Informe # 3 sobre la salud del Internet en Cuba

Autor
Diktyon

Hallazgos clave

Durante nuestro monitoreo en los meses de septiembre, octubre y noviembre de 2023, encontramos que 67 de los 240 dominios examinados, principalmente sitios de noticias y derechos humanos, estaban bloqueados en Cuba. Utilizamos 217 sitios de la lista de CitizenLab para Cuba y agregamos otros 23 con alta probabilidad de bloqueo en la isla para este estudio.

- En Cuba, se bloquearon 49 sitios web utilizando tecnología de inspección profunda de paquetes (DPI), manipulando la transmisión de paquetes.

- En el informe anterior descubrimos que al solicitar la versión HTTPS de 12 de los 60 dominios bloqueados, OONI los catalogaba como mediciones fallidas y que en realidad estaban siendo censurados mediante tecnología DPI. Este mes, hemos agregado 20 dominios más a esta lista, lo que suma un total de 32 dominios con mediciones fallidas en múltiples ocasiones que en realidad se trata de censura.

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 de tráfico con la herramienta WireShark para poder examinar los protocolos en detalle.

Introducción y objetivos

Este informe trimestral tiene como objetivo principal actualizar el listado de sitios web bloqueados en Cuba, así como investigar la utilización de tecnología DPI en dicha censura. Además, analizaremos el número de mediciones fallidas registradas por OONI para poder demostrar que efectivamente se trata de censura.
Por último, abordaremos en detalle el bloqueo de la herramienta Tor en Cuba, explorando las implicaciones técnicas y las restricciones que esto conlleva para la privacidad y la libertad de acceso a la información en Internet.
Con las mediciones de OONI y los análisis de capturas de paquetes de tráfico con WireShark, buscamos proporcionar una visión detallada y técnica sobre la censura de Internet en Cuba durante este trimestre.

Listado de dominios censurados:

A continuación, se enumeran los dominios censurados, sus categorías y el protocolo afectado por censura.

Durante el periodo de estudio, las mediciones de OONI identificaron 67 dominios sujetos a diversas formas de censura, incluyendo el bloqueo de los protocolos TCP y HTTP. La mayoría de estos casos involucraron el uso de la tecnología DPI. En esta lista, el término "fallidas" se refiere a las mediciones que OONI clasifica como "mediciones fallidas".

Tabla 1. Lista de sitios analizados1

# #	Dominio	Categoría	HTTP (Septiembre)	HTTPS (Septiembre)	HTTP (Octubre)	HTTPS (Octubre)	HTTP (Noviembre)	HTTPS (Noviembre)
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	Fallida	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	Bloqueo de TCP/IP
5*	conexioncubana.net	Turismo	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
6*	miscelaneasdecuba.net	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
7	directorio.org		Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
8*	cubadata.com	Sitios críticos con el gobierno	Censura por DPI/ Bloqueo de TCP/IP	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida

9*	idealpress.com	Religión	Censura por DPI	Bloqueo de TCP/IP	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	Bloqueo de TCP/IP
11*	cubademocraciayvida.org	Sitios críticos con el gobierno	Censura por DPI	Fallida	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	Bloqueo de TCP/IP
13*	solidaridadconcuba.com	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
14	victimsofcommunism.org	Sitios de Derechos Humanos	Bloqueo de TCP/IP	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	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
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	Bloqueo de HTTP	Bloqueo de HTTP
21	apretaste.com	Motores de búsqueda	Bloqueo de HTTP	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	Bloqueo de TCP/IP
24	911truth.org	Activismo	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
25	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	Bloqueo de TCP/IP
26*	canf.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
27*	cubacenter.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
28*	cubafreepress.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
29	dharmanet.org	Religión	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
30*	secure.avaaz.org	Activismo	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
31*	payolibre.com	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida

32*	periodicocubano.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
33	schwarzreport.org	Religión	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
34*	univision.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
35	asere.com	Sitios de noticias	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
36*	cubalex.org	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
37*	cadal.org	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
38	cubanosporelmundo.com	Sitios de noticias	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
39	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
40*	proyectoinventario.org	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por	Fallida
41*	rialta.org	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por	Fallida
42*	demoamlat.com	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
43	observacuba.org	Sitios de Derechos Humanos	Censura por	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por	Bloqueo de HTTP

44*	adncuba.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
45*	revistaelestornudo.com	Cultura	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
46*	hermanos.org	Religión	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
47*	somosmascuba.com	Activismo	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
48*	cubaenmiami.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
49*	unpacu.org	unpacu.org	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
50*	libertaddigital.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
51*	cafefuerte.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
52	icj.org	Derechos Humanos	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
53	cubanartnewsarchive.org	Cultura	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
54*	voanews.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
55*	corriente.org	Activismo político	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
56*	represorescubanos.com	Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
57*	pscuba.org		Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida

58	prisonersdefenders.org	Derechos Humanos	Fallida	Fallida	Accesible	Accesible	Accesible	Accesible
59*	sigloxxi.org		Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
60*	cubaxcuba.com	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
61*	oas.org	Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
62*	agendacuba.org	Turismo	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
63*	juventudlac.org						Censura por DPI	Fallida*
64*	cubalibredigital.com						Bloqueo de HTTP	Fallida*
65*	martinoticias.com		Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
66	americateve.com		Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
67*	cuballama.com						Censura por DPI	Bloqueo de HTTP

Censura que afecta al protocolo TCP

La censura que afecta al protocolo TCP (Transmission Control Protocol) es una práctica común en países donde existen restricciones en el acceso a internet. Esta forma de censura puede ser implementada por proveedoras de servicios de internet (ISP, por sus siglas en inglés).

Esta forma de censura se lleva a cabo mediante la manipulación de los paquetes de datos que se transmiten a través del protocolo TCP. En la mayoría de los casos, esta manipulación implica el envío de un TCP Reset, que es una señal enviada a través de la red con el propósito de interrumpir una conexión TCP existente. Cuando un paquete TCP Reset

es enviado, la conexión se cierra de manera abrupta, lo que resulta en la imposibilidad de acceder 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 el dominio es *icj.org*.

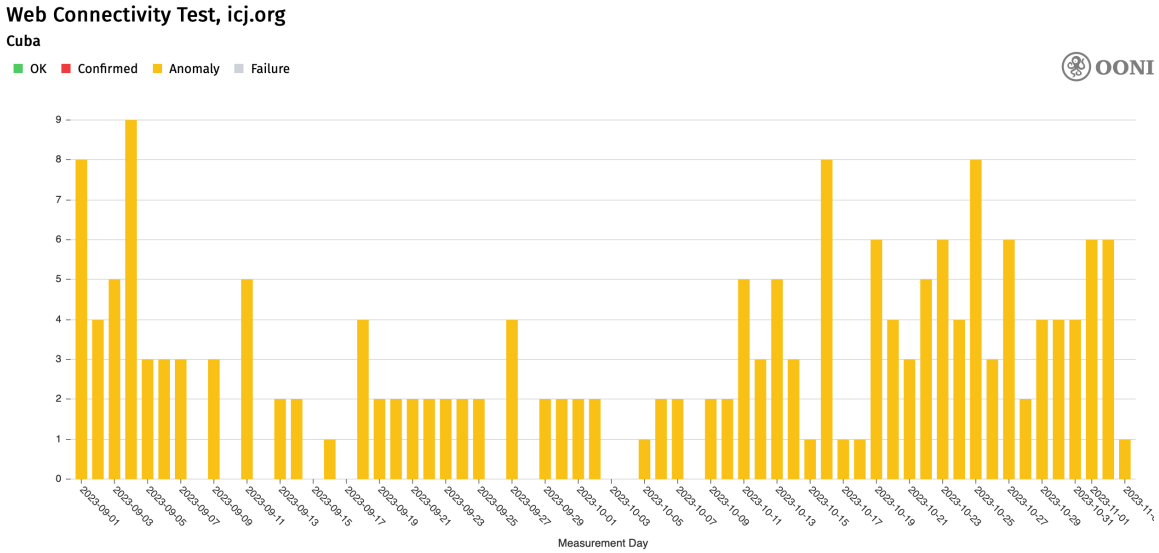


Imagen 1. Prueba de conectividad del dominio icj.org

Censura que afecta al protocolo HTTP

La censura que afecta al protocolo HTTP (Hypertext Transfer Protocol) se refiere a la práctica de bloquear el acceso a ciertos sitios web mediante la modificación de su contenido, cuando este protocolo no es transmitido de forma segura (encapsulado por un protocolo de seguridad). En este tipo de censura, es común encontrar mensajes de error falsos o páginas en blanco en lugar del contenido esperado.
Esta forma de censura se lleva a cabo manipulando las respuestas HTTP, lo que significa que se alteran los paquetes de datos que viajan entre las personas usuarias y el servidor web.
La censura que afecta al protocolo HTTP es una táctica utilizada por los ISP, para impedir el acceso a sitios web específicos o para controlar la información que las personas pueden ver en estos sitios web.

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

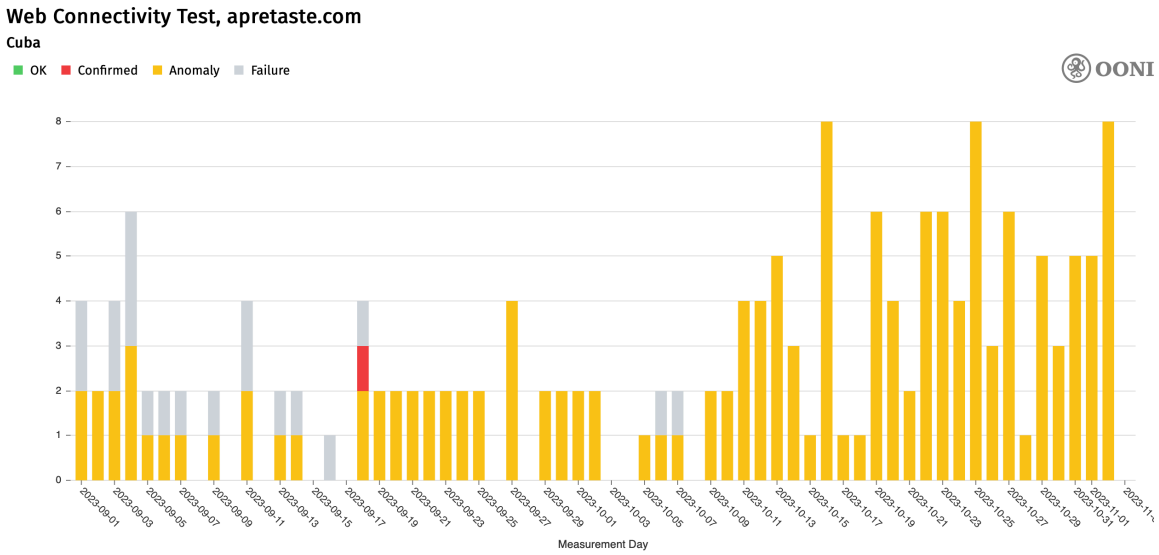


Imagen 2. Prueba de conectividad del dominio apretaste.com

Censura mediante tecnología DPI en Cuba

De los 67 sitios web identificados como bloqueados, se ha observado que 49 de ellos son afectados claramente por la tecnología DPI. Esto se ha confirmado a través de la identificación, en los resultados de las pruebas de OONI como también en las capturas de WireShark, del servidor con el identificante V2R2C00-IAE/1.0. Detalles adicionales sobre este hallazgo se encuentran disponibles en los informes #1 y #2 relativos al estado de la conectividad en Cuba.
La tecnología DPI permite ejercer un control y censura, al inspeccionar minuciosamente los paquetes de datos que circulan a través de la red. Este método de censura resulta en la capacidad de bloquear, manipular o limitar el acceso a sitios web específicos, lo que tiene un impacto significativo en la libertad de acceso a la información en internet.

En este gráfico podemos observar las mediciones realizadas en este trimestre a uno de los dominios que sufren censura mediante tecnología DPI, en este caso es el dominio proyectoinventario.org

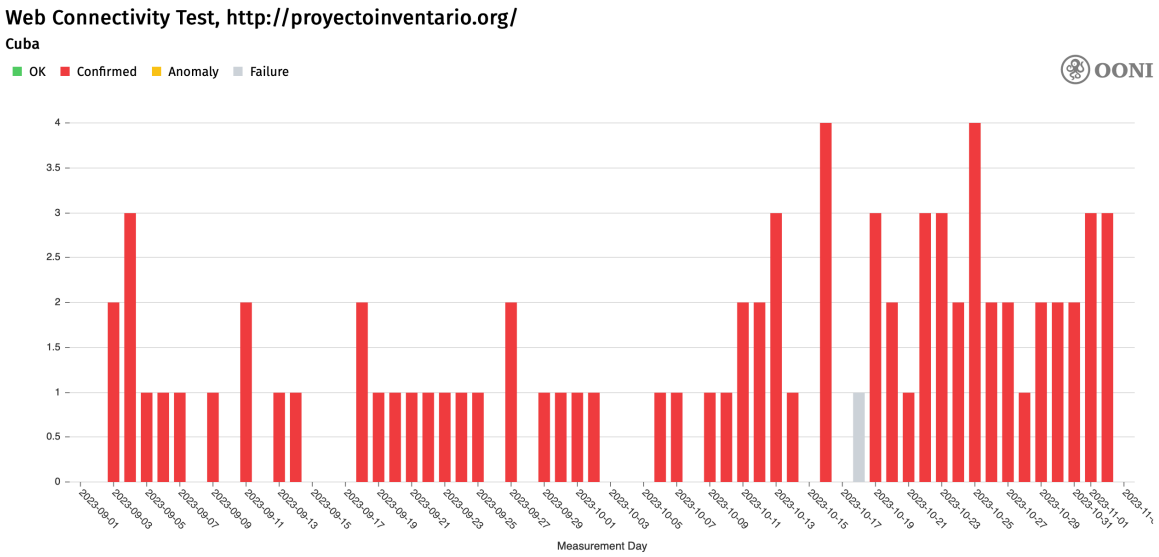


Imagen 3. Prueba de conectividad del dominio proyectoinventario.org

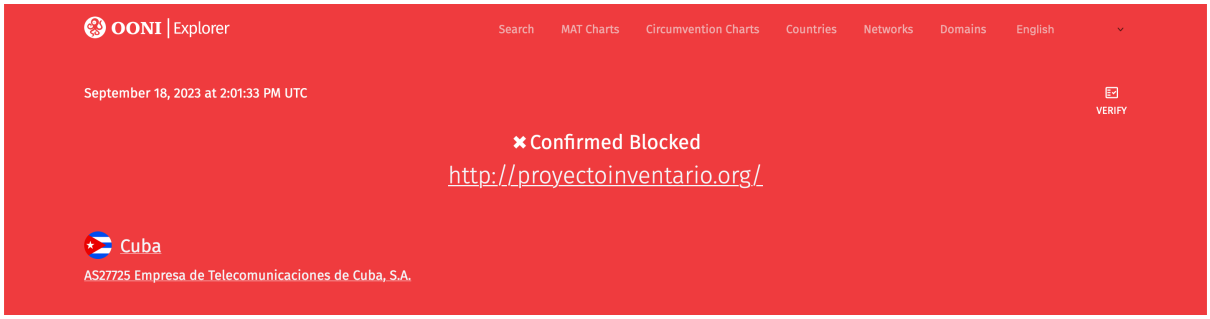


Imagen 4. Salida de OONI Explorer para prueba a proyectoinventario.org

Imagen 5. Encabezado HTTP que devuelven las peticiones del sitio proyectoinventario.org

En la prueba de OONI a este mismo sitio web apreciamos un "contenido" (body) totalmente vacío y el identificante del server en el "encabezado" (headers).

Mediciones fallidas

En el informe anterior, identificamos 12 dominios que, al solicitar su versión HTTPS, eran catalogados como mediciones fallidas por OONI, aunque en realidad estaban siendo censurados mediante tecnología DPI. Durante este trimestre, hemos agregado 20 dominios adicionales a esta lista, lo que suma un total de 32 dominios con mediciones fallidas en múltiples ocasiones.

Tabla 2. Dominios con mediciones fallidas

	Sitio web
1	cubasindical.org
2	damasdeblanco.com
3	anon.inf.tu-dresden.de
4	conexioncubana.net
5	miscelaneasdecuba.net
6	cubadata.com
7	cubademocraciayvida.org
8	solidaridadconcuba.com
9	freedomhouse.org
10	canf.org
11	cubacenter.org
12	cubafreepress.org
13	payolibre.com
14	proyectoinventario.org
15	rialta.org
16	somosmascuba.com
17	hermanos.org
18	somosmascuba.com
19	cubaenmiami.com
20	libertaddigital.com
21	cafefuerte.com
22	voanews.com
23	corriente.org

24	pscuba.org
25	sigloxxi.org
26	cubaxcuba.com
27	oas.org
28	agendacuba.org
29	juventudlac.org
30	cubalibredigital.com
31	martinoticias.com
32	directorio.org

Al analizar en detalle los resultados de OONI escritos en JSON observamos la misma línea informativa en la petición HTTPS de estos 32 dominios censurados, que nos informa de un problema en el handshake de TLS.

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

Imagen 6. Mensaje de error al realizar el handshake TLS

En el informe #2 tomamos de referencia el informe de OONI publicado en marzo de 2023, donde explican que los 40 sitios web estudiados, que daban este resultado, sufrían de censura.
Hemos analizado con WireShark las capturas de paquetes de tráfico a estos 32 dominios en su versión HTTPS, y hemos podido confirmar la utilización de tecnología DPI afectando el protocolo TLS.

El sitio web https://proyectoinventario.org/ es un ejemplo de esto como se muestra en el siguiente gráfico, las mediciones que se realizaron durante el periodo de estudio fueron catalogadas por OONI como “mediciones fallidas”.

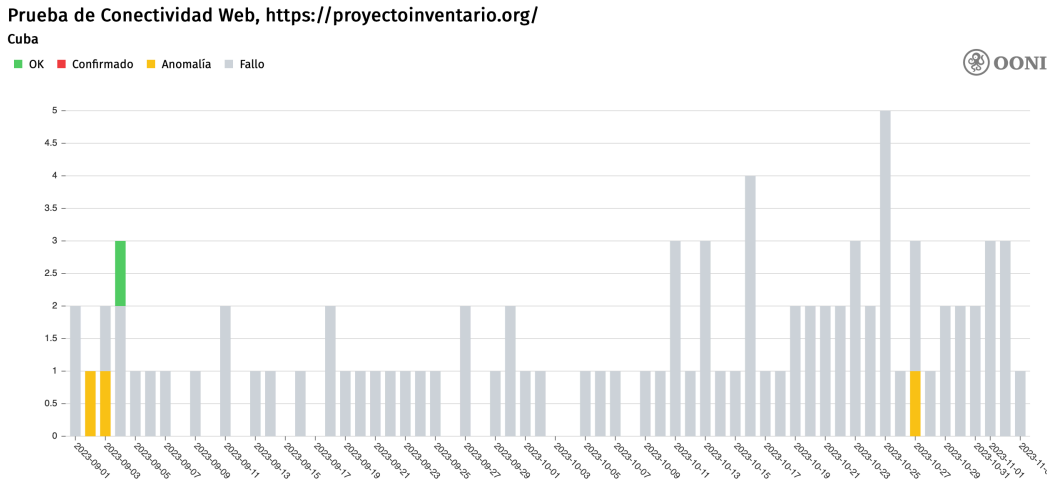
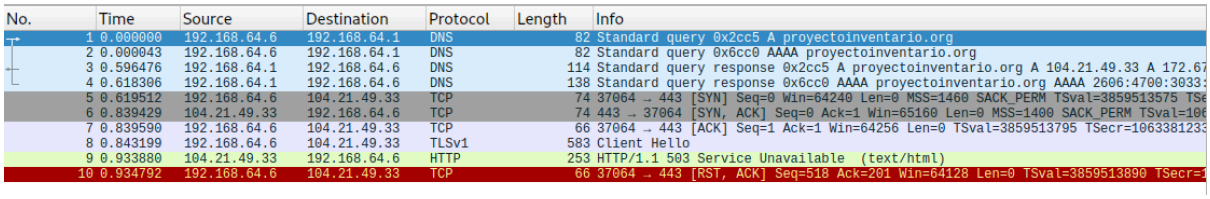


Imagen 7. Prueba de conectividad al sitio proyectoinventario.org333

. En la captura de WireShark al sitio web https://proyectoinventario.org/ observamos:

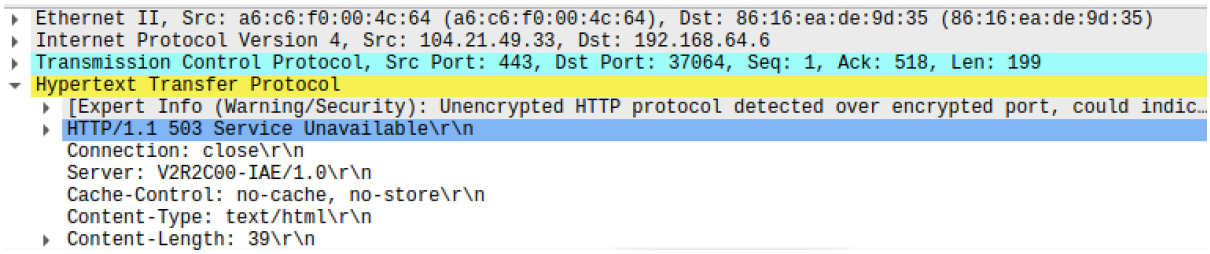


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.64.6	192.168.64.1	DNS	82	Standard query 0x2cc5 A proyectoinventario.org
2	0.000043	192.168.64.6	192.168.64.1	DNS	82	Standard query 0x6cc0 AAAA proyectoinventario.org
3	0.596476	192.168.64.1	192.168.64.6	DNS	114	Standard query response 0x2cc5 A proyectoinventario.org A 104.21.49.33 A 172.67
4	0.618306	192.168.64.1	192.168.64.6	DNS	138	Standard query response 0x6cc0 AAAA proyectoinventario.org AAAA 2606:4700:3033:
5	0.619512	192.168.64.6	104.21.49.33	TCP	74	37064 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3859513575 TSe
6	0.839429	104.21.49.33	192.168.64.6	TCP	74	443 → 37064 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1400 SACK_PERM TSval=106
7	0.839590	192.168.64.6	104.21.49.33	TCP	66	37064 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3859513795 TSecr=106338123
8	0.843199	192.168.64.6	104.21.49.33	TLSv1	583	Client Hello
9	0.933880	104.21.49.33	192.168.64.6	HTTP	253	HTTP/1.1 503 Service Unavailable (text/html)
10	0.934792	192.168.64.6	104.21.49.33	TCP	66	37064 → 443 [RST, ACK] Seq=518 Ack=201 Win=64128 Len=0 TSval=3859513890 TSecr=1

Imagen 8. Captura de Wireshark

1. En el paquete número 8 se sucede correctamente el primer intercambio del handshake de TLS (Client Hello),

2. No se da lugar el segundo intercambio del handshake de TLS, dado que es interferido por la máquina intermedia (DPI). Deducimos que esta máquina se hace pasar por el servidor de destino modificando la IP y respondiendo con el código de estado HTTP 503 (que nos indica que el servidor no está disponible temporalmente).
   Al revisar el paquete número 9 de la captura de WireShark vemos en los headers, el identificante del servidor: V2R2C00-IAE/1.0 (el cual esta asociado a la empresa china Huawei tal y como hemos visto en informes precedentes).



```
▸ Ethernet II, Src: a6:c6:f0:00:4c:64 (a6:c6:f0:00:4c:64), Dst: 86:16:ea:de:9d:35 (86:16:ea:de:9d:35)
▸ Internet Protocol Version 4, Src: 104.21.49.33, Dst: 192.168.64.6
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 37064, Seq: 1, Ack: 518, Len: 199
▾ Hypertext Transfer Protocol
  ▸ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indic…
  ▸ HTTP/1.1 503 Service Unavailable\r\n
    Connection: close\r\n
    Server: V2R2C00-IAE/1.0\r\n
    Cache-Control: no-cache, no-store\r\n
    Content-Type: text/html\r\n
  ▸ Content-Length: 39\r\n
```

Imagen 9. Detalle de respuesta HTTP444 al acceder a proyectoinventario.org

Lo mismo pasa en las peticiones HTTPS a los otros 31 dominios que OONI cataloga como mediciones fallidas en reiteradas ocasiones, donde observamos siempre el mismo identificante del servidor.

Esta situación pone de manifiesto la presencia de una máquina intermedia que interfiere en la comunicación al enviar un paquete de HTTP cuando se esta iniciando un handshake de TLS. Lo habitual en capturas sanas de WireShark es ver el handshake de TLS y seguidamente paquetes de TLS llamados “Application Data”. Pero en medio del handshake de TLS no se envían ni reciben paquetes HTTP.

En todas las capturas realizadas nunca hemos visto el código de estado HTTP que corresponde a bloqueos por motivos legales el 451., Por lo tanto, el gobierno está tratando de desviarnos para que creamos que el problema reside en el servidor de destino, cuando en realidad están bloqueando dicho contenido sin asumirlo, e infringiendo nuestros derechos de acceso a la información en internet.

Bloqueo en Cuba a la herramienta de elusión de censura Tor

En el transcurso de los meses septiembre, octubre y noviembre hemos llevado a cabo una serie de mediciones, utilizando la prueba “evasión” de OONI Probe para evaluar la accesibilidad a la red de Tor en Cuba. Los resultados obtenidos demuestran que el acceso a Tor está bloqueado en el país.

¿Qué es Tor?

Tor, cuyo nombre proviene de "The Onion Router" (el enrutador cebolla), hace referencia a la estructura de capas de seguridad que utiliza Tor para proporcionar anonimato en internet. La metáfora de la cebolla refleja la idea de que cada capa de seguridad añadida por Tor representa una capa adicional de anonimato para las personas que utilizan la red de Tor para navegar en internet. Al igual que las capas de una cebolla Tor encapsula nuestras tráfico con varias capas. De forma que cada nodo en el camino solo conoce la capa anterior y la siguiente en el enrutamiento, pero no puede ver todo el trayecto ni la identidad de las usuarias. Tor constituye una herramienta crucial para eludir la censura y preservar el anonimato en la navegación por Internet.
La red de Tor se inicia desde el momento en que una usuaria utiliza el Tor Browser, este navegador cliente de Tor se conectará a través de un proxy SOCKS (protocolo que permite la comunicación segura entre un cliente y un servidor a través de un proxy)

El funcionamiento de Tor se basa en una red anónima que utiliza relays o retransmisores, conectados entre ellos, tejiendo así una gran red de relays interconectados. La conexión a la red de Tor se establece creando un circuito de 3 relays desde el navegador de Tor del ordenador cliente al servidor de destino.

Las direcciones IP públicas de estos relays están disponibles en listas públicas, por lo que las ISP pueden fácilmente incluirlas en sus listas de direcciones IP bloqueadas o denegqadas (“Denylist IP addresses”). Para incrementar la seguridad y evitar posibles bloqueos, las usuarias tienen la opción de conectarse a bridges o puentes en lugar de los relays por defecto.
Los bridges son relays pero que sus direcciones IP no se encuentran en listas públicas, por lo que añade un poco de dificultad para las ISP que censuran por direcciones IP denegadas.

Dado que las ISP pueden analizar en profundidad el tráfico de paquetes (mediante tecnología DPI) estas pueden saber, analizando el tráfico, si las clientes se conectan a la red de Tor mediante la utilización de bridges. Es por esto que Tor ha desarrollado diferentes herramientas de elusión de censura conocidas como “Pluggable Transport” que añaden

capas de ocultación. Actualmente hay 4 en funcionamiento (obfs4, meek, Snowflake y WebTunnel) pero se han desarrollado otras.

Por ejemplo Snowflake esconde la conexión Tor en una conexión al protocolo WebRTC (protocolo utilizado en video streaming). Primero, es necesario que personas voluntarias, sin restricción a la red de Tor, se instalen el plugin Snowflake en su navegador. De esta manera, se creará una conexión de protocolo WebRTC entre el ordenador de la persona que sufre restricciones y el ordenador de la persona voluntaria. Permitiendo así esconder a la ISP restrictora el tráfico de la red de Tor dentro de una conexión WebRTC, como si estuvieran haciendo una videollamada. Las voluntarias actúan como relays temporales, facilitando el acceso a la red Tor de aquellos que enfrentan restricciones de censura.

Test de OONI

OONI realiza la prueba de accesibilidad a 4 servicios que permiten el funcionamiento de Tor . Son los siguientes:

1. El puerto de la autoridad de directorio, utilizado por los relays de Tor y nombrado en las pruebas de OONI como: *dir_port.* A través de este puerto los relays proporcionan información necesaria sobre la red facilitando así el enrutamiento, como la lista de relays disponibles.
2. El servicio ofrecido por el puerto Onion Route utilizado por los bridges de Tor y nombrado en las pruebas de OONI como: *or_port.*
3. El puerto en el que los servidores de la red Tor ofrecen el servicio de directorio y nombrado en las pruebas de OONI como: *or_port_dirauth.* Los clientes Tor se conectan a las autoridades de directorio a través de este puerto para obtener detalles actualizados sobre la red, lo que contribuye a un enrutamiento seguro y anónimo de su tráfico a través de la red Tor.
4. El equipo de Tor también ofrece un protocolo llamado obfs4 nombrado en las pruebas de OONI como: *obfs4*. Es un protocolo de seguridad que añade una capa de ocultación, utiliza llaves de cifrado más robustas que el protocolo de seguridad TLS.

Como veremos a continuación, en las pruebas realizadas durante este trimestre se observó un bloqueo a muchos de los nodos que permiten el funcionamiento de la red de Tor, afectando de diferentes formas a algunos de los 4 servicios nombrados.

Test a los retransmisores de Tor

Al examinar específicamente el resultado de este servicio, en la prueba de OONI realizada el día 25 de septiembre, se puede observar que el puerto de autoridad de directorio tiene disponibles 10 servidores, de los cuales solo uno se muestra accesible.

```
"dir_port_total" : int 10
"dir_port_accessible" : int 1
```

Test a los puentes de Tor

Para el servicio “OR port” no se muestra disponible ningún nodo para realizar un puente a través de él, como lo muestra la prueba de OONI realizada el 15 de noviembre.

```
"or_port_total" : int 0
"or_port_accessible" : int 0
```

Test a los clientes de Tor

Al examinar los test de Tor de los meses septiembre, octubre y noviembre en detalle, observamos que en múltiples mediciones se presentó una notación "0/10 OK" que muestran que 0 nodos de 10 son accesibles en referencia a las Autoridades del Directorio Tor.

```
"or_port_dirauth_total" : int 10
"or_port_dirauth_accessible" : int 0
```

Test al protocolo obfs4

Para el protocolo obfs4 se muestra una mejor situación aunque también sufre de censura. En el test de OONI efectuado el 1 de octubre de los 15 nodos disponibles, 11 se encuentran accesibles y 4 de ellos son inaccesibles. Lo que significa que pueden ser alcanzados y utilizados para enrutar el tráfico de forma exitosa. Sin embargo, también se señala que cuatro de estos nodos son inaccesibles, lo que indica que enfrentan algún tipo de restricción o bloqueo, posiblemente como resultado de intentos de censura

```
"obfs4_total" : int 15
"obfs4_accessible" : int 11
```

Resultados escritos en JSON de las mediciones de OONI

En el resultado de OONI al test de Tor el 25 de septiembre vemos que la conexión al relay con dirección IP 128.31.0.39 y puerto 9101 ha dado como mensaje de error “conexión rechazada” cuando trataba conectarse al puerto de la Autoridad del Directorio del servicio Onion Router. Más específicamente nos dice que se rechaza la conexión durante el handshake de TCP.

```
"targets" : { 35 items
  "128.31.0.39:9101" : { 11 items
    "agent" : string "redirect"
    "failure" : string "connection_refused"
    "network_events" : NULL
    "queries" : NULL
    "requests" : NULL
    "summary" : {...} 1 item
    "target_address" : string "128.31.0.39:9101"
    "target_name" : string "moria1"
    "target_protocol" : string "or_port_dirauth"
    "tcp_connect" : [ 1 item
      0 : { 6 items
        "ip" : string "128.31.0.39"
        "port" : int 9101
        "t" : float 62.598027379
        "status" : {...} 3 items
        "started" : float 62.481662648
        "oddity" : string "tcp.connect.refused"
```

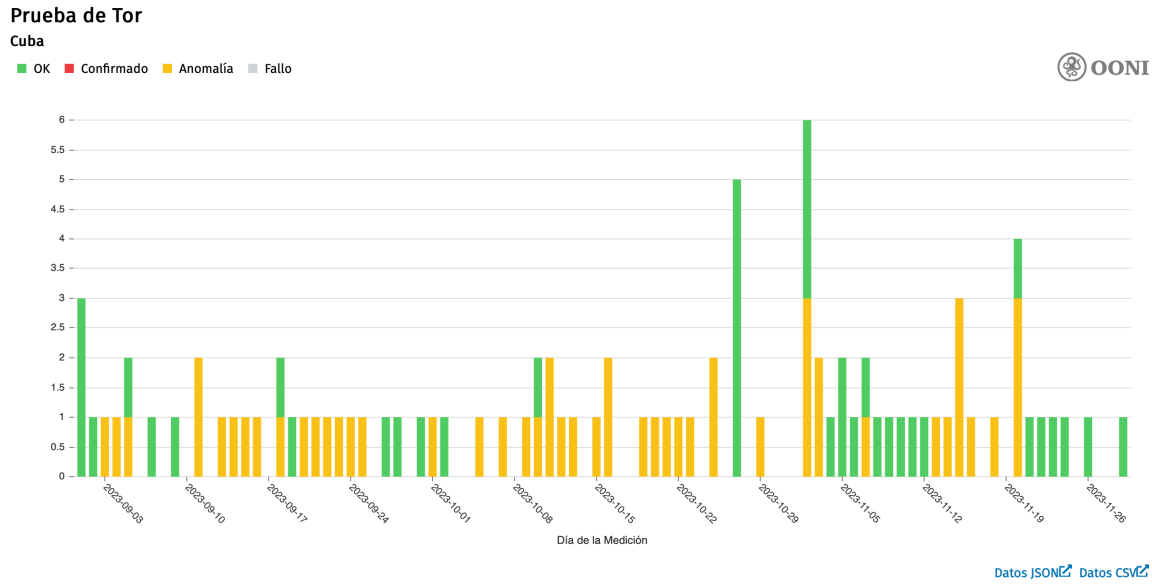

Y en este [resultado de OONI] escrito en JSON vemos que:
La conexión al nodo con la dirección IP 131.188.40.189 y puerto 443 resultó en un mensaje de error que indica un problema de tiempo de espera. Esto significa que la solicitud para conectarse al puerto de la Autoridad del Directorio del servicio Onion Router no pudo completarse dentro del período de tiempo establecido.


```
"targets" : { 35 items
  "128.31.0.39:9101" : {...} 11 items
  "128.31.0.39:9131" : {...} 11 items
  "131.188.40.189:443" : { 11 items
    "agent" : string "redirect"
    "failure" : string "generic_timeout_error"
    "network_events" : NULL
    "queries" : NULL
    "requests" : NULL
    "summary" : {...} 1 item
    "target_address" : string "131.188.40.189:443"
    "target_name" : string "gabelmoo"
    "target_protocol" : string "or_port_dirauth"
    "tcp_connect" : [...] 1 item
    "tls_handshakes" : NULL
```


En la [prueba de OONI del 25 de septiembre] hemos visto en estos dos resultados correspondientes a los nodos “moria1” y “gabelmoo” el primero nos da “connection_refused” y en el segundo obtenemos un “generic_timeout_error”.Los demás nodos que utilizan este servicio que analizamos (“or_port_dirauth”), Faravahar, maatuska, dannenberg, longclaw, bastet y dizum, coinciden con el nodo gabelmooy dan “generic_timeout_error”.

Resultado trimestral del test de Tor

La siguiente gráfica muestra los resultados de OONI a los test de Tor durante el trimestre de estudio. Se encontraron anomalías en 52 De las 88 Mediciones realizadas entre el 1 de septiembre y el 30 de octubre.



Conclusiones

Este informe revela preocupantes evidencias de censura por parte del gobierno cubano, indicando un significativo bloqueo de acceso a la información.

De los 240 dominios monitoreados, se confirmó que 68 estaban bloqueados, y de estos, 49 fueron bloqueados mediante tecnología de inspección profunda de paquetes (DPI), tecnología de un alto nivel de control.

También se confirmó que 32 de los dominios de los 240 monitoreados, inicialmente catalogados como mediciones fallidas por OONI, en realidad están siendo censurados mediante tecnología DPI.

Por último, el bloqueo de Tor en Cuba, monitorizado mediante las herramientas de OONI, agrega otra capa a la preocupación. Múltiples mediciones revelaron anomalías consistentes con bloqueos por parte del gobierno cubano a la herramienta de elusión de censura. Este bloqueo no solo representa una restricción al acceso a la información, sino que también añade una barrera de impedimiento a la utilización de herramientas que permiten navegar en internet de forma confidencial.

En resumen, este informe demuestra que la censura en Cuba se está llevando a cabo de manera extensa y sofisticada, afectando tanto a dominios específicos como a tecnologías diseñadas para preservar la privacidad y la libertad en línea. Estos hallazgos resaltan la

importancia de abogar por la libre circulación de información y la protección de los derechos digitales en la búsqueda de un servicio de Internet más libre y accesible en Cuba.

Trabajos futuros

Nuestro equipo tiene la intención de continuar monitoreando los dominios evaluados durante este trimestre, así como identificar y analizar otros dominios de posible interés. El objetivo principal es determinar la persistencia de bloqueos en los dominios previamente monitoreados y descubrir posibles nuevos casos de censura en la red.

En relación a Tor, se busca realizar una investigación más exhaustiva para continuar dándole seguimiento a la censura de Tor en Cuba. Este trabajo implica coordinar esfuerzos con los desarrolladores de Tor, Snowflake y OONI Probe. La colaboración con estas organizaciones permitirá obtener una comprensión más completa de las tácticas de censura utilizadas.