Investigadores de seguridad cibernética descubrieron esta semana un nuevo tipo de ransomware dirigido a usuarios de macOS que se propaga por medio de aplicaciones pirateadas.

Según los informes independientes del investigador de K7 Lab, Dinesh Devadoss, Patrick Wardle y Malwarebytes, la variante de ransomware llamada EvilQuest, se empaqueta con aplicaciones legítimas, que después de la instalación, se disfraza de CrashReporter de Apple, o Actualización de software de Google.

Además de encriptar los archivos de la víctima, EvilQuest también cuenta con capacidades para garantizar la persistencia, registrar pulsaciones de teclas, crear un shell inverso y robar archivos relacionados con billeteras de criptomonedas.

Con este desarrollo, EvilQuest se une a un grupo de cepas de ransomware que han seleccionado exclusivamente macOS, incluidos KeRanger y Patcher.

La fuente del malware parece ser unas versiones troyanizadas de software popular para macOS, como Little Snitch, Mixed in Key 8 y Ableton Live, que se distribuyen en sitios populares de torrents.

> *«Para empezar, el instalador legítimo de Little Snitch está empaquetado de forma atractiva y profesional, con un instalador personalizado bien hecho que está debidamente firmado por código. Sin embargo, este instalador fue un simple paquete de instalación de Apple con un ícono genérico. Peor aún, el paquete de instalación se distribuyó sin sentido dentro de un archivo de imagen de disco»,* dijo Thomas Reed, director de Mac y dispositivos móviles en Malwarebytes.

Una vez instalado el host infectado, EvilQuest realiza una comprobación de sandbox para detectar parches de sueño y viene equipado con una lógica anti-depuración para garantizar

que el programa de malware no se ejecute bajo un depurador.

> *«No es usual que el malware incluya demoras. Por ejemplo, el primer ransomware Mac, KeRanger, incluyó un retraso de tres días entre el momento en que infectó el sistema y el momento en que comenzó a encriptar archivos. Esto ayuda a ocultar la fuente del malware, ya que el comportamiento malicioso puede no ser inmediato asociado con un programa instalado tres días antes»*, dijo Reed.

También mata cualquier software de seguridad, como Kaspersky, Norton, Avas, DrWeb, McAfee, Bitdefender y Bullguard, que pueda detectar o bloquear el comportamiento malicioso en el sistema, y configura la persistencia utilizando el agente de lanzamiento y los archivos de la lista de propiedades de daemon (com.apple.questd.plist), para reiniciar de forma automática el malware cada vez que el usuario inicia sesión.

En la última etapa, EvilQuest lanza una copia de sí mismo y comienza a cifrar archivos, contando la billetera de criptomonedas (wallet.pdf) y el llavero relacionado de archivos, antes de mostrar las instrucciones de rescate para pagar 50 dólares en 71 horas o arriesgarse a dejar los archivos bloqueados.

Además, las características de EvilQuest son superiores a las de cualquier ransomware típico, ya que incluye la capacidad de comunicarse con un servidor de comando y control (andrewka6.pythonanywhere.com) para ejecutar comandos remotamente, iniciar keylogger, crear un shell inverso e incluso ejecutar una carga maliciosa directamente sin memoria.

> *«Armado con estas capacidades, el atacante puede mantener el control total sobre un host infectado»,* dijo Wardle.

Mientras se trabaja para encontrar una debilidad en el algoritmo de cifrado para crear una herramienta de descifrado, es recomendable que los usuarios de macOS creen copias de

seguridad para evitar la pérdida de datos y utilicen una utilidad como RansomWhere para frustrar estos ataques.

> *«La mejor forma de evitar las consecuencias del ransomware es mantener un buen conjunto de copias de seguridad. Guarde al menos dos copias de seguridad de todos los datos importantes, y al menos uno no debe mantenerse adjunto a su Mac en todo momento»*, concluyó Reed.