Un grupo de hackers contaminó con malware el popular activador para Windows, KMSPico, con el que los atacantes buscan implementar malware diseñado para robar credenciales y otra información de billeteras de criptomonedas.

El malware, denominado CryptoBot, es un ladrón de información capaz de obtener credenciales para navegadores, billeteras de criptomonedas, cookies de navegador, tarjetas de crédito y realizar capturas de pantalla en los sistemas infectados. Se implementa a través de software descifrado y la última campaña involucra al malware disfrazado de KMSPico.

KMSPico es una herramienta no oficial que se utiliza para activar de forma ilícita todas las funciones de copias pirateadas de software, como Microsoft Windows o la suite de Office.

> *«El usuario se infecta haciendo clic en uno de los enlaces maliciosos y descarga cualquier CryptoBot en el supuesto KMSPico. Los adversarios también instalan KMSPico, porque eso es lo que la víctima espera que suceda, mientras que de forma simultánea, implementan Cryptobot detrás de la escena»,* dijo el investigador de Red Canary, Tony Lambert.

La compañía estadounidense de seguridad cibernétca dijo que también observó que varios departamentos de TI utilizaban el software ilegítimo en lugar de licencias válidas de Microosft para activar sistemas, y agregó que los instaladores KMSPico alterados se distribuyen a través de varios sitios web que afirman ofrecer la versión «oficial» del activador.

Para evitar ser víctimas de este tipo de ataques, lo más recomendable es evitar el uso de software pirata en primer lugar.