Microsoft ha identificado una nueva variante de un malware conocido para macOS, llamado XCSSET, que ha sido detectado en ataques limitados en entornos reales.

> *«Siendo la primera versión detectada desde 2022, esta nueva variante de XCSSET presenta técnicas avanzadas de ofuscación, mecanismos de persistencia renovados y estrategias de infección mejoradas»*, informó el equipo de Inteligencia de Amenazas de Microsoft en una publicación en X.
>
> *«Estas nuevas capacidades se suman a las ya conocidas de esta familia de malware, como el robo de credenciales de billeteras digitales, la extracción de información de la aplicación Notas y la filtración de archivos y datos del sistema.»*

XCSSET es un malware modular sofisticado diseñado para infectar proyectos de Apple Xcode y comprometer a los usuarios de macOS. Fue identificado por primera vez por Trend Micro en agosto de 2020.

Las versiones posteriores del malware han demostrado su capacidad para adaptarse a ediciones más recientes de macOS y a los chipsets M1 de Apple. A mediados de 2021, expertos en ciberseguridad señalaron que XCSSET había evolucionado para extraer información de múltiples aplicaciones, como Google Chrome, Telegram, Evernote, Opera, Skype, WeChat y programas nativos de Apple, como Contactos y Notas.

Un informe adicional de Jamf, publicado en el mismo período, reveló que el malware aprovechaba la vulnerabilidad CVE-2021-30713, que afecta el sistema de Transparencia, Consentimiento y Control (TCC), permitiéndole tomar capturas de pantalla del escritorio de la víctima sin requerir permisos adicionales.

Más de un año después, el código malicioso fue actualizado nuevamente para incluir compatibilidad con macOS Monterey. Hasta la fecha, se desconoce su origen.

Los más recientes hallazgos de Microsoft representan la primera modificación significativa desde 2022, con técnicas de ofuscación mejoradas y métodos de persistencia optimizados para dificultar su detección y garantizar su ejecución en cada inicio de sesión del shell.

Una de las nuevas estrategias que XCSSET emplea para mantenerse activo es descargar una versión firmada de la herramienta «dockutil» desde un servidor de comando y control, con el fin de manipular los elementos del dock.

> *«El malware crea una versión falsa de la aplicación Launchpad y modifica su ruta en el dock, reemplazando la original con esta copia maliciosa. De esta forma, cada vez que el usuario inicia Launchpad desde el dock, tanto la aplicación legítima como el código malicioso se ejecutan simultáneamente»,* explicó Microsoft.