Masterhacks – WikiLeaks publicó este jueves una nueva entrega de Vault 7, la serie de documentos relacionados con las actividades de vigilancia masiva de la CIA.

Se trata del proyecto Imperial, en el que la CIA utilizó tres herramientas para hackear y tomar control de Mac OS X, de Apple.

La primera herramienta es Achilles, que permite al atacante acceder a una imagen de disco (DMG) e inyectar código en los archivos de instalación. Con esto, el usuario podría descargar un instalador de disco con código malicioso, instalarlo e infectar su equipo sin saberlo.

Otra herramienta es SeaPea, que proporciona a la agencia gubernamental las capacidades furtivas y de lanzamiento de otras herramientas, muy útil para esconder proceso y archivos que permiten al pirata informático mantener acceso a Mac OS X.

Finalmente, Aeris, un implante automatizado escrito en C, soporta varios sistemas basados en POSIX (Debian, RHEL, Solaris, FreeBSD, CentOS). Al ser instalado, el intruso puede tener acceso a archivos y comunicaciones cifradas.

Estas herramientas se han probado en los sistemas operativos OS X 10.6 y OS X 10.7, mejor conocidos como Snow Leopard y Lion, que se lanzaron al mercado por Apple en 2009 y funcionaron hasta 2016.

Imperial es una nueva entrega de Vault 7, un pack de documentos que WikiLeaks comenzó a publicar el pasado 7 de marzo y que muestra con detalle las actividades de la CIA para realizar vigilancia masiva por medio de dispositivos electrónicos.

En ese entonces, el fundador de WikiLeaks, Julian Assange afirmó que la agencia de inteligencia había *«perdido el control de todo su arsenal de armas cibernéticas»,* y que podrían estar en el mercado negro.

> *«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», dijo Assange en rueda de prensa.*