Aparece en el entorno una nueva versión de un malware diseñado para atacar los sistemas Apple macOS, denominado XLoader, que oculta sus características maliciosas bajo la apariencia de una aplicación de productividad de oficina denominada *«OfficeNote»*.

> *«Esta variante reciente de XLoader se encuentra en un paquete dentro de una imagen de disco estándar de Apple bajo el nombre de OfficeNote.dmg. La aplicación contenida en el interior está firmada con la identificación del desarrollador MAIT JAKHU (54YDV8NU9C)»*, informaron los investigadores de seguridad de SentinelOne, Dinesh Devadoss y Phil Stokes, en un análisis publicado el pasado lunes.

XLoader, que fue identificado por primera vez en 2020, se considera un sucesor de Formbook y se presenta como un software que roba información y registra las pulsaciones de teclado, y se ofrece bajo el modelo de malware como servicio (MaaS). Una versión de este malware diseñada para macOS emergió en julio de 2021, siendo distribuida como un programa Java en forma de un archivo .JAR compilado.

> *«Estos archivos necesitan el entorno de ejecución de Java, y por esa razón, el archivo .jar malicioso no se ejecutará en una instalación de macOS sin configuraciones adicionales, ya que Apple dejó de incluir JRE en sus sistemas hace más de una década»,* señaló la empresa de ciberseguridad en ese momento.

La versión más reciente de XLoader logra evadir esta limitación cambiando su enfoque hacia lenguajes de programación como C y Objective C, con el archivo de imagen de disco siendo firmado el 17 de julio de 2023. Desde entonces, Apple ha revocado dicha firma.

SentinelOne informó que detectó múltiples instancias del archivo sospechoso en VirusTotal a lo largo del mes de julio de 2023, lo que sugiere una campaña de propagación bastante extensa.

> *«Anuncios en foros dedicados al cibercrimen ofrecen la versión de XLoader diseñada para Mac en alquiler, con un costo de $199 al mes o $299 por un período de 3 meses. Es interesante notar que esto resulta relativamente más costoso en comparación con las variantes de XLoader diseñadas para Windows, que se comercializan a $59 al mes o $129 por un período de 3 meses»*, señalaron los investigadores.

Una vez que se ejecuta, OfficeNote muestra un mensaje de error que indica que *«no se puede abrir debido a que no se puede encontrar el elemento original»,* pero, en realidad, instala un Agente de Inicio en segundo plano para asegurar su persistencia en el sistema.

XLoader ha sido diseñado con el propósito de recopilar datos del portapapeles, así como información almacenada en las carpetas asociadas a navegadores web como Google Chrome y Mozilla Firefox. Sin embargo, Safari no se encuentra entre sus objetivos.

Además de implementar medidas para evitar ser detectado tanto de manera manual como por soluciones automatizadas, el malware está configurado para ejecutar comandos de pausa con el fin de retrasar su ejecución y pasar desapercibido.

> *«XLoader sigue representando una amenaza latente para los usuarios y las empresas que utilizan macOS»,* concluyen los investigadores.

> *«Esta última versión, que se camufla como una aplicación de productividad de oficina, evidencia que los objetivos de interés están claramente relacionados con usuarios en entornos de trabajo. El malware intenta sustraer secretos de navegadores web y del portapapeles, los cuales podrían ser utilizados o vendidos a otros actores de amenazas para llevar a cabo compromisos adicionales».*