Masterhacks – Un equipo de investigadores de seguridad localizó en la Deep Web dos sitios que tienen a la venta dos virus paquetizados, MacRansom y MacSpy, para que cualquier ciberdelincuente pueda efectuar ataques rápidos sin necesidad de conocimientos técnicos.

Se trata de un Ransomware as a Services (RaaS) y de un Malware as a Services (MaaS) respectivamente, ambos fueron desarrollados por el mismo delincuente informático y preparados para que cualquier persona pueda infectar ordenadores de Apple.

Las dos páginas que ponen a la venta los virus son sitios que se administran de forma cerrada, por lo que los usuarios tienen que ponerse en contacto con el autor para recibir las demos y negociar el precio de compra.

Los informes de los investigadores afirman que los dos virus son de poca calidad y creados por un desarrollador con poca experiencia, sin embargo, no significa que no sean peligrosos.

Fortinet, empresa de seguridad, afirma que MacRansom utiliza un cifrado simétrico, con las claves incluidas en el código fuente. El virus no se comunica con un servidor remoto de C&C, por lo que el autor no puede descifrar los archivos bloqueados.

A diferencia de otros RaaS, no cuenta con una interfaz web para que el atacante visualice los pagos, y por no tener una firma digital desencadenará alertas de seguridad al ejecutar una instalación estándar en MacOS.

Por otro lado, MacSpy fue analizado por la compañía Alien Vault, quienes afirman que se trata de un software espía para ordenadores Mac. Los expertos afirman que no es un malware profesional y tampoco dispone de firma digital.