

Asociación de Internautas



Adware a cambio de vídeos y música en P2P.

PandaLabs ha detectado la difusión por diversos medios en Internet de una serie de ficheros que supuestamente contienen música y vídeo, pero que además encierran un regalo envenenado: para poder disfrutar de ellos, se debe acceder a instalar adware. La excusa es la consecución de una licencia para poder reproducir los archivos, que implica la aceptación de la instalación del adware. Se da la circunstancia además de que los ficheros recibidos hasta el momento por PandaLabs no contienen realmente ningún tipo de vídeo ni música, aunque no se descarta que esto pueda ocurrir. Estos ficheros son detectados por Panda Software como WmaDownloader.B.

El problema comienza con la descarga, por parte del usuario, de un supuesto fichero de vídeo (*.wmv) o de audio (*.wma). En el momento en que el usuario pretende ejecutar dichos archivos para visualizarlos en su ordenador, éstos muestran una ventana que pide al usuario la adquisición de una licencia. En ella se explica que para obtenerla gratuitamente, el usuario debe instalar IST Toolbar, un conocido adware que es usado como puerta de entrada para muchas otras amenazas.

Pese a que se advierte al usuario de la instalación del adware, y se invita al usuario a visitar el acuerdo de licencia, ésta está formulada en términos claramente abusivos, y además se aprovecha de la circunstancia de que poca gente entiende las implicaciones que tiene instalar este adware y el impacto que puede llegar a tener en su equipo, ya que por medio de él acceden muchas otras amenazas al sistema, comenta Luis Corrons, director de PandaLabs. Además, no debemos olvidar que en las muestras recibidas por PandaLabs el sistema es aún más fraudulento, ya que ni siquiera hay vídeo o audio realmente tras los archivos.

En el momento en que se muestra esta ventana, a su vez se solicita la instalación de un control ActiveX, que es el propio IST Toolbar mencionado en la ventana. Si el usuario no acepta la instalación, el usuario no se infectará, así como tampoco podrá reproducir el vídeo y audio. Si el usuario acepta, se descargará IST Toolbar (detectado por Panda Software como ISTBar), infectando el sistema, lo que permite reproducir el fichero, en caso de haberlo. Aparecerá así mismo una ventana anunciando la adquisición de la licencia.

Sin embargo, puede que esto no siempre sea así, como comenta Luis Corrons: La advertencia de instalación del ActiveX no se mostrará en equipos cuya configuración de seguridad esté en nivel bajo, algo que puede ocurrir porque el propio usuario lo configure de esta manera, o porque alguna otra especie de malware con la capacidad de modificarlos haya actuado previamente. Por ello, es muy importante revisar la configuración del navegador para neutralizar la instalación de controles ActiveX de dudosa procedencia. Todo este proceso sólo es válido para equipos que tengan instalado en sus sistemas Windows Media Player 9 ó una versión posterior.

Fuente:

[PandaLabs](#)

Más información en:

