Investigadores de la Unidad 42 de Palo Alto Networks han identificado un nuevo malware que utiliza los datos almacenados en los buscadores de Internet para acceder a las plataformas de intercambio de criptomonedas.

Los investigadores publicaron el hallazgo en su sitio web el 31 de enero pasado. Explicaron que el malware, llamado CookiMiner, roba las cookies del navegador de los sitios visitados por las víctimas para obtener acceso a sus cuentas o carteras y robar sus fondos.

Aseguran también que CookieMiner podría haber sido desarrollado a partir del malware OSX.DarthMiner, conocido por atacar principalmente la plataforma Mac. Según los expertos, el nuevo malware también es capaz de robar los datos guardados en Chrome y Safari, e incluso intentar acceder a mensajes de texto de iPhone desde las copias de seguridad.

De este modo, los piratas informáticos pueden hacer uso de la información que el usuario haya almacenado en los navegadores, entre estos, sus nombres de usuario, contraseñas, credenciales de tarjetas de crédito, e incluso, datos de acceso a plataformas de intercambio de criptoactivos.

Cuando roba las cookies, el malware puede burlar el proceso de autenticación en dos pasos, que utiliza la mayoría de los sitios que manejan criptomonedas. De este moto, se inician sesiones en sitios asociados con un host previamente autenticado, por lo que no se emitirá ninguna alerta ni se solicitarán métodos de autenticación adicionales.

> *«Si los malos actores ingresan con éxito a los sitios web utilizando la identidad de la víctima, podrían realizar retiros de fondos. Esta puede ser una forma más eficiente de generar ganancias que la minería de criptomonedas. Además, los atacantes podrían manipular los precios de la criptomoneda con compras y/o ventas en gran volumen de activos robados, lo que resulta en ganancias adicionales»*, dice la Unidad 42 de Palo Alto Networks.

Además, también sería posible minar criptomonedas, ya que el malware instala un software

llamado Xmrig2 en el dispositivo de la víctima. Este programa se encarga de minar Monero, pero en realidad extrae Koto, una criptomoneda japonesa orientada a la privacidad, que puede ser extraída por medio del CPU. Para iniciar el proceso, el malware emite unos comandos que permiten configurar el equipo de la víctima, instalando dicho software de minado.

Funcionamiento de CookieMiner

Según el equipo de investigadores, los ataques dirigidos al sistema operativo de Mac comienzan con un script, con el que se copian las cookies del navegador Safari en una carpeta y se cargan en un servidor remoto. El ataque se dirige a las cookies asociadas con sitios de intercambio de criptomonedas o cualquier otra página que tenga la palabra blockchain en su nombre de dominio. Los investigadores aseguran que plataformas como Binance, Coinbase, Poloniex, Bittrex, Bitstamp, MyEtherWallet y otras son blancos del malware.

Para el caso de Google Chrome, CookieMiner descarga una secuencia de comandos de Python, llamada *harmlesslittlecode.py* y con esto logra extraer las credenciales de inicio de sesión almacenadas y la información de datos locales almacenados en Chrome.

Luego, el malware reporta a un servidor remoto todas las rutas de archivos relacionados con credenciales, claves de inicio de sesión, acceso a carpetas de criptomonedas y tarjetas de crédito, para poder robar la información de los emisores.