RED AZUL INFORMA: **AGOSTO-2018**

"LA POLICÍA NACIONAL ALERTA DE UNA NUEVA CAMPAÑA MASIVA DE EXTORSIÓN *ONLINE*"

Agentes de la Policía Nacional especializados en la lucha contra la ciberdelincuencia, han detectado un considerable aumento de casos de esta variedad de "sextorsión", que consiste en amenazar a los usuarios con la relevación de fotos, videos o información sobre su intimidad, obtenidas sin consentimiento previo, solicitándoles una cuantía económica a cambio de no realizar su difusión.

Para ello, les indican haber conseguido la contraseña de sus correos electrónicos o afirman haber instalado un malware en las páginas web pornográficas supuestamente visitadas. Además les indican haber conseguido imágenes o videos personales íntimos suyos tras activar la webcam de su ordenador cuando visitaban esas páginas.

Los "extorsionadores" solicitan pagos en bitcoins a diferentes monederos virtuales para no difundir las imágenes, debiendo abonar entre los 400 y los 2.900 dólares, en un plazo máximo de 24 horas.

La cuenta de correo **redesabiertas@policia.es**, gestionada por especialistas de la Policía Nacional en ciberdelincuencia, recibe unas 100 comunicaciones diarias de posibles casos que son analizados de forma individualizada.

La Policía Nacional informa que en realidad se trata de una campaña de ingeniería social. Al parecer, los password se habrían obtenido por filtraciones masivas ocurridas hace años en la Red, hecho por el cual la contraseña que se facilita a los usuarios y que dicen haber conseguido los delincuentes mediante la utilización de un software malicioso, no es otra que una contraseña antigua obtenida en la filtración de claves y contraseñas.

La Policía Nacional ofrece una serie de consejos para no ser víctima de esta nueva modalidad delictiva:

- No alarmarse ni considerar la amenaza como real.
- No realizar ningún pago solicitado.
- No contestar al correo o correos recibidos ni entablar ningún tipo de conversación con los "extorsionadores".

- Bloquear y marcar como correo no deseado al remitente de los correos.
- Desconfiar de cualquier correo que pueda parecer extraño y de origen desconocido.
- No “clicar” sobre enlaces del cuerpo del correo recibido.
- No abrir archivos adjuntos remitidos desde el email recibido.
- Renovar la contraseña del correo electrónico, equipo y aplicaciones informáticas regularmente y establecer contraseñas seguras.
- Mantener actualizados los equipos informáticos.

*“ALLÁ DONDE ESTÉ LA **SEGURIDAD PRIVADA**,*

*ESTÁ LA **POLICÍA NACIONAL**”*