Investigadores de seguridad informática han descubierto un conjunto de artefactos maliciosos que afirman formar parte de un conjunto de herramientas sofisticadas dirigidas a los sistemas Apple macOS.

> *«Hasta ahora, estas muestras han pasado en gran medida desapercibidas y se dispone de muy poca información sobre ninguna de ellas»,* indicaron los investigadores de Bitdefender Andrei Lapusneanu y Bogdan Botezatu en un informe preliminar publicado el viernes.

El análisis realizado por la empresa rumana se basa en el estudio de cuatro muestras que fueron cargadas en VirusTotal por una víctima no identificada. La muestra más antigua se remonta al 18 de abril de 2023.

Se dice que dos de los tres programas maliciosos son puertas traseras genéricas basadas en Python diseñadas para atacar sistemas Windows, Linux y macOS. Los cargamentos han sido denominados colectivamente como JokerSpy.

El primer componente es shared.dat, que, una vez activado, realiza una verificación del sistema operativo (0 para Windows, 1 para macOS y 2 para Linux) y establece contacto con un servidor remoto para obtener instrucciones adicionales para su ejecución.

Esto incluye recopilar información del sistema, ejecutar comandos, descargar y ejecutar archivos en la máquina víctima y finalizar por sí mismo.

En dispositivos que ejecutan macOS, el contenido codificado en Base64 obtenido del servidor se escribe en un archivo llamado *«/Users/Shared/AppleAccount.tgz»* que posteriormente se descomprime y se lanza como la aplicación *«/Users/Shared/TempUser/AppleAccountAssistant.app».*

El mismo procedimiento, en sistemas Linux, valida la distribución del sistema operativo mediante la verificación del archivo «/etc/os-release». Luego, se escribe código C en un

archivo temporal «tmp.c», que se compila en un archivo denominado «/tmp/.ICE-unix/git» utilizando el comando cc en Fedora y gcc en Debian.

Bitdefender también descubrió una *«puerta trasera más poderosa»* entre las muestras, un archivo etiquetado como «sh.py» que cuenta con un conjunto extenso de capacidades para recopilar metadatos del sistema, enumerar archivos, eliminar archivos, ejecutar comandos y archivos, y extraer datos codificados en lotes.

El tercer componente es un binario FAT conocido como xcc, escrito en Swift y dirigido a macOS Monterey (versión 12) y versiones más recientes. El archivo contiene dos archivos Mach-O para las dos arquitecturas de CPU gemelas, x86 Intel y ARM M1.

> *«Su propósito principal aparentemente es verificar los permisos antes de utilizar un componente potencial de software espía (probablemente para capturar la pantalla), pero no incluye el componente de software espía en sí»,* señalaron los investigadores.

> *«Esto nos lleva a concluir que estos archivos forman parte de un ataque más elaborado y que faltan varios archivos en el sistema que investigamos.»*

Las conexiones de espionaje de xcc se originan a partir de una ruta identificada dentro del contenido del archivo, *«/Users/joker/Downloads/Spy/XProtectCheck/»*, y debido a que verifica los permisos como Acceso a Disco, Grabación de Pantalla y Accesibilidad.

Aún se desconoce la identidad de los actores detrás de esta actividad. Actualmente tampoco está claro cómo se obtiene el acceso inicial y si implica algún tipo de manipulación social o spear-phishing.

Esta divulgación se produce un poco más de dos semanas después de que la compañía rusa

de ciberseguridad Kaspersky revelara que los dispositivos iOS han sido objetivo de una campaña móvil sofisticada y de larga duración llamada Operación Triangulación, que comenzó en 2019.