Se descubrió que los hackers están usando versiones troyanizadas de aplicaciones legítimas para implementar malware evasivo de minería de criptomonedas en sistemas macOS.

Jamf threat Labs, que hizo el descubrimiento, dijo que el minero de criptomonedas XMRig, se ejecutó mediante una modificación no autorizada en Final Cut Pro, un softwar ede edición de video de Apple.

> *«Este malware utiliza Invisible Internet Project (i2p) para descargar componentes maliciosos y enviar criptomonedas extraídas a la billetera del atacante»,* dijeron los investigadores de Jamf, Matt Benyo, Ferdous Saljooki y Jaron Bradley.

Trend Micro documentó una iteración anterior de la campaña hace exactamente un año, que señaló el uso de i2p por parte del malware para ocultar el tráfico de la red y especuló que podría haberse entregado como un archivo DMG para Adobe Photoshop CC 2019.

Apple, por su parte, dijo que la fuente de las aplicaciones de criptojacking se puede rastrear hasta Pirate Bay, y las primeras cargas datan de 2019.

El resultado es el descubrimiento de tres generaciones del malware, observadas primero en agosto de 2019, abril de 2021 y octubre de 2021, respectivamente, que trazan la evolución de la sofisticación y el sigilo de la campaña.

Un ejemplo de la técnica de evasión es un script de shell que monitorea la lista de procesos en ejecución para verificar la presencia del Monitor de actividad, y de ser así, finalizar los procesos de minería.

El proceso de minería malicioso se basa en que el usuario inicie la aplicación hackeada, sobre la cual el código incrustado en el ejecutable se conecta a un servidor controlado por el

hacker a través de i2p para descargar el componente XMRig.

La capacidad del malware para pasar desapercibido, junto con el hecho de que los usuarios que ejecutan software descifrado están voluntariamente haciendo algo ilegal, ha hecho que el vector de distribución sea muy eficaz durante muchos años.

Apple, sin embargo, ha tomado medidas para combatir ese abuso al someter las aplicaciones notariadas a verificaciones más estrictas de Gatekeeper en macOS Ventura, evitando así que se inicien aplicaciones manipuladas.

> *«Por otro lado, macOS Ventura no impidió que el minero se ejecutara. Para cuando el usuario recibe el mensaje de error, ese malware ya se ha instalado»,* dijeron los investigadores de Jamf.

> *«Evitó que se iniciara la versión modificada de Final Cut Pro, lo que podría generar sospechas para el usuario y reducir en gran medida la probabilidad de que el usuario inicie posteriormente».*