Cifra Tu Mundo

- Seguridad de comunicaciones móviles: SS7
- Tráfico de datos seguro con Tor y/o VPN
- Comunicaciones de voz y sms seguras con software libre. Signal y Linphone
- Cifrando archivos en la “nube”
- Asegurando tu red WiFi
- Hacktivismo nivel PRO

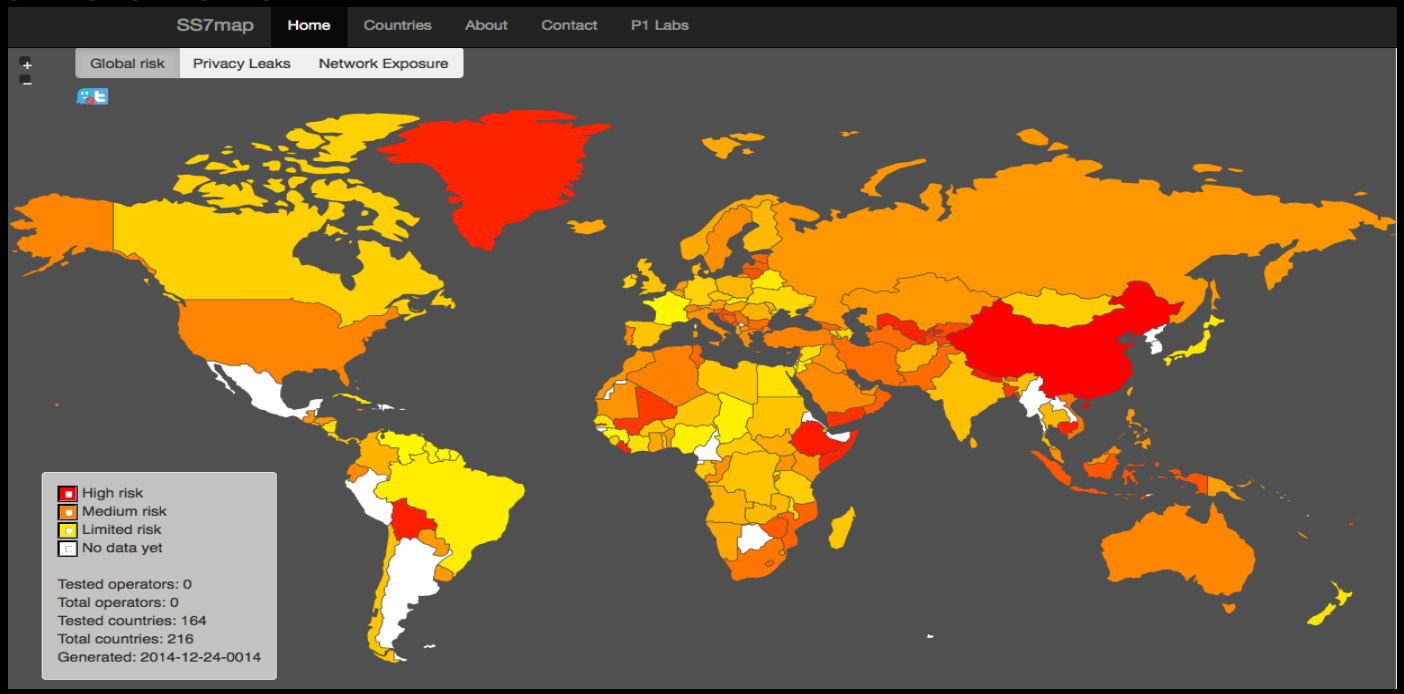
Signaling System nº7 (SS7)

- Protocolo de intercambio de información de señalización entre operadoras telefónicas
- Utilizado para encaminar mensajes, llamadas, reenviarlas, funciones de roaming
- Comando anyTimeInterrogation permite conocer el ID de la torre de telefonía que da servicio al objetivo. Bloqueado por la mayoría de las operadoras
- Usando una combinación de comando es posible obtener latitud y longitud en la que se encuentra el objetivo
- Existen servicios comerciales de operadoras y terceros para acceder a SS7 de manera sencilla

Signaling System nº7 (SS7)

Mapa de redes vulnerables realizado por P1 Sec: http://ss7map.p1sec.com/

De 2014, actualmente están realizando una nueva edición



Signaling System nº7 (SS7)

España, solo un operador bien configurado, 2 a medias, 1 mal

Permite localizar a usuarios a nivel de calle

SS7 Security of Spain

Country Mobile Network Worldwide Rank	51 / 164

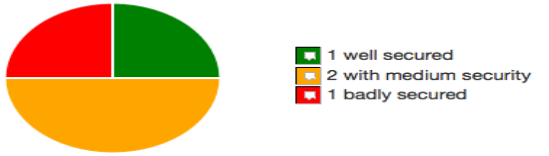
Scores for 4 operators surveyed

[+] Show all details [-] Hide all details

Global Risk level	51 / 164 1380.7
Privacy Risk level	41 / 164 759.4
SS7 messages disclosing subscriber city location	8
SS7 messages disclosing subscriber street location	4
SS7 messages disclosing private informations	7
Leak of subscriber keys	2
Leak of prepaid/postpaid status	1
Leak subscriber location through Home Routing bypass	?
Network Exposure level	149 / 164 1726
SCCP discovery attack surface	242
Network Elements fingerprint	242
Potential change of prepaid/postpaid status (fraud)	1

Tweet about Spain SS7 security:

Operators tested



4 surveyed operator / 4 operators

Signaling System nº7 (SS7)

Venezuela, un operador testeado y bien configurado, no permite localizar al objetivo ni a nivel de ciudad

SS7 Security of Venezuela, Bolivarian Republic of

Country Mobile Network Worldwide Rank	3 / 164

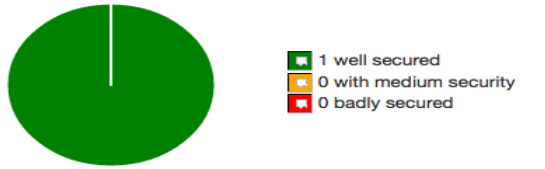
Scores for 1 operator surveyed

[+] Show all details [-] Hide all details

Global Risk level	3 / 164 569.4
Privacy Risk level	10 / 164 341.8
SS7 messages disclosing subscriber city location	0
SS7 messages disclosing subscriber street location	0
SS7 messages disclosing private informations	1
Leak of subscriber keys	0
Leak of prepaid/postpaid status	1
Leak subscriber location through Home Routing bypass	?
Network Exposure level	7 / 164 568.7
SCCP discovery attack surface	20
Network Elements fingerprint	20
Potential change of prepaid/postpaid status (fraud)	1

Tweet about Venezuela, Bolivarian Republic of SS7 security:

Operators tested



1 surveyed operator / 3 operators

Signaling System nº7 (SS7)

Bases de datos abiertas que contienen información geográfica de localización para unas 15 millones de antenas

SnoopSnitch para Android permite detectar ataques. Requiere root y chipset Qualcomm. Gratis en Play Store

Contribuye al proyecto http://gsmmap.org/

España mal parada en el informe de Junio 2016

Pocos usuarios, faltan datos

Signaling System nº7 (SS7)

Otras cosas que se pueden hacer teniendo acceso a SS7:

Reenviar llamadas de manera transparente para el objetivo

Grabar o escuchar llamadas

Leer mensajes SMS, “escuchar” el tráfico de datos

Lo mismo que SITEL, pero sin necesidad de SITEL

¿Podemos evitarlo? Sí, al menos en parte

Tráficos de datos seguro: Tor/VPN

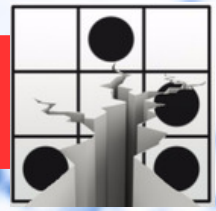
Tor y VPN, dos conceptos diferentes

Tor enruta de manera aleatoria el tráfico de datos a través de varios nodos antes de llegar a su destino vía el nodo de salida o al servidor alojado dentro de la red Tor

Tor nació como un servicio para militares de EE.UU, para proteger la privacidad de sus usuarios, pero no es un bálsamo de fierabrás

Existen multitud de nodos piratas que pueden escuchar el tráfico no cifrado

Tráficos de datos seguro: Tor/VPN



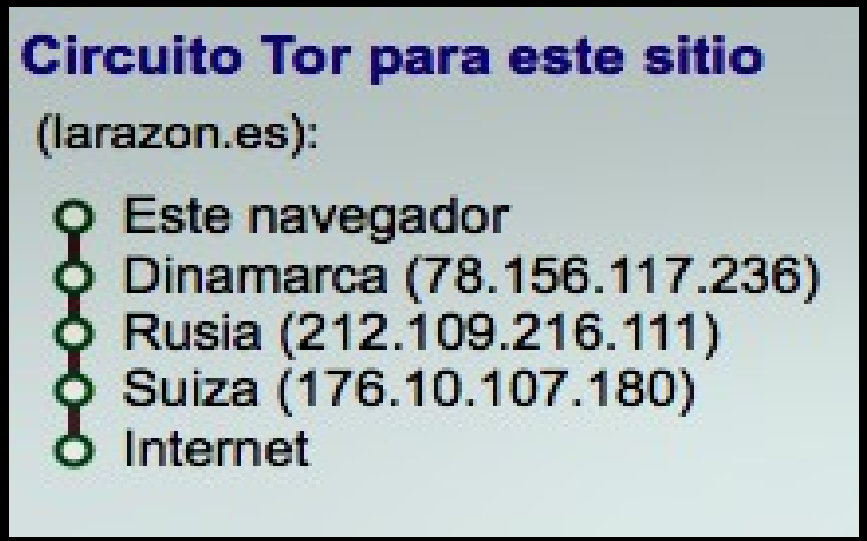
En Tor el tráfico sale cifrado del dispositivo

Algunos cortafuegos son capaces de bloquearlo, es necesario recurrir a obfsproxy para ofuscar el tráfico en algo que el cortafuegos acepte como válido

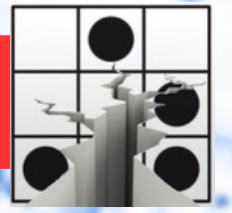
https://bridges.torproject.org/bridges?transport=obfs3

Tráficos de datos seguro: Tor/VPN

Ruta usada por Tor para acceder a un sitio web peligroso que no queremos que nos pueda trazar



Tráficos de datos seguro: Tor/VPN



Una VPN es un servicio que conecta de manera segura nuestro dispositivo con un servidor que es el que aparecerá en los logs del servicio de destino

El tráfico viaja cifrado hasta el servidor que funciona como punto de salida

Hay servicios de pago confiables

Con los conocimientos suficientes es posible montar uno propio

Tráficos de datos seguro: Tor/VPN

Servicios de alquiler de servidores virtuales con pago anónimo (paysafecard o Bitcoin):

https://en.myvirtualserver.com/

https://www.creeperhost.net/

https://coinshost.com/en/

Servicios de VPN con pago anónimo:

https://www.privateinternetaccess.com/

https://nordvpn.com

Tráficos de datos seguro: Tor/VPN

Usar Tor en el ordenador, tan fácil como:

A) Descargar el navegador Tor https://www.torproject.org/

B) Descargar el S.O. Tails https://tails.boum.org/

C) Descargar Whonix https://www.whonix.org

El navegador Tor solo ofrece privacidad navegando por la web

Tails hace que todo el tráfico del ordenador vaya por esta red, no solo las páginas web

Whonix se compone de dos máquinas para virtualizar, una de gateway y otra de Workstation

Tráficos de datos seguro: Tor/VPN

En Android, instalad la app Orbot

Para un funcionamiento óptimo requiere de permisos de root

Las últimas versiones permiten modo VPN a partir de Android 4.1. Es un modo experimental que no recomiendan usar si se pretende privacidad

Sin root funciona como un proxy, es necesario indicar a las app que se conecten al puerto 8118 del propio dispositivo

Algunas como Twitter permiten usar este modo proxy, pero tampoco hay que tener muchas expectativas de privacidad usando la app oficial.

Tráficos de datos seguro: Tor/VPN

Orbot en modo VPN

Tráficos de datos seguro: Tor/VPN

Orbot en modo VPN

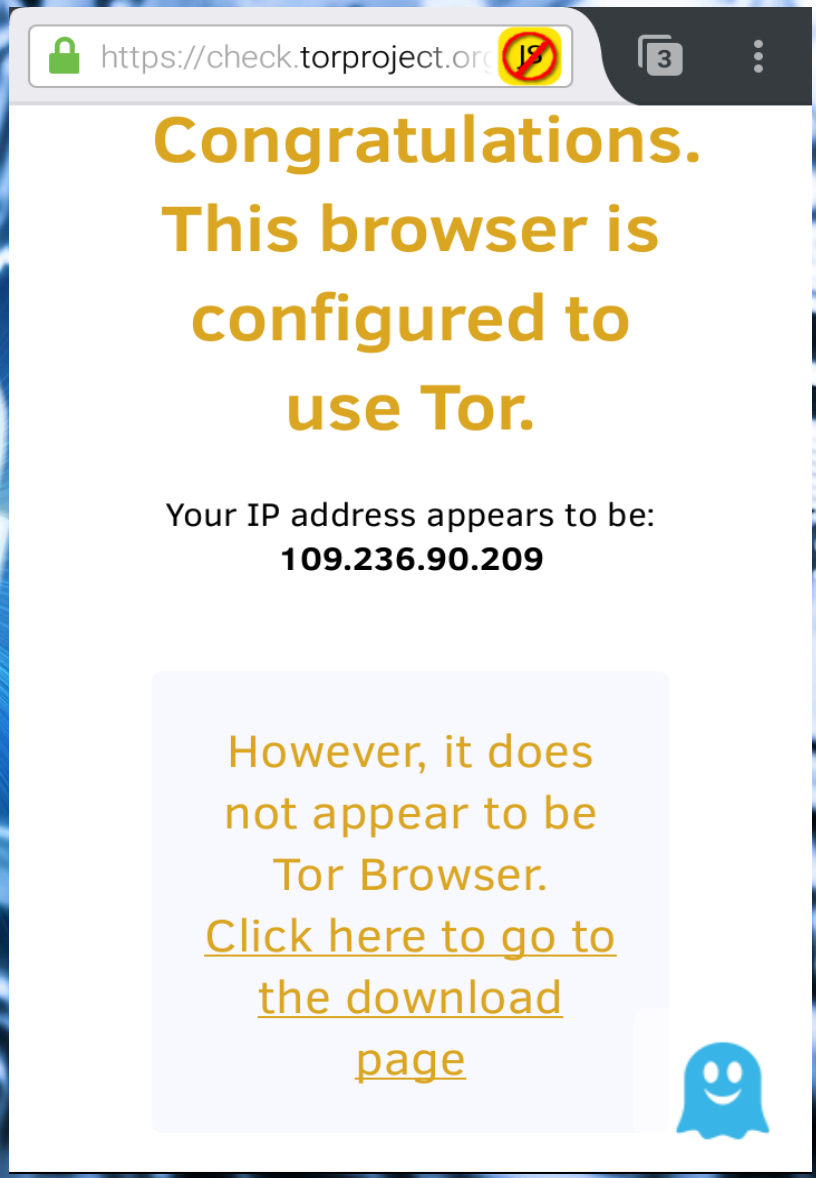
Tráficos de datos seguro: Tor/VPN

Navegando con Firefox for Android con Orbot en modo VPN

- Todo el tráfico iría por Tor sin necesidad de root
- Es algo experimental, sin garantías de privacidad

Existe Orfox para Android, su propia versión del navegador preparada para Tor

- Lleva demasiados meses sin actualizarse



Tráficos de datos seguro: Tor/VPN

VPN

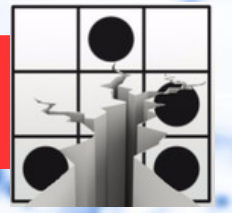
Una de las más populares es OpenVPN

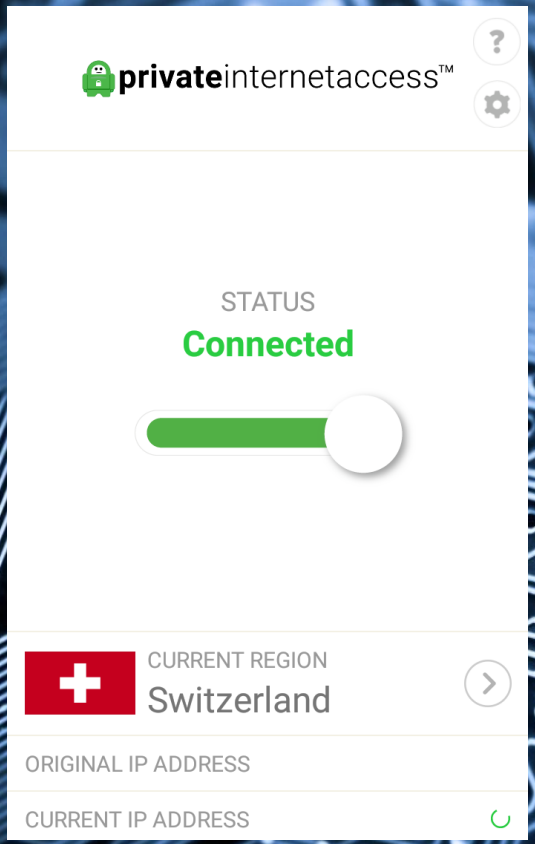
Permite utilizar puertos de http/https usando protocolo TCP para acceder al servidor de VPN

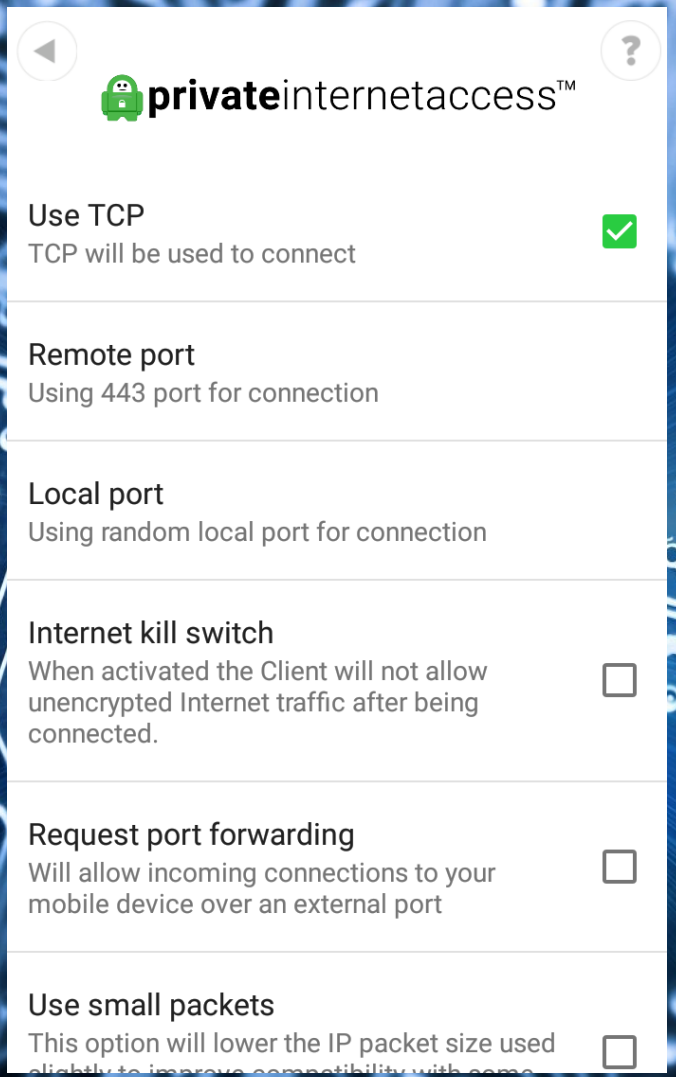
Esto permite saltarse muchos cortafuegos y los límites y bloqueos de red, como en la WiFi de la EMT

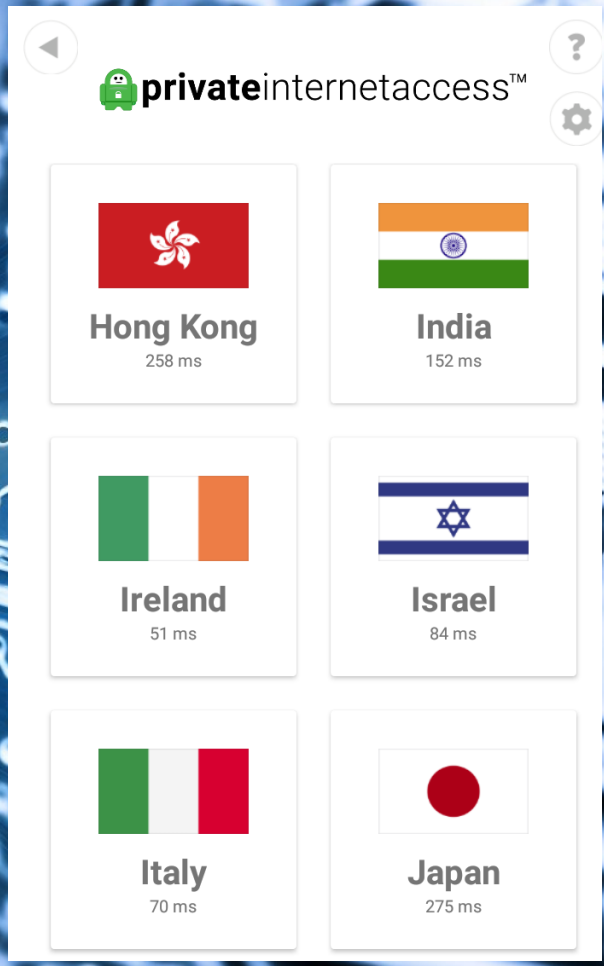
Los servicios de pago suelen disponer de su propia app para ordenadores, smartphones y tablets

Tráficos de datos seguro: Tor/VPN









Mensajería y VoIP: Signal/LinPhone

Signal es una app disponible en Android, iPhone y como plugin para navegadores Chrome

En Android substituye a la app original de SMS

Gestiona los SMS tradicionales y nos permite envío de mensajes de texto, imágenes y vídeo de manera segura con cifrado de punta a punta. Consume datos, no SMS/MMS con los destinatarios que sean también usuarios de la app.

Su sistema ha sido adoptado por WhatsApp y la nueva app de mensajería Google Allo (este último no lo activa por defecto)

Permite chats en grupo

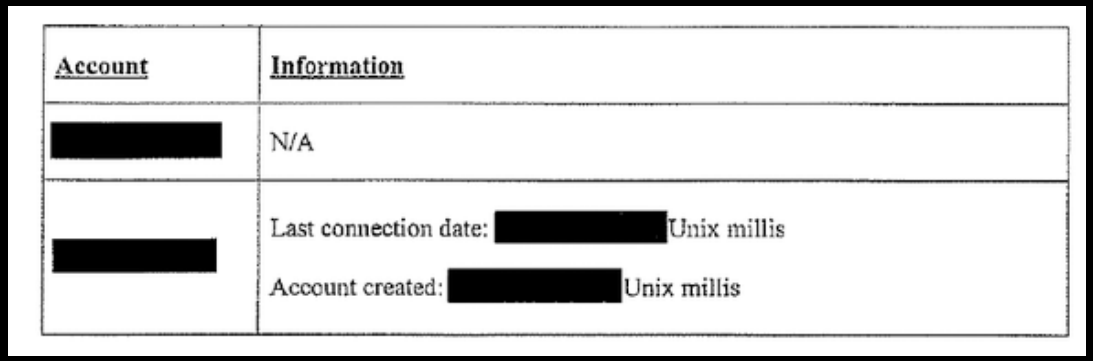
Es software libre https://github.com/WhisperSystems/Signal-Android

Permite realizar llamadas VoIP seguras a través de servidores en EE.UU. Mucha latencia, llamadas de mala calidad

Mensajería y VoIP: Signal/LinPhone

Sabemos exactamente que información guardan los servidores de Signal gracias a una citación del FIB, nada.

https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/



Account	Information
[redacted]	N/A
[redacted]	Last connection date: [redacted] Unix millis Account created: [redacted] Unix millis

Mensajería y VoIP: Signal/LinPhone

Linphone es otra aplicación de software libre disponible para Linux, OS X, Windows, Android, iPhone y Windows Phone

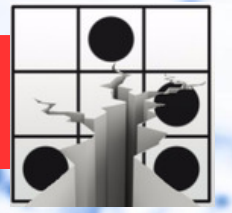
https://www.linphone.org/

Su principal función son las comunicaciones VoIP, aunque también dispone de un sistema de chat

Puedes montarte tu propio servidor VoIP

Usa ZRTP para comunicaciones seguras, como Signal

Mensajería y VoIP: Signal/LinPhone



ZRTP es una extensión de RTP (Protocolo de transporte en tiempo real)

Emplea el mecanismo Diffie-Hellman para realizar un intercambio seguro de claves que permitan establecer una clave de cifrado efímera para cada comunicación que establezcamos

Perfect Forward Secrecy, si un atacante intercepta las comunicaciones no tendrá ninguna clave con la que descifrarlas al ser claves efímeras

Mensajería y VoIP: Signal/LinPhone

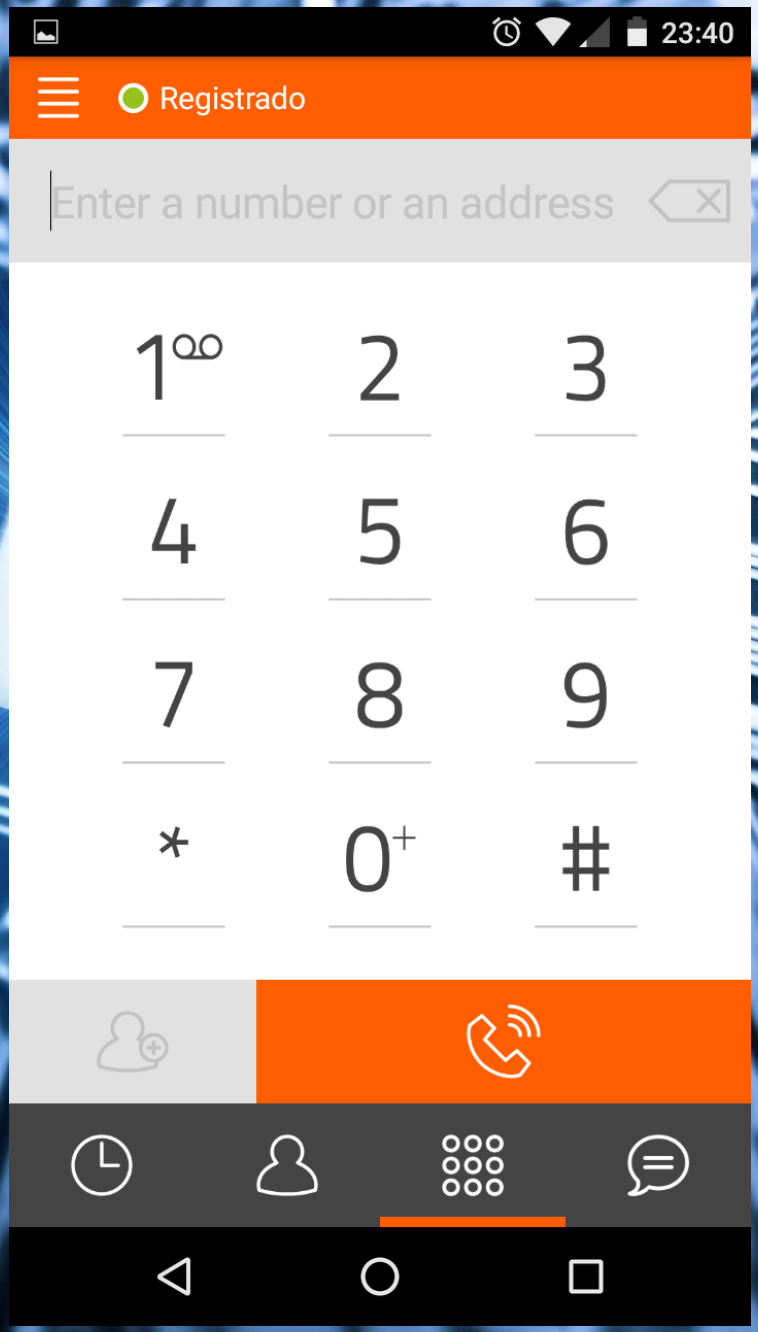
Aunque Linphone usa los mismos métodos que Signal para cifrar las comunicaciones, el que tengan sus servidores en Francia lo hace más interesante para el usuario medio, las llamadas son de mayor calidad gracias a una latencia de red menor

Registro gratuito en https://www.linphone.org/free-sip-service.html

Linphone permite elegir el método de transporte, usando TLS podemos utilizarlo sobre la red Tor

Direcciones sencillas: jorgesdb@sip.linphone.org

Mensajería y VoIP: Signal/LinPhone



Cifrado de archivos en la “nube”

La nube no existe, es el ordenador/servidor de otra persona donde almacenamos nuestros datos

Google Drive, Dropbox, OneDrive, Box, los datos que almacenemos ahí están a la vista de cualquiera

Idrive o SpiderOak ofrecen lo mismo pero permitiéndonos establecer una clave de cifrado. Los archivos salen del dispositivo ya cifrados. Zero Knowledge

Lo óptimo sería mantener nuestra soberanía sobre los datos, disponer de un servidor propio con software libre como OwnCloud, que permite el cifrado de los archivos almacenados. El cifrado se realiza en el propio servidor

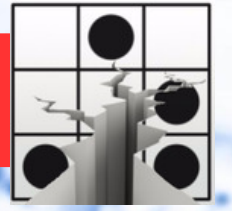
Cifrado de archivos en la “nube”

Para cifrar nuestros datos en la “nube”, existen aplicaciones cerradas y de pago como Boxcryptor y alternativas libres como Cryptomator

También existe EncFS no es 100% segura, como todo en esta vida, y existen un par de ataques teóricos bajo circunstancias muy concretas como que el atacante disponga de acceso con lectura y escritura al dispositivo desde el que se usa EncFS

Si el atacante tiene ese tipo de acceso, este sería el menor de nuestros problemas

Cifrado de archivos en la “nube”



Cryptomator está disponible para Windows, Mac, Linux y Android, gratuito en

https://cryptomator.org/

Cifrado de archivos en la “nube”

Para Debian podemos descargar el paquete desde su web, para Ubuntu, Mint, etc

sudo add-apt-repository ppa:sebastian-stenzel/cryptomator

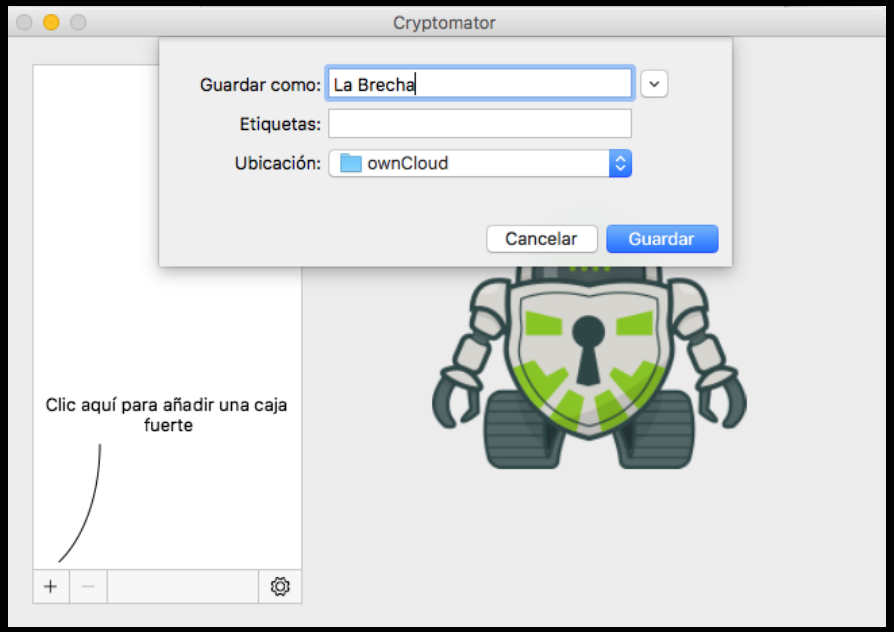
sudo apt-get update

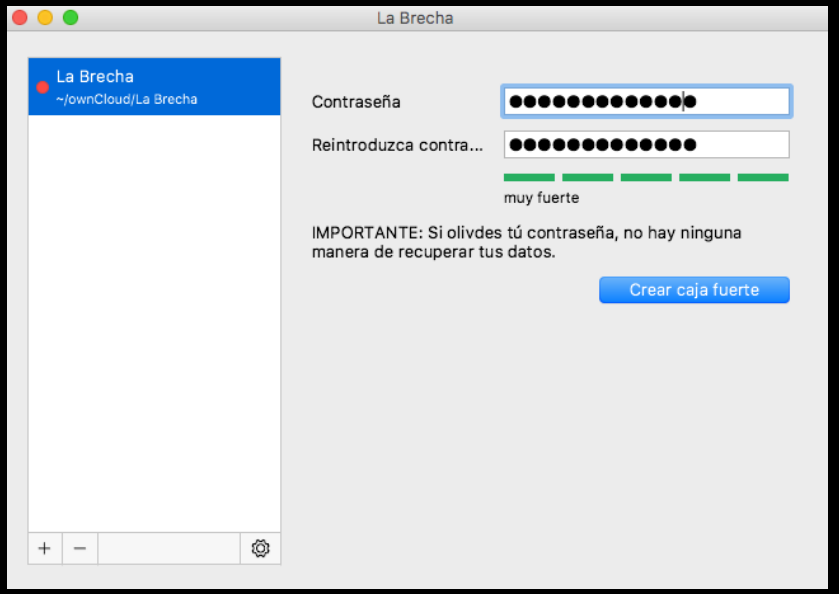
sudo apt-get install cryptomator

También hay paquetes para Fedora, CentOS o Archlinux

Cifrado de archivos en la “nube”

Tan solo hay que elegir la carpeta donde queremos almacenar el contenido cifrado, darle un nombre al contenedor y establecer una clave



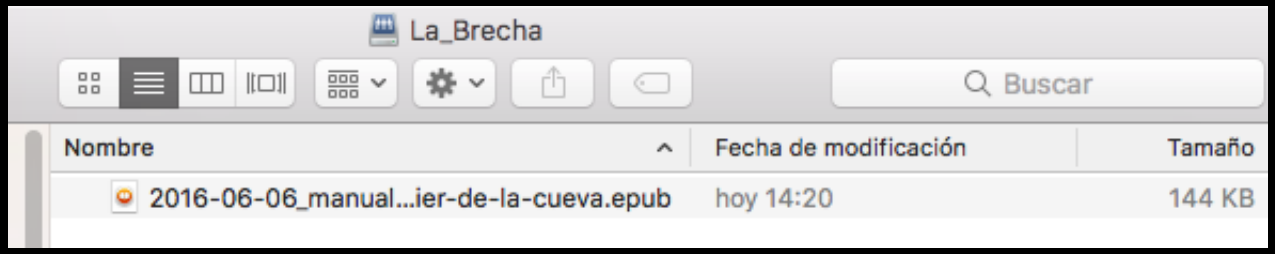


Cifrado de archivos en la “nube”

Para que esto vaya a la nube, la carpeta que hemos seleccionado debe estar dentro de la estructura que generan los clientes de Dropbox, Box, Owncloud, etc, de lo contrario estaremos almacenando solo en local los archivos cifrados

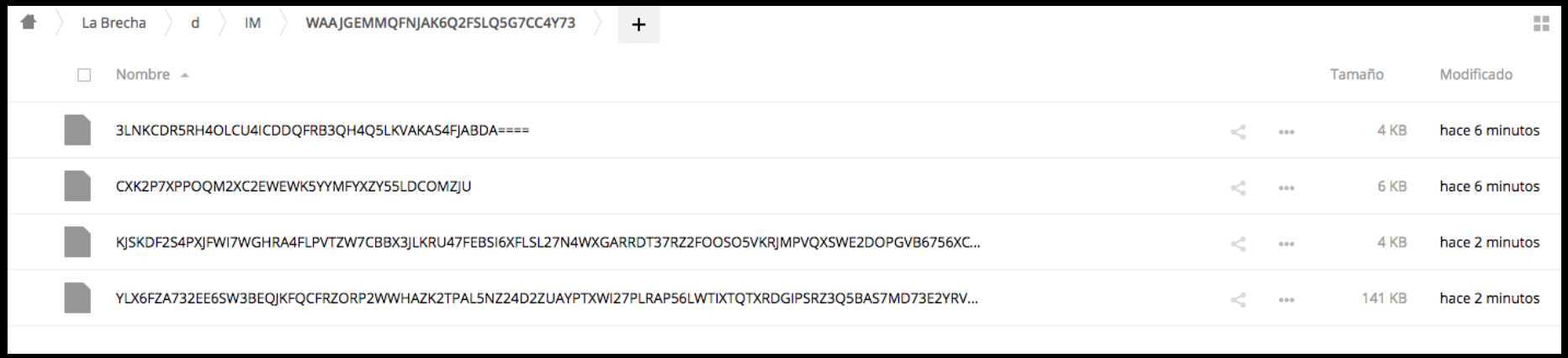
Cifrado de archivos en la “nube”

Copiamos la edición epub del Manual del Ciberactivista de @jdelacueva dentro del contenedor Cryptomator creado, que para la ocasión se encuentra dentro de un Owncloud

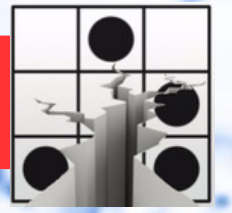


Cifrado de archivos en la “nube”

Si miramos en la carpeta de Owncloud esto sería lo que veríamos, pura basura para cualquiera que no conozca nuestra clave



Cifrado de archivos en la “nube”

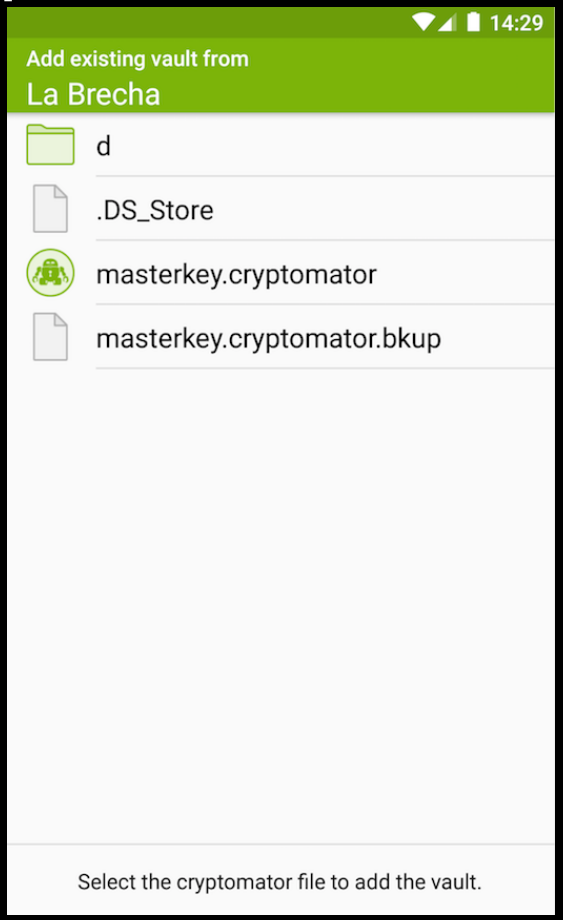


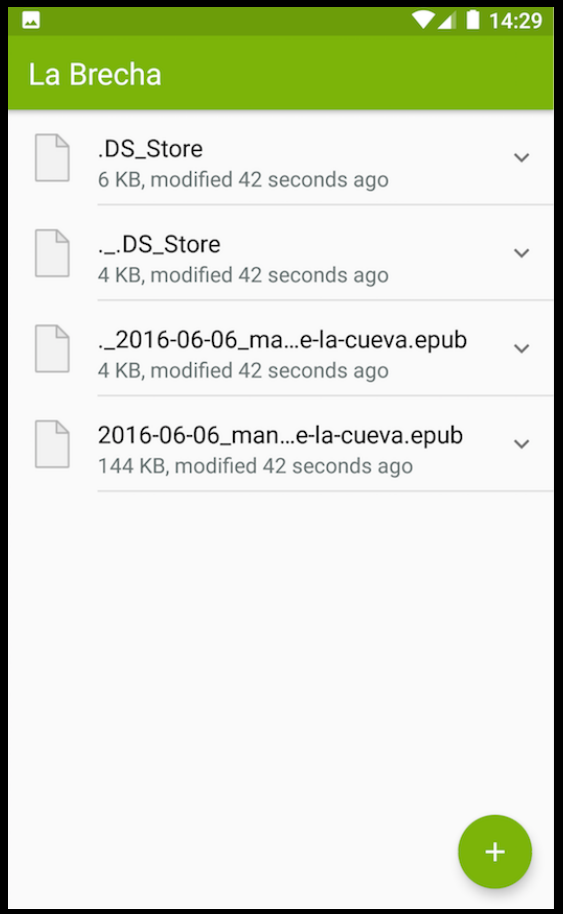
Y el contenido almacenado en la “nube” no es mucho mejor

YLX6FZA732EE6SW3BEQJKFQCFRZORP2WWHAZK2TPAL5NZ24D2ZUAYPTXWI27PLRAP56LWTIXTQTXRDGIPSRZ3Q5BAS7MD73E2YRV2ZKIBBHSMURYZP...

Cifrado de archivos en la “nube”

Podremos tener acceso desde nuestro dispositivo Android con su app (en Beta)





Asegurando tu red WiFi

Los routers ADSL/Fibra que nos “regalan” las operadoras suelen ser despojos tecnológicos muy baratos y muy mal configurados

El primer paso cuando se recibe uno nuevo es cambiar la clave de acceso al mismo y la clave de la red WiFi

Asegurando tu red WiFi

Aplicaciones libres como Router Keygen nos permiten verificar si nuestro router pertenece al selecto grupo que viene con una clave WiFi predecible

https://routerkeygen.github.io/

Asegurando tu red WiFi

Otro fallo común es que los routers vienen con el WPS (WiFi Protected Setup) activo de fábrica y sin ninguna medida de protección ante ataques de fuerza bruta.

El PIN WPS se compone de 7 dígitos + 1 dígito de control

Herramientas libres como Reaver pueden recuperar tu clave WPA/WPA2 en minutos, sin importar lo fuerte que esta sea

https://github.com/t6x/reaver-wps-fork-t6x

Asegurando tu red WiFi

Aunque 7 dígitos suponen 10 millones de claves diferentes, un fallo de diseño de WPS permite “adivinar” los primeros 4 dígitos y luego los 3 siguientes. El 8º dígito al ser de control se calcula en base a los otros 7

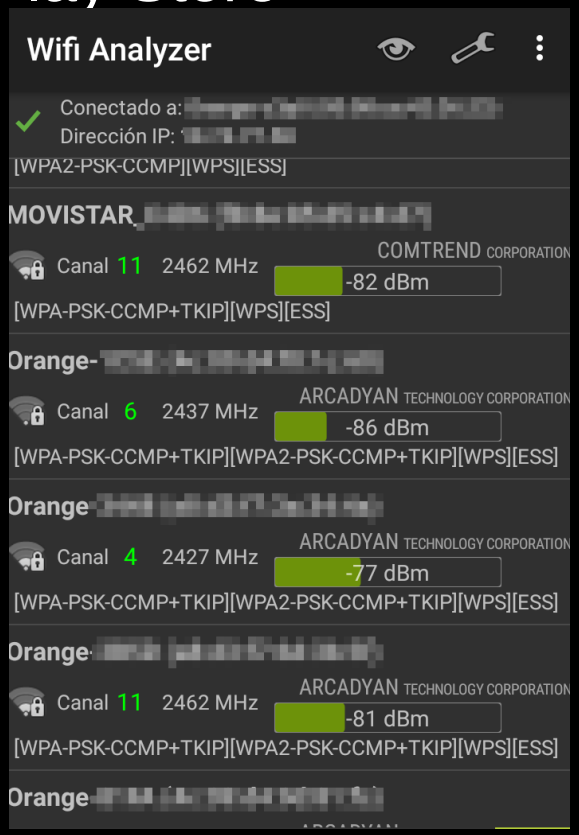
Esto supone tener que probar solo 11.000 claves que puede llevar unas pocas horas de prueba/error, sin contar que muchos traen por defecto el PIN 12345670, uno de los primeros que prueba Reaver.

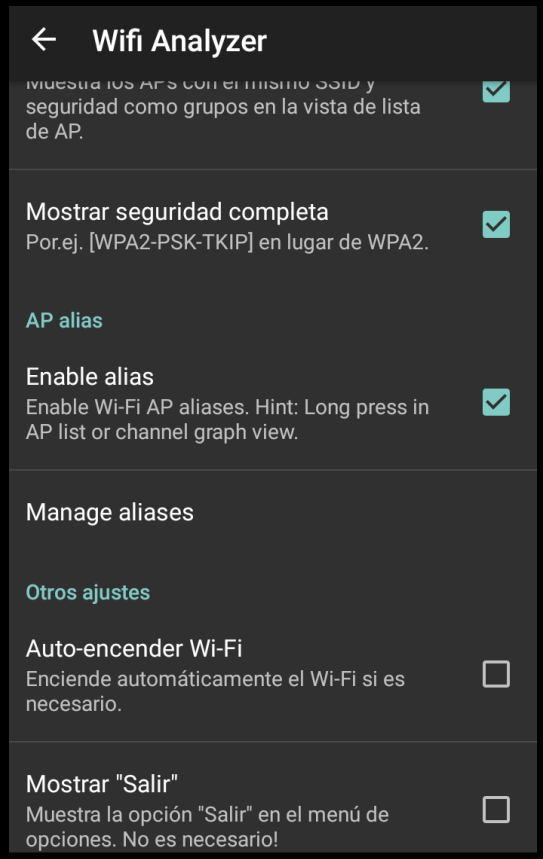
Si además el router está entre los afectados por el Pixie Dust Attack, el ataque se reduce a unos pocos minutos

Asegurando tu red WiFi

En ocasiones el router no dispone de una opción para desactivar WPS o bien no funciona

La mejor comprobación es usar la app WiFi Analyzer, gratuita en la Play Store





Hacktivismo nivel PRO

Las filtraciones de la NSA por parte de Snowden y las más actuales de la CIA nos han enseñado que no podemos confiar en nuestros dispositivos.

En lugar de atacar el software que cifra comunicaciones como Signal, atacan el propio sistema operativo, volviendo fútil cualquier cosa que hagamos por encima para proteger nuestra privacidad.

Y estas ciberarmas están ahora fuera de su control, no sabemos quien las tiene y para que, sin olvidar que existen otros servicios de inteligencia de los que se habla poco y tendrán una potencia de fuego similar.

Existen medidas poco costosas para ponerles las cosas un poco más difíciles.

Hacktivismo nivel PRO

Mini router GL AR150 https://www.gl-inet.com/ar150/

Puede usarse conectado a una red cableada o hacer de repetidor WiFi, firmware basado en OpenWRT

Incluye de serie OpenVPN para que todo el tráfico que pase por él salga a través de una VPN

Puede funcionar con una batería externa

Dispone de firmware con soporte

para redes Tor

http://www.gl-inet.com/firmware/ar150/tor/

Hacktivismo nivel PRO

Personal de ONG, periodistas en zonas de conflicto no deberían usar un dispositivo móvil para todas sus comunicaciones.

Un móvil para navegar, recibir emails sin interés, redes sociales, etc.

Otro móvil exclusivamente para comunicaciones que puedan comprometer su seguridad personal.

Este con un sistema android diferente, CopperHead OS y NOISE de cliente Signal para no depender de Google Play Store

https://copperhead.co/android/

Hacktivismo nivel PRO

Qubes OS, un sistema operativo realmente seguro y libre

https://www.qubes-os.org/

Diseñado pensando en la seguridad mediante aislamiento

Hardware, red, entorno gráfico y aplicaciones de usuario están aislados por ámbitos

Utiliza Xen para virtualizar estos ámbitos con diferentes niveles de confianza, por ejemplo uno para Trabajo, otro para Compras

No es Virtualbox ejecutándose sobre un sistema operativo, elimina esa necesidad y evita ser víctima de vulnerabilidades del sistema operativo bajo Virtualbox

Permite ejecutar encima sistemas operativos como Fedora, Debian, Whonix o Windows 7

Hacktivismo nivel PRO

Ordenador portátil Librem 13

Diseñado pensando en la seguridad y privacidad del usuario

No necesita tapar la webcam o el micrófono, tiene botones para desconectarlos por hardware, no software

Se puede comprar con Qube OS preinstalado

No es barato y no dispone de teclado en español

https://puri.sm/products/librem-13/

Hacktivismo nivel PRO

También existe una lista de otros portátiles compatibles con Qube OS:

https://www.qubes-os.org/hcl/

Importante que soporten:

Intel VT-x / AMD-v, soporte para virtualización

Intel VT-d / AMD-vi (IOMMU), para un aislamiento efectivo de la red

TPM 2.0 para evitar ataques Evil Maid

Disco SSD para que el funcionamiento sea fluido

Hacktivismo nivel PRO

Servicio de email confiable:

https://protonmail.com/ Se rigen por las leyes de privacidad de Suiza. 500MB gratis. Aceptan Bitcoin

https://www.startmail.com/ Situado en Holanda. No aceptan Bitcoin, 10GB por 49€ al año

https://www.tutanota.com/es/ En Alemania, 1GB gratis

https://mailbox.org/en/ En Alemania, 2GB por 12€ al año. Aceptan Bitcoin

Todos incluyen mecanismos internos de cifrado

Hacktivismo nivel PRO

Alternativas al email:

Están todas en fase beta, sistemas descentralizados:

https://bitmessage.org Usa protocolo P2P, no filtra metadatos

http://retroshare.net/ Chat, mensajes, compartir archivos, llamadas VoIP usando protocolos P2P

Hacktivismo nivel PRO

Buscadores:

StartPage https://www.ixquick.eu/ y https://www.startpage.com/

Alojado en servidores propios

Legislación europea de protección de datos

Privacidad auditada por terceros, EuroPrise

https://www.european-privacy-seal.eu/EPS-en/First-European-Privacy-Seal-Awarded

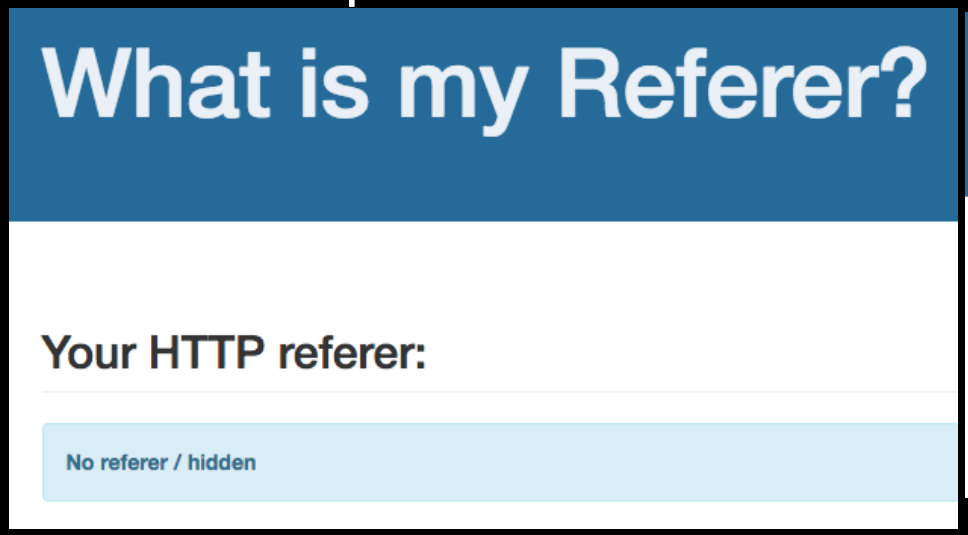
Hacktivismo nivel PRO

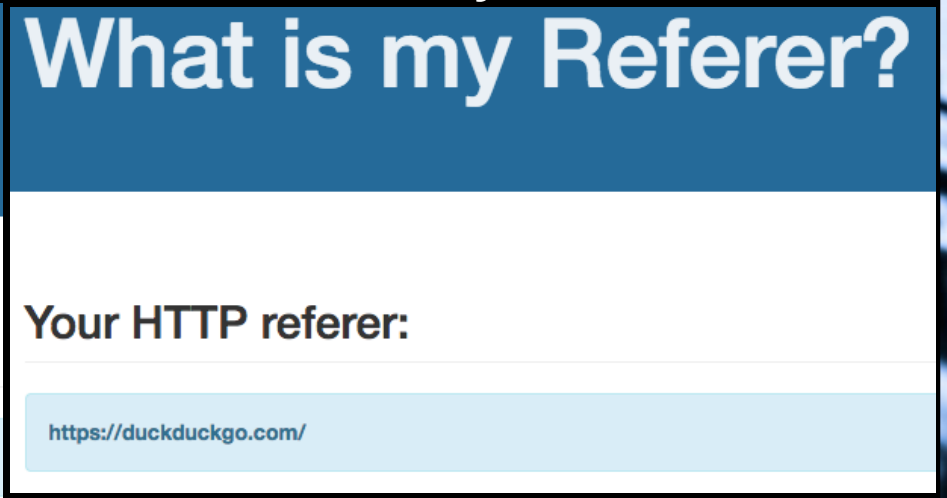
DuckDuckGo o Disconnect son empresas americanas alojadas en la nube de Amazon, en el caso de DuckDuckGo con fondos de capital riesgo como inversores.

Startpage solo cuenta con la inversión del dueño del servicio.

Startpage dispone de un proxy para anonimizar más las visitas, tan siquiera deja rastro en el referer.

Yendo al primer resultado de buscar “What is my referer”:





Hacktivismo nivel PRO

Seguridad en el Navegador Web

Usar un navegador libre como Firefox

Desactivar algunas funcionalidades como WebRTC, en about:config modificar las siguientes opciones:

media.peerconnection.turn.disable = true

media.peerconnection.use_document_iceservers = false

media.peerconnection.video.enabled = false

media.peerconnection.identity.timeout = 1

Hacktivismo nivel PRO

Otras opciones a modificar:

privacy.trackingprotection.enabled = true

browser.safebrowsing.phishing.enabled = false (peligrosa)

browser.safebrowsing.malware.enabled = false (peligrosa)

network.cookie.cookieBehavior = 1

network.cookie.lifetimePolicy = 2

browser.send_pings = false

webgl.disabled = true

dom.battery.enabled = false

browser.sessionstore.max_tabs_undo = 0

geo.enabled = false

Hacktivismo nivel PRO

Plugins para bloquear publicidad y trackers:

- Ublock Origin
- Self-Destructing Cookies
- HTTPS Everywhere
- Privacy Badger
- No Script Security Suite
- Canvas Defender
- Random Agent Spoofer

Hacktivismo nivel PRO

Donde comprobar que todo funciona y que información estamos filtando:

https://ipleak.net/

https://browserleaks.com/webrtc

https://browserleaks.com/canvas

https://browserleaks.com/webgl

Hacktivismo nivel PRO

Ocultar el tráfico de Tor/VPN

Tor y los diferentes tipos de VPN dejan una huella fácilmente reconocible para un adversario con capacidad DPI

OBFSPROXY es parte del proyecto Tor para enmascarar el tráfico y circunvalar estas medidas

https://www.torproject.org/docs/pluggable-transports.html.en

Proveedores de VPN lo ofrecen como servicio:

https://nordvpn.com/es/tutorials/obfsproxy/windows/

https://proxy.sh/panel/knowledgebase/1166/Combine-OpenVPN-with-obfsproxy-for-stealth-mode-Linux.html

Hacktivismo nivel PRO

Seguridad extra en la WiFi

Nuestros dispositivos WiFi cuando están activos y no conectados a un AP tienen la costumbre de ir gritando la lista de puntos WiFi a los que se conectó en el pasado mediante Probe Request.

Además los dispositivos son idiotas, cualquier AP que les responda diciendo que es uno de la lista filtrada previamente se convertirá en su punto de acceso WiFi inmediatamente.

Sin contar que con webs como Wigle podríamos sacar información interesante del objetivo.

Hacktivismo nivel PRO

En Linux es fácil evitarlo editando el archivo de configuración de wpa_supplicant y añadiendo:

passive_scan=1

Hay otro parámetro, scan_ssid que desde hace tiempo viene desactivado por defecto

En Android también es sencillo usando la app Wi-Fi Privacy Police

https://play.google.com/store/apps/details?id=be.uhasselt.privacypolice

Hacktivismo nivel PRO

Si salimos de casa y nos olvidamos de apagar la WiFi del móvil, esta app bloqueará los probe requests.

Además si encendemos la WiFi y el dispositivo se encuentra con una red inalámbrica que se llama como una que el dispositivo ya conoce, pero no coincide el BSSID del router WiFi, la app emitirá una alerta y no nos permitirá conectar automáticamente a esa red hasta que validemos que realmente es de confianza

Iphone >=9 ya no envía probe request, Android >=5 en teoría tampoco

Y llevad apagado Bluetooth salvo que sea estrictamente necesario su uso.

Hacktivismo nivel PRO

Limpiando unidades USB ajenas

Tanto si nos encontramos una unidad USB abandonada y queremos ver su contenido para devolvérsela al propietario, como si nos pasa una USB un colega, es mala idea conectarla directamente a nuestro ordenador, podría incluir archivos infectados o bien ser la unidad una BadUSB con el firmware modificado con alguna oscura inteción.

Sin contar que en el mercado hay dispositivos como los Rubber Ducky o las KillUSB para funcionar como una BadUSB o freirnos la placa base de nuestro equipo al conectarla.

https://www.usbkill.com/

https://hakshop.com/products/usb-rubber-ducky-deluxe

Hacktivismo nivel PRO

Hay dispositivos como el USG autodenominados USB firewall para evitar BadUSB

https://github.com/robertfisk/USG/wiki

Para empresas con más presupuesto hay dispositivos que sanean CD/DVD y unidades USB con soluciones específicas como el ABB File Sanitizer

http://www.abb.com/search.aspx?abbcontext=products&q=file%20sanitizer

Y soluciones libres sobre hardware de bajo coste como RaspBerry PI

Hacktivismo nivel PRO

CIRCLean, desarrollado por el Centro de Incidentes Informáticos de Luxemburgo tan solo requiere una Raspberry PI 2 / 3, una tarjeta SD de 8 GB y la imagen basada en Raspbian que se puede descargar desde aquí:

https://www.circl.lu/projects/CIRCLean/

Necesitaremos también una unidad USB limpia y de mayor capacidad que la de origen.

No es necesario tener la RaspBerry conectada a un monitor, con unos altavoces llega para saber si ha terminado su labor.

Hacktivismo nivel PRO

Conectamos la USB ajena en el conector superior izquierdo y nuestra USB en otro de los conectores disponibles y la encendemos.

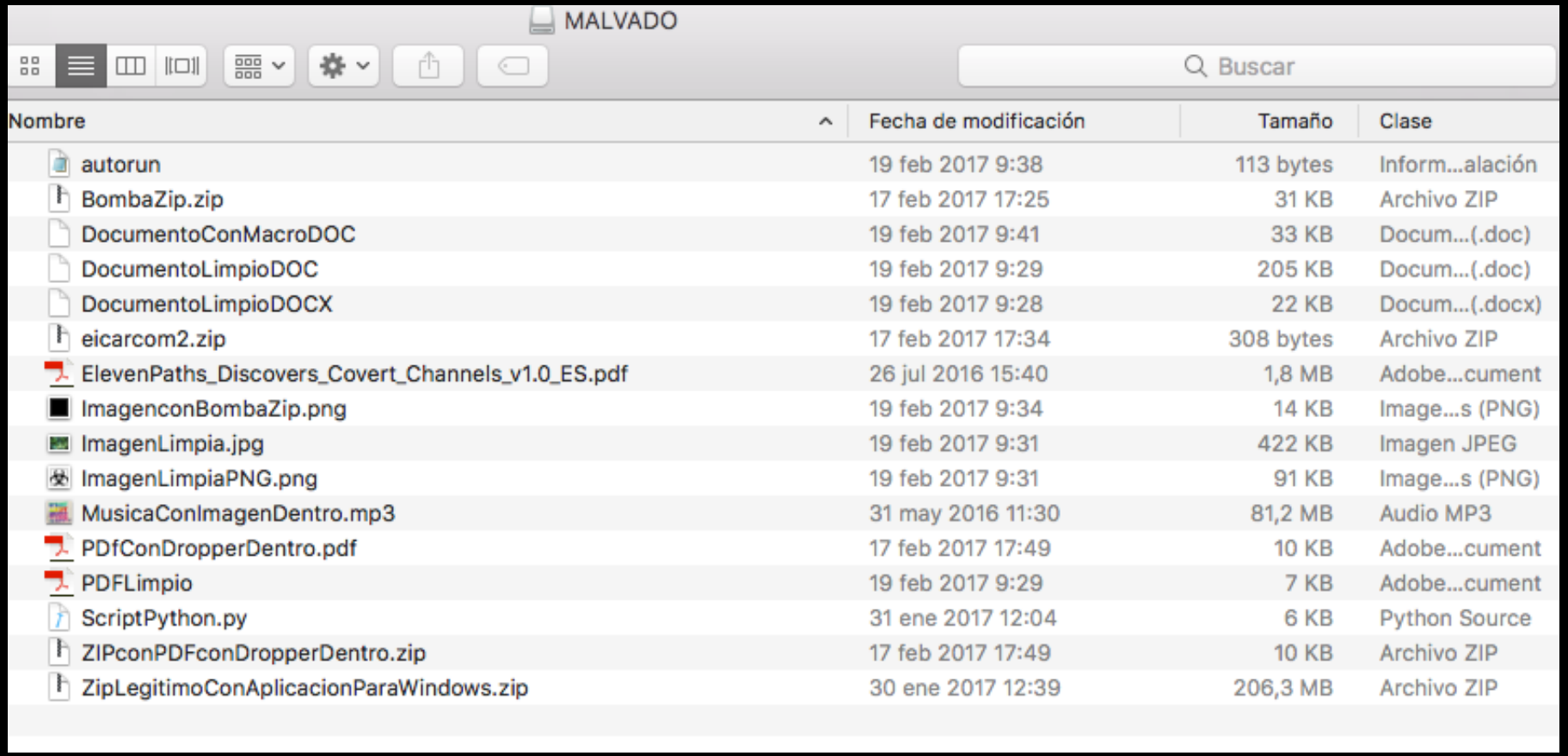
Por los altavoces escucharemos música mientras esté funcionando el proceso.

Cuando termine la música podemos apagarla, extraer las unidades USB y conectar la propia en nuestro equipo.

Soporta formatos ext3, ext4, FAT y NTFS. No soporta exFAT por el momento

Hacktivismo nivel PRO

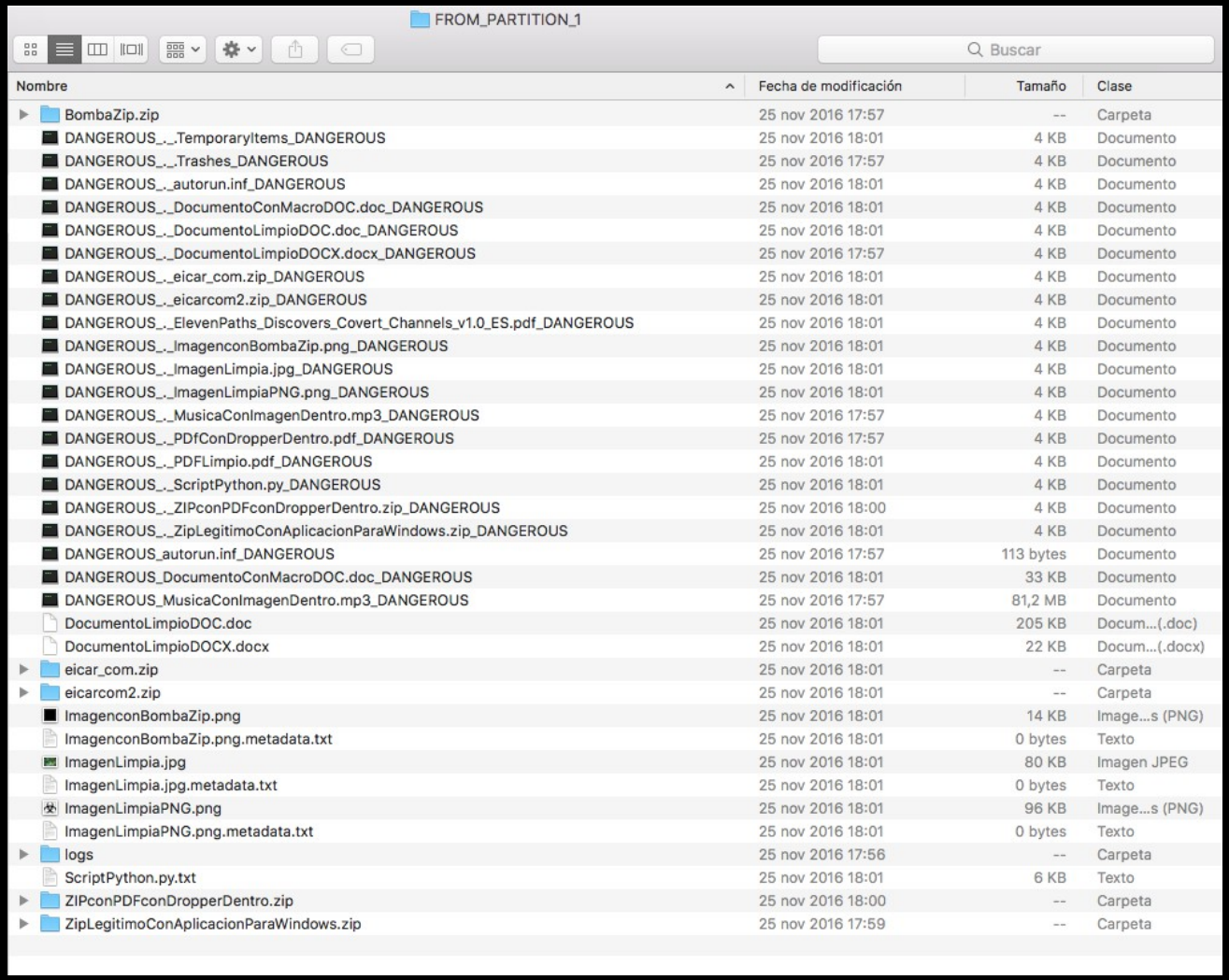
Contenido de la unidad USB original



Nombre	Fecha de modificación	Tamaño	Clase
autorun	19 feb 2017 9:38	113 bytes	Inform...alación
BombaZip.zip	17 feb 2017 17:25	31 KB	Archivo ZIP
DocumentoConMacroDOC	19 feb 2017 9:41	33 KB	Docum...(.doc)
DocumentoLimpioDOC	19 feb 2017 9:29	205 KB	Docum...(.doc)
DocumentoLimpioDOCX	19 feb 2017 9:28	22 KB	Docum...(.docx)
eicarcom2.zip	17 feb 2017 17:34	308 bytes	Archivo ZIP
ElevenPaths_Discovers_Covert_Channels_v1.0_ES.pdf	26 jul 2016 15:40	1,8 MB	Adobe...cument
ImagenconBombaZip.png	19 feb 2017 9:34	14 KB	Image...s (PNG)
ImagenLimpia.jpg	19 feb 2017 9:31	422 KB	Imagen JPEG
ImagenLimpiaPNG.png	19 feb 2017 9:31	91 KB	Image...s (PNG)
MusicaConImagenDentro.mp3	31 may 2016 11:30	81,2 MB	Audio MP3
PDfConDropperDentro.pdf	17 feb 2017 17:49	10 KB	Adobe...cument
PDFLimpio	19 feb 2017 9:29	7 KB	Adobe...cument
ScriptPython.py	31 ene 2017 12:04	6 KB	Python Source
ZIPconPDFconDropperDentro.zip	17 feb 2017 17:49	10 KB	Archivo ZIP
ZipLegitimoConAplicacionParaWindows.zip	30 ene 2017 12:39	206,3 MB	Archivo ZIP

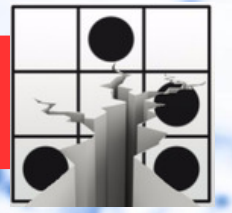
Hacktivismo nivel PRO

Contenido de nuestra USB



Nombre	Fecha de modificación	Tamaño	Clase
BombaZip.zip	25 nov 2016 17:57	--	Carpeta
DANGEROUS_._.TemporaryItems_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._.Trashes_DANGEROUS	25 nov 2016 17:57	4 KB	Documento
DANGEROUS_._autorun.inf_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._DocumentoConMacroDOC.doc_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._DocumentoLimpioDOC.doc_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._DocumentoLimpioDOCX.docx_DANGEROUS	25 nov 2016 17:57	4 KB	Documento
DANGEROUS_._eicar_com.zip_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._eicarcom2.zip_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._ElevenPaths_Discovers_Covert_Channels_v1.0_ES.pdf_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._ImagenconBombaZip.png_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._ImagenLimpia.jpg_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._ImagenLimpiaPNG.png_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._MusicaConImagenDentro.mp3_DANGEROUS	25 nov 2016 17:57	4 KB	Documento
DANGEROUS_._PDfConDropperDentro.pdf_DANGEROUS	25 nov 2016 17:57	4 KB	Documento
DANGEROUS_._PDFLimpio.pdf_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._ScriptPython.py_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_._ZIPconPDFconDropperDentro.zip_DANGEROUS	25 nov 2016 18:00	4 KB	Documento
DANGEROUS_._ZipLegitimoConAplicacionParaWindows.zip_DANGEROUS	25 nov 2016 18:01	4 KB	Documento
DANGEROUS_autorun.inf_DANGEROUS	25 nov 2016 17:57	113 bytes	Documento
DANGEROUS_DocumentoConMacroDOC.doc_DANGEROUS	25 nov 2016 18:01	33 KB	Documento
DANGEROUS_MusicaConImagenDentro.mp3_DANGEROUS	25 nov 2016 17:57	81,2 MB	Documento
DocumentoLimpioDOC.doc	25 nov 2016 18:01	205 KB	Docum...(.doc)
DocumentoLimpioDOCX.docx	25 nov 2016 18:01	22 KB	Docum...(.docx)
eicar_com.zip	25 nov 2016 18:01	--	Carpeta
eicarcom2.zip	25 nov 2016 18:01	--	Carpeta
ImagenconBombaZip.png	25 nov 2016 18:01	14 KB	Image...s (PNG)
ImagenconBombaZip.png.metadata.txt	25 nov 2016 18:01	0 bytes	Texto
ImagenLimpia.jpg	25 nov 2016 18:01	80 KB	Imagen JPEG
ImagenLimpia.jpg.metadata.txt	25 nov 2016 18:01	0 bytes	Texto
ImagenLimpiaPNG.png	25 nov 2016 18:01	96 KB	Image...s (PNG)
ImagenLimpiaPNG.png.metadata.txt	25 nov 2016 18:01	0 bytes	Texto
logs	25 nov 2016 17:56	--	Carpeta
ScriptPython.py.txt	25 nov 2016 18:01	6 KB	Texto
ZIPconPDFconDropperDentro.zip	25 nov 2016 18:00	--	Carpeta
ZipLegitimoConAplicacionParaWindows.zip	25 nov 2016 17:59	--	Carpeta

Hacktivismo nivel PRO

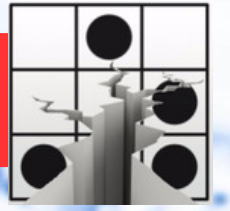


CIRCLean ha renombrado los archivos que considera potencialmente peligrosos, algunos como los archivos Doc sin macros nos los permite abrir directamente.

También extrae el contenido de los archivos comprimidos, en el caso de la BombaZip estaba preparada para generar 42TB de datos, lo ha bloqueado y evitado.

Y habría más cosas por ver, esto es lo básico para protegerse, quizás prepare una charla centrada en este último apartado para el futuro.

FIN



Esto es todo camaradas

Ruegos y preguntas