«Tenemos tu correo y te estamos grabando», el nuevo ataque a través de Internet

- 

A través de un
mensaje intimidatorio, se le hace creer a la persona que su computado fue
infectada con un troyano (programa malicioso en forma de aplicación indefensa)
y que el hacker tiene información confidencial sobre él; y para no difundirla
se solicita un pago mediante el envío de bitcoins.

El éxito de la
campaña se encuentra en la dirección desde la cual se envía el correo. Para
ello se utiliza una técnica conocida como spoofing, la cual permite falsificar
algún rasgo de una comunicación informática. De esa forma, el hacker hace creer

a la víctima que el mensaje salió de su propia cuenta de correo.

Esta técnica de suplantación se puede usar cuando no se incluyen los mecanismos de autenticación. “Si no se toman las medidas de precaución adecuadas a la hora de configurar los servicios de correo electrónico, cualquiera puede enviar correos falsificados, que a simple vista parecieran provenir de una dirección o un dominio legítimo, pero que en realidad no corresponden con el emisor”, explicó Cecilia Pastorino, Especialista en seguridad informática de ESET Latinoamérica.

Cuando ESET realizó la investigación, la billetera contaba con 0.35644122 Bitcoins, equivalente a poco más de 2.400 dólares.

Recomendaciones

No responder los correos de este estilo y entender que se trata de un engaño; por supuesto, tampoco se debe pagar a los atacantes.

Asimismo, hacer caso omiso a estos mensajes y realizar buenas prácticas en el uso del correo electrónico, por ejemplo, cambiar las contraseñas de manera regular, usar programas de seguridad en los equipos, y habilitar opciones de doble autenticación en los servicios de Internet.