Los operadores del malware XCSSET macOS aumentaron sus apuestas al realizar mejoras iterativas que agregan soporte para macOS Monterey al actualizar sus componentes de código fuente a Python 3.

> *«Los autores del malware pasaron de ocultar el ejecutable principal en una Xcode.app falsa en las versiones iniciales en 2020 a una Mail.app falsa en 2021 y ahora a una Notes.app falsa en 2022»,* dijeron los investigadores de SentinelOne, Phil Stokes y Dinesh Devadoss.

XCSSET, documentado por primera vez por Trend Micro en 2020, tiene muchas partes móviles que le permiten recopilar información confidencial de Apple Notes, WeChat, Skype y Telegram; inyectar código JavaScript malicioso en varios sitios web y descargar las cookies del navegador web Safari.

Las cadenas de infección implican el uso de un cuentagotas para comprometer los proyectos Xcode de los usuarios con la backdoor, y este último también toma medidas para evadir la detección haciéndose pasar por el software del sistema o la aplicación del navegador web Google Chrome.

El ejecutable principal es un AppleScript que está diseñado para recuperar cargas útiles de AppleScript de segunda etapa desde una red de servidores remotos que extraen datos almacenados en navegadores web como Google Chrome, Mozilla Firefox, Microsoft Edge, Brave y Yandex Browser, así como aplicaciones de chat como Telegram y Wechat.

También se sabe que el atacante usa un AppleScript personalizado («listing.applescript») para determinar *«qué tan actualizada está la víctima con la herramienta de eliminación de malware XProtect y MRT de Apple, presumiblemente lo mejor para atacarlos con cargas útiles más efectivas»,* dijeron los investigadores.

Uno de los aspectos novedosos del ataque es que la implmentación del malware dentro de los proyectos de Xcode se considera un método de propagación por medio de los repositorios

de GitHub para expandir aún más su alcance.

Además de aprovechar AppleScripts, el malware también aprovecha los scripts de Python para colocar iconos de aplicaciones falsas en el Dock de macOS y robar datos de la aplicación Notes legítima.

La última versión de XCSSET también se destaca por incorporar modificaciones a AppleScripts para dar cuenta de la eliminación de Python 2.7 de macOS 12.3 de Apple lanzada el 14 de marzo de 2022, lo que indica que los autores están actualizando continuamente el malware para aumentar sus posibilidades de éxito.

Con ese fin, se cree que el atacante actualizó su «*safari_remote.applescript*» al eliminar Python 2 a favor de Python 3 para sistemas que ejecutan macOS Monterey 12.3 y superior.

A pesar de estar en libertad por dos años, se sabe muy poco sobre la identidad de los atacantes y sus motivaciones o sus objetivos exactos. Se informaron ataques del malware XCSSET en China en mayo de 2022 que exigieron a las víctimas pagar 200 USDT a cambio de desbloquear cuentas robadas.

> *«En este momento, no está claro si estos repositorios infectados son víctimas o plantas de los actores de amenazas que esperan infectar a los usuarios desprevenidos. Se ha sugerido que los usuarios desprevenidos pueden ser señalados a los repositorios infectados por medio de tutoriales y capturas de pantalla para desarrolladores novatos»,* dijeron los investigadores.