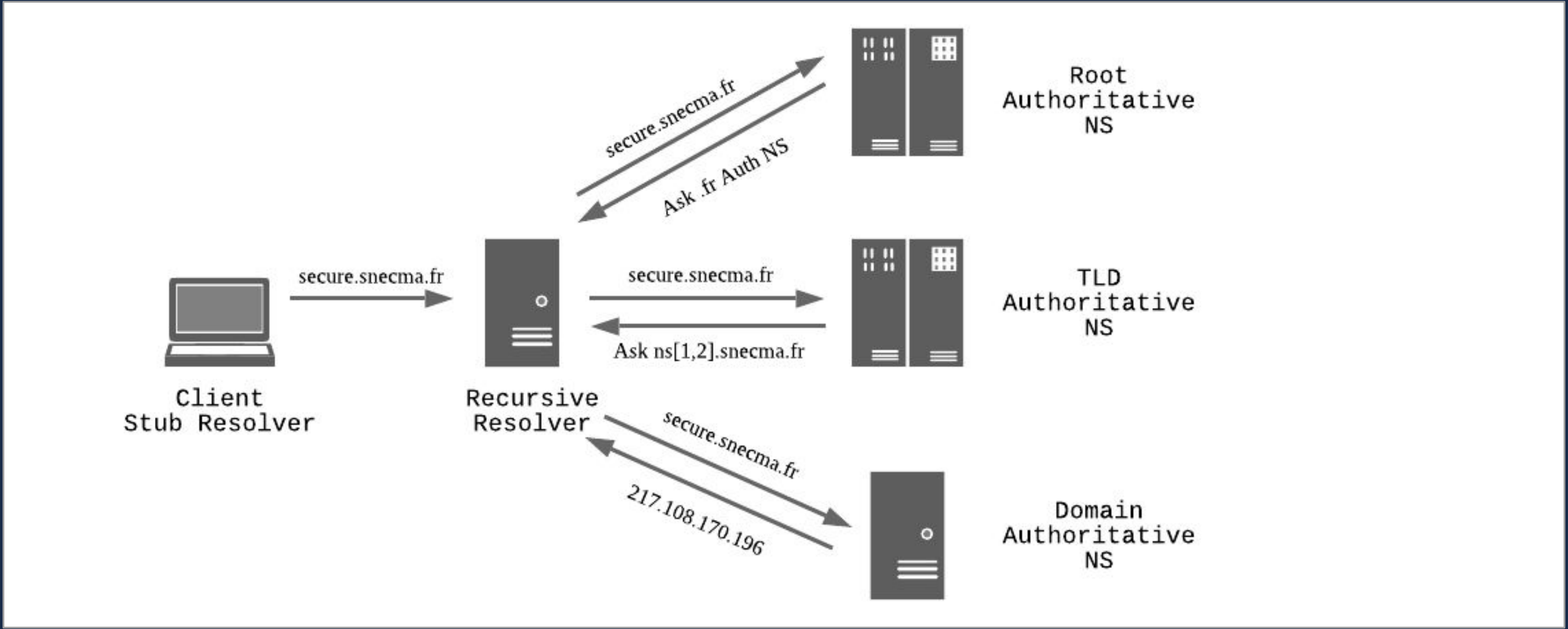
Normal Resolution



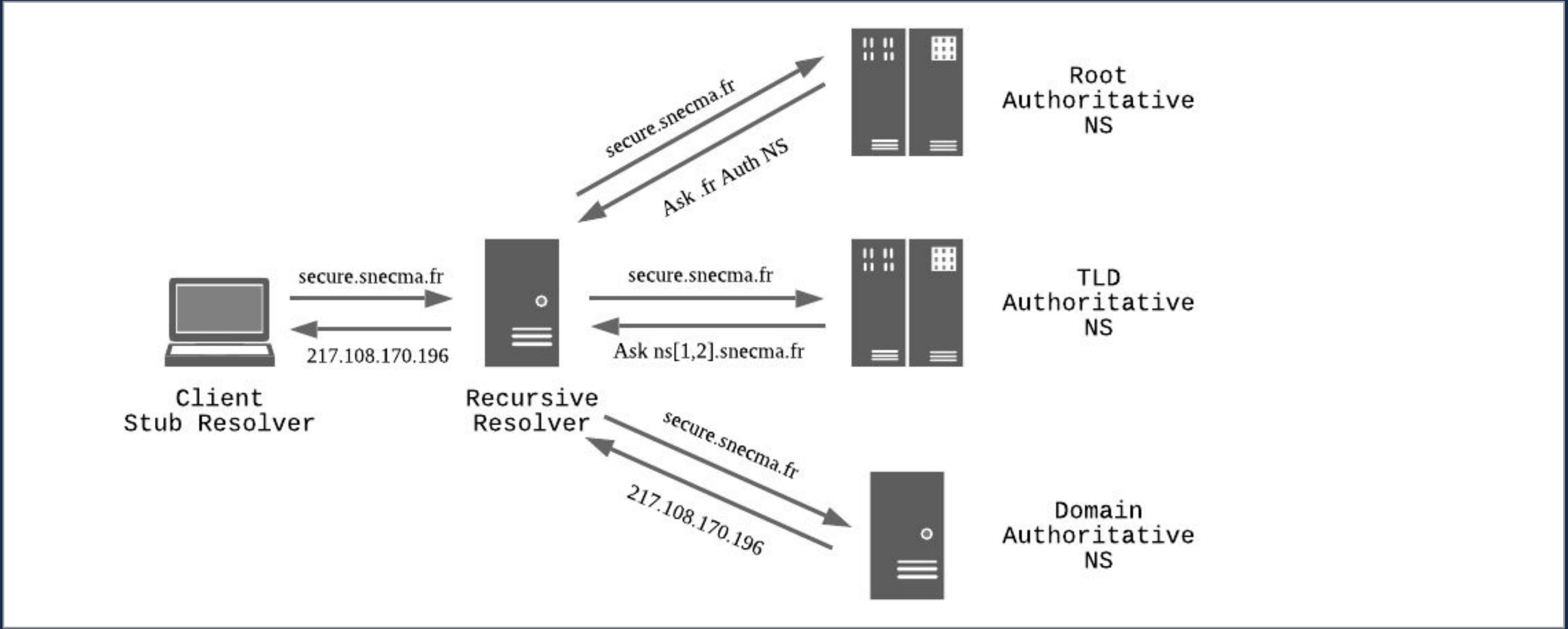
Normal Resolution



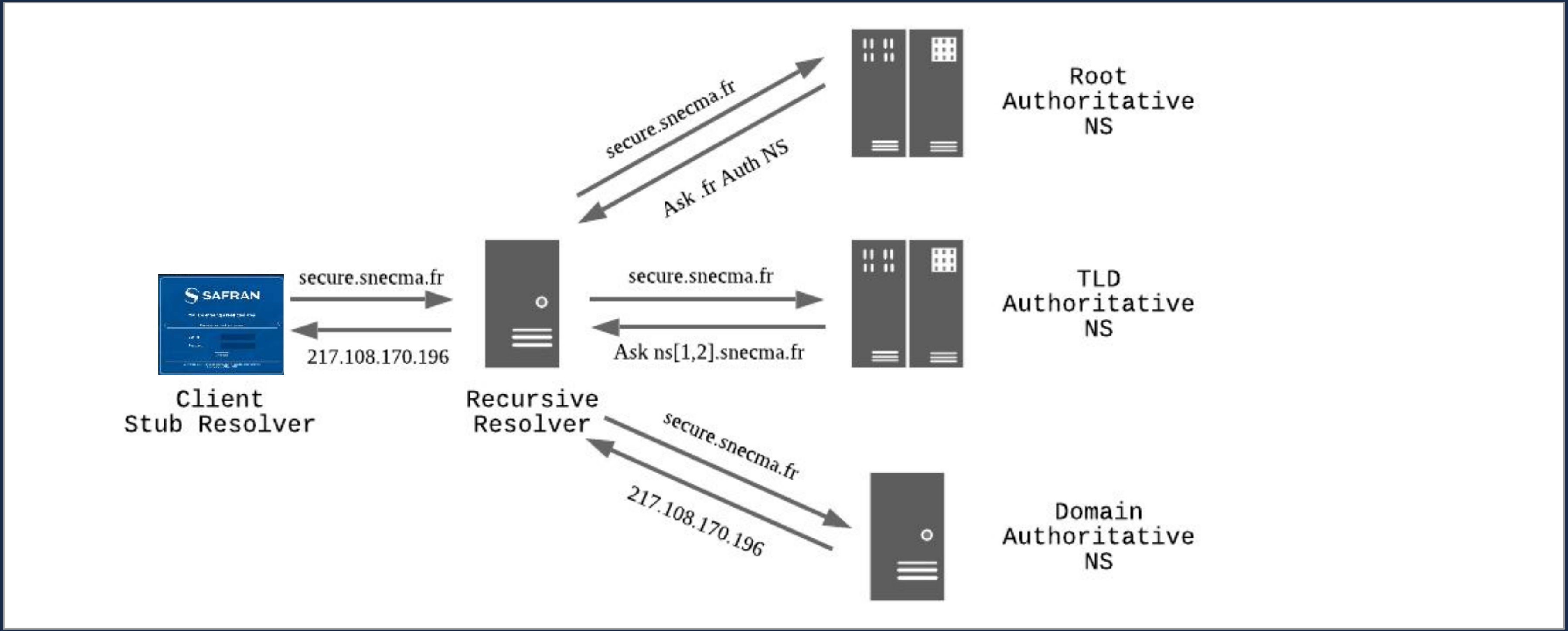
Normal Resolution



Normal Resolution



Normal Resolution



Root Authoritative NS

TLD Authoritative NS

Domain Authoritative NS

Client Stub Resolver

Recursive Resolver

secure.snecma.fr

217.108.170.196

secure.snecma.fr

Ask .fr Auth NS

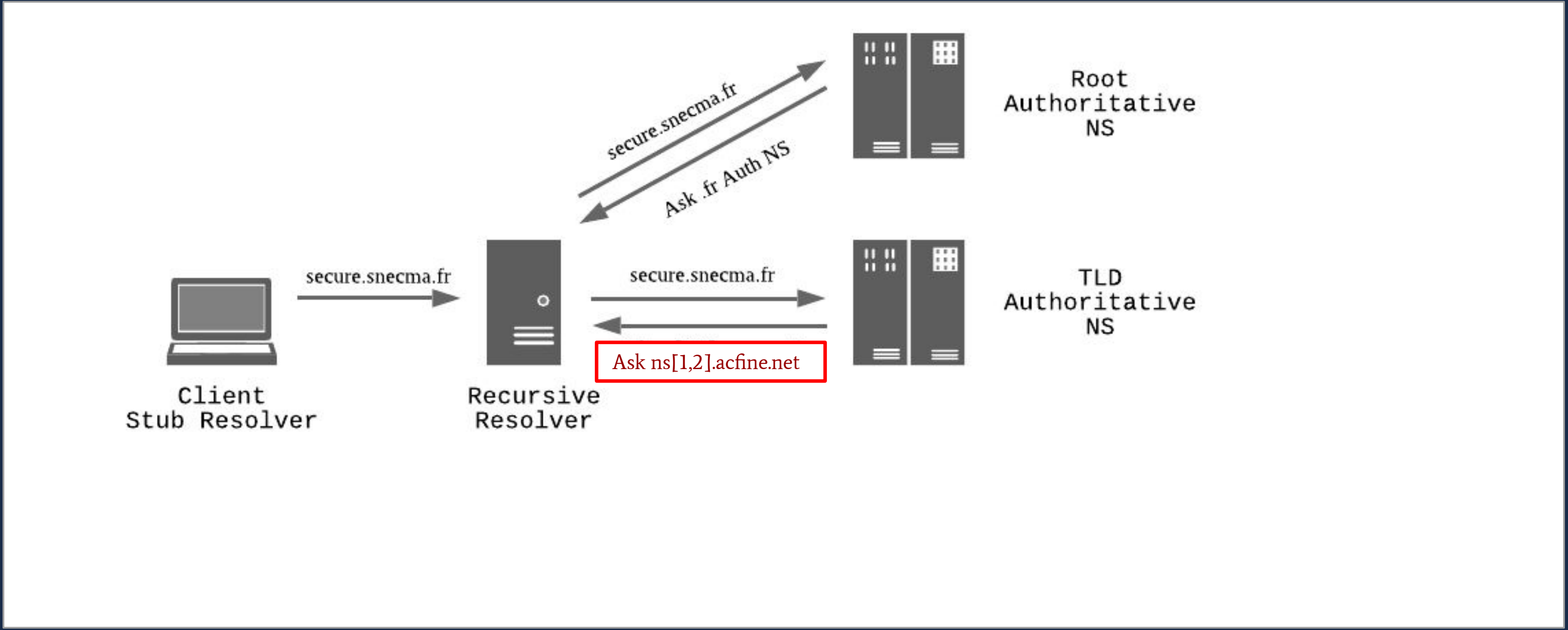
secure.snecma.fr

Ask ns[1,2].snecma.fr

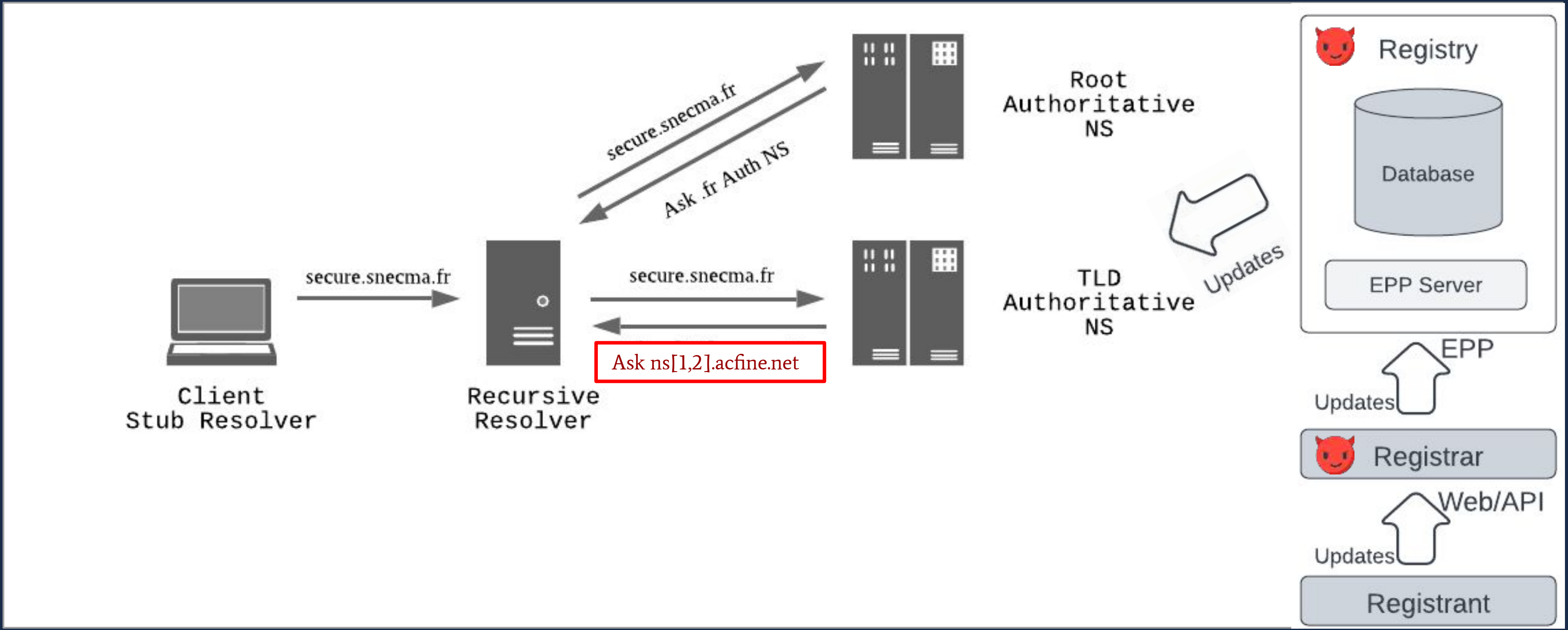
secure.snecma.fr

217.108.170.196

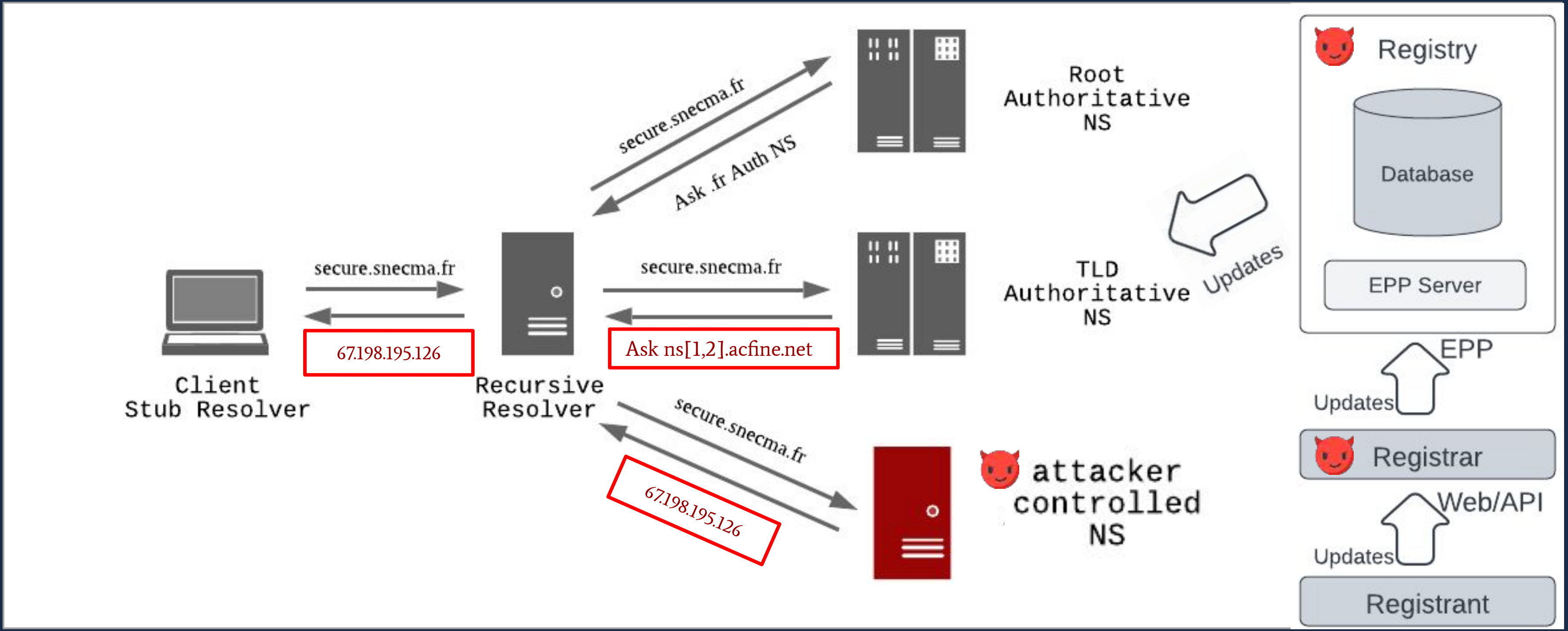
Malicious DNS Delegation Update (Circa 2014)



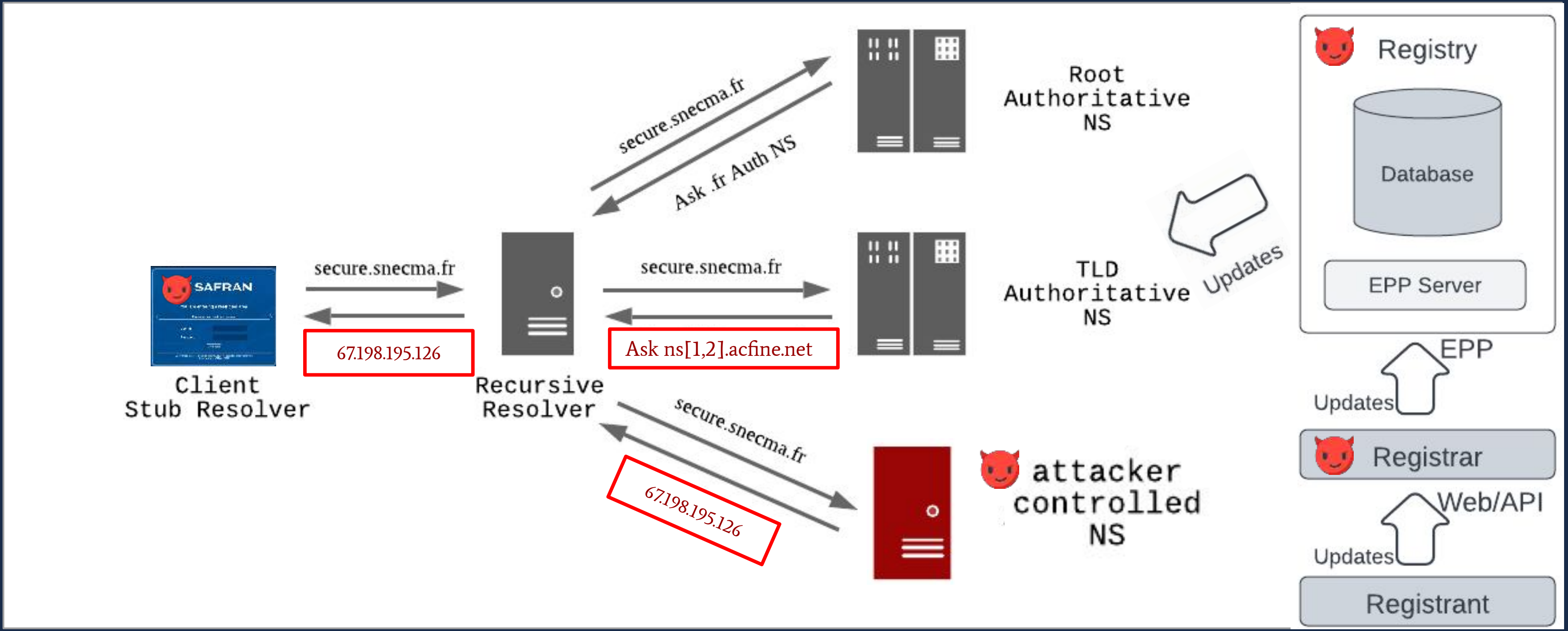
Attackers Target DNS Delegation Update Mechanism



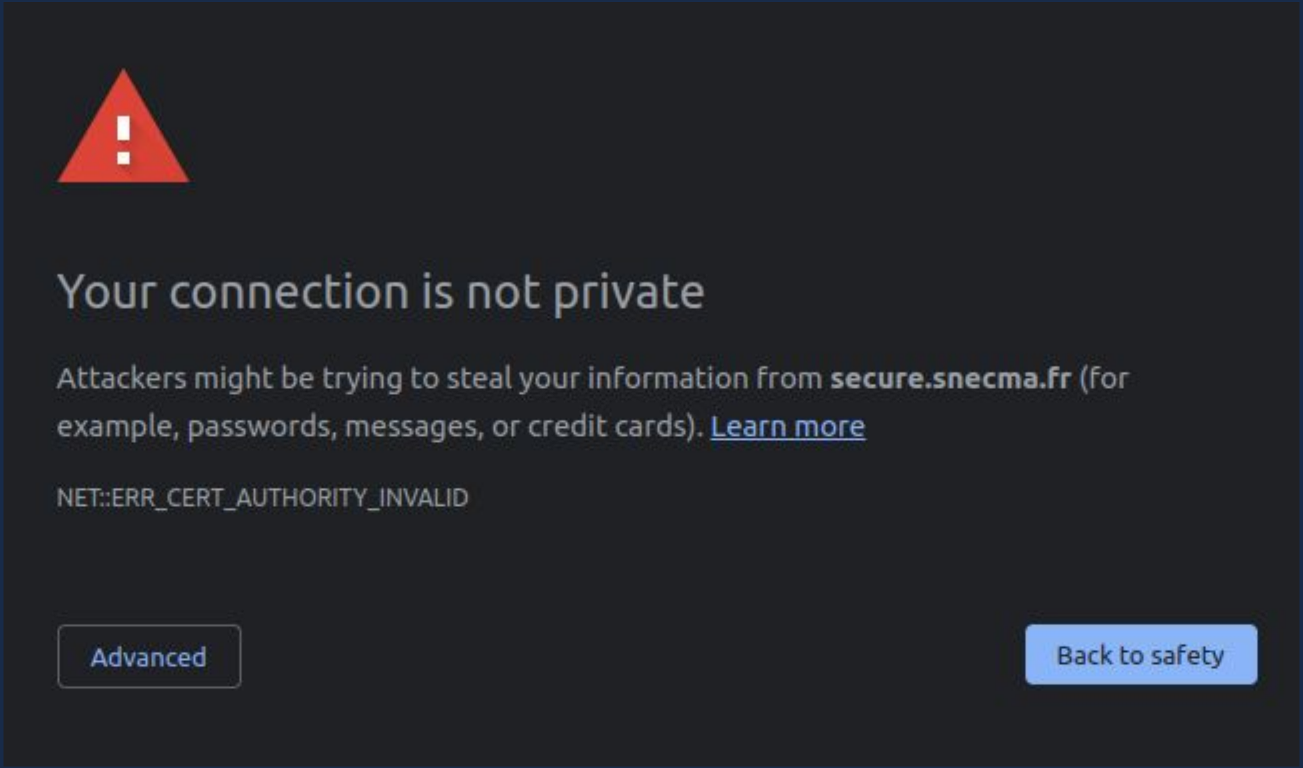
Attackers Redirect All Users



Attackers Redirect All Users



What about TLS Certificates?



Your connection is not private

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

NET::ERR_CERT_AUTHORITY_INVALID

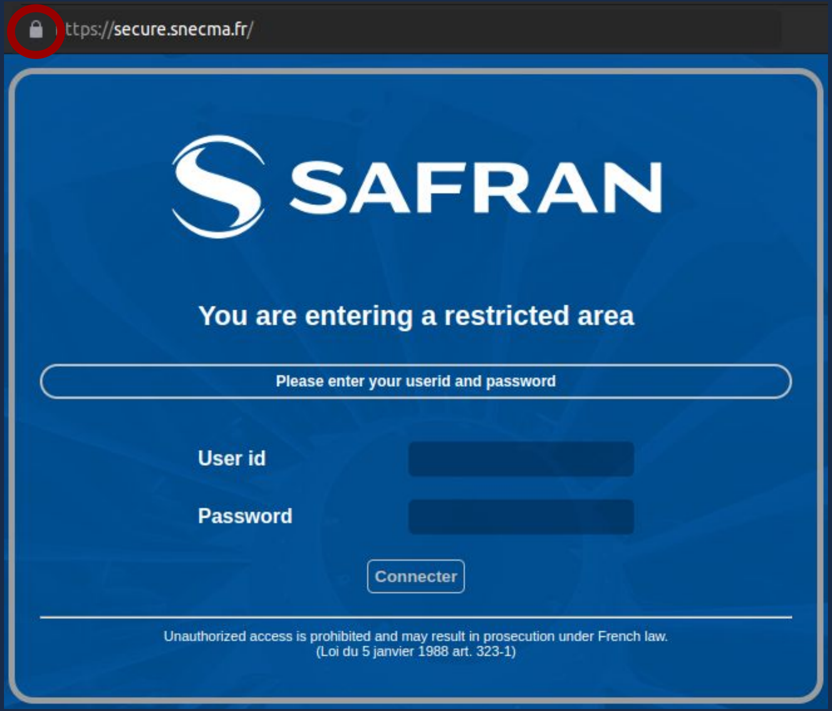
Implicit Trust Dependence

- 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!



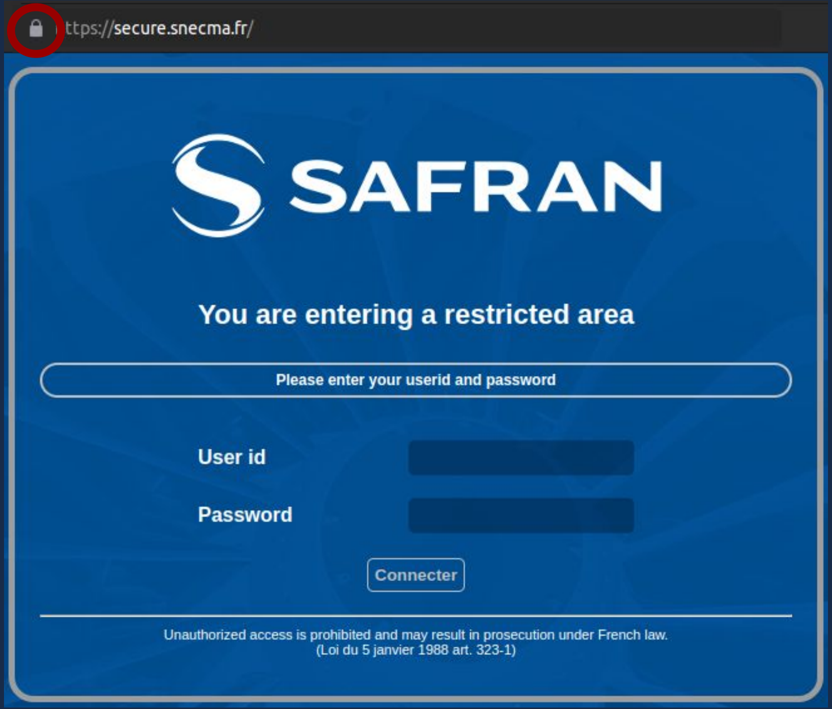
You are entering a restricted area

Please enter your userid and password

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

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!



ttps://secure.snecma.fr/

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 1988 art. 323-1)

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

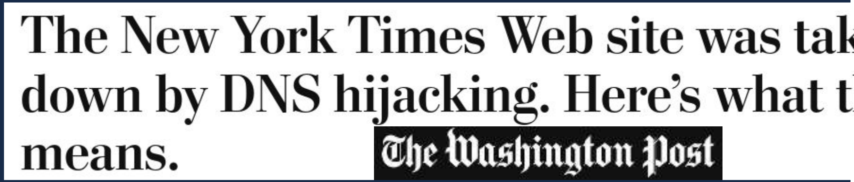
- ❑ Acquire ability to control DNS delegations
  - ❑ Hijacks characterized by multiple brief updates to evade detection
  - ❑ Attacker can bypass TLS, and DNSSEC protections
- ❑ Set up infrastructure to mimic target domain
  - ❑ Infrastructure uses maliciously obtained TLS certificate
  - ❑ Practically, 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

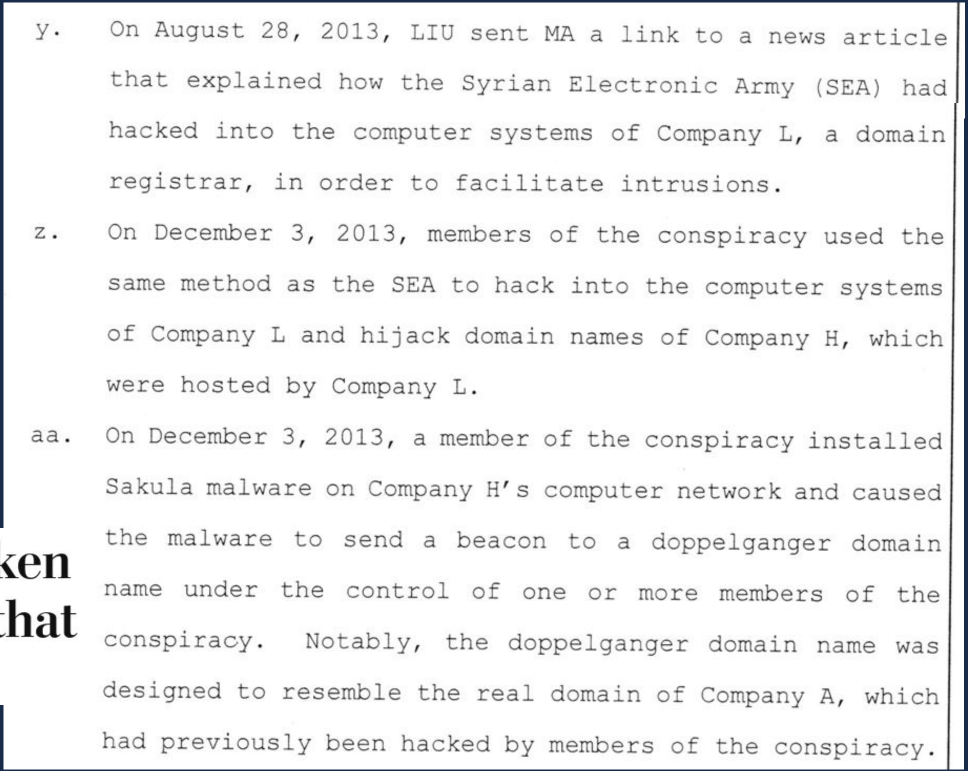
Learning New Tactics…

- ❑ 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

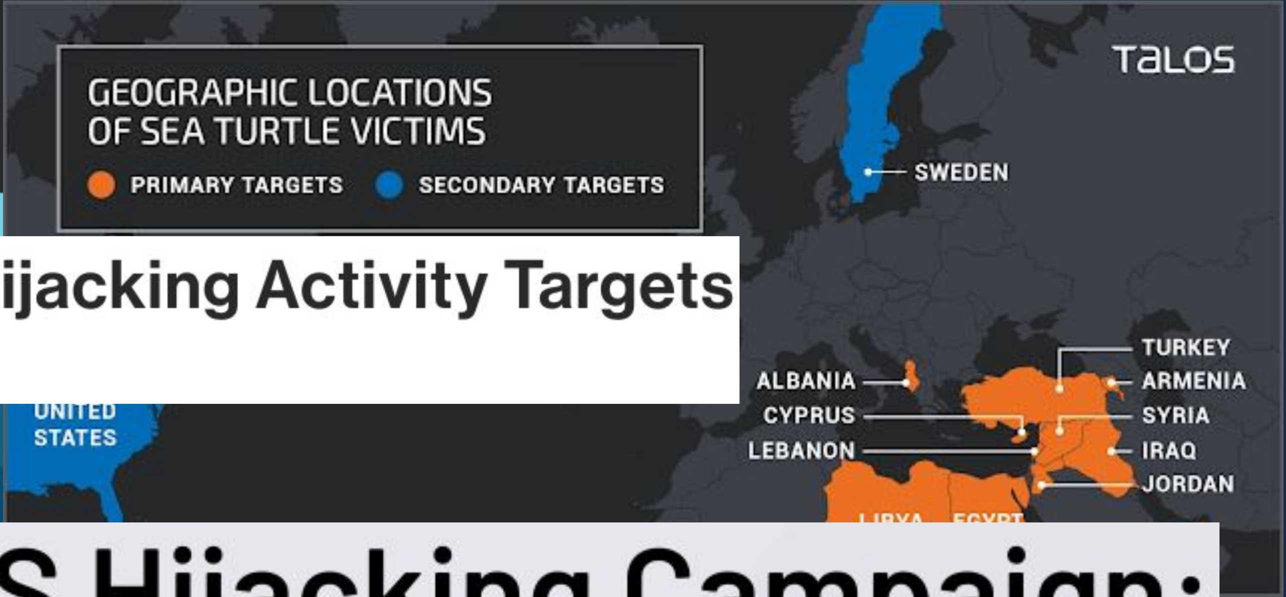


y. On August 28, 2013, LIU sent MA a link to a news article that explained how the Syrian Electronic Army (SEA) had hacked into the computer systems of Company L, a domain registrar, in order to facilitate intrusions.

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.

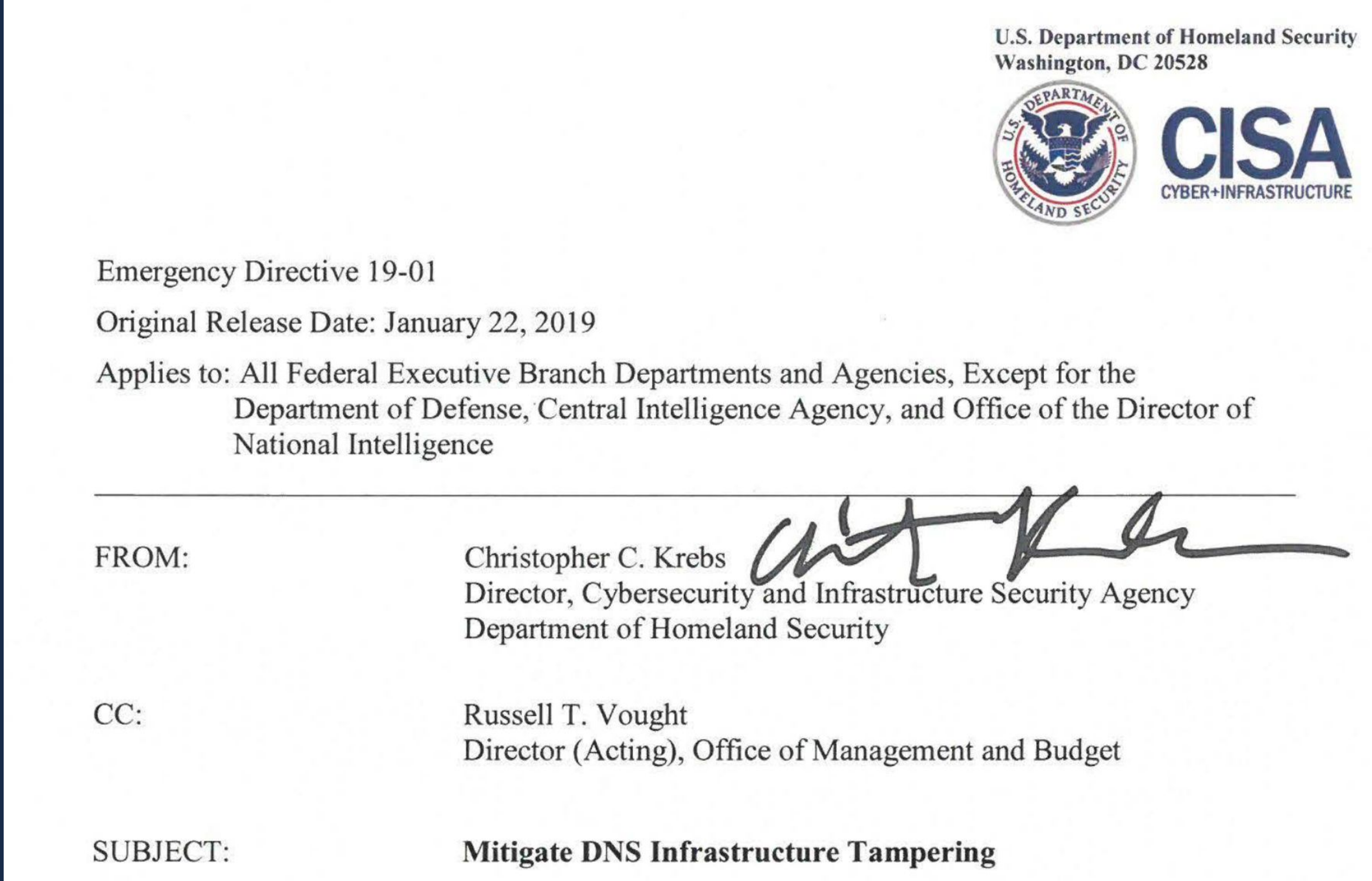
DNS Hijacking Abuses Trust In Core Internet Service



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.

The “Master” Plan

Phase 1: Gather Data

Phase 2: ??????

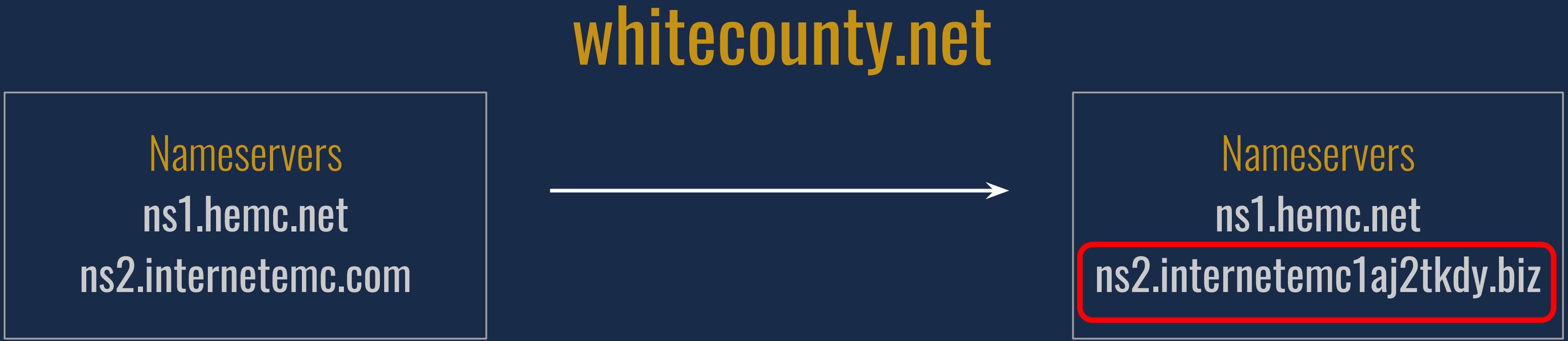
Phase 3: ~~Profit!!!~~ Identify Hijacks

THE DNS
1-603-532-8086
1-603-532-8086
IS DARK AND FULL OF TERRORS

“Now you have TWO problems”

Mystery Nameserver Change?

White County, Georgia Official Domain: *whitecounty.net*



whitecounty.net

Nameservers
ns1.hemc.net
ns2.internetemc.com

Nameservers
ns1.hemc.net
ns2.internetemc1aj2tkdy.biz

- **internetemc1aj2tkdy.biz** is not registered...
- So *anyone* can register the domain to be the authoritative nameserver
- We find thousands of similar domains. What happened here?

The Larger Picture

Domain Hijacks

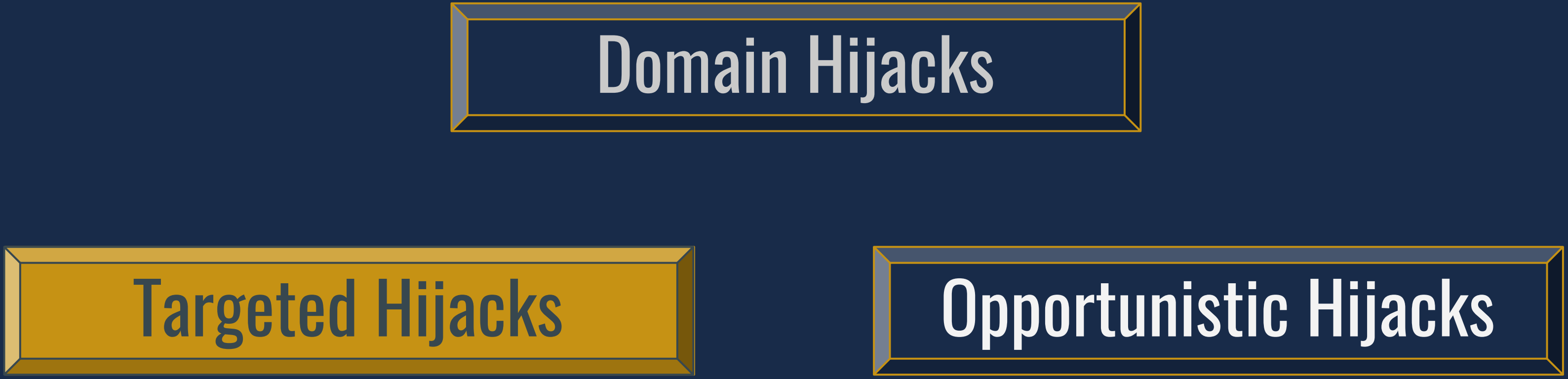
Targeted Hijacks

Opportunistic Hijacks

Retroactive Identification: IMC 2022

Risky BIZness: IMC 2021

The Larger Picture


Domain Hijacks

Targeted Hijacks

Opportunistic Hijacks

Retroactive Identification: IMC 2022

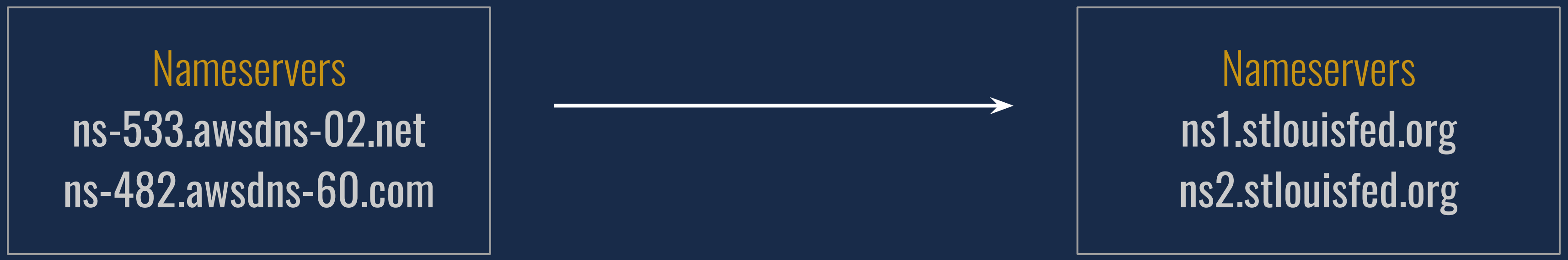
Risky BIZness: IMC 2021

Challenges in Identifying Targeted Hijacks

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

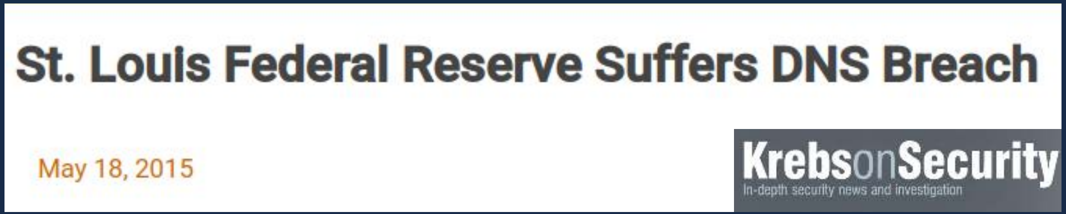
Malicious but looks Legitimate...

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

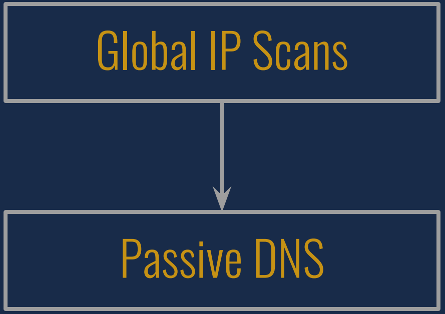
Attacker infrastructure will appear in global IP scans looking for certificates.

Identifying Targeted DNS Infrastructure Hijacks: Intuition

Global IP Scans

Identify Attacker Infrastructure. IP_A+ $Cert_A$

Identifying Targeted DNS Infrastructure Hijacks: Intuition



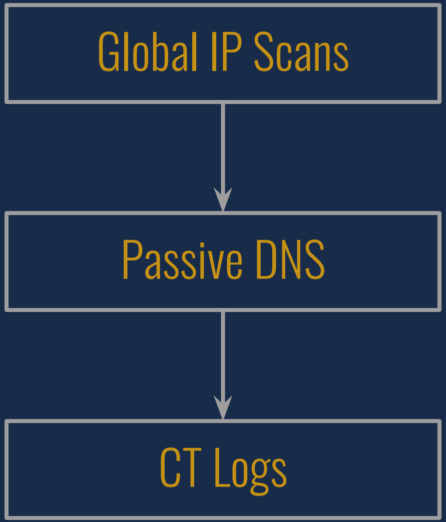
Global IP Scans

Passive DNS

Identify Attacker Infrastructure. IP_A + $Cert_A$

Corroborate target domain was redirected to IP_A

Identifying Targeted DNS Infrastructure Hijacks: Intuition



Global IP Scans

Identify Attacker Infrastructure. IP_A+ $Cert_A$

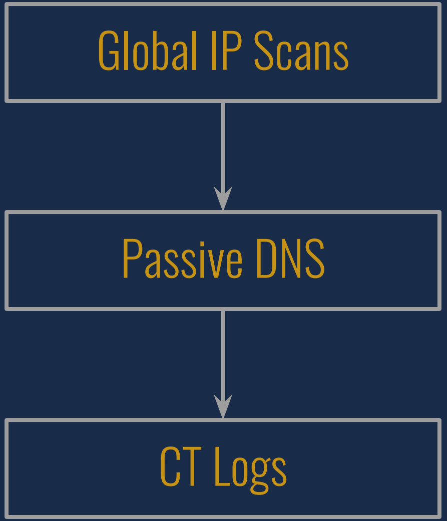
Passive DNS

Corroborate target domain was redirected to IP_A

CT Logs

Corroborate $Cert_A$ was issued during redirection

Identifying Targeted DNS Infrastructure Hijacks: Intuition



Global IP Scans

Passive DNS

CT Logs

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

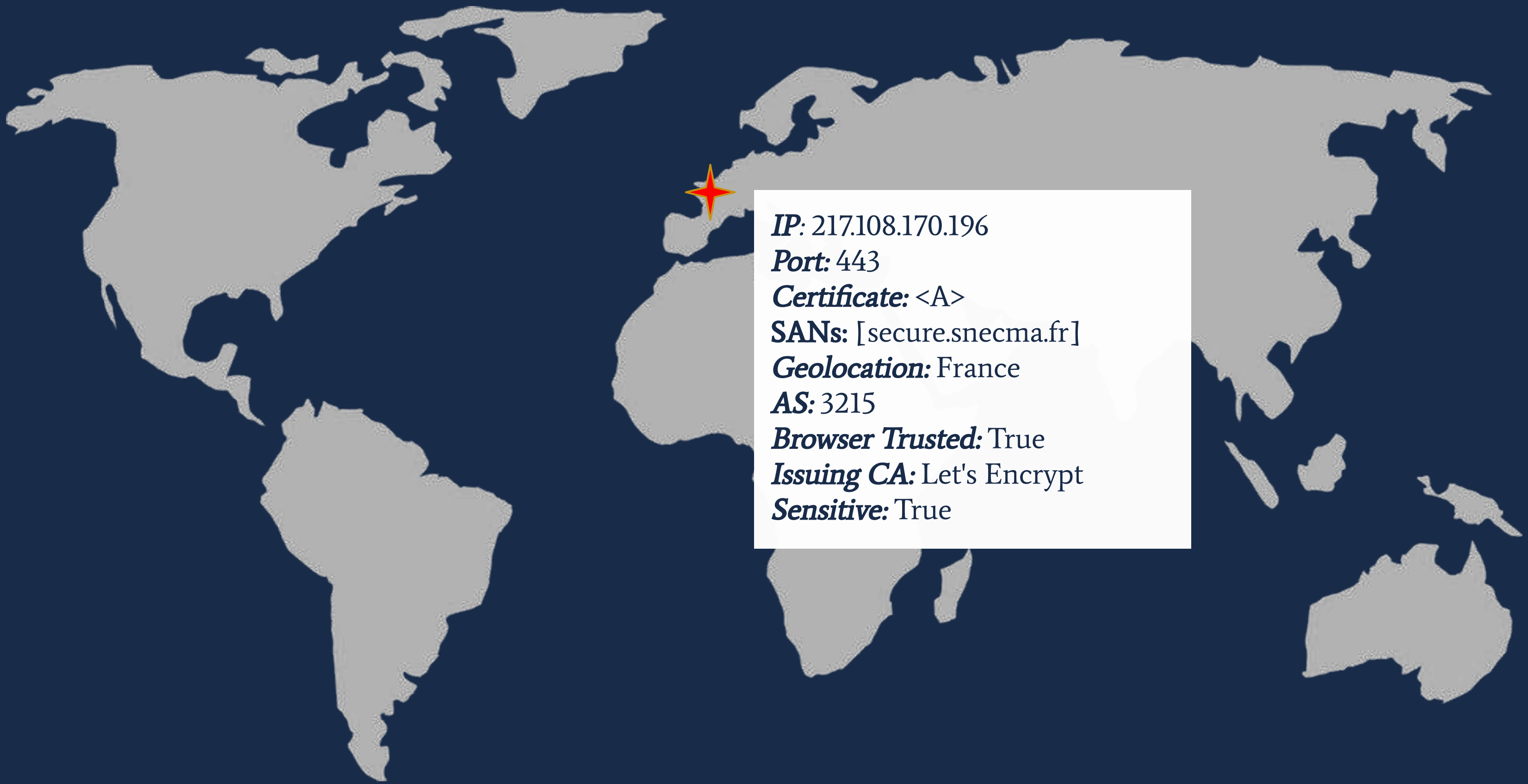
“Observable Infrastructure for a domain”

> *IP addresses and certificates that secure and serve the domain*

Observable Infrastructure

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.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: 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

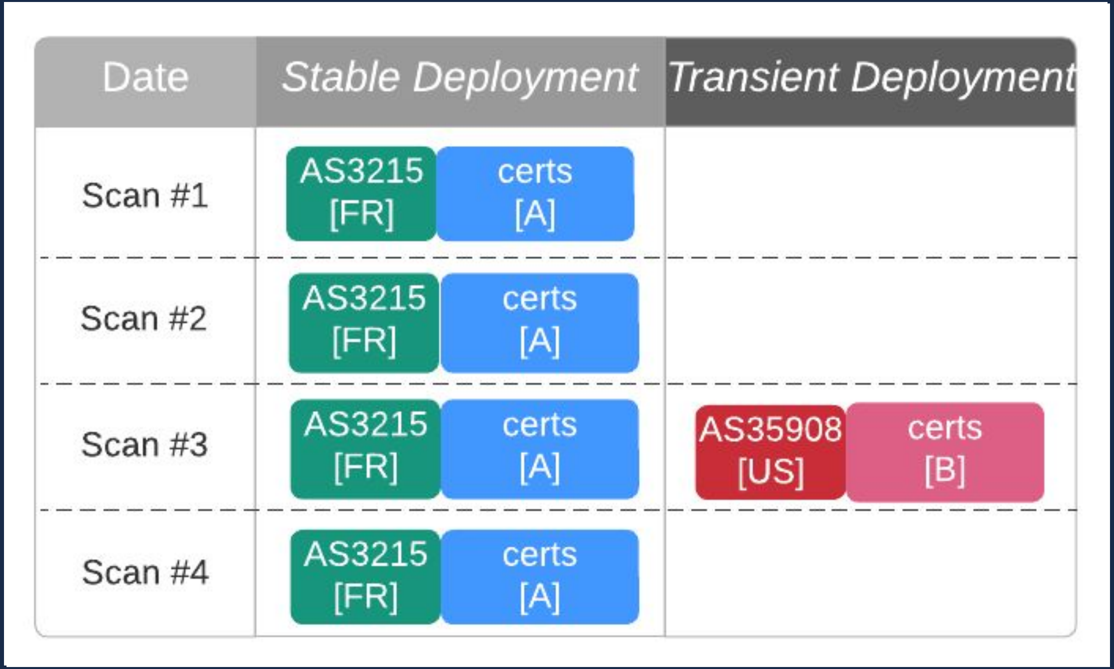
Legitimate or Malicious?

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

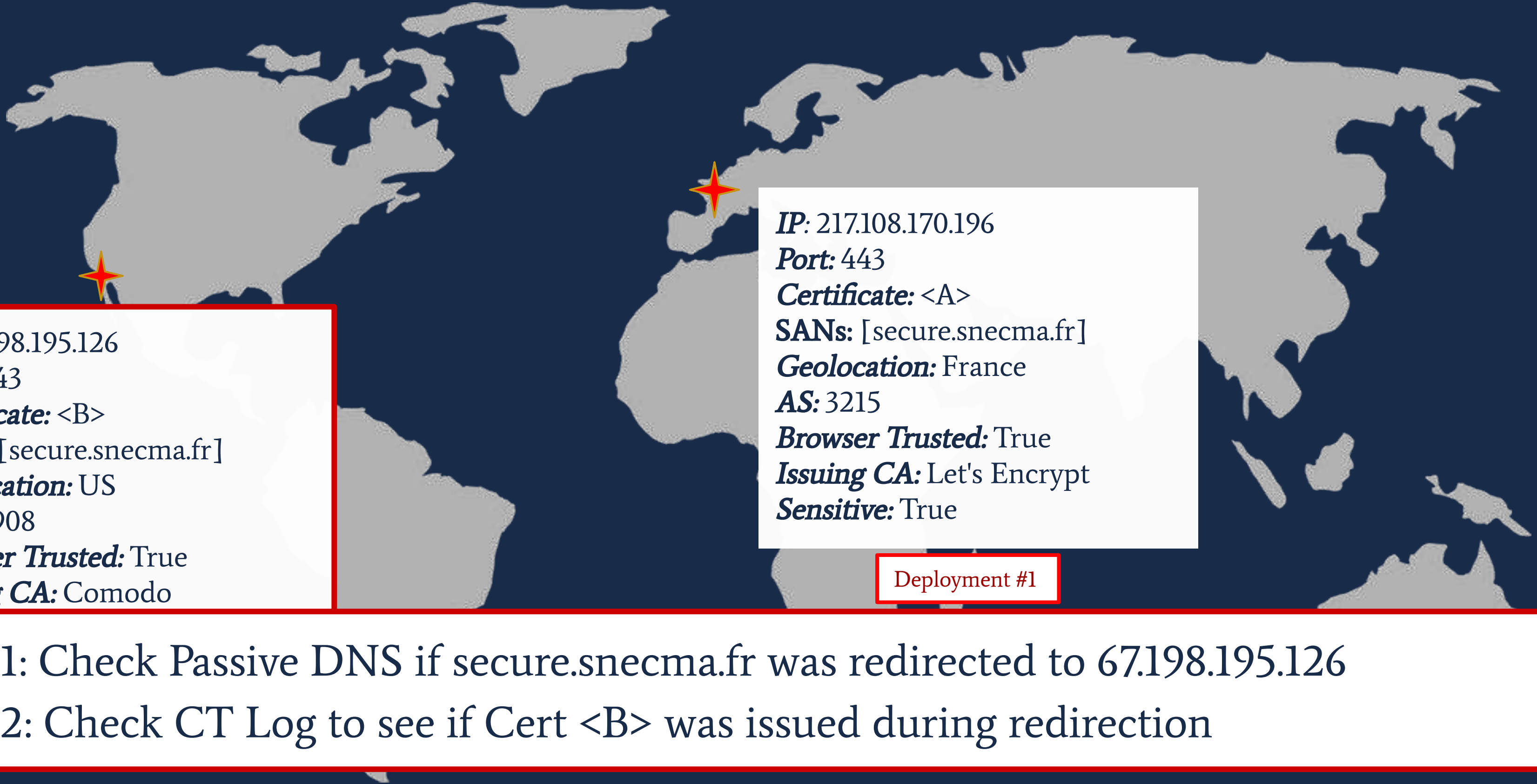
IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.snecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

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

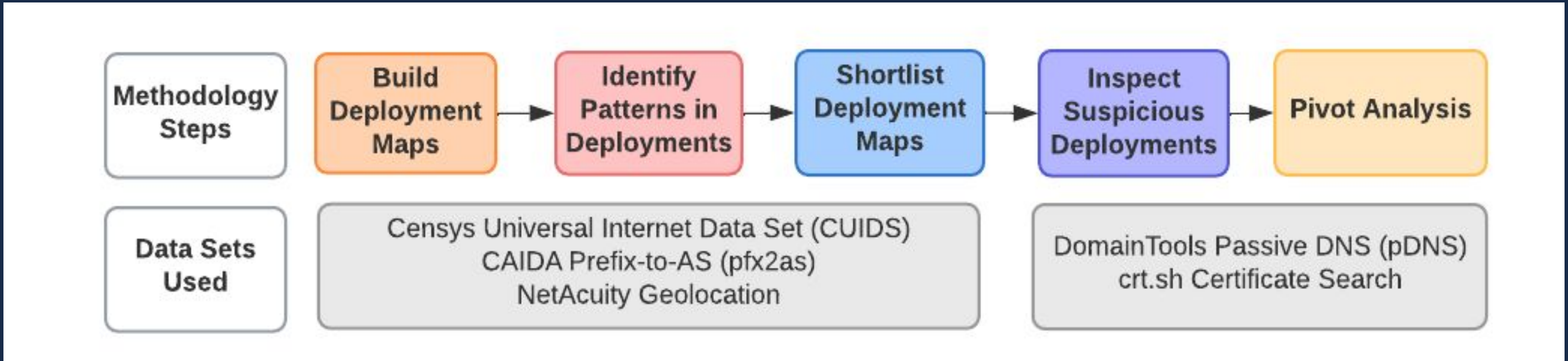
IP: 217.108.170.196
Port: 443
Certificate: <A>
SANs: [secure.snecma.fr]
Geolocation: France
AS: 3215
Browser Trusted: True
Issuing CA: Let's Encrypt
Sensitive: True

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

Methodology Summary



Methodology Steps

Build Deployment Maps → Identify Patterns in Deployments → Shortlist Deployment Maps → Inspect Suspicious Deployments → Pivot Analysis

Data Sets Used

Censys Universal Internet Data Set (CUIDS)
CAIDA Prefix-to-AS (pfx2as)
NetAcuity Geolocation

DomainTools Passive DNS (pDNS)
crt.sh Certificate Search

Hijacked Domains

Identified 41 domains as hijacked (between 2017-2020)

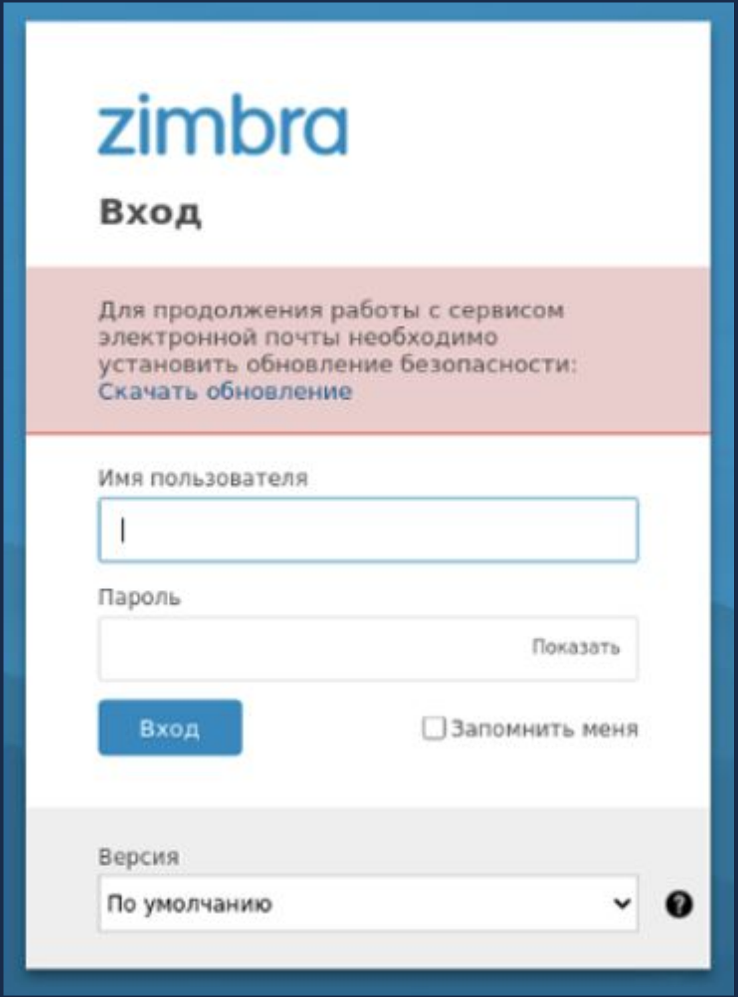
- 33 domains re-identified and verified from previous reports
- 8 domains not previously identified

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



zimbra

Вход

Для продолжения работы с сервисом электронной почты необходимо установить обновление безопасности: Скачать обновление

Имя пользователя

Пароль

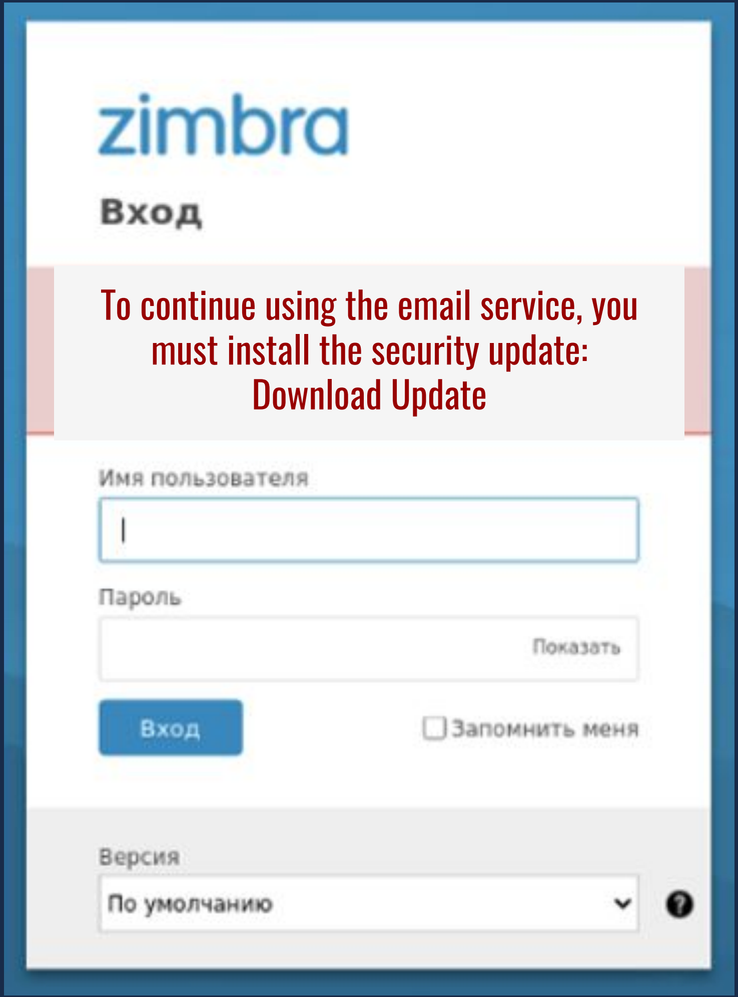
Показать

Вход

□ Запомнить меня

Версия

По умолчанию



zimbra

Вход

To continue using the email service, you must install the security update:
Download Update

Имя пользователя

Пароль

Показать

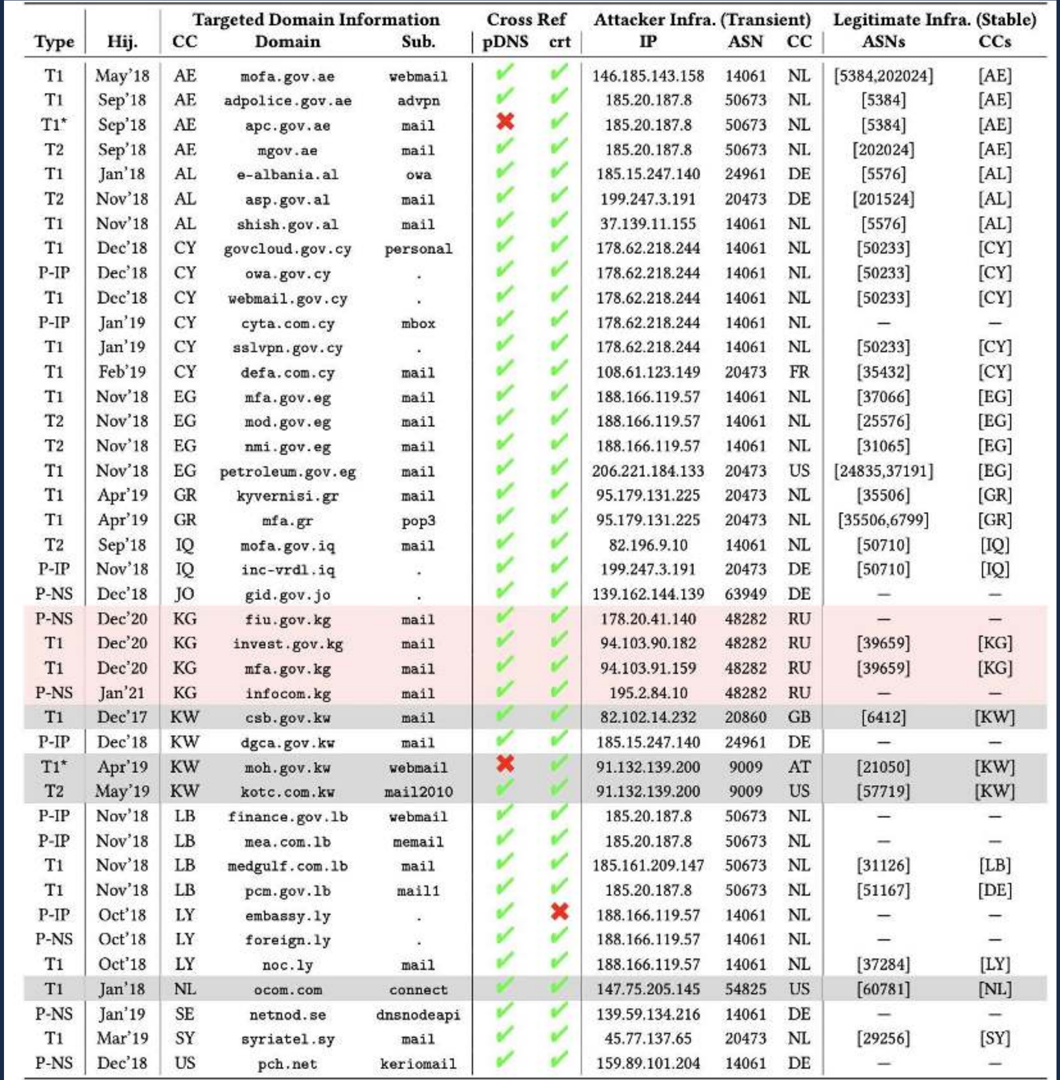
Вход

□ Запомнить меня

Версия

По умолчанию

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



		Targeted Domain Information			Cross Ref		Attacker Infra. (Transient)			Legitimate Infra. (Stable)	
Type	Hij.	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

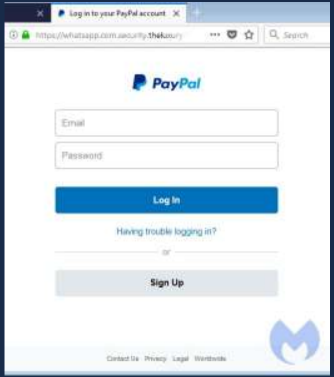
Parting Thoughts

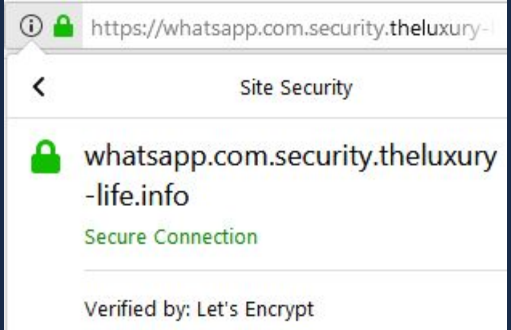
Thought #1

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

Not a hypothetical risk. Operators are prime targets.

Thought #2


Log in to your PayPal account
https://whatsapp.com.security.theluxury
Search
PayPal
Email
Password
Log In
Having trouble logging in?
or
Sign Up
Contact Us
Privacy
Legal
Worldwide


https://whatsapp.com.security.theluxury-

Site Security

whatsapp.com.security.theluxury-life.info

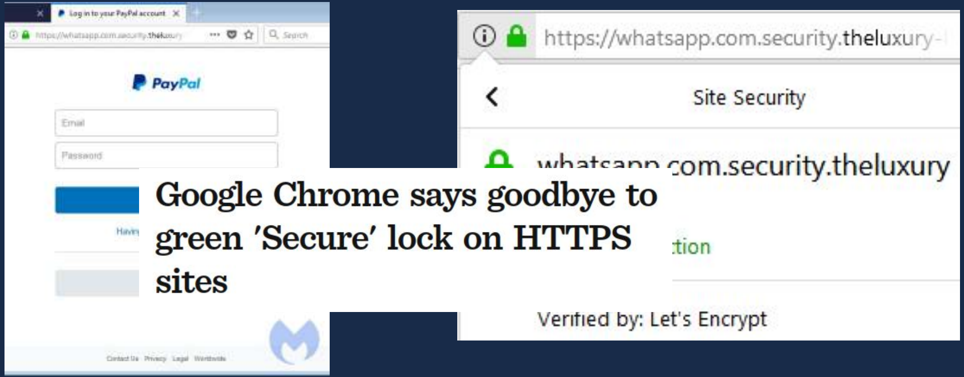
Secure Connection

Verified by: Let's Encrypt

Secure protocols do not *always* mean secure.

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

Thought #2



Log in to your PayPal account
https://whatsapp.com.security.theluxury
PayPal
Email
Password
Search

https://whatsapp.com.security.theluxury-

Site Security

whatsapp.com.security.theluxury

Verified by: Let's Encrypt

Google Chrome says goodbye to green 'Secure' lock on HTTPS sites

Secure protocols do not *always* mean secure.

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

Thought #3

Monitoring and Transparency are important

“You cannot secure what you cannot measure!”

DNS Transparency

- Organizations cannot tell if their nameservers ever changed!
  - Have apricot.net 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?

Thank You!

Collaborators

Geoffrey Voelker

Ian Foster

KC Claffy

Mattijs Jonker

Raffaele Sommese

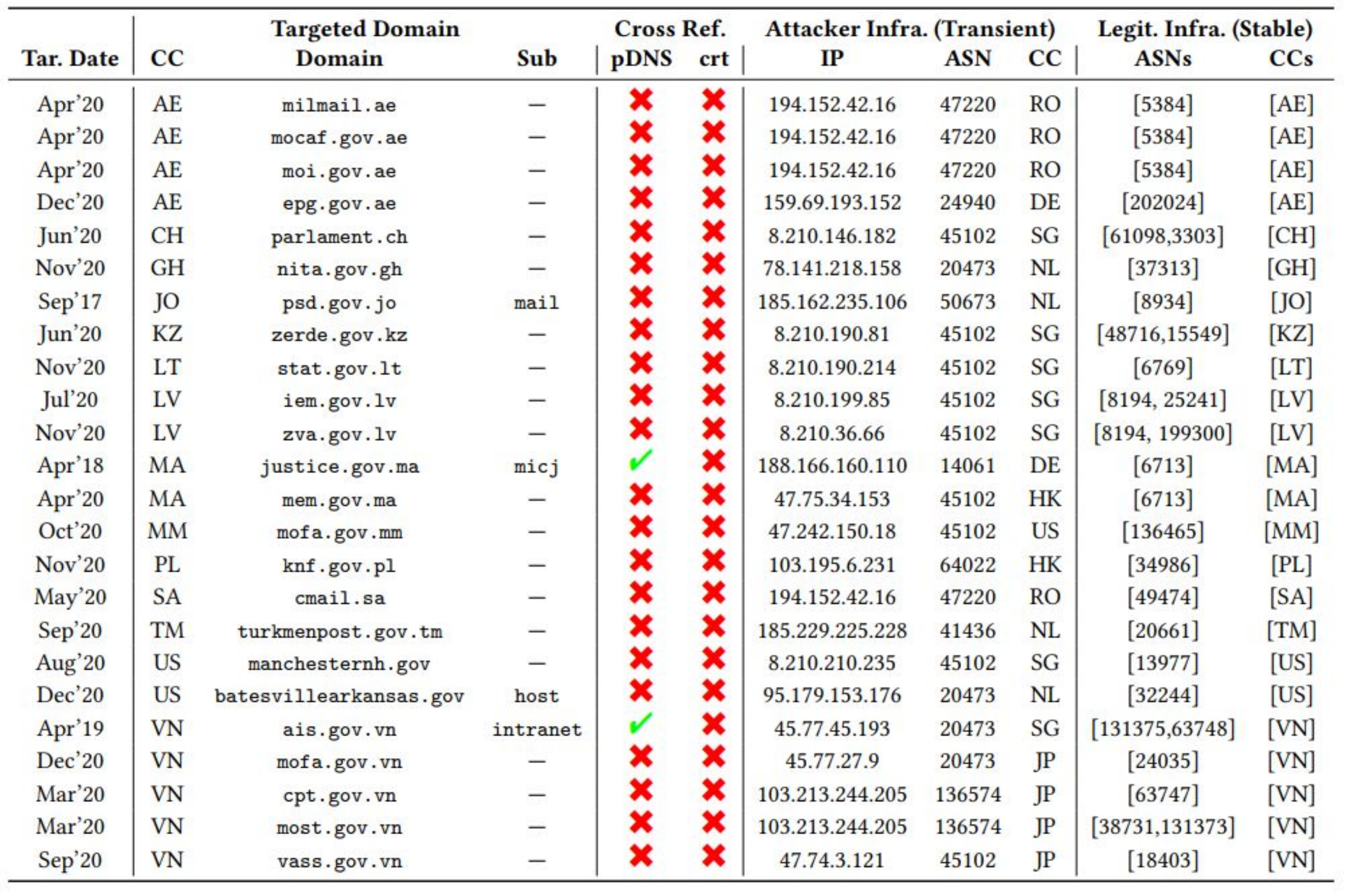
Stefan Savage

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]