Se ha identificado la presencia de aplicaciones piratas dirigidas a usuarios de Apple macOS que incluyen un backdoor capaz de proporcionar a los atacantes control remoto sobre las máquinas infectadas.

> *«Estas aplicaciones se encuentran alojadas en sitios web chinos dedicados a la piratería, con el objetivo de atraer víctimas»,* indicaron los investigadores de Jamf Threat Labs, Ferdous Saljooki y Jaron Bradley.
>
> *«Una vez activado, el malware descarga y ejecuta múltiples elementos en segundo plano con el fin de comprometer de manera encubierta el sistema de la víctima».*

Los archivos de imagen de disco (DMG) comprometidos, que han sido alterados para establecer comunicación con una infraestructura controlada por actores malintencionados, incluyen aplicaciones legítimas como Navicat Premium, UltraEdit, FinalShell, SecureCRT y Microsoft Remote Desktop.

Estas aplicaciones no firmadas, además de ser hospedadas en un sitio web chino llamado macyy[.]cn, incorporan un componente de carga denominado «dylib» que se ejecuta cada vez que se abre la aplicación.

Este componente actúa como un conducto para obtener un backdoor («bd.log») y un descargador («fl01.log») desde un servidor remoto, utilizado para establecer persistencia y obtener elementos adicionales en la máquina comprometida.

El backdoor, ubicado en la ruta «/tmp/.test», es una herramienta completa construida sobre la base de un conjunto de herramientas de post-explotación de código abierto llamado Khepri. La elección de la ruta «/tmp» implica que será eliminado al apagar el sistema.

A pesar de esto, se volverá a crear en la misma ubicación la próxima vez que se ejecute la aplicación pirateada y se active el componente de carga.

Por otro lado, el descargador se escribe en la ruta oculta «/Users/Shared/.fseventsd», tras lo cual crea un LaunchAgent para asegurar persistencia y envía una solicitud HTTP GET a un servidor controlado por los atacantes.

Aunque el servidor ya no está accesible, el descargador está diseñado para escribir la respuesta HTTP en un nuevo archivo ubicado en /tmp/.fseventsds y luego ejecutarlo.

Jamf señaló que este malware comparte varias similitudes con ZuRu, previamente observado propagándose a través de aplicaciones pirateadas en sitios chinos.

> *«Es plausible que este malware sea una evolución del malware ZuRu, dada su orientación específica hacia ciertas aplicaciones, modificaciones en los comandos de carga y la infraestructura de los atacantes»,* concluyeron los investigadores.