

BE GONE PHISHING
(CA magazine, december 2007)
Traducción para Veritas del Colegio de
Contadores Públicos de México
por Antonio Berges

NO SE CREA USTED TAN LISTO

** Richard DeBruyne y Denis Posten*

Justamente cuando usted piensa que es muy inteligente para que le hagan un fraude en Internet, ya viene en cambio la próxima generación de ataques en grande.

La incidencia de fraudes basados en Internet no es nada nuevo, pero viene creciendo a un porcentaje sorprendente. Uno de tales fraudes que esta plagando el mundo de los negocios y la tecnología es el llamado (phishing).

A pesar de tan raro nombre, se trata de un fraude con malas intenciones perpetrado por bandas internacionales de delincuentes organizados y de delitos multimillonarios que sigue en aumento, a pesar de ser algo conocido y de los intentos que se hacen para detenerlo.

Es un tipo de correo electrónico (e-mail) que luce como emitido por un proveedor legítimo y que pide al usuario de computadores actualizar su información personal y financiera. De hecho, se trata de un intento para obtener información personal de alguien que pueda usarse para acceder a una cuenta bancaria, tarjetas de crédito o para asumir la personalidad de alguien con otros propósitos.

Resulta fácil pensar que las personas capturadas en esas redes deben estar muy próximas a ser víctimas de un fraude tan malvado. ¿podría alguien pensar honradamente en haber ganado una lotería en África del Sur o heredado millones de algún pariente desconocido largamente olvidado?

¿Quién en su sano juicio podría aceptar esos lasos llenos de errores ortográficos y de proporcionar a continuación los números de su cuenta de banco, de tarjetas de crédito y los números pin además de la información personal que le están pidiendo en estos fraudes?

Pero los fraudes phishing están llegando por correo electrónico de múltiples formas.

Pesca de Incautos

Aunque el phishing ha venido operando por mas de una década, actualmente es mas sofisticado. Los delincuentes lo han llevado al nivel próximo usando tecnología avanzada. Su objetivo es circunvenir la desconfianza de la actividad en línea, alineando los fraudes a nuestros elevados estándares y expectativas.

Un phishing atractivo

Si usted piensa que puede detectar un falso website, se esta engañando a si mismo. Los website falsos se han vuelto técnicamente eficaces y estéticamente correctos. Puede ser virtualmente imposible para usted distinguir un sitio real de uno falso. Hay herramientas de programación sofisticada, tal como el Juego Rock Phish, que permite a los delincuentes duplicar exactamente el aspecto y sensación de websites legítimos con muy poco esfuerzo.

Unas pocas modificaciones al código original proporcionan un sitio que tiene cada función del original y aun pasar a través del sitio original. De esa forma, cuando usted quiera examinar las locaciones de sucursales de un banco, la información estará ahí. Sin embargo, unas pocas funciones clave del sitio falso habrán sido alteradas para capturar la información financiera de alguien y enviarla al delincuente para que lo estafen.

No caiga en la trampa

Sabiendo que los usuarios de Internet suelen ser muy precavidos ante los fraudes, los perpetradores de los mismos pueden personalizar sus ataques usando información personal robada o disponible al escoger a sus victimas.

Esta ("pesca con arpón") proporciona un falso sentido de autenticidad por que el defraudador conoce algo sobre la persona.

Otro método es secuestrar relaciones de confianza que ya existen.

Las mayores y bien conocidas maquinas de búsqueda han experimentado incidentes donde los delincuentes o bien han pagado por enlaces publicitarios o manipulado sus jerarquías para poder atraer a personas a websites ilegítimos diseñados para robar números de tarjetas de crédito u otra información.

También, websites legítimos han quedado comprometidos y sean alterado sus anuncios u otros contenidos con enlaces de contenido específico. De esta forma, un sitio de confianza puede haberse vuelto malo sin ninguna advertencia o conocimiento sobre el mismo.

Nuevamente, los enlaces han sido inapropiadamente alterados y se convierten en una fuente de mala información que conducen al usuario a un sitio falso para capturar su información personal.

¿Qué puede usted hacer para protegerse? Desarrolle una desconfianza saludable de los enlaces a los websites. Si usted se traslada a un sitio para realizar actos de comercio o proporcionar información privada, siempre registre cuidadosamente su URI o use una marca de libro que usted haya creado cuidadosamente. El punto básico es que cualquier enlace en línea deberá considerarse sospechoso.

Aspectos técnicos del shishing

Los enlaces no son la única forma que utilizan los phishers para atraerlo a sus actividades ilícitas. La Domain Name Service (DNS) es a menudo el banco de los delincuentes. DNS es un lugar para trasladar el URI, que usted mecanografía en su buscador dentro de direcciones reales de Internet.

Cuando usted registra www.cra-arc.gc.ca, (el DNS busca la dirección Internet 198.103.185.14) Si los delincuentes son capaces de contaminar el proceso de candado DNS, pueden enviar a alguien a cualquier sitio sin tomar en cuenta el URI mecanografiado.

Existen varias formas para que los defraudadores hagan esto. La primera es usar programación incorrecta (malware) para alterar los puntos fijos en la computadora de alguien. Básicamente se trata de una parte de código escrita para comprometer la computadora de alguien sin que esa persona lo sepa.

Hay varios lugares donde la computadora es potencialmente vulnerable a un ataque por programación incorrecta. Uno es la configuración DNS de puntos fijos TUIP. En los puntos fijos de la red de trabajo de una PC, hay una opción para especificar la dirección del servidor DNS usado por el buscador.

La programación incorrecta podría insertar una dirección falsa de servidor DNS y colocar así al usuario a merced de los delincuentes cada vez que el utilice el buscador. El servidor falso DNS podría dirigir a alguien hacia un sitio bancario falso aunque se haya registrado el URI correcto. Otra forma de dirigir a alguien a un sitio falso es que la programación incorrecta añada traducciones específicas a un archivo de "huésped local", que tienen todas la PC.

Si el traslado de una dirección aparece en el archivo "huésped local", lo usara y olvidara el enlace DNS. Si el archivo de huésped local esta envenenado por la programación incorrecta, el usuario podría dirigirlo a un sitio falso aunque se haya mecanografiado un URI específico.

Otra forma de un ataque DNS es comúnmente referido como un ataque tipo "pharming". El mismo se enfoca hacia las configuraciones DNS de redes inalámbricas. Los delincuentes "navegaran" por las vecindades buscando redes de trabajo inalámbricas pobremente configuradas. Cuando encuentran una que utiliza un enrutador sin palabra de contraseña, simplemente lo registran y cambian los puntos fijos del servidor DNS para señalar otro servidor envenenando DNS.

En tales ejemplos de envenenamiento DNS, los delincuentes muestran su servidor ilegítimo DNS con alteraciones de dirección fijadas URIs específicos directos a o websites falsos. En otro caso, de raro ataque de tipo DNS, el intento fraudulento consiste en envenenar un servidor legítimo DNS mediante el cambio de traslaciones de dirección para cualquiera que use el servidor. Afortunadamente, la mayor parte de los administradores DNS están conscientes de los riesgos de tener sus servicios comprometidos. Como resultado, los usuarios encontraran generalmente una posición enfurecida de seguridad vigente para protegerlos y pocos incidentes que impliquen su compromiso.

Con una elevada conciencia de phishing y comportamiento modificado para reducir las oportunidades de ser defraudado, ¿Cómo puede la gente eliminar los trucos técnicos usados por los delincuentes? Primero utilice una versión de buscador actualizado que tenga capacidad de anti-phishing interconstruida. Estos productos eliminarán los lazos que se presenten en la Internet y que intentan advertir a un usuario si identifican algo fuera de lo ordinario. La mayor parte de estos nuevos buscadores pueden buscar los hiperlazos presentados y compararlos contra bases de datos extensas de conocidos o sospechosos sitios phishing.

Estos buscadores son un activo valioso que proporcionará una capa de protección añadida.

Después, asegúrese de que su computadora esté actualizada en su tecnología. Aplique todos los parches conocidos a su sistema incluyendo la seguridad del sistema operativo y parches de integridad, parches para su buscador web y para cualquier otra programación que interactúe en línea o que pueda presentar vulnerabilidades explotables.

El propósito de algún ataque phishing no es solamente obtener acceso a información confidencial o de credencial, si no también empujar la programación incorrecta hacia la máquina de alguien para que pueda usarse como una puerta trasera para la información. Los sistemas de control remoto, los registros del teclado y la programación de comunicaciones para dirigir el spam o plática de relay de Internet (para enviar su información a los delincuentes) son ejemplos de programación incorrecta. Asegure que su máquina esté apropiadamente protegida para eliminar tales intentos. Cheque las revisiones y compre el mejor sistema de protección contra programación incorrecta que pueda encontrar. Incluya un completo sistema de protección contra virus, protección contra espionaje de programación y una robusta pared antifuego. Luego, mantenga estas herramientas actualizadas y úselas.

Atienda los mensajes de error o advertencias de estos productos. Mucha gente está demasiado apresurada para teclear OK antes de comprender la importancia del mensaje. Estos mensajes pueden informarle sobre problemas potenciales tales como certificados no reconocidos o enlaces inapropiados. Todos son pistas significativas que pueden ayudarle a mantener un usuario seguro.

Si usted opera con una red de trabajo inalámbrica, cambie la contraseña en su enrutador inalámbrico y utilice la forma más fuerte que pueda para encriptar.

Los protocolos de encriptación van del más débil al más fuerte y son WEP, WPA, WPA2. Si usted tiene aparatos más antiguos en su red de trabajo inalámbrica (tiene que comprar nuevos adaptadores inalámbricos para usar las formas más fuertes de encriptado).

Finalmente, hágales la vida más difícil a los delincuentes al reportar intentos sospechosos de phishing a las agencias que supervisan y ayudan a vigilar el Internet. Hay un número de organizaciones con buena reputación que sirven esta función. Un ejemplo es: <http://www.castlecops.com>. En este sitio puede ir a la pagina PIRT/Fried Phish para recortar el sitio de phishing.

Hay más por venir.

Phishing se ha vuelto una industria en el Internet y ha avanzado junto con la tecnología y los juegos de habilidad disponibles para la misma. Con todos los avances de esta área, sería tonto asumir que somos muy listos para ser capturados en la red. La siguiente generación de estos ataques (phishing 2.0) está apareciendo en línea y representa un juego de problemas completamente nuevo.

Tenga cuidado.

** Richard DeBruyne, CISA, CISM ISP, es administrador principal con Grant Thornton LLP en Calgary, Canadá.*

** Denis Posten, CA= IT es socio con Grant Thornton en Calgary, Canadá. Editor Técnico: Yves Godbout, CA= IT, CA= CISA, director de servicios IT, director de servicios IT, Oficina del Auditor General de Canadá.*

El Colegio de Contadores Públicos de México, se reserva la reproducción total o parcial de este material