Estafas por Internet: ¿qué es el pharming y cómo protegerse de ataques?

10 enero, 2020

El pharming es un astuto tipo de fraude en Internet que subvierte los cimientos mismos de la red.

Mediante la manipulación del tráfico web, los atacantes intentan engañar al objetivo para que les entregue valiosa información personal.

Debido a lo furtivo del pharming, muchas víctimas no son conscientes de que han sido engañadas hasta que es demasiado tarde. En este
artículo aprenderá qué es el pharming, cómo funciona y, lo que es más
importante, qué puede hacer para evitar que le suceda a usted.

¿Qué es el pharming?

El pharming se produce cuando un hacker (o «pharmer») dirige

a un usuario de Internet hacia un sitio web falso, no hacia uno legítimo. Estos sitios «falsificados» pueden capturar información confidencial de la víctima, como nombres de usuario, contraseñas y datos de tarjetas de crédito, o bien pueden instalar malware en el ordenador. Los pharmers suelen centrarse en sitios web del sector financiero, como bancos, plataformas de pago en línea u otros destinos de comercio electrónico, a menudo con el robo de la identidad como objetivo.

Los ataques de pharming son efectivos porque engañan tanto a la víctima como a su ordenador. El pharmer engaña al ordenador de la víctima y la envía a su sitio web falsificado, no al lugar donde la víctima pretendía ir.
Así es como funciona:

Cuando un usuario va a un sitio web, introduce la dirección URL del sitio, que un servidor DNS convierte en una dirección IP numérica. ¿Le resulta confuso? Es sencillo. Piense que un servidor DNS es una lista telefónica en el que la URL es el nombre de un sitio web y la dirección IP el número de teléfono. Los pharmers pueden modificar la lista telefónica y cambiar los números de teléfono pertenecientes al sitio web elegido.

En términos informáticos, el pharming, compromete el tráfico de Internet en el nivel de DNS y envía al usuario a un sitio web falsificado construido por el hacker.

Pharming frente a phishing

¿Y cuál es la diferencia entre el pharming y el phishing?
Las dos estafas son similares, pero no exactamente iguales. El phishing emplea un cebo: los hackers envían un correo electrónico (u otra comunicación) de aspecto oficial donde se invita a la víctima a que visite el sitio web falsificado e introduzca su información personal.

El pharming omite el cebo y envía a las víctimas al sitio web falsificado sin su conocimiento o consentimiento. Como es la víctima la que escribe la dirección URL en vez de hacer clic en un vínculo de un correo electrónico sospechoso, es menos probable que detecte el fraude. Es una estafa más sutil en comparación con las más evidentes técnicas del phishing.

Cómo protegerse contra el pharming

Por suerte, existen estrategias probadas que puede poner en práctica para protegerse de los ataques de pharming. Además de estas sugerencias contra el pharming, nunca es mala idea repasar los fundamentos de seguridad en Internet en la era digital.

Escoja un proveedor de servicios de Internet (ISP) de confianza: la mayoría de los grandes ISP filtra automáticamente las redirecciones fraudulentas de los pharmers, lo que evita que llegue usted a los sitios web falsificados. Los nuevos ISP pueden parecer tentadores con sus atractivas ofertas y sus increíbles velocidades, pero confirme que estén tan comprometidos con su seguridad como los proveedores más

asentados.

Compruebe las direcciones URL por si contienen errores: cuando vaya a un sitio web, espere a que se cargue por completo y examine atentamente la URL. Los pharmers suelen disfrazar sus sitios con pequeños errores ortográficos, como letras cambiadas o sustituciones de letras: «aug.com» en vez de «avg.com», por ejemplo.

Busque URL que comiencen con HTTPS: cuando vea HTTPS, significa que todo el tráfico entre usted y el sitio web se cifra, por lo que un tercero no puede interceptarlo. Los sitios web con este nivel de seguridad mejorada cambian automáticamente su URL de HTTP a HTTPS para indicarle que sus datos están a salvo. Esta sugerencia es especialmente importante cuando realiza una transacción o intercambio financiero.

Manténgase alejado de sitios web sospechosos: utilice el buen juicio cuando navegue por Internet. Cíñase a sitios web en los que pueda confiar y aléjese de cualquier cosa que parezca sospechosa.

Evalúe los sitios web antes de realizar ninguna acción: si un sitio web de confianza no tiene el aspecto de siempre, tal vez se encuentre en la versión creada por un pharmer. Haga algunos clics para asegurarse de que todas las páginas están presentes. Muchos pharmers no se molestan en incluir los términos del servicio o las políticas de privacidad.

Evite vínculos y archivos de orígenes desconocidos: tenga cuidado cuando descargue archivos y piénseselo dos veces antes

de hacer clic en vínculos extraños. A los pharmers les resulta mucho más difícil engañarle si no son capaces de instalar malware en su ordenador.

Aléjese de las ofertas de comercio electrónico increíbles: si un descuento parece demasiado bueno para ser cierto, es muy probable que no lo sea. Muchos pharmers intentarán atraerlo con precios un 10 o un 20 % más bajos que los ofrecidos por las tiendas legítimas. Dedique unos minutos a comparar los precios de distintos sitios antes de realizar una compra.

Confíe en su software antivirus: preste atención cuando el navegador o el software antivirus le indiquen que no es recomendable visitar un sitio determinado. Aunque haya utilizado antes el sitio, una advertencia puede ser una indicación de que la página se infectó desde su última visita.

Cómo funciona el pharming

Una técnica común requiere la instalación de malware en el ordenador del cliente, lo que puede producirse cuando visita o descarga contenido de sitios web fraudulentos. Una vez que está instalado, el malware daña determinada información en el ordenador de la víctima para preparar el escenario del ataque de pharming.

Los ordenadores mantienen, en un archivo de «hosts» almacenado de forma local, una lista de sitios web y direcciones IP visitadas previamente. ¿Recuerda que el sistema de DNS es como un listín

telefónico que empareja un sitio web con su dirección IP asignada? La siguiente vez que el usuario visita un sitio web almacenado, el ordenador no tiene que solicitar la dirección IP al servidor DNS: simplemente consulta su archivo de hosts.

El malware de pharming altera el archivo de hosts cambiando las direcciones IP almacenadas, de modo que el ordenador envíe el tráfico al sitio falsificado del pharmer, no al auténtico. Con este tipo de ataque de pharming solo se ve afectado un PC, pero, como verá, algunos pharmers pueden optar por arrojar una red más amplia.

El envenenamiento de la caché DNS es un antiguo método de pharming que se basa en dañar el propio servidor DNS. Cuando un usuario desea visitar una URL con su navegador de Internet, este se pone en contacto con el servidor DNS para solicitar la dirección IP del dominio deseado. Cada servidor DNS cuenta con su propio conjunto de listados, además de con registros temporales (o «cachés») de listados obtenidos de otros.

Cuando un pharmer realiza un ataque de envenenamiento de caché DNS, reescribe las reglas que gobiernan el flujo del tráfico hasta un dominio especificado para redirigirlo a la dirección IP del sitio web falsificado. Puede hacerse mediante una técnica denominada secuestro de DNS. Como el ataque del pharmer se dirige contra un servidor, no contra un único ordenador, el envenenamiento de caché DNS tiene el

potencial de afectar a
varios usuarios a la vez. Algunos pharmers también utilizan la técnica de
secuestro DNS para atacar routers desprotegidos, como los que proporcionan
wi-fi pública gratuita.

Cómo reconocer si ha sufrido un ataque de pharming

¿Cómo puede saber si ha sufrido un ataque de pharming? Como se ha dicho, es posible que no se entere hasta después de quebrarse su
seguridad. En ese caso, es posible que reciba un correo electrónico (de su
proveedor de correo o del banco) pidiéndole que confirme que un nuevo inicio de
sesión ha sido cosa suya. El proveedor de correo electrónico o el banco sospechan
si detectan un inicio de sesión desde una ubicación o un dispositivo inusuales.
Si recibe un mensaje así, debe confirmar de inmediato que no se trataba de
usted y seguir los pasos indicados por el proveedor del servicio para denunciar
el fraude.

Puede notar otras actividades extrañas si ha sido víctima del pharming:

Cargos desconocidos en la tarjeta de crédito o débito, o en PayPal.

Cambios de contraseña en cualquiera de sus cuentas en línea.

Nuevas publicaciones o mensajes en redes sociales que usted no ha realizado.

Solicitudes de amistad en redes sociales que usted no ha enviado.

Nuevos programas que aparecen espontáneamente en su dispositivo.

Sugerencia adicional: puede comprobar si su dirección de correo electrónico ha estado expuesta a cualquier infracción de la seguridad mediante este servicio.

¿Qué debe hacer si nota cualquiera de las señales anteriores?

Siga los procedimientos de denuncia de fraudes de su entidad bancaria en línea, proveedor de correo o red social, si corresponde.

Cambie todas sus contraseñas y asegúrese de que utiliza contraseñas seguras y exclusivas para cada una de sus cuentas en línea (y si le parece un dolor de muelas, pruebe a emplear un administrador de contraseñas).

Aumente la seguridad de sus cuentas en línea añadiendo la identificación de doble factor donde sea posible.

Limpie su navegador: borre las cookies, líbrese de cualquier complemento desconocido y borre el historial.

Elimine los programas que no haya instalado usted.

Realice un análisis de antivirus y elimine cualquier malware detectado.

Grandes casos de pharming

El pharming no es una herramienta nueva en el arsenal de los hackers, pues tenemos ejemplos de pharming de alto nivel que se remontan a principios de la década de 2000. En 2004, un adolescente alemán logró realizar una transferencia de DNS de eBay.de y, aunque eBay mantuvo que

ningún
dato de los usuarios se había visto comprometido, el suceso provocó un
importante caos en la empresa y en los usuarios.

Una década más tarde, los ataques de pharming habían
evolucionado considerablemente. Un gran ataque de pharming en 2015 afectó
a los usuarios en Brasil con routers de determinadas marcas. Los atacantes
crearon archivos que parecían enviados desde una empresa de telecomunicaciones
de confianza y que contenían vínculos maliciosos. Cuando un usuario hacía clic
en un vínculo, los atacantes intentaban acceder a su router y alterar la
configuración DNS con el fin de dirigir a la víctima a los sitios de pharming.

¿Por qué se llama «pharming»?

Pharming es una combinación de los términos «phishing» y
«farming». Los ataques de phishing atraen a las víctimas desprevenidas con un
cebo, mientras que los de pharming guían a un gran número de usuarios de
Internet hacia un sitio web falsificado por un hacker.

Puede pensar en el pharming como en un «phishing sin el
cebo».

Manténgase vigilante y protéjase

El pharming es taimado y peligroso, pero, con las
precauciones adecuadas, es fácil evitar la estafa. Proteja su información
personal de los pharmers practicando buenos hábitos de navegación por Internet:

Escoja un ISP de confianza.

Una vez cargado un sitio web, compruebe que la URL está correctamente
escrita.

Confirme que la URL de los sitios web de finanzas y comercio electrónico comienza con «https».

Evite los sitios web, descargas y vínculos sospechosos.

Siga estas recomendaciones y podrá disfrutar de una experiencia en Internet libre de pharming.

Fuente: AVG