



Ciberdefensa Personal

DESERT SEQ
HACK MEETING

¿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

DESERTSEC
HACKMEETING

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

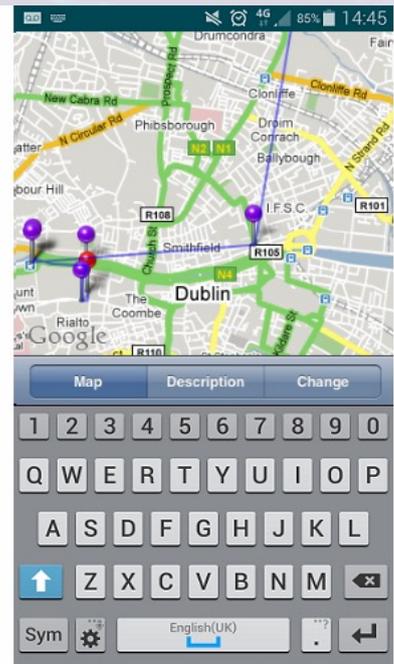
DESERTSEC
HACKMEETING

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 autenticación 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 interceptación 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

DESERTSEQ
HACKMEETING

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

DESERTSEQ
HACKMEETING

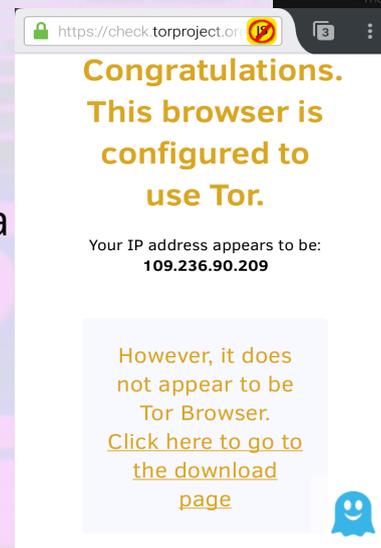
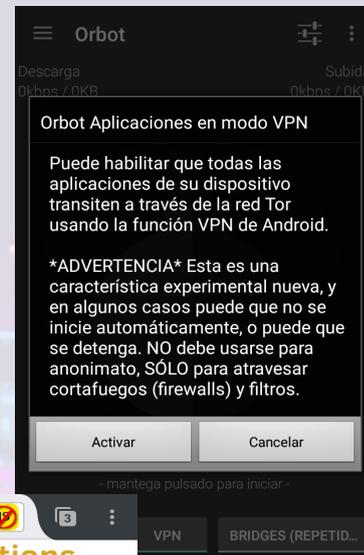
Comunicaciones - TOR

- 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



DEFENSIVE
HACKMEETING

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

GL.iNet ADMIN PANEL

- INTERNET
- WIRELESS
- CLIENTS
- UPGRADE
- FIREWALL
- VPN**
 - OpenVPN Client
 - OpenVPN Server
 - WireGuard Client**
 - WireGuard Server
 - Internet Kill Switch

WireGuard® Client

ⓘ If you enabled VPN but the VPN cannot connect to its server, there will be NO Internet.
When you change server while VPN is connected, VPN will not be leaked.

Status Management

Allow Access Local Network ⓘ

Server GLiNet ▾

IP Address	10.10.10.20
Upload / Download	782.99 KB / 10.82 MB

Disconnect

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 diversos 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.

HACKMEETING

Comunicaciones - DNS



Mi primer perfil ▾

jorge@louzao.net ▾

Instalación

Seguridad

Privacidad

Control parental

Lista negra

Lista blanca

Estadísticas

Registros

Ajustes

Fuentes de inteligencia sobre amenazas

Bloquea los dominios conocidos por distribuir malware, lanzar ataques de phishing y alojar servidores de comando y control utilizando una combinación de las fuentes de inteligencia de amenazas más acreditadas — todas actualizadas en tiempo real.

 Protege contra el phishing COVID-19.

Utilizar las fuentes de inteligencia sobre amenazas

Detección de amenazas basada en la IA BETA

Bloquee millones de amenazas detectadas por nuestra tecnología de inteligencia artificial: un motor de inteligencia artificial patentado diseñado desde cero para DNS con cientos de señales, terabytes de datos de entrenamiento y toma de decisiones en tiempo real.

Activar la detección de amenazas basada en la IA

Navegación Segura de Google

Bloquea los dominios de software malicioso y suplantación de identidad mediante la Navegación Segura de Google — una tecnología que examina miles de millones de URL todos los días en busca de sitios web no seguros. A diferencia de la versión incrustada en algunos navegadores, esta no asocia tu dirección IP pública a amenazas y no permite eludir el bloqueo.

Habilitar la Navegación Segura de Google

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 ▾

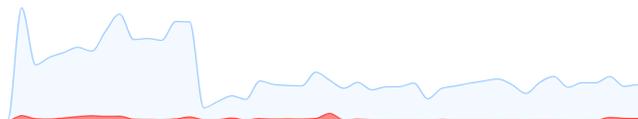
1.066.537
consultas

42.950
consultas bloqueadas

4,03 %
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

GL.iNet ADMIN PANEL

- CLIENTS
- UPGRADE
- FIREWALL
- VPN
- APPLICATIONS
- MORE SETTINGS
 - Admin Password
 - LAN IP
 - Time Zone
 - MAC Clone

Custom DNS Server

DNS Rebinding Attack Protection ?

Override DNS Settings for All Clients ?

DNS over TLS (Cloudflare or NextDNS)

Select DNS Server

NextDNS ID ?

Dnscrypt-Proxy Settings

Manual DNS Server Settings

Comunicaciones



WANT TO
HACK MEETING

Comunicaciones

GL.iNet | Panel De Administración v4.2.1

AdGuard Home Gestiona las Solicitudes de los Clientes ?

Aplicar

34 Consultas DNS

12 Bloquear por Filtros 35.29%

0 Malware/Phishing Bloqueado 0.00%

0 Sitio Web para Adultos Bloqueado 0.00%

Dominios más consultados

en las últimas 24 horas

tags.tiqcdn.com	1	2.94%
www.elsaltodiario.com	1	2.94%
r3.o.lencr.org	1	2.94%
firefox-api-proxy.cdn.mozilla.net	1	2.94%
e00-ue.uecdn.es	1	2.94%

Dominios más bloqueados

en las últimas 24 horas

cdn.permutive.com	1	8.33%
content.zeotap.com	1	8.33%
ib.adnxs.com	1	8.33%
shb.richaudience.com	1	8.33%
bidder.criteo.com	1	8.33%

- INTERNET
- CLIENTES
- VPN
- APLICACIONES
 - Complementos
 - DNS Dinámico
 - GoodCloud
 - Almacenamiento en Red
 - Adguard Home
 - Control Parental
 - ZeroTier
 - Tailscale
- RED
- SISTEMA

Comunicaciones

GL.iNet | Panel De Administración v4.2.1 ? ⏻ ↺ | 🗨️ 🇪🇸

🏠 CLIENTES

🛡️ VPN

📺 APLICACIONES

🌐 RED

🔥 Firewall

🌐 Multi-WAN

🌐 LAN

DNS

🌐 Modo de Red

🌐 IPv6

🌐 Dirección MAC

🌐 Suplantación (spoofing) de puerta de enlace

🌐 IGMP Snooping

🌐 Aceleración por Hardware

DNS Editar Hosts

i Si establece servidores DNS personalizados, todos los nombres de dominio se resolverán a través de los servidores DNS establecidos aquí en lugar del servidor obtenido de las configuraciones de Ethernet, repetidor, móvil, hotspot compartido o de la configuración VPN.

Protección contra Ataques de Reemplazo (Rebind) de DNS

Anular y Reemplazar la Configuración DNS para Todos Clientes

Configuración del Servidor DNS

Modo	DNS encriptado
Tipo de Encriptación	DNS over TLS
Proveedor DNS	NextDNS
NextDNS ID	<input type="text" value="brume2"/>

Aplicar

Comunicaciones

GL.iNet | Panel De Administración v4.2.1

GL.iNet | Panel De Administración v4.2.1

CLIENTES

VPN

APLICACIONES

RED

Firewall

Multi-WAN

LAN

DNS

Modo de Red

IPv6

Dirección MAC

Suplantación (spoofing) de puerta de enlace

IGMP Snooping

Aceleración por Hardware

SISTEMA

DNS

Editar Hosts

Si establece servidores DNS personalizados, todos los nombres de dominio se resolverán a través de los servidores DNS establecidos aquí en lugar del servidor obtenido de las configuraciones de Ethernet, repetidor, móvil, hotspot compartido o de la configuración VPN.

Protección contra Ataques de Reemplazo (Rebind) de DNS

Anular y Reemplazar la Configuración DNS para Todos Clientes

Configuración del Servidor DNS

Modo DNS encriptado

Tipo de Encriptación DNS over HTTPS

Servidores **quad9-doh-ip4-port443-filter-pri**

DNSSEC Filtering No Log

[+ Seleccionar Servidores](#)

Aplicar

Copyright © 2023 GL.iNet. Todos los derechos reservados

Comunicaciones

↓ DOWNLOAD Mbps

425.75

↑ UPLOAD Mbps

374.13

Ping ms ⚡ 10

↓ 23 ↑ 19

GO



Connections

Multi



Adamo

Madrid

[Change Server](#)



Movistar

HOW DOES THE CUSTOMER SERVICE OF MOVISTAR
COMPARE WITH YOUR EXPECTATIONS?

1

2

3

4

5

Much worse

As expected

Much better

By submitting this feedback, you acknowledge and agree that Ookla may use this information to

HACK MEETING

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.

<u>Account</u>	<u>Information</u>
██████████	N/A
██████████	Last connection date: ██████████ Unix millis Account created: ██████████ 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

DESERTSEQ
HACKMEETING

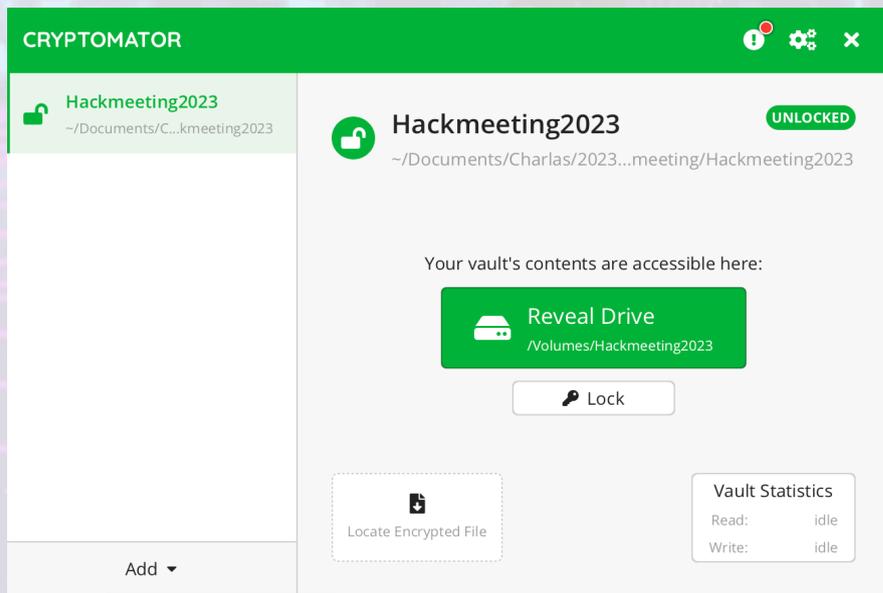
Almacenamiento en la Nube

- 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

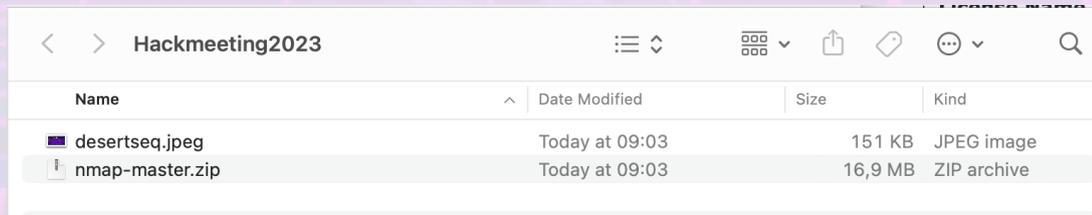
HACKMEETING

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>



The screenshot shows the Cryptomator application window. The title bar is green and contains the text 'CRYPTOMATOR' and three icons (info, settings, close). The main content area is divided into a left sidebar and a main pane. The sidebar shows a green header with a lock icon and the text 'Hackmeeting2023' and the path '~/Documents/C...kmeeting2023'. The main pane shows a green header with a lock icon, the text 'Hackmeeting2023', and a green 'UNLOCKED' badge. Below this, the path '~/Documents/Charlas/2023...meeting/Hackmeeting2023' is shown. The main content area contains the text 'Your vault's contents are accessible here:' followed by a green button with a cloud icon and the text 'Reveal Drive' and the path '/Volumes/Hackmeeting2023'. Below this is a 'Lock' button with a key icon. At the bottom left is a 'Locate Encrypted File' button with a magnifying glass icon. At the bottom right is a 'Vault Statistics' box with the text 'Read: idle' and 'Write: idle'. An 'Add' button is visible at the bottom left of the sidebar.



The screenshot shows a file explorer window titled 'Hackmeeting2023'. The window contains a table with the following columns: Name, Date Modified, Size, and Kind. The table lists two files: 'desertseq.jpeg' and 'nmap-master.zip'.

Name	Date Modified	Size	Kind
desertseq.jpeg	Today at 09:03	151 KB	JPEG image
nmap-master.zip	Today at 09:03	16,9 MB	ZIP archive

Almacenamiento en la Nube

- Esto es lo que vería un atacante

The image shows a cloud storage interface with a file list and a terminal window displaying a hex dump of a file.

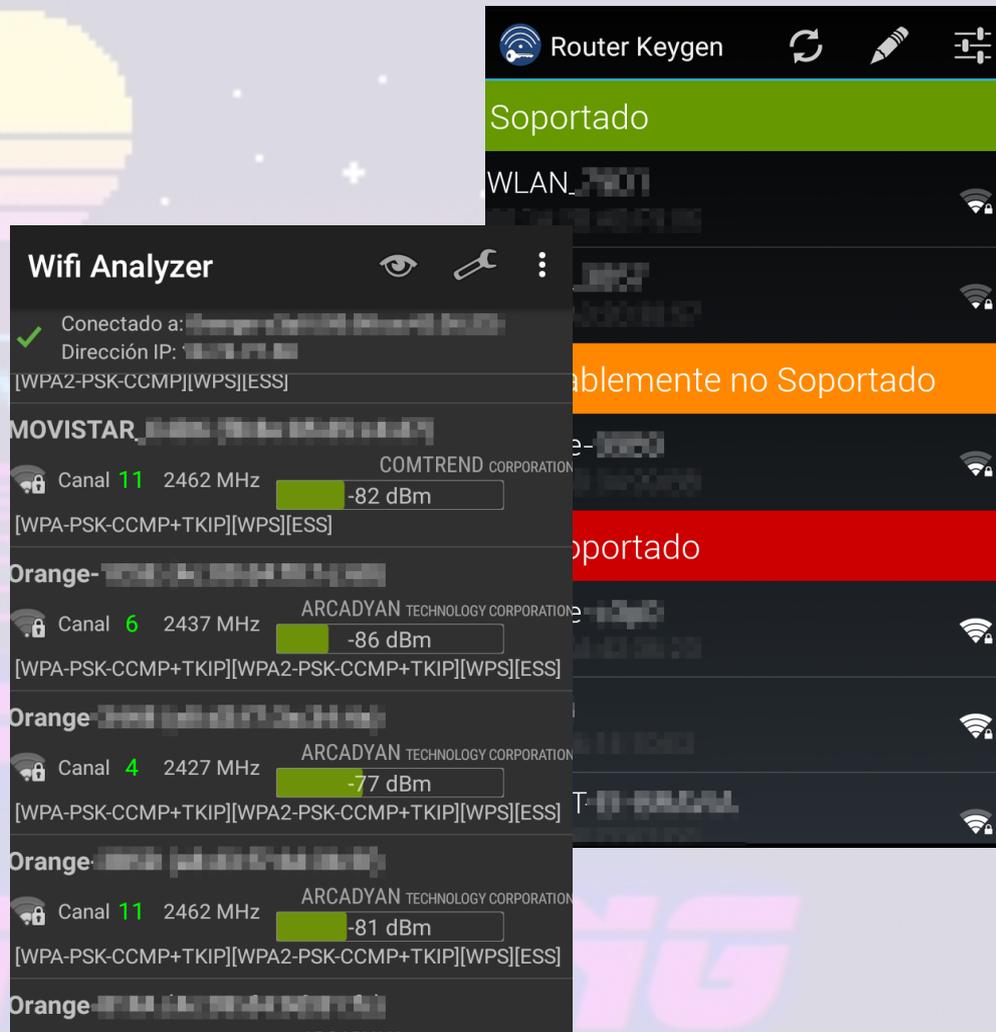
Name	Date Modified	Size	Kind
OMjHQfuDPV_nEin1Eq4zSA-AeqYkVhcsBA==.c9r	Today at 09:01	6 KB	Crypto...ed Data
2an-nw4-rm_9i65T9Ge...9RsWDx8BX1M4T5d.c9r	Today at 09:03	152 KB	Crypto...ed Data
31Q0MniMUhX82KxsJFaJL5sTJ8Ea1AKE-hvV.c9r	Today at 09:00	4 KB	Crypto...ed Data
dirid.c9r	Today at 08:59	68 bytes	Crypto...ed Data
KIXdfvbVv6AYkBXIOApZ...gyl79mYvxjzflI4Q==.c9r	Today at 09:03	16.9 MB	Crypto...ed Data
Pv5cizVNoel0hpQa2Hl9...LtMjxT52WoyQzaug4.c9r	Today at 09:03	4 KB	Crypto...ed Data
TowPEyYBzVoGrV_P8kF...YjZoliwiD1l6-m7zvU=.c9r	Today at 09:03	4 KB	Crypto...ed Data

```
2an-nw4-rm_9i65T9GeXkBAGZ9RsWDx8BX1M4T5d.c9r
"UX_I`jKQ"S>3-" . #/,XD±>`¶@±Iq"G±V"Y70æèLLAC{érÀèie 0$V;Et«8"fiU'Agè±" 'Eöw -"#06«Äfð3igðA&"i6"ä"m"?
rC"Ycè!"rTIE[[]+á·wÁcöïµ}ðfíð|`sæf«áNò`isú_ΣEW[~èIZ,,èaV¶¶; <1_~uàèY0ISäözi
"« ðfi"XK;9" NMð[]i`·#i` [íð?_ðifipæ"w`d`A±#%`=«`Aèg?§=0h92uwoNN>é`&Æ+ðú ñ. 'eÆ.¶0V8`Ü
YiüB»A`lkj}wv±ÉÇ}pÈh`-fib+á`JP`qç¥..á=s~Δ\`úðue}s]~SfiÜÇ"0#>°
É:æY±¶i>ð§Ç±¥Á<óUÉAnúT{^80JBàjÁw@_I`"Ç#DÆ|i/|©0ÚªðÁf°Mfi§rnf¶. °5U}èfÖL`±µ,,áí
rEm<gÜ-Uèc"ÁÇð>`iüðΔÉAvUQ:Éi`°N$ð
ç, Qù« [ð6. Qí¶fKÉ`UD9±0~.) È`Öxt, %^Ij`ñúá}ivüÜxN<9"Înè4`úíÆè`è±1"em*ui*M`®Xµ"Áç/
'ig, u`snÜÀè±yæ3QC
X`_sf#
: ç! l8ºfVfi"W`À-mCİL,,1eé=qZ
K&±.Cf,T1Éfh`ÍKuS0±f*. 5UE="§)ÜG0ú+, ðt`ÍÜ`rQ4ú Í3zñfiÈ«xi¶i`/ÉÁ. ]70±èiA+i@Ä09R
ç±. j`πj±, θi|Ti«æE!ð±T
i`°...0dl
±It`H">ç§qÇ, £n. ø`Ñiàl, @:, ;jB, }πÜ=äðæBtÜ{É±±IiðQoð£èLÁAZ"fiF8USUÉ¶Á5A
: x)2«,,0Íðíä
DÄñi...ñ«SÝøtaðIæçPòV$
üiIEùY m`ç<F|/ÁèQð<ªÄ Úhà+dçf`QP ^`Ä±ið/@·}iIQ^£ºPñÑ
Ó`ÈuráÄ±>SÄL`Ad(;
Y±8`Σufñ0Ü~ft¶¶]7f¶|", ©càYÄ)PÄ`}4±, ðk<b-nqcc+Ä/7º9M`úsÄZΔ+kqæ±æÉ ©. BÖ/Èñ¥`8wv`ð00£|~B.
i,, "ú`icjü+ì+«J`¶`Á
{`>Va&g*EL3@è/IG
UF#l®, é=I¶sið. *. uIQY>. ìh. `f¥çñ`~=: "uèuìif/naz±4aA`p«ÇAUH2a~. , A1`°ÜçhtL0` [iÄ6, §
02i0>«Ü. #%ß«Uo«"óqnF+WM0ÉäYÇ
ÚÁ):&ü`4-E); f#0ð`5*é `E`Eù
úcy<«U@F k0d`à, h. fi`«5*KΣI±â7}$P. i4fQ7= Ü(, "CJüèðN0±"x
0yΣ¶¶«+è0·YèàÄ`b07/éÉ}<è~`D~</ð|e!bì`BÌºQFj`i_ÍA~wä, à`Áv,,+ª¶`tíiids`±IΣiC1, xB, tÜÜ. +ó
ó, äf; rÉ
```

DESE
HACKMEETING

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

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

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:...

2023-09-30T06:41:21.727170

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

iPad 17:05 100%

PineAP

Tracking

Logging

Reporting

Networking

Configuration

Advanced

Help

Timestamp	Event	MAC	SSID
May 6 15:49:21	Probe Request	d47b14547f121f	SUPER Engineer Network V5 TURBO
May 6 15:49:27	Probe Request	007b3254112a1a	Tesla
May 6 15:49:53	Probe Request	04552305122212	TropicThunder
May 6 15:49:56	Probe Request	92322212121212	Sarigar-5G
May 6 15:49:58	Probe Request	007b3254112a1a	Tesla
May 6 15:49:59	Probe Request	f8322212121212	Sarigar-5G
May 6 15:49:59	Probe Request	d47b14547f121f	SUPER Engineer Network V5 TURBO
May 6 15:49:59	Probe Request	d47b14547f121f	Sanmi
May 6 15:50:10	Probe Request	f8322212121212	Sarigar-5G
May 6 15:50:10	Probe Request	007b3254112a1a	Tesla
May 6 15:50:15	Probe Request	92322212121212	Sarigar-5G
May 6 15:52:52	Probe Request	d47b14547f121f	Sanmi II
May 6 15:53:59	Probe Request	d47b14547f121f	SUPER Engineer Network V5 TURBO
May 6 15:53:59	Probe Request	d47b14547f121f	Sanmi
May 6 15:54:26	Probe Request	347b3254112a1a	Tesla
May 6 15:54:51	Probe Request	04552305122212	TropicThunder
May 6 15:55:14	Probe Request	d47b14547f121f	SUPER Engineer Network V5 TURBO
May 6 15:55:14	Probe Request	d47b14547f121f	Sanmi
May 6 15:55:14	Probe Request	d47b14547f121f	MOVISTAR_987

Redes WiFi

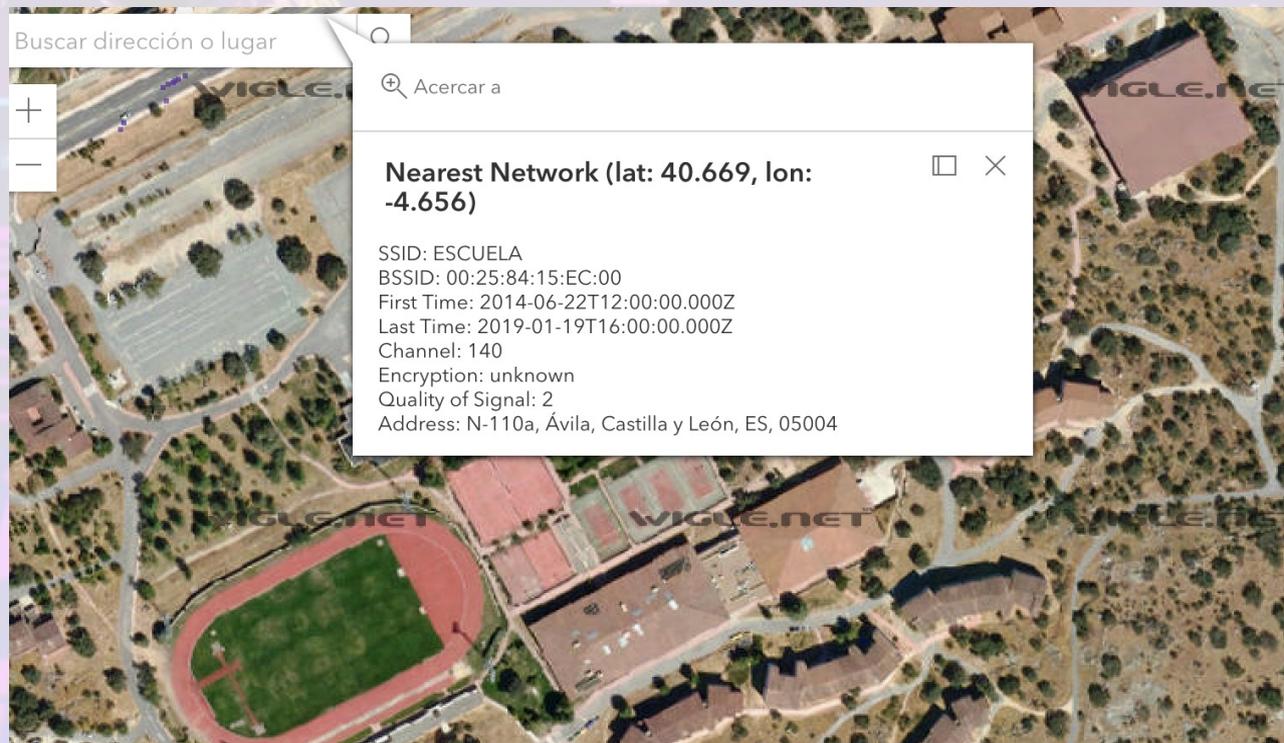
The screenshot shows the 'Servicios' (Services) page for a WiFi network named 'Morla'. The status bar at the top indicates 'iPad', signal strength, time '17:13', and '100%' battery. The network name 'Morla' is shown with a back arrow and a refresh icon. Below the network name, it says 'Generic' and '6 servicios hace 32 segundos'. The list of services includes:

Port	Protocol	Service Name	Action
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	

The bottom dock contains icons for 'Dispositivos', 'Mis redes', 'Herramientas', and 'Fingbox'.

Redes WiFi

- <https://wigo.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.

DESERTSEQ
HACKMEETING



Mandos



DE
HAC

EQ
TING

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.

DESERTSEQ
HACKMEETING



NFC



DE
HAC



DE
TING

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.

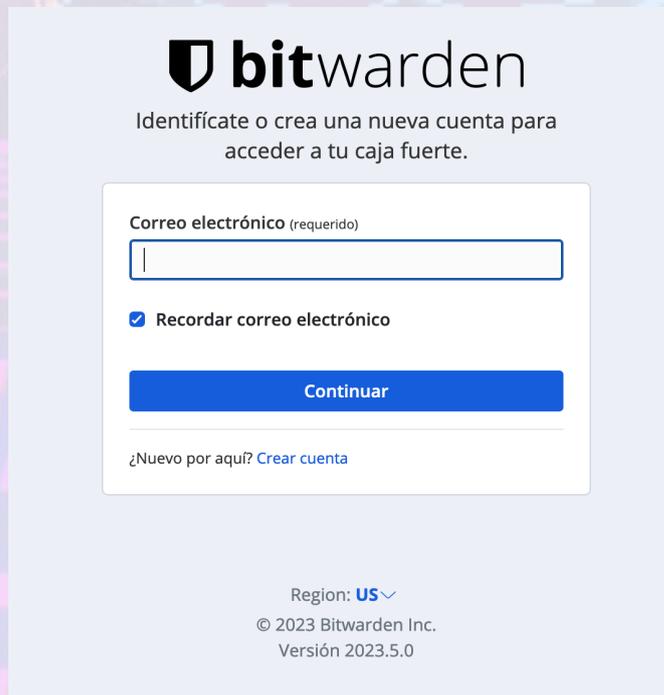
Servicios de Email

- 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

DESERTSEQ
HACKMEETING

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...



The image shows a screenshot of the Bitwarden login page. At the top, the Bitwarden logo is displayed, consisting of a shield icon and the text 'bitwarden'. Below the logo, the text reads 'Identifícate o crea una nueva cuenta para acceder a tu caja fuerte.' (Log in or create a new account to access your safe). The main form area contains a text input field for the email address, labeled 'Correo electrónico (requerido)'. Below the input field is a checkbox labeled 'Recordar correo electrónico' which is checked. A blue 'Continuar' button is positioned below the checkbox. At the bottom of the form, there is a link that says '¿Nuevo por aquí? [Crear cuenta](#)'. Below the form, the page indicates the region is 'US' with a dropdown arrow, and includes the copyright information '© 2023 Bitwarden Inc.' and the version number 'Versión 2023.5.0'.

bitwarden

Identifícate o crea una nueva cuenta para acceder a tu caja fuerte.

Correo electrónico (requerido)

Recordar correo electrónico

[Continuar](#)

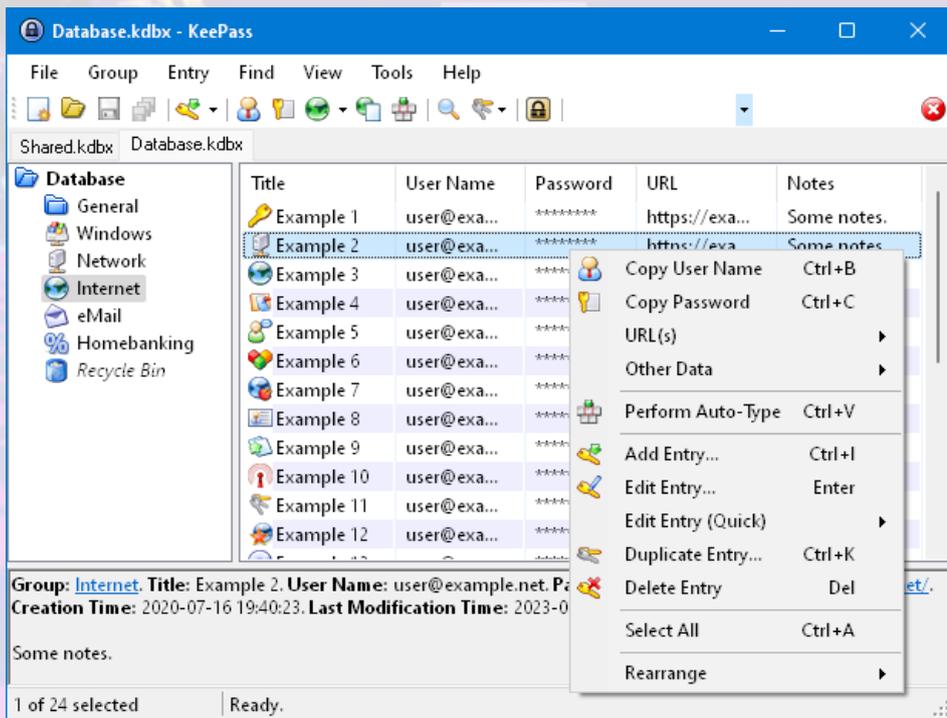
¿Nuevo por aquí? [Crear cuenta](#)

Region: **US** ▾

© 2023 Bitwarden Inc.
Versión 2023.5.0

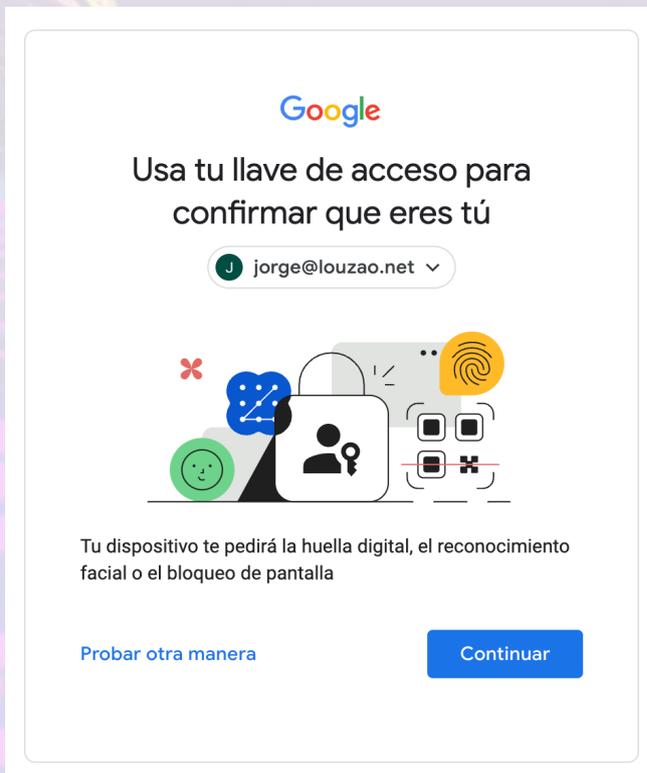
Gestión de Contraseñas

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



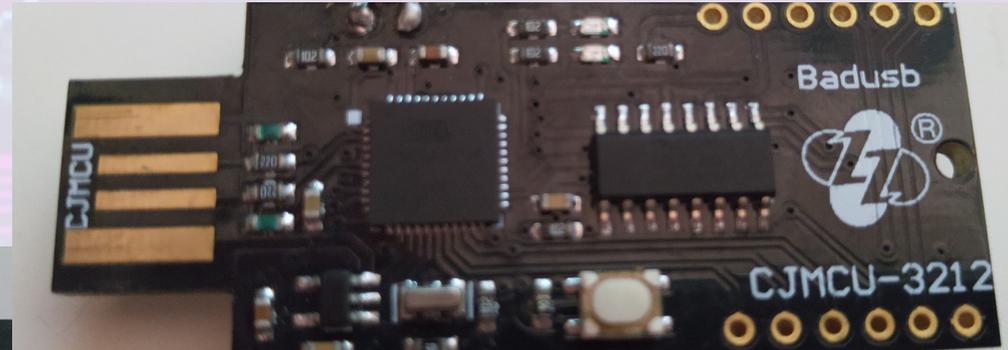
Gestión de Contraseñas

- 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/>

DESERTSEQ
HACKMEETING

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

DESERTSEQ
HACKMEETING

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

DESERTSEQ
HACKMEETING

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/>

DESERTSEQ
HACKMEETING

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



The screenshot shows the La Liga app interface. At the top, there is a navigation bar with a menu icon (MENÚ), a 'NUEVO' button, a search icon (BUSCAR), and the 'LaLiga android' logo. Below the navigation bar, a news article is displayed with the headline: 'La app oficial de La Liga espía tu micrófono y ubicación para detectar bares que ponen fútbol sin licencia'. Underneath the headline are social media sharing icons for Facebook, Twitter, and Email. The main image of the article shows a hand holding a smartphone displaying the La Liga app's 'CLASIFICACIÓN' (standings) screen. The screen shows match results for 'JUEVES 10 JUN 2018' and 'VIERNES 11 JUN 2018'. A vintage-style microphone is positioned in front of the phone, symbolizing the article's claim that the app listens to the microphone.

MENÚ NUEVO BUSCAR LaLiga android

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

f t e

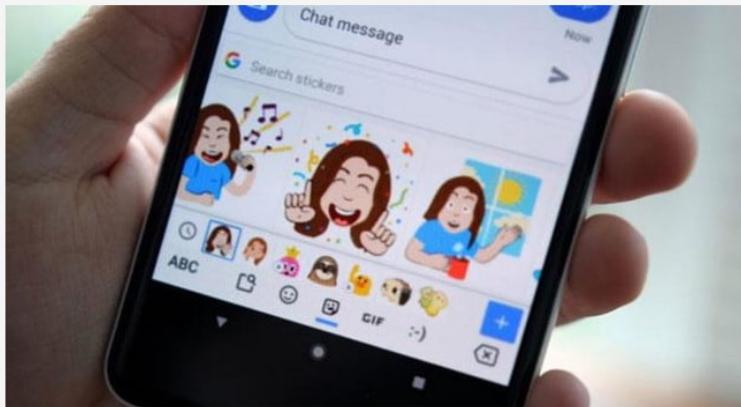
CLASIFICACIÓN

Equipo	Puntos	Partidos Jugados	Partidos Ganados	Partidos Empatados	Partidos Perdidos
Zaragoza	1	2	0	1	1
Murcia	2	2	1	0	1
Sporting	1	2	0	1	1
Valladolid	2	2	1	0	1

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>

DESERTSEQ
HACKMEETING

Pulseras de entrenamiento



HACKMEETING

Pulseras de entrenamiento



HACKMEETING



Fin

Ruegos y preguntas

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

DESERTISEQ
HACKMEETING