

PELIGRO INFORMÁTICO

Interior alerta de un correo 'spam' que simula ser de la policía y contiene un virus

Al abrilo, el mensaje descarga un troyano de procedencia brasileña que infecta la máquina del usuario. El envío, remitido desde policia@gobierno.es, hace alusión a una supuesta "notificación de la Audiencia".

Sábado, 11 de diciembre - 10:51h.

El Ministerio del Interior ha alertado de la difusión de un correo electrónico spam remitido desde la dirección policia@gobierno.es, con el asunto "entimación", que contiene un virus. En un comunicado, el departamento que dirige Alfredo Pérez Rubalcaba advierte de que los mensajes hacen alusión a una supuesta "notificación de asistencia en la Audiencia" y contienen un enlace denominado "notificación-mpf.scr" que, al pulsarlo, descarga un troyano de procedencia brasileña que infecta la máquina del usuario.

Los agentes especializados en la lucha contra el cibercrimen de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, que han detectado la difusión del correo, piden a los ciudadanos que, para evitar la difusión de este tipo de software, informen a la policía de los incidentes que detecten a través de la página web www.policia.es. Además, los especialistas recomiendan eliminar directamente este correo sin pulsar los links que se adjuntan.

Proceso de desinfección

A todos aquellos que piensan que su equipo ya ha sido infectado, la policía les aconseja seguir cuatro pasos para desinfectar el equipo. El primero de ellos es matar el proceso: 'juzched.exe' desde el administrador de tareas. El segundo, pulsar las teclas Inicio/Ejecutar y escribir Regedit para eliminar la clave HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\juzche d. En tercer lugar, hay que suprimir el fichero C:\Documents and Settings\ñnombre de usuario\Datos de Programa\NortonUpdate.exe, para después eliminar el directorio C:\Documents and Settings\ñnombre de usuario\Datos de Programa\Extensions\ con todo lo que tenga dentro. Es importante borrar C:\Documents and Settings\ñnombre de usuario\Datos de Programa\Extensions\juzched.exe, ya que se trata del propio troyano que se ejecuta al reiniciar el sistema.

Ante cualquier duda, los usuarios pueden consultar el servicio gratuito de gestión de incidentes de la Oficina de Seguridad del Internauta OSI (www.osi.es) que, gestionado desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO), ofrece diferentes herramientas y consejos para la desinfección de sus equipos informáticos.

Según la Policía, diariamente se envían correos electrónicos que parece que proceden de organismos oficiales, pero que en realidad llevan archivos adjuntos que en caso de abrirlos infectan el ordenador del usuario. De este modo, los delincuentes pueden obtener datos de la intimidad de la víctima, claves de acceso a la banca on line o datos de tarjetas de crédito, entre otras cosas.