Investigadores en ciberseguridad han identificado una nueva variante de un ladrón de información para macOS conocido como MacSync, que se distribuye mediante una aplicación Swift firmada digitalmente y notarizada, la cual se hace pasar por un instalador de una app de mensajería para eludir los controles de Gatekeeper de Apple.

"A diferencia de las variantes anteriores de MacSync Stealer, que se apoyaban principalmente en técnicas de arrastrar al terminal o en métodos tipo ClickFix, esta muestra adopta un enfoque mucho más engañoso y prácticamente sin interacción del usuario", señaló Thijs Xhaflaire, investigador de Jamf.

La empresa de gestión de dispositivos Apple y seguridad indicó que la versión más reciente se propaga como una aplicación Swift firmada y notarizada, incluida dentro de una imagen de disco (DMG) llamada "zk-call-messenger-installer-3.9.2-lts.dmg", alojada en "zkcall[.]net/download".

El hecho de que esté firmada y notarizada permite que el archivo se ejecute sin ser bloqueado ni marcado por los controles de seguridad integrados, como Gatekeeper o XProtect. No obstante, se ha observado que el instalador muestra instrucciones que invitan a los usuarios a hacer clic derecho y abrir la aplicación, una táctica habitual para esquivar estas protecciones. Apple ya revocó el certificado de firma de código asociado.

Posteriormente, el dropper basado en Swift realiza una serie de comprobaciones antes de descargar y ejecutar un script codificado a través de un componente auxiliar. Entre estas validaciones se incluyen la comprobación de conectividad a Internet, la imposición de un intervalo mínimo de ejecución de aproximadamente 3600 segundos para limitar la frecuencia, así como la eliminación de atributos de cuarentena y la validación del archivo antes de su ejecución.

"Resulta especialmente llamativo que el comando curl utilizado para recuperar la carga útil presenta claras diferencias frente a variantes anteriores", explicó Xhaflaire. *"En lugar de emplear la combinación habitual -fsSL, las banderas se han separado en -fL y -sS, y además se han añadido opciones como –noproxy"*.

"Estos cambios, junto con el uso de variables que se rellenan dinámicamente, apuntan a una modificación intencional en la forma en que se obtiene y valida la carga útil, probablemente con el objetivo de mejorar la fiabilidad o evadir la detección".

Otro mecanismo de evasión detectado en esta campaña es el uso de archivos DMG inusualmente grandes, cuyo tamaño se incrementa hasta 25.5 MB mediante la inclusión de documentos PDF sin relación alguna.

La carga útil codificada en Base64, una vez decodificada, corresponde a MacSync, una versión renombrada de Mac.c que apareció por primera vez en abril de 2025. Según Moonlock Lab de MacPaw, MacSync incorpora un agente completo basado en Go, que no solo roba información, sino que también habilita capacidades de control y comando remoto.

Cabe destacar que también se han detectado archivos DMG maliciosos firmados que imitan a Google Meet en ataques destinados a propagar otros ladrones de macOS, como Odyssey. Aun así, los actores de amenazas han seguido recurriendo a imágenes de disco sin firmar para distribuir DigitStealer incluso tan recientemente como el mes pasado.

"Este cambio en los métodos de distribución refleja una tendencia más amplia en el ecosistema de malware para macOS, donde los atacantes buscan cada vez más introducir su malware en ejecutables firmados y notarizados, haciéndolos pasar por aplicaciones legítimas", concluyó Jamf.