Así ataca la CIA los sistemas operativos de Apple

27/07/2017

En este caso, bajo el nombre de proyecto 'Imperial', el portal de Julian Assange revela información sobre tres herramientas que utilizó la agencia de espionaje estadounidense para hackear y controlar Mac OS X, el sistema operativo de Apple.

La primera de ellas es 'Achilles', que permite a un atacante acceder a una imagen de disco (.DMG) e inyectar código en los archivos de instalación.

Como resultado, el usuario podría descargar un instalador de disco infectado en su Mac, abrirlo e instalar el software sin conocimiento del ataque.

Por otro lado, 'SeaPea' es una herramienta que proporciona a la CIA capacidades furtivas y de lanzamiento de otras herramientas, por lo que sirve para esconder los procesos y archivos que permiten al intruso mantener el acceso a Mac OS X.

Por último, está 'Aeris', un implante automatizado escrito en lenguaje de programación C que soporta varios sistemas basados ??en POSIX (Debian, RHEL, Solaris, FreeBSD, CentOS). Una vez instalado, permite al intruso la exfiltración de archivos y comunicaciones cifradas.

Todas estas herramientas fueron probadas en los sistemas operativos OS X 10.6 y OS X 10.7, más conocidos como 'Snow Leopard' y 'Lion', que fueron lanzados al mercado por Apple en 2009 y estuvieron en funcionamiento hasta el año 2016.

El proyecto 'Imperial' es una nueva entrega de 'Vault 7', una serie de documentos que Wikileaks comenzó a publicar el pasado 7 de marzo y que detalla las actividades de la CIA para llevar a cabo vigilancias masivas a través de dispositivos electrónicos, así como guerras cibernéticas.

En ese momento, el fundador del portal de filtraciones alertó de que la agencia de inteligencia estadounidense había "perdido el control de todo su arsenal de armas cibernéticas", que podrían estar en el mercado negro a disposición de "hackers" de todo el mundo.

"Es el mayor arsenal de virus y troyanos del mundo. Puede atacar la mayoría de los sistemas que utilizan periodistas, gente de los gobiernos y ciudadanos corrientes. No lo protegieron, lo perdieron, y luego trataron de ocultarlo", lamentó Assange durante una rueda de prensa a través de Internet.

El conjunto de archivos, fechados entre 2013 y 2016, incluyen detalles sobre las prestaciones del programa encubierto de 'hacking' (ataque cibernético) de la CIA, como la capacidad de comprometer televisores y teléfonos inteligentes, así como los sistemas operativos de Windows, macOS y Linux.