Los grupos de hackers están anunciando un nuevo ladrón de información para el sistema operativo Apple macOS, llamado Atomic macOS Stealer (AMOS) en Telegram por $1,000 dólares por un mes, uniéndose a MacStealer.

> *«Atomic macOS Stealer puede robar varios tipos de información de la máquina de la víctima, incluyendo las contraseñas del llavero, la información completa del sistema, los archivos del escritorio y la carpeta de documentos, e incluso la contraseña de macOS»,* dijeron los investigadores de Cyble en un informe técnico.

Entre otras características, se incluye su capacidad para extraer datos de navegadores web y billeteras de criptomonedas como Atomic, Binance, Coinomi, Electrum y Exodus. Los hackers que compran el ladrón a sus desarrolladores también reciben un panel web listo para usar para administrar a las víctimas.

El malware toma la forma de un archivo de imagen de disco sin firmar (Setup.dmg) que, al ejecutarse, insta a la víctima a ingresar su contraseña del sistema en un aviso falso para escalar los privilegios y realizar sus actividades maliciosas, una técnica también adoptada por MacStealer.

El vector de intrusión inicial usado para entregar el malware no está claro inmediatamente, aunque es posible que los usuarios sean manipulados para descargarlo y ejecutarlo bajo la apariencia de software legítimo.

El artefacto, enviado a VirusTotal el 24 de abril de 2023, también lleva el nombre «Notion-7.0.6.dmg», lo que sugiere que se propaga como la popular aplicación para tomar notas. Otras muestras desenterradas por MalwareHunterTeam se distribuyen como «Photoshop CC 2023.dmg» y «Tor Browser.dmg».

> *«El malware como Atomic macOS Stealer podría instalarse explotando vulnerabilidades o alojándose en sitios web de phishing»,* dijo Cyble.

Después, Atomic procede a recopilar los metadatos del sistema, los archivos, el llavero de iCloud, así como la información almacenada en los navegadores web (por ejemplo, contraseñas, autocompletado, cookies, datos de tarjetas de crédito) y extensiones de billetera criptográfica, todo lo cual se comprime en un archivo ZIP y se envía a un servidor remoto. Después, el archivo ZIP de la información compilada se envía a los canales de Telegram preconfigurados.

El desarrollo es otra señal de que macOS se está convirtiendo cada vez más en un objetivo lucrativo más allá de los grupos de hackers de los estados nacionales para implementar malware ladrón, por lo que es imperativo que los usuarios solo descarguen e instalen software de fuentes confiables, habiliten la autenticación de dos factores, revisen los permisos de las aplicaciones y se abstengan de abrir enlaces sospechosos recibidos por medio de correos electrónicos o mensajes SMS.