Jul 9 2014

Distribución Linux Tails

By mar10

Hace poco me llegaron alertas al correo electrónico de noticias que me parecen alucinantes. Comentaban el interés de la NSA (Agencia de Seguridad Nacional de EEUU) por rastrear a usuarios que utilicen TAILS (distribución linux que hace un especial énfasis en la seguridad y el anonimato) aunque había otras que iban más allá y decían que simplemente por usuar linux los USA nos espían. Seguramente a los servicios de inteligencia y agencias de seguridad de muchos paises no les hará mucha gracia que redes como TOR , distribuciones como Tails sean también accesibles para otros mortales. Creo que estas noticias buscan "acojonar a los usuarios" que precisamente son más anónimos y navegan con más seguridad con una distribución como TAILS que con su Windows de toda la vida. Quizás la mayoría de los que se han hecho eco de esta noticia son defensores de Linux y toda su filosofía, pero bueno decir que una agencia de los EEUU como la NSA casi que te tiene fichado por usar linux es acojonar al personal. Por cierto acabo de bajar Tails para curiosearlo. En la página oficial tenéis el enlace de descarga del sistema el archivo .iso y el archivo de la firma criptográfica para verificar:

Página Oficial
https://tails.boum.org/
1 Imagen del sistema (ISO)
http://dl.amnesia.boum.org/tails/stable/tails-i386-1.0.1/tails-i386-1.0....
2 Firma Criptográfica
https://tails.boum.org/torrents/files/tails-i386-1.0.1.iso.sig
La firma criptográfica nos sirve para comprobar que el archivo que hemos descargado no ha sufrido ninguna modificación por algún tercero.
¿Cómo comprobamos teniendo los 2 archivos la integridad de nuestra imagen ISO?. Abrimos la terminal. Nos vamos con el comando cd al directorio donde tenemos el archivo .ISO y el archivo .SIG y lanzamos:

```
gpg --keyid-format long --verify tails-i386-1.0.1.iso.sig tails-i386-1.0.1.iso
```

Resultado:

```
gpg: Firmado el dom 08 jun 2014 21:32:53 CEST
gpg:                usando RSA clave 1202821CBE2CD9C1
gpg: Firma correcta de "Tails developers (signing key) " [desconocido]
gpg:                 alias "T(A)ILS developers (signing key) " [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg:           No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 0D24 B36A A9A2 A651 7878  7645 1202 821C
BE2C D9C1@boum.org>@boum.org>
```

En otras distrubuciones o simplente en otras descargas se utiliza el checksum. Según la wiki:
Una suma de verificación, (también llamada suma de chequeo o checksum), en telecomunicación e informática, es una función hash que tiene como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión. La idea es que se transmita el dato junto con su valor hash, de esta forma el receptor puede calcular dicho valor y compararlo así con el valor hash recibido. Si hay una discrepancia se pueden rechazar los datos o pedir una retransmisión. Esto es empleado para comunicaciones (Internet, comunicación de dispositivos, etc.) y almacenamiento de datos (archivos comprimidos, discos portátiles, etc.).
Normalmente aumentar la capacidad de detectar más tipos de error aumenta la complejidad del algoritmo y el coste, pues aumenta las necesidades de proceso de éste. Sin embargo, proporciona medios de detectar errores en el código de forma fiable.
Igualmente para ver el cheksum de nuestra ISO, ejemplo md5sum, abrimos terminal:

```
md5sum tails-i386-1.0.1.iso
```

Resultado:

```
32eaddc8e335bd126e8d1bd16f4cdfb4  tails-i386-1.0.1.iso
```

Tags:
Linux-Distro
Linux
Linux seguridad
Tails

- Inicie sesión o regístrese para comentar
- 4641 lecturas