Vault 7 Files: Los tentáculos del ciberespionaje

Los documentos filtrados por Wikileaks que acusan a la CIA de hackear dispositivos electrónicos domésticos, vuelven a sacudir el escenario mundial de la ciberseguridad. **Laura del Rio**

iPhones, dispositivos Android, Linux, Windows, Smart TV... todos los elementos que hacen de la actual una sociedad conectada y que la mayoría de usuarios ha incorporado a su vida laboral y personal como parte casi imprescindible de ella, son el objetivo principal del equipo de hackers de la CIA. Como en su día ocurrió con las filtraciones de Edward Snowden, Wikileaks hacía públicos a principios del mes de marzo los documentos conocidos con el nombre de Vault 7, que dejaban al descubierto el sofisticado programa de ciberespionaje que ha estado llevando a cabo la Agencia Central de Inteligencia estadounidense desde 2013 hasta 2016.

Que las agencias de inteligencia asuman tareas de espionaje no es algo que debería sorprender, sin embargo, teniendo en cuenta la magnitud de los documentos sacados a la luz, los usuarios se preguntan hasta dónde llegan las armas cibernéticas de la CIA y hasta qué punto está la información recopilada a salvo de caer en manos de los ciberdelincuentes. "La ciberinteligencia salva vidas", aclara Francisco Lázaro, director del Centro de Estudios de Movilidad e Internet de las Cosas de ISMS Forum, por tanto, "en un principio no deberíamos temerla". Algo tan importante como impedir un ataque terrorista es ahora mucho más factible gracias al desarrollo de estas prácticas. Detectar el fraude también es más sencillo, como es el caso de la detención en diciembre de 2013 de 80 empleados de los servicios de bomberos y de la policía de Nueva York que participaron en las labores de rescate del atentado del 11S. Estos fueron acusados de fraude de beneficios federales, cuya cantidad rondaba los 400 millones de dólares, al alegar discapacidad por enfermedad mental e imposibilidad de salir de su vivienda derivado del terror vivido en esas horas. Los investigadores empezaron a tirar del hilo al descubrir varias fotos de uno de los expolicías en redes sociales de vacaciones y a los mandos de una moto acuática.

El problema reside en ejercer el control adecuado sobre los datos. Aunque de momento los expertos no consideran que estas complejas herramientas se estén utilizando masivamente contra el común de los internautas, sino que más bien son ataques dirigidos, lo cierto es que nadie que se conecte a la Red está a salvo, "todos somos objetivo: ya sea por nosotros mismos, por personas con las que nos relacionamos o como peones de ataques a terceros", sentencia Lázaro. "Cuando entran en juego actores con intereses personales como empresas de seguridad que venden sus herramientas al mejor postor, es cuando la información se vuelve más vulnerable", añade. Al fin y al cabo, organizaciones gubernamentales, empresas particulares o redes de ciberdelincuencia utilizan herramientas muy similares que terminan formando parte del arsenal de todas y cada una de estas organizaciones.

No obstante, a pesar de que siempre sea la CIA la protagonista en este tipo de filtraciones, Estados Unidos no es el único país que ha puesto a sus servicios de inteligencia a trabajar en este ámbito. De hecho, el experto sospecha en que pronto habrá más fugas de información de otros países, como por ejemplo Rusia, aunque es difícil que estas filtraciones provengan de Estados con déficit de valores democráticos, que sean tan detalladas en medios públicos y que tengan como origen la propia organización de inteligencia.

Televisores, neveras, muñecas, coches, hasta marcapasos. Aunque ahora, y más con la evolución del Internet de las Cosas, todo es 'hackeable', el empeño por proteger la privacidad está lejos de convertirse en una obsesión, sino todo lo contrario. La sociedad aún está muy poco concienciada y muchos consideran el ciberespionaje como algo lejano, que solo ocurre en las películas. Tanto es así, que hasta las empresas y fabricantes continúan cometiendo errores de seguridad básicos como tener en sus equipos conexiones abiertas; contraseñas inexistentes, triviales, documentadas por defecto o predecibles; comunicaciones no cifradas; derechos excesivos; servidores no protegidos y un largo etcétera.

Pese a todo, Lázaro se muestra optimista y considera que el diseño de una normativa que se adapte al nuevo escenario de ciberseguridad, así como la inversión de los fabricantes, llegarán, "pero necesitan ser reclamadas e identificadas como necesarias por la sociedad", y en ese aspecto aún queda mucho por hacer. _

"La sociedad aún está muy poco concienciada y muchos consideran el ciberespionaje como algo lejano"