

ATAQUE DIRIGIDO – CORREO INFECTADO

1. Introducción

Una de las fuentes de infección en las empresas sigue siendo a través de *malware* que viene como ficheros adjuntos a los correos electrónicos recibidos por los empleados. Tanto al correo electrónico corporativo como al correo personal consultado desde Internet.

Por esta razón, es muy importante concienciar a los usuarios de las consecuencias que puede tener para la organización el hecho de que descargue y ejecute en su equipo un adjunto infectado.

La presente prueba consiste en el envío de un correo electrónico a través de una cuenta de correo falsificada, simulando ser un usuario interno de la compañía. Para ello se creará una cuenta ficticia que puede ser personal o genérica (lista de correo).

De una forma sencilla, se creará un correo con el cual convencer al usuario de que descargue y abra un fichero adjunto infectado.

Para ello se ha diseñado un archivo que, al ser ejecutado, abre automáticamente un navegador en el equipo del usuario y le redirige directamente a una página Web de INCIBE.

En esta Web, especialmente diseñada para esta prueba, se advierte al usuario del peligro que supone para la empresa la descarga y ejecución de un fichero adjunto a un correo. Además, se le indican una serie de medidas preventivas para prevenir posibles infecciones, implicando de esta forma al usuario a mantener la seguridad de la red corporativa.

Es importante indicar que no será identificado ni utilizado ningún dato personal de los participantes en la prueba.

2. Descripción

Esta prueba está basada en el envío de un correo electrónico con un fichero infectado, el cual, al ser ejecutado, muestra al usuario un portal Web advirtiéndole del peligro que supone lo que acaba de hacer. Para ello, deben seguirse los siguientes pasos.

a. El correo

En primer lugar, es necesario contar con la colaboración de los administradores o responsables del correo electrónico de la empresa. Con su ayuda, se creará una cuenta de correo ficticia para la prueba. Esta puede ser de carácter personal, haciendo uso del mismo patrón que tenga la empresa para las cuentas de correo (inicial del nombre y primer apellido, nombre y apellido separados por un punto, primer apellido y nombre...). Otra opción es el uso de una cuenta de correo genérica, con el nombre de un departamento de la compañía (real o ficticio) como pueden ser: informática@empresa.es, sistemas@empresa.es o rrhh@empresa.es

En el caso de que no se disponga del servicio de correo en la propia empresa, se deberá solicitar una nueva cuenta de correo a quien gestione este servicio.

Seguidamente se crea y envía el correo utilizando la cuenta recién creada:

- Se añaden como destinatarios las cuentas de correo que van a formar parte de la prueba.
- Es recomendable, para dar credibilidad al correo, que éste lleve incluido en copia (campo CC) a algún cargo importante de la empresa. Antes debe obtenerse el permiso explícito de esta persona para incluirlo en la prueba.
- El asunto o *Subject* debe ser el título con el que queremos que lleguen los correos, por lo que debe ser lo más claro y creíble posible.
- A continuación debemos escribir el correo. Para cumplir con el contexto en el que se basa esta prueba, es recomendable generar un correo remitido por algún área técnica de la empresa o alguno de sus miembros. De esta forma, se aporta una confianza extra al usuario ya que el objetivo es que este se descargue y abra un fichero ejecutable. Un ejemplo de correo “gancho” podría ser el siguiente:

Asunto: Auditoría de Seguridad Interna

Buenos días,

Desde el Departamento de Informática os hacemos llegar este correo en relación con la Auditoría de Seguridad que se está llevando a cabo actualmente en la empresa.

Uno de los procedimientos exige que se realicen ciertas comprobaciones en los equipos de usuario de la red interna.

Por ello, hemos adjuntado a este correo un fichero que debe ser descargado y ejecutado en cada uno de vuestros equipos de trabajo, con el fin de obtener el estado actual de los parches de seguridad del sistema operativo y de las actualizaciones de las aplicaciones.

Gracias por vuestra colaboración.

Departamento de Informática

Empresa

- Finalmente, es imprescindible no olvidar adjuntar el fichero infectado al correo a enviar. A continuación hablamos de él.
- Como último paso, una vez finalizada la prueba, será necesario eliminar la cuenta de correo ficticia creada. Además, se recomienda explicar los motivos de la prueba a los usuarios implicados en la misma.

b. El fichero

El fichero que se ha preparado es un programa escrito en el lenguaje de programación Delphi.

La única misión de este fichero es abrir el navegador de usuario o, en el caso de que ya esté abierto, abrirle una pestaña, directamente a un portal Web de INCIBE <https://www.incibe.es/protege-tu-empresa/kit-concienciacion/ataque-simulado> donde se expongan los peligros de las acciones que acaba de realizar, así como las medidas que debe tomar para no provocar una posible infección de malware en la red de la empresa.

El fichero debe ser renombrado a un nombre que esté acorde con el texto escrito en el correo. En el caso del correo de ejemplo, podría renombrarse el fichero como *Audit2014.exe*, *auditoria_seguridad.exe* o *audit-<nombre empresa>-2014.exe*

Este fichero NO es identificado por los antivirus como una amenaza. Sin embargo, al tratarse de un fichero ejecutable, es lógico que el navegador advierta al usuario de que está descargando un fichero que puede ser peligroso para el equipo. Una de las razones de esta prueba es observar que decide hacer el usuario en este punto.

Una vez finalizada la prueba, se solicitará a los usuarios involucrados que eliminen el fichero descargado.

Nota: Si desea revisar el código fuente del fichero puede solicitarlo a INCIBE a través del formulario de contacto.