Investigadores de seguridad cibernética descubrieron un spyware previamente no documentado dirigido al sistema operativo Apple MacOS.

Se cree que el malware, cuyo nombre en código es CloudMensis por la compañía de seguridad cibernética ESET, utiliza exclusivamente servicios de almacenamiento en la nube pública como pCloud, Yandex Disk y Dropbox para recibir comandos de atacantes y extraer archivos.

> *«Sus capacidades muestran claramente que la intención de sus operadores es recopilar información de las Mac de las víctimas extrayendo documentos, pulsaciones de teclas y capturas de pantalla»,* dijo Marc-Etienne M. Léveillé, investigador de ESET.

CloudMensis, escrito en Objective-C, se descubrió por primera vez en abril de 2022, y está diseñado para atacar a las arquitecturas de silicio de Intel y Apple. El vector de infección inicial de los ataques y los objetivos aún son desconocidos. Pero su distribución muy limitada es una indicación de que el malware se está utilizando como parte de una operación altamente dirigida contra entidades de interés.

La cadena de ataque detectada por ESET abusa de la ejecución de código y los privilegios administrativos para lanzar una carga útil de primera etapa que se usa para obtener y ejecutar un malware de segunda etapa alojado en pCloud, que a su vez, extrae documentos, capturas de pantalla y archivos adjuntos de correo electrónico, entre otros.

También se sabe que el descargador de primera etapa borra los rastros de Safari sandbox y exploits de escalada de privilegios que hacen uso de cuatro vulnerabilidades de seguridad ya resueltas en 2017, lo que sugiere que CloudMensis puede haber pasado desapercibido durante muchos años.

El implante también cuenta con funciones para eludir el marco de seguridad de Transparencia, Consentimiento y Control (TCC), cuyo objetivo es garantizar que todas las aplicaciones obtengan el consentimiento del usuario antes de acceder a archivos en Documentos, Descargas, Escritorio, iCloud Drive y volúmenes de red.

Esto se logra al explotar otra vulnerabilidad de seguridad parcheada rastreada como CVE-2020-9934 que se dio a conocer en 2020. Otras funciones compatibles con la puerta trasera incluyen obtener la lista de procesos en ejecución, realizar capturas de pantalla, enumerar archivos de dispositivos de almacenamiento extraíbles y ejecutar comandos shell y otras cargas útiles arbitrarias.

Además, un análisis de los metadatos de la infraestructura de almacenamiento en la nube muestra que las cuentas de pCloud se crearon el 19 de enero de 2022, y los compromisos comenzaron el 4 de febrero y alcanzaron su punto máximo en marzo.

> *«La calidad general del código y la falta de ofuscación muestran que los autores pueden no estar muy familiarizados con el desarrollo de Mac y no son tan avanzados. Sin embargo, se invirtieron muchos recursos para hacer de CloudMensis una poderosa herramienta de espionaje y una amenaza para los objetivos potenciales»,* dijo M. Léveillé.