Un malware conocido por apuntar al sistema operativo macOS se actualizó nuevamente para agregar más funciones a su conjunto de herramientas que le permiten acumular y exfiltrar datos confidenciales almacenados en una variedad de aplicaciones, incluyendo Google Chrome y Telegram, como parte de más *«refinamientos en sus tácticas».*

XCSSET se descubrió en agosto de 2020, cuando se supo que estaba dirigido a desarrolladores de Mac utilizando un medio de distribución inusual que implicaba inyectar una carga útil maliciosa en proyectos IDE de Xcode que se ejecuta en el momento de crear archivos de proyecto en Xcode.

El malware cuenta con muchas capacidades, como leer y descargar cookies de Safari, inyectar código JavaScript malicioso en varios sitios web, robar información de aplicaciones como Notes, WeChat, Skype, Telegram y encriptar archivos de usuario.

A inicios de abril, XCSSET recibió una actualización que permitió a los autores de malware apuntar a macOS 11 Big Sur, así como a Mac que se ejecuten en el chipset M1, eludiendo las nuevas políticas de seguridad agregadas por Apple en el último sistema operativo.

> *«El malware descarga su propia herramienta abierta de su servidor C2 que viene pre-firmada con una firma ad-hoc, mientras que si estuviera en las versiones 10.15 de macOS y anteriores, aún utilizaría el comando de apertura integrado del sistema para ejecutar las aplicaciones»,* dijeron los investigadores de Trend Micro.

Ahora, según un nuevo artículo publicado por la compañía de seguridad este jueves, se ha descubierto que XCSSET ejecuta un archivo AppleScript malicioso para comprimir la carpeta que contiene los datos de Telegram («~ / Library / Group Containers / 6N38VWS5BX.ru.keepcoder.Telegram») en un archivo ZIP, antes de cargarlo en un servidor remoto bajo su control, lo que permite que el actor de la amenaza inicie sesión con las cuentas de la víctima.

Con Google Chrome, el malware intenta robar las contraseñas almacenadas en el navegador

web, que a su vez se cifran con una contraseña maestra llamada *«clave de almacenamiento seguro»*, engañando al usuario para que otorgue privilegios de root mediante un cuadro de diálogo fraudulento, abusando de los permisos elevados para ejecutar un comando de shell no autorizado para recuperar la clave maestra del llavero de iCloud, después de lo cual, el contenido se descifra y se transmite al servidor.

Además de Chrome y Telegram, XCSSET también tiene la capacidad de robar información valiosa de varias aplicaciones como Evernote, Opera, Skype, WeChat y las propias aplicaciones de Contactos y Notas de Apple al recuperar dichos datos de sus respectivos directorios sandbox.

> *«El descubrimiento de cómo puede r*obar información de varias aplicaciones destaca el grado en que el malware intenta robar de forma agresiva varios tipos de información de los sistemas afectados», dijeron los investigadores.