



McAfee Phishing/Pharming

Phishing & Pharming

Entendiendo el *Phishing* y el *Pharming*

Índice

Introducción – Entendiendo el <i>Phishing</i> y el <i>Pharming</i>	3
¿Qué son el <i>Phishing</i> y el <i>Pharming</i> ?	4
Figura #1 – Tendencia de ataques exclusivos de <i>Phishing</i> en 2003-2004	4
Primeros intentos	4
Ataques sistemáticos	5
Figura #2 - Sitios de <i>Phishing</i> Activo 2004-2005	5
Quedándose más listos	5
Impacto financiero, <i>Pharming</i> – Nace una nueva amenaza	6
Reducción de <i>Phishing</i> y <i>Pharming</i> con McAfee	7
Filtrado <i>Anti-Spam</i> – Protección contra <i>Phishing</i>	7
Resumen del Antivirus de McAfee, sobre la protección de <i>desktops</i>	7
Protección contra Intrusiones de <i>Hosts</i> y Redes	7
El <i>phishing</i> – Evolución, Conclusión	8

Introducción

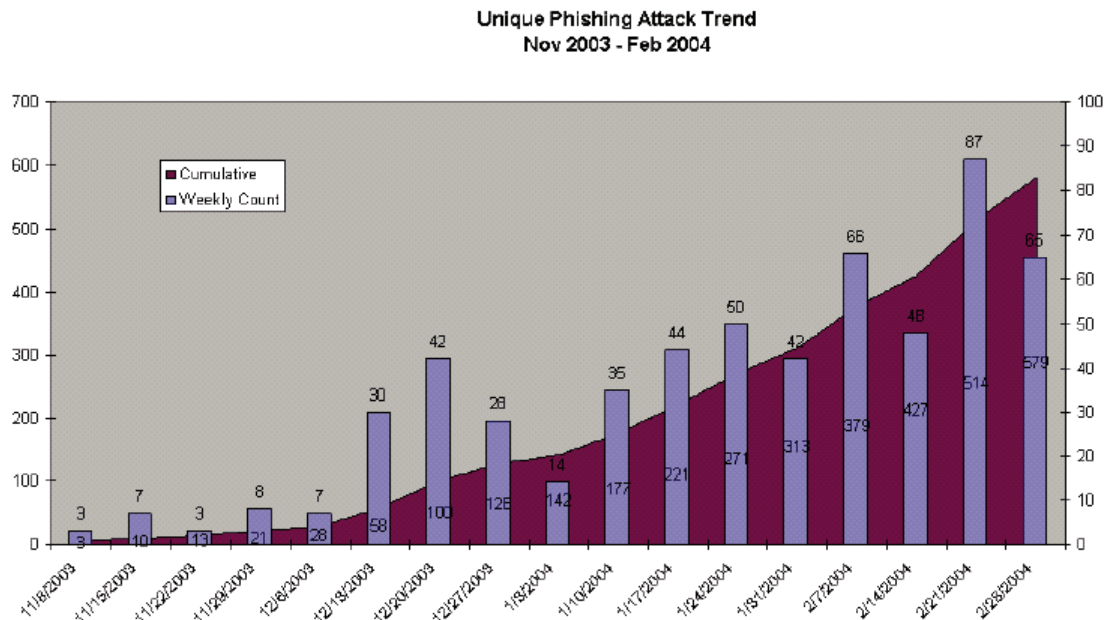
Entendiendo el *Phishing* y el *Pharming*

Para proteger correctamente sus recursos esenciales de negocios contra los ataques actuales de “Phishing” (*pesca*), usted necesita, antes de todo, comprender la historia del *Phishing*, los tipos de técnicas de *Phishing* usados en el submundo de la seguridad de hoy, y las formas con las cuales McAfee puede ayudarle a detectar y defenderse contra esos ataques. Además, se necesita saber cuál es la más nueva tendencia en ataques a la seguridad, conocida como “Pharming”, actual evolución del “Phishing”, en qué es distinto, qué se puede hacer para la defensa, y cuáles son las mejores técnicas de resolución para ambos tipos de ataques.

Con información sobre las amenazas de *Phishing* y *Pharming* (véanse las definiciones), el objetivo de este artículo es ayudar a identificar qué es un ataque de *Phishing*, cómo se presenta en una red, y cómo se lo puede atenuar. Además, mostramos el aspecto de los ataques de *Pharming*, según distintas situaciones de ataque, y cómo atenuar los efectos sobre sus recursos de negocios. También delineamos cómo esos dos tipos de ataques se convirtieron en el sofisticado “dúo fatal” de hoy dirigido a las empresas, a los consumidores y organismos públicos.

¿Qué son el Phishing y el Pharming?

Los ataques de *Phishing* utilizan ingeniería social y subterfugios técnicos para robar datos personales y credenciales de cuentas bancarias de los consumidores. Los esquemas de ingeniería social utilizan *e-mails* falsificados para llevar los consumidores a sitios falsos creados para inducir a los destinatarios a divulgar datos financieros tales como números de tarjeta de crédito, nombres de usuarios de cuentas, contraseñas y números de documentos. “Secuestrando” marcas de bancos, tiendas virtuales y administradoras de tarjetas de crédito, los *Phishers* logran convencer a los destinatarios a responder. Los esquemas de subterfugio técnico “plantan” programas criminales en las PC para robar credenciales directamente, a menudo utilizando Troyanos, programas de captura de tecleo y programas espías. Los programas criminales de *Pharming* llevan a los usuarios a sitios o servidores de proxy fraudulentos, normalmente a través del secuestro o “envenenamiento” de DNS.



Tendencia de ataques exclusivos de Phishing en 2003-2004

Primeros intentos

Las primeras “pescas” de información de tarjetas de crédito, etc. eran menos sofisticadas. El *e-mail* contenía un enlace a un sitio que parecía legítimo (pero, en verdad, no lo era – por supuesto). Muy a menudo, la dirección del sitio no era un dominio, sino simplemente una Dirección IP como 162.122.19.2 y los *e-mails*, a menudo, eran muy mal escritos, con errores de gramática y ortografía, y la poca atención

a los detalles denunciaban lo que realmente eran: estafas despreciables.

Según se espera, los nuevos ataques de *Phishing* evolucionaron rápidamente y los *e-mails* se quedaron más difíciles de reconocer, más sofisticados, mejor escritos, con mejor ortografía y más convincentes. Rápidamente, los *Phishers* se volvieron más eficientes en el uso de HTML conteniendo imágenes y gráficos de los verdaderos bancos o instituciones financieras; los enlaces representados en dichos *e-mails* llevaban a sitios que realmente se parecían

con los sitios de las instituciones representadas, llevando a la víctima a creer que el remitente era la institución verdadera.

Eso es muy sencillo porque el HTML en el cual aparece el enlace puede tener cualquier nombre o descripción y el verdadero destino puede permanecer oculto.

Ataques sistemáticos

Entonces, hacia fines de 2003, el *Phishing* se volvió más siniestro: los datos bancarios y la información de tarjetas de crédito de las personas empezaron a ser “pescadas” y, posteriormente, usadas para obtener dinero o adquirir productos.

El año pasado, el número de ataques de *phishing* aumentó con una velocidad alarmante, según lo muestra la Fig. 2.

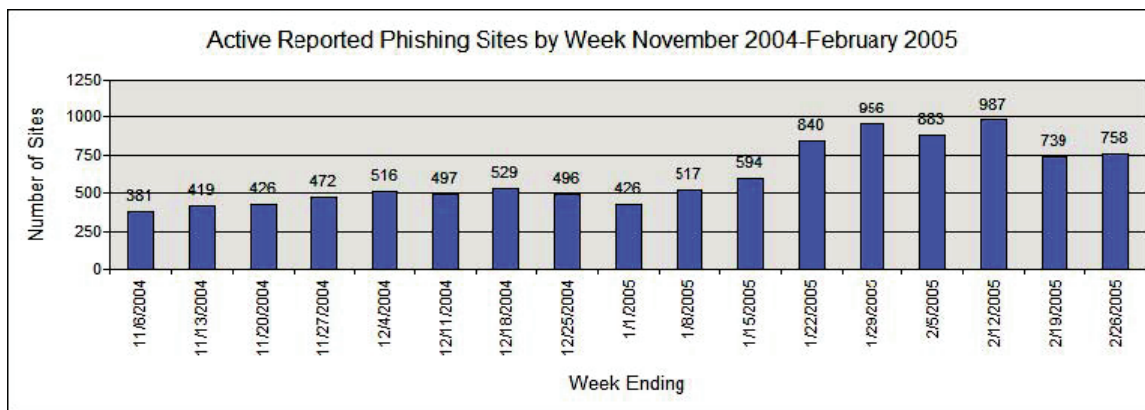


Fig. 2 – Número de sitios de *phishing* activos denunciados entre Nov 2004 y Feb 2005 (datos del Grupo de Trabajo Anti-Phishing)

Quedándose más listos

Para el ojo entrenado, todavía era relativamente fácil identificar los sitios de *phishing*. Los consumidores fueron instruidos para verificar si el sitio que visitaban contenía la URL correcta y el candado amarillo garantizando la seguridad del sitio.

Los *Phishers* estaban, otra vez, un paso adelante. Un fallo en la tecnología del Microsoft Internet Explorer permitía que los *scripts* ocultaran la barra de URL, ocultando la dirección del sitio con la verdadera dirección del banco. La misma técnica permitía que

El cebo de dichos ataques de *phishing* es, normalmente, enviado por *e-mail*. Se envía un mensaje de *e-mail* a un gran número de personas, con un enlace a un sitio. Normalmente, el *e-mail* solicita que el usuario actualice su información, con el pretexto de ‘reforzar los sistemas de seguridad’ o de una posible fuga de información. Se utiliza una amplia gama de técnicas de ingeniería social.

Cuando el usuario pulsa en el enlace, se le envía a una página que se asemeja mucho al de la verdadera institución, pero, en verdad, es una falsificación. Cuando el usuario inserta su información personal, se la almacena, lo que permite que el *hacker* las acceda posteriormente a gusto.

exhibieran un candado falso en la barra de *status*.

El consumidor está cada vez más listo. Por lo tanto, otra vez, reaccionaron los *Phishers*. En vez de enviar *e-mails* para persuadir a los consumidores para que visiten los sitios, empezaron a enviar Troyanos de captura de teclado. Cuando el usuario visita el sitio de su banco, todas las teclas oprimidas se almacenan y transmiten, dándole al *hacker* el número de la cuenta, las contraseñas y otros datos esenciales.

Los bancos y las instituciones financieras intentaron reaccionar a la amenaza solicitando sólo contraseñas parciales, pero, a lo largo del tiempo, los insistentes *Phishers* lograrán, asimismo, obtener la contraseña completa.

La batalla sigue: los bancos introducen listas suspensas de selección de contraseñas y teclados

El impacto financiero

Los cálculos aproximados de cuánto dinero se pierde debido a los ataques de *phishing* varían mucho. La Asociación Australiana de Bancos registró pérdidas de A\$10 millones debido a fraudes por Internet el año pasado. Se calcula que el costo del *phishing* para los bancos y emisores de tarjetas de crédito estadounidenses alcanzó a US\$1200 millones en indemnizaciones, en 2003 (InternetNews.com), y la Asociación de Servicios de Compensación de Pagos del Reino Unido relató que las pérdidas directas causadas por estafas de *phishing* costaron £12 millones, en 2004.

Independientemente del número real, los *Phishers* se ganan mucho dinero y se cree que son miembros de grupos criminales organizados o terroristas. Las complejas redes de cuentas bancarias y personas reclutadas para procesar el dinero en valores menores (a menudo sin saberlo) dificultan cada vez más su rastreo por las autoridades.

Más recientemente, los ataques de *Phishing* fueron responsables del comprometimiento de decenas de miles de registros bancarios y de tarjetas de crédito de consumidores de empresas a las cuales se paga para proveer dicha información a entidades legítimas. Los ataques de *Phishing* realizados por las organizaciones criminales organizadas aumentaron de 6597 en octubre de 2004 a 14411 en abril de 2005, un aumento de aproximadamente 45 por ciento en los últimos 7 meses.

Pharming – Nace una nueva amenaza

Una nueva tendencia en la batalla por el fraude de identidades en Internet es una técnica conocida como 'Pharming' (*plantación*). Se utilizan dos técnicas: la primera involucra el uso de un virus o Troyano para modificar el archivo de 'Hosts' del usuario. Dicho archivo es un remanente de los primordios de Internet, y se lo utiliza para relacionar una dirección de la Web (URL) a la dirección específica de una máquina (dirección IP). Es un archivo de texto sencillo. La técnica de *Pharming*

virtuales, y los *Phishers* contestan con programas de captura de ratón y de pantalla para obtener la información. *Phishers* y empresas están utilizando técnicas cada vez más sofisticadas, pues hay mucho en juego.

modifica dicho archivo, insertando en él la dirección Web de bancos e instituciones financieras conocidos con la dirección IP del sitio de *phishing*. Por lo tanto, cuando el usuario abre el navegador y teclea la dirección de su banco, se le envía al sitio de *phishing*. No necesita pulsar en enlaces de *e-mails* etc.

La segunda técnica es igualmente siniestra y, otra vez, depende de una función obsoleta, ahora implementada en el DNS, que reemplaza al archivo local de *hosts* como mecanismo de conversión de direcciones de la Web en direcciones IP específicas. Cuando el usuario teclea una dirección, se la consulta en el servidor de DNS. Si dicho servidor no conoce la dirección IP, consultará la dirección en otros servidores de DNS y, entonces, obtendrá el resultado. El problema es que una parte del protocolo también permite la transmisión de otra información. Entonces, el *Phisher* envía un *e-mail* conteniendo un enlace a un sitio. Cuando se realice la consulta de dicha dirección en el DNS, se incluye dicha información adicional en la URL del banco, pero está dirigida a un sitio de *phishing*. Este ejemplo describe mejor el ataque:

1. El *Phisher* envía un *spam* a 'www.phishsite.com'
2. Se consulta 'www.phishsite.com' en el DNS
3. El servidor de DNS 'www.phishsite.com' también envía datos a 'www.thebank.com', que se queda almacenado en el DNS.
4. Cuando una persona, utilizando el mismo proveedor de Internet, intenta visitar 'www.thebank.com', se la redirige al sitio de *phishing*.

Este tipo de ataque se puede evitar fácilmente a través de la configuración del servidor de DNS para que no acepte dichos registros adicionales, pero las vulnerabilidades son grandes porque es un ataque relativamente nuevo y exclusivo, y la mayoría de los gerentes de TI no lo conoce.

Reducción del Phishing y Pharming con McAfee

Filtrado anti-spam – Protección contra Phishing

La familia de productos McAfee SpamKiller posee reglas y filtros específicos para detectar ataques de *phishing*. Utilizando varias técnicas heurísticas para identificar las características comunes de *e-mails* de *phishing*, se pueden detectar y bloquear los ataques aunque antes no haya sido intentado un ataque específico (“ataque desconocido”). Pruebas independientes realizadas en datos enviados al Grupo de Trabajo Anti-Phishing (APWG) y datos recopilados por las capturas de *spam* de McAfee demuestran tasas de detección siempre superiores al 97%, para *e-mails* de *phishing* tanto conocidos como desconocidos. McAfee SpamKiller se puede instalar de varias formas, dependiendo de sus necesidades y aplicaciones específicas. Es una solución física que se puede instalar directamente en sus servidores de *e-mail* (Microsoft Exchange o Lotus Domino), en su *firewall* (Microsoft ISA Server) y, finalmente, como un servicio gestionado hospedado por McAfee (para los clientes que desean una solución de servicios tercerizados).

Tecnología de Exploración de virus de McAfee

El mecanismo de exploración antivirus de todos los productos de McAfee para *e-mail* también detecta los blancos más comunes de *phishing*, detectando características específicas y clasificándolas como Phish- bankfraud.eml.

Además, muchos sitios de *phishing* utilizan vulnerabilidades conocidas de Internet Explorer (según se describió más arriba) para intentar ocultar la verdadera ubicación y, a menudo, utilizan Troyanos, *Backdoors* y programas de captura de teclado. McAfee ya posee amplios bloqueos implementados contra esos tipos de ataques.

¿Y sobre la protección de desktops?

McAfee VirusScan Enterprise 8.0i, con su tecnología integrada de protección contra intrusiones y de *firewall*, es un mecanismo eficaz de protección contra las amenazas de *Phishing* siempre cambiantes. Con la simple inclusión de una regla, se pueden frustrar los intentos de secuestro del archivo de *host* local de los usuarios. La tecnología de *firewall* impide que los Troyanos o *backdoors* envíen los datos recopilados al *Phisher*, además de evitar que la máquina sea reclutada para ser parte de una ‘bot-net’ para distribuir *e-mails* de *spam*. Todo eso, además de la detección de altísima calidad del mecanismo de exploración y de la organización de investigaciones AVERT de McAfee.

Protección contra Intrusiones de Host y Red

A menudo, el blanco de los *Phishers* son las máquinas mal protegidas, ya sea para hospedar su sitio de *Phishing*, para comprometer el servidor de Web legítimo o utilizando máquinas sin seguridad para distribuir *e-mails* de *Phishing* posteriormente, recopilando los datos para la explotación.

Las soluciones Intercept, Desktop Firewall e IntruShield de McAfee ayudan a impedir que los recursos de las empresas sean usados inadvertidamente para fines ilegales dirigidos hacia fuera de su infraestructura, pero también ayudan a proteger a sus usuarios y clientes contra ataques de *Phishing*.

Phishing – La evolución

‘Phishing’ es la práctica de intentar obtener información confidencial como tarjetas de crédito, información bancaria, información de cuentas, etc., de usuarios inocentes, y fue creada como un medio de obtener credenciales de *login* de AOL. Simplemente se enviaba un *e-mail* fingiendo ser alguien de AOL solicitando el nombre de *login* y la contraseña de un usuario, normalmente bajo el pretexto de algún fallo en la seguridad. Usuarios inocentes envían los datos solicitados, dándole al *Phisher* la información personal necesaria para acceder a la información confidencial de su cuenta.

Conclusión

Phishing y *Pharming*, junto con los robos de identidad asociados a ellos, siguen creciendo con velocidad alarmante, causando grandes daños a la economía mundial y a la situación financiera de individuos. Como dichos golpes son difíciles de detectar, y como las organizaciones criminales están ganando mucho dinero con dichas actividades, la complejidad y la frecuencia de los ataques seguirá creciendo pues hay mucho más dinero que podrá ganarse.

La probada protección de sistemas de McAfee ayuda a evitar el secuestro de las computadoras por los *Phishers*, impide que envíen *spam*, bloquea el recibimiento de *spam*, detecta Troyanos y programas de captura de teclado, protege contra técnicas de *Pharming* y bloquea los sitios de *phishing*. La familia de probados y preventivos productos de seguridad de McAfee brinda varios niveles de protección contra esa creciente amenaza.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766

McAfee y/u otras marcas mencionadas en este documento son marcas comerciales, ya sean registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo usado para denotar la seguridad es una marca distintiva de los productos que llevan la marca McAfee. Todas las otras marcas comerciales, ya sean registradas o no, mencionadas en este documento, pertenecen exclusivamente a sus respectivos titulares. © 2005 McAfee, Inc. Todos los derechos están reservados.

Phishing & Pharming WP V.002– (Archivo: Phishing Pharming WP 08-17-05.pdf)