Todo lo que debes saber sobre Vault 7, el arma cibernética de la CIA

Publicado: 7 mar 2017 19:40 GMT | Última actualización: 10 mar 2017 06:17 GMT

Una nueva filtración de WikiLeaks revela los sistemas de 'hacking', software malicioso y armas cibernéticas empleados por la agencia de espionaje estadounidense.

El portal de filtraciones Wikileaks ha comenzado este martes a difundir miles de documentos de un programa encubierto de 'hacking' (ataque cibernético) de la CIA, como parte de una serie de siete entregas, llamada 'Vault 7', que ha definido como **"la mayor filtración de datos de inteligencia de la historia"**.

Según ha informado la organización, la CIA perdió recientemente el control de la mayoría de su arsenal de 'hackeo', incluyendo malware, virus, troyanos, sistema de control remoto y documentación asociada, entre otros.

"Esta extraordinaria colección de varios cientos de millones de códigos dan a su poseedor la **capacidad de 'hacking' íntegra de la CIA**", explica Wikileaks en el comunicado. Así, el archivo parece haber estado circulando de forma no autorizada entre antiguos hackers y proveedores del Gobierno, uno de los cuales le ha proporcionado fragmentos a Wikileaks.

Esta primera entrega, llamada "Year Zero" (Año Cero), comprende **8.761 documentos y archivos**, procedentes de "una red aislada y de alta seguridad situada en el Centro de Inteligencia Cibernética de la CIA en Langley, Virginia". La mayoría de los documentos publicados exponen los sistemas de 'hacking', software malicioso y armas cibernéticas empleados por la agencia para el espionaje.

Todo sobre este tema

WikiLeaks 'desnuda' a la CIA

¿Una oportunidad para los denunciantes? WikiLeaks se burla del anuncio de pasantías en la CIA

Rusia demanda explicaciones de la CIA sobre las filtraciones de WikiLeaks

"El 'espionaje' a Trump podría ser el mayor escándalo en la historia de EE.UU."

Malware para hackear iPhones, Android y Smart TVs, entre otros

Wikileaks ha explicado que el arsenal de pirateo desarrollado por la CIA, concretamente por el Engineering Development Group (Grupo de Desarrollo de Ingeniería) ha alcanzado a todo tipo de dispositivos electrónicos y afecta a una amplia gama de productos estadounidenses y europeos, entre ellos el iPhone de Apple y el Android de Google.

Los teléfonos infectados envían a la CIA la **geolocalización del usuario, sus comunicaciones de audio y textos**, y también **activan la cámara y el micrófono** del aparato. Estas técnicas permiten a la CIA sortear el cifrado de WhatsApp, Signal, Telegram, Wiebo, Confide y Cloackman y recibir cualquier información de móviles 'hackeados' a distancia.

Además, el portal subraya que la CIA ha conseguido infectar Smart TVs para que, incluso estando apagadas, **funcionen como micrófonos** y, tras grabar las conversaciones que se desarrollan en la sala donde se encuentran, las retransmitan a un servidor de la agencia de espionaje.

Windows, McOs, Linux y Solaris, otros de los perjudicados

Wikileaks también revela que la agencia "realiza un esfuerzo muy importante para infectar y controlar a los usuarios de Microsoft Windows con su malware", y asegura que la capacidad de espionaje de la CIA también abarca a los sistemas operativos MacOS, Solaris y Linux, entre otros.

En este caso, los malwares pueden estar en dispositivos USB, CD, DVD, en áreas cubiertas en los discos o en sistemas para ocultar datos de imágenes. Además, realizan **ataques contra las redes de Internet y sus servidores** través de la Network Devices Branch (Red del Sistema de Dispositivos) de la CIA.

El consulado de EE.UU. en Fráncfort es una base de hackers de la CIA

Según los documentos filtrados, la CIA tiene en la localidad alemana de Francfort uno de sus mayores centros de ciberespionaje (el Agency's Center for Cyber Intelligence Europe Engineering), cuyo radio de acción **abarca toda Europa, el Norte de África y Oriente Próximo**.

Además, tal y como señala el portal, una vez en Francfort los hackers de la CIA pueden viajar sin ningún control de fronteras a cualquiera de los "25 países europeos que forman parte del espacio Schengen, incluyendo Francia, Italia y Suiza".

La proliferación de armas cibernéticas son un grave riesgo

Esta primera entrega pone de manifiesto que "las armas cibernéticas, **una vez desarrolladas, son muy difíciles de controlar**", ya que "las mismas personas que las desarrollan y las utilizan tienen las habilidades para hacer copias sin dejas huellas".

"En los últimos tres años, el sector de inteligencia de EE.UU., que consiste en agencias gubernamentales como la CIA y la NSA - la Agencia de Seguridad Nacional - y sus contratistas, como Booze Allan Hamilton, ha estado sujeto a una serie sin precedentes de filtraciones de datos por parte de sus propios trabajadores", denuncia el portal.

Además, Wikileaks subraya la existencia de un **"mercado de vulnerabilidad"** global que paga cientos de miles de millones de dólares por copias de esas "armas". Del mismo modo, los contratistas y las empresas que obtienen tales "armas" a veces las utilizan para sus propios fines, obteniendo una ventaja sobre sus competidores en la venta de servicios de "hacking".

Los ataques de 'día cero' de la CIA

Los 'día-cero' (en inglés, zero-day attacks) son ataques contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para la gente y el fabricante del producto, por lo que **no existen parches o sistemas que los combatan**.

La herramienta que la CIA usaría para 'maquillar' ciberataques y presentarlos como si fueran rusos

En este sentido, a raíz de las filtraciones de Edward Snowden sobre la Agencia de Seguridad Nacional estadounidense, la industria de la tecnología consiguió un compromiso de la administración Obama por el cual el ejecutivo estadounidense informaría de todos los peligros que podían vulnerar la seguridad de estas empresas.

Así, los documentos publicados por Wikileaks exponen no solo el alcance y la dirección del programa de 'hacking' encubierto de la CIA, sino todo un arsenal malicioso que incluye **docenas de posibles ataques de 'día cero'**, a través de fallos de software, contra varios productos.

La CIA evita las investigaciones forenses y los anti-virus

Según expone Wikileaks, la CIA utiliza malware para ayudar a los investigadores en las escenas de un crimen y, así, **eliminar cualquier huella digital** de la agencia, del Gobierno estadounidense o de sus empresas afiliadas.

En este sentido, el portal denuncia que la agencia de espionaje estadounidense utiliza mecanismos similares para ocultar sus 'hackeos' y las comunicaciones de malware. Además, los hackers de la CIA habrían desarrollado ataques contra los programas anti-virus más conocidos de las principales compañías informáticas.

Por último, WikiLeaks asegura que, al difundir toda esta documentación, ha tenido cuidado de no distribuir "armas cibernéticas cargadas" hasta que "emerja un consenso sobre la naturaleza política y técnica del programa de la CIA y de cómo tales 'armas' deben ser analizadas, desactivadas y publicadas".

María Jesús Vigo Pastur