



WikiLeaks publica nueva herramienta utilizada por la CIA para acceder remotamente a sitios web

Masterhacks - WikiLeaks publicó este jueves más documentos sobre Vault7, las herramientas de hacking que utiliza la CIA.

En este caso, el portal fundado por Julian Assange, afirma que la CIA pretende robar datos de los usuarios y obtener acceso remoto a un servidor o sitio web.

«Los implantes descritos en ambos proyectos están diseñados para interceptar y robar los datos SSH, pero funcionan en sistemas operativos y vectores de ataque diferentes», dice un comunicado difundido por WikiLeaks.

SSH es un protocolo criptográfico que proporciona a los usuarios acceso remoto a un servicio de portal web con detalles confidenciales de acerca de la dirección del servidor, número del puerto, usuario y contraseña.

WikiLeaks afirma que el «malware» BothanSpy ataca el programa cliente de SSH para el sistema Windows, robando los datos del usuario en las sesiones activas de SSH, datos que van a un servidor controlado por la CIA o se encriptan y se mantienen para ser utilizados después.

Para Linux existe un malware parecido denominado Gyrfalcon.