



Masterhacks - WikiLeaks añadió otra filtración a Vault7, una serie de filtraciones del portal que se relacionan con las herramientas de hacking de la CIA para espiar a sus enemigos. Esta nueva filtración se denomina CherryBlossom, un proyecto de la Agencia Central de Inteligencia estadounidense para hackear dispositivos WiFi para acceder a las redes públicas y privadas.

Según el informe de WikiLeaks, CherryBlossom se desarrolló e implementó con la ayuda de la organización Stanford Research Institute (SRI International). Es un firmware modificado que es capaz de comprometer dispositivos de red inalámbricos, como los routers y puntos de acceso que se utilizan como parte de la instalación de Internet en los hogares, espacios públicos y empresas.

Ante esto, resultaría fácil atacar routers y puntos de acceso para monitorizar, controlar y manipular el tráfico de Internet de los usuarios conectados a la red.

Este firmware se puede instalar de forma remota en algunos dispositivos, ya que en ocasiones permiten la actualización del firmware mediante un enlace. Al ser infectado, el dispositivo se convierte en un FlyTrap, que funciona como una baliza que se conecta a un servidor C&C por medio de Internet para proporcionar a los piratas cualquier información y ejecutar las acciones correspondientes.

Según WikiLeaks, dichas acciones incluyen tareas como monitorizar el correo electrónico y conversaciones de mensajería instantánea, recopilar direcciones MAC y números VoIP, o realizar copias de todo el tráfico de la red.

Con esta suman 12 filtraciones relacionadas con las armas de espionaje de la CIA.