¿Se van a quedar mis dispositivos sin internet?

Publicado el El Informatico - 3 de octubre de 2021 -

Imagen de Pixabay cortesia de Pexels

Desde hace unos días han aparecido noticias en todos los medios de todo tipo, augurando un «apocalipsis» en internet debido a que «los dispositivos viejos sin actualizar se van a quedar sin internet». Como de costumbre, **ésto no es completamente cierto**. Y la razón es simple: la prensa aún no comprende lo que es Internet, lo que es la web, ni cómo funciona ninguna de las tecnologías mencionadas.

Si quieres enterarte de lo que pasa y de por qué pasa, entonces échale un vistazo a éste artículo.

Problema número 1: Expira un certificado raíz

Como ya he explicado por encima en otros artículos, la web (término que hace referencia exclusivamente al protocolo HTTP que usamos para conectarnos a los servicios web) utiliza hoy en día una serie de protocolos de encriptación simétricos y verificación que denominamos SSL y TLS. Siendo TLS el sucesor de SSL, y el protocolo que todo servicio web debería usar hoy en día.

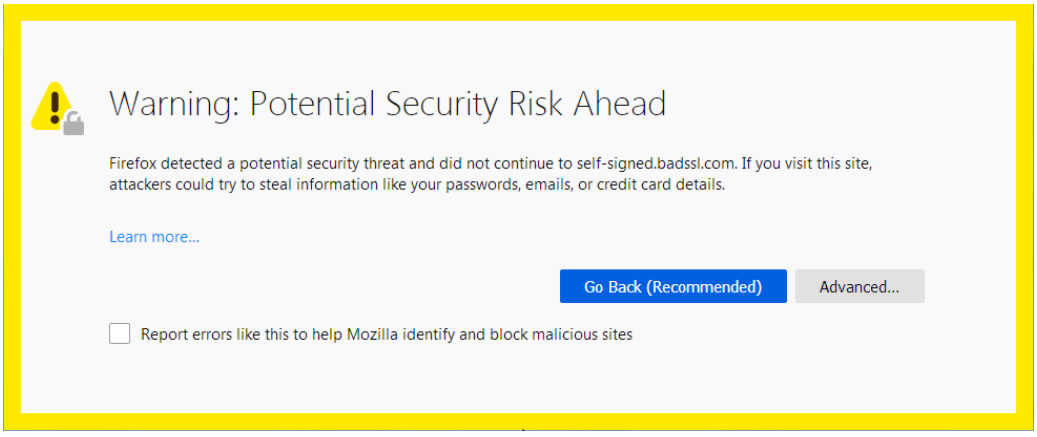
Para que nos entendamos, un protocolo es un *estandard* que establece el modo en el que las computadoras (en éste caso) se comunican entre si. El uso de éstos protocolos no es realmente obligatorio y los navegadores aún conectan a los servicios web que no usen encriptación, pero la idea es que en un futuro cercano no pueda ser así.

El protocolo TLS hace que la comunicación entre dos equipos, en éste caso el servidor web y el cliente (el navegador web) deben cifrar la comunicación intercambiando una **clave pública**. Funciona de la siguiente manera: tanto el emisor como el receptor han generado previamente una clave privada, que no deben compartir con nadie. Mediante un algoritmo matemático, ambos generan una clave pública, que deben intercambiar entre si para poder cifrar la comunicación. Al intercambiar la información cifrada, cada receptor podrá descifrar los paquetes (para entendernos, los mensajes que se envían) con su clave privada. De ésta forma, ningún otro receptor podrá descifrar el mensaje sin esa clave privada.

En el caso de SSL y TLS, la clave pública se envía adjunto a un **certificado**. Este certificado tiene dos finalidades: por un lado, para cifrar la información (como ya he explicado), y por otro **para verificar la identidad del emisor**.

El certificado TLS contiene datos sobre el servicio web asociado al mismo, que se usan para identificarse. Ahora bien, ¿Cómo sabemos que el emisor es quien dice ser? Para verificarlo, existe una figura autoritaria que denominamos **autoridad de certificado** (Certificate Authority, o CA en inglés). Esta autoridad es la autoridad que emite los certificados y además certifica que dichos certificados sean válidos. Por ejemplo, Let's Encrypt, Verisign, etcétera.

Cada vez que conectamos con un servicio web a través de éste protocolo, el navegador verifica que el certificado sea válido comprobando que se corresponda con el dominio asociado, que no haya expirado, y además consulta a la autoridad correspondiente para verificar que el certificado sea válido. De no ser así, el navegador mostrará una pantalla de alerta indicando que el certificado no es válido y que la conexión no es segura.



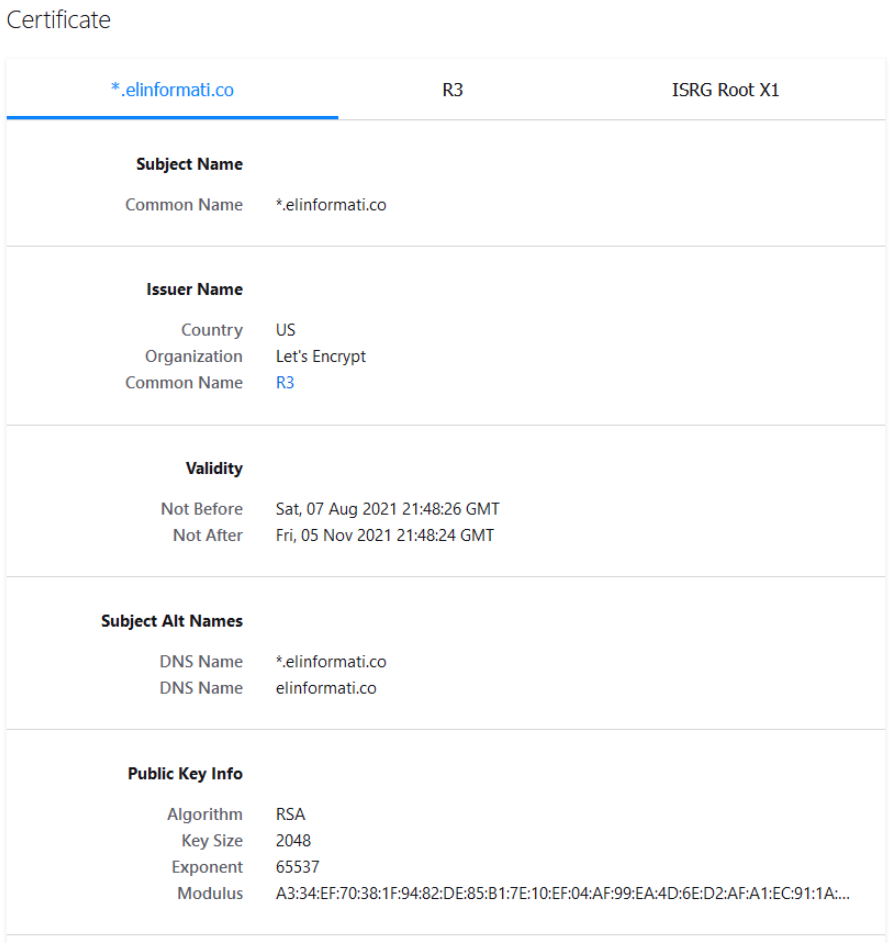
Mensaje de alerta de Firefox indicando que estamos intentando conectar con

una página web cuyo certificado no es válido.

Por seguridad, éstos certificados **tienen una fecha de expiración**, tras la cuál el certificado deja de ser válido. Por éste motivo, es necesario renovar los certificados cada pocos años.

Pero hay otro problema. En el pasado, se daban casos en los que agentes maliciosos llegaban a falsificar certificados de modo que dichas autoridades podían validar certificados maliciosos, o incluso llegando a suplantar a dichas autoridades. Para solucionar éste problema, se crearon lo que se denominan **cadenas de certificados**.

Una cadena de certificados es lo que sugiere el nombre: certificados que certifican a certificados. Un CA genera un certificado, que a su vez sirve para cifrar y verificar que otro certificado sea válido. De modo que un certificado depende, a su vez, de otro certificado.



Cadena de 3 certificados usado por ésta web. Puedes ver ésta información desde la información de certificados de tu navegador.

Esto quiere decir que múltiples certificados dependen de un solo certificado, creando una **cadena de confianza**. Ahora bien, si los certificados tienen fecha de expiración, el certificado raíz también tendrá fecha de expiración, ¿verdad?

Eso es exactamente lo que está pasando: Uno de los certificados raíz,

denominado DST Root CA X3 de Let's Encrypt ha llegado a su fecha de expiración. Lo que quiere decir que todos los certificados que dependieran de éste otro certificado expiran con él. En su lugar, ahora son reemplazados por el nuevo **ISRG Root X1**.

El problema está en la **cadena de confianza**. Los navegadores están diseñados para confiar en éstos certificados raíz. **Esto quiere decir que los navegadores y sistemas antiguos que no estén actualizados no soportarán el nuevo certificado, y por tanto, no podrán conectar con los servicios web que utilicen la nueva cadena de certificados**.

¿Quiere ésto decir que se van a quedar sin internet? Técnicamente hablando, no. **Pero no podrán conectar con ninguna página o servicio que utilice ésta cadena de certificados, incluyendo ésta misma página web**.

Problema 2: Nuevos estándares WiFi

La gente quiere redes inalámbricas más seguras y más rápidas, y los ingenieros quieren redes mejor estructuradas. Por esto, cada cierto tiempo debemos actualizar las tecnologías que usamos para comunicarnos de forma inalámbrica. ya empezamos a hablar de un nuevo estándar WiFi al que llaman **WiFi 6**.

Las actualizaciones de la red WiFi no son nuevas y cada cierto tiempo sacan una nueva versión. Probablemente hayas oído hablar del estándar 802.11ac, o simplemente ac. O los estándares b, a, g, n. Todos éstos estándares se corresponden con las versiones WiFi del 1 al 5, siendo la 802.11ac la actual, y la 6 la que se va a imponer ahora.

¿Quiere ésto decir que los dispositivos que no soporten WiFi 6 se quedaran sin conexión a internet? Tengo que reconocer que de ésto no estoy completamente seguro porque el tema del Wifi 6 me pilla de nuevas, pero **en un principio diría que no**. Y el motivo es simple: **todos los estándares Wifi han sido siempre retrocompatibles**. Esto quiere decir que si intentas conectarte a internet con un móvil de hace 9 años a través de una red wifi 802.11ac, el router o punto de acceso conectará el dispositivo a través de éste estándar sin problemas.

No obstante, ésto sólo te puede afectar si te conectas a través de redes inalámbricas. Si te conectas por red cableada, entonces no te afecta.

¿Qué consecuencias tendrá todo ésto?

Pues que si intentamos acceder a un servicio que utilice una cadena de certificados basada en **DST Root CA X3** no podrán conectar con dicho servicio y mostrará un mensaje de alerta o error al hacerlo.

No obstante, aún podremos conectar con otros servicios que utilicen otra cadena de

certificados que sí se encuentren en la lista de certificados de confianza y que no hayan caducado aún, o incluso a servicios web que no utilicen un certificado (con el consiguiente riesgo, obviamente).

En otras palabras: **no**. **No va a haber apagón de internet** (Siempre y cuando el precio de la luz no lo permita). Pero si es cierto que los dispositivos antiguos que no tengan actualización o soporte **no podrán conectar con muchos servicios web**.

ANTERIOR

Houston, tenemos un problema energético en Europa... y es grave.

SIGUIENTE

Diferencias entre Internet y La Web. ¿Qué es cada uno?

Entradas Recientes

- La memoria del ordenador, a fondo
- Operaciones lógicas (Lógica booleana) y Bit Shifting
- Historia de los medios de almacenamiento digitales
- Sistemas de numeración usados en la tecnología digital
- Bits y bytes. Cómo funciona la información digital.
- Desinformación, Bulos, Fake News y manipulación de la información

Categorías

Actualidad | Android | Básicos | Ciberseguridad | Clima | Criptografía | Emulación / Virtualización | FOSS | Hacking | Hardware | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS

Inicio
Catálogo
PDFs
Manuales
Política de privacidad
Política de Cookies
Acerca de mi
Acerca de ElInformati.co