Un malware que aparenta ser una actualización de Adobe Flash está circulando por la red, haciendo creer a los usuarios que se trata de una actualización legítima, sin embargo, el malware se instala para minar criptomonedas.

Investigadores de seguridad de Palo Alto Networks, aseguran que no se trata de una técnica nueva ni eficiente, pero en agosto de este año se ha comenzado a detectar el malware que es un poco más avanzado y puede utilizar la notificación del instalador oficial de Adobe para engañar al usuario.

Si la víctima cae en el engaño, el malware además de instalar programas como XMRig, un software de minado, además actualiza Flash Player a la última versión, para evitar que el usuario sospeche.

Los archivos ejecutables que se han detectado para Windows tienen nombres que comienzan con *«AdobeFlashPlayer»,* provenientes de servidores en la nube que no son de Adobe.

Este tipo de campaña ha resultado muy efectiva ya que se aprovecha de una actividad legítima, al actualizar Adobe Flash Player.