09-05-2015

Cifrando tus archivos, una forma de ejercer tu derecho a la privacidad informática

Israel Pirra
Rebelión

Hace poco menos de un año recibimos la noticia de que el proyecto TrueCrypt dejaba de desarrollarse, y no sólo eso, si no que los mismos desarrolladores recomendaban no usarlo ya que era inseguro, un misterio que hasta el dia de hoy no se sabe a ciencia cierta que ocurrió, sólo rumores.

TrueCrypt era una herramienta multiplataforma, que cifraba archivos en una carpeta generada desde tu sistema operativo sin necesidad de cifrar el disco entero, aparte de cifrarlos también escondía dicha carpeta de modo que mientras no se arrancara TrueCrypt en la computadora, éstos archivos cifrados permanecían, hasta cierto punto, invisibles.

Sin duda una herramienta muy útil para la privacidad de tus datos archivados en tu computadora, aunque desgraciadamente a este tipo de maravillas de cifrado informático siempre se le da un punto de vista malévolo haciendo pensar que quieres esconder algo "malo", nosotros creemos que no es que se quiera esconder algo "malo", más bien es ejercer el pleno derecho a la privacidad de tus datos, actualmente hay un abuso excesivo con la vigilancia de nuestros datos informáticos con intereses que van desde mercadotécnicos hasta políticos.

El misterio de TrueCrypt apareció el 28 de mayo del 2014 cuando en su sitio se anunciaba que ya no se desarrollaría más y que era inseguro, al mismo tiempo recomendaban una versión que sólo podía descifrar los archivos pero no cifrarlos. El proyecto siempre fué anónimo, nunca hubo contacto sobre los desarrolladores aunque siempre fué de código abierto, pero la mayoría de la comunidad de GNU/Linux no siempre confió del todo, ya que tenía una licencia un tanto restrictiva por lo cúal no era libre, como en la entrada en español de Wikipedia menciona: "El programa TrueCrypt se encuentra bajo una licencia muy pobre, que no solo no es libre, sino que es activamente peligrosa para los usuarios finales que la acepten, haciéndoles susceptibles a posibles acciones legales incluso si cumplen todos los términos de la licencia. Fedora ha hecho grandes esfuerzos para intentar trabajar con los desarrolladores de TrueCrypt para solucionar estos errores de su licencia, pero no ha tenido éxito."

Otras curiosidades es que la organización "TrueCrypt Foundation" estaba registrada en Estados Unidos bajo el nombre de Ondrej Tesarik y como marca registrada en República Checa por David Tesarik, aunque diversas páginas webs afirman que Ondrej Tesarik es un anagrama de "Trained Jokers" osea: "Bromistas Entrenados", vaya juego de palabras muy típico del mundo Nerd, y por último el dominio truecrypt.org estaba registrado en la Antártida.

A partir del cese del proyecto el rumor más grande fué de que TrueCrypt tuvo algunos problemas relacionados con la NSA (National Security Agency - Agencia Nacional de Seguridad) y decidieron parar el servicio, justo unos meses antes había mucha persecusión a proyectos informáticos por los casos de Chelsea Maning, Julian Assange y Edward Snowden, de hecho el servicio de correo Lavabit que se caracterizaba por tener medidas de provacidad y cifrado para sus usuarios, tuvo que cerrar en agosto del 2013, no se revelaron las causas pero el rumor más grande es de que la NSA pidio información sobre usuarios asi que decidieron desaparecer el proyecto antes de entregar archivos, como dato curioso, alguien que tenía su cuenta de correo electrónico en Lavabit era Edward Snowden, el ex-contratista de la NSA que decidió revelar las prácticas de vigilancia de los Estados Unidos.

Ante todo esto aún hay muchas herramientas que podemos utilizar para proteger nuestra privacidad, una de ellas muy similar a TrueCrypt es EncFS (Encrypted Filesystem http://www.arg0.net/#!encfs/c1awt) que cuenta con diversas intefaces gráficas para hacer más fácil su uso.
Entonces, como vemos, los intereses del control sobre nuestros datos es un problema latente y que no nos damos cuenta, hay manera de poder defendernos de éste abusivo ataque, como vemos, no solo organizaciones sociales sufren éste acoso, si no que también grandes proyectos como los antes mencionados han tenido que desaparecer sus servicios antes de entregar o descifrar sus contenidos.

Aunque el cifrado no es la seguridad absoluta (que de hecho no la hay) si es una buena práctica recomendada para el buen resguardo de nuestros datos privados. Juntate con los tuyos e informense, acudan al Hacklab o Hackerspace más cercano o bien entren a los foros y tutoriales en internet, hay mucha información útil.

Aquí comparto un temario que venimos experimentando desde el HacklabZAM hasta los proyectos que hoy en día estamos: https://we.riseup.net/hacklab+asamblea/seguridad_informatica