Informe # 4 sobre la salud del Internet en Cuba

Autoría: Diktyon

Hallazgos clave

Durante el monitoreo en los meses de enero, febrero y marzo de 2024, identificamos que 61 dominios, en una lista de 240, permanecen censurados desde Cuba. En su mayoría se trata de sitios sobre noticias y derechos humanos.

Para este estudio utilizamos 217 sitios web de la lista de CitizenLab para Cuba y agregamos el resto mediante la evaluación de nuestro equipo de Diktyon debido a su alta probabilidad de ser censurados en la isla.

- 46 sitios web permanecen bloqueados utilizando tecnología de Inspección Profunda de Paquetes (DPI por sus siglas en inglés).
- Al solicitar las versiones HTTPS de 27 dominios, OONI los cataloga como *mediciones fallidas* cuando en realidad pudimos comprobar que se trata de censura.

Durante los dos primeros meses de 2024, Cuba mantuvo velocidades de Internet extremadamente lentas por medio de datos móviles y banda ancha fija.

- Se observó que las velocidades de Internet en Cuba estuvieron notablemente por debajo de los estándares ideales necesarios para un acceso eficaz a la red de redes.

En este informe, igualmente empleamos 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. Además, realizamos capturas de paquetes de tráfico con la herramienta WireShark para examinar los protocolos en detalle y utilizamos la herramienta Speed Test de Ookla para evaluar el rendimiento de la conexión a Internet.

Introducción y objetivos

En este informe exploramos la censura de Internet en Cuba durante los primeros tres meses de 2024, actualizando el listado de sitios bloqueados en el informe # 3 sobre la salud de Internet en Cuba publicado en diciembre de 2023.

Nos enfocamos en entender la censura mediante tecnología DPI y analizar las “mediciones fallidas” (catalogadas así por OONI) de los sitios webs restringidos. Además, abordamos el bloqueo de Tor, la popular herramienta de elusión de censura, examinando las diferentes pruebas que ofrece OONI Probe para Tor.

Por otra parte, incluimos un análisis sobre la velocidad de Internet en Cuba. Nos apoyamos en la herramienta *Speed Test* de *Ookla* para evaluar el rendimiento de la conexión a Internet.

Finalmente, prestamos especial atención a la potencial censura de la aplicación de mensajería Signal, teniendo en cuenta las mediciones inusuales anteriores realizadas por OONI.

Signal

El surgimiento de las anomalías sobre Signal, tuvo como raíz las protestas del 11 de julio del 2021, donde se aplicó un apagón de Internet en toda la isla.

En estos últimos meses del 2024 y finales del 2023 ha existido un aumento de protestas en la isla lo que ha llevado a un aumento de comportamientos sospechosos sobre esta aplicación de mensajería. Por eso, en este informe se incluye un apartado donde se profundiza en el estudio de Signal y un reporte las mediciones realizadas con OONI.

Nuestro objetivo es proporcionar una comprensión profunda de la salud del Internet en Cuba durante el primer trimestre de 2024.

Listado de dominios censurados:

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

##	Dominio	Categoría	HTTP (Enero)	HTTPS (Enero)	HTTP (Febrero)	HTTPS (Febrero)	HTTP (Marzo)	HTTPS (Marzo)
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	directorio.org	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
7	cubadata.com	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo de TCP/IP	Bloqueo de TCP/IP
8	idealpress.com	Religión	Censura por DPI	Bloqueo de TCP/IP	Censura por DPI	Bloqueo de TCP/IP	Censura por DPI	Bloqueo de TCP/IP
9	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
10	cubademocraciayvida.org	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
11	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
12	solidaridadconcuba.com	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
13	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	Bloqueo de TCP/IP
14	freedomhouse.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida

15	14ymedio.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
16	cibercuba.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
17	cubanet.org	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
18	diariodecuba.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
19	cubaencuentro.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
20	apretaste.com	Motores de búsqueda	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP
21	change.org	Activismo	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
22	911truth.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
23	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
24	canf.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
25	cubacenter.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
26	cubafreepress.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
27	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
28	secure.avaaz.org	Activismo	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
29	payolibre.com	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida
30	periodicocubano.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP
31	schwarzreport.org	Religión anti-comunista	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP
32	univision.com	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Censura por DPI	Fallida

33	asere.com	Sitios de noticias	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo por HTTP	Bloqueo por HTTP
34	cubalex.org	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP
35	cadal.org	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP
36	cubanosporelmundo.com	Sitios de noticias	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo por HTTP	Bloqueo de HTTP
37	cubadecide.org	Sitios críticos con el gobierno	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo por TCP/IP	Bloqueo por TCP/IP
38	proyectoinventario.org	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
39	rialta.org	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
40	demoamlat.com	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP
41	observacuba.org	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP - Bloqueo por
42	adncuba.com	Sitios de noticias	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo HTTP
43	revistaelestornudo.com	Cultura	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP
44	hermanos.org	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Fallida
45	somosmascuba.com	Sitios de noticias	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
46	cubaenmiami.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Bloqueo por HTTP
47	unpacu.org	Sitios críticos con el gobierno	Censura por DPI	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP
48	libertaddigital.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida

49	cafefuerte.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
50	icj.org	Sitios de Derechos Humanos	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo TCP/IP	Bloqueo TCP/IP
51	cubanartnewsarchive.org	Cultura	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo de TCP/IP	Bloqueo TCP/IP	Bloqueo TCP/IP
52	voanews.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
53	corriente.org	Activismo político	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
54	represorescubanos.com	Sitios de Derechos Humanos	Censura por DPI	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo HTTP
55	cubaxcuba.com	Sitios críticos con el gobierno	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
56	oas.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
57*	agendacuba.org	Turismo	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
58	juventudlac.org	Sitios de Derechos Humanos	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
59	martinoticias.com	Sitios de noticia	Censura por DPI	Fallida	Censura por DPI	Fallida	Bloqueo por DPI	Fallida
60	americateve.com	Sitios de noticia	Bloqueo de	Bloqueo de	Bloqueo de	Bloqueo de	Bloqueo por	Bloqueo por
61	cuballama.com	Sitios de noticia	Censura por DPI	Bloqueo de HTTP	Censura por DPI	Bloqueo de HTTP	Bloqueo por DPI	Bloqueo por HTTP

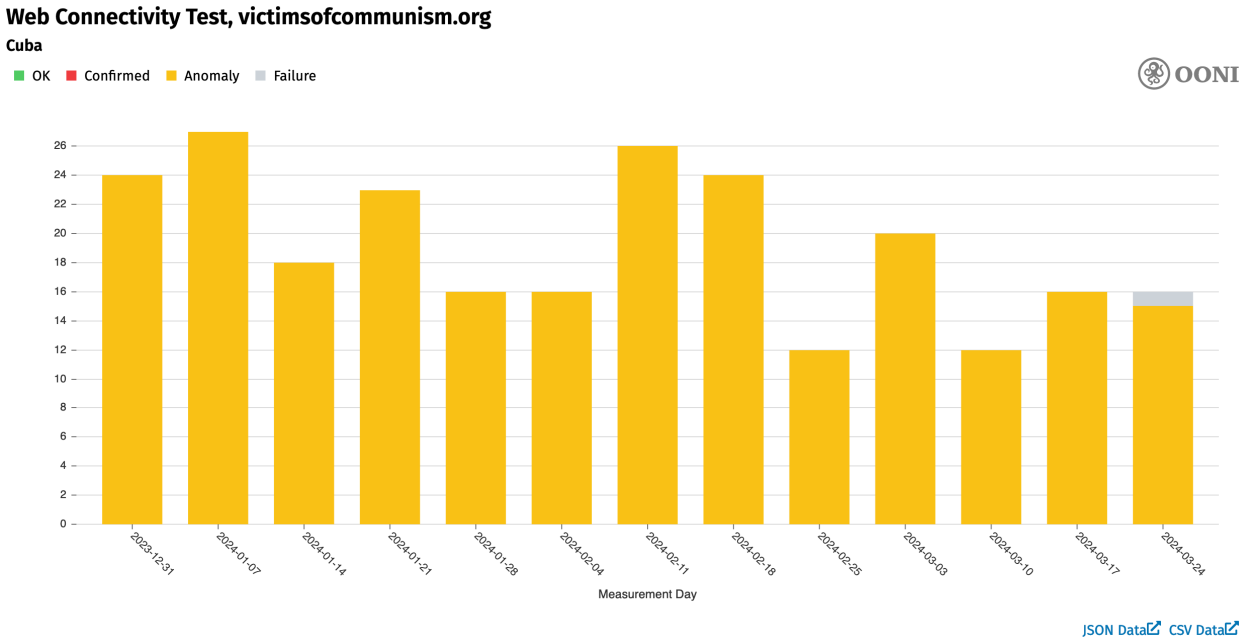
Observación: Aunque agendacuba.org (sitio 57*) es actualmente reconocido como un portal turístico y no ejerce influencia en los ámbitos social, cultural o económico de Cuba aparte del turismo, en octubre de 2005 su contenido tenía connotaciones políticas, lo que posiblemente provocó su bloqueo. Este bloqueo ha persistido hasta la fecha actual, a pesar de que su contenido haya sido alterado.

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 las 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.

Este gráfico ilustra un ejemplo de un dominio que experimentó anomalías en el protocolo TCP durante el período de estudio, lo que resultó en su censura. En este caso particular, el dominio afectado es *victimsofcommunism.org*.



Tal y como se puede apreciar, el color amarillo es el otorgado para las anomalías. Teniendo en el eje horizontal las fechas comprendidas entre el 1 de enero y el 31 de marzo. Y en el eje vertical la cantidad de mediciones diarias realizadas. De esta forma, podemos visualizar que prácticamente todas las mediciones realizadas en este periodo son anómalas, con excepción del 24 de marzo en el que se aprecia una sola medición fallida.

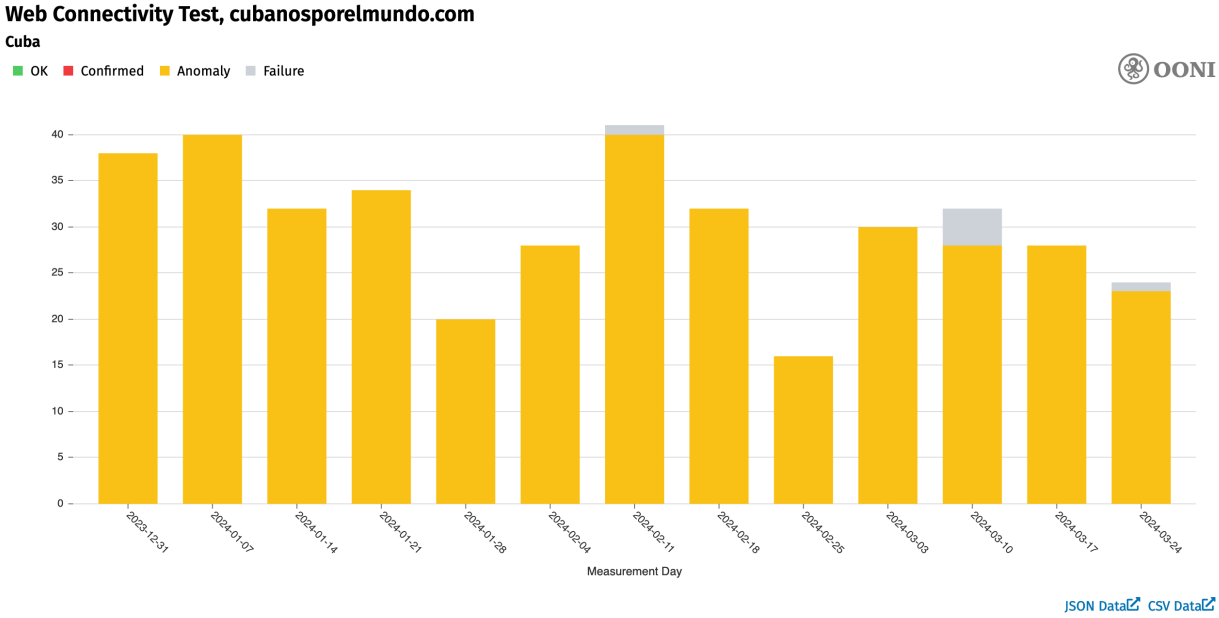
Censura que afecta al protocolo HTTP

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, protocolo TLS que veremos a continuación). 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 las ISP, para impedir el acceso a sitios web específicos o para controlar la información que las personas pueden ver en estos sitios web.

En este gráfico, se presentan las mediciones realizadas al dominio *cubanosporlemundo.com* durante el periodo de estudio de este informe.



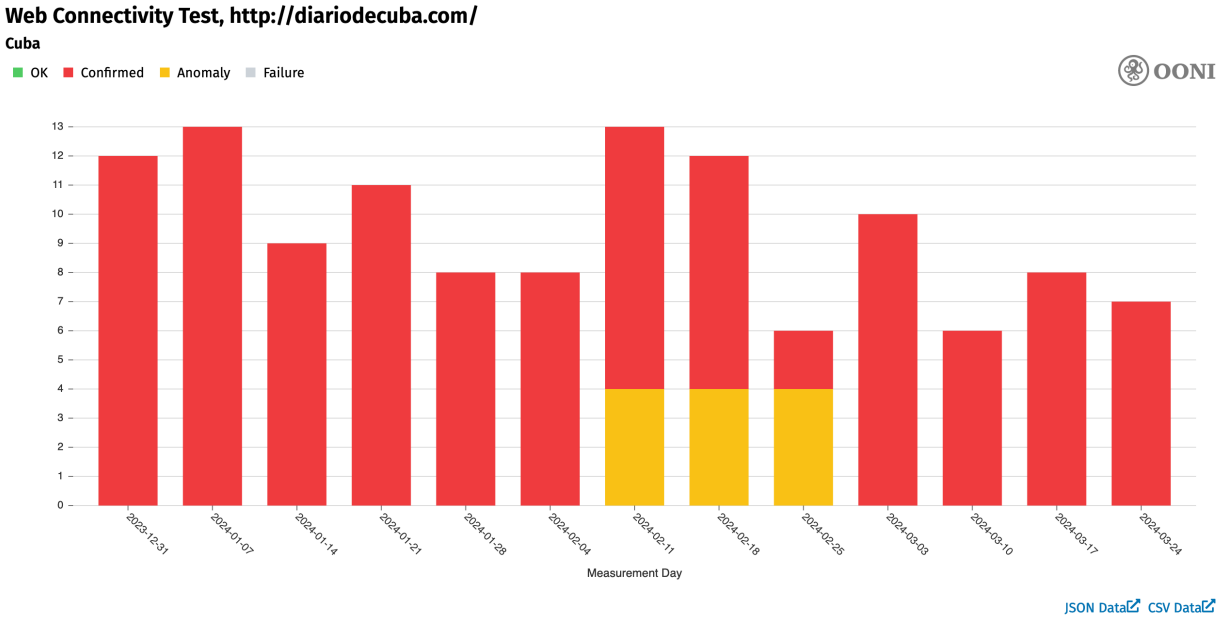
Tal y como se puede apreciar, el color amarillo es el otorgado para las anomalías. Teniendo en el eje horizontal las fechas comprendidas entre el 1 de enero y el 31 de marzo. Y en el eje vertical la cantidad de mediciones diarias realizadas.
De esta forma, podemos visualizar que prácticamente todas las mediciones realizadas en este periodo son anómalas, con excepción del 11 de febrero y 24 de marzo en los que se aprecia una sola medición fallida (en color gris) y el 10 de marzo en el cual se registran 4 mediciones fallidas.

Censura mediante tecnología DPI en Cuba

Se ha identificado que de los 61 sitios web bloqueados, 46 de ellos están claramente censurados mediante tecnología DPI, dato que se ha podido corroborara través de los resultados de las pruebas de OONI y las capturas de WireShark, que revelan la presencia del equipo con el identificador V2R2C00-IAE/1.0. Equipo de la empresa china Huawei llamado eSight, tal y como hemos detallado en informes precedentes: Censura y Restricciones de Internet en Cuba: Resumen de 9 meses de monitoreo, publicado en diciembre de 2023.

La tecnología DPI permite un control y censura detallados al procesar minuciosamente los datos de los paquetes de red. Esta forma de censura posibilita manipular o restringir el acceso a sitios web específicos. Para profundizar en este tipo de censura en Cuba se pueden consultar nuestros informes pasados (#1, #2 y # 3). .

El siguiente gráfico presenta las mediciones efectuadas durante enero en uno de los dominios afectados por la censura mediante la tecnología DPI. En este caso, se trata del dominio diariodecuba.com.



Tal y como se puede apreciar, el color rojo es el otorgado para los bloqueos confirmados y el anaranjado se refiere a las anomalías. Teniendo en el eje horizontal las fechas comprendidas entre el 1 de enero y el 31 de marzo. Y en el eje vertical la cantidad de mediciones diarias realizadas. De esta forma, podemos visualizar que todas las mediciones realizadas en este periodo son bloqueos confirmados.

En la prueba de OONI a este sitio web apreciamos un “contenido” (body) totalmente vacío y el identificante V2R2C00-IAE/1.0 del *server* en el “encabezado” (headers).

1 de enero de 2024, 4:47:54 UTC

VERIFICAR

✖ Bloqueo confirmado

http://diariodecuba.com/

Cuba

AS27725 Empresa de Telecomunicaciones de Cuba, S.A.

Solicitud de HTTP

URL

```
GET http://diariodecuba.com/
```

Encabezados de respuesta

```
Cache-Control: no-cache, no-store
Content-Length: 39
Content-Type: text/html
Server: V2R2C00-IAE/1.0
```

Cuerpo de la Respuesta.

```
<html><head></head><body></body></html>
```

Mediciones fallidas

En el informe anterior identificamos 32 dominios que al solicitar su versión HTTP eran catalogados por OONI como “mediciones fallidas”. Durante este trimestre hemos identificado un total de 27 dominios con mediciones fallidas en múltiples ocasiones.

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

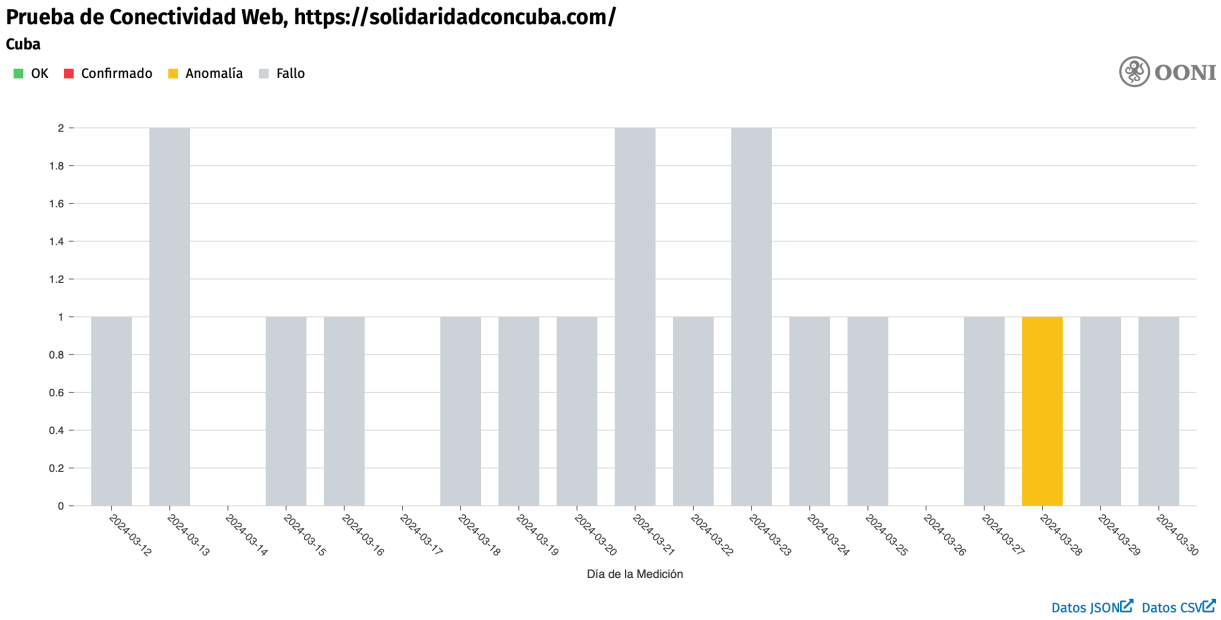
Al analizar detalladamente los resultados de OONI, escritos en formato JSON, notamos un patrón consistente en las solicitudes HTTPS para estos 27 dominios censurados. Estas solicitudes indican un problema durante el handshake de TLS.

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

Este resultado también se reflejó en el [informe de OONI publicado en marzo de 2023](), en el cual se explica que este problema de handshake de TLS se aparecía en 40 sitios web que sufrían de censura. Esta referencia la hemos nombrado en nuestros informes precedentes ([#2](), [#3]()) publicados en 2023.

Al examinar las capturas de tráfico de paquetes utilizando WireShark en relación a estos 27 dominios en su versión HTTPS, hemos verificado el uso de tecnología DPI que afecta el protocolo TLS.

El sitio web *https://solidaridadconcuba/* ejemplifica esto, como se ilustra en el siguiente [gráfico]().

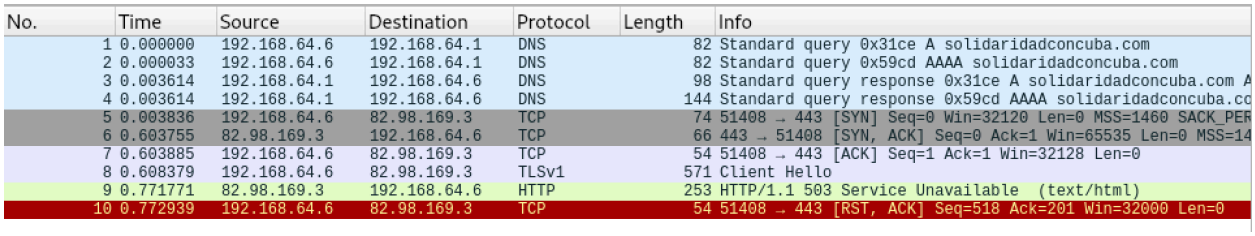


Tal y como se puede apreciar, el color gris es el otorgado para los fallos (mediciones fallidas). Teniendo en el eje horizontal las fechas comprendidas entre el 1 de enero y el 31 de marzo. Y en el eje vertical la cantidad de mediciones diarias realizadas. De esta forma, podemos visualizar que prácticamente todas las mediciones realizadas en este periodo son mediciones fallidas, excepto el día 19 de febrero con anomalías (en amarillo) y el 27 de febrero sin ningún bloqueo (en verde).

En la captura de WireShark al sitio web https://solidaridadconcuba.com/ podemos observar:

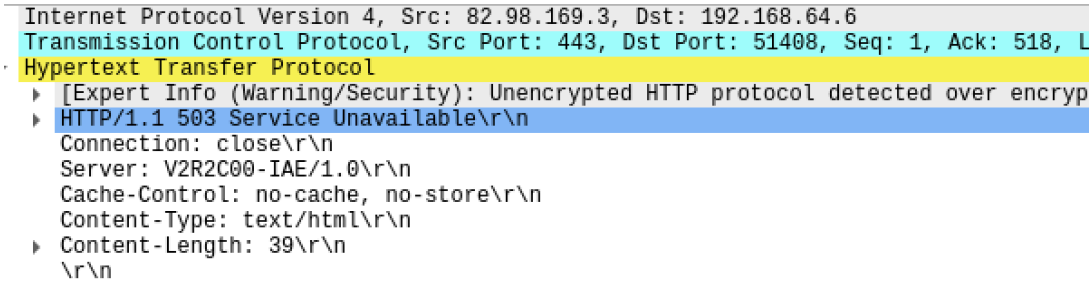
Que en el paquete número 8, el primer intercambio del handshake de TLS (Client Hello) ocurre correctamente.
Sin embargo, en el segundo intercambio del handshake de TLS, esta absente en esta captura, podemos suponer que no se completa debido a la interferencia de una máquina intermedia (DPI).

Se deduce que el equipo de DPI se hace pasar por el servidor de destino al modificar la IP y responder con el código de estado HTTP 503, indicando que el servidor no está disponible temporalmente, tal y como podemos apreciar en el paquete 9.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.64.6	192.168.64.1	DNS	82	Standard query 0x31ce A solidaridadconcuba.com
2	0.000033	192.168.64.6	192.168.64.1	DNS	82	Standard query 0x59cd AAAA solidaridadconcuba.com
3	0.003614	192.168.64.1	192.168.64.6	DNS	98	Standard query response 0x31ce A solidaridadconcuba.com A
4	0.003614	192.168.64.1	192.168.64.6	DNS	144	Standard query response 0x59cd AAAA solidaridadconcuba.co
5	0.003836	192.168.64.6	82.98.169.3	TCP	74	51408 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PER
6	0.603755	82.98.169.3	192.168.64.6	TCP	66	443 → 51408 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
7	0.603885	192.168.64.6	82.98.169.3	TCP	54	51408 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0
8	0.608379	192.168.64.6	82.98.169.3	TLSv1	571	Client Hello
9	0.771771	82.98.169.3	192.168.64.6	HTTP	253	HTTP/1.1 503 Service Unavailable (text/html)
10	0.772939	192.168.64.6	82.98.169.3	TCP	54	51408 → 443 [RST, ACK] Seq=518 Ack=201 Win=32000 Len=0

Al examinar el paquete número 9 de la captura de WireShark, se observa en los headers el identificador del equipo “servidor: V2R2C00-IAE/1.0”.



```
Internet Protocol Version 4, Src: 82.98.169.3, Dst: 192.168.64.6
Transmission Control Protocol, Src Port: 443, Dst Port: 51408, Seq: 1, Ack: 518, L
Hypertext Transfer Protocol
  [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encryp
  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
  \r\n
```

En las solicitudes HTTPS a los otros 27 dominios, que OONI clasifica como *mediciones fallidas* en múltiples ocasiones, también observamos el mismo identificador.

Este fenómeno es consistente con lo que mencionamos en el informe anterior (#3) y sigue ocurriendo en nuestras observaciones actuales. A pesar de nuestra búsqueda exhaustiva, nunca hemos detectado el código de estado HTTP 451, código específico para indicar bloqueos por motivos legales.
En cambio, encontramos que el gobierno está empleando tácticas haciendo parecer que el problema radica en el servidor de destino. Sin embargo, nuestros análisis indican claramente que están bloqueando el contenido sin admitirlo explícitamente.

Censura a la aplicación de mensajería Signal en Cuba

Signal es una aplicación de mensajería gratuita y de código abierto desarrollada por la organización sin fines de lucro Signal Foundation, sucesora de Open Whisper Systems. Ofrece llamadas de voz cifradas y mensajes instantáneos, destacando por su enfoque en la seguridad.

Entre el 1 de abril de 2021 y el 15 de septiembre de 2021, OONI llevó a cabo un estudio para evaluar posibles bloqueos de la aplicación Signal en varios países, incluyendo Cuba. En el caso específico de Cuba, la mayoría de las pruebas se realizaron a partir de julio del 2021, posiblemente en respuesta a bloqueos previos de redes sociales durante protestas masivas. Dentro de los análisis realizados por OONI sobre los países en los que existe censura de la aplicación Signal, se detectó que dentro de estos se encuentra Cuba.

Signal fue bloqueada temporalmente en Cuba a mediados de **julio del 2021**, coincidiendo con un período de intensas protestas masivas contra el gobierno de la isla.
Específicamente desde el 12 de julio del 2021 hubo un aumento considerable de mediciones anómalas de Signal desde la isla, mencionar también afectaciones a las redes sociales de WhatsApp, Telegram, Facebook y TikTok.

Durante las mediciones realizadas en este período sobre Signal, se pudo identificar que el protocolo de TLS (Seguridad de la Capa de Transporte) tuvo fallos continuos con los servicios de Signal. Lo que es señal probable, como explica OONI en su informe, que sea uso de tecnología DPI (Inspección a fondo de los paquetes) sobre el campo SNI (Indicación del nombre del servidor) del protocolo TLS. Aunque todavía no se a podido asegurar con total certeza.

La prueba de OONI para Signal está diseñada para evaluar la accesibilidad de la aplicación de mensajería Signal dentro de una red específica. Esta prueba verifica la capacidad de establecer una conexión TLS, validando el certificado TLS con el certificado raíz personalizado de *Signal CA* (Autoridad Certificadora), y envía una solicitud *HTTP GET* a los servidores *backend* de Signal desde la perspectiva de la persona usuaria de Signal.
Si la prueba logra realizar con éxito la solicitud HTTPS a los servers finales de Signal, se considera que la aplicación es accesible en la red probada.
Sin embargo, si las conexiones a cualquiera de los servidores finales de la señal fallan, la medición se etiqueta como "anómala", indicando que Signal podría ser inaccesible o bloqueada en esa red específica.

En este último trimestre se ha venido monitoreando Signal y a partir de la investigación realizada se puede ver que desde finales de año del 2023 se ha visto un aumento de mediciones anómalas tal y como podemos apreciar en el siguiente gráfico.

Tal y como se puede apreciar, el color verde es el otorgado para las pruebas carentes de bloqueos, el color amarillo para las pruebas que resultan con anomalías y el color gris para los fallos. Teniendo en el eje horizontal las fechas comprendidas entre el 1 de marzo de 2023 y el 31 de marzo de 2024. Y en el eje vertical la cantidad de mediciones mensuales realizadas. De esta forma, podemos visualizar que a partir de diciembre 2023 se empezaron a registrar un aumento en las anomalías aunque ya se habían registrado fallos desde marzo de 2023.

Este aumento desde diciembre viene desencadenado por el aumento del número de protestas realizada en la isla, realizándose 529 en este mes.
En las mediciones realizadas y analizadas durante este último trimestre se pudo identificar varias anomalías, estas contienen diferentes tipos de fallos que vamos a detallar en este informe.

Tal y como hemos explicado las pruebas de OONI sobre Signal consisten en medir la accesibilidad de la aplicación dentro de una red específica, simulando ser una persona usuaria.

Específicamente estas pruebas tratan de establecer conexiones con los servidores de Signal, verificando si es posible establecer una conexión TLS y realizando peticiones *HTTP GET.*
*S*egún la documentación oficial de OONI solo hacen prueba a 4 *endpoints de Signal*.
Pero desde el pasado noviembre de 2023 se han añadido 10 endpoints más. Actualmente los test de OONI sobre Signal se realizan a los 14 *endpoints* siguientes*:*

- https://api.backup.signal.org
- https://cdn.signal.org
- https://cdn2.signal.org
- https://cdn3.signal.org
- https://cdsi.signal.org
- https://chat.signal.org
- https://contentproxy.signal.org
- https://sfu.voip.signal.org
- https://storage.signal.org
- https://svr2.signal.org
- https://ud-chat.signal.org
- https://updates.signal.org
- https://updates2.signal.org
- https://uptime.signal.org

Estos *endpoints* pueden verse afectados por censura de DNS, por TCP, HTTP y TLS y según la documentación de OONI, en caso de que al menos uno se vea afectado, se considera que Signal no es accesible o sufre bloqueo. En caso contrario que las pruebas sobre estos *endpoints* sean correctas, se considera que la la aplicación es accesible.

A continuación mostramos y analizamos diferentes resultados de algunas anomalías. Estos resultados de OONI están escritos en formato JSON.

1/ Fallo en la resolución del DNS.

En 10 pruebas de 100 realizadas durante el primer trimestre de 2024, OONI las cataloga bajo el error **“android_dns_cache_no_data”.**

Este fallo es debido a la inconsistencia en la resolución del DNS (Sistema de Nombre de Dominios) de un *host* de Signal y por lo tanto no se recibe respuesta del mismo.
En este caso , tomando como ejemplo una prueba concreta, en el apartado de pruebas DNS (“queries” llamado así por OONI en el resultado escrito en formato JSON), concretamente en las mediciones 20 y 21, vemos que sobre el host “*svr2.signal.org” apreciamos que* no se ha obtenido ninguna respuesta (`“answers” : null`).

Como consecuencia de este fallo en la resolución del DNS las pruebas a los protocolos HTTP y TCP van a estar comprometidos.

En HTTP (“request” en el resultado JSON) se presenta el fallo “***generic_timeout_error***”,y también el fallo “***android_dns_cache_no_data***” , ambos devuelven una respuesta vacía (`*body: “”*`).

En el protocolo TCP se puede ver el fallo ***"generic_timeout_error"*** en la dirección IP 240.0.0.1 asociada al hostname *"api.backup.signal.org"*, en donde el servidor tarda demasiado en completar la solicitud.

2/ Mal funcionamiento del servidor DNS

En el caso del fallo **dns_server_misbehaving** que tiene un total de 5 apariciones de 100, apreciamos un mal funcionamiento del servidor DNS.

Concretamente, se aprecian errores en el apartado de nombre de dominio ("queries" llamado así en el resultado JSON de OONI), donde los *hostname* "*uptime.signal.org*" y "*storage.signal.org*" no logran ser resueltos y no retornan ninguna respuesta ("answers" : NULL).

```
▾ 6 : { 10 items
  "answers" : NULL
  "engine" : string "system"
  "failure" : string "dns_server_misbehaving"
  "hostname" : string "uptime.signal.org"
  "query_type" : string "A"
  "resolver_hostname" : NULL
  "resolver_port" : NULL
  "resolver_address" : string ""
  "t" : float 5.883562115
  "tags" : NULL
}
▸ 7 : {...} 10 items
▾ 8 : { 10 items
  "answers" : NULL
  "engine" : string "system"
  "failure" : string "dns_server_misbehaving"
  "hostname" : string "storage.signal.org"
  "query_type" : string "A"
  "resolver_hostname" : NULL
  "resolver_port" : NULL
  "resolver_address" : string ""
  "t" : float 5.883572768
  "tags" : NULL
}
▸ 9 : {...} 10 items
```


Por lo que en las mediciones del protocolo HTTP (“request” llamado así en los resultados) aparece el error "*dns_server_misbehaving*" para el hostname "*storage.signal.org*". Donde devuelve una respuesta vacía coincidiendo con el host del apartado DNS que no se pudo determinar.


```
"failure" : string "dns_server_misbehaving"
▾ "request" : { 8 items
  "body" : string ""
  "body_is_truncated" : bool false
  ▸ "headers_list" : [...] 4 items
  ▸ "headers" : {...} 4 items
  "method" : string "GET"
  ▸ "tor" : {...} 3 items
  "x_transport" : string "tcp"
  "url" : string "https://storage.signal.org/"
}
```


3/ **Sin respuesta del servidor.**

El fallo *“**generic_timeout_error**”* es el fallo más común presente en las anomalías de Signal desde la isla con un total de 36 apariciones.

Tomando como ejemplo este test, si analizamos las mediciones sobre el protocolo HTTP, se muestra el error "generic_timeout_error" en *"api.backup.signal.org"* , devolviendo una respuesta vacía (body: “”) resultado del tiempo excesivo que toma el servidor en procesar la petición.


```
▼ 10 : { 5 items
  "failure" : string "generic_timeout_error"
  ▼ "request" : { 8 items
    "body" : string ""
    "body_is_truncated" : bool false
    ▶ "headers_list" : [...] 4 items
    ▶ "headers" : {...} 4 items
    "method" : string "GET"
    ▶ "tor" : {...} 3 items
    "x_transport" : string "tcp"
    "url" : string "https://api.backup.signal.org/"
  }
  ▼ "response" : { 5 items
    "body" : string ""
    "body_is_truncated" : bool false
    "code" : int 0
    ▶ "headers_list" : [] 0 items
    ▶ "headers" : {} 0 items
  }
  "t" : float 15.200011489
  "tags" : NULL
}
```


Las mediciones por el protocolo TCP devuelven un error "generic_timeout_error" sobre la dirección IP 240.0.0.1 que pertence al host *api.backup.signal.org*, coincidiendo con el mismo escenario que tuvo el protocolo HTTP.


```
▼ 10 : { 5 items
  "ip" : string "240.0.0.1"
  "port" : int 443
  ▼ "status" : { 2 items
    "failure" : string "generic_timeout_error"
    "success" : bool false
  }
  "t" : float 15.199739951
  "tags" : NULL
}
]
```

Conclusiones sobre el bloqueo a Signal en Cuba

Se puede apreciar entonces que en estos últimos meses hay un aumento de las anomalías presentes en Signal desde Cuba.
Tras la ejecución de 100 pruebas realizadas desde el primero de enero hasta el 25 de marzo de este 2024, se pudieron detectar 51 anomalías. En las anomalías detectadas, 10 fueron consecuencia del fallo ***"android_dns_cache_no_data"*** que afecta el protocolo DNS al producirse inconsistencias al resolver los hosts de Signal, tales como el ejemplo presentado "*svr2.signal.org"* y por tanto también se producen afectaciones sobre el protocolo HTTP y TCP.
Además también se vieron afectados estos dos host:
"updates2.signal.org"
"updates.signal.org"

Otro de los fallos que afectaron el protocolo DNS fue ***"dns_server_misbehaving"*** presente en 5 de las anomalías detectadas, provocado por un mal funcionamiento en la resolución del DNS, en este caso los hosts afectados fueron "*storage.signal.org*" y "*uptime.signal.org*".
Además también se ve afectado el host:
"chat.signal.org"

Si bien estos dos errores afectan directamente al protocolo DNS, OONI los cataloga de forma diferente. No queda totalmente claro del motivo, por ello en futuros estudios se profundizará sobre el tema.

Finalmente, analizando el fallo ***"generic_timeout_error"*** con 36 apariciones (siendo este el más predominante entre las anomalías), se produce al tratar de establecer una conexión mediante el protocolo TCP. El servidor toma un tiempo excesivo en procesar la petición, por lo que nunca se tiene respuesta, entre los ejemplos expuestos se aprecia como el host *api.backup.signal.org* se ve afectado, desencadenando errores también sobre el protocolo HTTP.

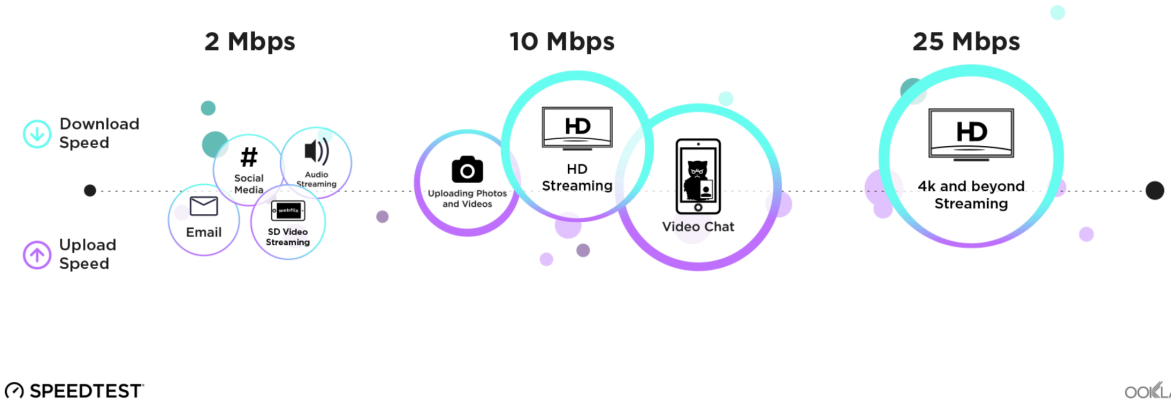
A todos estos fallos estuvieron presentes también pero de forma aislada, 2 apariciones del error ***"network_unreachable"*** *sobre "updates.signal.org"* y una del error ***"connection_reset"*** en donde se repite el host *"updates.signal.org"*

Si bien en OONI se menciona que el método más probable de censura que se realiza sobre Signal en Cuba es por DPI, no se tiene la certeza exacta si es totalmente verídico. Por eso en próximos estudios se profundizará sobre el tipo de censura que se aplica sobre esta herramienta de mensajería instantánea.

Velocidad de Internet

La velocidad de Internet, medida en términos de la velocidad de transferencia de datos, impacta directamente en la experiencia de las usuarias al utilizar servicios en Internet. Sin embargo, es importante destacar que esta velocidad puede verse afectada por diversos factores y su medición varía según la fuente utilizada.

En este informe nos centraremos en Ookla, como fuente para evaluar la velocidad de Internet en Cuba. Ookla es una empresa de pruebas de redes conocida por su herramienta Speed Test, recopila información voluntaria de las usuarias para determinar la velocidad de conexión. Aunque útil para medir el ancho de banda máximo en condiciones de saturación, su muestra no representa necesariamente la diversidad total de conexiones en el país.

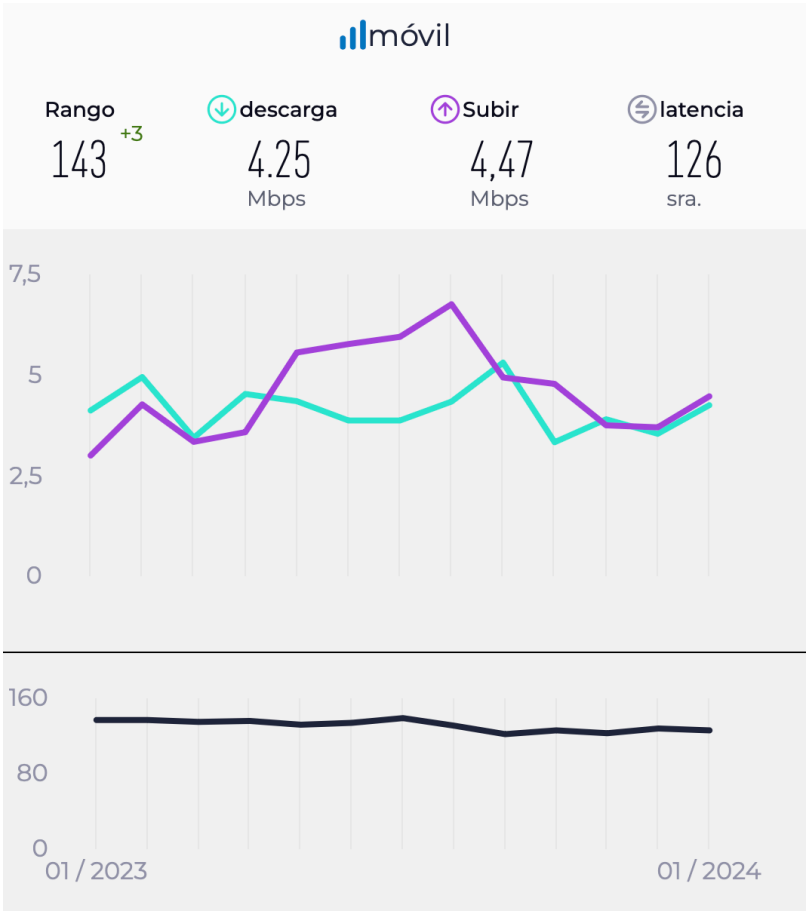


Una buena velocidad de Internet puede variar dependiendo de las actividades en internet que realicen las usuarias. Según datos de Ookla, se recomienda una velocidad mínima de al menos 2 Mbps para realizar actividades básicas como el correo electrónico, la transmisión de video en definición estándar (SD), el uso de redes sociales y la transmisión de audio en tiempo real.

Por otro lado, para actividades que requieren un mayor ancho de banda, como subir fotos y videos, realizar chat de video y transmitir video en alta definición (HD), se recomienda una velocidad de al menos 10 Mbps para garantizar una experiencia fluida y sin interrupciones.

Para aquellos que desean disfrutar de contenido en resolución 4K, se sugiere una velocidad de al menos 25 Mbps para asegurar una reproducción de alta calidad y sin problemas. Estas recomendaciones son importantes para que las usuarias puedan compararlas con los datos de velocidad de internet en Cuba y evaluar la calidad de la conexión disponible en el país.

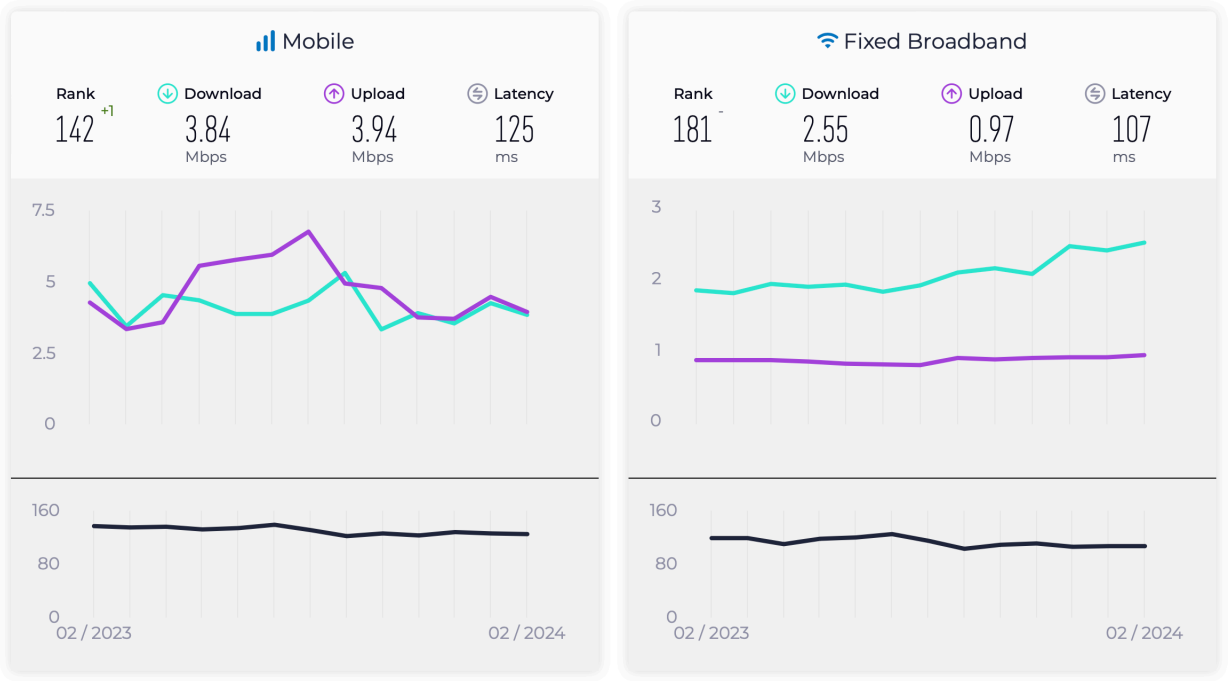
Enero 2024



En enero de 2024, Cuba tuvo una velocidad media de internet móvil de 4.25 Mbps para descarga y 4.47 Mbps para carga, lo que la colocó como la más lenta de América Latina según el Índice Global Speedtest de Ookla. Además, ocupó el puesto 143 de 144 países incluidos en la muestra de Ookla en ese mismo período.

En lo que respecta a la velocidad de banda ancha fija, Cuba se encontró en la cola de la clasificación en enero de 2024, según el Índice Global Speedtest de Ookla. Ocupando el último puesto, número 181, el país registró una velocidad media de descarga de 2.44 Mbps y una velocidad de subida promedio de 0.94 Mbps.

Febrero 2024



En el mes de febrero la velocidad media de internet móvil fue de 3.84 Mbps para descarga y 3.94 Mbps para carga, lo cual representa una disminución en comparación con el mes anterior, indicando una peor calidad de la velocidad de internet. A pesar de esto Cuba mejoró su posición en el ranking mundial al ubicarse en el puesto 142 de 143 países medidos, lo que la coloca como la más lenta de América Latina según el índice global de Speedtest de Ookla en febrero de 2024.

Además, en cuanto a la velocidad de banda ancha fija, Cuba ocupó el último puesto, 181, con una velocidad media de descarga de 2.55 Mbps y una velocidad promedio de subida de 0.97 Mbps.

Estas cifras reflejan una notable disparidad en comparación con otros países evaluados en el estudio, destacando la necesidad de mejoras significativas en la infraestructura de conectividad en Cuba.

Bloqueo en Cuba a la herramienta de elusión de censura Tor

En los primeros meses del año 2024 hemos continuado nuestras mediciones utilizando la prueba evasión de OONI Probe para evaluar la accesibilidad a la red de Tor en Cuba. Los resultados obtenidos confirman que el acceso a Tor sigue bloqueado en el país. Desde finales de 2023, hemos estado llevando a cabo estas mediciones de forma regular para monitorear cualquier cambio en la situación.

La red de Tor se inicia desde el momento en que una usuaria utiliza *Tor Browser*, este navegador de Tor se conectará a través de un proxy SOCKS (protocolo que permite la comunicación segura entre un ordenador 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. Esta conexión 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 denegadas ("*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.

Prueba de evasión en OONI a Tor (Tor Test)

Al examinar específicamente el resultado de este servicio en la prueba de OONI realizada el día 18 de febrero de 2024, se puede observar que el resultado coincide con otras pruebas realizadas el pasado año y que fueron publicadas en el informe número 3 del 2023. En dicho informe se pueden ver algunas de las definiciones usadas en el siguiente apartado que procedemos a detallar.

Al examinar específicamente el resultado del servicio de retransmisores de Tor (*dir_port*), se puede observar que el puerto de autoridad de directorio tiene disponibles 10 servidores, de los cuales solo uno se muestra accesible.

Para el protocolo *obfs4* se muestra una mejor situación aunque también sufre de censura. 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.

Al analizar el puerto de autoridad de directorio (*or_port_dirauth*), podemos ver que tiene disponibles 10 servidores, de los cuales ninguno es accesible.

Para el servicio “OR port” no se muestra disponible desde Cuba ningún nodo para realizar un puente a través de él, como se muestra en la imagen.

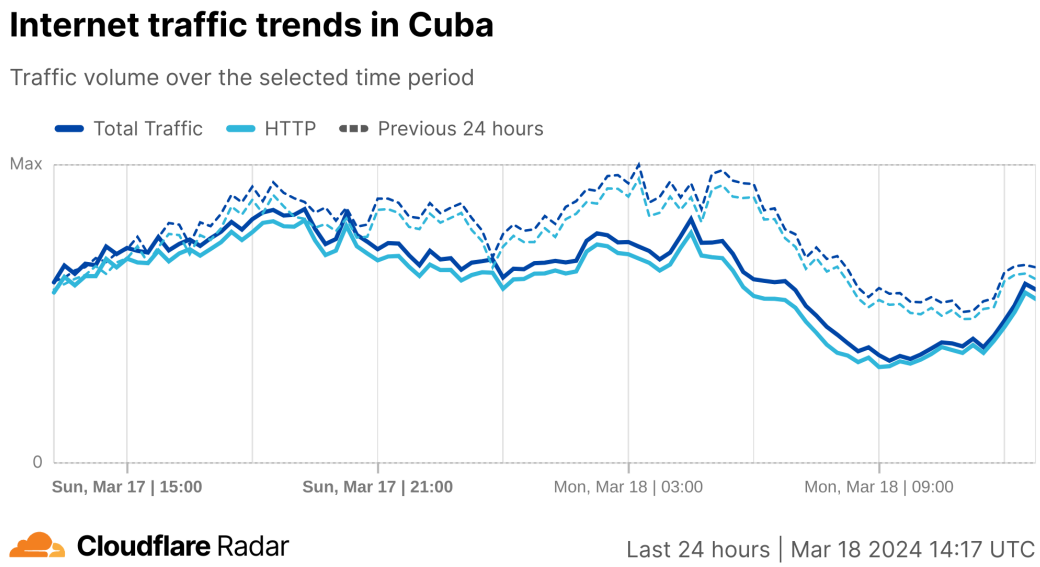
Conclusiones sobre las pruebas de Tor

Hemos podido confirmar que todos los datos recogidos desde el último trimestre de 2023 son idénticos y que la censura a la herramienta de Tor sigue aplicandose. A partir de esto podemos concluir que las medidas e intentos de bloqueo de Tor por parte del proveedor de servicios de Internet cubano no han variado.

Reseña de lo ocurrido en Cuba durante el levantamiento popular del 17 de marzo de 2024

El domingo 17 de marzo de 2024 sucedieron algunas protestas populares en varios lugares de Cuba. Lo que comenzó en Santiago de Cuba, rápidamente se extendió a El Cobre, Bayamo y Santa Marta (en Cárdenas). Al grito de “Corriente y comida” o “Patria y vida”, miles de cubanos se lanzaron a la calle a exigir el fin de la miseria provocada por el régimen comunista.

A diferencia de lo ocurrido en ocasiones anteriores, el gobierno cubano no cortó el servicio de Internet en la isla sino que lo hizo en algunos segmentos geográficos de la red. Por voluntarios sabemos que al menos en Guantánamo y Santiago de Cuba se dieron cortes por varias horas. Esto se ve reflejado en una ligera disminución del volumen de tráfico de Internet durante el domingo 17 y el lunes 18 de marzo. A pesar de esto no se puede decir que existió un apagón en el Internet de Cuba, evidenciando un cambio de estrategia por parte del régimen.



En la gráfica de tráfico de Internet de ese día, generada por CloudflareRadar, se va viendo una disminución del volumen de tráfico con respecto al día anterior, el 16 de marzo, e incluso con respecto al domingo anterior, el 10 de marzo. Nuestro equipo cree que ese comportamiento es debido a los cortes de Internet en lugares específicos del país donde se dieron las protestas.

Conclusiones

Este informe resalta la persistente censura del internet en Cuba, enfocándose en la significativa limitación del acceso a la información en el país. Durante los meses de enero a marzo de 2024 hemos encontrado evidencias gracias a las mediciones de OONI y capturas de tráfico de paquetes de red, con la herramienta WireShark, de que al menos 61 sitios web han sido censurados en ese período. Entre estos, 46 sitios están bloqueados utilizando tecnología DPI, la cual se ha implementado desde 2017 en la isla para censurar sitios web.

Las mediciones realizadas revelan que se sigue utilizando el mismo equipo, que proviene de la empresa china Huawei, para llevar a cabo la censura por DPI .

Además se ha observado que el gobierno utiliza métodos engañosos, como falsos códigos de estado HTTP, para hacer creer a las usuarias que el problema radica en el servidor de destino y no en el bloqueo de estos sitios web monitoreados.

El estudio de la censura de Signal en la isla, ha sido un punto a incorporar en este informe. A lo largo de este primer trimestre, entre enero y marzo se han realizado 100 pruebas sobre esta aplicación de mensajería, en las que se detectó un total de 54 anomalías.

Dentro de las anomalías se detectaron distintos fallos, entre ellos se encuentran afectaciones a varios hosts de Signal debido a inconsistencias a la hora de resolver los hosts y, errores que afectan el protocolo DNS, lo que tiene como consecuencia que no se tenga respuesta a las peticiones realizadas a Signal, impidiendo su uso correctamente.

En las anomalías detectadas sobre Signal, el fallo que más ha predominado, con 36 apariciones, es por un consumo excesivo de tiempo para procesar una petición. Provocando que nunca se terminara de completar y por tanto nunca se obtiene una respuesta.

Si bien OONI en su informe menciona la suposición del tipo de bloqueo que se emplea en Cuba sobre Signal, no se tienen los suficientes elementos para asegurar con total certeza que sea del todo cierto, por lo que en futuros trabajos se indagará sobre el origen del bloqueo de Signal en la isla.

En este informe empezamos a monitorear el tema de la velocidad de internet en la isla, como un factor clave que impacta la experiencia de las usuarias al utilizar servicios en internet, ya que la reducción de la velocidad puede ser otra estrategia para dificultar el acceso a internet. Donde Cuba registra velocidades de internet móvil y banda ancha fija que se sitúan entre las más lentas de América Latina, según los índices de Speedtest de Ookla. Las velocidades actuales en Cuba, tanto para internet móvil como para banda ancha fija, están por debajo de las recomendaciones mínimas. Esto se traduce en un servicio muy lento para la población.

Trabajos futuros

Nuestro equipo seguirá monitoreando de cerca los dominios evaluados este trimestre y explorará otros de posible interés. Nos enfocaremos en detectar la persistencia de bloqueos previos y descubrir nuevas formas de censura en la red. Además, continuaremos supervisando los sitios censurados y aquellos no medidos, y realizaremos pruebas periódicas en OONI para evaluar cualquier cambio en las restricciones y su evolución.

Además, nuestro equipo continuará analizando la velocidad de Internet en la isla a través de herramientas como Speedtest de Ookla y otras similares. Esta evaluación nos permitirá proporcionar información actualizada a las usuarias sobre la calidad y eficiencia de la conexión a Internet en Cuba, lo cual es crucial para entender el panorama completo de la infraestructura de telecomunicaciones en el país y las posibles mejoras necesarias. A esto agregar, la continuación del estudio de la censura de Signal y profundizar en el origen de la misma, sumado a la exploración de cualquier tipo de censura que se aplique sobre cualquier aplicación de mensajería instantánea.