Masterhacks – WikiLeaks publicó una nueva herramienta que entra en la serie de filtraciones de Vault7, herramientas de hacking que utiliza la CIA para espiar a sus objetivos.

Se trata de Brutal Kangaroo, un malware desarrollado por la Agencia Central de Inteligencia de Estados Unidos, que tiene como objetivo infiltrarse en redes seguras conocidas como Air Gapped, compuestas por computadoras con Windows.

Una equipo air gapped es una máquina o red que se encuentra completamente aislada del exterior para proteger su seguridad. Por ello, no están conectadas a Internet ni a otro dispositivo, por lo que son más difíciles de hackear.

Según WikiLeaks, la CIA utilizaba Brutal Kangaroo para penetrar en los ordenadores seguros. Se compone de un conjunto de herramientas que emplean una memoria USB contaminada, con la finalidad de crear una red personalizada encubierta dentro de la red del objetivo.

El primer paso, según WikiLeaks, consiste en infectar un equipo conectado a Internet dentro de la empresa, este recibe el nombre de huésped primario. Ya que el malware está instalado en la computadora inicial, contamina con un virus diferente cualquier memoria USB o disco duro extraíble.

Luego, se espera que algún miembro de la organización utilice la unidad para conectarse al ordenador air gapped.

El proyecto Brutal Kangaroo se compone de los siguientes componentes:

- Drifting Deadline: herramienta de infección de la memoria USB.
- Shattered Assurance: herramienta de servidor que gestiona la infección automatizada de unidades de almacenamiento.
- Broken Promise: sistema que evalúa la información recogida.
- Shadow: mecanismo que actúa como una red encubierta de C&C.

El malware se aprovecha de una vulnerabilidad de Windows que se puede explotar mediante

enlaces a archivos hechos a mano que cargan y ejecutan programas sin la interación del usuario.

Con esta, ya son 13 las filtraciones de WikiLeaks relacionadas con herramientas de hacking de la CIA.