Una nueva variante del malware para macOS rastreado como UpdateAgente fue detectada, lo que indica intentos continuos por parte de sus autores para actualizar las funcionalidades del malware.

> *«Quizás una de las características más identificables del malware es que se basa en la infraestructura de AWS para alojar sus diversas cargas útiles y realizar las actualizaciones de estado de infección en el servidor»,* dijeron los investigadores de Jamf Threat Labs.

UpdateAgent, detectado por primera vez a fines de 2020, se convirtió desde entonces en un lanzador de malware, lo que facilita la distribución de cargas útiles de segunda etapa, como el adware, al mismo tiempo que evita las protecciones de macOS Gatekeeper.

EL gotero basado en Swift recién descubierto, se hace pasar por binarios de Mach-O llamados «PDFCreator» y «ActiveDirectory» que al ejecutarse, establecen una conexión con un servidor remoto y recuperan un script bash para ejecutarlo.

> *«La principal diferencia es que llega a una URL diferente desde la que debe cargar un script bash»,* dijeron los investigadores.

Estos scripts de bash, llamados *«activedirec.sh» o «bash_qolveevgclr.sh»,* incluyen una URL que apunta a depósitos de Amazon S3 para descargar y ejecutar un archivo de imagen de disco (DMG) de segunda etapa en el punto final comprometido.

> *«El continuo desarrollo de este malware muestra que sus autores siguen activos, tratando de llegar a la mayor cantidad de usuarios posible»,* dijeron los investigadores.