La Ciberseguridad como Instrumento de Mejora del Negocio en la Pyme.

✓ ***Soluciones Prácticas***

La ciberseguridad como activo indispensable en el nuevo escenario de conectividad permanente

FRANCISCO ANDRADES GALINDO

- ***Formación destacadas:***
  - ✓ **Tesis doctoral (UMA) sobre internet como territorio de conflicto**
  - ✓ **Postgrado (UDIMA) en Informática Forense**

- ***Experiencia profesional :***
  - ✓ **18 años en la administración pública como Coordinador de Informática (Diputación de Málaga y sus organismos)**
  - ✓ **Ultima experiencia como Experto en *eAdministración* y certificaciones digitales**
  - ✓ **Colaborador en medios tecnológicos como divulgador:**
    - ❖ ***Nación Red*** **(ahora *Genbeta*) o *Eldiario.es* entre otros**

www.andradesfran.com

soy@andradesfran.com

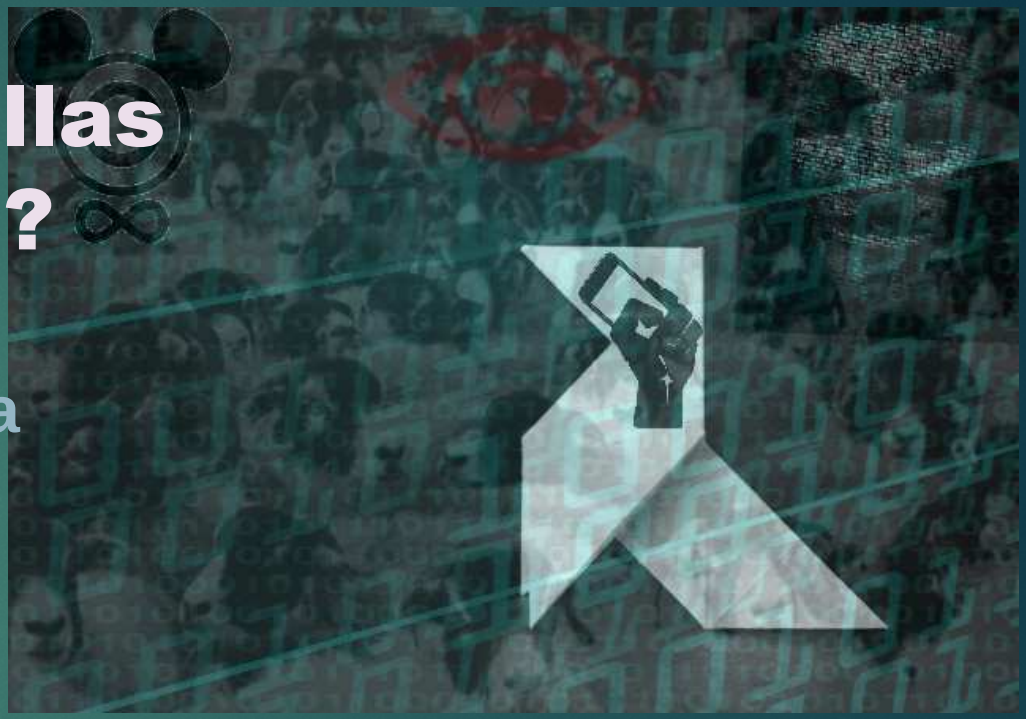
Canales con actualizaciones de contenidos:

https://telegram.me/plectica
https://telegram.me/hackingtools

https://es.linkedin.com/in/andradesfran

Referencia internacional como investigador:
http://orcid.org/0000-0001-8218-4250

¿Hay Soluciones sencillas a problemas complejos?



Inspirado en **Glen Mann la idea de la *pléctica* es una forma de explicarnos y buscar soluciones concretas**

La evolución del delito en la red y la dependencia tecnológica de factores externos (nube, software restrictivo,…)

Diversos escenarios de desprotección con métodos similares:

1) La captación de datos privados por parte de grandes de Internet
2) El espionaje masivo ciudadano
3) El acceso de delincuentes en la red

V. Cerf

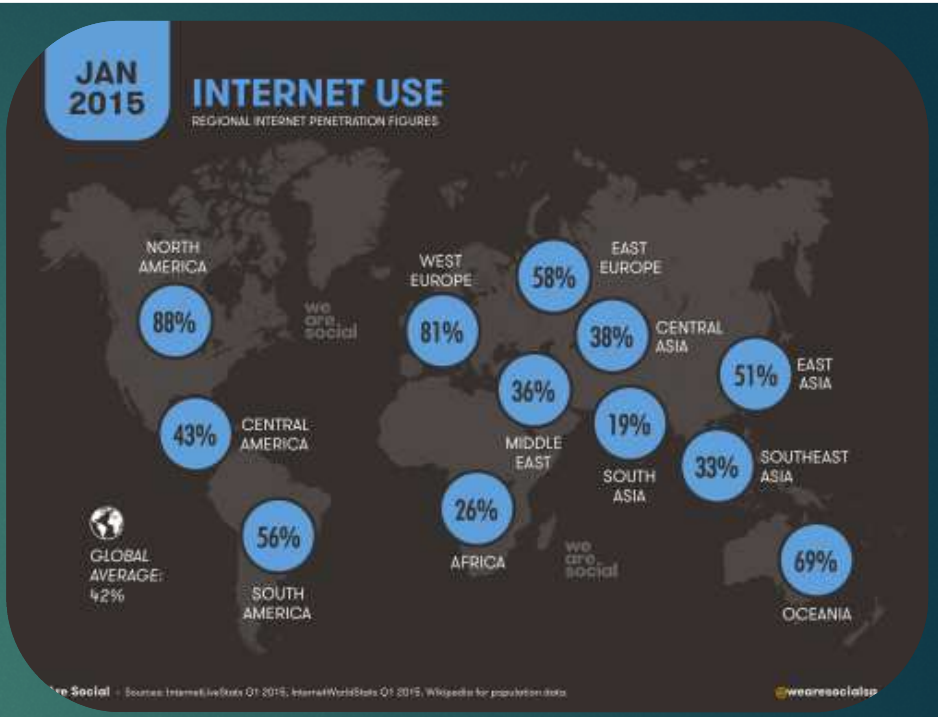
La red fue creada para funcionar incluso en condiciones muy limitadas, no para que fuera segura

El incremento del uso de internet

→ Perdida hegemonía TV y medios tradicionales.

Penetración de Internet 2015

- ✓ **3.010.000 personas**. **42% de la población mundial**
- ✓ **1.685.000** usuarios en cuentas en redes sociales (23%)
- ✓ uso de dispositivos móviles 51% de la población
- ✓ Europa -El norte de América- 80% Usa Internet



España

- ✓ **50 millones de conexiones móviles (más que población)**
- ✓ **conexión redes sociales 38% (con móvil). 47% (general)**
- ✓ **77% de la Población es usuaria activa de Internet.**
- ✓ **Servicios más usados:**
  - o **WhatsApp 42%**
  - o **Facebook 33%**
  - o **Twitter 17%**
  - o **Resto no llega al 10%**

1. Cómo nos espían las grandes corporaciones de la red y porqué no podemos ceder nuestros datos

There is NO CLOUD, just

other people's computers

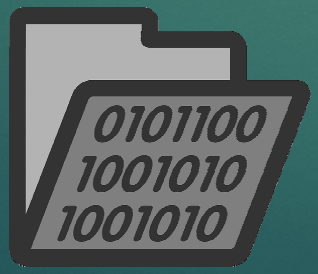
fsfe.org

La privacidad frente al Big Data

EL DATO= Elemento esencial del negocio

- Manejo de complejidad
- Base de muchos negocios de la red de nuestro tiempo y empresas de la Nueva Economía

Estados, empresas y delincuentes convergen en la compulsiva adquisición de datos personales



Unas redes sociales que son sociedades privadas

- ✓ **Facebook** 1.366.000 usuarios registrados
- ✓ WhatsApp, WheChat y Skype
- ✓ **Twitter**, con 560 millones de cuentas
- ✓ **Instagram** 150 millones

Todas redes buscan hegemonía y tiempos de permanencia de usuarios.

→ **Integración servicios (NO salga de su "ecosistema")**

→ **Formar un Big Data completo (Publicidad Orientada)**

- ➢ Al arbitrio de **políticas de empresas** (*suspensión de cuentas y censura*)
- ➢ **Auditoría constante**. Empleo de **datos personales. Privacidad- Seguridad**
- ➢ Indefensión ciudadana. Necesidad toma control del medio

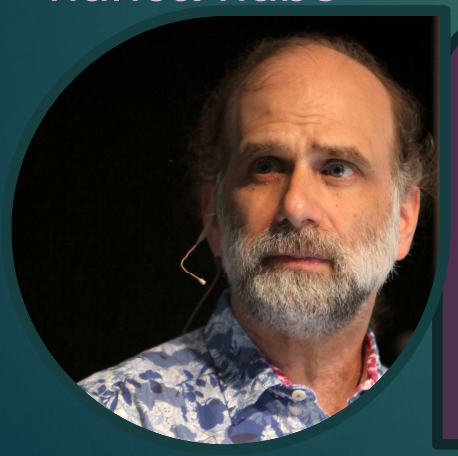
La guerra por el DATO PERSONAL

una CONVERGENCIA de intereses:

- ✓ Los que los **recogen**
- ✓ Los que los **usan**
- ✓ Los que **hacen negocio** con ellos

La trampa de los servicios ***gratuitos***

- ➢ Capacidad de fiscalización como nunca hubo



La guerra por los datos personales la libran empresas, gobiernos y cibercriminales *contra la ciudadanía*

Bruce Shneier

La Clave está en adquirir un **perfil de usuario** preciso

Identificadores web:

- Google 43%

- Facebook 46%

Volumen y cantidad de datos disponibles

A cambio de la comodidad (la "usabilidad") hemos cedido buena parte de nuestra privacidad

L. Lessing.

➢Perfil personal preciso

80’-90’ Wal-Mart

- **la mayor base de datos personales del mundo**

Ej. El caso de Malte Spitz

→ Denuncia a *Deutsche Telekom*

- ✓ ***35,830 líneas de código*** sobre 6 meses de su actividad con su móvil, al detalle, por minutos, localización etc...

Sistemas de "*asistencia a usuario*" de las cuatro grandes

- ***Google Now, Cortana, Siri, Facebook M***
- **La base de su uso es la recolección de datos personales**
- **Colaboración con NSA (puertas traseras)**

Alphabet
Apple
Microsoft
facebook

Disputa de las grandes de internet por el tiempo de permanencia de usuarios

- **Facebook**--- 13% del uso *(Instagram y WhatsApp*)
- **Google**--- 12% (*YouTube, Gmail, Blogger*)

EL NEGOCIO DE GOOGLE:

- ✓ **Buscador y Pagerank**
- ✓ **Adwords y Adsense**

¿Podemos Degooglizarnos?

Múltiples casos de espionaje empresarial y conductas abusivas:

Lenovo

Inclusión de BloatWare (software Basura) en sus equipos

Google

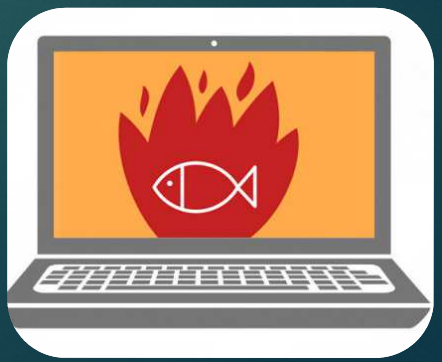
Incluir de forma obligada sus aplicaciones e Android

Apple

Forzar empleo de aplicaciones y entornos de datos propios

Samsung

Inclusión de BloatWare imborrable en sus terminales



2. También espían estados y organismos delegados no siempre transparentes

Internet es un centro de Poder Global

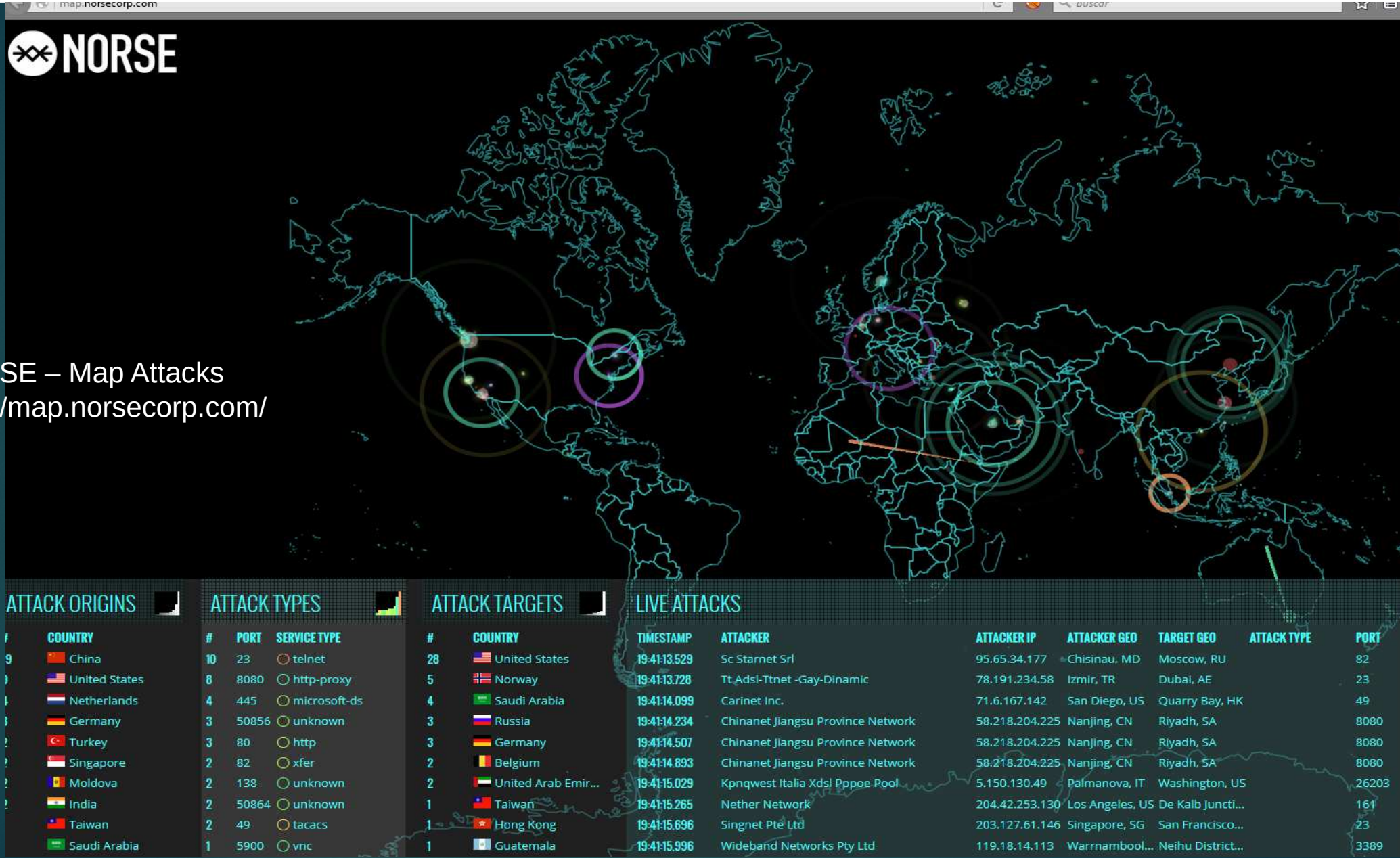
- Nuevo escenario de disputa.
  - 1/3 del trafico 2015 fueron ataques DDoS (responsables Kali Linux en la *Defcon* de las Vegas)

Tres contextos:

1) **Estados *Enemigos* (Hacking estatal)**
2) **Hacking delictivo**
3) **Terrorismo**

Ciberguerra y cibercrimen
Emparentados en métodos

NORSE – Map Attacks
http://map.norsecorp.com/



El impulso de la vigilancia mundial

→Patriot Act desde 11-S

- Antes existían Echelon, o el programa TIA (Total Information Awareness- Vigilancia Informática Total)

→ **Homeland Security Act, de 2003**

Poner en **suspenso derechos individuales**

Recogida general de *datos biométricos*

FBI -- NGI (Next Generation Identification)

- *reconocimiento facial instantáneo a 200 metros*
- *reconocimiento del iris a tres metros*

El espionaje masivo ciudadano: Un Gran Hermano global y privado

→ **Revelaciones de WikiLeaks y Edward Snowden**

- **Nivel de vigilancia**
- **Integración de Bases de Datos biométricos**

Papel de las grandes empresas de la Red

Filtraciones hacen público grandes sistemas de espionaje

- ***PRISM, XKeyscore, Boundless Informant***

UE

- **Shengen**
  - Despliega prerrogativas más allá del control fronterizo
- directiva de **retención de datos**
- legislaciones de protección de **derechos de autor**:
  - fiscalizan conexión usuarios

- **INDECT**
  - ✓ **rastreo de la videovigilancia urbana**
  - ✓ **control y catalogación de conductas en la red**

OSEMINTI

- ✓ **informaciones de vigilancia masiva**
- ✓ **Intercepción completa de comunicaciones**

El espionaje español

- **SITEL**

Caso **Hacking Team**. Compra de sistemas ilegítimos de espionaje

Proceso de Privatización de la seguridad

Contratistas privados → **Cesión de datos** ciudadanos

El auge de reglamentaciones sobre uso de datos personales:

→ **Sistema de Información Shenguen** 1990

→ **Eurodac** 2003

→ **VIS**, Sistema de Información sobre Visados 2009

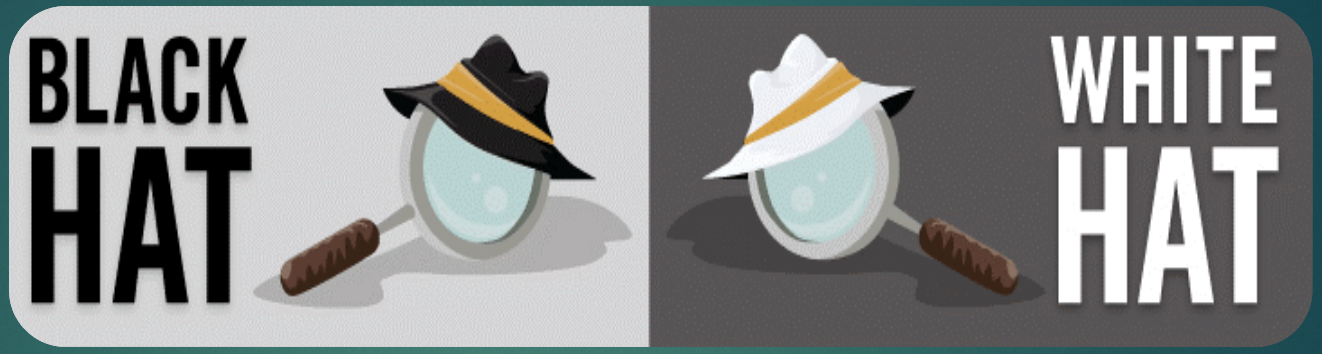
Directiva europea 2006/24/CE, incorpora aspectos básicos de la **Patriot Act**

- **Retención de datos**, ej España, *Ley sobre Conservación de datos de las Comunicaciones Electrónicas 2007.*

Privacy Shield*, El reemplazo de *Safe Harbor
Cesión de datos personales EEUU- UE

3. También la ciberdelincuencia lo tiene cada vez mas fácil

Delitos y cibercrimen



El mercado de hacking- Facilidad y rentabilidad.

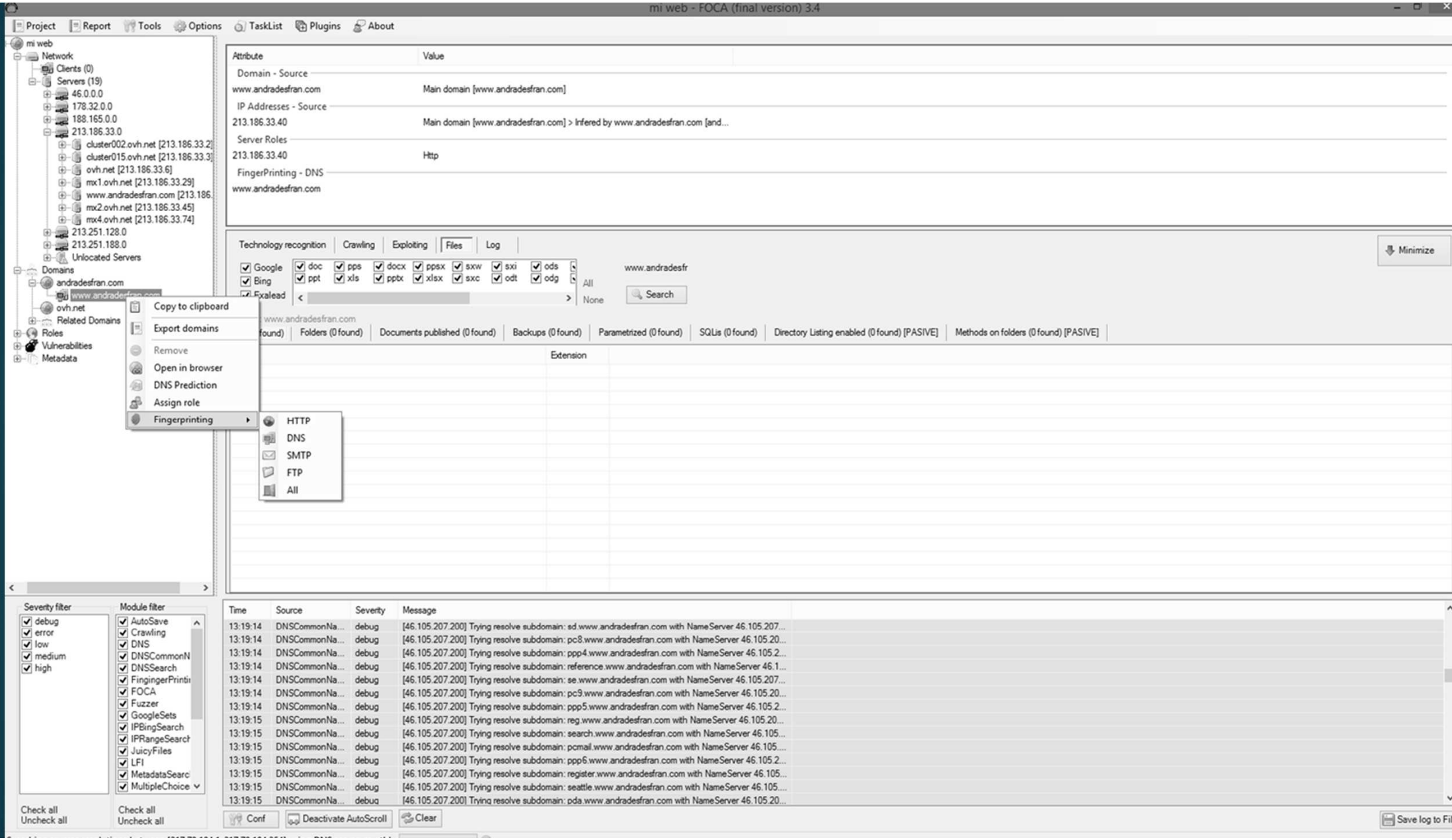
Transición **de reto intelectual y lúdico a negocio.**

Rusia, China, EEUU y América Latina

✓ Hasta 2010, el hacking no sería delito según el código penal español

Facilidad ***explotación de vulnerabilidades*** de sistemas:

- ✓ **Herramientas OSINT** (Open Source Inteligence), búsqueda de Información y recolección de datos.
- ✓ Incremento en las formas de **adquisición de datos**
- ✓ **Herramientas y procedimientos de explotación estandarizados**
  - APT- ataques persistentes
  - Ransonware- Secuestro y cifrado de datos
  - Suplantación de identidad o la redirección de páginas web


mi web - FOCA (final version) 3.4
Project
Report
Tools
Options
TaskList
Plugins
About
mi web
Network
Clients (0)
Servers (19)
46.0.0.0
178.32.0.0
188.165.0.0
213.186.33.0
cluster002.ovh.net [213.186.33.2]
cluster015.ovh.net [213.186.33.3]
ovh.net [213.186.33.6]
mx1.ovh.net [213.186.33.29]
www.andradesfran.com [213.186.
mx2.ovh.net [213.186.33.45]
mx4.ovh.net [213.186.33.74]
213.251.128.0
213.251.188.0
Unlocated Servers
Domains
andradesfran.com
www.andradesfran.com
ovh.net
Related Domains
Roles
Vulnerabilities
Metadata
Copy to clipboard
Export domains
Remove
Open in browser
DNS Prediction
Assign role
Fingerprinting
HTTP
DNS
SMTP
FTP
All
Attribute
Value
Domain - Source
www.andradesfran.com
Main domain [www.andradesfran.com]
IP Addresses - Source
213.186.33.40
Main domain [www.andradesfran.com] > Infered by www.andradesfran.com [and...
Server Roles
213.186.33.40
Http
FingerPrinting - DNS
www.andradesfran.com
Technology recognition
Crawling
Exploiting
Files
Log
Minimize
Google
Bing
Exalead
doc
pps
docx
ppsx
sxw
sxi
ods
ppt
xls
pptx
xlsx
sxc
odt
odg
All
None
www.andradesfr
Search
www.andradesfran.com
found)
Folders (0 found)
Documents published (0 found)
Backups (0 found)
Parametrized (0 found)
SQLis (0 found)
Directory Listing enabled (0 found) [PASIVE]
Methods on folders (0 found) [PASIVE]
Extension
Severity filter
debug
error
low
medium
high
Check all
Uncheck all
Module filter
AutoSave
Crawling
DNS
DNSCommonN
DNSSearch
FingingerPrinti
FOCA
Fuzzer
GoogleSets
IPBingSearch
IPRangeSearch
JuicyFiles
LFI
MetadataSearc
MultipleChoice
Check all
Uncheck all
Time
Source
Severity
Message
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: sd.www.andradesfran.com with NameServer 46.105.207...
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: pc8.www.andradesfran.com with NameServer 46.105.20...
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: ppp4.www.andradesfran.com with NameServer 46.105.2...
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: reference.www.andradesfran.com with NameServer 46.1...
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: se.www.andradesfran.com with NameServer 46.105.207...
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: pc9.www.andradesfran.com with NameServer 46.105.20...
13:19:14 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: ppp5.www.andradesfran.com with NameServer 46.105.2...
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: reg.www.andradesfran.com with NameServer 46.105.20...
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: search.www.andradesfran.com with NameServer 46.105...
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: pcmail.www.andradesfran.com with NameServer 46.105....
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: ppp6.www.andradesfran.com with NameServer 46.105.2...
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: register.www.andradesfran.com with NameServer 46.105...
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: seattle.www.andradesfran.com with NameServer 46.105....
13:19:15 DNSCommonNa... debug [46.105.207.200] Trying resolve subdomain: pda.www.andradesfran.com with NameServer 46.105.20...
Conf
Deactivate AutoScroll
Clear
Save log to File


KEEP
CALM
AND
RESET YOUR
ROUTER

Servicios difíciles de intervenir:

Por NSA. (Informes filtrados ***a Der Spiegel)***

- **PGP** (*cifrado de correos*) muy complejo
- ***VPN*** (*redes privadas virtuales*). Casi imposible de intervenir si usa cifrados altos
- ***Cifrado de archivos***. *Ejemplo de Truecrypt*
- ***Cambio de las DNS***. *Escapa al control de operadoras y empresas.*
- ***TOR***. *Si es empleado con precaución y con nodos confiables.*

La guerra del cifrado

Amy Goodman, de la ONG Democracy Now

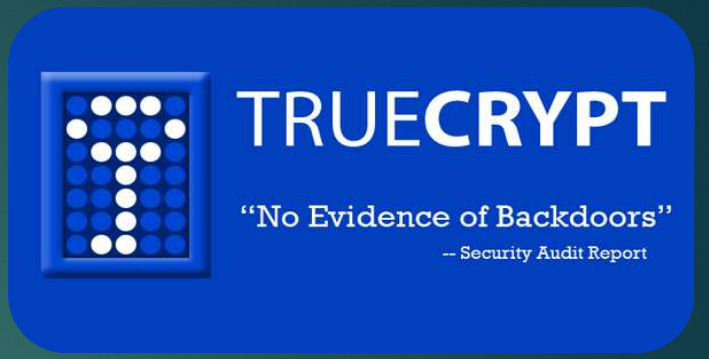
- ✓ Debate en el senado EEUU sobre la obligatoriedad de permitir saltarse el cifrado de empresas estadounidenses, traído por el FBI.
- ✓ Presiones de gobiernos a empresas que manejan datos cifrados

Lavabit

- Ofrecía correo cifrado (lo usaba Snowden)
- FBI obliga a **espiar tráfico** y luego a revelar claves cifrado
- La empresa cierra ante las presiones

Silenc Circle

- *Phil Zimmermann* inventor de **PGP**.
- Emigra con su empresa a Suiza para ofrecer Blackphone y Silent text



TrueCrypt

- ➢ **Utilidad de cifrado más extendida**. Cierre **repentino** y anuncio tipo ***warrant canary*** (revelación sutil)
- ➢ ***Open Crypto Audit Project***. Hizo auditoria 2015. *En Windows más débil pero confiable*
- ➢ ***Pure Privacy. Buscar alternativas:***
  - ✓ ***VeraCrypt y CipherShed***

Comisión de Derechos Humanos de las Naciones Unidas

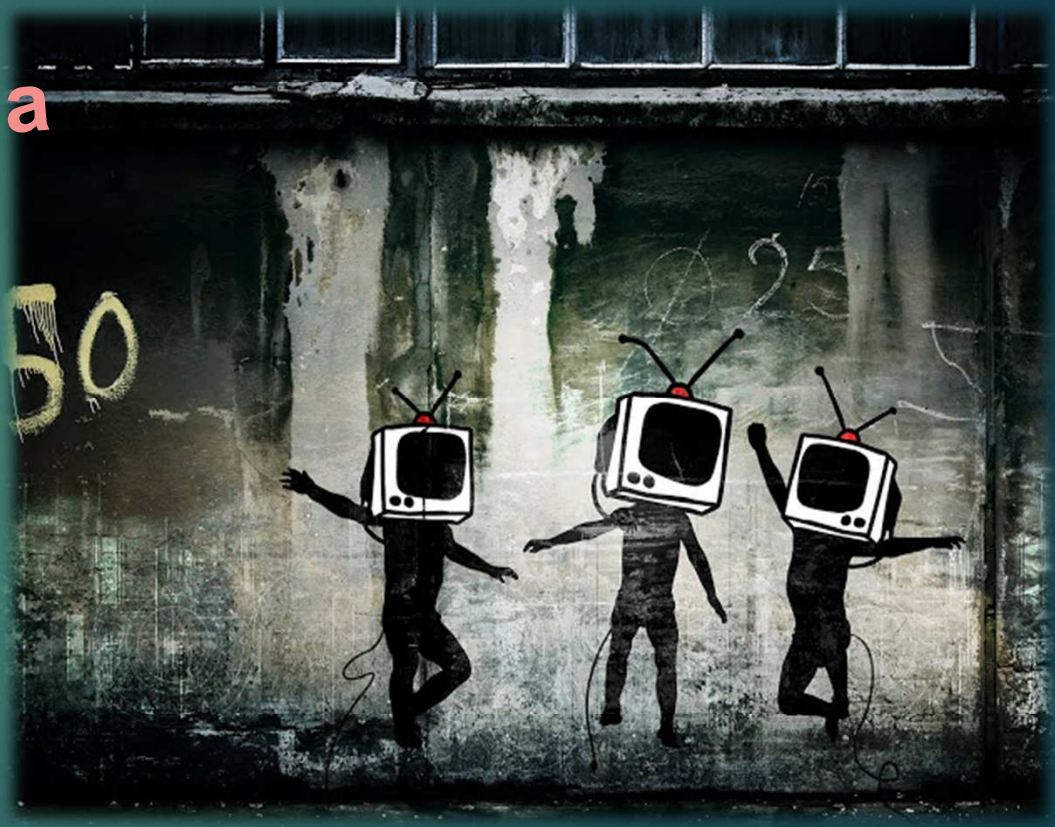
Informe mayo 2015.

- ➢ ***Derecho al cifrado parte del derecho a la intimidad y la libre expresión***

Las formas de espionaje y las técnicas de evasión tienen desarrollos paralelos

¿Cómo son de seguras nuestras empresas en la actualidad?

¿Somos objetivo probable de ataques?



"Tormenta perfecta"

Confluencia de circunstancias han propiciado el auge incidentes.

- ✓ **Dependencia tecnológica** (software privativo, restringido)
- ✓ **Crisis y recortes** en todos los aspectos públicos
- ✓ **Maduración del hacking** (publicación contantes de cvc)
- ✓ **BYOD y extensión de dispositivos** con acceso

✓Capacidad defensiva no ha avanzado tanto como la capacidad de espionaje.

Vías mas usuales de infección e intrusión en sistemas:

- **Correos electrónicos con enlaces a malware**
    - ***Adjuntos y enlaces***
- **Páginas web con enlaces falsos y/o maliciosos**
    - **Navegadores con java, Flash, web RTC**
    - **No actualizados**
    - **Sin bloqueos ni seguridad**
- **Archivos descargados por redes P2P *sin firma***
- **BYOD**

Fallos mas explotados:

- Firmas de antivirus no actualizadas
- Sistemas antiguos no actualizados (no hardering)
- Redes desatendidas
- Wifi no bastionado. Implementaciones defectuosas (WPS, WEP, WPA…)
- Mala gestión de contraseñas
- Conexiones no cifradas ni auditadas
- Falta de cifrado. Zonas DMZ, delimitación de redes…
- Páginas web compartiendo entornos con equipos de oficina
- Páginas desactualizadas. No vigilancia de Plugins, CMS…

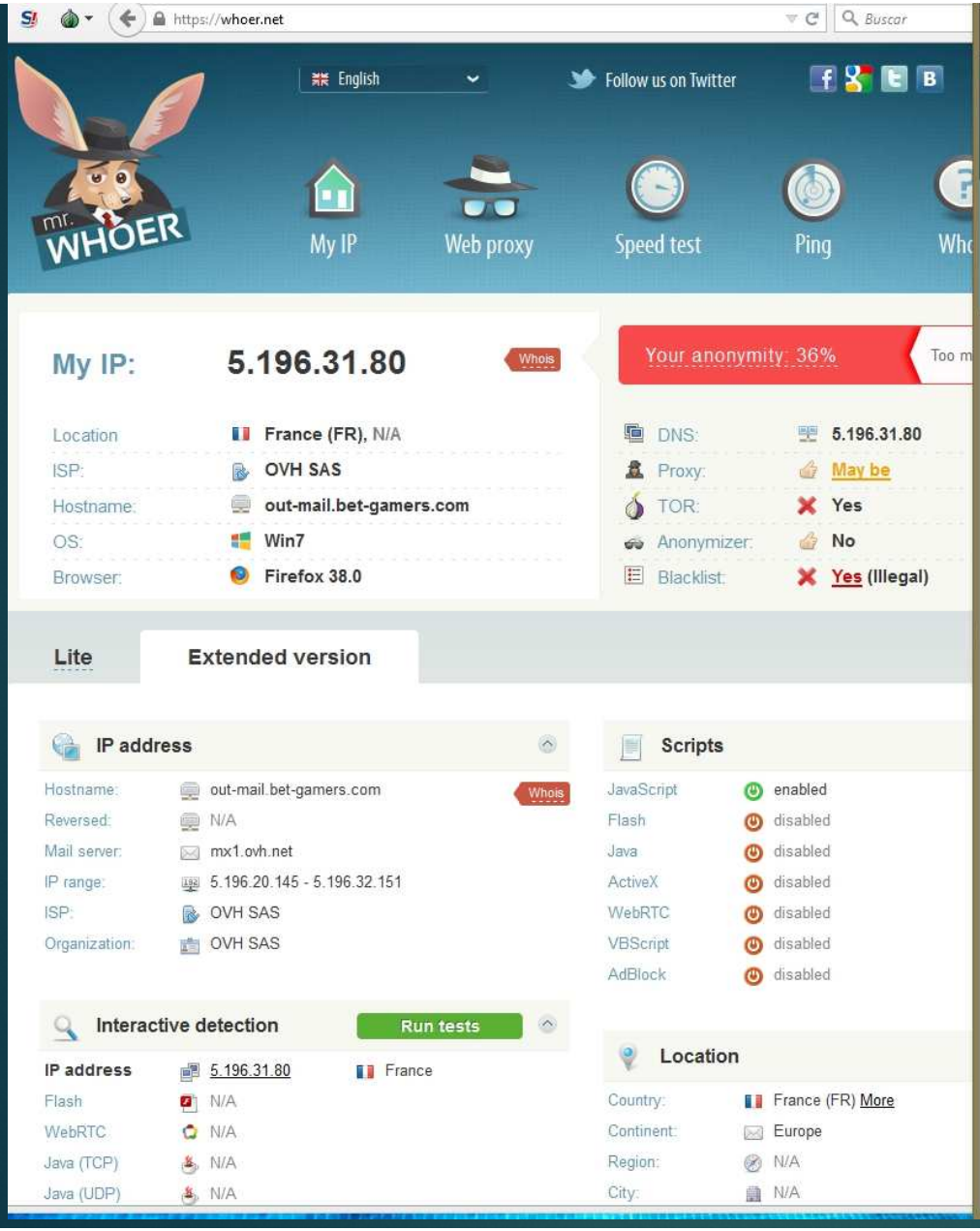
El gran error : NO TENER COPIAS DE SEGURIDAD

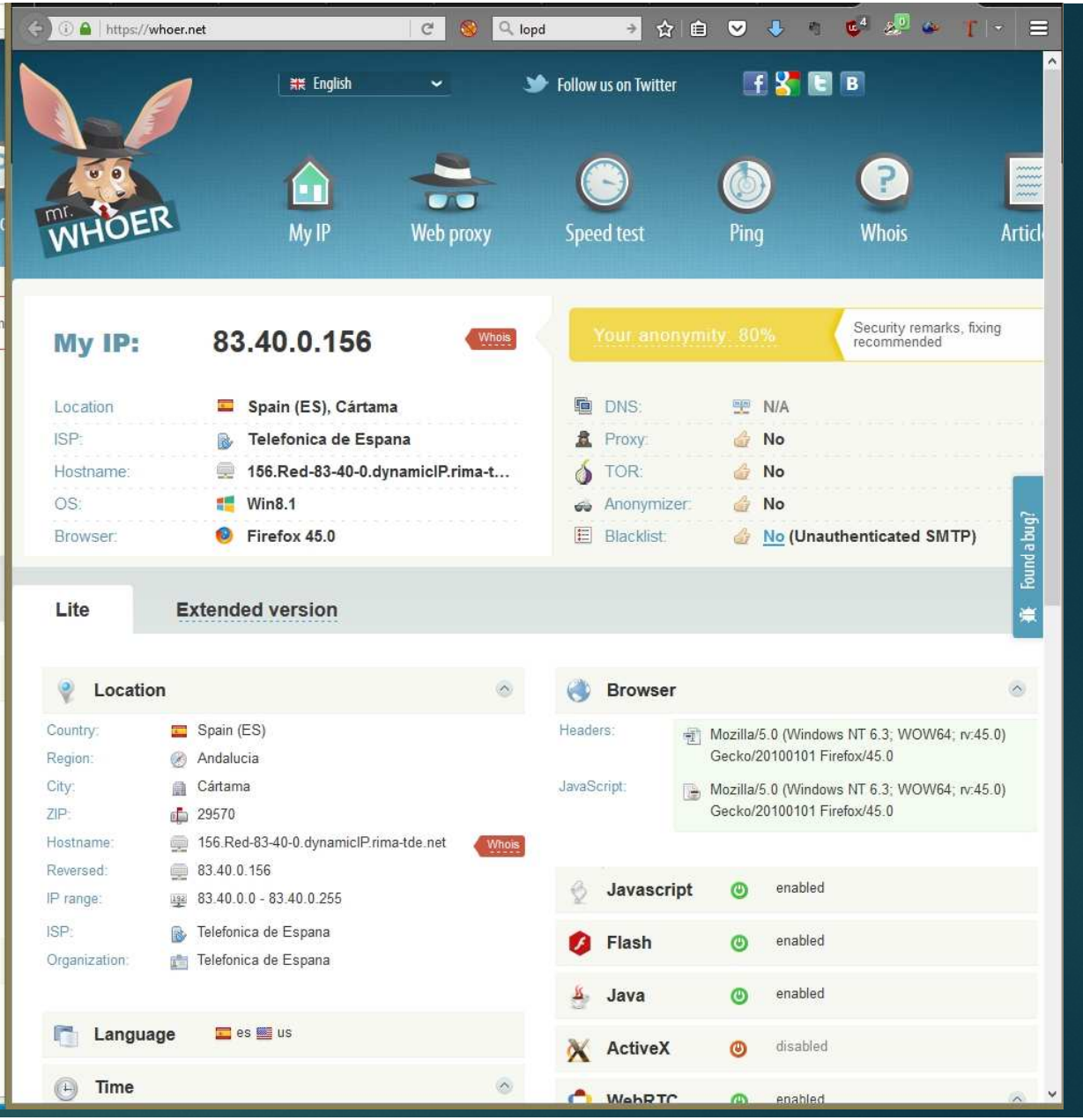
Las diez amenazas mas extendidas en 2015

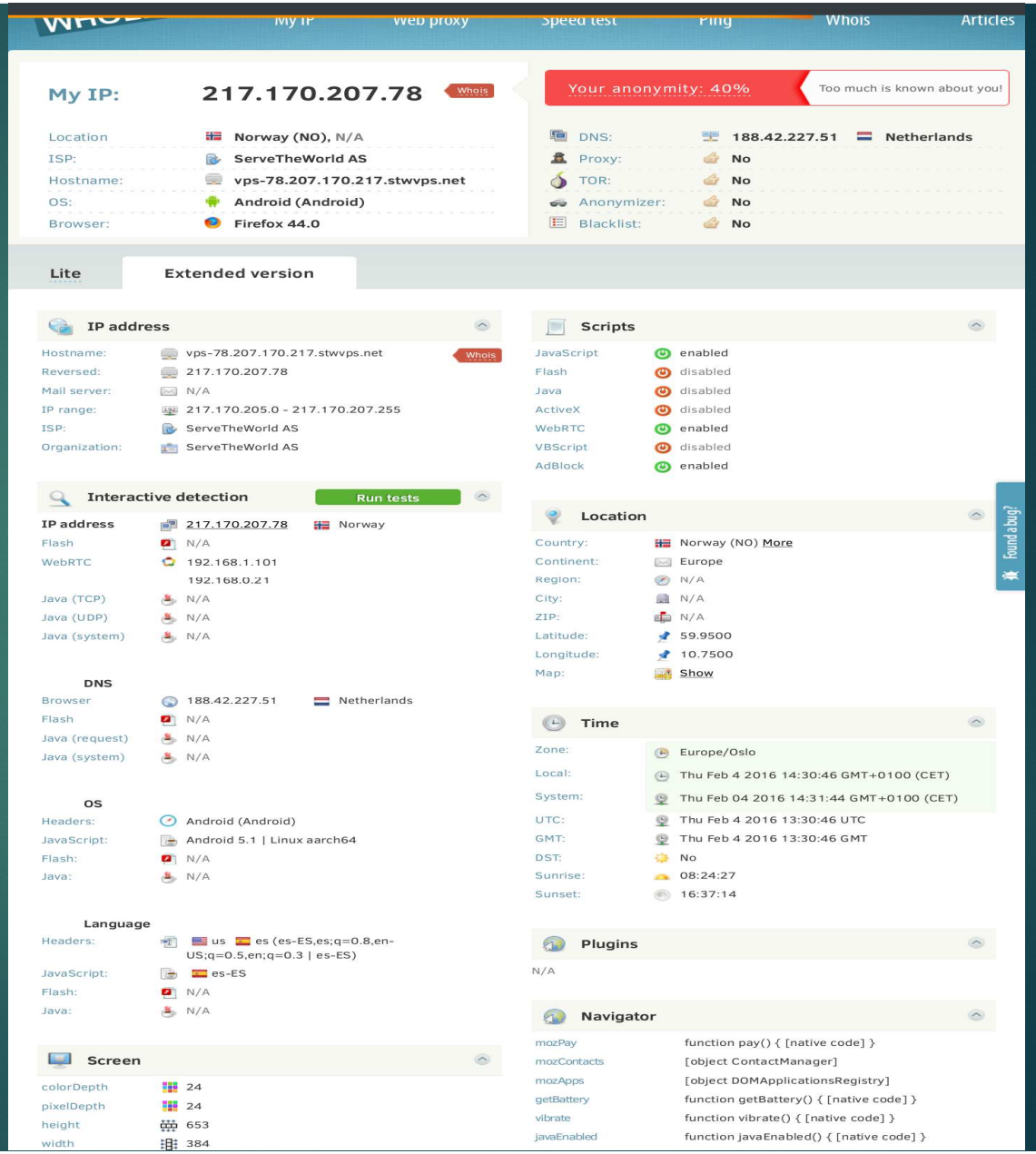
Incrementando la seguridad en nuestras conexiones a la red desde el usuario:

Tres ejemplos:

1. Desde Firefox solo con plugins
2. Desde Tor
3. Desde VPN con cambio de DNS


https://whoer.net
Buscar
English
Follow us on Twitter
mr. WHOER
My IP
Web proxy
Speed test
Ping
My IP: 5.196.31.80
Whois
Your anonymity: 36%
Too m
Location France (FR), N/A
ISP: OVH SAS
Hostname: out-mail.bet-gamers.com
OS: Win7
Browser: Firefox 38.0
DNS: 5.196.31.80
Proxy: May be
TOR: Yes
Anonymizer: No
Blacklist: Yes (Illegal)
Lite
Extended version
IP address
Hostname: out-mail.bet-gamers.com
Reversed: N/A
Mail server: mx1.ovh.net
IP range: 5.196.20.145 - 5.196.32.151
ISP: OVH SAS
Organization: OVH SAS
Scripts
JavaScript enabled
Flash disabled
Java disabled
ActiveX disabled
WebRTC disabled
VBScript disabled
AdBlock disabled
Interactive detection
Run tests
IP address 5.196.31.80 France
Flash N/A
WebRTC N/A
Java (TCP) N/A
Java (UDP) N/A
Location
Country: France (FR) More
Continent: Europe
Region: N/A
City: N/A


https://whoer.net
lopd
English
Follow us on Twitter
mr. WHOER
My IP
Web proxy
Speed test
Ping
Whois
My IP: 83.40.0.156
Whois
Your anonymity: 80%
Security remarks, fixing recommended
Location Spain (ES), Cártama
ISP: Telefonica de Espana
Hostname: 156.Red-83-40-0.dynamicIP.rima-t...
OS: Win8.1
Browser: Firefox 45.0
DNS: N/A
Proxy: No
TOR: No
Anonymizer: No
Blacklist: No (Unauthenticated SMTP)
Found a bug?
Lite
Extended version
Location
Country: Spain (ES)
Region: Andalucia
City: Cártama
ZIP: 29570
Hostname: 156.Red-83-40-0.dynamicIP.rima-tde.net
Reversed: 83.40.0.156
IP range: 83.40.0.0 - 83.40.0.255
ISP: Telefonica de Espana
Organization: Telefonica de Espana
Language es us
Time
Browser
Headers: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
JavaScript: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
Javascript enabled
Flash enabled
Java enabled
ActiveX disabled
WebRTC enabled

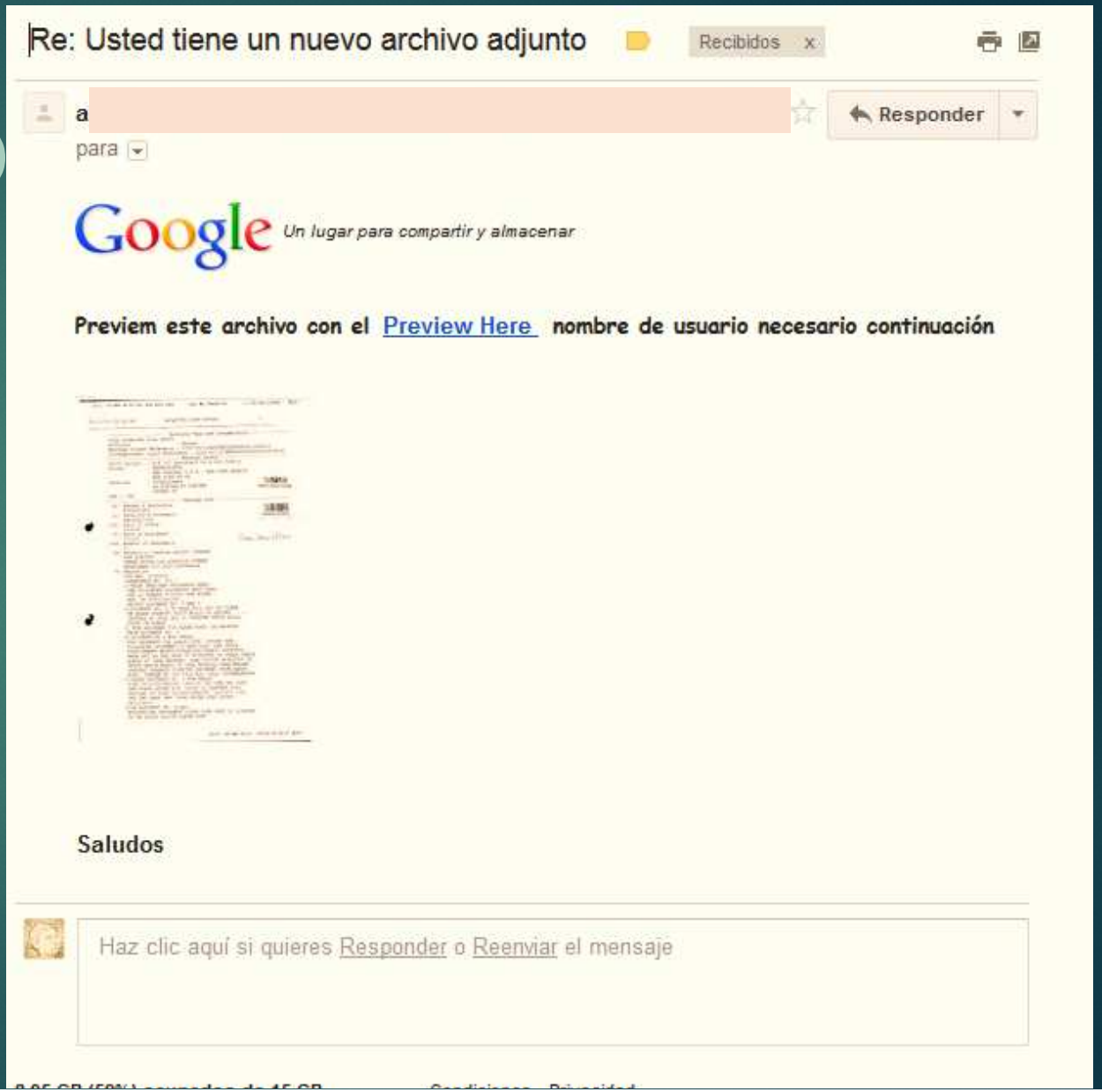

My IP
Web proxy
Speed test
Ping
Whois
Articles
My IP: 217.170.207.78
Whois
Your anonymity: 40%
Too much is known about you!
Location Norway (NO), N/A
ISP: ServeTheWorld AS
Hostname: vps-78.207.170.217.stwvps.net
OS: Android (Android)
Browser: Firefox 44.0
DNS: 188.42.227.51 Netherlands
Proxy: No
TOR: No
Anonymizer: No
Blacklist: No
Lite
Extended version
IP address
Hostname: vps-78.207.170.217.stwvps.net
Whois
Reversed: 217.170.207.78
Mail server: N/A
IP range: 217.170.205.0 - 217.170.207.255
ISP: ServeTheWorld AS
Organization: ServeTheWorld AS
Interactive detection
Run tests
IP address 217.170.207.78 Norway
Flash N/A
WebRTC 192.168.1.101
192.168.0.21
Java (TCP) N/A
Java (UDP) N/A
Java (system) N/A
DNS
Browser 188.42.227.51 Netherlands
Flash N/A
Java (request) N/A
Java (system) N/A
OS
Headers: Android (Android)
JavaScript: Android 5.1 | Linux aarch64
Flash: N/A
Java: N/A
Language
Headers: us es (es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 | es-ES)
JavaScript: es-ES
Flash: N/A
Java: N/A
Screen
colorDepth 24
pixelDepth 24
height 653
width 384
Scripts
JavaScript enabled
Flash disabled
Java disabled
ActiveX disabled
WebRTC enabled
VBScript disabled
AdBlock enabled
Location
Country: Norway (NO) More
Continent: Europe
Region: N/A
City: N/A
ZIP: N/A
Latitude: 59.9500
Longitude: 10.7500
Map: Show
Time
Zone: Europe/Oslo
Local: Thu Feb 4 2016 14:30:46 GMT+0100 (CET)
System: Thu Feb 04 2016 14:31:44 GMT+0100 (CET)
UTC: Thu Feb 4 2016 13:30:46 UTC
GMT: Thu Feb 4 2016 13:30:46 GMT
DST: No
Sunrise: 08:24:27
Sunset: 16:37:14
Plugins
N/A
Navigator
mozPay function pay() { [native code] }
mozContacts [object ContactManager]
mozApps [object DOMApplicationsRegistry]
getBattery function getBattery() { [native code] }
vibrate function vibrate() { [native code] }
javaEnabled function javaEnabled() { [native code] }
Found a bug?

Intento de ataque de Malware (probablemente algún Ransonware)

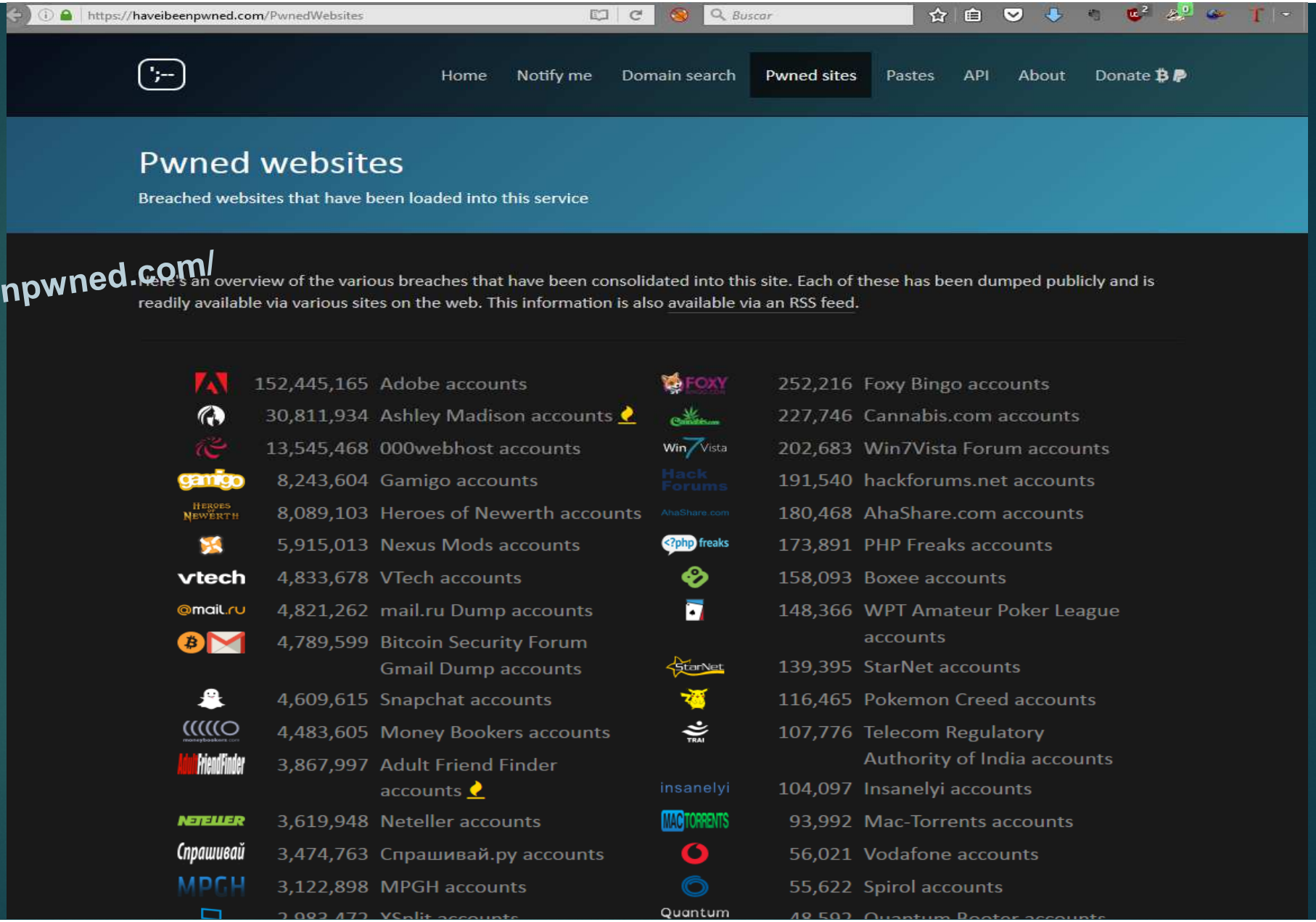
El correo *trata de parecerse* a Google

Sospechas:

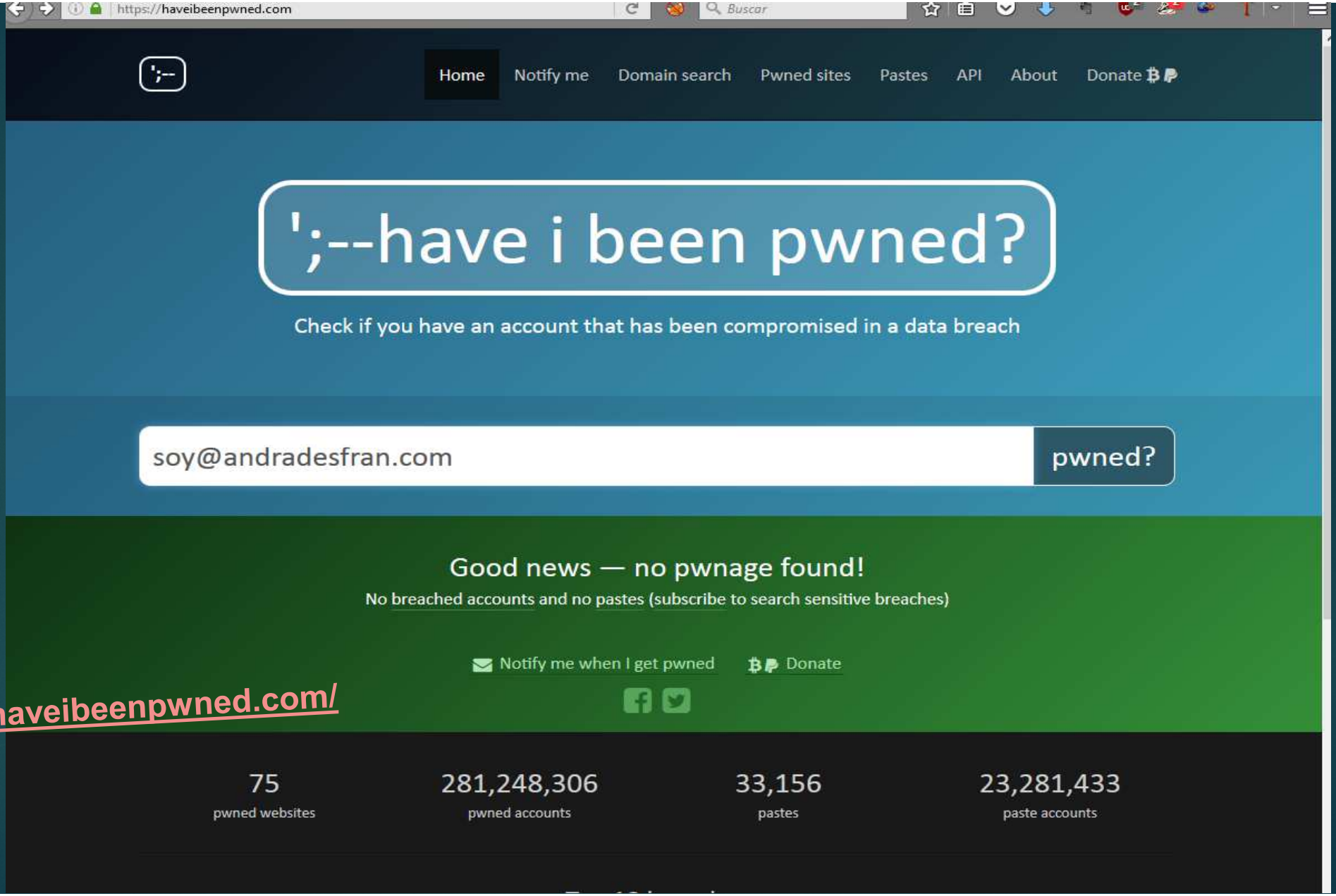
1. Envío de documento no solicitado
2. Gmail no hace *preview (vista previa)* estática
3. El enlace apunta a http://www.athollcentre.org.uk/qqq/gdoc/index.html un sitio falso que procederá a instalarte malware



https://haveibeenpwned.com/



https://haveibeenpwned.com/



https://haveibeenpwned.com/

Defacement: suplantación de pagina web

Ransonware

Secuestro de ordenador

Según CCN además de software adecuado y políticas de seguridad, la virtualización, el uso de VPN y el cifrado impiden en muchos casos su extensión

ADVERTENCIA

nos cifrar sus archivos con Crypt0L0cker

Los archivos más importantes (incluidos los de los discos de red, USB, etc): fotos, vídeos, documentos, etc. se cifran con nuestro virus Crypt0L0cker. La única manera de restaurar los archivos es pagarnos. De lo contrario, se perderán los archivos.

Precaución: Extracción de Crypt0L0cker no restaurará el acceso a los archivos cifrados.

Haga clic aquí para pagar por la recuperación de archivos

Preguntas más frecuentes

[+] ¿Qué pasó con mis archivos?

La comprensión de la cuestión

[+] ¿Cómo puedo restaurar mis archivos?

La única manera de restaurar los archivos

[+] ¿Qué debo hacer ahora?

Comprar descifrado

[+] No puedo acceder a su sitio web. ¿Qué debo hacer?

Acceso a sitios web utilizando espejos

Importancia de tener una política correcta de copias de seguridad

La necesidad de una gestión de la seguridad en los entornos corporativos

La Seguridad es un Proceso, no una Compra

Decálogo de ciberseguridad del CCN

1. Aumentar la capacidad de vigilancia de las redes y los sistemas.

2. Monitorización y correlación de eventos.

Uso de herramientas capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etc.

3. Política de Seguridad Corporativa restrictiva.

Adecuación progresiva de los permisos de usuario, servicios en la "nube" y la utilización de dispositivos y equipos propiedad del usuario (BYOD).

4. Configuraciones de seguridad en todos los componentes de la red corporativa. *Se incluirán los dispositivos móviles y portátiles*

5. Uso de productos, equipos y servicios confiables y certificados.

Redes y sistemas acreditados para información sensible o clasificada.

CCN-CERT
centro criptológico nacional

6. **Automatizar e incrementar el intercambio de información.** ***Reciprocidad con otras organizaciones y Equipos de Respuesta a Incidentes de Seguridad de la Información (CERTs)***

7. **Compromiso de la Dirección con la ciberseguridad.**
Los cargos directivos deben ser los primeros en aceptar que existen riesgos y promover las políticas de seguridad

8. **Formación y la Sensibilización de usuarios (eslabón más débil de la cadena).**
Todos y cada uno de los niveles de la organización (dirección, gestión e implantación) deben ser conscientes de los riesgos y actuar en consecuencia

9. **Atenerse a la legislación y buenas prácticas.**
Adecuación a los distintos estándares (en el caso de las Administraciones Públicas al Esquema Nacional de Seguridad -ENS-)

10. **Trabajar como si se estuviese comprometido.**
Suponer que los sistemas están ya comprometidos o lo estarán pronto y proteger los activos fundamentales

CCN-CERT
centro criptológico nacional

Las claves del Decálogo de ciberseguridad del CCN

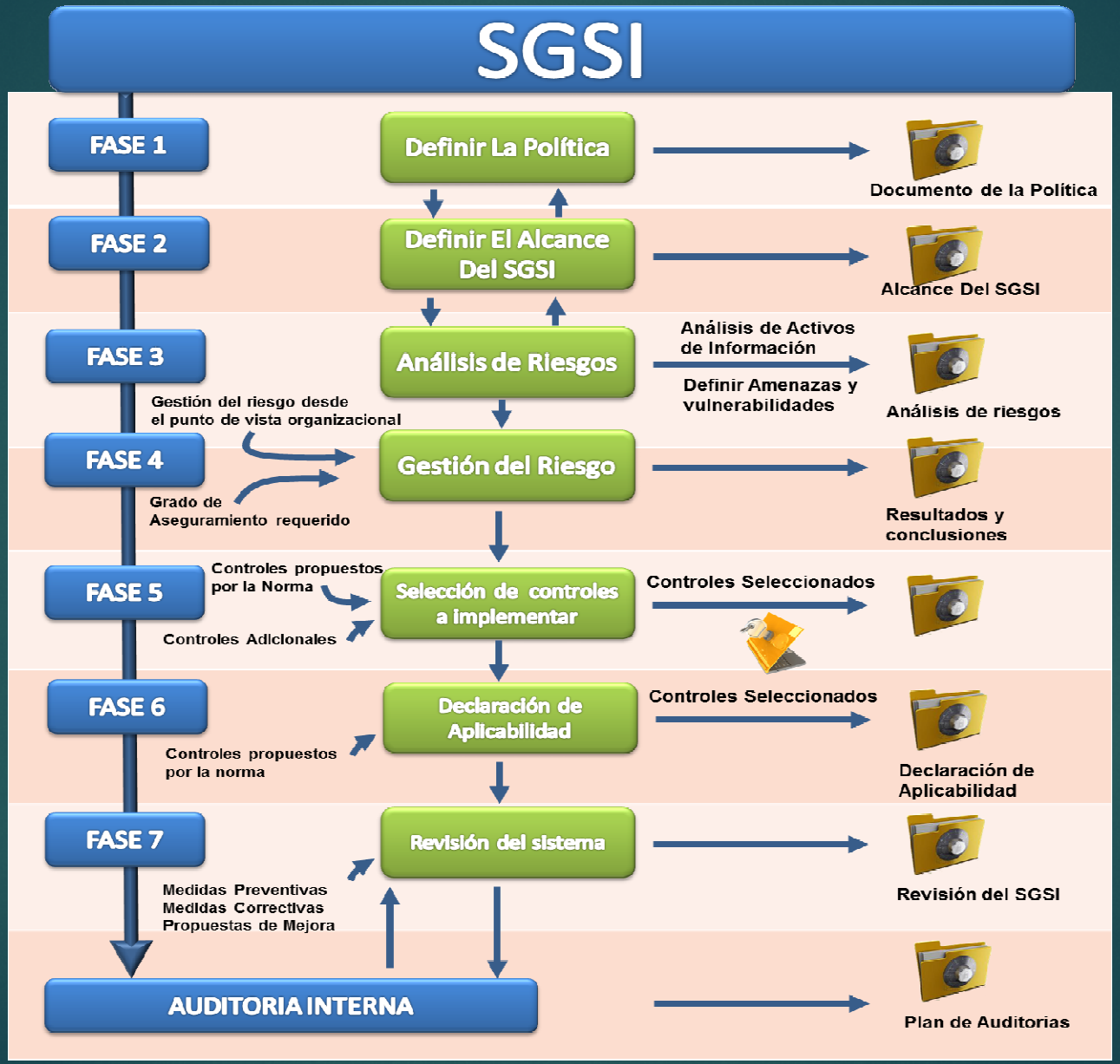
- Toma de conciencia de la importancia de sistemas seguros
- Prevención
- Establecimiento de políticas de seguridad

➢ Importancia actual de una auditoría externa adecuada

SGSI

Sistemas de Gestión de la seguridad de la Información

- LOPD (Ley Orgánica de protección de datos)
- ENS (esquema Nacional de Seguridad)
- UNE/ ISO 27001 y la UNE-ISO/IEC 27002:2005
- OWASP Top 10
- STAR- CLOUD CONTROLS MATRIX


SGSI
FASE 1
Definir La Política
Documento de la Política
FASE 2
Definir El Alcance Del SGSI
Alcance Del SGSI
FASE 3
Análisis de Riesgos
Análisis de Activos de Información
Definir Amenazas y vulnerabilidades
Análisis de riesgos
Gestión del riesgo desde el punto de vista organizacional
FASE 4
Gestión del Riesgo
Grado de Aseguramiento requerido
Resultados y conclusiones
Controles propuestos por la Norma
FASE 5
Selección de controles a implementar
Controles Seleccionados
Controles Adicionales
FASE 6
Declaración de Aplicabilidad
Controles Seleccionados
Controles propuestos por la norma
Declaración de Aplicabilidad
FASE 7
Revisión del sistema
Revisión del SGSI
Medidas Preventivas
Medidas Correctivas
Propuestas de Mejora
AUDITORIA INTERNA
Plan de Auditorias

UNE/ ISO 27001 - ISO/IEC 27002:2013

- 14 DOMINIOS
- 35 OBJETIVOS DE CONTROL
- 114 CONTROLES

✓ **Importancia de un sistema identificable con unos parámetros concretos**

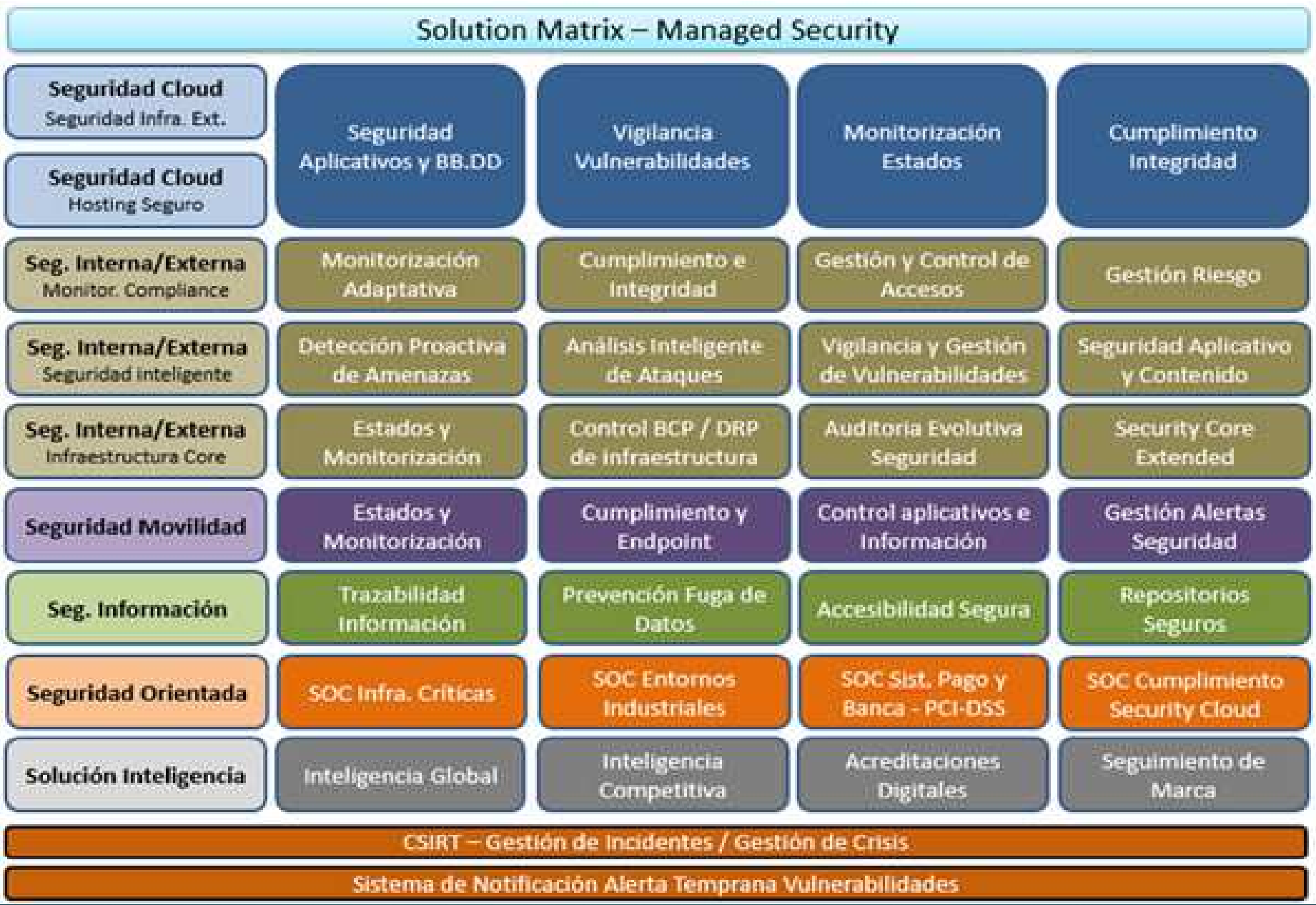
Esquema Nacional de Seguridad

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES[11]

NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	**Ciberespionaje**	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
MUY ALTO	**Interrupción de los Servicios IT / Exfiltración de datos / Compromiso de los servicios**	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.

Esquema Nacional de Seguridad

ALTO	**Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación**	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL. - Spear phising / pharming	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	**Logro o incremento significativo de capacidades ofensivas /** **Desfiguración de páginas web / Manipulación de información**	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social. -	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de de algún sistema.
BAJO	**Ataques a la imagen / menosprecio / Errores y fallos**	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.


Solution Matrix – Managed Security
Seguridad Cloud
Seguridad Infra. Ext.
Seguridad Cloud
Hosting Seguro
Seguridad Aplicativos y BB.DD
Vigilancia Vulnerabilidades
Monitorización Estados
Cumplimiento Integridad
Seg. Interna/Externa
Monitor. Compliance
Monitorización Adaptativa
Cumplimiento e Integridad
Gestión y Control de Accesos
Gestión Riesgo
Seg. Interna/Externa
Seguridad inteligente
Detección Proactiva de Amenazas
Análisis Inteligente de Ataques
Vigilancia y Gestión de Vulnerabilidades
Seguridad Aplicativo y Contenido
Seg. Interna/Externa
Infraestructura Core
Estados y Monitorización
Control BCP / DRP de Infraestructura
Auditoria Evolutiva Seguridad
Security Core Extended
Seguridad Movilidad
Estados y Monitorización
Cumplimiento y Endpoint
Control aplicativos e Información
Gestión Alertas Seguridad
Seg. Información
Trazabilidad Información
Prevención Fuga de Datos
Accesibilidad Segura
Repositorios Seguros
Seguridad Orientada
SOC Infra. Críticas
SOC Entornos Industriales
SOC Sist. Pago y Banca - PCI-DSS
SOC Cumplimiento Security Cloud
Solución Inteligencia
Inteligencia Global
Inteligencia Competitiva
Acreditaciones Digitales
Seguimiento de Marca
CSIRT – Gestión de Incidentes / Gestión de Crisis
Sistema de Notificación Alerta Temprana Vulnerabilidades

Consejos básicos

- ✓ ***Saquemos provecho del conocimiento que tenemos***

Servicios difíciles de intervenir:

Por NSA. (Informes filtrados ***a Der Spiegel)***

- **PGP** (*cifrado de correos*) muy complejo
- ***VPN*** (*redes privadas virtuales*). Casi imposible de intervenir si usa cifrados altos
- ***Cifrado de archivos***. *Ejemplo de Truecrypt*
- ***Cambio de las DNS***. *Escapa al control de operadoras y empresas.*
- ***TOR***. *Si es empleado con precaución y con nodos confiables.*

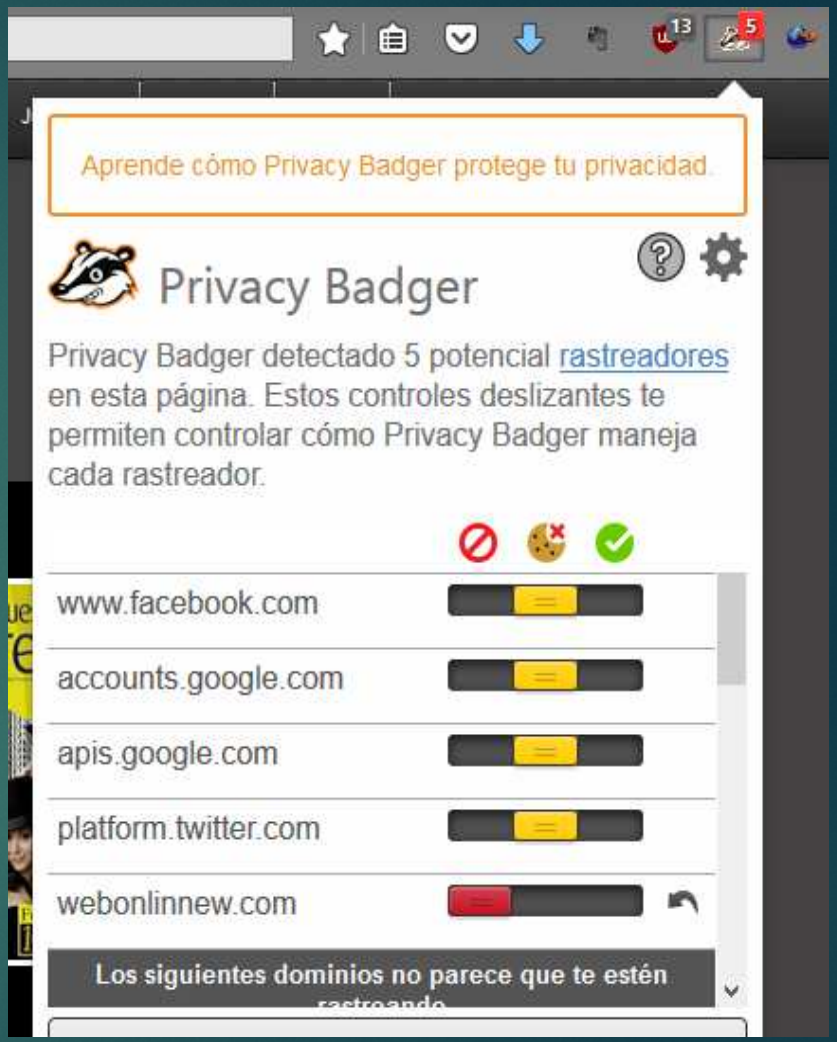
Bloqueo de “*indeseables*”

- ✓ **Firefox**: Software Libre, debidamente revisado.
- ✓ Usar plugins de bloqueo conocidos ***no vinculados comercialmente a ninguna empresa***

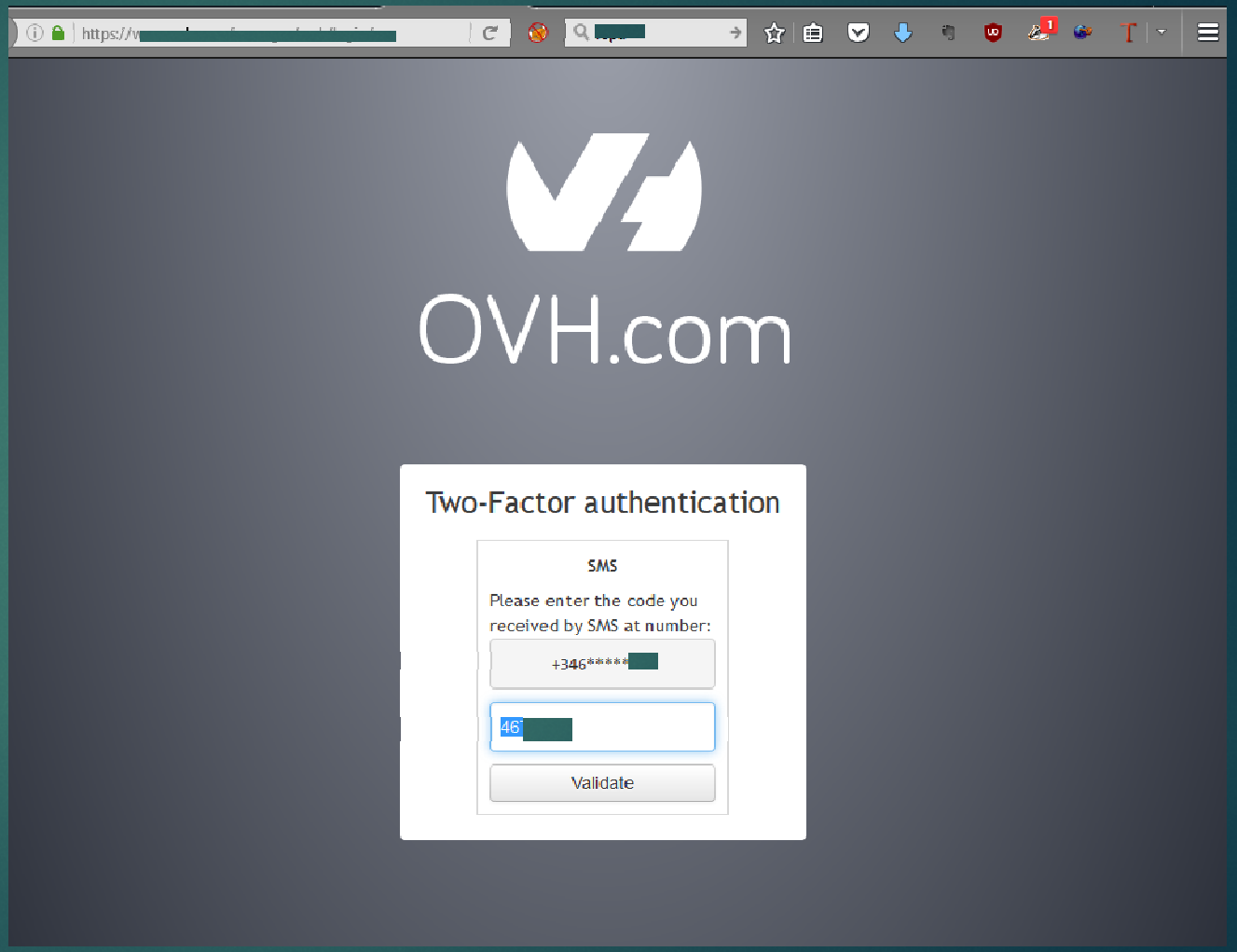
uBlock

uBlock Origin

HTTPS Everywhere



Autentificación con dos factores



Contar con una buena gestión de contraseñas, independiente de la “nube”

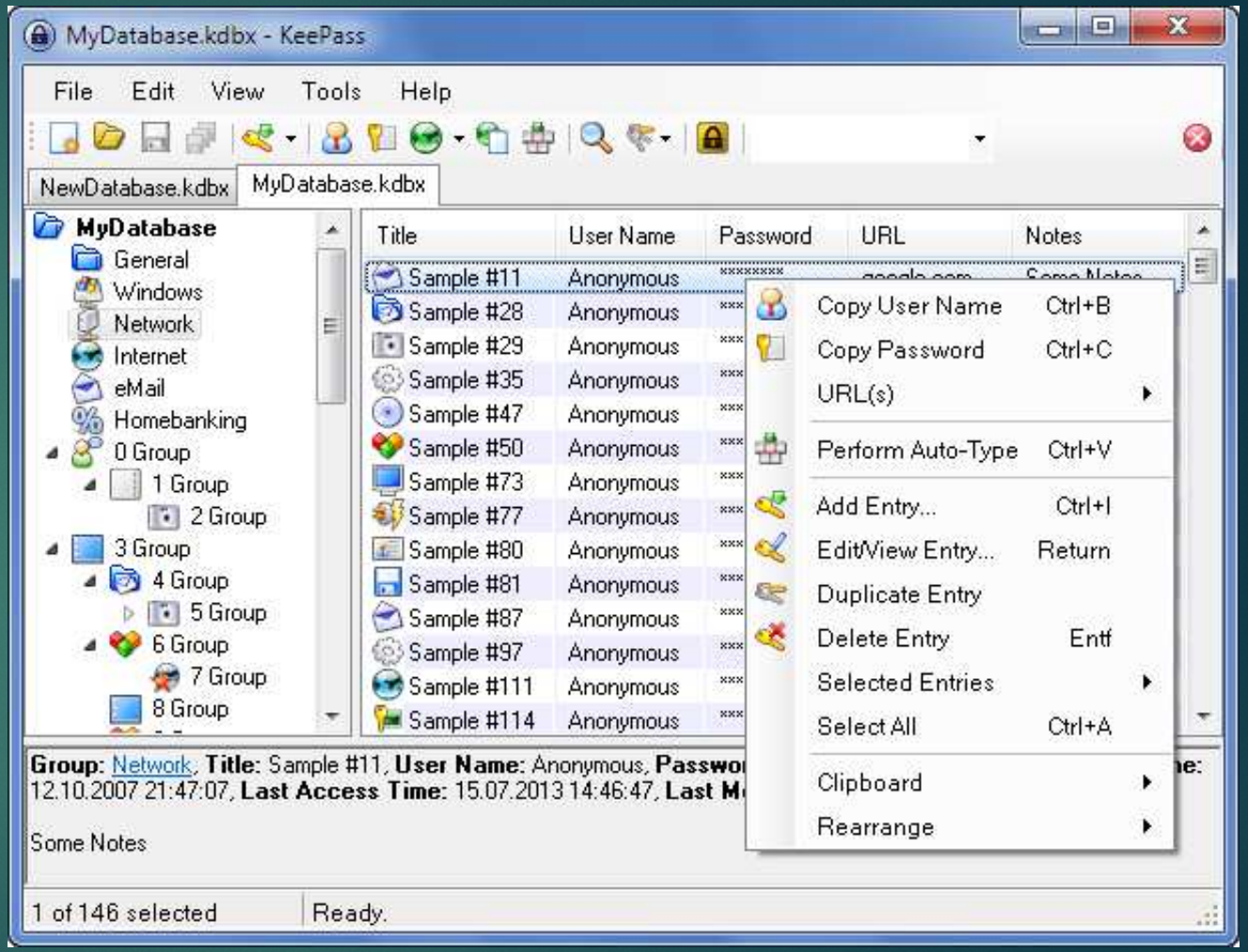
KeeFox

Lastpass.

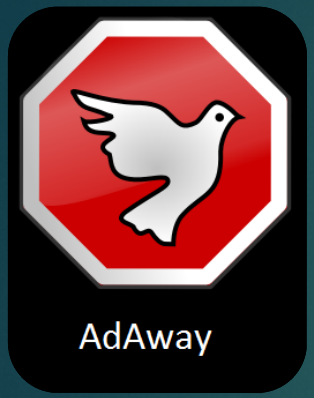
- ✓ Problemas de seguridad.
- ✓ Empresa privada sujeta a legislación EEUU

Chrome y Firefox

- ✓ fácilmente accesibles



En el móvil:

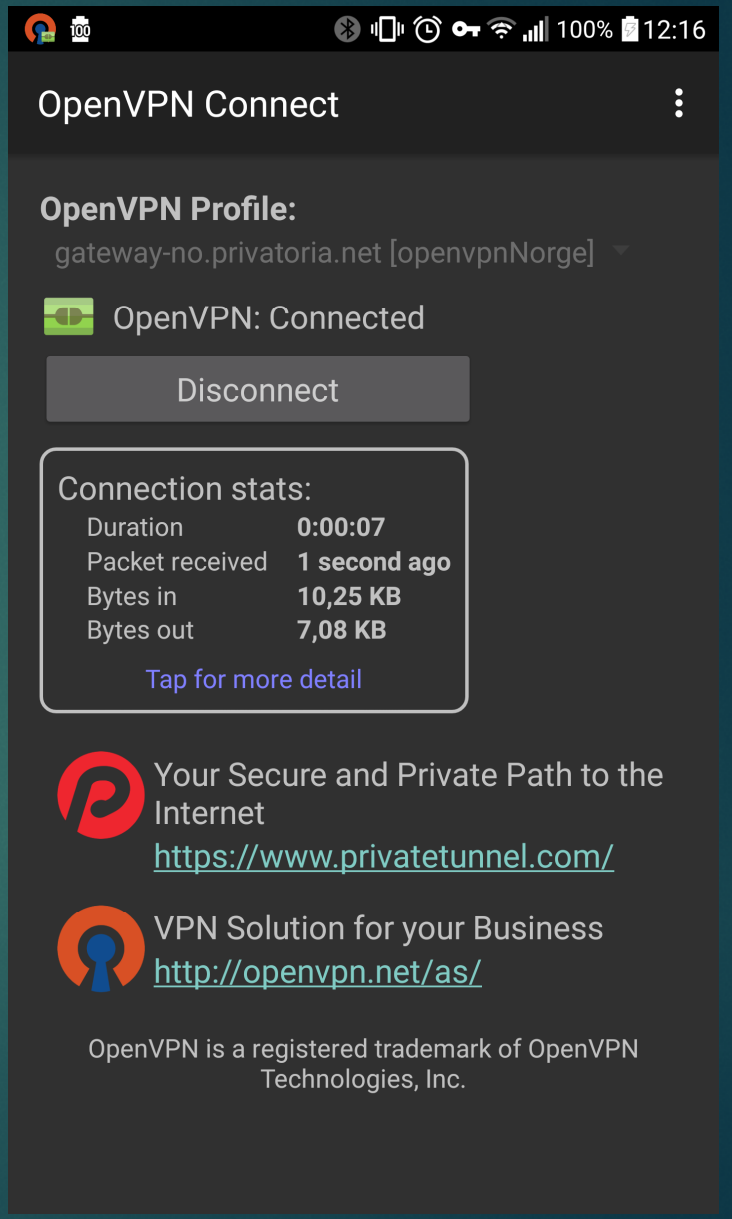


El mismo proceder que en escritorio:

- ✓ ***Bloqueo Ads y trackers***
- ✓ ***VPN y cambio de DNS***
- ✓ ***Nunca concertarse a Wifi públicas***
- ✓ ***Control de permisos***
- ✓ ***Instalación de apps de fuentes fiables***

- ❖ Aplicaciones *poco fiables* de grandes hangout, WhatsApp, Facebook App

¿Root? ***Un peligro y una ventaja***



Algunos pasos esenciales en el *securizado* de nuestro entorno:

- **Detección.**
  - **-Software siempre actualizado**
  - **-Instalación de fuentes fiables**
  - **-Antivirus, firewall…**
- **No abrir correos electrónicos de desconocidos.**
  - **-Dudar de cualquier adjunto o enlace**
- **Siempre conectar a la red de forma segura (https)**
- **Control de la "promiscuidad USB"**
- **Comprobar si el sitio que visitamos es autentico**
- **Nadie nos pide datos personales, claves etc. por mail o teléfono**
- **SENTIDO COMÚN- el vector de infección suele ser siempre una persona**

El gran error : NO TENER COPIAS DE SEGURIDAD

Algunos sitios divulgativos para aprender sobre seguridad personal en la red:

https://ssd.eff.org/es/index

https://info.securityinabox.org/es

- ✓ **Listado de proveedores de correo seguros**
  http://www.prxbx.com/email/

- ✓ **Listado de aplicaciones libres de espionaje**
  https://prism-break.org/es/

- ✓ **En la actualidad no nos podemos “bajar” de la nube, pero debemos tomar control del proceso, ser capaces de decidir, retomar la soberanía de nuestros datos y controlar su itinerario.**


✓ Gracias

www.andradesfran.com

soy@andradesfran.com

Canales con actualizaciones de contenidos:

https://telegram.me/plectica
https://telegram.me/hackingtools

https://es.linkedin.com/in/andradesfran

Referencia internacional como investigador:
http://orcid.org/0000-0001-8218-4250