

Se llama Tails y es un sistema operativo basado en una versión de Linux que no solo es seguro y gratis, también anónimo. Es de hecho el sistema que Edward Snowden ha utilizado en muchas de sus comunicaciones, entre otras cosas porque se puede instalar en una memoria USB y conectar a cualquier ordenador sin dejar pista.

Los sistemas operativos basados en Linux e instalables en un lápiz USB no son nada nuevo, pero la diferencia de Tails es que promete anonimato completo. Snowden reconoce utilizarlo, y también el periodista Glenn Greenwald, quien destapó el espionaje masivo de la NSA gracias a los documentos filtrados por ex-agente de la CIA.

Los desarrolladores de Tails explican en su página que se trata de un sistema diseñado para preservar tu anonimato:

Te ayuda a navegar por Internet de forma anónima y a saltarte la censura casi en cualquier lugar que estés y en cualquier ordenador, pero sin dejar rastro a no ser que quieras hacerlo. Es un sistema operativo diseñado por completo para utilizarse desde un DVD, memoria USB o tarjeta SD, independientemente del sistema operativo original del ordenador.



La idea suena bien, o no, según se mire. Como señalan en *Wired*, los creadores de Tails son a su vez anónimos, nadie sabe muy bien quién está detrás. El motivo: ayudar a mantener el código del programa lejos de las manos de los gobiernos, aseguran. El problema es que debes confiar a ciegas en un sistema operativo del que no sabes nada en cuanto a sus creadores o qué ocurre con datos que ellos puedan recibir (si alguno). El único punto de garantía es que Edward Snowden o Glenn Greenwald lo han utilizado (y siguen haciéndolo). Que no es poco.

Tails utiliza Tor para navegar y mantener tu anonimato, además del programa *Pretty Good Privacy* o PGP, el sistema de gestión de contraseñas *KeePassX* y el plug-in *Off-the-Record* para cifrar chats. Los creadores de Tails aseguran que en ningún momento utiliza el disco duro del ordenador sobre el que lo utilices. El único espacio de almacenamiento al que recurre Tails es la memoria RAM, que se elimina automáticamente cuando se apaga el ordenador. Es decir, no habrá rastro ni de Tails ni de lo que has hecho con el portátil. Por eso sus creadores lo llaman un sistema operativo "*amnésico*". Aunque si se desea Tails, puede almacenar los resultados de su navegación en un dispositivo removible si está instalado en él y cuenta con una partición cifrada independiente, pero eso es solo optativo, perdiendo todas las ventajas de no dejar rastro si solo se ejecuta en memoria RAM.

Actualmente Tails en su versión 1.7 permite emular una visualización de que se está operando desde un Windows 8.1 para pasar desapercibido mientras es usado, sin embargo en versiones anteriores Tails emulaba la visión de ser un Windows XP, evidentemente solo lo aparentaba, ya que después disponía de herramientas de anonimización que carece cualquier otro Windows.

Pero Tails, no es solo su navegador TOR y sus proxys, Tails implementa una serie de herramientas de seguridad y anonimizado que posibilitarán su función. Por ello Tails reúne lo esencial de las herramientas y software (libres) que permiten comunicarse con una completa seguridad. Lo ideal es utilizar Tails como sistema operativo. Dicho esto, usted podría decidir instalar en su ordenador de trabajo todo o parte del software que viene preinstalado (el cual, en su mayoría, está disponibles para Windows o Mac, y por supuesto para GNU/Linux), en función de sus necesidades, con el fin de aprovechar sus funcionalidades, sin tener que instalar o utilizar Tails... excepto si usted se arriesga a utilizar estas puertas blindadas dejando una o más ventanas abiertas:

- Tor y su interfaz gráfica Vidalia para navegar en la red sin dejar rastro, y Torbutton para protegerse de códigos JavaScript maliciosos
- I2P, una red descentralizada y dinámica que permite navegar y comunicarse de forma segura y con un completo anonimato,
- HTTPS Everywhere, una extensión que obliga a su navegador a sólo acceder a los sitios Web más conocidos y utilizados en modo https (de forma

segura y cifrada),

- Pidgin preconfigurado con el módulo OTR (“Off-The-Record”), el software de mensajería instantánea (tipo GTalk, MSN, AIM o ICQ) seguro, cifrado y verdaderamente privado (que archiva dichas conversaciones... opción que puede desactivarse – en las “preferencias” si el acceso al sistema operativo no es lo suficientemente seguro ),
- GnuPG, versión “libre” de PGP, el software más popular y conocido de cifrado de e-mails y archivos, que permite además “firmar” sus correos y autenticarlos, para evitar cualquier usurpación de identidad: el software permite crear cajas fuertes cuya puerta está abierta, y donde cualquier persona puede dejar un mensaje, archivo o datos, antes de cerrar la puerta: únicamente el propietario de la clave de la caja fuerte podrá abrir la puerta... lo que hace de GPG uno de los estándares de la industria en lo que se refiere a seguridad informática,
- TrueCrypt, que permite crear particiones cifradas, o cajas fuertes electrónicas,
- PWGen, un generador de contraseñas sólidas,
- Florence un “teclado virtual” que permite introducir contraseñas pulsando en casillas con el ratón (o el trackpad) en lugar de utilizar el teclado, con el fin de protegerse de los keyloggers que registran todo lo que se escribe con el teclado del ordenador,
- MAT para dotar de anonimato a los meta datos contenidos en los archivos (fechas de creación y modificaciones, coordenadas GPS, identidad del usuario del ordenador o de la cámara de fotos, etc).

Pero Tails es algo más que una plataforma de navegación segura, como cualquier distribución de Unix/linux, es una plataforma de pentesting para lograr introducirse en sistemas y redes con fines lícitos o ilícitos, lo que lo hace muy versátil y a la vez peligroso en manos de usuarios desaprensivos o poco experimentados, ya que aunque se tenga una sensación de seguridad de que somos totalmente invulnerables e indetectables, recientemente se ha desarrollado software para evitar este anonimato en la red, el proyecto se ha denominado TORTazo.

Puede descargarlo aquí