



Tecnocrática

Centro de datos - SNI y TLS



TECNOCRÁTICA

¿Internet es un mundo feliz?



Suplantación del certificado

Visor de certificados: extratorrent.si

General

Detalles

Emitido para

Nombre común

extratorrent.si

Organización (O)

<No forma parte del certificado>

Unidad organizativa (UO)

<No forma parte del certificado>

Emitido por

Nombre común

allot.com/emailAddress=info@allot.com

Organización (O)

Allot

Unidad organizativa (UO)

Allot

Período de validez

Emitido el

viernes, 16 de diciembre de 2016, 14:07:49

Fecha de expiración

miércoles, 16 de diciembre de 2026, 14:07:49


Huellas digitales de SHA-256

Certificado

416d5cc4c2d6a694bffb2fadf977021a9c24b0a4339c774bb322fcc8f1aac421

Clave pública

42cb3fc1f0ab8a1e446c8a29b16a3d8a3749dc950754730b8d0063056e57111b





Su conexión no es privada.


Es posible que los atacantes estén intentando robar tu información de **extratorrent.si** (por ejemplo contraseñas, mensajes o tarjetas de crédito).

NET::ERR_CERT_AUTHORITY_INVALID

Avanzado

Volver

 No seguro | <https://extratorrent.si>

Contenido bloqueado por requerimiento de la Autoridad Competente, comunicado a esta Operadora

¿Por qué?



Demanda

Juzgado de lo Mercantil nº de Madrid.

Autos:

Demandante: TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U.

Demandado: VODAFONE ESPAÑA, S.A.U., VODAFONE ONO, S.A.U., ORANGE ESPAGNE, S.A.U., MASMOVIL IBERCOM, S.A., EUSKALTEL, S.A., R CABLE Y TELECABLE TELECOMUNICACIONES, S.A.U., LYCAMOBILE, S.L., TELEFÓNICA DE ESPAÑA, S.A.U., TELEFÓNICA MÓVILES ESPAÑA, S.A.U.

SENTENCIA N°.

En Madrid, a

Vistos por mí, J los autos del Juicio Ordinario, procedo a dictar la siguiente resolución.

ANTECEDENTES DE HECHO.

PRIMERO.- Por la representación procesal de TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. se interpuso demanda de Juicio Ordinario contra VODAFONE ESPAÑA, S.A.U., VODAFONE ONO, S.A.U., ORANGE ESPAGNE, S.A.U., MASMOVIL IBERCOM, S.A., EUSKALTEL, S.A., R CABLE Y TELECABLE TELECOMUNICACIONES, S.A.U., LYCAMOBILE, S.L., TELEFÓNICA DE ESPAÑA, S.A.U., TELEFÓNICA MÓVILES ESPAÑA, S.A.U. en fecha

SEGUNDO.- Por decreto se admitió a trámite la demanda, dándose traslado de la misma a la parte demandada para su contestación. En el mismo escrito de contestación a la demanda, la parte demandada se allanó a las pretensiones de la demandante.

Fallo de la sentencia

Vistos los preceptos citados y demas de general y pertinente aplicacion,

FALLO.

Estimo totalmente la demanda interpuesta por la representación procesal de TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. contra VODAFONE ESPAÑA, S.A.U., VODAFONE ONO, S.A.U., ORANGE ESPAGNE, S.A.U., MASMOVIL IBERCOM, S.A., EUSKALTEL, S.A., R CABLE Y TELECABLE TELECOMUNICACIONES, S.A.U., LYCAMOBILE, S.L., TELEFÓNICA DE ESPAÑA, S.A.U., TELEFÓNICA MÓVILES ESPAÑA, S.A.U., por lo que condeno a las demandadas a la siguiente medida de cesación de la actividad ilícita detectada, como medida de protección de los derechos de propiedad intelectual, afines o conexos, en Internet:

Fase 1: Acordar el bloqueo, por los Operadores de acceso a Internet, del acceso a las webs piratas identificadas a continuación en la presente resolución y en el punto sexto de los antecedentes de hecho de la demanda (listado adjunto con la Demanda en fichero txt), en toda su identificación como recurso web (URLs, Dominios, Direcciones IP), y bajo acceso en protocolos HTTP y HTTPS, en el plazo máximo de setenta y dos (72) horas desde la notificación de la Sentencia del presente proceso.

ID Nombre comercial URLs/Dominios ID IP

1 [REDACTED] 1891222/22

h [REDACTED]

1 [REDACTED]

Bloqueos solicitados en la resolución

- URL
- Dominio
- Dirección IP
- Protocolo HTTP
- Protocolo HTTPS



HTTPS - HyperText Transfer Protocol Secure

- El envío de datos mediante HTTPS está protegido mediante TLS (Transport Layer Security) proporcionando:
 - Cifrado
 - Integridad de datos
 - Autenticación
- Necesitamos un certificado

Certificado

- Los certificados tenían la limitación que se no permitían el disponer de varias webs en el mismo servidor, para eso se inventó la extensión de TLS: **SNI (Server Name Indicator)**.
- Gracias a SNI a día de hoy podemos tener certificados para todas las webs sin necesitar usar una IP por web.

Problema de SNI

- Al usar HTTPS el handshake de TLS se realiza antes de la encriptación de HTTPS, así que podemos conocer la web que se va a visitar con HTTPS.
- Conclusión, es posible ver el nombre de la web y por tanto filtrarla.

Ver el server name de SNI

```
▶ Frame 4: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface enp7s0, id 0
▶ Ethernet II, Src: RealtekU_d2:fb:bc (52:54:00:d2:fb:bc), Dst: RealtekU_a6:56:bf (52:54:00:a6:56:bf)
▶ Internet Protocol Version 4, Src: 192.168.150.100, Dst: 31.47.77.63
▶ Transmission Control Protocol, Src Port: 49650, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▼ Transport Layer Security
```

```
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 512
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    Random: 33e28fb580fbe6b98e72f2fda6081a331449eada4c6fd8e79dd01794b3842711
    Session ID Length: 32
    Session ID: 8d6ffeb3332e14cd5bcd5bcb626a84b7cb14fed824936b52efbfd66a1da1c8d9
    Cipher Suites Length: 34
    ▶ Cipher Suites (17 suites)
    Compression Methods Length: 1
    ▶ Compression Methods (1 method)
    Extensions Length: 401
    ▼ Extension: server_name (len=21)
      Type: server_name (0)
      Length: 21
      ▼ Server Name Indication extension
        Server Name list length: 19
        Server Name Type: host_name (0)
        Server Name length: 16
```

Server Name: tecnocratica.net

```
▶ Extension: extended_master_secret (len=0)
▶ Extension: renegotiation_info (len=1)
▶ Extension: supported_groups (len=14)
▶ Extension: ec_point_formats (len=2)
▶ Extension: session_ticket (len=0)
▶ Extension: application_layer_protocol_negotiation (len=14)
▶ Extension: status_request (len=5)
▶ Extension: Unknown type 34 (len=10)
▶ Extension: key_share (len=107)
▶ Extension: supported_versions (len=5)
▶ Extension: signature_algorithms (len=24)
▶ Extension: psk_key_exchange_modes (len=2)
```

Marcado en Mikrotik

not invalid

Enabled ☒

Comment

▼ General

Chain

prerouting ▼

Src. Address ▼

Dst. Address ▼

Src. Address List ▼

Dst. Address List ▼

Protocol

☐ tcp ▼

Src. Port ▼

Dst. Port

☐ 443

Any. Port ▼

In. Interface ▼

▼ Advanced

Layer7 Protocol ▼

Content ▼

Connection Bytes ▼

Connection Rate ▼

Per Connection Classifier ▼

Src. MAC Address ▼

Out. Bridge Port ▼

In. Bridge Port ▼

In. Bridge Port List ▼

Out. Bridge Port List ▼

IPsec Policy ▼

TLS Host

☐ *.tecnocratica.net

Ingress Priority ▼

▼ Action

Action

mark connection ▼

Log ☐

Log Prefix ▼

New Connection Mark

Conexion_SNI ▼

Passthrough ☒

Descarte de tráfico en Mikrotik

not invalid

Enabled ☒

Remove

Comment

Reset Counters

▼ General

Chain

Src. Address ▼

Dst. Address ▼

Src. Address List ▼

Dst. Address List ▼

Protocol ▼

Src. Port ▼

Dst. Port ▼

Any. Port ▼

In. Interface ▼

Out. Interface ▼

In. Interface List ▼

Out. Interface List ▼

Packet Mark ▼

Connection Mark ☐

Routing Mark ▼

▼ Action

Action

Log ☐

Log Prefix ▼

Otras opciones

- ESNI (Encrypted SNI)
 - Tiene que soportarlo ambos extremos y no todos los servidores lo soportan.
 - Sólo soporta el problema del SNI, no vale para ALPN.
- ECH (Encrypted ClientHello)
 - Preferible, de hecho Firefox lo puso en la versión 85 para reemplazar el soporte de ESNI.

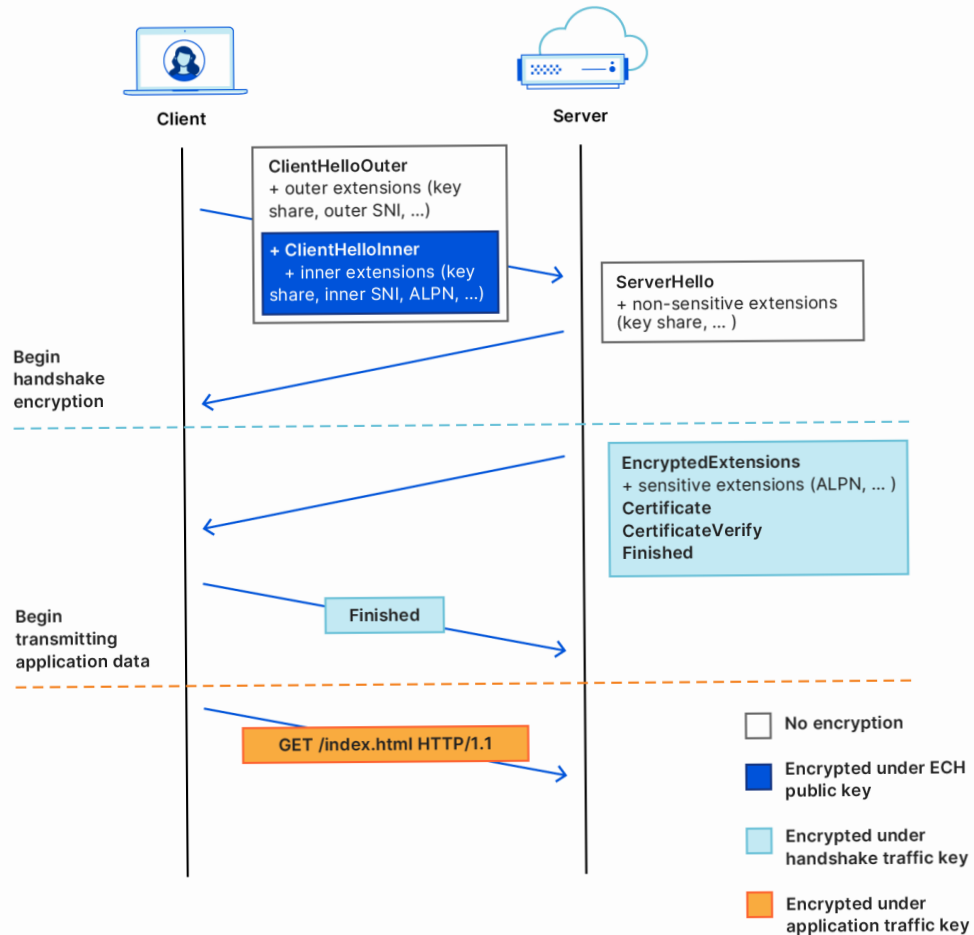
ECH (Encrypted ClientHello)

- El ECH hace que el handshake del TLS se mantenga secreto, y esto solucionaría el problema del SNI, pero no se queda en solucionar el problema del SNI, sino que soluciona todos los problemas generados por la negociación en plano del handshake del TLS.
- La extensión de TLS ALPN que decide qué protocolo superior se usará una vez realizado el handshake de TLS también se solucionaría con el ECH pues ya no se podrá ver en los paquetes al ir encriptada.

Cómo funciona TLS 1.3 sin ECH

- En un primer momento el cliente envía el ClientHello con la clave compartida. En ese mismo mensaje además viaja el SNI y el ALPN entre otros. Todo esto sin cifrar porque no ha habido aún intercambio de claves.
- El servidor contesta con el ServerHello que tiene la clave compartida del servidor. Este mensaje también va sin encriptar.
- A partir de aquí el cliente ya conoce su llave y la del servidor, con lo que ya se puede encriptar porque ya hemos tenido el intercambio de llaves
- El primer mensaje encriptado va desde el servidor al cliente y es el EncryptedExtensions donde se envían los parámetros sensibles del servidor como por ejemplo el ALPN del servidor y por supuesto el certificado.

Handshake de TLS 1.3 con ECH



Muchas gracias





C/ Salvatierra 4, 28034, Madrid, Spain

(+34) 910 059 045

comercial@tecnocratica.net



<https://tecnocratica.net>



<https://twitter.com/TecnocraticaCPD>



<https://www.youtube.com/@TecnocraticaNet>



<https://www.linkedin.com/company/tecnocratica>