WikiLeaks saca a la luz una nueva bestia de la CIA: cómo crackear intranets

ACTUALIDAD RT / LA HAINE :: 23/06/2017

La última tanda de documentos publicados por el portal de filtraciones muestra cómo funciona un programa 'malware' diseñado para penetrar en las redes corporativas más cerradas y mejor protegidas del mundo.

Usar memorias USB como conectores para superar la 'cortina de hierro' que separa la red local de las computadoras conectadas a Internet dentro de un mismo recinto, no es una tecnología nueva. Aprovechar las USB para robar datos necesarios para las agencias de los Estados dictatoriales es una posibilidad y ahora sabemos que la CIA la puso su práctica entre el 2015 y el 2016.

WikiLeaks ha publicado varios documentos que revelan cómo funciona este método bastante primitivo en la época de tecnología inalámbrica que vivimos. Un manual de usuario emitido por el Centro de Operaciones de Información de la CIA en febrero del 2016 enseña: la memoria USB es la herramienta principal.

El programa se llama 'Brutal Kangaroo'. Los documentos recolectados por el proyecto de Julian Assange demuestran que esta clase de espionaje solo funciona en las máquinas con sistema operativo Microsoft Windows.

Las redes físicamente aisladas existen en muchos bancos y entidades financieras, la industria de la energía nuclear, agencias de inteligencia y ejércitos, y también en algunas redacciones más avanzadas, que las usan para proteger sus fuentes, recuerda el diario 'La Repubblica', que ha sido el primero en analizar la nueva tanda filtrada por WikiLeaks.

Cómo funciona paso a paso:

- Primero se infecta la computadora conectada a Internet.

- Cuando el usuario inserta una memoria USB, la infección salta a ese pequeño dispositivo, ya en forma de un programa diferente.

- El tercer 'salto' del 'canguro' es conectar la USB a una computadora que forma parte de la red local protegida, una operación que algunos empleados reiteran varias veces en cada jornada laboral.

- Cuarto, la computadora local infecta a toda la red activando un plan de sabotaje o robo de datos.

Si múltiples computadoras en las redes protegidas están sometidas al control de la CIA, juntas "forman una red encubierta para coordinar tareas e intercambiar de datos", indica

WikiLeaks. El envío de datos de vuelta a la agencia se hace posible, asimismo, por medio de inserción sucesiva de un USB primero en las computadoras aisladas y luego en cualquier dispositivo conectado con Internet.

Aunque todo ese esquema no parece ser el proyecto más eficaz de la CIA, en realidad ha facilitado a los agentes infiltrarse en algunas redes que de otra manera permanecerían inalcanzables. Según los datos disponibles, el desarrollo del 'Brutal Kangaroo' arrancó en el 2012, dos años después del éxito del gusano informático Stuxnet, que supuestamente afectó a centenares de centrifugadoras en las plantas nucleares de Irán.

_____

https://www.lahaine.org/mm_ss_mundo.php/wikileaks-saca-a-la-luz