Censura y Restricciones de Internet en Cuba:

Resumen de 9 meses de monitoreo

Marzo a Noviembre, 2023

Autor: Diktyon – Twitter: @DiktyonCuba

Hallazgos claves

Durante el año 2023, se realizaron tres informes exhaustivos sobre la censura en Internet en Cuba, revelando patrones consistentes de restricción del acceso a la información.

- En el primer informe, abarcando desde marzo a mayo, se monitorearon 230 sitios, confirmando que 56 de ellos estaban bloqueados, destacando el uso de tecnología de Inspección Profunda de Paquetes (DPI por sus siglas en inglés).
- En el segundo informe, de junio a agosto, se expandió la lista de sitios bloqueados a 60, y en 40 de estos se confirmó el uso de tecnología DPI para censurar.
- En el tercer informe, de septiembre a noviembre, se identificaron 67 sitios bloqueados, y en 49 de estos se confirmó el uso de tecnología DPI para censurar.
- De los resultados de OONI catalogados como "mediciones fallidas", se confirmó, en múltiples casos, el uso de tecnología DPI para censurar.
- En el tercer informe se constató el bloqueo sistemático de Tor en Cuba, evidenciando una restricción significativa en el acceso a esta herramientas de elusión de censura.

Introducción

Cuba ha experimentado un prolongado gobierno socialista desde la Revolución de 1959, caracterizado por un control estatal y económico a través de un único partido. La salud del Internet en el país se ve afectada por una infraestructura limitada y altos costos de conexión, junto con estrictos controles gubernamentales que restringen el acceso y contenido en Internet, generando inquietudes sobre la libertad de expresión y el libre acceso a la información en Internet.

Estos 9 meses de investigación hemos medido y estudiado la censura de Internet en Cuba, para poder documentar e informar de los hallazgos significativos.

Los sitios web que son considerados inaceptables por el gobierno, han sido censurados por la Proveedora de Servicios de Internet (ISP por sus siglas en inglés) ETECSA, única ISP en Cuba.

El derecho de acceso a Internet es un derecho fundamental reconocido como tal por la Organización de las Naciones Unidas (ONU).

Este resumen tiene como objetivo primordial hacer un resumen de los hallazgos más significativos en los tres informes publicados durante el año 2023, donde destacan las listas actualizadas de los sitios web bloqueados en Cuba en cada trimestre.

Nos hemos ayudado de las diferentes herramientas del proyecto de Observatorio Abierto de Interferencias de la Red (OONI, por sus siglas en inglés), precisamente OONI Probe y OONI Probe Cli para la obtención de diferentes muestras y OONI Explorer para su posterior análisis.

Además, se realizaron capturas de paquetes de datos con WireShark, permitiendo un examen exhaustivo del tráfico de paquetes en cada uno de los protocolos que se suceden y permiten visualizar una web.
Un tema fundamental fue el relacionado con las múltiples mediciones fallidas de OONI en las pruebas realizadas, donde pudimos confirmar la utilización de tecnología de DPI para censurar cada una de estas webs.
A lo largo de nuestros estudios realizados, cada vez que hemos observado el mismo identificador relacionado con el equipo utilizado para censurar mediante la DPI, hemos catalogado las pruebas como confirmadas censuras mediante DPI. Es por esta razón que cada trimestre se ha aumentado la lista de sitios web censurados mediante tecnología DPI.

También se realizaron pruebas de evasión en OONI para analizar el bloqueo de la herramienta Tor, donde en el informe 3 ofrecemos una comprensión detallada sobre el bloqueo de esta herramienta de elusión de la censura..

Dominios censurados durante estos 9 meses

Informe # 1 (marzo-mayo de 2023)
Durante este período, se monitorearon 230 sitios, confirmando la existencia de al menos 56 sitios web bloqueados en Cuba, principalmente aquellos relacionados con noticias, medios independientes y derechos humanos que publican contenido que podría no ser del agrado del gobierno cubano. Para el estudio utilizamos varios dominios de la lista de CitizenLab de Cuba y añadimos otros que consideramos de relevancia. Estos últimos fueron seleccionados por las publicaciones que han realizado, las cuales no son acordes con la postura del régimen cubano, y creemos en la posibilidad de que en el futuro serán bloqueadas.

La censura afectó a los diferentes protocolos necesarios para acceder a cualquier web, Entre ellos se afectaron TCP (Protocolo de Control de Transmisión), protocolo de la capa de transporte que permite el intercambio de paquetes de Internet entre dispositivos; DNS (Sistema de Nombres de Dominio), protocolo de la capa de aplicación utilizado para la resolución de nombres de dominio; HTTP/HTTPS (Protocolo de Transferencia de Hipertexto/Protocolo Seguro de Transferencia de Hipertexto), protocolos también de la capa de aplicación que permiten la visualización de la web mediante la interpretación del código que la compone; y TLS (Seguridad en la Capa de Transporte), protocolo de la capa de transporte que añade seguridad y que permite cifrar parte de la comunicación entre dos dispositivos.

De los 56 sitios web bloqueados durante este periodo, 25 fueron objeto de censura mediante DPI. Empresas como Huawei, Fortinet, y Allot comercializan estos equipos que son vendidos a quienes controlan el acceso a Internet (las proveedoras). La ISP podrá inspeccionar todo el tráfico de Internet que pasa por ella y podrá aplicar censura según su interés.
En nuestro primer informe pudimos observar el identificante "V2R2C00-IAE/1.0" que gracias a las investigación de Qurium del año 2020 entendimos que se trataba de un equipo de la empresa Huawei llamado eSight, revelando la presencia de tecnología DPI en la red cubana. En este mismo informe se explica que el “encabezado IAE sugiere la presencia de un "Motor de Conciencia Inteligente", que podría referirse a un Huawei NIP6000, un avanzado Sistema de Prevención de Intrusiones de Nueva Generación (NGIPS) que admite las Desconexiones de Sesión”.
Además en la investigación de Valentin Weber publicada en un informe de Open Technology Fund en 2020 revelaba la detecciónа de cajas intermedias de vigilancia de Huawei con la huella digital V2R2C00-IAE/1.0 en varios países, entre ellos Cuba.

Se reconfirmó en el artículo en NTD - News, donde también mencionaba que este encabezado está vinculado con un equipo de la marca Huawei conocido como eSight.

El objetivo principal de nuestro estudio fue evaluar el estado actual de la censura en Internet en Cuba y compararlo con los hallazgos de OONI en 2017.

Informe 2 (junio-agosto de 2023)

En este trimestre se monitorearon 233 sitios y gracias a los resultados de OONI pudimos confirmar 60 dominios bloqueados, los cuales sufrían afectaciones en diferentes protocolos que permiten la navegación en internet y la visualización de una web (TCP, DNS y HTTP). De los 60 sitios bloqueados, 40 lo son mediante DPI, gracias al identificante de servidor "V2R2C00-IAE/1.0" que ya vimos en el primer informe.

Este informe 2 profundiza en los hallazgos presentados en el informe 1, enfocándose en la censura selectiva y el control de acceso a través de la inspección detallada de paquetes.

Informe 3 (septiembre-noviembre de 2023)
En este período, se observaron detalladamente 240 sitios, identificando al menos 67 sitios bloqueados. Se utilizaron 217 sitios de la lista de CitizenLab y otros agregados por Diktyon. Las mediciones de OONI identificaron 67 dominios sometidos a diversas formas de censura, incluyendo el bloqueo de los protocolos TCP y HTTP, con el uso prevalente de la tecnología DPI.
Se confirmaron 9 sitios web más, afectados por esta tecnología, sobre un total de 49. Se confirmó la utilización de tecnología DPI en los resultados de OONI catalogados como “mediciones fallidas” para las pruebas HTTPS.

Las “mediciones fallidas” de OONI

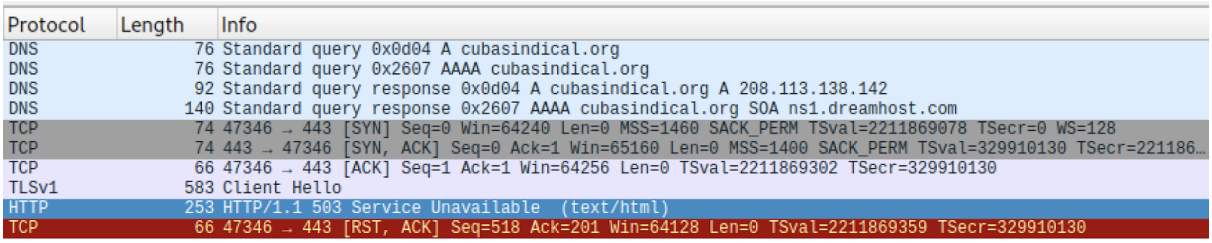
Durante los dos últimos informes, se confirmó que, las conocidas censuras registradas por OONI como "mediciones fallidas", sufren de la intervención mediante tecnología DPI. Cuando en el análisis detallado de las pruebas en formato JSON de OONI encontramos un mensaje de “fallo desconocido” que indica un problema en el handshake de TLS.

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

En un informe previo de OONI, publicado en marzo de 2023, se confirmaron como censura todas las 40 mediciones que presentaban este mismo mensaje de “fallo desconocido” por parte del software de OONI. También señalaron que están trabajando para mejorar su software, a fin de que reconozca el problema en el handshake de TLS como una anomalía y no como una medición fallida.

En el segundo informe publicado se destacó que 12 sitios web, cuyas versiones HTTPS fueron catalogadas como "mediciones fallidas" por OONI, presentaban el mismo mensaje de fallo desconocido.

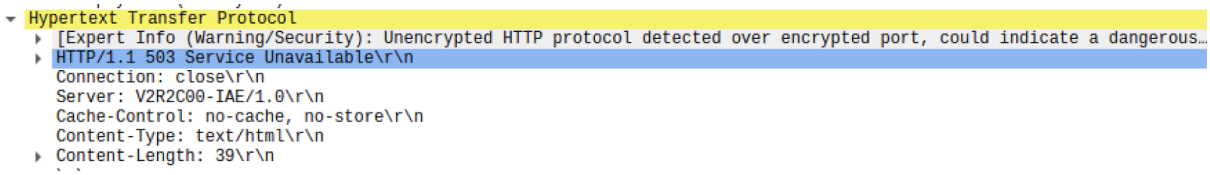
Tras un análisis detallado de las capturas de tráfico de paquetes utilizando WireShark se confirmó que estos sitios fueron censurados mediante tecnología DPI.



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 (Client Hello) del handshake se realiza correctamente.
2. El segundo no nos llega nunca dado que es interferido por la máquina intermedia (DPI). Que modificando la IP se hace pasar por el servidor de destino e incluye un código de estado de HTTP 503, el cual nos indica que el servidor no está disponible temporalmente.

Adicionalmente, en esta captura de WireShark hemos observado en los encabezados del paquete HTTP, que el servidor se identifica como V2R2C00-IAE/1.0.



En todas las capturas efectuadas durante estos 9 meses, nunca se ha encontrado el código de estado HTTP 451, el cual indica bloqueos por razones legales. Esto sugiere que la censura no obedece a mandatos judiciales, haciéndonos creer que el problema proviene del servidor de destino.

Bloqueo a Tor, herramienta de elusión de censura

Durante los meses de septiembre, octubre y noviembre, se llevaron a cabo mediciones para evaluar la accesibilidad a la red de Tor en Cuba, utilizando la prueba de "evasión" de OONI Probe. Los resultados concluyen que el acceso a Tor está siendo bloqueado en el país como explicamos en el informe 3.

Cuando estudiamos la salud de Tor mediante OONI Probe, el software de OONI realiza la prueba de accesibilidad a cuatro servicios que permiten el funcionamiento de Tor.
En las pruebas realizadas durante este trimestre se observó un bloqueo a muchos de los relays que permiten el funcionamiento de esta red. Por ejemplo en las mediciones realizadas 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, uno de los cuatro servicios que permiten el funcionamiento de Tor.

Conclusiones

Este informe, a lo largo de nueve meses, revela prácticas continuas de censura de Internet por

parte de la ISP cubana. Es evidente que va en aumento la utilización de tecnología que permite la DPI, dado que al acabar el año 2023 podemos demostrar su utilización sobre 49 sitios web de los 67 sitios web bloqueados.

Cabe destacar el positivo hallazgo para la comunidad que trabaja en anticensura: la interceptación en el hanshake de TLS encontrado en las capturas de WireShark. Esperemos que esto ayude a ampliar la visión y la comprensión de los diferentes mecanismos aplicados por máquinas intermedias, permitiendo así el aprendizaje y la mejora de las herramientas de detección de censura.

Por último el bloqueo sistemático de Tor durante el período analizado subraya la restricción significativa en el acceso a herramientas de elusión de censura y realza la importancia del desarrollo de protocolos y herramientas más complejas que permitan la elusión de censura.

Trabajos futuros

Diktyon continuará monitoreando los sitios web censurados y realizará pruebas periódicas con las herramientas de OONI para evaluar la persistencia de restricciones y cualquier cambio en la censura aplicada. Se profundizará en la investigación de dominios bloqueados, combinando pruebas de OONI con un análisis exhaustivo de paquetes utilizando WireShark.
Profundizar en las pruebas de “evasión de censura de OONI” y estudiar los diferentes protocolos de Tor, como Snowflake, que permiten una mejor elusión en lugares con más restricciones.

El objetivo es mantener a la población informada sobre la libertad en Internet en Cuba, estando alerta ante posibles cambios. Además, queremos colaborar con personas desarrolladoras de Tor y OONI Probe para entender mejor las tácticas de censura.