

## ATAQUE DIRIGIDO – PENDRIVE INFECTADO

### 1. Introducción

Una de las fuentes de infección en las organizaciones y los hogares es a través de *malware* alojado en dispositivos de almacenamiento externos, usualmente memorias USB o *pendrives*.

Por esta razón, es fundamental el concienciar a los usuarios de las posibles consecuencias que puede conllevar el mal uso de aquellos dispositivos tecnológicos presentes en nuestro día a día y que en realidad tan poco se conocen.

La presente prueba tiene como objetivo mostrar al usuario como el hecho de encontrarse un *pendrive* y acceder al contenido interno del mismo, puede provocar una infección en su equipo y propagarse por toda la infraestructura de la empresa.

Para ello, se preparará un fichero infectado que no sea reconocible por los antivirus. Este será almacenado en una memoria USB y será «perdido» en algún lugar de la empresa.

Cuando el usuario acceda al contenido del *pendrive*, se abrirá un navegador en su equipo que le llevará directamente a una página web de INCIBE. En ella se indicarán los peligros de la acción que acaba de realizar y que medidas deben seguirse para evitar el escenario de una posible infección en la red de la empresa.

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



### 2. Descripción

La presente prueba está basada en la presencia de un fichero infectado en una memoria USB extraviada, 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 *pendrive*

En primer lugar, es necesario adquirir el *pendrive* donde irá almacenado el fichero «infectado». Es recomendable que el fichero vaya acompañado de otro tipo de contenido totalmente inofensivo como un directorio llamado «Fotos» y otro «Trabajo» donde en cada uno de ellos haya ciertos ficheros genéricos como imágenes descargadas de internet, documentos PDF y/o documentos *Excel* o *Word*. Junto a ellos, se ubicará el fichero infectado, pudiendo ser renombrado para con algún título atrayente para cualquier persona como por ejemplo: *Confidencial.exe* o *Material\_Privado.exe*.

## **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 una página web de INCIBE <https://www.incibe.es/protege-tu-empresa/kit-concienciacion/ataque-simulado> donde se exponen 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.

**Es fundamental que el fichero sea renombrado con un nombre «atractivo para el usuario», a ser posible relacionado con la propia empresa.**

Este fichero NO es identificado por los antivirus como una amenaza. Sin embargo, al tratarse de un fichero ejecutable, es probable que el sistema operativo solicite confirmación de que se desea ejecutar. 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 devuelvan el dispositivo *pendrive* y que eliminen el fichero en el caso de que haya sido copiado a su equipo.

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

## **c. El despliegue**

El objetivo de esta prueba es que el usuario encuentre y utilice el *pendrive* localizado.

Para ello, se deberá «abandonar» el dispositivo en una ubicación en la que sea muy probable que un usuario pueda encontrarlo. Algunos de estos lugares pueden ser:

- Ascensor.
- Entrada principal.
- Sala de café o comida.
- Los servicios.
- Pasillo transitado.

Es importante que el encargado de desplegar el *pendrive* no sea detectado durante el proceso.

En el caso de que el usuario devuelva el *pendrive* al departamento de Informática o cualquier otro responsable, se le explicará la prueba y su finalidad, se le solicitará que no comente nada al resto de compañeros y se iniciará de nuevo el proceso, desplegando el *pendrive* en otra ubicación. Es importante indicar al usuario lo correcto de su decisión de devolver el *pendrive* sin haberlo usado.

Según el tamaño de la sede de la empresa y el número de empleados, pueden ser «olvidados» varios *pendrives* por diferentes ubicaciones, aumentando así la probabilidad de éxito del test.