WikiLeaks revela la nueva arma de la CIA que actúa a través de las redes WiFi

ACTUALIDAD RT / LA HAINE :: 16/06/2017

La nueva filtración sobre el arsenal de ciberespionaje cibernético del régimen estadounidense pone al descubierto un arma llamada CherryBlossom que monitorea y controla dispositivos a través de las redes inalámbricas.

WikiLeaks ha revelado este jueves información sobre sobre el arsenal cibernético de la CIA que obtuvo en el marco de la filtración histórica apodada Vault 7. La nueva filtración, denominada CherryBlossom, versa sobre una arma homónima que afecta a los usuarios con WiFi en casas, oficinas de pequeñas y medianas empresas así como en espacios públicos.

La CIA habría desarrollado esta herramienta con apoyo de la ONG SRI International.

CherryBlossom es un programa informático que afecta a los dispositivos de las redes inalámbricas, como 'routers' para monitorear la actividad de sus usuarios y manipular su tráfico de Internet, aprovechando las vulnerabilidades de los dispositivos.

CherryBlossom puede instalarse en los dispositivos por vía inalámbrica, sin acceder a ellos físicamente, informa WikiLeaks. Una vez afectan a los dispositivos, los agentes de la CIA pueden realizar tareas de administración del sistema.

Filtraciones anteriores en el marco de Vault 7:

El programa Pandemic permite instalar 'troyanos' en toda las computadoras de una red local que opera bajo Windows.

El programa espía Athena es capaz de controlar todo el sistema informático de Microsoft Windows, incluyendo la configuración y el manejo de tareas, para descargar o cargar archivos desde o hacia un directorio específico.

Los 'software' maliciosos AfterMidnight y Assassin están diseñados para operar dentro del sistema operativo Microsoft Windows, donde monitorean y reportan acciones en el equipo 'host' y ejecutan acciones especificadas por la CIA.

El 'malware' llamado Archimedes permite hacerse rápidamente con el control de las computadoras de una red de área local (LAN), haciéndose pasar por una sesión común y corriente de navegadores de Internet.

La herramienta Scribbles de laCIA permite etiquetar y rastrear documentos creados con el software de Microsoft Office filtrados por informantes o robados por "oficiales de Inteligencia extranjeros".

La herramienta Weeping Angel de la CIA puede grabar, enviar o almacenar audio a través del micrófono incorporado en las televisiones inteligentes de la serie F de Samsung.

El 'software' Dark Matter está diseñado para infectar productos de la compañía estadounidense Apple aún después de borrar el disco duro y reinstalar el sistema operativo del dispositivo.

El programa Marble 'disfraza' los 'hackeos' de la CIA impidiendo a los investigadores forenses atribuirles virus, troyanos y ataques cibernéticos.

Desde octubre de 2014 la CIA estudia la posibilidad de infectar sistemas de control de vehículos utilizados por los coches y camiones modernos para "realizar asesinatos indetectables".

El programa malicioso Hive es usado por la agencia para enviar información desde máquinas atacadas por la CIA y permite hacerse con su control para efectuar tareas específicas.

La herramienta Grasshopper, indetectable por la mayoría de programas antivirus, va destinada a crear datos dañinos de forma individual para el sistema Windows.

_____

https://www.lahaine.org/mm_ss_mundo.php/wikileaks-revela-la-nueva-arma