



En las fuentes del 'phishing'

Las últimas tasas de crecimiento de ataques de 'phishing' a las identidades activas en la Red y su investigación, parecen indicar que en esta ocasión no estamos frente a desarrolladores individuales de virus, gusanos o troyanos, que trabajan para la mayor gloria de su enfermiza vanidad, sino que, en este caso, hay asociaciones, conjuntos de personas que se ponen de acuerdo para reunir distintas prácticas y tecnologías informáticas (spam, troyanos, *spyware*, *root-kits*, servidores ligeros, etc.) para cometer timos y estafas a gran escala e indiscriminadamente.

Lo curioso de esta situación es que el *phishing*, al tratarse de un ataque con robo de identidad y suplantación, no es una acción que requiera de sofisticadas herramientas y escasos o profundos conocimientos informáticos. Como todo el mundo sabe, el *phishing* consiste en suplantar la identidad de un servidor (de banca electrónica, por ejemplo), y hacer que los auténticos clientes de ese servicio se relacionen con él sin detectar la suplantación. En esta peligrosa e inadvertida relación, el cliente (la víctima) pronto desvelará todos sus identificadores extrínsecos (secretos) y, con ello, ya tenemos servida una exitosa duplicación y robo de identidad.

Los primeros procedimientos de ataque por *phishing* fueron los de mimetizar la estética de instrumentos originales (correos-e con logotipos y estilos de redacción adecuados) pero hoy hay ya suficientes defectos en los equipos de los sistemas utilizados por los clientes (en aplicaciones, en el sistema operativo, en la configuración, en el uso del sistema, etc.) como para hacer prácticamente invencibles los ataques por *phishing* que utilicen el *cross-site-scripting*, troyanos, *key-loggers*, capturadores de pantalla, etc. La idea del *phishing* avanzado es sencilla: para permitir una suplantación de identidad perfecta lo que hay que hacer es colocarse entre el cliente y el servidor auténticos, y escuchar pacientemente la conversación entre ellos. Esto quiere decir dos cosas: 1) que el sistema de autenticación que están siguiendo el cliente y el servidor puede "aprenderse", y 2) que la autenticación no es mutua.

Los sistemas actualmente en explotación utilizan identificadores extrínsecos, como son los nombres de usuario y las palabras o frases clave, para autenticar a los clientes que quieren acceder al servicio; pero, realmente, en estos casos el servicio no se autentica frente al cliente. Al

De manera ostensiblemente creciente, los servicios de banca electrónica, de subastas, de comercio y administración electrónica, etc, están siendo diana de los denominados ataques de *phishing*, y las posibilidades reales de defenderse de las últimas versiones parecen ser pocas. Conviene no olvidar que la esencia del *phishing* es la falta absoluta de autenticación real en los sistemas en explotación en Internet, por lo que esta plaga la han traído aquellos mismos que diseñaron y pusieron en pie los sistemas hoy amenazados.

no ser mutua la autenticación, lo que siempre se puede hacer es: primero, suplantar al servicio auténtico para que el cliente nos entregue inadvertidamente su genuina identidad y, después, suplantar al cliente frente al servicio auténtico y dejarle "con una mano delante y otra detrás". De siempre, los únicos sistemas aceptables de autenticación son los de autenticación mutua (y simultánea), al estilo del "santo y seña" de los escenarios bélicos. Además de esto, todavía quedaría el serio problema de que la identidad pueda "aprenderse", y eso es consecuencia directa de que los identificadores usados sean extrínsecos y no cambien ni con el tiempo ni con la transacción.

La no autenticación mutua y el uso de pruebas de identidad inmutables son la esencia sobre la que se construye el *phishing*, por lo que hay que entender este fenómeno como algo inherente al sistema de autenticación elegido, y que está en explotación hoy en día.

La necesidad de que el servicio se autentique frente al cliente es algo que algunos ya han entendido, y han recurrido a los certificados digitales y demás parafernalia PKI. Sin embargo, y debido a cómo se ha hecho la implantación de la tecnología basada en certificados digitales en los servicios comerciales, esos certificados digitales no impiden el *phishing* tal y como han puesto en evidencia los ataques más recientes a VISA¹. Dado que es el software cliente el que tiene que participar y verificar todos los pasos de protocolos de comunicaciones seguras como el SSL, basta con alterar dicho software en la máquina del cliente y con ello el atacante puede conseguir engañar hasta al usuario más versado en estos temas.

Las entidades que pretenden hacer negocios en ámbitos tan inhóspitos, anárquicos e inseguros como Internet deberían prestar más atención, interés y empeño en proteger y divulgar sus propias identidades digitales. El hecho de usar certificados VeriSign (o cualquier otro) por el hecho de que sus raíces están preinstaladas en muchos navegadores —lo que hace que se veri-

fiquen automáticamente las cadenas de confianza que terminan en esa raíz—, lo único que ha conseguido es mantener al usuario humano muy lejos de temas tan importantes como son los de la autenticidad y la identidad, por lo que no es de extrañar que ahora estemos hablando de robos de identidad como herramientas útiles de ataque.

El *phishing* es una consecuencia de la asimetría que existe entre corporaciones y clientes individuales. Los diseñadores y los que ponen en pie los sitios Web de bancos y corporaciones de todo tipo siguen creyendo que ellos son "grandes" y que son los "pequeños" (clientes) los que tienen que demostrar poder hacer lo que solicitan a través de su identificación. Si esos bancos y corporaciones no hacen todo lo posible para identificarse con toda seguridad ante cualquiera, sus marcas, logotipos e identidad en general serán de dominio público y podrán ser usurpados por cualquiera y, en ese caso, el *phishing* está servido y es invencible, ya que un cliente nunca podrá estar seguro de estar en contacto con el servidor correcto. Además de controlar seriamente su identidad, las entidades preocupadas por que se pueda practicar el *phishing* entre sus clientes, deberían abandonar sistemas "no mutuos" de autenticación, como es el caso de las combinaciones usuario/contraseña. Si el web de un banco nos pide un identificador y un número secreto para probar que nosotros somos quienes decimos ser, ese web también debería presentar al usuario un identificador y un secreto que sólo el banco y el cliente saben.

Además de equilibrar la autenticación, los valores probatorios que intercambian el cliente y el servicio web deberían cambiar con cada uso, con el tiempo y con la identidad de que se trate. De este modo, cualquiera que pudiese colocarse "en medio" de las comunicaciones entre el cliente y el servicio web no aprendería ningún secreto útil por ser testigo de esas conversaciones. Este tipo de autenticación mutua y de un solo uso **no requiere sofisticados criptosistemas asimétricos** al estilo

de los empleados en el mundo PKI, sino que se pueden implementar con cualquier buen cifrador simétrico, con un buen generador de números pseudo-aleatorios y siguiendo una correcta gestión de claves simétricas. Ahora bien, estos cálculos no los va a hacer el cliente

humano de cabeza, por lo que tendrá que realizarlos una maquina en su nombre. Si esa aplicación se almacena, invoca y ejecuta en el mismo PC del cliente, entonces tenemos otro problema que es el de **controlar la integridad de esa aplicación antes de ejecutarla**.

Lo más conveniente es que la aplicación encargada de autenticar al cliente se ejecute en un hardware específico y dedicado a ello, y que pueda acompañar al cliente a cualquier sitio al que vaya. Un ejemplo de ese hardware lo son las muy mentadas tarjetas inteligentes cuyos precios, cuando sólo realizan operaciones criptográficas simétricas, son bajos, por lo que se descartarían justificaciones económicas para no utilizarlos.

Con el advenimiento del *phishing* se pone de manifiesto un viejo problema informático bastante universal y es el de cómo poder estar seguros de que la máquina, el PC que usamos, realmente manda, recibe, procesa o almacena lo que nos muestra en la pantalla. En general no podemos estar seguros de nada a menos que esa máquina tenga correctamente controlada la integridad y la autenticidad del sistema operativo en ejecución, y de todas las aplicaciones involucradas en el servicio que pretendemos proteger. Cualquier otra cosa es hacer suposiciones infundadas al estilo de las que son las fuentes del *phishing*. Por ello, es preciso que los equipos de los clientes cuenten con algún sistema de control de integridad de las aplicaciones que se ejecutan y, además, su gestión debe ser, en todo momento, la correcta.

En un sistema bien diseñado e implementado desde el punto de vista de la seguridad, el *phishing* nunca hubiese sido posible. Así pues, que cada cual coja su parte de responsabilidad en este asunto y se ponga manos a la obra para hacer que, cuanto antes, el *phishing* sea, simplemente, una lección ejemplar más. ■

JORGE DÁVILA MUÑOZ
Director
Laboratorio de Criptografía
LSIIS – Facultad
de Informática – UPM
jdavila@fi.upm.es

¹ Ver <http://www.antiphishing.org/phishing_archive/12-14-04_VISA/12-14-04_VISA.html>