Aviso a navegantes: HTTPs implica seguridad, no legitimidad

El escenario actual a nivel de comunicaciones privadas es muchísimo más halagüeño que hace unos cuantos años. Gracias a proyectos como Let's Encrypt es posible que cualquier página web cuente con una conexión SSL que asegura, entre otras cosas, que todo lo que llega y sale de ese servidor se trabaja de manera cifrada. Todo lo que entra y sale, ojo, que lo que se haga dentro de sus fronteras es otro tema.

Pablo F. Iglesias, Analista de información en PabloYglesias.com y CTO en la consultora SocialBrains @PYDotCom

El problema es que durante años hemos educado al usuario a diferenciar URLs fraudulentas por un elemento que no implicaba legitimidad, sino garantías de seguridad.

E incluso, si el propio administrador no lo ha habilitado tenemos de cara al cliente extensiones como HTTPs Everywhere. Herramientas que por supuesto no ofrecen las mismas garantías (sin ir más lejos, nuestro ISP puede ver el hostname, ya que éste se comparte en texto plano), pero que son un acercamiento a agradecer.

Esto es un paso necesario a la hora de dotar al usuario de su legítimo derecho de comunicarse de manera privada. Gracias a la paulatina migración de los servicios digitales a conexiones SSL, y aunque sea debido a la presión que ejercen autoridades como Google mediante su sistema de rankeo en el buscador (HTTPs lleva ya meses siendo un factor más de los cientos que considera Google a la hora de posicionar una página, y previsiblemente acabará siendo tan importante como lo es a día de hoy el que esa web tenga versión para móviles), las operadoras pueden saber que estamos consumiendo tráfico de X tipo, que nos conectamos desde X lugar y que navegamos por X páginas, pero no qué hacemos en ellas. Y esto, viendo cómo se están poniendo las cosas por EEUU, es una gran victoria.

Pero tiene dos handicaps principales:

- Se discrimina a aquellos servicios que quizás han sido abandonados o que preferirían seguir siendo lo más descentralizados posible. Firmar un SSL lo puede hacer cualquier administrador de sistemas. El problema es que para que esa firma sea aceptada por la amplia mayoría de navegadores y filtros anti-phishing, tiene que venir firmada por una autoridad conocida. Y solo hay unas cuantas a nivel mundial. En la práctica ofrecemos mayores garantías al usuario a cambio de aceptar una suerte de dependencia extra hacia X organismos. Y puesto que conforme más pase el tiempo más necesario será que un servicio digital ofrezca SSL como conexión por defecto, realmente estamos discriminando a aquellos proyectos que aunque quizás sigan teniendo valor en la sociedad, estén abandonados, y otros que por principios no quieran pasar por el aro. Renovarse o morir, ya sabes...
- El segundo, que es en el que nos centraremos, es que implementar un SSL no significa dotar a la página de una suerte de identificación verificada, sino simplemente de una verificación de conexiones seguras. Hace unos años, cuando las entidades certificadoras se contaban con los dedos de las manos, el sistema de verificación era muchísimo más estricto, por lo que aunque a veces hubiera errores, podíamos considerar que toda web que tuviera un candadito verde en la barra de URLs era, además de segura, la legítima. Actualmente, con la proliferación de proyectos como Let's Encrypt, que además de gratuito autofirma los SSL, no existe tal validación. Actualmente no podemos de una manera visual inmediata decidir si una web con SSL implementado es la legítima o no. Solo que en efecto estaremos compartiendo datos con ella de forma privada.

Verificación no implica identidad

El mejor ejemplo lo tenemos en la imagen que acompaña a estas palabras. **Ver Imagen 1**

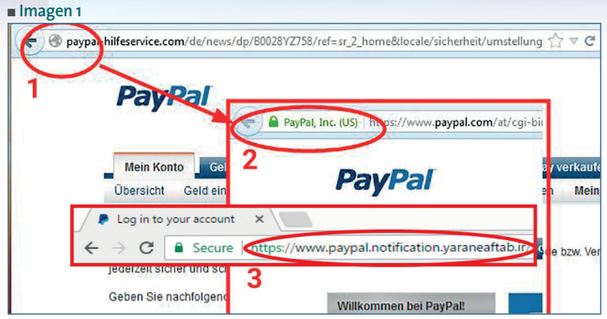
1. En el primer punto tenemos un caso típico de phishing que utiliza la interfaz de PayPal para robar credenciales a la víctima. La página tiene una URL que no es paypal.com, y además no cuenta con un SSL habilitado (ese iconito de la bola del mundo que dentro de poco será sustituido por un "No Seguro").
2. En el segundo tenemos una conexión hecha a PayPal. La url si es paypal.com y viene firmada por un SSL que además identifica a la compañía (PayPal Inc). Esta página es la legítima, y no cabe duda alguna de ello.
3. En el tercer caso tenemos una campaña de phishing reciente, semejante a la primera, pero que además si viene firmada con un SSL. La URL por supuesto no es paypal.com (no podría serlo), pero aparece el candadito verde y Chrome muestra un "Secure", que previsiblemente engañará a la mayoría de víctimas.

El problema entonces no es que Chrome, Firefox, Safari o IE estén haciendo mal las cosas. El problema es que durante años hemos educado al usuario a diferenciar URLs fraudulentas por un elemento que no implicaba legitimidad, sino garantías de seguridad. Y aquellos que se hayan quedado con la copla son ahora víctimas potenciales de nuestro error.

Recientemente, sonaban todas las alarmas por la acusación de Google hacia Symantec (una de las entidades certificadoras) de que ésta habría firmado miles de certificados que estaban siendo utilizados por la industria del crimen. Symantec ha respondido que más que miles habían sido 127, que los tiene fichados, y que quien esté libre de pecado que tire la última piedra.

Además, una investigación realizada por Vincent Lynch de The SSL Store sacaba a relucir el problema que he comentado. Let's Encrypt está sirviendo a la industria del crimen para auto-firmar campañas de phishing sin tener que pasar por las entidades certificadoras tradicionales (entre ellas, la propia The SSL Store). Según su estudio, el 96,7% de los certificados fraudulentos que utilizan la palabra "PayPal" vienen de Let's Encrypt. Cerca de 15.000 páginas fraudulentas que pululan por la red firmadas. Y lo mismo ocurre con otras expresiones como "AppleID" o "Facebook".

■ Imagen 1



Actualmente no podemos de una manera visual inmediata decidir si una web con SSL implementado es la legítima o no. Solo que en efecto estaremos compartiendo datos con ella de forma privada.

Si bien en el caso de Symantec si se debe a un error, en el de Let's Encrypt no, sencilla y llanamente porque la organización no está obligada a verificar el dominio ni su contenido. Según el Internet Security Research Group, a los emisores de certificados no les corresponde incorporar protección contra phishing. Su papel es solo ofrecer garantías de privacidad en las comunicaciones.

Exigir lo contrario, por si se lo pregunta, es además utópico. Estos emisores no tienen la capacidad ni los recursos para realizar este tipo de verificación. Volviendo a Let's Encrypt, lo único que hacen es comparar las peticiones con la base de datos de Google Safe Browsing. Pero claro, en este listado solo aparecen los casos de phishing que ya están en funcionamiento, no los nuevos, que son los que un cibercriminal va a querer firmar.

Así que en estas estamos. Pagando el pato de haber utilizado un elemento que definía otra cosa como apaño para educar al usuario. El candado verde nunca ha significado legitimidad, pero es ahora cuando, gracias a la democratización del SSL, más lo estamos notando. ●