
Sexo, troyanos, y phishing

Ya lo decía Nietzsche, "el sexo es una trampa de la naturaleza para no extinguirse". Ahora son los phishers los que están utilizando esta trampa como reclamo para infectar a los usuarios con troyanos y capturar sus claves de acceso a la banca electrónica.

El phishing tradicional se presenta en forma de correo electrónico simulando provenir de la empresa suplantada, la mayoría de las veces una entidad financiera, e instando al usuario con cualquier excusa a introducir sus claves en un formulario que realmente envía los datos al phisher.

Aunque simple, llega a ser efectivo. El hecho de que continúen con esa estrategia lo demuestra por si sólo, sin necesidad de contar con estadísticas o datos concretos de incidentes reales, tema tabú por otro lado.

Dejando claro que el phishing tradicional es un tema importante, que mueve mucho dinero, no es menos cierto que en muchas ocasiones es más el ruido que las nueces. Ruido que suele traducirse en daño a la imagen corporativa, publicidad negativa difícil de cuantificar, si bien no son pocas las veces que ese efecto colateral supera a la pérdida directa del ataque, ya que el phisher no obtiene ningún resultado.

Por una causa u otra, en ocasiones por ambas, el phishing tradicional es sin duda temido y bien conocido. Sin embargo, pese a su popularidad, no es ni el único ni, tal vez, el método más efectivo de ataque que utilizan los phishers. Existe una amenaza oculta, casi fantasma, de la que apenas se tienen datos globales, y que lleva ya tiempo siendo explotada de forma efectiva por los phishers: troyanos.

A diferencia del phishing tradicional, los troyanos permiten diversidad de ataques una vez la máquina del usuario está comprometida. El phishing tradicional es efectivo en el caso de contraseñas estáticas, requiere que el usuario se crea que el e-mail fraudulento proviene de su banco, y que meta las claves en una página cuya dirección no corresponde a la web de su entidad. Amén de que son rápidamente detectados y su desactivación varía entre pocas horas y, en el peor de los casos, algunos días.

Por su parte, los troyanos pasan mucho más desapercibidos y pueden capturar los datos sin levantar sospechas al usuario, no necesitan exponerse al conocimiento público a través de un spam, y su esperanza

de vida es mucho mayor, suelen descubrirse semanas o meses después de haber iniciado su actividad.

Además, los troyanos no tienen las limitaciones de una página web falsa y pueden burlar las protecciones más habituales. Un troyano puede capturar tanto las pulsaciones de teclado, como pequeñas áreas de pantalla alrededor del cursor en el caso de teclados virtuales, o capturar los datos del formulario en claro, antes de que el navegador lo pase por SSL. Pueden modificar las páginas que la web del banco presenta al usuario, o los datos que el usuario envía al servidor seguro de la entidad, llevar a cabo ataques tipo hombre en medio, vulnerar los sistemas basados en clave única, tokens, SMS, DNI electrónico, etc.

Una vez una máquina está comprometida, no se puede garantizar la seguridad de una transacción realizada a través de ella.

En el laboratorio de Hispasec llegamos a analizar más de 50 muestras diarias distintas de troyanos bancarios, que son enviadas al servicio VirusTotal. Distinguimos principalmente dos escuelas, internamente las denominamos rusa y brasileña, que difieren bastante en la estrategia, técnicas utilizadas, y programación.

Si bien, además del fin común que persiguen (robar claves de acceso a la banca electrónica), hemos encontrado otro punto en común que suele aparecer con asiduidad en ambas escuelas: el sexo como reclamo para infectar usuarios.

El sexo es un tema utilizado recurrentemente en ingeniería social (término utilizado en seguridad informática a las técnicas para engañar al usuario), así como otras temáticas mucho más románticas. No olvidemos el famoso "iloveyou", gusano que hiciera aparición en mayo de 2000, y que se propagó por todo el mundo gracias a que pocos se resistieron a abrir una supuesta carta de amor que llegaba a su buzón de correo.

En el caso de los troyanos bancarios que nos ocupa las temáticas suelen ser menos románticas y más explícitas. Pueden llegar adjuntos en un e-mail como una supuesta foto algo subida de tono, hasta ahora siempre de una fémina, o un mensaje, tipo spam, que nos invita a visitar una página con contenidos para adultos.

En ambos casos, y como norma general, el usuario logra visualizar el contenido que esperaba, lo que minimiza las sospechas de que algo irregular ha ocurrido.

En el caso de los adjuntos el archivo suele ser un ejecutable, con la extensión real ofuscada y que aparece representado en Windows con el icono utiliza para los formatos gráficos. Al ser abierto el ejecutable muestra la esperada foto, pero al mismo tiempo que el usuario se recrea en su visualización, de forma oculta, el troyano es instalado en su sistema.

En la otra variante ampliamente utilizada, la del mensaje que incita al usuario a visitar una página, también se muestran los contenidos adultos. En esta ocasión la página web suele incluir además algún exploit que aprovecha vulnerabilidades conocidas del navegador, la mayoría de veces contra Internet Explorer por ser el que mayor cuota de mercado tiene y por tanto, a priori, augura mayor número de infecciones al atacante.

En el caso de que el usuario no mantenga su sistema actualizado con los últimos parches de seguridad, el troyano es descargado e instalado en su sistema de forma oculta mientras visualiza el contenido adulto.

Algunos ejemplos de los contenidos utilizados por los últimos troyanos pueden encontrarse en: http://blog.hispasec.com/laboratorio/118

Las recomendaciones para prevenir este tipo de infecciones son básicas, por un lado debemos ignorar todos los mensajes de spam, no abrir sus archivos adjuntos ni visitar sus enlaces, directamente borrarlos. Las soluciones antispam también minimizarán el riesgo de recibir este tipo de mensajes.

Por otro lado es fundamental que mantengamos el sistema operativo puntualmente actualizado con los últimos parches de seguridad. Especial atención a disponer de la última versión de nuestro navegador. En el caso de Windows, sistema al que de momento se dirigen este tipo de troyanos, se recomienda activar las actualizaciones automáticas y/o visitar periódicamente el sitio http://windowsupdate.microsoft.com

Un buen antivirus también será de gran ayuda para prevenir estas vías de infección y otras estrategias de distribución seguidas por los troyanos bancarios y el resto del malware.

Como hemos visto, en el terreno virtual también es necesario tomar una serie de precauciones para disfrutar del sexo de forma segura. Por terminar como empezamos, con una cita, debemos ser más críticos con lo que nos ofrecen en Internet y no dejarse ofuscar como Woody Allen, que llegó a decir, "Solo existen dos cosas importantes en la vida. La primera es el sexo y la segunda no me acuerdo".

EVENTO:

Los días 8 y 9 de Junio se desarrollara el 3 ***Congreso Internacional en Sistemas e Informática*** en la **Escuela Politécnica del Ejército,** sede Sangolquí.

En este evento se trataran las últimas tendencias en desarrollo de software, seguridades informáticas y tecnologías de redes de computadoras.

Para mayor información escriba a:

fgalarraga@espe.edu.ec , gnacato@espe.edu.ec , adelatorre@espe.edu.ec

Telf: (593-2) 2338831 ext 2621

NOTA DEL EDITOR

La seguridad informática es algo que podemos fácilmente remediar, por tanto no nos debe enojar y más bien debemos trabajar para evitar ser una victima mas. En caso de haber sido ya victimas del hurto informático es algo que ya no podemos remediar, es decir tampoco nos debe enojar.

Conclusión: es nuestra decisión prevenir a tiempo las perdidas que podemos sufrir por efecto de la cyberdelicuencia y no buscar culpables en caso de que suceda.

Saludos cordiales,

Arturo de la Torre