
Ciberdefensa Personal
DESERTSEQ
HACKMEETING

¿Quien soy?

- Jorge Louzao
- Ingeniero de infraestructuras IT en una empresa del Nasdaq
- Certified Ethical Hacker
- DevSecOps, la primera línea de batalla
- Paranoico full time

Amenazas en el mundo digital

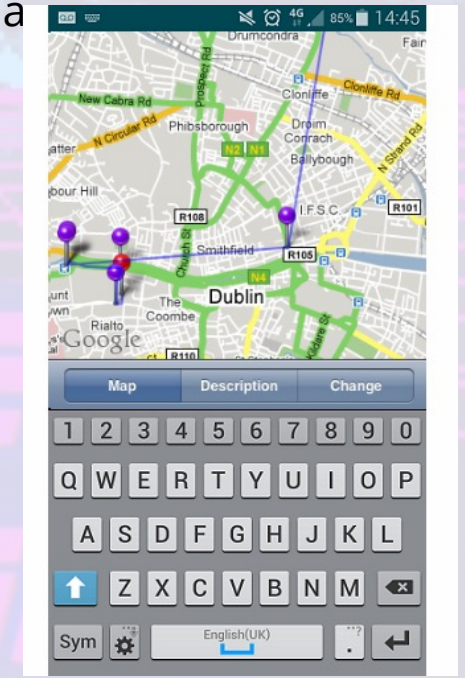
- Comunicaciones móviles, SS7, voz, datos, SMS
- Almacenamiento en la nube
- Redes WiFi privadas y públicas
- Otras frecuencias de radio, NFC, IR
- Ordenadores, móviles, tablets, routers, IoT, ¿Smart?TV, robots de cocina
- Phishing, Malware, Malvertising, 0day
- Nosotros mismos

Comunicaciones móviles - SS7

- SS7 es un protocolo de intercambio de información de señalización entre operadoras telefónicas
- Funciones peligrosas: Grabar o escuchar llamadas, geolocalizar al objetivo a nivel de calle, leer SMS, interceptar tráfico de datos, reenvío transparente de llamadas
- Lleva años usándose para interceptar los SMS bancarios de autentificación 2FA, es conocido el caso de 2017 en el que clientes de bancos en Alemania sufrieron este ataque, siendo los SMS de 2FA reenviados a un tercer operador desconocido y sus cuentas vaciadas. https://arstechnica.com/security/2017/05/thieves-drain-2fa-protected-bank-accounts-by-abusing-ss7-routing-protocol/
- Muchas redes a nivel global siguen siendo vulnerables https://youtu.be/b_B7r3byUPo

Comunicaciones móviles - SS7

- Sin demasiados conocimientos técnicos y por unos céntimos podemos localizar a usuarios con varios servicios vía web como http://www.txtnation.com/mobile-messaging/vlr-number-lookup/
- El resto de funciones de intercepción son un poco más complicadas de realizar, pero tampoco demasiado si la red del objetivo no está bien configurada



Comunicaciones - Datos

- Todo debería ir cifrado HTTPS, SMTP, FTPS, pero no siempre es así y aun existen muchos servidores mal configurados que permiten interceptar protocolos cifrados
- Para añadir una capa extra de seguridad existen las VPN y la red TOR, nacida como un servicio para los militares de EE.UU en zonas de conflicto
- Son dos métodos de cifrar nuestro tráfico y evitar ser visto por un adversario con capacidad para interceptar nuestra conexión

Comunicaciones - TOR

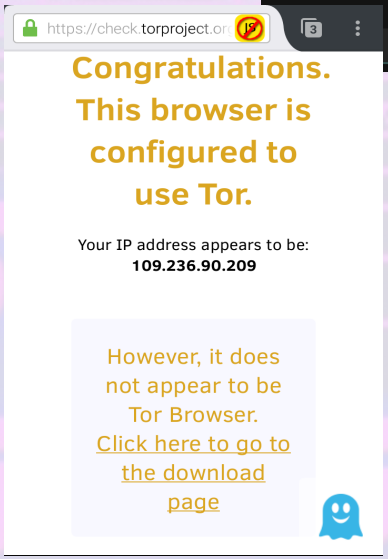
- La opción más sencilla es usar TOR Browser como navegador en nuestro ordenador Windows/Linux/Mac https://www.torproject.org/download/download-easy.html.en
- Tor Browser en Android https://play.google.com/store/apps/details?id=org.torproject.torbrowser&hl=es
- Onion VPN en iPhone/iPad https://itunes.apple.com/us/app/onion-vpn-anonymous-encrypted-secure/id793839665?mt=8
- Usar hardware específico, por ejemplo un router con DD-WRT

Comunicaciones - TOR

- Tor envía nuestro tráfico a través de 3 nodos hasta el destino
- Si el protocolo empleado no es HTTPS el nodo de salida puede escuchar nuestro tráfico e interceptar contraseñas, existen nodos piratas en la red
- Solo aquello que veamos en el Tor Browser irá a través de TOR, el resto del tráfico de nuestro ordenador irá por la conexión normal

Comunicaciones - TOR

- Orbot en Android tiene 3 modos de funcionamiento
- Como Proxy, que luego hay que configurar manualmente en las aplicaciones que dispongan de esta posibilidad, como la de Twitter o Firefox para Android
- Como proxy transparente, que solo funciona cuando el móvil está rooteado
- Como VPN, para móviles sin rooteado, utiliza la API de VPN de Android para que todo el tráfico vaya por TOR, está en beta, los desarrolladores no recomiendan usarlo aun
- Tor Browser está basado en Firefox, no necesita Orbot para funcionar en Android



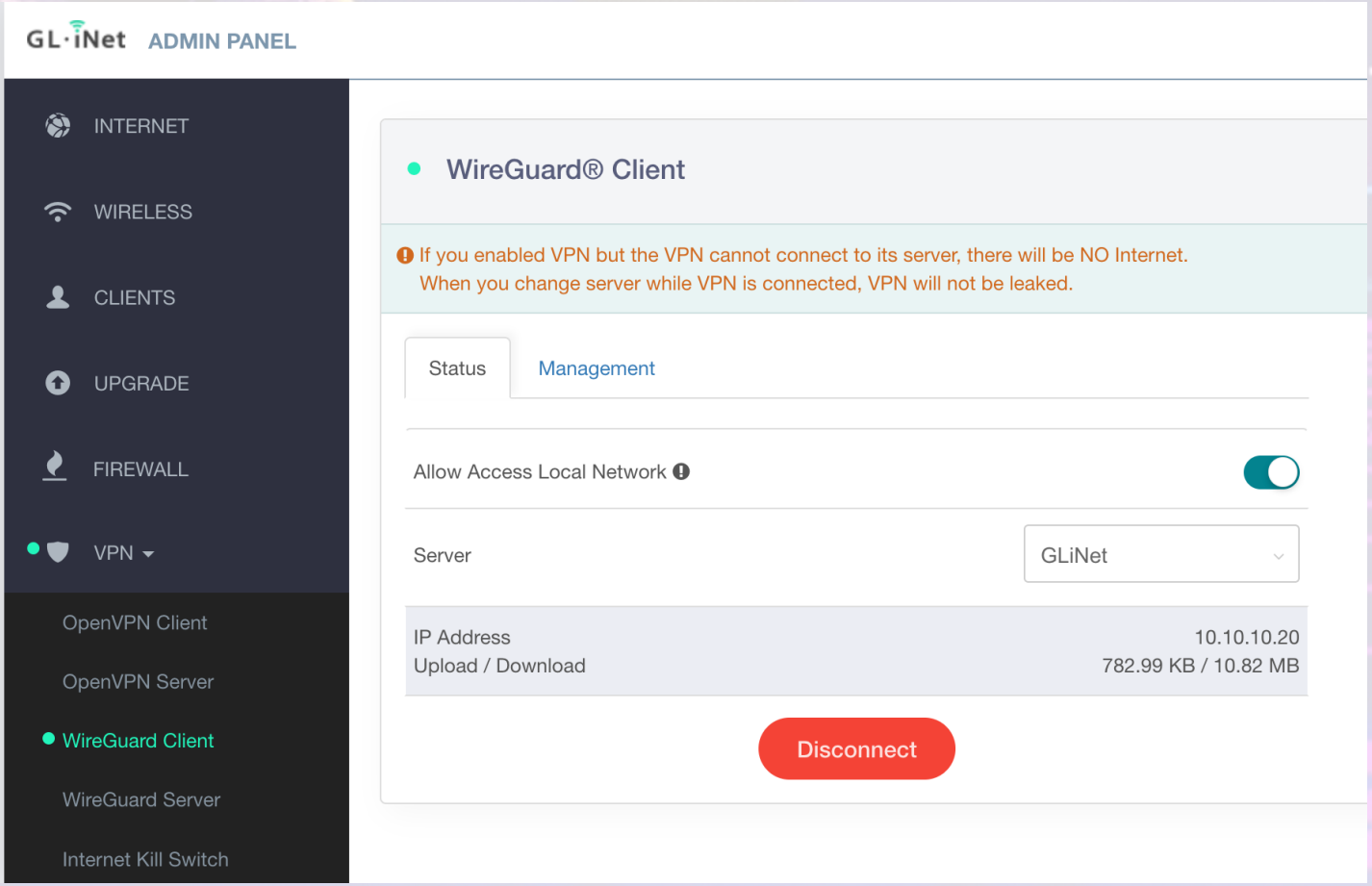
Comunicaciones - TOR

- El mini router GL AR750S viene con OpenWRT y OpenVPN de serie, permite conectar una segunda antena con un USB WiFi, poco consumo, se puede usar con batería externa, económico https://www.gl-inet.com/products/gl-ar750s/
- Con este dispositivo nos aseguramos de que todo nuestro tráfico va por TOR o VPN según nuestras preferencias
- Dispone de conexiones gigabit lan, WiFi 2.4 y 5Ghz.
- Otras opciones son usar S.O. basados en Linux como Tails https://tails.boum.org o Whonix https://www.whonix.org que usan TOR por defecto en todas las comunicaciones

Comunicaciones - VPN

- El software más conocido es OpenVPN disponible para todas las plataformas
- Existen servicios confiables como NordVPN (que también da acceso desde su VPN a TOR) https://nordvpn.com
- Si el servicio es gratuito y no hay una asociación o fundación detrás, no lo uses, el producto eres tú
- Otros como ProtonVPN https://protonvpn.com/ que ofrecen salida por un nodo diferente al de entrada, TOR y también ofrece un servicio de email cifrado, Protonmail.
- Proxy SH https://proxy.sh/ que también ofrece salida por un nodo diferente al de entrada, TOR y utilizar obfsproxy para simular tráfico normal en lugar de una VPN como puede hacer TOR, saltándose restricciones de sistemas de inspección de paquetes que bloqueen el tráfico detectado como OpenVPN o TOR
- Todos ofrecen ya Wireguard, una VPN más rápida e igualmente segura. Es una VPN connection-less

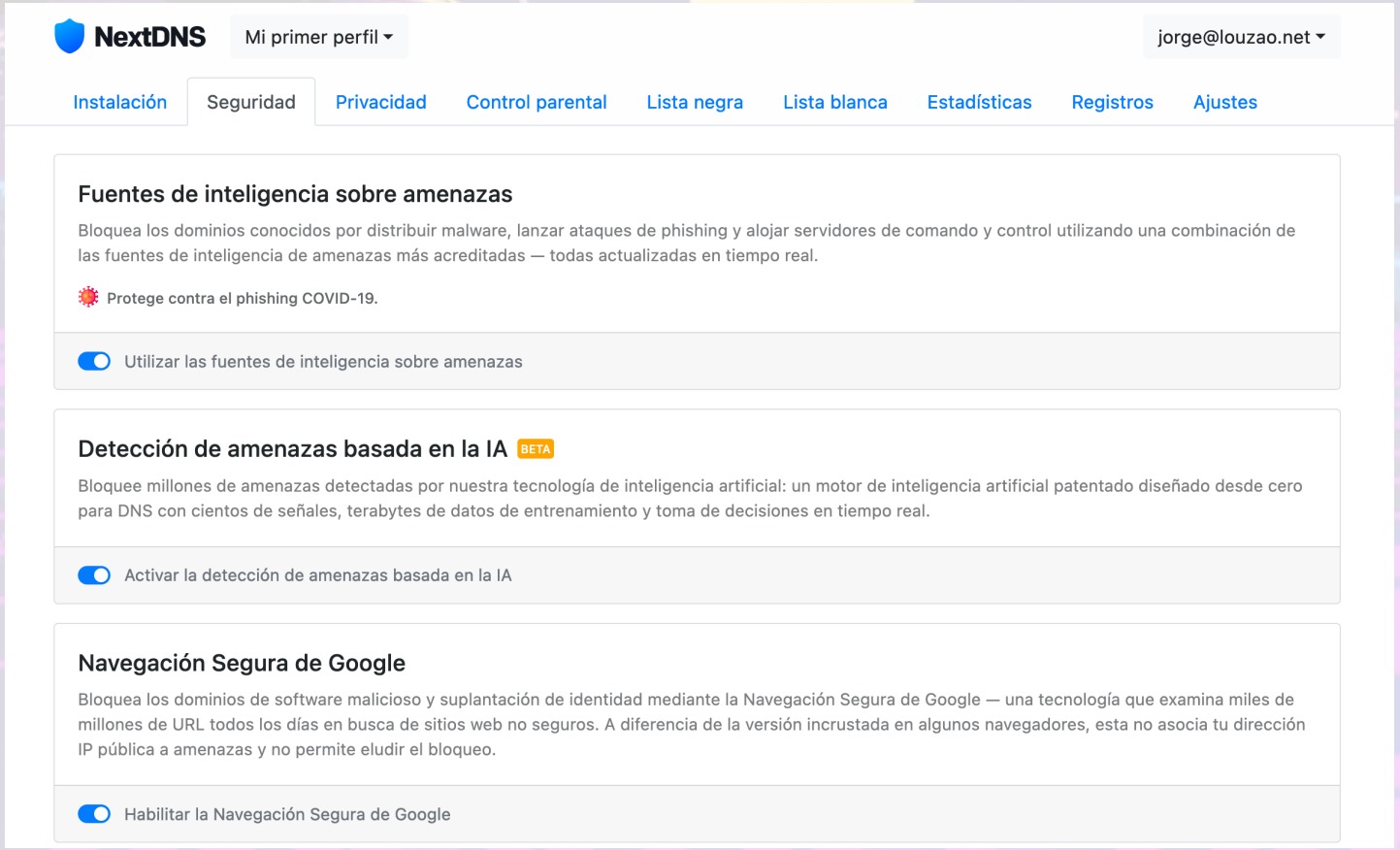
Comunicaciones - VPN



Comunicaciones - DNS

- En el día a día, desde casa, cuando no necesitamos VPN, dependemos de los DNS que nos ofrece nuestra operadora de Internet, que dejan pasar cualquier consulta que nuestros dispositivos les envíen, incluyendo peticiones a sitios de malware, phishing, etc. Además de que estamos usando un protocolo que no va cifrado.
- Existen disversos servicios gratuitos y de pago para subsituir nuestros DNS por otros más seguros y que emplean métodos de comunicación cifrados.
- Quad9 es una empresa sin ánimo de lucro radicada en Suiza que vive de donaciones y patrocinadores. Incluye inteligencia de diversas fuentes para no resolver sitios maliciosos. https://quad9.net/
- DNS 0 es una ONG francesa que ofrece un servicio similar.
- Sus creadores tiene otro servicio de pago en EE.UU que permite un control granular, https://nextdns.io/ que es gratuito si no hacemos más de 300.000 consultas DNS al mes.

Comunicaciones - DNS



Comunicaciones - DNS

validación o verificación de identidad. Mientras que los nombres de host DDNS legítimos son raramente accedidos en el uso diario, sus contrapartes maliciosas son muy utilizadas en las campañas de phishing - por ejemplo, paypal-login.duckdns.org.

Si estás usando DDNS, ten en cuenta que esta configuración no bloqueará el sitio web de los servicios DDNS o su API de actualización.

Bloquear nombres de host DNS dinámicos

Bloquear dominios aparcados

Los dominios aparcados son sitios web de una sola página que a menudo están cargados de anuncios y carecen de valor. La monetización de dominios estacionados a veces puede confundirse con prácticas sospechosas y contenido malicioso.

Bloquear dominios aparcados

Bloquear dominios de nivel superior (TLD)

Bloquea todos los dominios y subdominios que pertenecen a TLD específicos.

.mov ×

.zip ×

AÑADIR UN TLD

Bloquear material de abuso sexual infantil

Bloquea los dominios que alojan material de abuso sexual infantil con la ayuda del Project Arachnid, operado por el Canadian Centre for Child Protection. No se transmite información a Project Arachnid cuando se bloquea un dominio.

Bloquear material de abuso sexual infantil

Comunicaciones - DNS

Listas de bloqueo

Bloquea anuncios y rastreadores utilizando las listas de bloqueo más populares disponibles — todas actualizadas en tiempo real.

Lista de bloqueo de anuncios y rastreadores de NextDNS

Una lista de bloqueo completa para bloquear anuncios y rastreadores en todos los países. Esta es la lista de bloqueo inicial recomendada.

194.788 entradas • Actualizado hace un día

AÑADIR UNA LISTA DE BLOQUEO

Protección de rastreo nativo BETA

Bloquea rastreadores de amplio espectro — que a menudo operan a nivel del sistema operativo — que rastrean tu actividad en un dispositivo. Esto podría incluir todos los sitios web que visitas, todo lo que escribes o tu ubicación en todo momento.

Apple
iOS, macOS, tvOS

Samsung
Teléfonos, tabletas, TV inteligentes

Windows
Todas las versiones

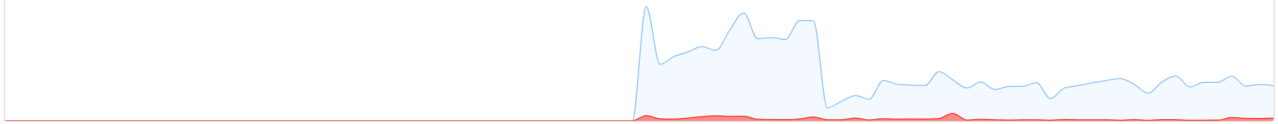
Comunicaciones - DNS

Todos los dispositivos ▾ | Últimos 3 meses ▾

1.066.537	42.950	4,03 %
consultas	consultas bloqueadas	de consultas bloqueadas

Consultas

Evolución de las consultas en el tiempo.



Dominios resueltos

Dominios que se resolvieron sin ser bloqueados por ninguna configuración o porque se permitieron manualmente.

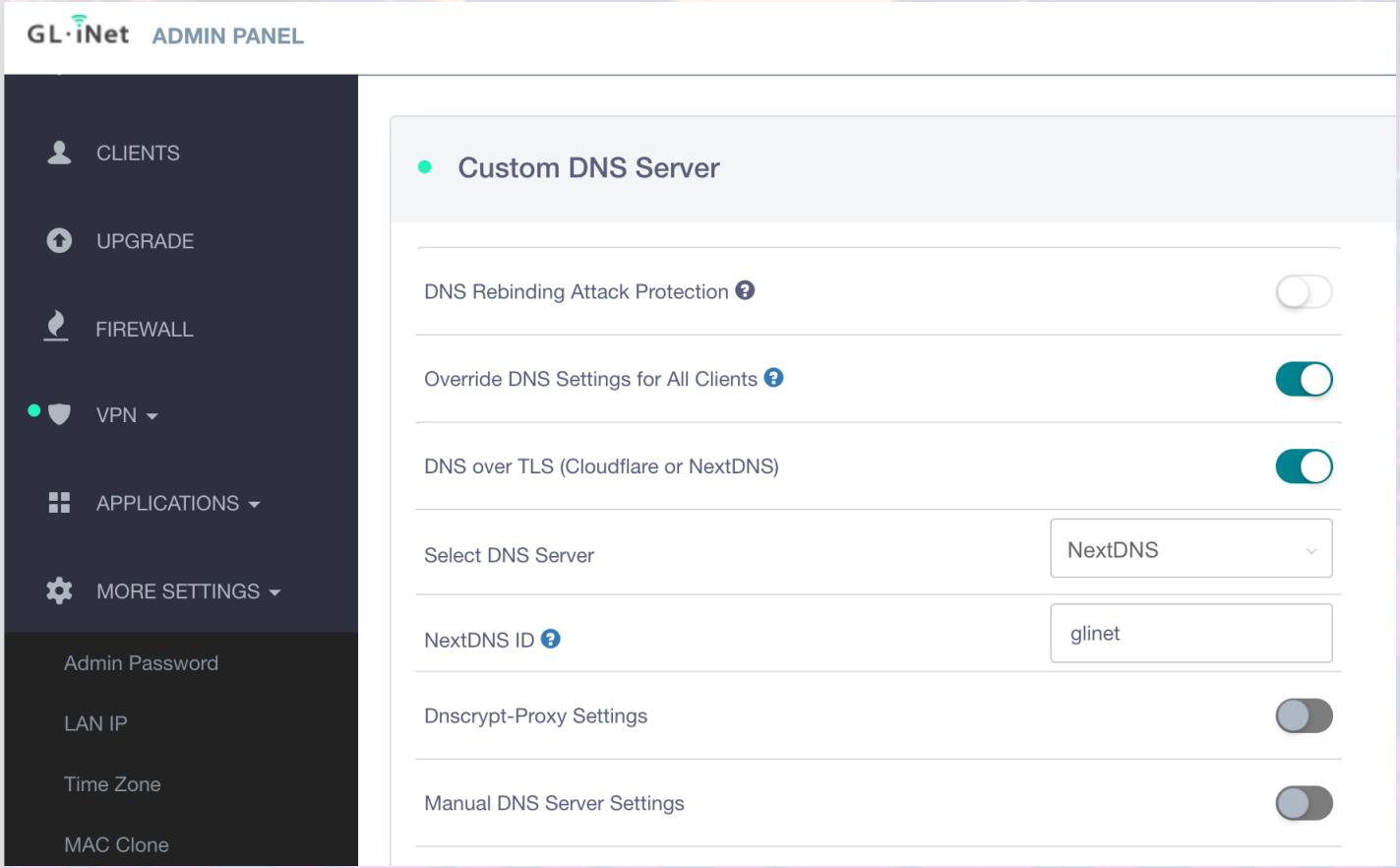
tracker.dutchtracking.com	60.267
tracker.filetracker.pl	54.512
scs.samsungqbe.com	32.489
staging.mycloud.com	26.901
tracker2.wasabii.com.tw	24.578

Dominios bloqueados

Dominios bloqueados por una configuración de Seguridad, Privacidad y/o Control Parental o porque fueron bloqueados manualmente.

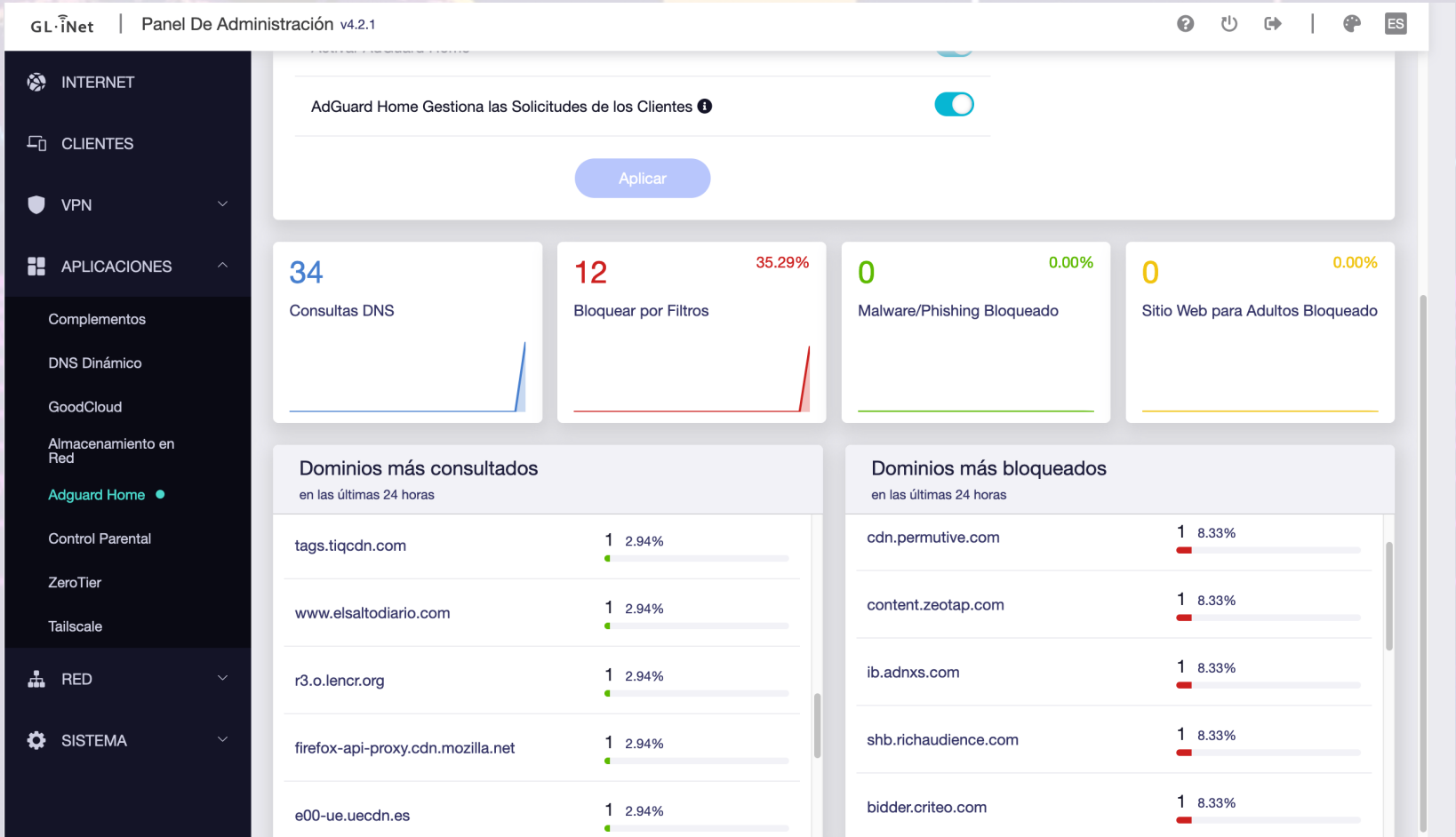
incoming.telemetry.mozilla.org	2196
www.googletagmanager.com	2157
mobileconfig.sascdn.com	2081
4ac1dd56e493354be504f063e4ae3440a13c6776.cws.conviva.com	2071

Comunicaciones - DNS

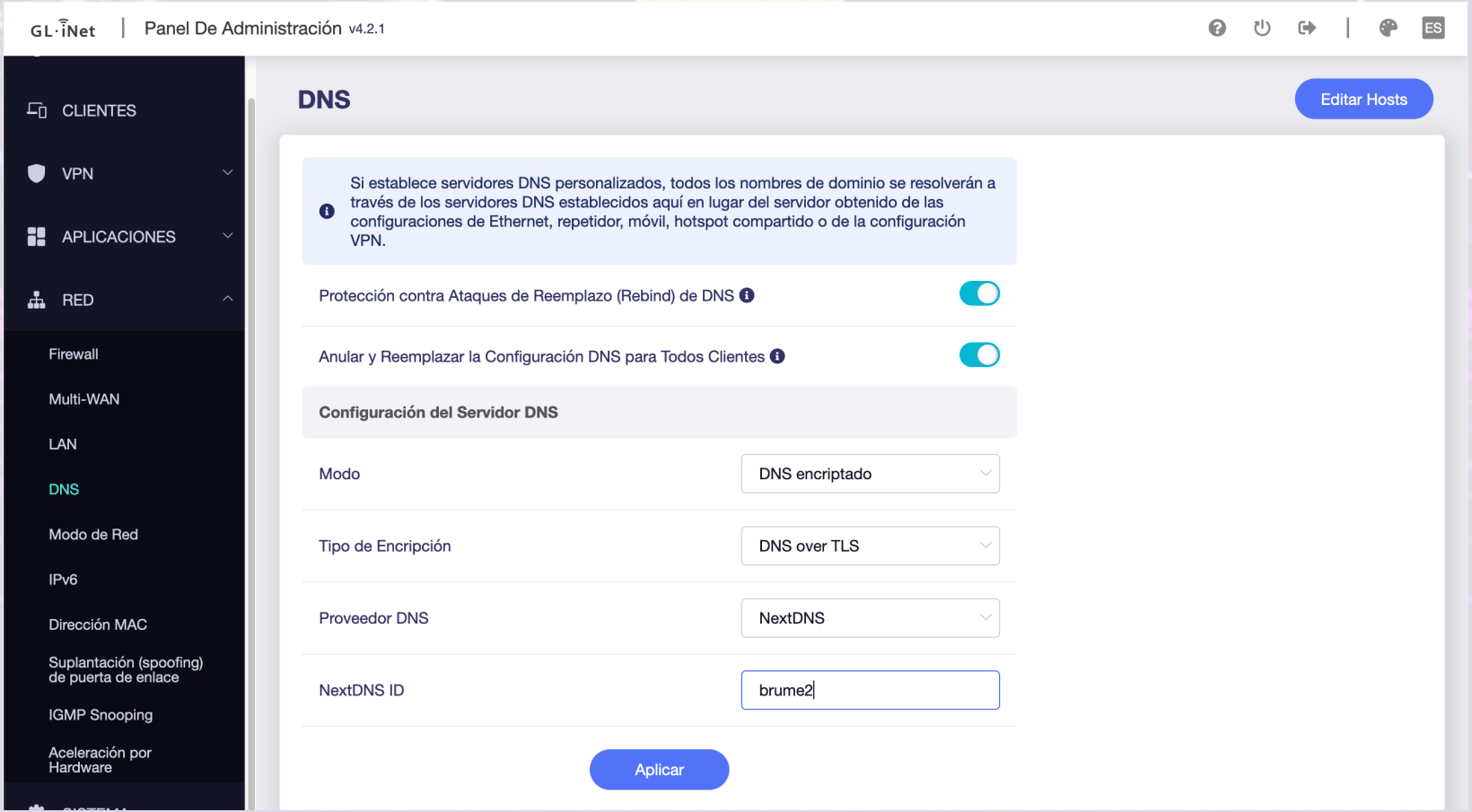


Comunicaciones

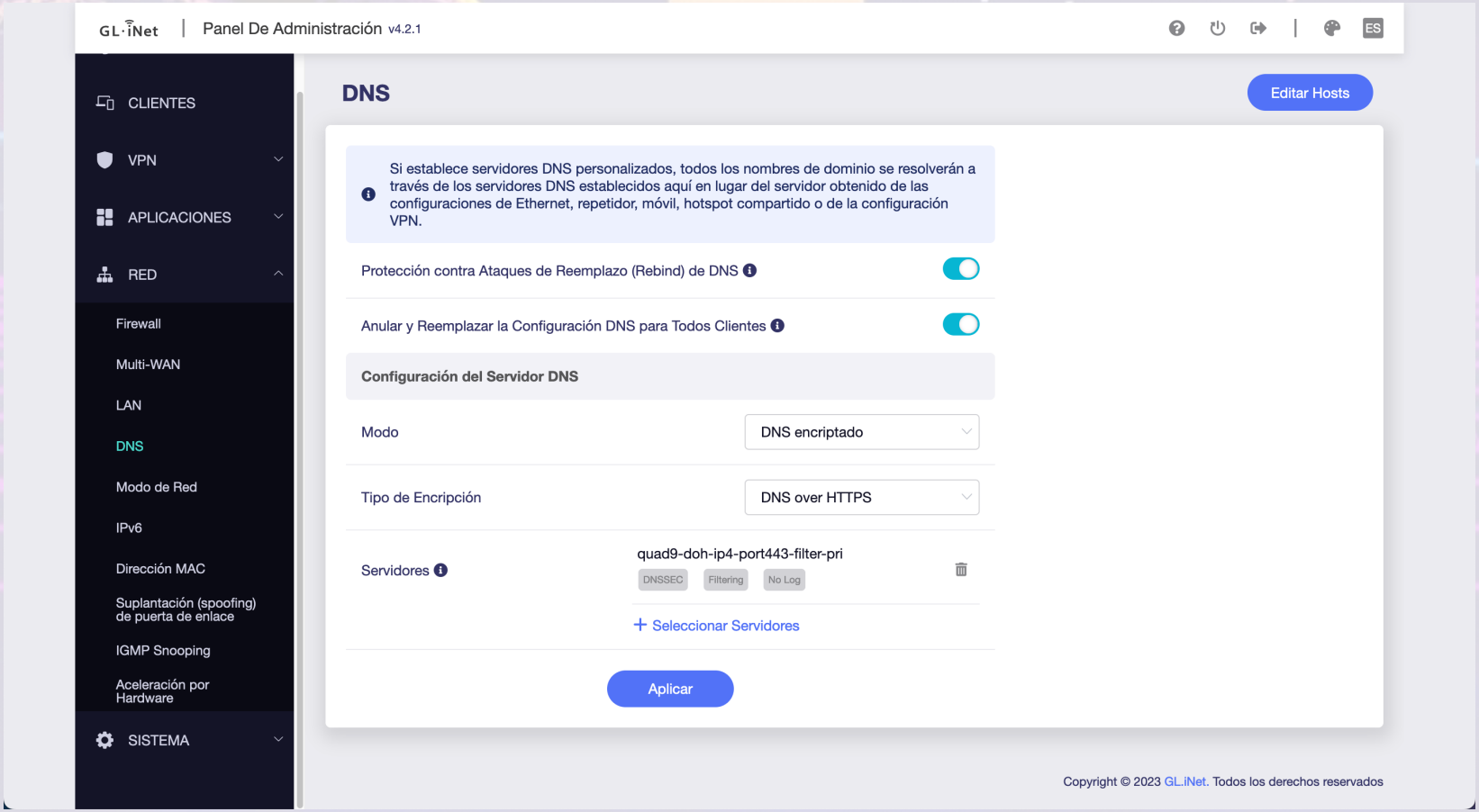
Comunicaciones



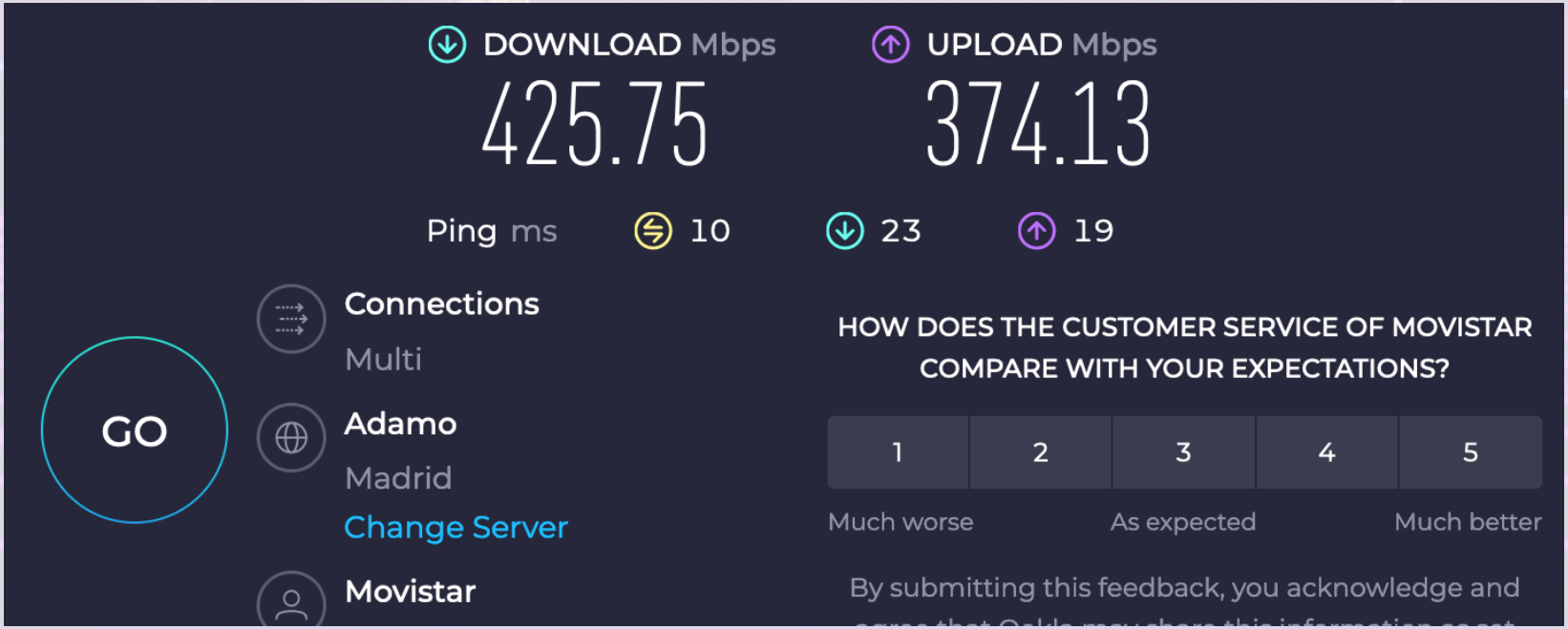
Comunicaciones



Comunicaciones



Comunicaciones



Comunicaciones - Mensajería

- Signal está disponible para Android, iOS y como plugin para navegadores Chrome
- Gestiona los SMS tradicionales y usa su servicio de mensajería segura cuando el destinatario es usuario de la aplicación. Usa datos en lugar de SMS/MMS, permite envío cifrado de imágenes y vídeos. Chats cifrados en grupo
- Es software libre https://github.com/WhisperSystems/Signal-Android
- Permite realizar llamadas VoIP y videollamadas cifradas. Servidores en EE.UU
- Gracias al FBI sabemos que no almacenan nada de las conversaciones, metadatos, etc.

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

Comunicaciones - VoIP

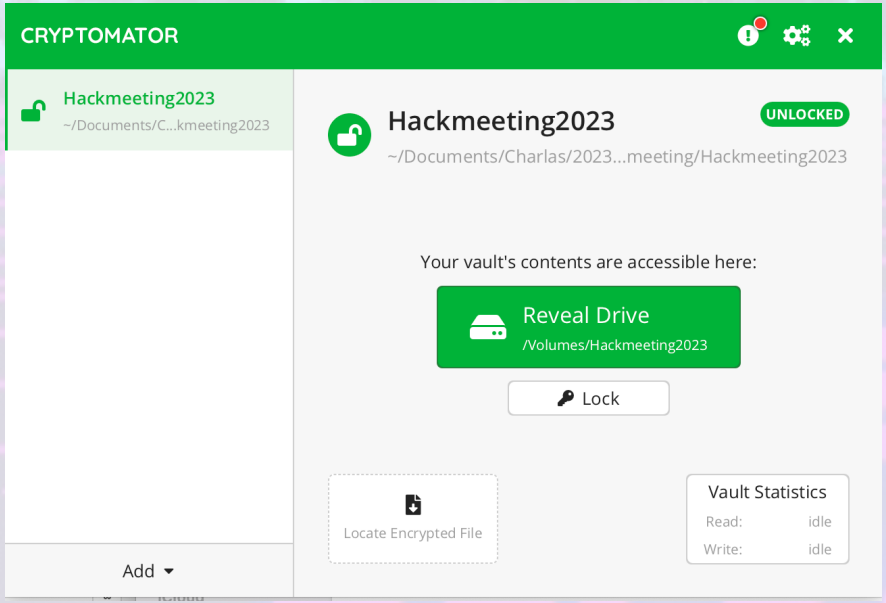
- Linphone es una app de software libre para todas las plataformas de escritorio y móviles, incluso Windows Phone. https://www.linphone.org
- Emplea ZRTP para cifrar las comunicaciones, igual que Signal. También dispone de videollamada. Sus servidores están en Francia.
- Puedes montar tu propio servidor o usar una cuenta gratuita: jorgesdb@sip.linphone.org
- ZRTP es una extensión de RTP (Protocolo de transporte en tiempo real) con intercambio seguro de claves mediante Diffie-Hellman. Las claves son efímeras y con soporte Perfect Forward Secrecy

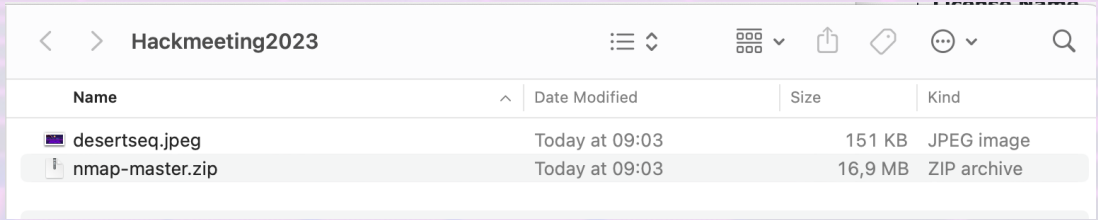
Almacenamiento en la Nube

- La nube no existe, es el ordenador de otra persona en el que almacenamos nuestros datos
- Google Drive, DropBox, OneDrive, Box, los datos están al alcance de cualquiera con los privilegios suficientes
- iDrive o SpiderOak ofrecen lo mismo pero permitiendo el uso de una clave de cifrado, los archivos salen cifrados de nuestros dispositivos. Cero conocimiento
- Con un poco más de conocimiento podemos montar nuestro propio almacenamiento con Nextcloud. Cifra los archivos almacenados al recibirlos el servidor, no en nuestro dispositivo, siempre que hayamos configurado esta función.
- También permite guardar nuestros contactos y calendario para usarlo luego desde un dispositivo móvil con app como CardDAV-Sync y así no almacenarlos en Google

Almacenamiento en la Nube

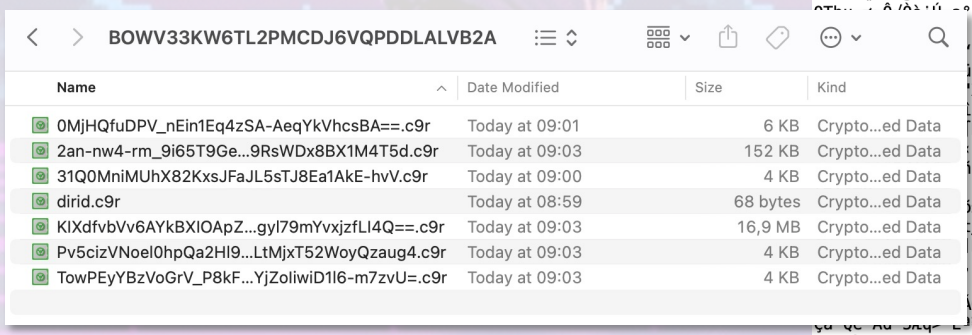
- También podemos usar servicios no confiables como Dropbox o Google Drive con app de código abierto como EncFS o Cryptomator disponibles para todas las plataformas https://cryptomator.org





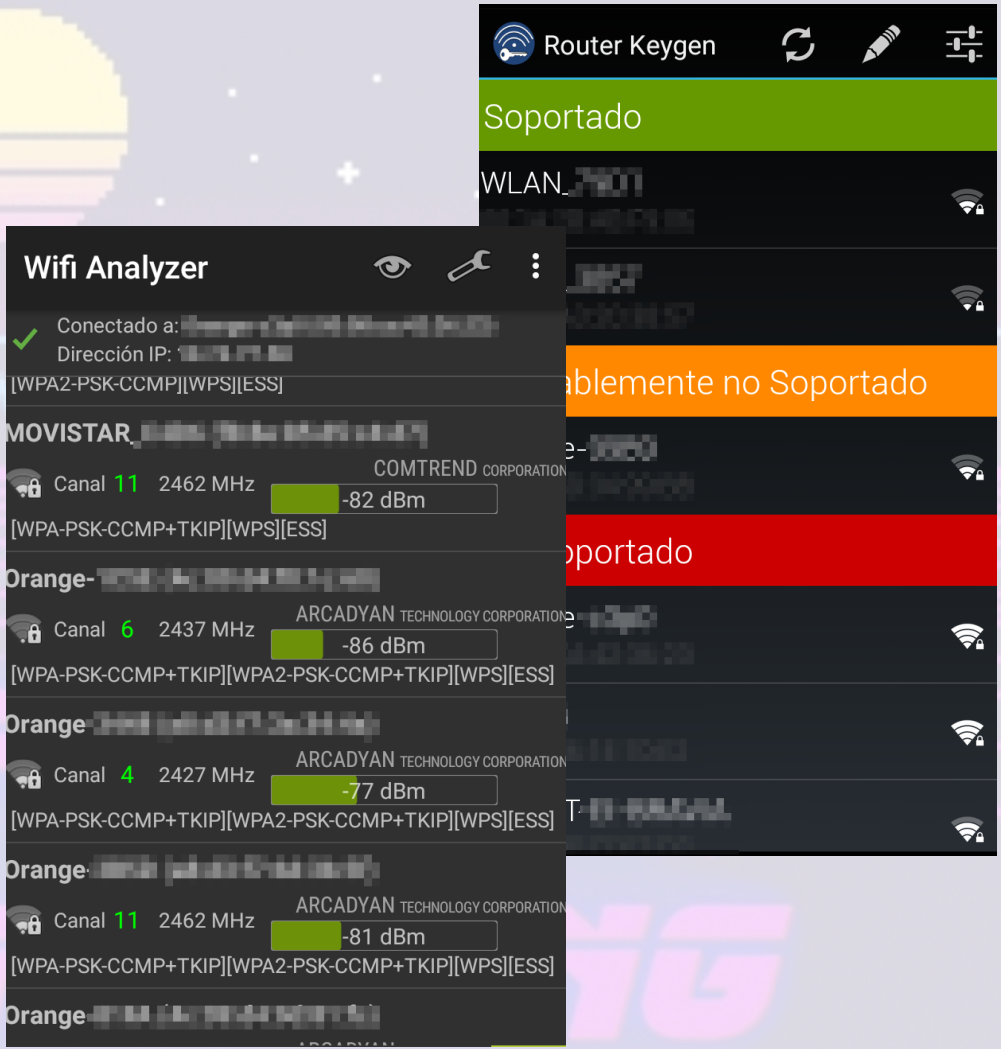
Almacenamiento en la Nube

- Esto es lo que vería un atacante



Redes WiFi

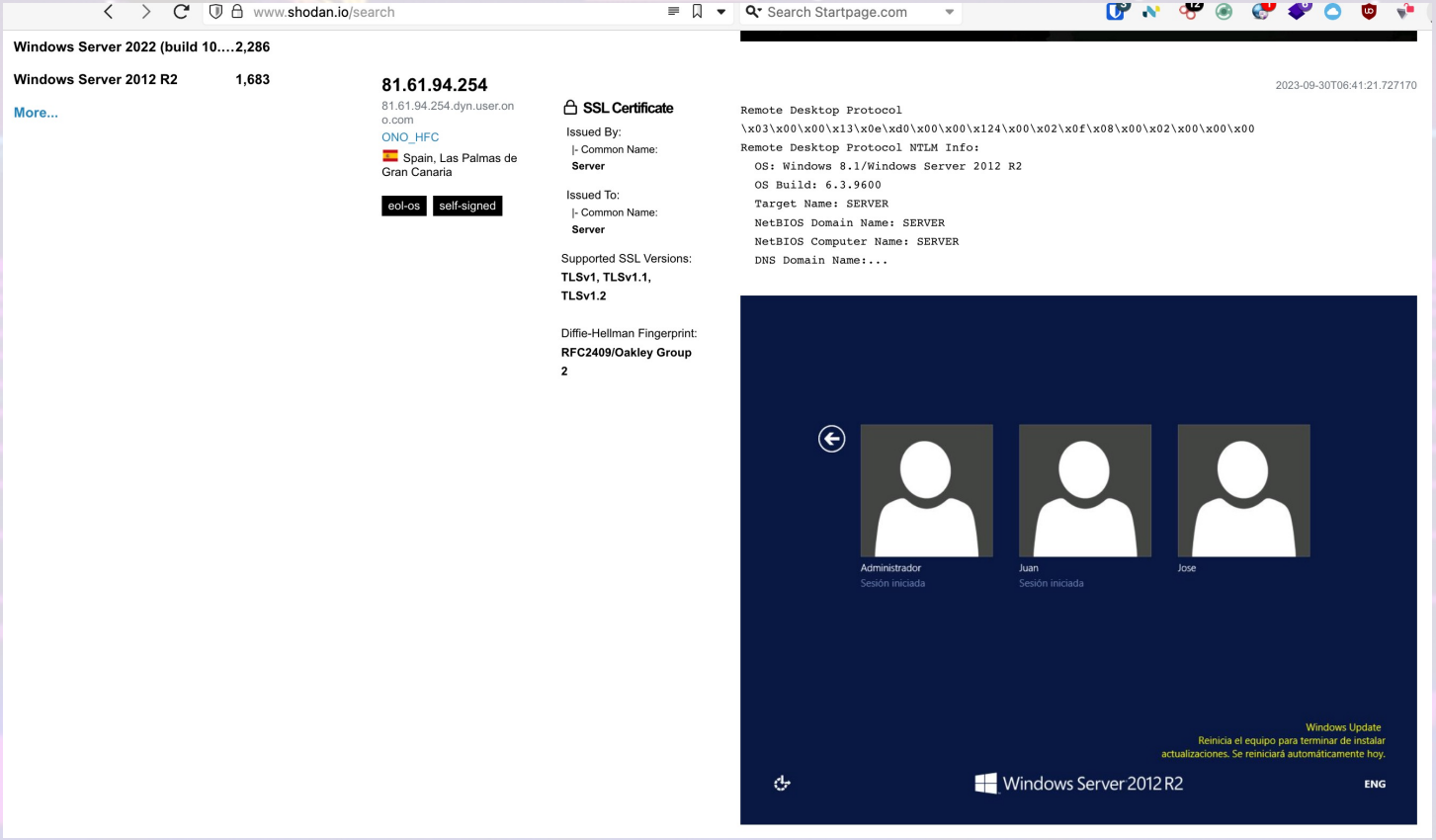
- No hay que confiar en ninguna red WiFi, incluyendo las privadas
- En el router de nuestra operadora cambiar claves de admin, WiFi, desactivar WPS y uPNP y asegurarnos que usamos WPA2 con AES, no con TKIP, o las nuevas WPA3/SAE (Simultaneous Authentication of Equals)
- Aplicaciones como https://routerkeygen.github.io/ y WiFi Analyzer pueden ayudarnos a comprobar que está bien configurado



Redes WiFi

- WPS (WiFi Protected Setup) tiene un modo de funcionamiento basado en un PIN de 8 dígitos numéricos, el 8º es un dígito de control, con lo que el PIN real son 7 dígitos
- Por un fallo de diseño es posible obtenerlo mediante fuerza bruta con tan solo 11.000 claves diferentes como máximo, 10.000 de los 4 primeros dígitos, 1.000 de los 3 siguientes, que se pueden calcular por separado en lugar de tener que probar 1.000.000 de claves con 7 dígitos
- Hay otros ataques que afectan a algunos modelos de router como el Pixie Dust, que nos permite recuperar la clave WPA2 en pocos minutos
- uPNP abre puertos al exterior cuando una aplicación lo pide, DLNA, Windows Remote Desktop, BitTorrent y un largo etc

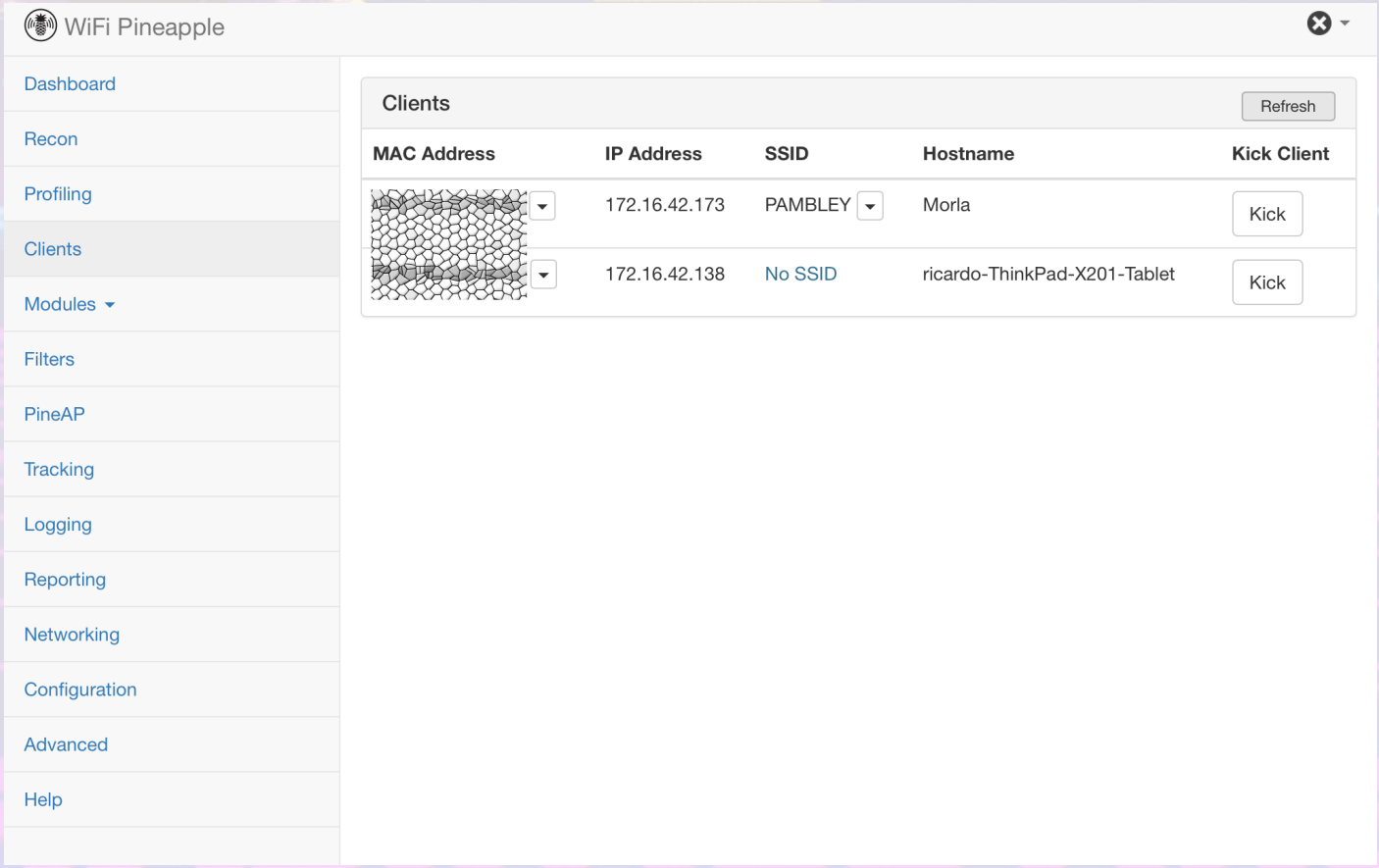
Redes WiFi


www.shodan.io/search
Search Startpage.com
Windows Server 2022 (build 10....2,286
Windows Server 2012 R2 1,683
More...
81.61.94.254
81.61.94.254.dyn.user.ono.com
ONO_HFC
Spain, Las Palmas de Gran Canaria
eol-os
self-signed
SSL Certificate
Issued By:
|- Common Name:
Server
Issued To:
|- Common Name:
Server
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2
2023-09-30T06:41:21.727170
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
OS: Windows 8.1/Windows Server 2012 R2
OS Build: 6.3.9600
Target Name: SERVER
NetBIOS Domain Name: SERVER
NetBIOS Computer Name: SERVER
DNS Domain Name:...
Administrador
Sesión iniciada
Juan
Sesión iniciada
Jose
Windows Update
Reinicia el equipo para terminar de instalar actualizaciones. Se reiniciará automáticamente hoy.
Windows Server 2012 R2
ENG

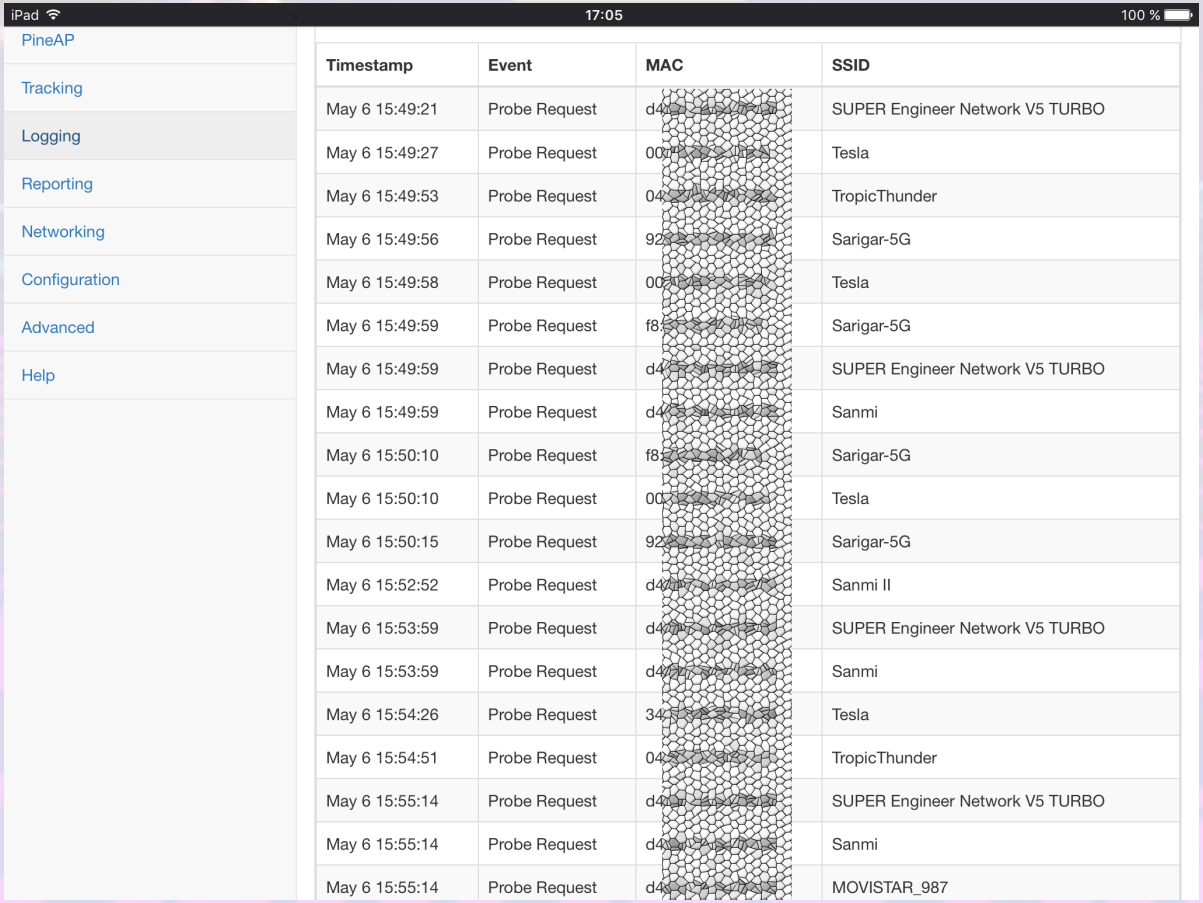
Redes WiFi

- En WiFi públicas, jamás conectarse sin usar una VPN, y si podemos evitar usarlas, mejor
- Nuestros dispositivos WiFi de ordenador o móvil van lanzando Probe Requests, una lista de todos los SSID a los que han estado conectados con anterioridad y se intentarán conectar a cualquier dispositivo que les responda diciendo que es la WiFi que está buscando. No llevar la WiFi activada si no estamos, por ejemplo, en casa
- En Linux se desactiva poniendo passive_scan=1 en la configuración de wpa_supplicant
- En Android se puede evitar con la app Wi-Fi Privacy Police
- Lo mismo con Bluetooth, apagado siempre que no se use

Redes WiFi

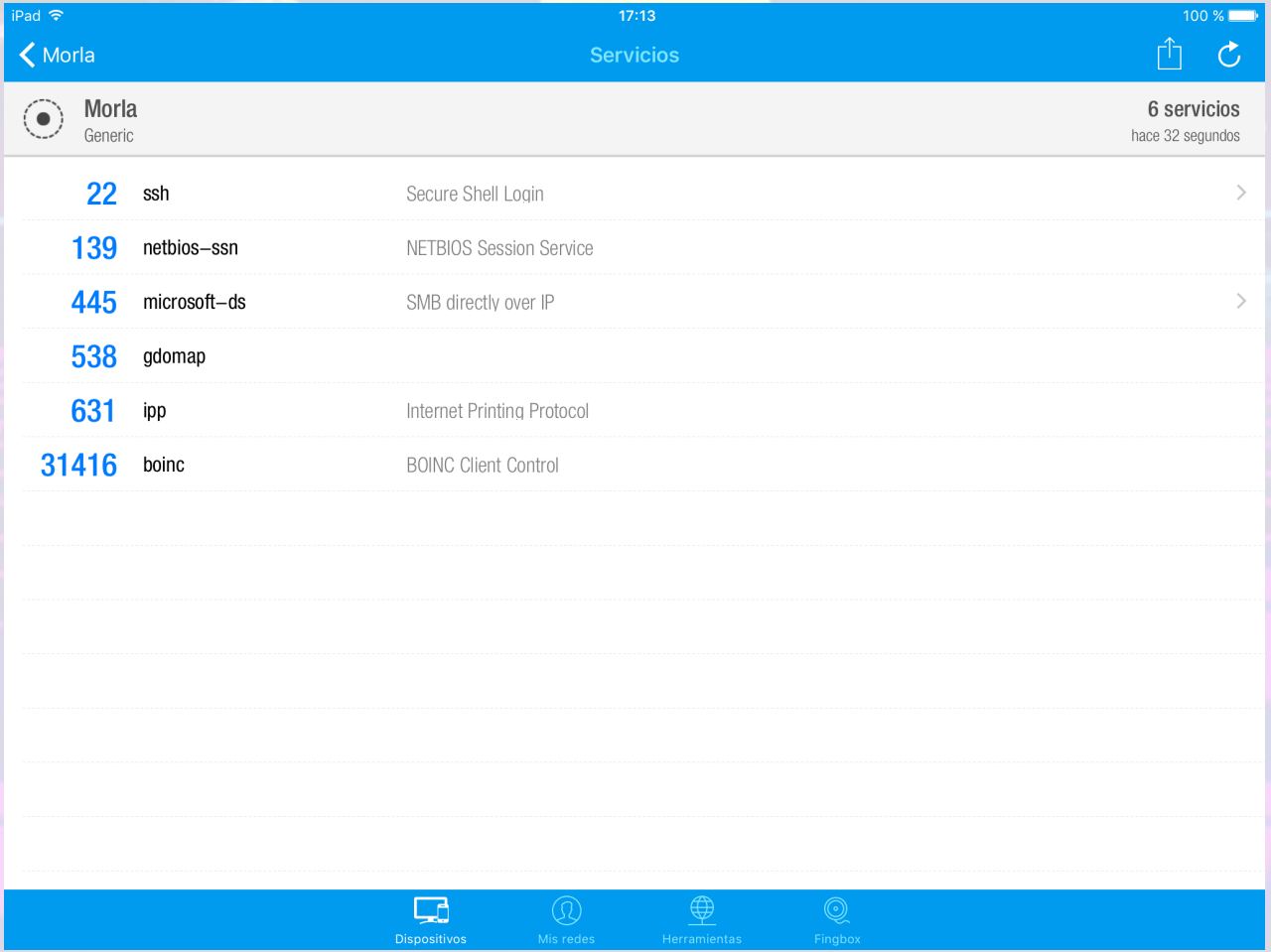

WiFi Pineapple
Dashboard
Recon
Profiling
Clients
Modules
Filters
PineAP
Tracking
Logging
Reporting
Networking
Configuration
Advanced
Help
Clients
Refresh
MAC Address
IP Address
SSID
Hostname
Kick Client
172.16.42.173
PAMBLEY
Morla
Kick
172.16.42.138
No SSID
ricardo-ThinkPad-X201-Tablet
Kick

Redes WiFi



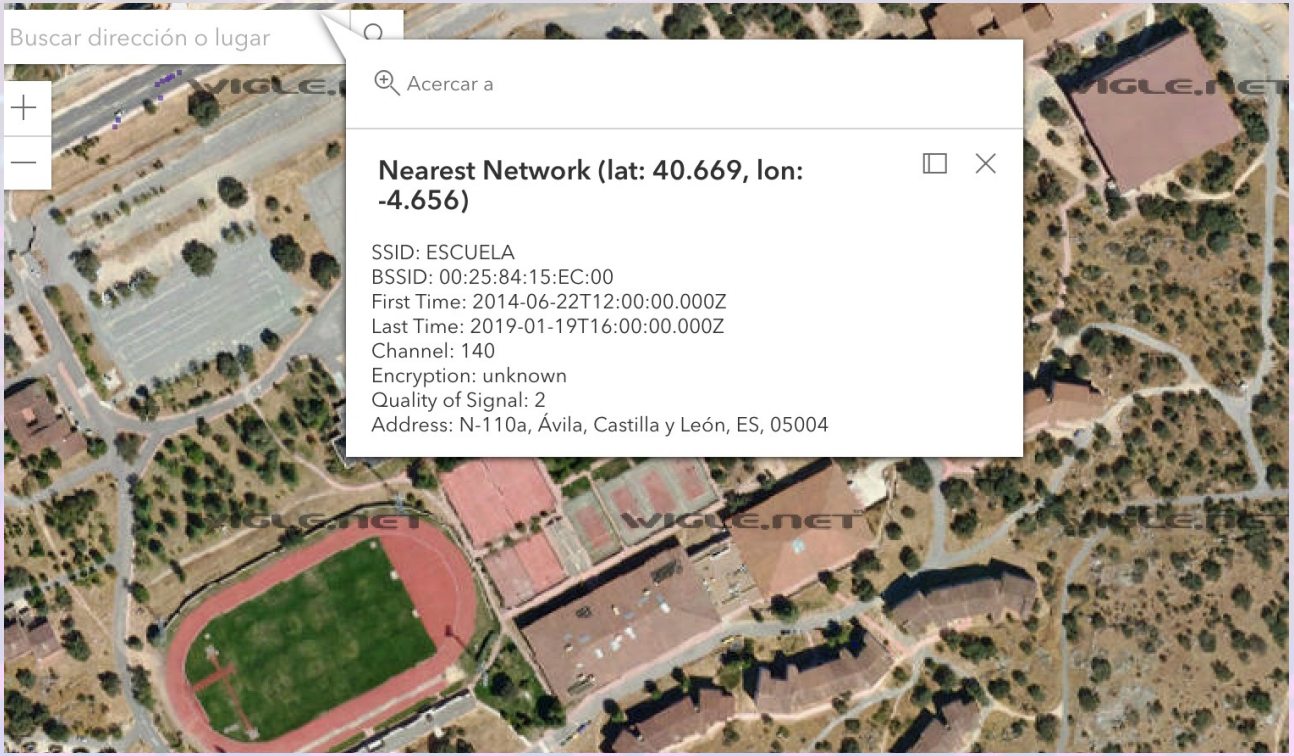
Timestamp	Event	MAC	SSID
May 6 15:49:21	Probe Request	d4[redacted]	SUPER Engineer Network V5 TURBO
May 6 15:49:27	Probe Request	00[redacted]	Tesla
May 6 15:49:53	Probe Request	04[redacted]	TropicThunder
May 6 15:49:56	Probe Request	92[redacted]	Sarigar-5G
May 6 15:49:58	Probe Request	00[redacted]	Tesla
May 6 15:49:59	Probe Request	f8[redacted]	Sarigar-5G
May 6 15:49:59	Probe Request	d4[redacted]	SUPER Engineer Network V5 TURBO
May 6 15:49:59	Probe Request	d4[redacted]	Sanmi
May 6 15:50:10	Probe Request	f8[redacted]	Sarigar-5G
May 6 15:50:10	Probe Request	00[redacted]	Tesla
May 6 15:50:15	Probe Request	92[redacted]	Sarigar-5G
May 6 15:52:52	Probe Request	d4[redacted]	Sanmi II
May 6 15:53:59	Probe Request	d4[redacted]	SUPER Engineer Network V5 TURBO
May 6 15:53:59	Probe Request	d4[redacted]	Sanmi
May 6 15:54:26	Probe Request	34[redacted]	Tesla
May 6 15:54:51	Probe Request	04[redacted]	TropicThunder
May 6 15:55:14	Probe Request	d4[redacted]	SUPER Engineer Network V5 TURBO
May 6 15:55:14	Probe Request	d4[redacted]	Sanmi
May 6 15:55:14	Probe Request	d4[redacted]	MOVISTAR_987

Redes WiFi


iPad
17:13
100 %
Morla
Servicios
Morla
Generic
6 servicios
hace 32 segundos
22 ssh Secure Shell Login
139 netbios–ssn NETBIOS Session Service
445 microsoft–ds SMB directly over IP
538 gdomap
631 ipp Internet Printing Protocol
31416 boinc BOINC Client Control
Dispositivos
Mis redes
Herramientas
Fingbox

Redes WiFi

- https://wigle.net



Mandos a distancia

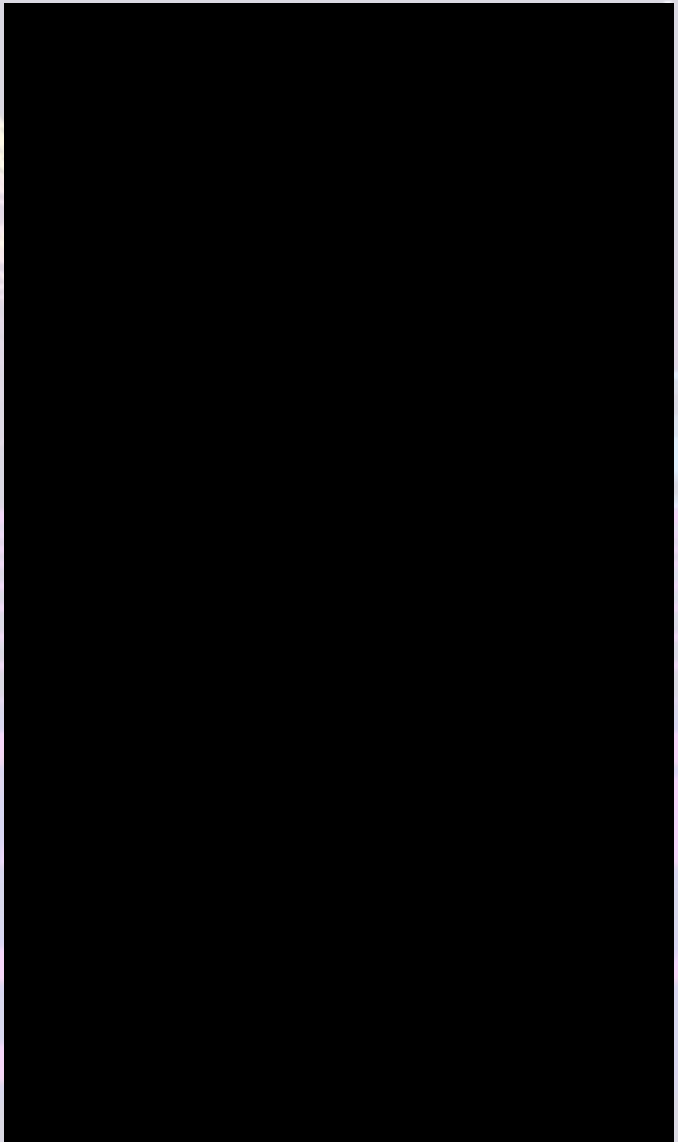
- Existen dispositivos como Flipper Zero o HackRF que permiten interceptar y reproducir señales de radio de diferentes tipos de dispositivos, por ejemplo mandos de garaje, coche. No es sencillo con todos, algunos no se han vulnerado aun, es cuestión de tiempo.

Mandos

NFC

- Aunque las tarjetas NFC cada día son más complejas y difíciles de vulnerar, aún quedan muchas en circulación con un cifrado débil fácil de romper.

NFC



Privacidad en Buscadores

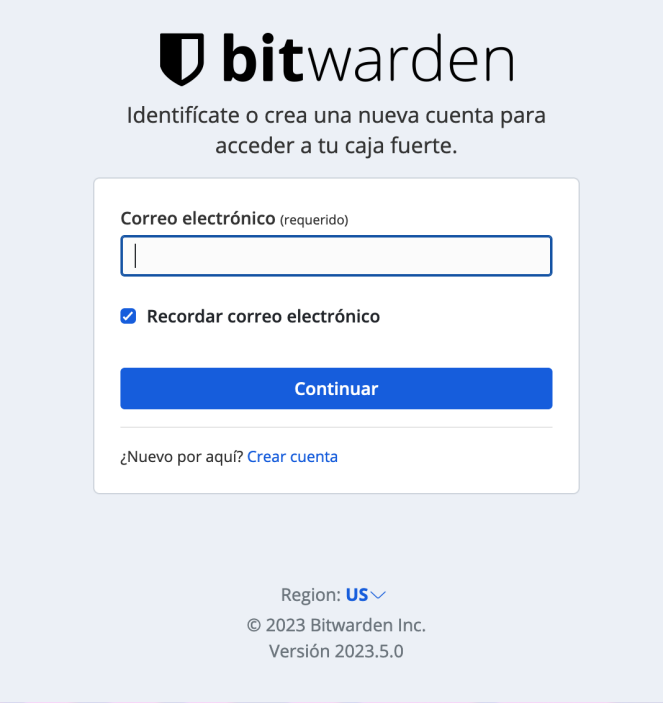
- Swisscows https://swisscows.com/es
- Alojado en servidores propios
- Legislación Suiza de protección de datos
- Startpage. Privacidad auditada por terceros, EuroPrise
- https://www.european-privacy-seal.eu/EPS-en/First-European-Privacy-Seal-Awarded
- DuckDuckGo o Disconnect son empresas americanas 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.

Servicios de Email

- 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, 20GB 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

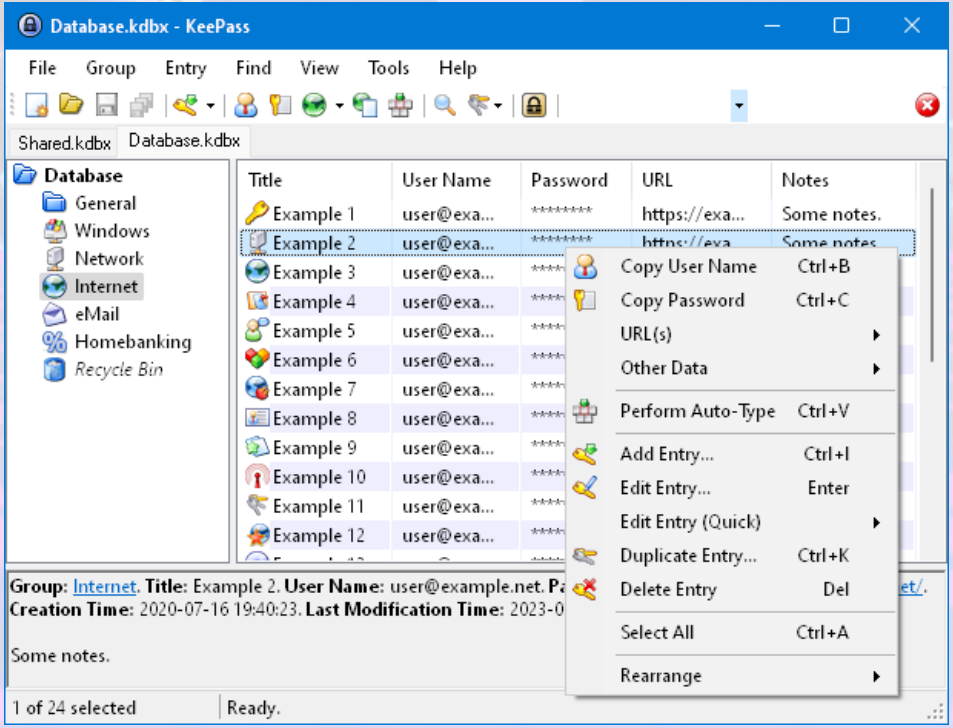
Gestión de Contraseñas

- Hay muchos servicios de gestión de contraseñas. Online mi favorito es Bitwarden. Google y Microsoft ofrecen un servicio similar. Lastpass (que fue vulnerado varias veces), 1Password...



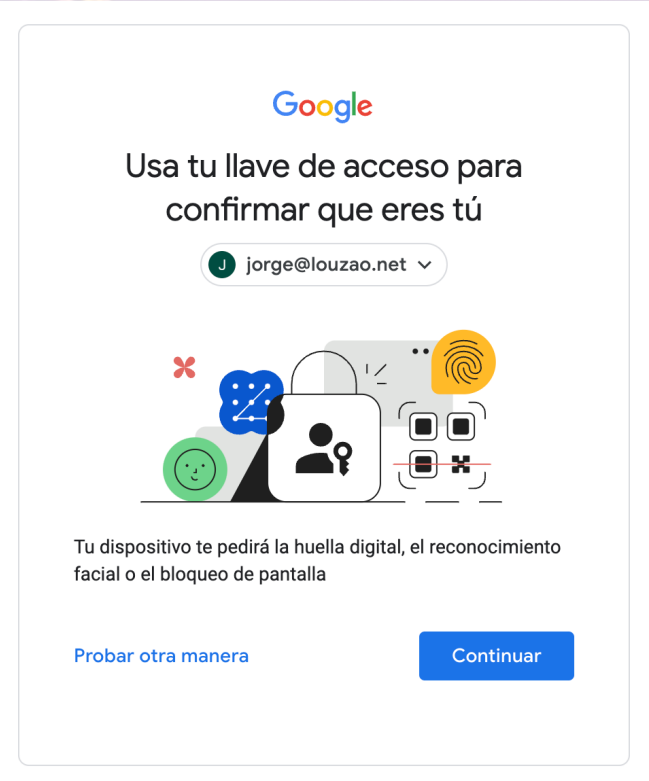
Gestión de Contraseñas

- También hay aplicaciones locales si no queremos tener nuestras claves en la nube



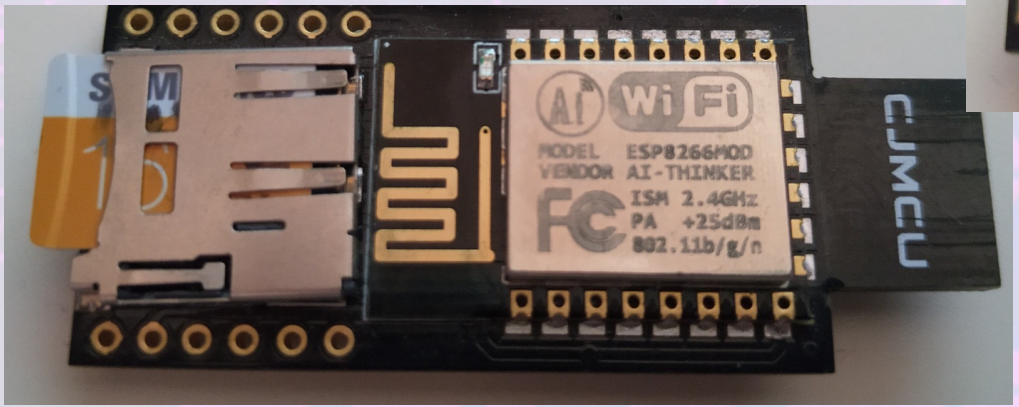
Gestión de Contraseñas

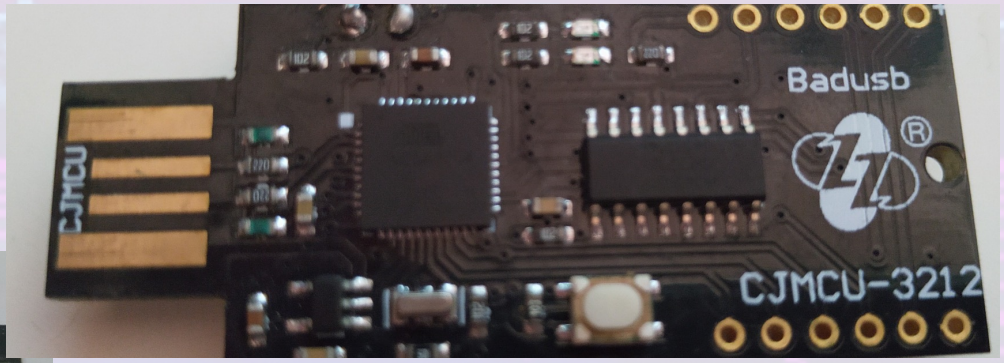
- Existen ya sistemas passwordless.
- Microsoft tiene el suyo, Google está usando ya Passkeys que es una implementación software de FIDO



Dispositivos USB

- No debemos olvidar los BadUSB, dispositivos programados para emular dispositivos como un teclado mientras se hacen pasar por un disco USB normal. Cuestan unos pocos euros en sitios como Aliexpress y los más avanzados vienen incluso con WiFi para exfiltrar información
-





Asegurando dispositivos

- Personal 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 y su sistema de alertas push
- https://copperhead.co/android/

Asegurando dispositivos

- En zonas de conflicto la información importante que obligatoriamente debamos llevar encima conviene que vaya cifrada y fuera del ordenador a ser posible
- Llevando el sistema operativo Tails en un USB que podamos esconder fácilmente, como la gama Ultra Fit de Sandisk que es poco mayor que una uña
- Otros como Whonix requieren dos equipos o dos máquinas virtuales, una con el sistema operativo y otra que hace de gateway con TOR
- Otra opción es usar Qubes OS en el ordenador https://www.qubes-os.org/ requiere equipos bastante potentes para virtualizar otros sistemas operativos como Fedora, Debian, Whonix o Windows 7

Asegurando dispositivos

- Existe una lista de 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

Asegurando dispositivos

- También existe hardware diseñado para Qubes OS, el portátil Librem 14
- 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-14/

Internet de las c...

- El micrófono inteligente de Amazon que también te escucha

≡ EL PAÍS TECNOLOGÍA

MÓVILES REDES SOCIALES BANCO DE PRUEBAS RETINA MERISTATION

Empleados de Amazon escuchan a diario conversaciones que mantienen los usuarios con Alexa

La compañía reconoce anotar un pequeño número de interacciones para "mejorar la experiencia del cliente"

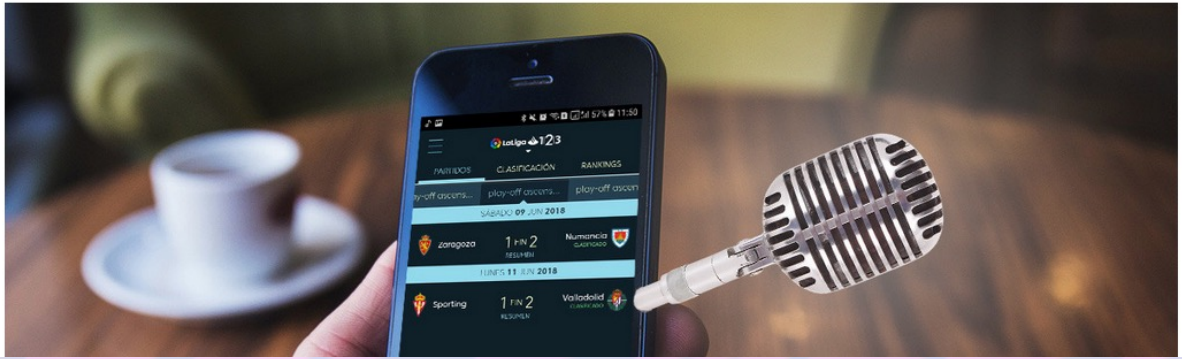
Internet de las c...

- Tu móvil también te escucha

MENÚ NUEVO BUSCAR

Xataka android

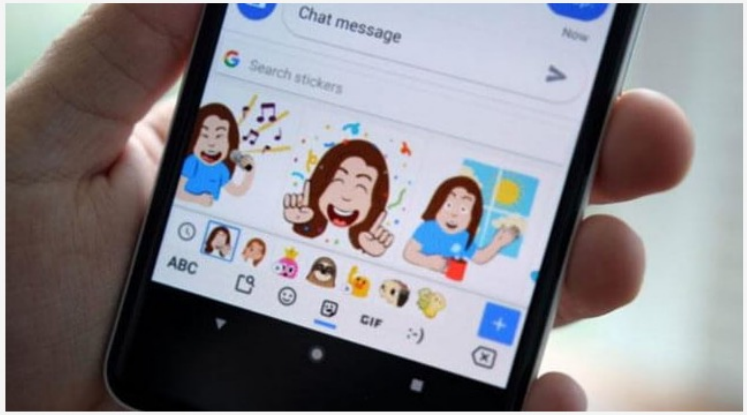
La app oficial de La Liga espía tu micrófono y ubicación para detectar bares que ponen fútbol sin licencia



Internet de las c...

- Hasta el teclado de tu móvil es capaz de „escucharte“

Teclado Gboard de Google recomendará GIFs basándose en tu conversación



A los usuarios del teclado Gboard de Google pronto les resultará mucho más fácil encontrar imágenes GIF y stickers relacionados con sus conversaciones. Google está publicando una actualización de Gboard que incluirá una función que, según el contexto de lo que escribas, te sugerirá imágenes que la inteligencia artificial cree que podrían estar relacionadas con tu conversación.

Pulseras de entrenamiento

- Las pulseras en si mismas no son un problema, el problema es las apps con las que las manejamos, donde acaban nuestros datos y como están estos protegidos
- https://www.strava.com/heatmap

Pulseras de entrenamiento

Pulseras de entrenamiento

Fin

Ruegos y preguntas

https://masto.louzao.network/@louzao