En macOS, se ha descubierto recientemente una amenaza de seguridad que opera de manera encubierta para acceder a inicios de sesión, información bancaria y otros datos confidenciales. El nuevo malware de macOS se conoce como *«ShadowVault»*. No está claro si ShadowVault ha sido detectado en uso y cómo se distribuirá en el entorno salvaje. Sin embargo, dado que funciona en segundo plano en Macs, es probable que los usuarios necesiten ser persuadidos para descargarlo y utilizarlo.

Se ha observado recientemente un nuevo malware específico para Mac llamado MacStealer, que tiene la capacidad de robar contraseñas, números de tarjetas de crédito, carteras de criptomonedas y otra información sensible. Una versión mejorada del primer malware ha surgido posteriormente, conocida como ShadowVault macOS Stealer. Se desconoce cuáles son sus capacidades y cómo proteger tu Mac, pero se detallarán a continuación.

Los desarrolladores del nuevo ShadowVault macOS Stealer están cobrando una tarifa mensual por su servicio de *«malware como servicio»*, siguiendo el modelo del Atomic macOS Stealer que apareció por primera vez en abril. En el momento de su descubrimiento, ShadowVault se vendía a $500 al mes. Alega poder recuperar *«todas las extensiones basadas en Chromium», «contraseñas, cookies, tarjetas de crédito, carteras» y «todas las extensiones basadas en Chromium».*

¿Qué puede robar el nuevo malware de macOS, ShadowVault?

El nuevo malware de macOS, ShadowVault, puede robar tu información y causarte daño de diversas maneras. Los expertos de 9to5Mac han enumerado algunos de los peligros asociados. A continuación, se presenta una lista completa:

- Extraer contraseñas, cookies, tarjetas de crédito, carteras y todas las extensiones basadas en Chromium (Opera, Chrome, Edge, Vivaldi, Brave, Torch, Yandex y más de 50 navegadores con complementos).
- Extraer contraseñas, cookies, tarjetas de crédito, carteras y todas las extensiones de

Firefox.
- Extraer archivos (puedes agregar/eliminar cualquier extensión).
- Extracción de la base de datos del llavero (descifrada y lista para ser importada).
- Soporte y descifrado de carteras de criptomonedas de todos los navegadores (Metamask, Coinomi, Binance, Coinbase, Atomic, Exodus, Keplr, Phantom, Trust, Tron Link, Martian).
- Captura de mensajes de Telegram.
- Posibilidad de configurar registros de pulsaciones en varios lugares al mismo tiempo.

Dado que la mayoría de los atacantes de malware se enfocan en sistemas Windows y Linux, se considera que las computadoras macOS son relativamente seguras contra ataques de malware. En comparación con los dispositivos de Apple, los dispositivos macOS son más asequibles y cuentan con una mayor cantidad de usuarios. Sin embargo, a medida que los dispositivos macOS se vuelven cada vez más integrados en la vida cotidiana de los consumidores, se vuelven más atractivos para los vendedores en línea.