Informe # 2 sobre la salud del internet en Cuba

Autor
Diktyon

Hallazgos claves

En nuestro monitoreo entre junio, julio y agosto de 2023, encontramos que 60 dominios, principalmente sitios de noticias y derechos humanos, estaban bloqueados de un total de 233 dominios monitoreados.

- Se censuraron 40 sitios, manipulando la transmisión de paquetes, mediante tecnología de inspección profunda de paquetes (DPI por sus siglas en inglés).

- Encontramos que las versiones HTTPS de 12 sitios web son catalogadas por OONI como mediciones fallidas, pero que en realidad estos 12 sitios webs están siendo censurados mediante tecnología DPI.

Para este informe, utilizamos las herramientas del Observatorio Abierto de Interferencias de la Red (OONI, por sus siglas en inglés):
OONI Probe para obtener muestras, OONI Explorer para analizarlas y OONI MAT para crear gráficas.

También realizamos capturas de paquetes con la herramienta WireShark para poder examinar los protocolos en detalle.

Introducción y objetivos

Este informe trimestral actualiza nuestra última publicación de los meses entre marzo y mayo de 2023, detallando la censura de internet en Cuba y enfocándonos en determinar las diferencias de censura según el protocolo utilizado (HTTP o HTTPS). Realizamos capturas de tráfico de paquetes para entender mejor cómo se censuran los dominios.

En este informe analizamos las mediciones de OONI catalogadas como fallidas que confirman interferencia en el handshake de TLS. Realizamos capturas de paquetes de tráfico en WireShark y demostramos que se trata de censura por tecnología DPI.

TLS

El protocolo TLS agrega una capa de seguridad al encapsular las peticiones HTTP y cifrar la comunicación en Internet, protegiéndola de ataques y garantizando la privacidad de los datos. El handshake de TLS es el proceso en el que cliente y servidor establecen una conexión segura intercambiando mensajes con información sobre el protocolo y algoritmos de cifrado utilizados en la comunicación en la comunicación que van a establecer a continuación.

Listado de dominios censurados:

A continuación, se enumeran los dominios censurados, sus categorías y el protocolo analizado, distinguiendo los meses de junio, julio y agosto.

Durante el periodo de estudio, OONI lista 60 dominios que experimentaron diferentes tipos de censura, afectando al protocolo TCP, DNS y HTTP, en la mayoría de estos casos se utilizó tecnología DPI. Cuando decimos fallidas en esta lista nos referimos a las mediciones que OONI cataloga como "mediciones fallidas".

#	Dominio	Categoría	HTTP (Junio)	HTTPS (Junio)	HTTP (Julio)	HTTPS (Julio)	HTTP (Agosto)	HTTPS (Agosto)
1	cubasindical.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
2	damasdeblanco.com	Sitios de Derechos Humanos	Censura por DPI		Censura por DPI	Fallida	Censura por DPI	Fallida

3	anon.inf.tu-dresden.de	Herramientas de elusión y anonimización	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
4	gatopardo.com	Sitios de noticias	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
5	conexioncubana.net		Censura por DPI		Censura por DPI	Fallida	Censura por DPI	Fallida
6	miscelaneasdecuba.net	Sitios de noticias	Censura por DPI		Censura por DPI	Bloqueo de HTTP	Censura por DPI	Fallida
7	centroconvivencia.org	Sitios críticos con el gobierno	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP		Bloqueo de HTTP
8	cubadata.com	Sitios críticos con el gobierno	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
9	idealpress.com	Religión	Censura por DPI		Censura por DPI	Bloqueo de TCP/IP	Censura por DPI	Bloqueo de TCP/IP
10	shavei.org	Religión	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
11	cubademocraciayvida.org	Sitios críticos con el gobierno	Censura por DPI		Censura por DPI	Fallida	Censura por DPI	Fallida
12	nieman.harvard.edu	Sitios de noticias	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
13	solidaridadconcuba.com	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Fallida
14	victimsofcommunism.org	Sitios de Derechos Humanos		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
15	freedomhouse.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
16	14ymedio.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
17	cibercuba.com	Sitios críticos con el gobierno	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
18	cubanet.org	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
19	diariodecuba.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
20	cubaencuentro.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
21	apretaste.com	Motores de búsqueda		Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
22	change.org	Activismo	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
23	cubaposible.com	Sitios de Derechos Humanos	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
24	trello.com	Herramientas de comunicación	TCP/IP DNS	DNS	TCP/IP DNS	TCP/IP DNS	TCP/IP DNS	TCP/IP DNS
25	911truth.org	Activismo	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
26	beerinfo.com	Alcohol y drogas	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
27	canf.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallido	Censura por DPI	Fallida
28	cubacenter.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Bloqueo de HTTP		Bloqueo de HTTP

29	cubafreepress.org	Sitios de Derechos Humanos	Censura por DPI		Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de TCP/IP/ HTTP
30	dharmanet.org	Religión		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
31	avaaz.org		Censura por DPI		Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
32	payolibre.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Fallida	Censura por DPI	Fallida
33	periodicocubano.com	Sitios de noticias		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
34	schwarzreport.org	Religión	Bloqueo de TCP/IP		Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
35	univision.com				Censura por DPI	Fallida	Censura por DPI	Fallida
36	asere.com	Sitios de noticias		Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
37	cubalex.org	Sitios de Derechos Humanos		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
38	cadal.org	Sitios de Derechos Humanos		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
39	cubanosporelmundo.com	Sitios de noticias		Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP		Bloqueo de HTTP
40	cubadecide.org	Sitios críticos con el gobierno	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
41	proyectoinventario.org	Sitios críticos con el gobierno	Censura por DPI		Censura por DPI	Bloqueo de HTTP		Bloqueo de HTTP
42	rialta.org	Sitios de noticias	Censura por DPI		Censura por DPI	Fallida	Censura por DPI	Fallida
43	demoamlat.com	Sitios de Derechos Humanos		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de TCP/IP/ HTTP
44	observacuba.org	Sitios de Derechos Humanos		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
45	adncuba.com	Sitios de noticias		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de TCP/IP/ HTTP
46	revistaelestornudo.com	Cultura		Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
47	hermanos.org	Religión			Censura por DPI		Censura por DPI	
48	somosmascuba.com				Censura por DPI	Fallida	Censura por DPI	Fallida
49	cubaenmiami.com	Sitios de noticia			Censura por DPI	Fallida	Censura por DPI	Fallida
50	unpacu.org	Sitios de Derechos Humanos			Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
51	libertaddigital.com	Sitios de noticia			Censura por DPI	Bloqueo de HTTP	Censura por DPI	Fallida
52	cafefuerte.com	Sitios de noticia			Bloqueo de HTTP	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
53	icj.org				Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
54	cubanartnewsarchive.org				Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP

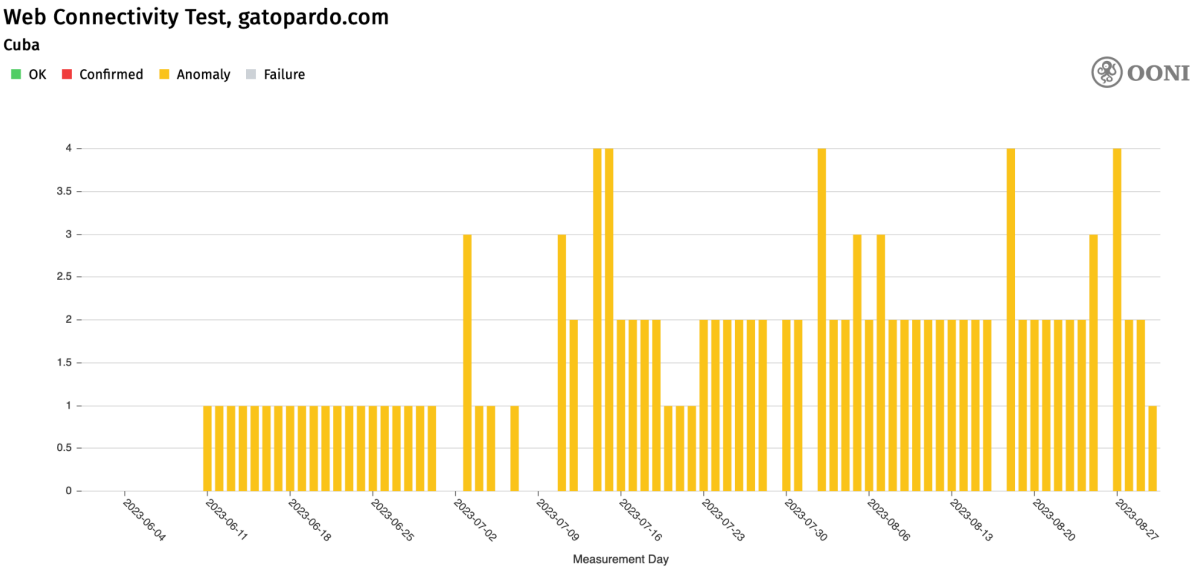
55	voanews.com				Censura por DPI	Fallida	Bloqueo de HTTP	Bloqueo de HTTP
56	corriente.org				Censura por DPI	Fallida	Censura por DPI	Fallida
57	represorescubanos.com				Censura por DPI	Fallida	Censura por DPI	Bloqueo de HTTP
58	pscuba.org				Censura por DPI	Fallida	Censura por DPI	Fallida
59	prisonersdefenders.org				Fallida	Fallida		Fallida
60	sigloxxi.org				Censura por DPI		Censura por DPI	Fallida

Censura que afecta al protocolo TCP

El protocolo TCP (Transmission Control Protocol) es un protocolo de transporte en internet necesario para que la comunicación entre aparatos funcione correctamente.
La censura afectando este protocolo es una práctica común en países donde hay restricciones de acceso a internet y puede ser llevada a cabo por las empresas, gobiernos y otras entidades proveedoras de servicio de internet (ISP por sus siglas en inglés).

Se lleva a cabo manipulando los paquetes de datos que se envían a través de este protocolo. En la mayoría de casos se manipula la comunicación enviando un TCP Reset, esta es una señal que se envía a través de la red para interrumpir una conexión TCP existente, cuando un paquete TCP reset es enviado, la conexión se cierra abruptamente imposibilitando el acceso al sitio web o servicio deseado.

A continuación un gráfico en el cual podemos observar un ejemplo de dominio que durante el periodo de estudio sufrió anomalías en el protocolo TCP dando como resultado la censura del mismo, en este caso gatopardo.com

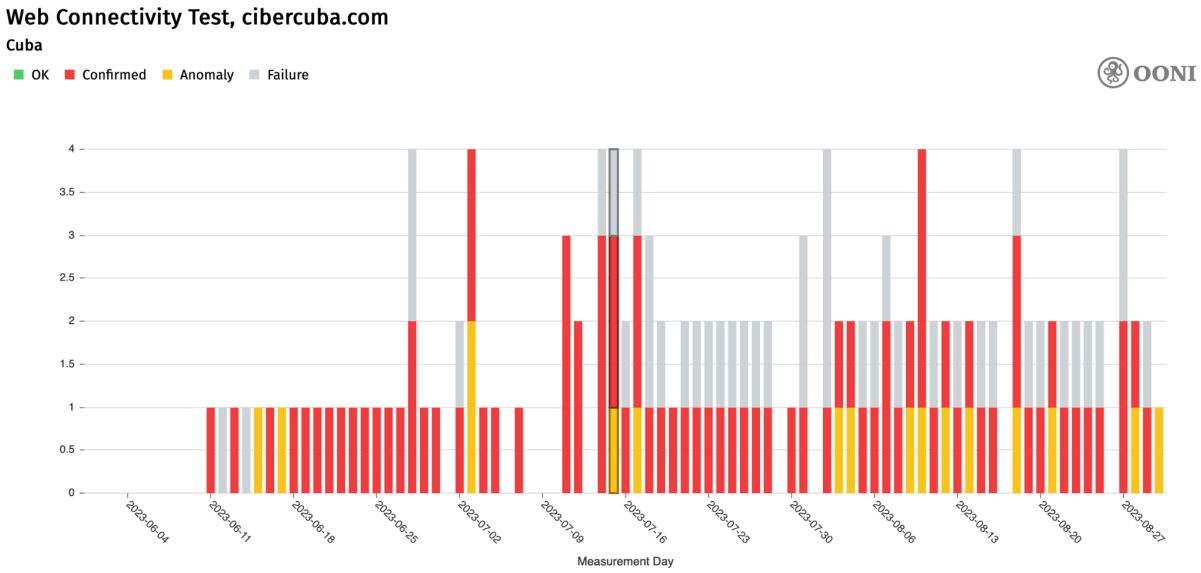


Censura que afecta al protocolo HTTP

El protocolo de transferencia de hipertexto (HTTP por sus siglas en inglés) es el protocolo utilizado por los sitios web y que nos permite visualizar la web.

La censura que afecta este protocolo se refiere a la práctica de bloquear el acceso a ciertos sitios web mediante la modificación de su contenido, dado que este no viaja encapsulado en protocolo de seguridad. Así que nos encontramos mensajes de error falsos o páginas en blanco.

En el siguiente gráfico podemos observar las mediciones al dominio cibercuba.com, el cual durante el periodo de estudio sufrió anomalías en el protocolo HTTP, resultando en la censura del mismo.

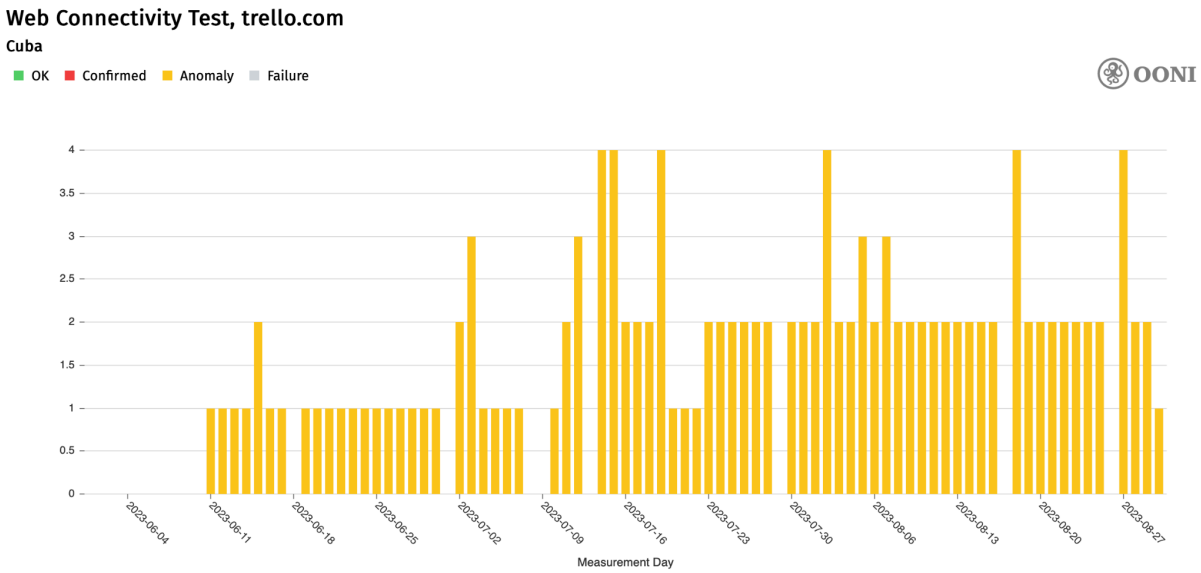


Censura que afecta al protocolo DNS

Gracias al protocolo DNS (servicio de nombre de dominio) se traducen los nombres de dominio en direcciones IP. Un dispositivo hace una solicitud y el DNS resolver que esté configurado responderá con la IP relacionada al dominio solicitado.

Las empresas, los gobiernos u otras entidades proveedoras de servicio de internet pueden gestionar el DNS resolver y aprovechar de este control para bloquear ciertos sitios web manipulando estas respuestas DNS. Por lo tanto, al intentar acceder a una web bloqueada, la consulta DNS nos responde con una dirección IP diferente, impidiendo así el acceso al contenido deseado.
La censura por DNS es una forma comúnmente utilizada para restringir el acceso a información y controlar la navegación en internet en la gran mayoría de países.

En el siguiente gráfico observamos las mediciones al dominio trello.com, el cual durante el periodo de estudio sufrió anomalías en el protocolo DNS, por lo que se encontró bloqueado al intentar acceder desde Cuba.



Censura mediante tecnología DPI en Cuba

De los 60 sitios bloqueados, 40 de ellos son claramente por tecnología DPI, ya que hemos encontrado el identificante del servidor, V2R2C00-IAE/1.0 asociado a la empresa china Huawei. Información explicada detalladamente en el informe # 1 sobre la salud del internet en Cuba.

Esta tecnología permite controlar y censurar el acceso a ciertos contenidos en internet mediante la inspección detallada de los paquetes de datos que se envían a través de la red. En otros sitios web no podemos asegurar que se trate de censura por tecnología DPI porque no tenemos suficiente evidencia.

Mediciones fallidas

Al hacer mediciones en la versión HTTPS de estos dominios, descubrimos que en 12 de los 60 dominios censurados las mediciones fueron catalogadas como fallidas por OONI en la mayoría de las ocasiones.

Al analizar los JSON de OONI en detalle observamos la misma línea informativa en los 12 dominios censurados:

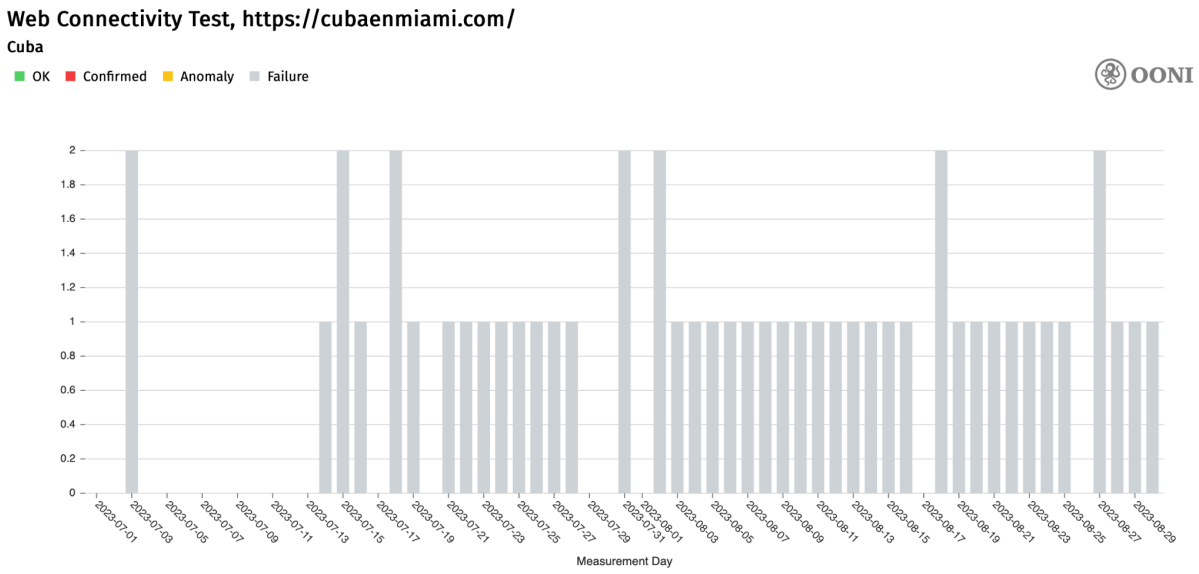
```
unknown_failure: tls: first record does not look like a TLS handshake
```

Este mensaje de fallo desconocido significa que está ocurriendo un problema en el handshake de TLS.

En el primer informe nos quedó la sospecha y gracias a las capturas de tráfico de paquetes realizadas con WireShark durante el periodo de julio y agosto, hemos podido confirmar la utilización de tecnología DPI afectando el protocolo TLS.

En el [informe de OONI publicado en marzo de 2023], muchas de estas mediciones pueden ser consideradas como formas de censura. Pero precisamente el mensaje de fallo desconocido, significa que el sitio está sufriendo censura. En el informe nos explican también que están trabajando para mejorar el software de OONI y que este reconozca el problema del handshake de TLS como una anomalía.

El sitio web [https://cubaenmiami.com/] es un ejemplo de esto, ya que en todas las mediciones que se realizaron durante el periodo de estudio fueron catalogadas por OONI como “mediciones fallidas”.

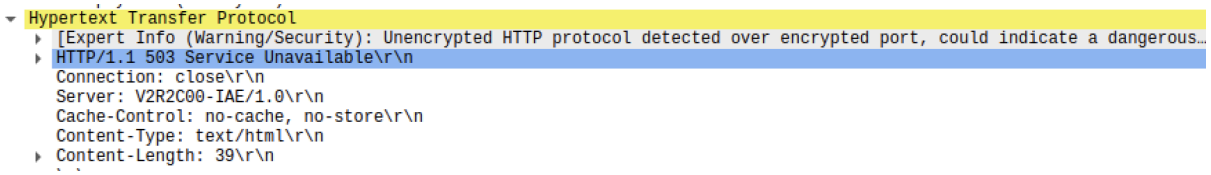


Al analizar el tráfico de paquetes con WireShark, confirmamos interferencia en el handshake de TLS. En esta captura de WireShark podemos observar:

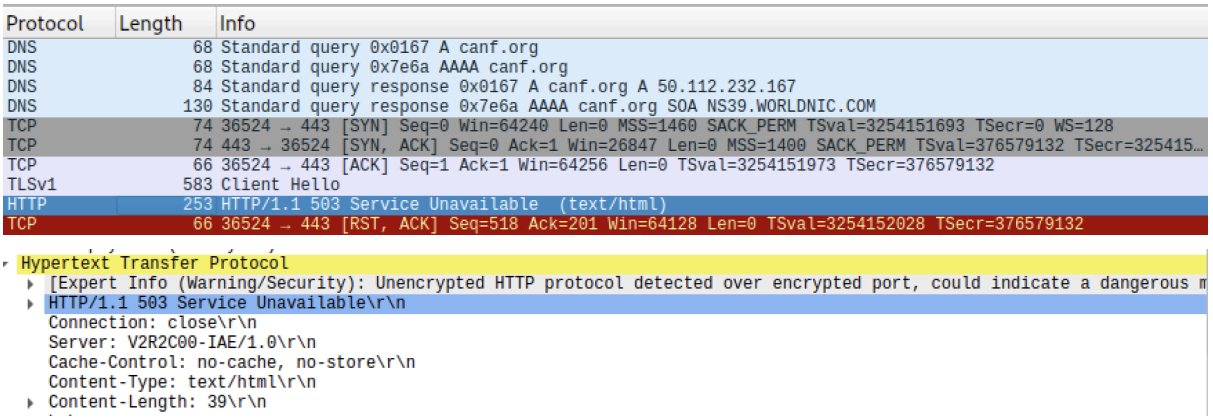
Protocol	Length	Info
DNS	76	Standard query 0x0d04 A cubasindical.org
DNS	76	Standard query 0x2607 AAAA cubasindical.org
DNS	92	Standard query response 0x0d04 A cubasindical.org A 208.113.138.142
DNS	140	Standard query response 0x2607 AAAA cubasindical.org SOA ns1.dreamhost.com
TCP	74	47346 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2211869078 TSecr=0 WS=128
TCP	74	443 → 47346 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1400 SACK_PERM TSval=329910130 TSecr=221186…
TCP	66	47346 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2211869302 TSecr=329910130
TLSv1	583	Client Hello
HTTP	253	HTTP/1.1 503 Service Unavailable (text/html)
TCP	66	47346 → 443 [RST, ACK] Seq=518 Ack=201 Win=64128 Len=0 TSval=2211869359 TSecr=329910130

1. El primer intercambio del handshake funciona correctamente
2. El segundo es interferido por la máquina intermedia (DPI), modifica la IP y se hace pasar por el servidor de destino, respondiendo con un [código de estado] de HTTP 503 que indica que el servidor no está disponible temporalmente.

Normalmente los paquetes de HTTP van encapsulados dentro de TLS después de un handshake correcto entre cliente y servidor. En una captura de tráfico de paquetes sana, después del Handshake de TLS veríamos paquetes con contenido cifrado mediante las llaves de TLS. Igualmente no recibimos paquetes de HTTP antes de finalizar el handshake de TLS.
Además, en los headers del paquete, podemos ver el identificante del servidor, V2R2C00-IAE/1.0 asociado a la empresa china Huawei. El mismo hardware utilizado para censurar mediante DPI, explicado en el informe 1 sobre la salud del internet en Cuba.



Lo mismo pasa en la petición al sitio https://canf.org/ donde observamos el mismo servidor asociado a la censura por DPI.



Esta situación nos muestra la existencia de una máquina intermedia que interfiere en la comunicación al enviar un código de estado falso al decirnos que el servicio no es accesible.

Existen muchos códigos de estado, incluido el código de estado 451 utilizado cuando un contenido web ha sido bloqueado por razones legales. Por lo que podemos concluir que el gobierno está intentando engañarnos para no dejarnos acceder a determinados contenidos en internet y que pensemos que el problema es del servidor de destino, y no la verdad, que es que el gobierno nos está bloqueando este contenido y violando nuestros derechos de poder acceder a la información.

Conclusiones

Este informe confirma que la censura en Internet en Cuba continúa siendo una realidad. Durante los meses de junio, julio y agosto de 2023, se recopilaron pruebas a través de las mediciones de OONI, revelando que al menos 60 sitios web de los 233 monitoreados fueron

censurados en ese período. Se observó que 40 de estos sitios fueron bloqueados utilizando tecnología DPI, la cual ha estado en uso desde al menos 2017.

Además, las pruebas demuestran que el hardware utilizado para llevar a cabo la censura por DPI proviene de la empresa china Huawei. También se descubrió que el gobierno intenta engañar a través de falsos códigos de estado de HTTP, haciendo creer a las personas que el problema está en el servidor y no en la violación de nuestra libertad de acceso a ciertos contenidos en Internet.

Trabajos futuros

Además de los hallazgos presentados en este informe, nuestro equipo tiene planes para seguir supervisando los sitios web que fueron censurados durante el período de estudio, así como otros que podrían estar bloqueados pero que aún no se han medido. Realizaremos pruebas periódicas en OONI para determinar si las restricciones han sido levantadas o si persisten, y observar su evolución.

También profundizaremos en la investigación de algunos de los dominios censurados para comprender mejor cómo funciona el bloqueo. Para esto, complementaremos las pruebas de OONI con análisis del tráfico de red a través de capturas de paquetes mediante Wireshark.

Nuestro objetivo es seguir trabajando para informar sobre el estado de la libertad en Internet en la isla y actualizaremos si se produce algún cambio