WikiLeaks revela cómo la CIA se hace con el control de los navegadores

05/05/2017

'WikiLeaks' ha publicado este viernes una nueva filtración en la que revela cómo funciona el 'malware' llamado Archimedes, que usa la Agencia Central de Inteligencia de EE.UU. Esta herramienta 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.

Por lo general las redes LAN unen varios dispositivos dentro de las oficinas, pero también son usadas por algunos usuarios en sus casas.

La CIA espía el historial de los navegadores web de usuarios

El 'malware' infecta una computadora de la Red y envía el navegador web de esta computadora a un servidor especial que busca las vulnerabilidades mientras el usuario no percibe nada sospechoso. De esta forma la CIA puede infiltrarse en las redes locales para controlar y afectar a las computadoras de las que consta, explica WikiLeaks.

En el marco de la filtración sobre Archimedes, WikiLeaks publicó un manual sobre su uso, elaborado por la CIA, así como tres apéndices sobre el mismo y el manual de uso del programa malicioso Fulcrum, que permite usar

una compudadora infectada para afectar a otro dispositivo de una red local, así como espiar el tráfico de comunicaciones HTTP de las computadoras afectadas. Es decir, el programa espía el historial de los navegadores web de usuarios y permite ver qué páginas visita.

Esta publicación forma parte de la filtración a gran escala de archivos sobre armas cibernéticas de la CIA denominada Vault 7.

Filtraciones anteriores revelaron, entre otras cosas, que:

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.