Publicado en Ciudad de México el 19/09/2018

# [Avast alerta a clientes de fraude que se vale de la sextorsión](http://www.notasdeprensa.es)

## Los estafadores usan las contraseñas robadas, obtenidas en filtraciones de datos, para engañar a los usuarios

 Avast (LSE: AVST), líder global en productos de seguridad digital, advierte a los usuarios de la existencia de un nuevo fraude llamado “sextorsión” y que está diseminándose. Los usuarios reciben un correo electrónico que asegura que el remitente conoce la contraseña del usuario y que tiene un video comprometedor en su poder, grabación que fue captada por la cámara del propio usuario mientras miraba pornografía. El atacante amenaza con enviar el video a toda la lista de contactos del usuario si éste no hace un pago con bitcoins a una dirección proporcionada por el estafador. En tal sentido, Avast informa a los usuarios que esta estafa es falsa y les pide no responder a la misma. Los investigadores de Avast examinaron una muestra de los correos fraudulentos y encontraron que la suma que los estafadores estaban pidiendo oscilaba entre 1.900 y 7.000 dólares estadounidenses; sin embargo, infieren que pueden existir versiones de estos correos en los cuales se exigen cifras más elevadas. Los estafadores aseguran, asimismo, que el video ha sido renderizado en un formato de pantalla dividida que muestra a la vez el clip porno que el usuario está observando y la reacción del usuario en tiempo real. "Solo el usuario puede confirmar si dicho video realmente existe, sin embargo, nuestra investigación sobre la estafa ha probado que la misma es falsa", afirma Luis Corrons, evangelizador de seguridad de Avast. "El estafador busca avergonzar al usuario con la idea de la existencia de este video, con el objetivo de asustarlo y hacerlo pagar la extorsión solicitada sin pensar. La carta que tiene para jugarse el estafador es contar con la contraseña del usuario. El hecho de tenerla en su poder le da a toda la estafa una apariencia de legitimidad; sin embargo, el usuario no debe caer en esta trampa". Los investigadores de Avast concluyeron que los estafadores obtuvieron las contraseñas y las direcciones de correo electrónico en la dark web, donde es posible encontrar listas que contienen decenas de millones de claves de acceso, recopiladas los últimos años por medio de filtraciones de datos y que están disponibles para la venta o para ser descargadas de forma gratuita. Los usuarios que no cambian sus contraseñas a menudo o cuyas direcciones de correo han estado comprometidas en filtraciones de datos son los más vulnerables a esta operación de chantaje. Existen varios grupos detrás de estos ataques y usan diferentes mensajes, lo que hace prever que se observará un aumento de este tipo de arremetidas en el futuro -y que posiblemente habrá que lidiar con un ataque totalmente automatizado. Cómo los usuarios pueden detectar un correo fraudulentoLos usuarios pueden enterarse de que se han convertido en el objetivo de una campaña de sextorsión si se topan con las siguientes señales: El correo electrónico recibido menciona una cámara web y la grabación secreta de un video. Se hace un pedido de dinero -cuyo monto debe ser enviado en bitcoins. Incluye una contraseña real (usualmente vieja) empleada en el pasado. Emplea una táctica intimidatoria, que incluye la amenaza de enviar el video comprometedor a la lista de contactos del usuario. Lo que deben hacer los usuarios si reciben un correo que busca estafarlosEl cibercrimen se está volviendo más sofisticado cada día, pero la llave sigue siendo la misma: apelar a tácticas intimidatorias que juegan con el temor del usuario. Avast recomienda a los usuarios que sigan estos pasos para protegerse de este tipo de amenazas: Si los usuarios reciben este tipo de amenazas, no deben pagar el monto solicitado a modo de extorsión. Todo se trata de una estafa sofisticada. Los usuarios deben cambiar sus contraseñas frecuentemente, así como usar largas, únicas y complicadas combinaciones de caracteres. A menudo, las contraseñas obtenidas con servicios de encriptación, al ser complejas, no son fáciles de desencriptar por los atacantes. Los usuarios que deseen asegurarse de que no están siendo filmados a través de su cámara web deben desactivarla o cubrirla. Avast también ofrece la función Webcam Shield con su versión Avast Premier (http://www.avast.com), que impide que las aplicaciones y el malware accedan a la cámara web del usuario sin su consentimiento, de tal forma que aplicaciones no confiables no puedan capturar imágenes o videos del usuario o comprometer su seguridad. Acerca de AvastAvast Software (www.avast.com), líder global en productos de seguridad digital para consumidores y empresas, protege a más de 400 millones de personas en línea. Avast ofrece productos con las marcas Avast y AVG que protegen a los usuarios de amenazas en internet y el escenario de amenazas de Internet de las Cosas que está en constante evolución. La red de detección de amenazas de la empresa está entre las más avanzadas del mundo, y utiliza tecnologías de aprendizaje automático e inteligencia artificial para detectar y detener amenazas en tiempo real. Los productos de seguridad digital Avast para dispositivos móviles, PC o Mac están clasificados como los mejores y certificados por VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, West Coast Labs, entre otros.

**Datos de contacto:**

Marketing Q

Agencia de Relaciones Públicas

56152196

Nota de prensa publicada en: [https://www.mexicopress.com.mx/avast-alerta-a-clientes-de-fraude-que-se-vale\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Ciberseguridad Dispositivos móviles Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)