# Women On Web
# web censurada en España

*May, 15, 2020* *Vasilis Ververis, Fadelkon, Ana, Bita, Samba*

---

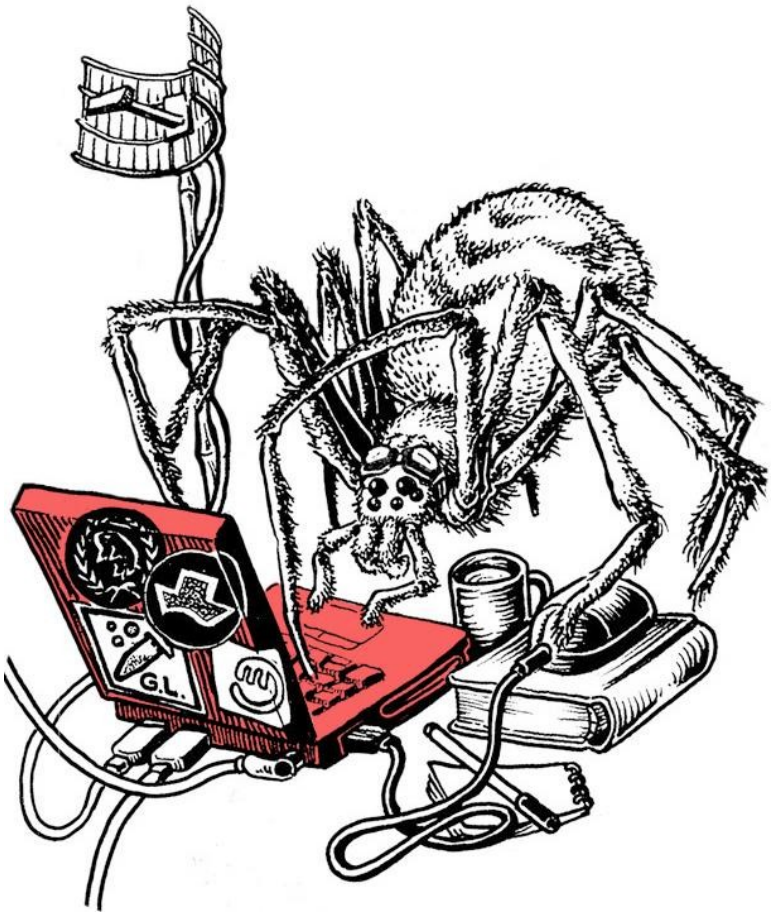
**Translation(s):**

- English: Women on Web website censored in Spain

---

**Updates:**

- `Actualización (2020-05-20)`: Revisión ortográfica, gráfico traducido
- `Actualización (2020-05-26)`: Traducción actualizada
- `Actualización (2020-05-26)`: Mencionamos medidas de Euskaltel que sugieren un bloqueo basado en DNS
- `Actualización (2020-06-07)`: Añadimos sección Contribuir con un enlace OONI Run



**Web bloqueada:** womenonweb.org

**Los vendedores de cajas intermedias de DPI:** Allot, Fortinet

**Métodos de bloqueo:** Manipulación de DNS, Bloqueo de HTTP, Interceptación TLS, Reinicios de TCP

**Bloqueada en las ISP:** Vodafone (AS12357 y AS12430), Vodafone Ono (AS6739), Orange (AS12479 y AS12715), CSUC (AS13041), MÁSMÓVIL (AS15704), XFERA (AS16299), Telefónica/Movistar (AS3352)

---

Con este artículo queremos concienciar sobre la creciente censura de sitios web y los controles de información que han iniciado compañías proveedoras de servicios de internet (ISP por sus siglas en inglés) en territorio español. Compartiremos todos los detalles técnicos del consistente bloqueo de la página web de Women On Web en la mayoría de las ISP españolas.

# Introducción

La web de Women On Web womenonweb.org, una organización sin ánimo de lucro que ofrece apoyo a mujeres y personas embarazadas, ha sido bloqueada por varias compañías ISP españolas. El Observatorio Abierto de Interferencias en la Red, OONI, una comunidad global que mide las censuras en internet, provee herramientas para que cualquiera, teniendo una conexión de red, pueda contribuir voluntariamente con su datos a informes globales. Las medidas recientes indican que la web de Women On Web ha sido bloqueada desde finales de enero de 2020 y sigue bloqueada en la mayoría de las compañías proveedoras de servicios de internet españolas a la fecha de la realización de este escrito, en mayo de 2020.

Esta no es la primera vez que la web Women on Web ha sido bloqueada. OONI publicó un informe en 2019 analizando el bloqueo confirmaron de las webs Women on Waves y Women on Web en Brasil, Irán, Turquía, Corea del Sur y Arabia Saudí.

**Esta es la primera vez que vemos Women on Web bloqueada en España.**

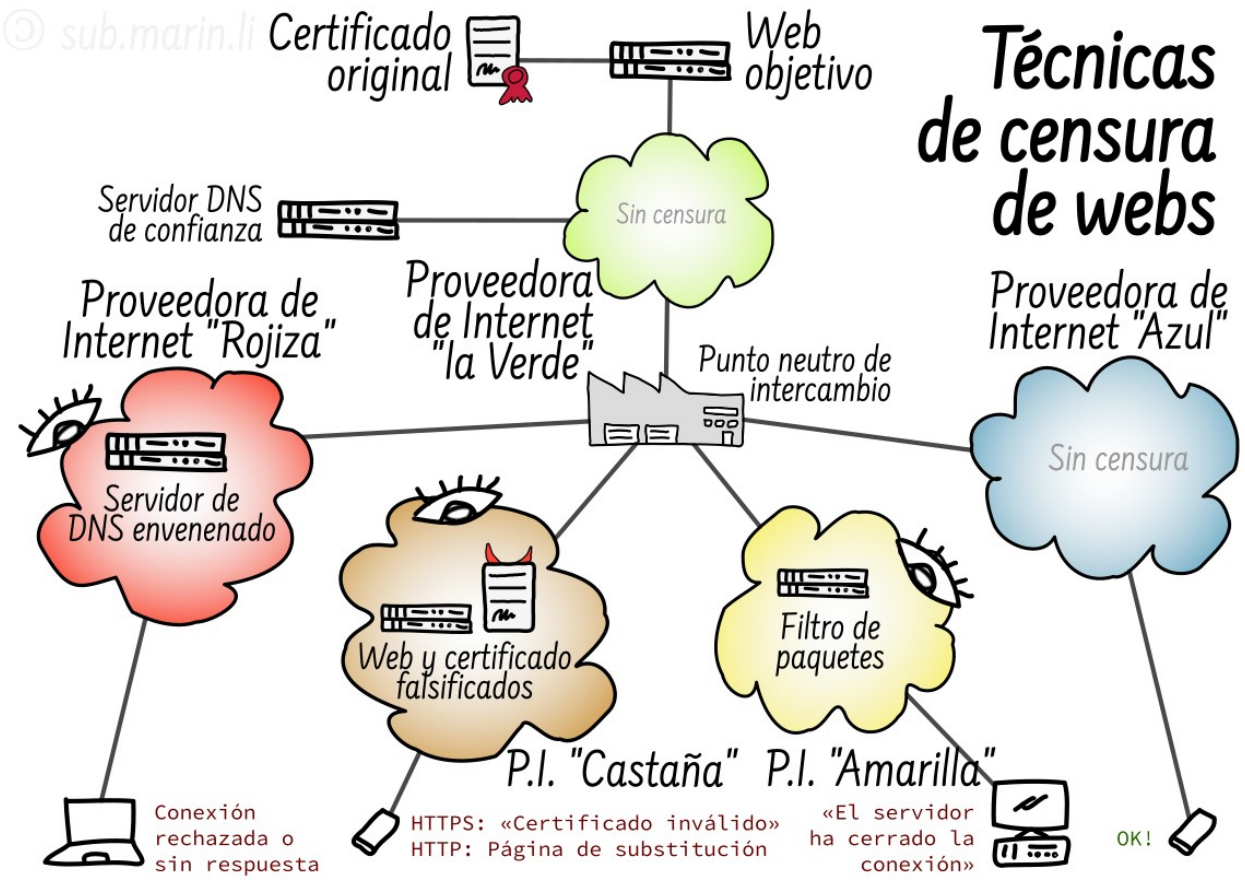
En este artículo describimos cómo las mayores compañías ISP españolas bloquean la web **womenonweb.org**. Dichas compañías vienen bloqueando la web por medio de manipulación de DNS (Servidor de Nombre de Dominio), reinicio de TCP (Protocolo de Control de Transmisión), bloqueo de HTTP, usando la infraestructura de Inspección Profunda de Paquetes (DPI por sus siglas en inglés). Nuestro análisis de datos se basa en medidas de la red, informaciones procedentes de OONI.

# Estrategias de bloqueo de la red de las ISP

## Tabla resumen

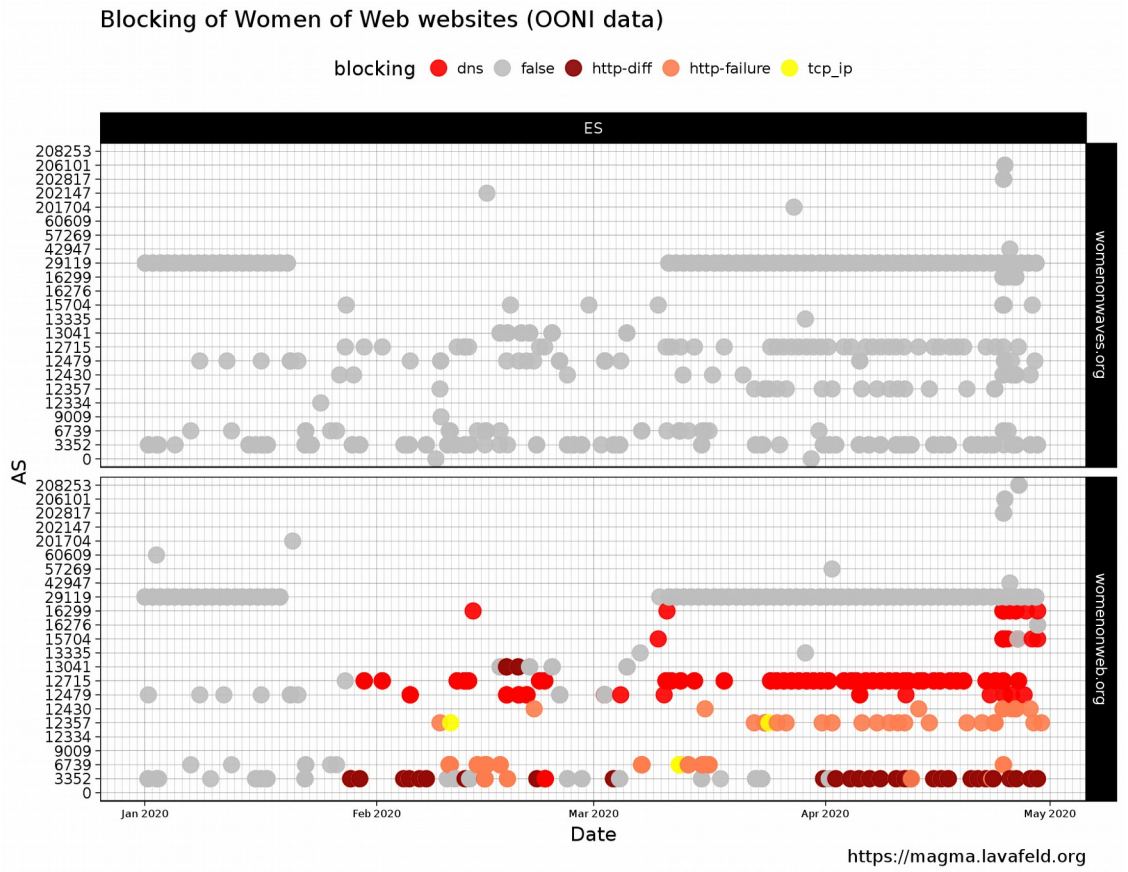
| ISP | Metodología de bloqueo | Caja intermediaria DPI |
|---|---|---|
| Telefónica/Movistar | Manipulación DNS, Bloqueo HTTP, Reinicio TCP | Fortinet |
| Vodafone/Ono | Bloqueo HTTP, Interceptación TLS, Reinicio TCP | Allot |
| Orange/Jazztel | Manipulación DNS | - |
| MÁSMÓVIL/XFERA | Manipulación DNS | - |
| CSUC | Bloqueo HTTP, Reinício TCP | Fortinet |
| Euskaltel* | Basado en DNS* | - |

Puedes descargar nuestro análisis de datos (como un archivo CSV) aquí.



## AS/gráfica de tiempos

El gráfico ilustra las mediciones de red de OONI desde el 1 de enero de 2020 hasta el 30 de abril de 2020 de las webs **www.womenonweb.org** y **www.womenonwaves.org**. En el eje 'y' del gráfico aparecen los nombres de las redes de sistemas autónomos (AS) de los proveedores de servicios de internet, y en el eje 'x' la fecha de las mediciones. Los colores del gráfico indican el tipo de bloqueo (`dns`, `http-diff`, `http-failure` y `tcp_ip`), o ningún tipo de bloqueo indicado en gris. Estos tipos de bloqueo están descritos en detalle en las especificaciones de la prueba de conectividad web de OONI. En la parte superior del gráfico, podemos ver que, según las medidas de red, la web **www.womenonwaves.org** no está bloqueada por ninguna ISP española (al menos de las que tenemos datos); todas las mediciones son de color gris significando que no se observa bloqueo. En el gráfico de la parte inferior, se ilustran las medidas de red de la web **www.womenonweb.org**. Aquí podemos ver un escenario muy diferente donde la mayoría de compañías ISP están bloqueando la web por medio de manipulación del DNS, reinicio de TCP y bloqueo HTTP con el uso de DPI.




La web **www.womenonweb.org** está bloqueada en las siguientes redes: Vodafone (AS12357 y AS12430), Vodafone Ono (AS6739), Orange (AS12479 y AS12715), CSUC (AS13041), MÁSMÓVIL (AS15704), XFERA Móviles (AS16299), Telefónica/Movistar (AS3352). En las siguientes secciones vamos a analizar cómo han bloqueado la web las compañías ISP.

# Manipulación del DNS

Hemos encontrado que las compañías ISP de Orange (AS12715 y AS12479), XFERA Móviles (AS16299), Telefónica (AS3352) y MÁSMÓVIL (AS15704) bloquean el acceso a la web **www.womenonweb.org** mediante la manipulación del DNS.

Las ISP de Telefónica (AS3352) y Orange (AS12715 y AS12479) bloquean la web secuestrando el nombre del dominio y apuntando su DNS (registro A) a la dirección IP `127.0.0.1`. Esta dirección IP es asignada para su uso como la dirección de bucle de retorno del huésped de internet y dichas direcciones IP no deben aparecer en ninguna red y en ningún lugar (de acuerdo con RFC1700).

De forma similar MÁSMÓVIL (AS15704) y XFERA (AS16299) están bloqueando la web secuestrando el nombre del dominio de la web **womenonweb.org** para que apunte falsamente a la dirección IP `192.168.1.254`, que pertenece a un espacio de dirección privado. Típicamente esta es una dirección IP destinada a pequeñas redes privadas en viviendas u oficinas, y nunca deberían ser usadas para servidores de web públicos ni para un servício online puesto que no puede ser dirigido a través del internet público. En cualquier caso esta no es la dirección IP perteneciente a **www.womenonweb.org**.

En estos dos casos de manipulación del DNS, una navegadora que visite la web no recibirá una página de bloqueo ni ninguna información del porqué la web se encuentra bloqueada e inaccesible. Navegadoras que intentan acceder a dicha web procedentes de Orange y Telefónica pueden falsamente entender que hay un problema técnico con la web y no que se encuentra bloqueada por su ISP.

A continuación podemos ver las últimas mediciones de red en todas las ISP, que muestran evidencias del bloqueo de la web mediante la manipulación del DNS.

| ASN | ISP | Web bloqueada | Informe de OONI | Método de bloqueo |
|---|---|---|---|---|
| AS12715 | Orange | www.womeonweb.org | 2020-04-24 17:49:32 | Manipulación del DNS |
| AS12479 | Orange | www.womeonweb.org | 2020-04-25 19:42:54 | Manipulación del DNS |
| AS16299 | XFERA Móviles | www.womeonweb.org | 2020-04-25 15:01:30 | Manipulación del DNS |
| AS3352 | Telefónica | www.womeonweb.org | 2020-02-23 12:33:58 | Manipulación del DNS |
| AS15704 | MÁSMÓVIL | www.womeonweb.org | 2020-04-25 08:17:30 | Manipulación del DNS |
| AS12338 | Euskaltel* | www.womeonweb.org | 2020-05-03 11:10:49 | Basado en DNS* |

***Nota**: Después del período de análisis de abril, recibimos pruebas de OONI de que Euskaltel estaba participando en el bloqueo, junto con quejas de usuarias que confirmaron la sospecha. Lo hemos añadido a las tablas de resumen para la visibilidad sin más análisis*

# Deep Packet Inspection (DPI)

De las muchas técnicas con las que las compañías ISP pueden censurar webs, la "Inspección Profunda de Paquetes" (DPI por sus siglas en inglés) es la base de las formas más avanzadas de censura. Generalmente, las compañías ISP implementan censura manipulando los registros DNS de las webs en cuestión. Sin embargo, algunas compañías ISP usan tecnologías más invasivas para censurar webs: la DPI. La usan con frecuencia para hacer una vigilancia más intrusiva o para interceptar las comunicaciones de red de sus usuarias, lo cual no es posible con una simple manipulación del DNS.

Hay aparatos especiales que tienen la facilidad, no solamente de mirar en la capa 3 o las cabeceras de la capa 4 de la red, sino también mirar en el interior de la carga útil de todos y cada uno de los paquetes. Dichos aparatos pueden distinguir paquetes que van a un servidor y, o bien impedir que alcancen su objetivo, o bien cambiar la respuesta del servidor, o incluso redirigir los paquetes a otro servidor. Estos dispositivos realizan un trabajo hostil y activo de ataque del 'monstruo-en-el-medio' (MITM) en cada uno de los clientes que se conectan a la red a través de ellos.

Durante nuestra investigación hemos identificado 2 diferentes compañías de DPI: Fortinet en la red de Telefónica y Allot en la red de Vodafone. Ambas han sido usadas para manipular activamente el tráfico de red de las usuarias y bloquear las webs de **womenonweb.org**.

## Bloqueo por HTTP

### Visión general de Movistar con Fortinet

Hemos encontrado que AS3352, propiedad de Movistar (una compañía de Telefónica), intercepta la comunicación de sus usuarias para mostrar un sitio web falso que muestra un texto que dice `HTTP 404 error`, es decir, un código de estado de la web para anunciar que la página específica no existe. Sin embargo, esto no es cierto, ya que como podemos observar en las mediciones de control de OONI Web Connectivity, hay datos recolectados al mismo tiempo pero en otras redes, que confirman que la página sí que existe.

Además, dentro del contenido de la página HTML de la respuesta HTTP, podemos ver más pruebas de que esta proveedora de internet está usando DPI para censurar la web **www.womenonweb.org**. Dentro de una sección del código HTML mostrado abajo, encontramos la cadena `FGT_HOSTNAME`, a partir de la cual podemos deducir que esta compañía está usando un producto DPI de Fortinet llamado Fortigate. Esto se ve confirmado por la propia Página de ayuda de Fortinet. Más específicamente, el valor de este campo (`FGT_HOSTNAME`), menciona también lo que parece ser el identificador único de host de la máquina de DPI que ha generado esta respuesta falsificada, `RFFBTB1-01`.

Buscando online este identificador único de host, `RFFBTB1-01`, podemos encontrar una pregunta al servicio comunitario de asistencia de Movistar titulada 'Bloqueo de página web'. Una usuaria en dicho servicio de asistencia de la comunidad de Movistar preguntaba por qué

la web `http://www.argenteam.net/` estaba siendo bloqueada. Leyendo a lo largo del post, pudimos encontrar textualmente la misma página de bloqueo (`ERROR 404 - File not found`) que la encontrada en el bloqueo de la web de Women on Web. Además, la presencia del hostname (`FGT_HOSTNAME: RFFBTB1-01`) en el servicio de asistencia de Movistar sugiere que otras webs están siendo bloqueadas por la red de Movistar con la misma metodología.

Adicionalmente, el mismo tipo de página de bloqueo de Movistar ha sido encontrado en unas mediciones de red de OONI en 2018, mostrando el bloqueo de la web **thepiratebay.org**.

### Página de bloqueo de Movistar con Fortinet

Movistar utiliza la siguiente página de bloqueo para censurar el acceso a la web de Women on Web:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<!--
CATEGORY:
DEST_IP:  67.213.76.19
FGT_HOSTNAME:  RFFBTB1-01
SOURCE_IP:  [REDACTED]
-->
<html>
  <head>
    <title id="3">
      Error 404
    </title>
  </head>
  <body>
    <CENTER>
      <h1>
        ERROR 404 - File not found
      </h1>
    </CENTER>
  </body>
</html>
```

La página de bloqueo completa y la evidencia técnica del bloqueo pueden encontrarse en las mediciones de red de OONI.

Gracias a las mediciones tomadas desde diferentes puntos de observación en la red de Movistar, hemos podido identificar tres páginas de bloqueo casi idénticas con diferentes nombres de host Fortigate, establecidos como `RFFBTB1-01`, `RFFBTB1-02` y `RFFMNO1-01`. Adicionalmente, el título de etiqueta HTML de la página de bloqueo parece ser uno diferente por cada servidor/hostname `id="1"`, `id="3"` y `id="4"`. Según sus estructuras de configuración y sus nombres de hostname son probablemente diferentes servidores DPI operando para la misma ISP.

Comparación en paralelo de las tres páginas de bloqueo devueltas por la herramienta DPI Fortigate de Fortinet. En la línea 6 hay 3 hostnames únicos de Fortigate. Las mediciones de red de OONI que revelan las páginas de bloqueo de Movistar con todos los detalles técnicos se pueden encontrar aquí, aquí y aquí.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD
<!--
CATEGORY:
DEST_IP:  67.213.76.19
FGT_HOSTNAME:  RFFMNO1-01
SOURCE_IP:  [REDACTED]
-->
<html>
  <head>
    <title id="1">
      Error 404
    </title>
  </head>
  <body>
    <CENTER>
      <h1>
        ERROR 404 - File not found
      </h1>
    </CENTER>
  </body>
</html>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD
<!--
CATEGORY:
DEST_IP:  67.213.76.19
FGT_HOSTNAME:  RFFBTB1-01
SOURCE_IP:  [REDACTED]
-->
<html>
  <head>
    <title id="3">
      Error 404
    </title>
  </head>
  <body>
    <CENTER>
      <h1>
        ERROR 404 - File not found
      </h1>
    </CENTER>
  </body>
</html>
```

```
<!DOCTYPE html PUBLIC "-/
<!--
CATEGORY:
DEST_IP:  67.213.76.19
FGT_HOSTNAME:  RFFBTB1-02
SOURCE_IP:  [REDACTED]
-->
<html>
  <head>
    <title id="4">
      Error 404
    </title>
  </head>
  <body>
    <CENTER>
      <h1>
        ERROR 404 - File
      </h1>
    </CENTER>
  </body>
</html>
```

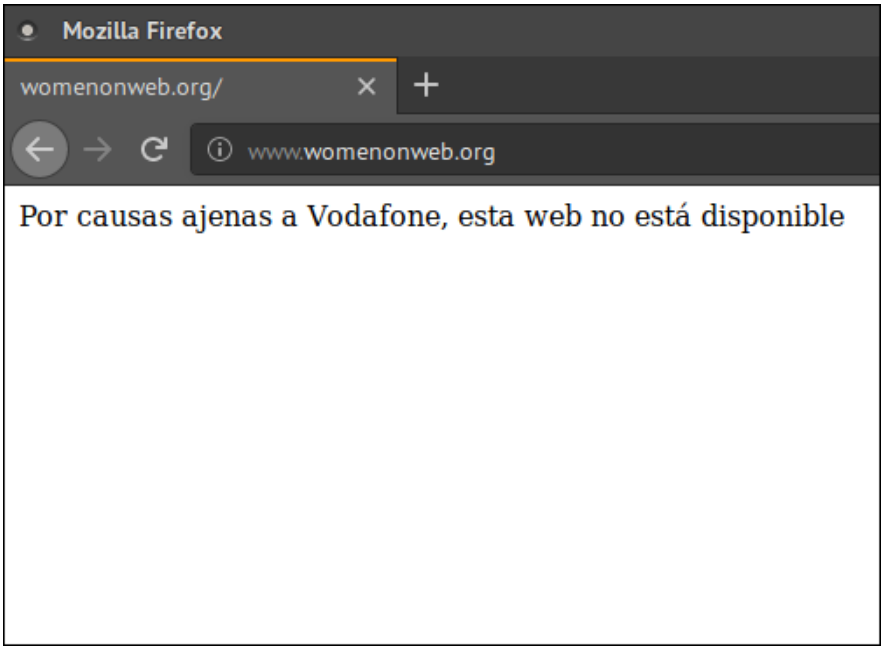
Algunas mediciones de red de OONI del Consorci de Serveis Universitaris de Catalunya (CSUC) revelan la misma página de bloqueo con Telefónica, dado que el CSUC aparentemente utiliza Telefónica como su ISP.

| ASN | ISP | Web bloqueada | Informe de OONI | Método de bloqueo |
|---|---|---|---|---|
| AS3352 | Telefónica | www.womeonweb.org | 2020-04-17 08:31:33 | HTTP blocking (DPI) |
| AS13041 | CSUC | www.womeonweb.org | 2020-02-18 08:34:35 | HTTP blocking (DPI) |

### Página de bloqueo de Vodafone con Allot

A las usuarias de Vodafone ISP (AS12357 y AS12430) se les muestra la siguiente página de bloqueo genérico cuando visitan (la versión HTTP) del sitio web **womenonweb.org**

Esta página de bloqueo es otra indicación de que Vodafone bloquea el sitio web.



## Interceptación de TLS

La proveedora Vodafone (AS12357 y AS12430), igual que Movistar, está usando una técnica conocida en seguridad de redes como “middle-person attack”, o “ataque de intermediaria”.

Vodafone no corta la conexión TLS (Seguridad de la Capa de Transporte) durante el handshake TLS (saludo de seguridad), como hace Movistar. En su lugar, en las redes AS12357 y AS12430 el handshake TLS (saludo de seguridad) se termina y el navegador usuario recibe un certificado falsificado asegurando que pertenece a la web www.womenonweb.org

| ASN | ISP | Web bloqueada | Muestras OONI | Técnica de bloqueo |
|---|---|---|---|---|
| AS12357 | Vodafone | www.womeonweb.org | 2020-04-23 15:20:11 | Interceptación TLS |
| AS12430 | Vodafone | www.womeonweb.org | 2020-04-25 19:41:43 | Interceptación TLS |

Varias muestras de red de Vodafone (AS 12357 y AS 12430) presentan un error de verificación de certificado

`ssl_error: error:14007086:SSL routines:CONNECT_CR_CERT:certificate verify failed`,

lo que indica que es probable que la proveedora haya desplegado una regla de interceptación de TLS en la red para el sitio **www.womenonweb.org**. Este mensaje de error de la librería OpenSSL indica que el handshake TLS, saludo de seguridad, ha terminado y que el cliente no puede verificar el certificado que ha recibido de parte del servidor.

Usando la herramienta de línea de comandos que ofrece OpenSSL para hacer pruebas más detalladas, confirmamos la interceptación TLS para las conexiones al servidor web de Women on Web, condicionada a unos supuestos que especificamos a continuación.

### Certificado TLS falsificado

Una vez establecida la conexión TCP (no vemos un reinicio TCP aquí), el navegador que quiere acceder a la web HTTPS envía al servidor un mensaje de saludo de seguridad TLS del tipo `Client Hello`, como primer paso para establecer un canal cifrado y autentificado. Lo reproducimos aquí con la línea de comandos de OpenSSL:

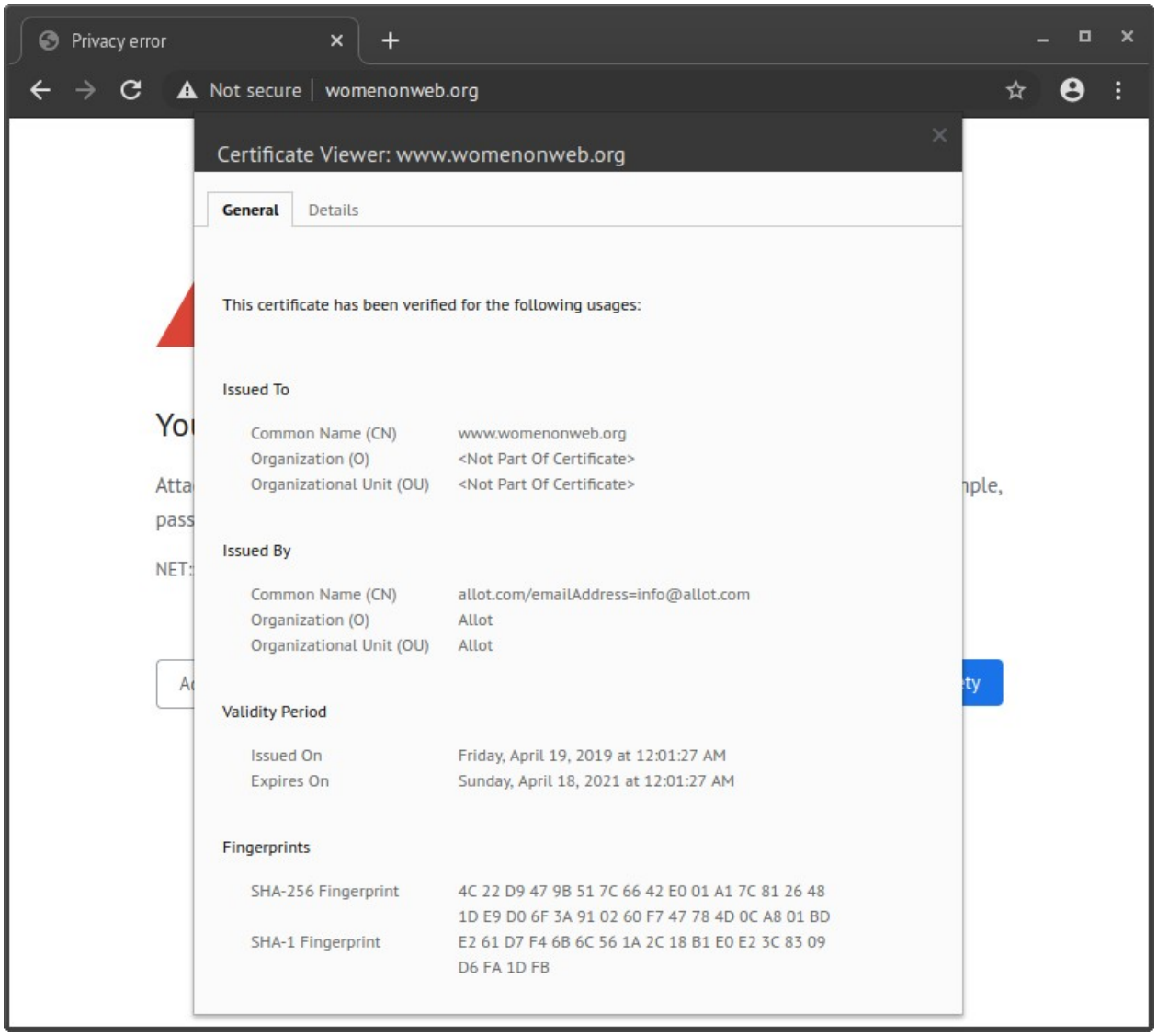
```
> openssl s_client -connect 67.213.76.19:443 -servername www.womenonweb.org  < /dev/null |& egrep
'issuer|subject'
subject=CN = www.womenonweb.org
issuer=C = ES, ST = Madrid, L = Madrid, O = Allot, OU = Allot, CN =
allot.com/emailAddress=info@allot.com
```

Detalle del comando:

1. `s_client`: Usa el cliente TLS integrado
2. `-connect ...`: Conecta a la dirección IP de Women on Web al puerto HTTPS (443)
3. `-servername ...`: Indica el hostname al que queremos acceder
4. `< /dev/null`: Cierra la conexión TLS una vez establecida
5. `|& egrep ...`: Muestra sólo las líneas que contengan los campos `issuer` y `subject` del certificado recibido.

El resultado del comando anterior muestra claramente cómo la respuesta presenta un certificado TLS falseado, asegurando ser válido para **www.womenonweb.org** (campo "Common Name" del `subject`) y emitido por Allot, que de ninguna manera es una Autoridad de Certificación (CA) reconocida.

Como las pruebas de OONI no guardan los certificados TLS que devuelven los servidores, nuestro equipo ha subido el certificado falseado de Allot para su inspección pública. El certificado falsificado ofrecido por Vodafone tiene fecha de emisión del 27 de enero de 2019, un año antes del principio de nuestro análisis de datos que mostraban señales de bloqueo.




## Filtrado por SNI

Un detalle importante del comando de antes es el parámetro `-servername` que añadimos. Controla la extensión de TLS llamada "Server Name Indication" (SNI), que se envía dentro del mensaje de saludo `ClientHello`. Se envía sin cifrar desde el cliente al servidor y su uso previsto es ayudar a los servidores web que alojan más de un sitio habilitado con seguridad (HTTPS) en la misma dirección IP, a poder responder con un mensaje de seguridad `ServerHello` con el certificado correspondiente al sítio pedido, puesto que cada sítio HTTPS puede tener su propio certificado.

Sin embargo, esto también conlleva un riesgo. Como el campo SNI se envía sin cifrar, hay sistemas de censura que lo usan para identificar e interceptar conexiones a los dominios o webs que quieren bloquear. Por tanto, hemos intentado repetir la conexión anterior pero quitando el campo SNI, por medio de la opción `-noservername` de la herramienta de OpenSSL. Es decir:

```
> openssl s_client -connect 67.213.76.19:443 -noservername < /dev/null |& egrep 'issuer|subject'
subject=CN = womenonweb.org
issuer=C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
```

La respuesta abreviada nos muestra un certificado emitido para `womenonweb.org` (nótese la falta de `www.`), y firmado por la Autoridad Certificadora Let's Encrypt. Aunque estas dos líneas son insuficientes para demostrar que el certificado sea válido, lo hemos descargado y comprobado que sí lo es. De hecho, se trata del mismo certificado devuelto por la web `https://67.213.76.19/`, en redes sin bloqueo. Parece que Women on Web tiene configurado como sitio HTTPS por defecto `womenonweb.org`, que solo contiene una redirección a `www.womenonweb.org`. Sería interesante ver qué pasaría si el sitio HTTPS por defecto fuera `www.womenonweb.org`, es decir, el que devuelve el contenido deseado, en vez de el que tiene el contenido.

### Diferencias con el "Bloqueo por SNI"

El SNI es un campo que tiene un valor que va a ser el dominio, por ejemplo `www.womenonweb.org` o `womenonweb.org`. Tal como hemos mostrado, el sistema de DPI de Allot que opera en las redes de Vodafone está usando este campo SNI para filtrar el tráfico. Sin embargo, esto no significa que el bloqueo ocurra en todos y cada uno de los paquetes que empiezan una conexión TLS que contengan un campo SNI con el valor del dominio a bloquear. Por tanto, observamos que en esta situación es un parámetro necesario, pero no suficiete, para que Allot intercepte la comunicación y bloquee efectivamente la website.

En una reciente entrada en el blog de OONI, OONI explicó que en el caso de Irán, cualquier paquete que contenga un valor SNI prohibido estaba siendo bloqueado. Demostramos que no es el caso de Vodafone basándonos en los experimentos con el comando OpenSSL, que se muestran en las siguientes secciones.

Con el fin de comparar, elegimos Wikipedia.org como un conocido servidor web accesible desde España. Necesitamos un servidor web de control que no esté siendo bloqueado, para ver qué pasa si intentamos establecer una conexión TLS con él, pero modificando el SNI para indicar el nombre de host de Women on Web:

```
> openssl s_client -connect wikipedia.org:443 -servername www.womenonweb.org  < /dev/null |& egrep
'issuer|subject'
subject=C = US, ST = California, L = San Francisco, O = "Wikimedia Foundation, Inc.", CN =
*.wikipedia.org
issuer=C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Assurance Server CA
```

El resultado corresponde a una respuesta válida del servidor web de Wikipedia, y por lo tanto, deducímos que el sistema de DPI no ha intercepta la conexión.

De esta y las pruebas anteriores, podemos deducir que sólo los paquetes que se dirigen a ciertas direcciones IP son inspeccionados buscando un nombre de host bloqueado en el campo del SNI.

Vale la pena decir que el experimento que OONI utilizó para la investigación de Irán, llamado *SNI Blocking* (Bloqueo del SNI), no se ajustaba a nuestras necesidades. Colaboramos con los desarrolladores de OONI y probamos una nueva metodología de medición diseñada para reunir automáticamente toda la información necesaria para analizar este escenario específico de bloqueo.

### Variaciones de dominios y subdominio

Por lo que respecta a las redirecciones, tanto la versión HTTP de `womenonweb.org` como la HTTPS, las dos sin el prefijo o subdominio `www.`, no aparecen bloqueadas en las redes Vodafone que hemos analizado. En el caso de HTTPS, no vemos ninguna falsificación de certificado:

```
> openssl s_client -connect 67.213.76.19:443 -servername womenonweb.org  < /dev/null |& egrep
'issuer|subject'
subject=CN = womenonweb.org
issuer=C = US, O = Let's Encrypt, CN = Let's Encrypt Auhority X3
```

Sin embargo, este dominio solo redirige a `https://www.womenonweb.org`, que es, entonces, interceptado.

### Página falsa de substitución

Finalmente, el contenido que Vodafone nos presenta, si aceptamos el certificado falso, es similar pero no idéntico al devuelto en la versión HTTP, que hemos explicado en la sección de bloqueo HTTP, arriba.

La web de sustitución, no cifrada, que nos devuelve si accedemos por HTTP es:

```
 > curl http://www.womenonweb.org
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<META HTTP-EQUIV="Expires" CONTENT="-1">
<html>Por causas ajenas a Vodafone, esta web no est disponible</html>
```

*(hemos añadido saltos de línea para facilitar la lectura)*

Sin embargo, si accedemos por HTTPS, desestimando, con la opción `--insecure`, los errores de seguridad generados por el certificado falso, entonces recibimos:

```
curl --insecure https://www.womenonweb.org
<html><body><p>Por causas ajenas a Vodafone, esta web no est disponible</body></html>
```

Esta simple página web difiere de la primera en que carece de las etiquetas `META`, pero envuelve su contenido en una etiqueta `body`, y abre otra etiqueta `p` interna sin la correspondiente etiqueta de cierre.

## TCP Reset

Un ataque de reinicio de TCP es la forma de manipular y terminar una conexión a internet enviando un paquete de reinicio de TCP falsificado (Wikipedia: Ataque de reinicio de TCP).

Los resultados `response_never_received` (respuesta nunca recibida) y `ECONNRESET` significan que el otro lado de la conversación TCP cerró abruptamente su extremo de la conexión. Indicando un posible ataque de reinicio de TCP.

| ASN | ISP | Web bloqueada | Informe de OONI | Método de bloqueo |
|---|---|---|---|---|
| AS6739 | Vodafone | www.womenonweb.org | 2020-03-08 07:01:48 | Reinicio TCP (`response_never_received`) |
| AS3352 | Movistar | www.womenonweb.org | 2020-04-23 04:36:10 | Reinicio TCP (`response_never_received`) |
| AS3352 | Movistar | www.womenonweb.org | 2020-04-25 22:07:44 | Reinicio TCP (`ECONNRESET`) |
| AS13041 | CSUC | www.womenonweb.org | 2020-02-19 18:57:37 | Reinicio TCP (`response_never_received`) |

Vale la pena mencionar que pruebas posteriores de AS6739 muestran otra estrategia de bloqueo, sistemáticamente a lo largo del tiempo, sugiriendo que entre el 16 de marzo de 2020 y el 24 de abril de 2020, Vodafone cambió de una estrategia más simple a una más complicada, al menos en esta red (AS6739).

# Elusión del DPI

Durante nuestra búsqueda hemos encontrado el artículo Qurium sobre mecanismos técnicos usados para bloquear las webs relacionadas con el referéndum catalán en octubre de 2017. Hemos podido eludir el bloqueo del DPI de la misma manera.

Específicamente el sistema DPI mantiene su estado de sesión durante 10 segundos. Así, retrasando la transmisión de la petición HTTP GET (`"GET / HTTP/1.1"`) podemos eludir con éxito el DPI, ya que la sesión TCP no es rastreada después de 10 segundos. El comando siguiente nos permite eludir el DPI en Vodafone ISP (AS12357 y AS12430) que usa la infraestructura del DPI de Allot.

```
input () {
  sleep 20
  echo "GET / HTTP/1.1"
  echo "Host: www.womenonweb.org"
  echo
  echo
}

input | nc www.womenonweb.org 80
```

Otra estrategia publicada en 2013 por OONI aprovecha el proceso de saneamiento de cabeceras HTTP que realizan los servidores web, en contraste con la falta de éste en los sistemas DPI.

Adaptar el comando previo para explorar esta estrategia también resultó ser un éxito:

```
input () {
  echo "GET / HTTP/1.1"
  echo -e "Host: www.womenonweb.org\t"
  echo
  echo
}

input | nc www.womenonweb.org 80
```

En ambos casos, sobre eludir el DPI, la respuesta es un HTTP redireccionado a HTTPS. Esta es una práctica esperada y un estándar el redireccionar usuarias a la versión HTTPS de **www.womenonweb.org** (en una conexión no censurada):

```
HTTP/1.1 302 Found
Cache-Control: no-cache
Content-length: 0
Location: https://www.womenonweb.org/
Connection: close
```

# Conclusiones

Nuestro análisis técnico de los datos de OONI recogidos por múltiples voluntarias en el periodo del 1 de enero hasta el 30 de abril de 2020 revelan bloqueos sistemáticos de la web Women on Web (**www.womenonweb.org**). Encontramos pruebas de bloqueos en 9 redes usadas por las 5 mayores compañías proveedoras de servicios de internet de banda ancha y móvil en España.

Pudimos verificar el uso de tecnología DPI perteneciente a Fortinet y Allot usadas por Telefónica y Vodafone para bloquear el acceso a la web. Además detectamos 2 tipos diferentes de páginas de bloqueo en las mismas redes.

Basándonos en evidencias a partir de mediciones de red analizadas en este artículo, pudimos verificar el bloqueo de la web Women on Web por medio de la manipulación del DNS, bloqueo de HTTP, interceptación del TLS y reinicio de TCP.

Estos métodos no son de ninguna manera exclusivos de la censura de este sitio web; parecen ser usados de forma rutinaria como muestran los informes regulares publicados por OONI.

# Eludir la censura

Nuestro hallazgos revelan censura en territorio español de la web **womenonweb.org** con manipulación del DNS, DPI, interceptación del TLS, bloqueo de HTTP y reinicio de TCP.

Para los casos de manipulación del DNS puede que consigas eludir la censura y acceder a la web cambiando los resolutores DNS.

Sin embargo encontramos que en algunas redes las compañías ISP han implementado bloqueos de DPI y manipulación de DNS, y en esos casos cambiar los resolutores de DNS puede no ser adecuado para eludir la censura.

Podrás evitar la censura y el bloqueo de la web usando Tor Browser.

# Cobertura previa

- [catalán] Donestech: Censura a l'estat espanyol de la web womenonweb.org
- [castellano] Freakspot: Censura de sitio web de Women on Web en España
- [castellano] Ana: Women On Web

# Agradecimientos


## Contribuyentes y ensayistas

Muchas ideas, desubrimientos y ensayos a través de redes y tiempo deben ser acreditados a:

- Lista de correos del Hackmeeting
- Sala Cafe de la comunidad de SinDominio
- Miembras de la comunidad y del núcleo de OONI
- Calbasi, Benhylau, y muchas, muchas amigas, compañeras, familiares, y testers anónimas.

# Colectivos de apoyo

Este trabajo no habría sido posible sin la infraestructura de apoyo de:

- Sindominio.net
- Autistici.org
- Indymedia.org
- Riseup.net
- Aktivix.org
- Coletivos.org


# Referencias


- Fortinet - Security Profiles
- Movistar community helpdesk
- OONI - Sobre el bloqueo de las páginas web sobre el derecho al aborto: Women on Waves & Women on Web
- OONI - Tab tab, come in!
- OONI - Ensayos de conectividad de web
- Qurium - Técnica de bloqueo en Catalunya
- RFC 1700
- Tor
- Wikipedia - Ataque de reinicio de TCP
- Wikipedia - MITM attack

# Contribuir

En este informe hemos referenciado y enlazado a muestras de OONI tomadas por personas voluntarias. Es importante seguir realizando medidas para poder detectar cambios en las técnicas de censura, nuevos casos, o hasta el levantamiento de bloqueos.

Gracias a las aplicaciones que OONI ha desarrollado, hacer pruebas de conectividad es simple. Para ayudar a hacer el seguimiento de las webs de Women on Web y Women on Waves, clica en este botón y sigue las instrucciones.


# Contacto

**Contacto de grupo:** nobloc(arroba)3msg.es