Publicado en el 14/04/2015

La Policía Nacional alerta de una oleada de emails que simulan ser Correos u otros servicios de mensajería para estafar a usuarios de Internet

Se insta a los destinatarios a descargarse una notificación que resulta ser un programa malicioso que, una vez ejecutado, procede al cifrado de todos los documentos del ordenador infectado con la extensión "ENCRYPTED"

Mantener el antivirus actualizado, no abrir links o descargar archivos de procedencia dudosa y nunca ejecutar archivos .EXE desconocidos, son algunos de los consejos que ofrece la Policía para evitar ser víctimas de este fraude

11-abril-2015.- La Policía Nacional alerta de la existencia de una nueva campaña de distribución del ransomware TorrenLocker mediante el envío masivo de emails. Estos correos electrónicos suplantan la identidad de Correos u otros servicios de mensajería para inducir a error y estafar a usuarios de Internet. En estos mensajes se insta a los destinatarios a descargarse una notificación que resulta ser un programa malicioso que, una vez ejecutado, procede al cifrado de todos los documentos del ordenador infectado con la extensión "ENCRYPTED". Este malware ataca a los archivos del usuario aplicando un cifrado sobre ellos y solicitando 299 euros para obtener la clave para descifrarlos. En caso de no satisfacer el pago en un determinado plazo la cantidad a abonar por la clave se duplica.

A finales del mes de marzo y principios del mes de abril se ha detectado por parte de los agentes especializados de la Unidad de Investigación Tecnológica de la Policía Nacional una nueva oleada de estas supuestas notificaciones de Correos u otros servicios de mensajería similares. Los mensajes, enviados con el asunto "CARTA CERTIFICADA NO ENTREGADA A USTED", contienen dos enlaces -"descargar información sobre su envío" y "haga click aquí"- que ejecutan el programa malicioso capaz de encriptar los documentos que contiene el equipo informático.

Consejos para no ser víctima de estos "ataques":

1. Mantener el software y el antivirus siempre actualizado.

2. Nunca abrir links o descargar archivos de procedencia dudosa o desconocida.

3. Realizar copias de seguridad frecuentes que posibiliten la recuperación de los archivos, siempre guardarlas en un dispositivo independiente, como puede ser un disco duro externo.

4. Mostrar extensiones de los archivos y nunca ejecutar archivos con la extensión .EXE desconocidos.

5. Utilizar el sentido común. Si se recibe un correo sospechoso no abrirlo hasta contrastar su procedencia, incluso contactando con el supuesto remitente o la compañía de transporte.

En algunas ocasiones, la restauración del sistema operativo a un punto anterior a la infección ha conseguido recuperar gran parte de los archivos encriptados.

Datos de contacto:

Nota de prensa publicada en:

Categorías: Nacional