WikiLeaks publica el código fuente de HIVE, la herramienta de control de malware de la CIA

RUBÉN VELASCO :: 13/11/2017

WikiLeaks es el conocido portal a través del cual se han dado a conocer distintos secretos de la CIA y la NSA [y del régimen de EEUU]. Hace dos meses, por ejemplo, este portal publicaba información, bajo el nombre de "Vault 7", sobre 23 herramientas hacking utilizadas por la CIA para poder atacar y espiar cualquier ordenador del mundo a través de Internet. Continuando con sus filtraciones, hace algunas horas, este portal publicaba Vault 8, una nueva filtración de información de la CIA que, esta vez, nos da a conocer la herramienta que utiliza esta organización para controlar su malware a través de Internet.

Vault 8 es la nueva filtración de WikiLeaks centrada en dar a conocer Project HIVE. HIVE es una herramienta desarrollada por la CIA para controlar su malware de forma remota a través de Internet. Esta nueva filtración ha dado a conocer el código fuente de esta herramienta de control, así como los registros de desarrollo de la misma que nos permiten comprender mejor cómo funcionan.

Project HIVE es un centro de comando y control (C&C) utilizado por la organización para poder tener siempre su malware controlado de forma remota a través de Internet. A través de esta herramienta, la CIA se conectaba a su propio malware de manera que pudiera darle órdenes, enviarle comandos específicos y poder recuperar fácilmente toda la información que el software malicioso había recopilado sobre las víctimas.

HIVE ha sido diseñado para permitir controlar una gran cantidad de malware al mismo tiempo, como si se tratase de una botnet. Además, la CIA implementó una serie de medidas de seguridad (como tráfico VPN y conexiones a múltiples servidores que no tenían nada que ver con el Gobierno de Estados Unidos) de manera que, si por algún motivo un usuario detectaba esta herramienta ejecutándose en su sistema, no pudiera asociarla de ninguna manera a la CIA.

Esta herramienta ha permanecido en secreto durante mucho tiempo. Sin embargo, igual que en ocasiones anteriores, gracias a WikiLeaks la hemos podido conocer, y no solo eso, sino que el portal ha filtrado su código fuente de esta herramienta, ahora disponible para todos, que permite, no solo conocer mejor su funcionamiento, sino que piratas informáticos utilicen este software a su favor.

El código fuente de HIVE, publicado por Vault 8, no supone ningún peligro para los usuarios

El código fuente de HIVE ahora está disponible para cualquier usuario interesado en él a través de Internet. Por suerte, a diferencia de lo que ha ocurrido en otras ocasiones, cuando se dieron a conocer vulnerabilidades como EternalBlue, las filtraciones de Vault 8 no suponen un peligro, al menos directo, para los usuarios.

Es cierto que los piratas informáticos enseguida van a estudiar el código e implementar funciones en sus herramientas maliciosas, pero, directamente, no ofrece mucho más peligro para los usuarios.

Lo peligroso sería que WikiLeaks hiciera público el código fuente de las herramientas maliciosas de Vault 7. Estas herramientas sí suponen un peligro real para los usuarios ya que utilizan técnicas de ataque para ser indetectables y vulnerabilidades desconocidas que en minutos pueden poner en peligro a medio Internet.

Por suerte, de momento las filtraciones de Vault 7 no se han dado a conocer, y esperamos que siga así si no queremos enfrentarnos a un nuevo WannaCry, o a algo peor.

www.redeszone.net

---

https://www.lahaine.org/mm_ss_mundo.php/wikileaks-publica-el-codigo-fuente