Los teléfonos inteligentes son los equipos preferidos de las agencias de inteligencia para recabar información.

El arsenal secreto de la CIA

Modelos antiguos de los televisores inteligentes de Samsung también están en el centro de atención porque la CIA los utiliza para grabar conversaciones privadas. FOTO: SAMSUNG

SERGIO ALEJANDRO GÓMEZ

El mundo conoce cada vez mejor el funcionamiento y alcance de los servicios de espionaje de Estados Unidos. Si el excontratista Edward Snowden reveló en el 2013 el programa de vigilancia masiva de la NSA, ahora le tocó el turno a la Agencia Central de Inteligencia (CIA), considerada un Estado dentro del Estado por sus *modus operandi* e independencia del poder ejecutivo.

Según las más recientes revelaciones del portal Wikileaks, dirigido por el británico Julian Assange, la CIA comanda una red de hackers (piratas informáticos) que se dedica a explotar las brechas de seguridad de los equipos más usados del mundo, con el objetivo de recabar información e incluso llevar a cabo operaciones secretas.

Bajo el nombre clave de «Año Cero», el portal dispone de 8 761 documentos y archivos clasificados, que corresponden a un periodo entre el año 2013 y el 2016. El paquete proviene de una red de alta seguridad en el Centro de Inteligencia Cibernética de la CIA, en Langley, Virginia.

Para finales del 2016, según Wikileaks, la Agencia contaba con cerca de 5 000 especialistas dedicados a la ciberinteligencia y había producido más de mil programas de «hackeo», armas cibernéticas y software (programas) maliciosos para acceder a computadores, teléfonos inteligentes e incluso televisores Samsung.

La agencia perdió control sobre la mayor parte de su arsenal y este llegó a manos de antiguos hackers del gobierno y otros agentes privados de manera «no autorizada». Fue uno de ellos quien hizo llegar la información a Wikileaks.

Esta sería solo la primera entrega de una serie de revelaciones de mayor calado identificada como «Voult 7», que el portal clasifica como la mayor filtración de documentos confidenciales de la historia.

Assange, quien se encuentra en la embajada de Ecuador en Londres desde el 2012, refirió que existe un «riesgo extremo de proliferación en el desarrollo de ciberarmas» y las revelaciones de «Año Cero» abren un debate en las dimensiones políticas, legales y forenses de la problemática.

MÁS QUE TELEVISORES

Uno de los programas más llamativos incluye televisores inteligentes de la marca Samsung, de un modelo ya descontinuado.

El proyecto, nombrado One, utiliza los micrófonos integrados a las pantallas como un dispositivo de escucha electrónico, incluso cuando el equipo aparenta estar apagado. La información se guarda en el disco duro y se transmite a los servidores de la CIA una vez que el televisor se conecta a la red de redes.

Según el portal, este programa fue desarrollado en conjunto con la inteligencia británica.

ARMAS EN LOS BOLSILLOS

De acuerdo con lo revelado por Wikileaks, los teléfonos celulares son los objetivos preferidos por las agencias de inteligencia. Estos equipos se han convertido en parte de la vida diaria de miles de millones de personas en el mundo y guardan información sensible de los usuarios.

Los programas de la CIA estaban mayormente dirigidos a explotar brechas de seguridad en los sistemas operativos de los teléfonos, ya fueran Android (creado por Google) o iOs (de Apple).

Al hackear el sistema operativo se asegura el control sobre cualquier aplicación, independientemente del sistema que utilice para proteger los datos.

Para las empresas afectadas, que muchas veces anuncian sus teléfonos como los «más seguros del mundo», la noticia sobre cómo se utilizan sus vulnerabilidades cayó como un cubo de agua fría.

Apple aseguró que «la mayoría» de las brechas ya fueron resueltas en la última versión del sistema operativo que llevan los famosos Iphone y tabletas Ipad. Samsung, su gran rival sudcoreano y principal referente de los teléfonos Android, refirió por su parte que «la privacidad de los usuarios y la seguridad de nuestros dispositivos son prioritarias».

MENSAJERÍA CIFRADA

Otro paradigma de la tecnología moderna que parece amenazado por las recientes revelaciones es la invulnerabilidad de los servicios de mensajería cifrados más populares, como son Whatsapp, Signal y Telegram.

Muchos servicios de mensajería encriptan sus mensajes por seguridad, pero la CIA explota las vulnerabilidades de los teléfonos para acceder a la información. FOTO: AP

Los documentos muestran que la CIA cuenta con herramientas que permiten acceder a las conversaciones de dichos programas, recopilando mensajes de audio o texto.

Sin embargo, los especialistas aclaran que las técnicas utilizadas no son para romper el cifrado, sino que se valen de las vulnerabilidades del teléfono antes de que la información se encripte.

Open Whisper Systems, la empresa que desarrolló la tecnología de mensajería instantánea encriptada Signal, subrayó en Twitter que todos los documentos divulgados por Wikileaks mostraban sistemas que consistían «en introducir virus en los teléfonos. Ninguna de las fallas se encontró en Signal ni rompieron su protocolo de encriptamiento».

SISTEMAS OPERATIVOS EN LA MIRA

Las computadoras, servidores y equipos de redes tampoco quedaron bien parados en esta ocasión. Ya Apple, Microsoft y Google estuvieron en aprietos en el 2013 cuando Snowden demostró cómo la Agencia de Seguridad Nacional estadounidense (NSA) accedía a sus servidores.

Ahora se sabe también que la CIA posee técnicas para infectar y controlar las computadoras que corren el sistema operativo Windows. Uno de ellos, con el nombre clave de «Martillo Taladrador», se distribuye a través de los programas que se instalan desde unidades de CD y USB para hacer vulnerables a los usuarios.

La agencia también cuenta con armas «multiplataforma» que son capaces de explotar deficiencias en las computadoras con sistemas operativos MAC OS (Apple), Solaris y Linux.

DE CIENCIA FICCIÓN

Si bien las noticias de espionaje electrónico no son nada nuevo, muchos consideran que las revelaciones de Wikileaks abren una nueva era.

«Lo interesante es que muchas de las cosas que pensábamos que eran de ciencia ficción en realidad son posibles», dijo al sitio web especializado Teknautas Sergio de los Santos, director del área de Innovación y Laboratorio de la empresa de tecnología ElevenPaths.

Se abre incluso la posibilidad del acceso a los sistemas de control de los nuevos vehículos autónomos (conducidos por computadora) que, en opinión de De los Santos, podrían usarse «en asesinatos indetectables».

Otro programa, «Umbrage», estaría encargado de «recoger y administrar» las técnicas de ataque de otros países o agencias de espionaje, con el objetivo de «camuflar» las operaciones propias y confundir a los investigadores.

El propio Snowden, quien aún es buscado por Estados Unidos por las filtraciones del 2013, criticó en Twitter los métodos de la inteligencia de su país. «Imagina un mundo en que la CIA se pase el tiempo tratando de averiguar cómo espiarte a través de tu televisor. Eso es hoy», escribió.