

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2008-015

Distribución de correos electrónicos fraudulentos

Durante los últimos 12 meses UNAM-CERT ha documentado el incremento en la distribución de correos electrónicos fraudulentos que aparentan ser emitidos por diversas organizaciones del sector público, financiero y privado de México. Estos correos se envían de forma masiva a través de mensajes de correo electrónico no solicitado, conocido como correo spam y buscan engañar a los usuarios, usando la ingeniería social, para poder obtener de ellos información personal que después es utilizada para defraudar a los usuarios. Las dos técnicas principalmente utilizadas para este tipo de fraude son: Phishing Scam y Pharming.

Fecha de Liberación: 11 de Junio de 2008

Última Revisión: 11 de Junio de 2008

Fuente: UNAM-CERT

Riesgo

Crítico

I. Usuarios afectados

Todos los usuarios que utilicen algún equipo con conexión a Internet para enviar o recibir correo electrónico.

II. Descripción

A. Phishing Scam

El Phishing Scam es una técnica de fraude que opera a través del envío de mensajes por correo electrónico principalmente, aunque también los hay por mensajería instantánea. Estos mensajes buscan engañar al usuario para que proporcione información sensible como nombres de usuario, contraseñas o información detallada sobre tarjetas de crédito o tarjetas de prepago de algún servicio. Los defraudadores solicitan que la información sea enviada por correo electrónico, a través del acceso a un sitio web falso (usurpando la identidad de alguna organización) o incluso solicitando que se llame a algún número telefónico.

Aunque no es el único, el servicio que con mayor frecuencia se afecta es el de banca electrónica, solicitando a los usuarios información de acceso a sitios de banca en línea. Una vez que los defraudadores obtienen la información, la utilizan para usurpar la identidad del usuario y disponer de sus recursos (económicos, de información, etc).

Las 5 características más importantes del Phishing Scam

1. Se distribuye a través de correo electrónico no solicitado (Spam).
2. Redirige a sitios falsos similares a los originales a través de enlaces en el contenido del correo electrónico.
3. En los sitios de Phishing Scam se solicita información personal o sensible (nombre de usuario, contraseña, detalles de tarjetas de crédito, etc.)
4. Las organizaciones de gobierno o comerciales serias NO solicitan información confidencial o sensible de los usuarios a través de mensajes de correo electrónico.
5. Los defraudadores utilizan la información para usurpar la identidad del usuario y disponer de sus recursos (económicos, de información, etc.).

El portal de Usuario Casero del DSC/UNAM-CERT ha desarrollado una animación didáctica sobre la operación del Phishing Scam que puede consultarse en el siguiente enlace:

<http://www.seguridad.unam.mx/usuario-casero/secciones/phishing.dsc>

B. Pharming

Pharming es otra técnica que, aunque no es nueva, está siendo utilizada con mayor frecuencia para defraudar a usuarios de servicios en línea. Al igual que el Phishing Scam, la variante del Pharming que UNAM-CERT ha observado en los meses recientes inicia con el envío de correo spam. El título y el contenido de este tipo de correos electrónicos buscan ser llamativos para los usuarios. UNAM-CERT ha ubicado los temas más recurrentes que utilizan este tipo de mensajes:

- ◆ Noticias falsas y amarillistas
- ◆ Envío de tarjetas postales electrónicas
- ◆ Supuesta obtención de algún premio
- ◆ Supuestos boletines informativos de alguna institución

Algunos de estos correos electrónicos indican al usuario que debe bajar un archivo para poder acceder a la información que indica el mensaje. Otros redirigen al usuario a algún sitio donde puede observar un video supuestamente relacionado con la noticia. Y algunos mas no piden realizar ninguna de las dos acciones anteriores pero, a través del contenido del propio mensaje de correo electrónico, pueden afectar el equipo del usuario.

El objetivo de los correos electrónicos es modificar el sistema del usuario a través del contenido del propio correo, del contenido de alguna página web visitada, de la ejecución de alguna animación o video en línea o de la ejecución de algún archivo descargable, permitiendo a un intruso redirigir al usuario hacia sitios falsos al utilizar un servicio en línea. Los sitios falsos pueden estar

ubicados en cualquier sitio ya que ocultan su verdadera identidad a través de la modificación del sistema de usuario. Las modificaciones realizadas en los sistemas y los sitios falsos tienen por objetivo, al igual que el Phishing Scam, robar información sensible de los usuarios.

Un vez que los usuarios han sido convencidos de acceder al contenido del correo electrónico y se hace la modificación a la configuración del sistema, el defraudador (phisher) puede usurpar la identidad del usuario para defraudarlo en el servicio legítimo.

Las 5 características más importantes de esta variante de Pharming

1. El ataque inicia con el envío de mensajes de correo no solicitado con títulos y contenidos llamativos para los usuarios.
2. Los correos aparentan ser enviados por organizaciones reconocidas del gobierno, instituciones comerciales, medios de comunicación, etc., con la intención de usurpar su identidad y engañar al usuario.
3. El contenido del correo electrónico, el sitio visitado o el archivo descargado modifica la configuración del sistema del usuario de forma transparente para que el usuario no advierta la actividad maliciosa
4. Cuando el usuario haga uso del servicio en línea afectado, será dirigido a sitios falsos que serán difíciles de identificar como tales para robarle información sensible.
5. Los defraudadores utilizan la información para usurpar la identidad del usuario y disponer de sus recursos.

Algunos de estos ataques podrían no ser detectados por los sistemas antivirus. Algunos ejemplos de los correos electrónicos fraudulentos sobre los que UNAM-CERT ha recibido reportes, pueden consultarse en el siguiente enlace

<http://www.seguridad.unam.mx/pharming.dsc>

El portal de Usuario Casero del DSC/UNAM-CERT ha desarrollado una animación didáctica sobre la operación del Pharming que puede consultarse en el siguiente enlace:

<http://www.seguridad.unam.mx/usuario-casero/secciones/pharming.dsc>

III. Impacto

Los usuarios que sean víctimas de este tipo de correos fraudulentos podrían revelar datos e información sensible como nombres de usuario, contraseñas, información detallada de tarjetas de crédito que puede ser utilizada por los defraudadores.

IV. Solución

5 recomendaciones para protegerse de fraudes por correo electrónico

1. No abrir correos electrónicos de remitentes desconocidos
2. No proporcionar información sensible (usuarios, contraseña, datos de tarjetas de crédito) por correo electrónico o a través de enlaces a sitios web contenidos en mensajes de correo electrónico no solicitado.

UNAM-CERT

3. No descargar archivos a través de enlaces contenidos en un correo electrónico no solicitado
4. Instalar y/o actualizar software antivirus y software antispyware
5. Reportar los correos sospechosos a phishing at seguridad o incidentes at seguridad.unam.mx

V. Referencias

- ◆ Nota de Seguridad UNAM-CERT-2007-001 – <http://www.cert.org.mx/nota/?vulne=5534>
 - ◆ Proyecto Malware UNAM – <http://www.malware.unam.mx>
 - ◆ Portal de Usuario Casero – <http://www.seguridad.unam.mx/usuario-casero>
 - ◆ Vulnerabilidad de autenticación en ruteadores 2Wire, DSC/UNAM-CERT – <http://www.seguridad.unam.mx/doc/?ap=tutorial>
 - ◆ Buenas prácticas de seguridad – <http://www.seguridad.unam.mx/usuario-casero/secciones/bpracticadsc>
 - ◆ Política de publicación de alertas, boletines y notas de seguridad del DSC – <http://www.seguridad.unam.mx/acerca/politicadsc>
 - ◆ Participa en el portal de Usuario Casero – <http://www.seguridad.unam.mx/usuario-casero/secciones/participadsc>
-

El Departamento de Seguridad en Cómputo/UNAM-CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Juan Carlos Guel Lopez (cguel at seguridad dot unam dot mx)
 - Oscar Raúl Ortega Pacheco (oortega at seguridad dot unam dot mx)
 - Ruben Aquino Luna (raquno at seguridad dot unam dot mx)
 - Jesús Mauricio Andrade Guzmán (mandrade at seguridad dot unam dot mx)
-

UNAM-CERT

Equipo de Respuesta a Incidentes UNAM

Departamento de Seguridad en Cómputo

incidentes at seguridad.unam.mx

phishing at seguridad.unam.mx

http://www.cert.org.mx

http://www.seguridad.unam.mx

ftp://ftp.seguridad.unam.mx

Tel: 56 22 81 69

Fax: 56 22 80 47