

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Mitos, debilidades y delitos imperfectos en

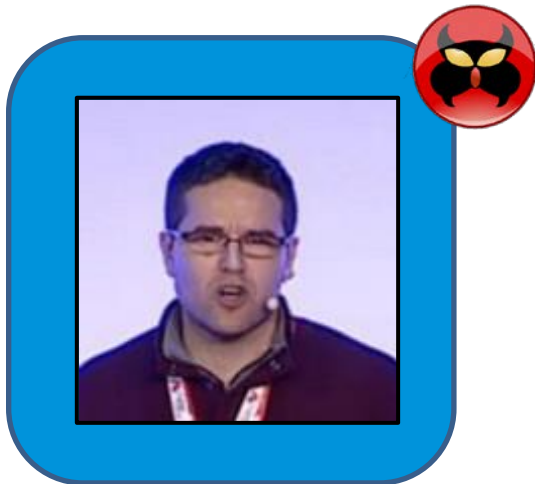




- Manuel Guerra **@CiberpoliES**
- Analista Forense UIT
- Editor del Blog Glider.es



GLIDER

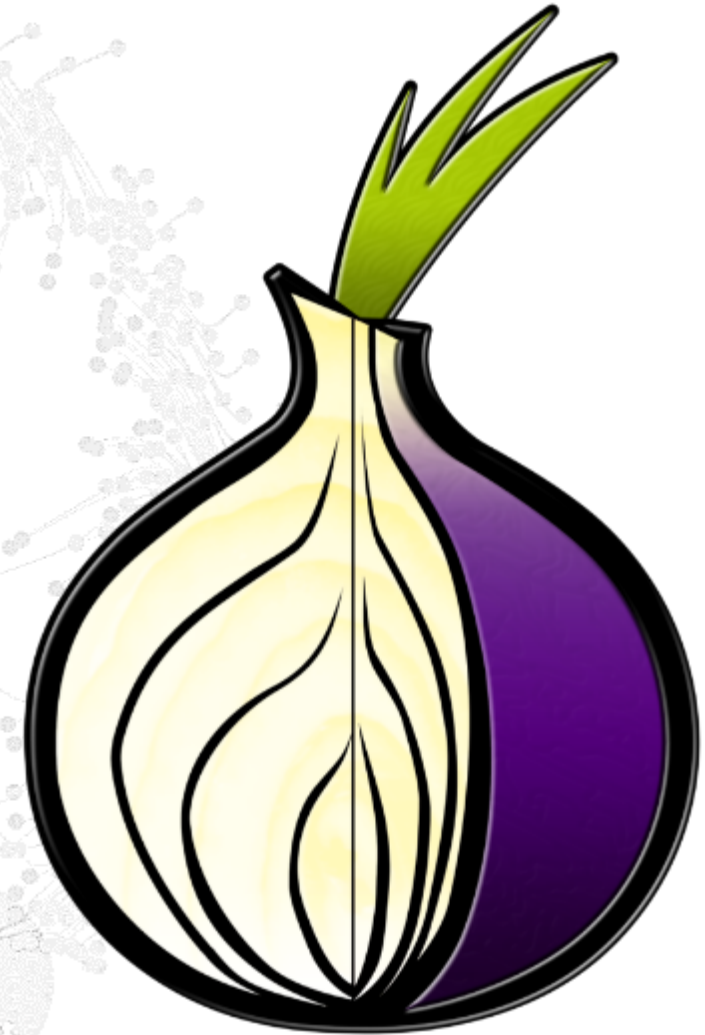


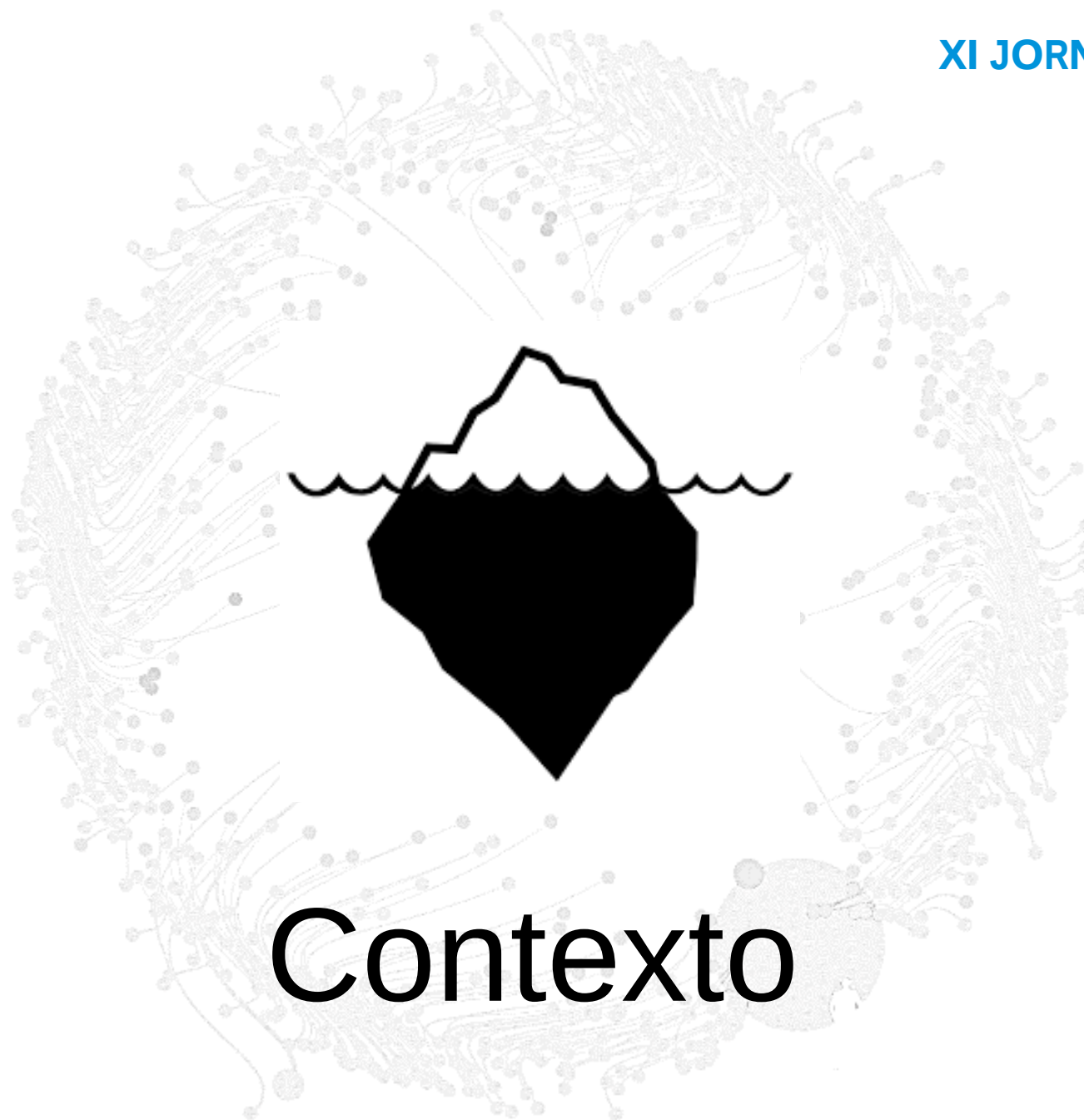
- Francisco J. Rodriguez **@0fjrm0**
- Miembro del Instituto Nacional de Ciberseguridad de España (INCIBE)
- Investigación de ciberdelitos



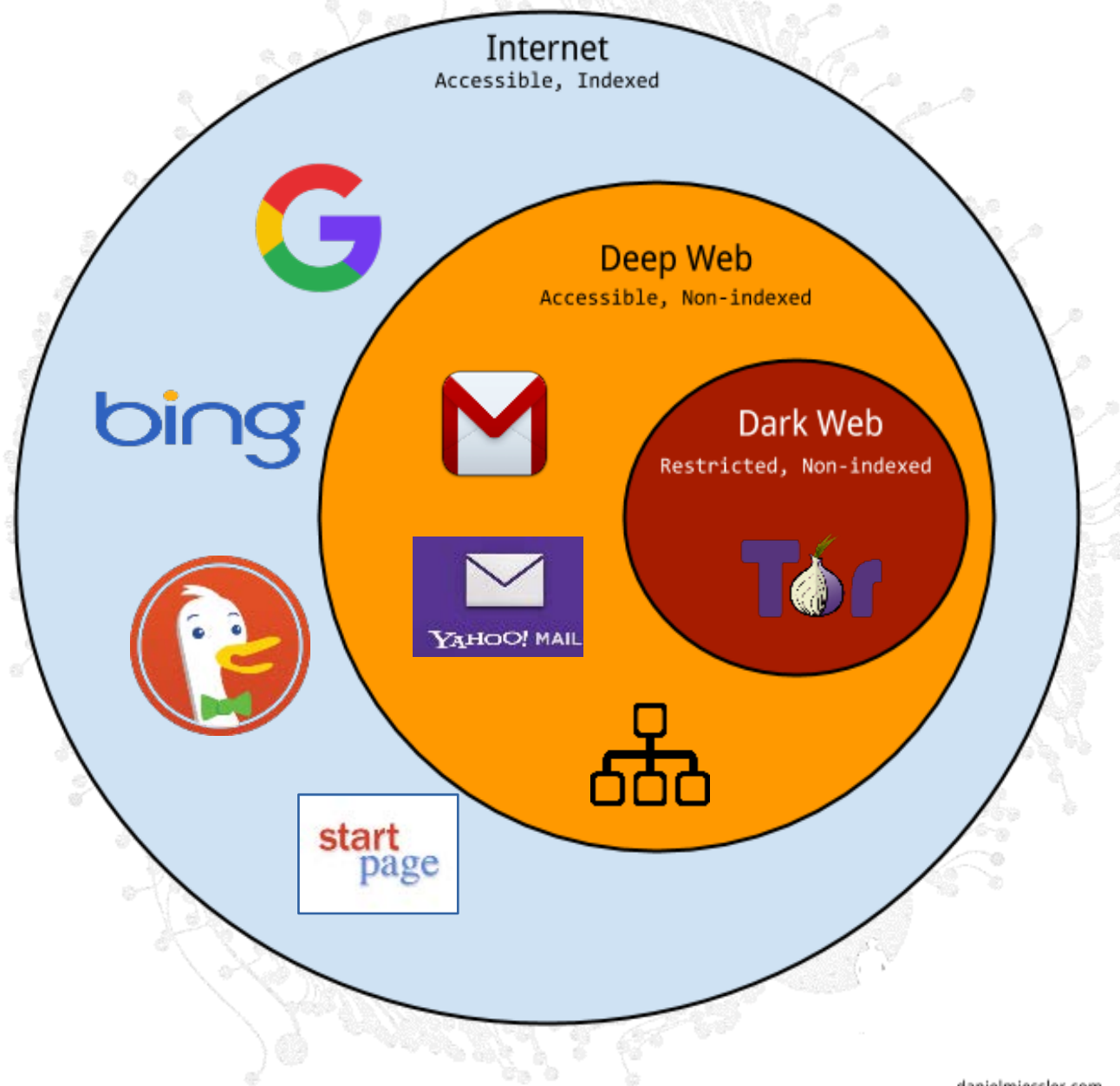
Índice

1. Contexto
2. Mitos
3. Debilidades
4. Delitos imperfectos
5. Demo





Contexto



Contexto

danielmiessler.com



PRIVACIDAD

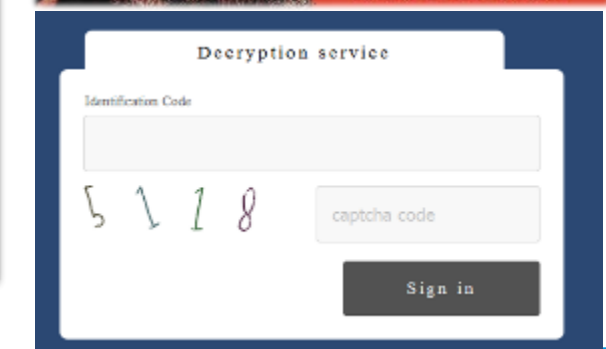
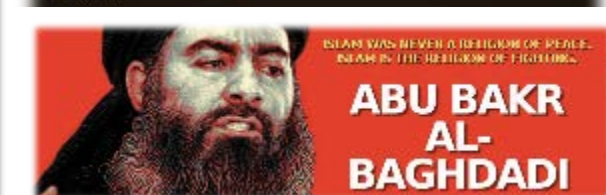
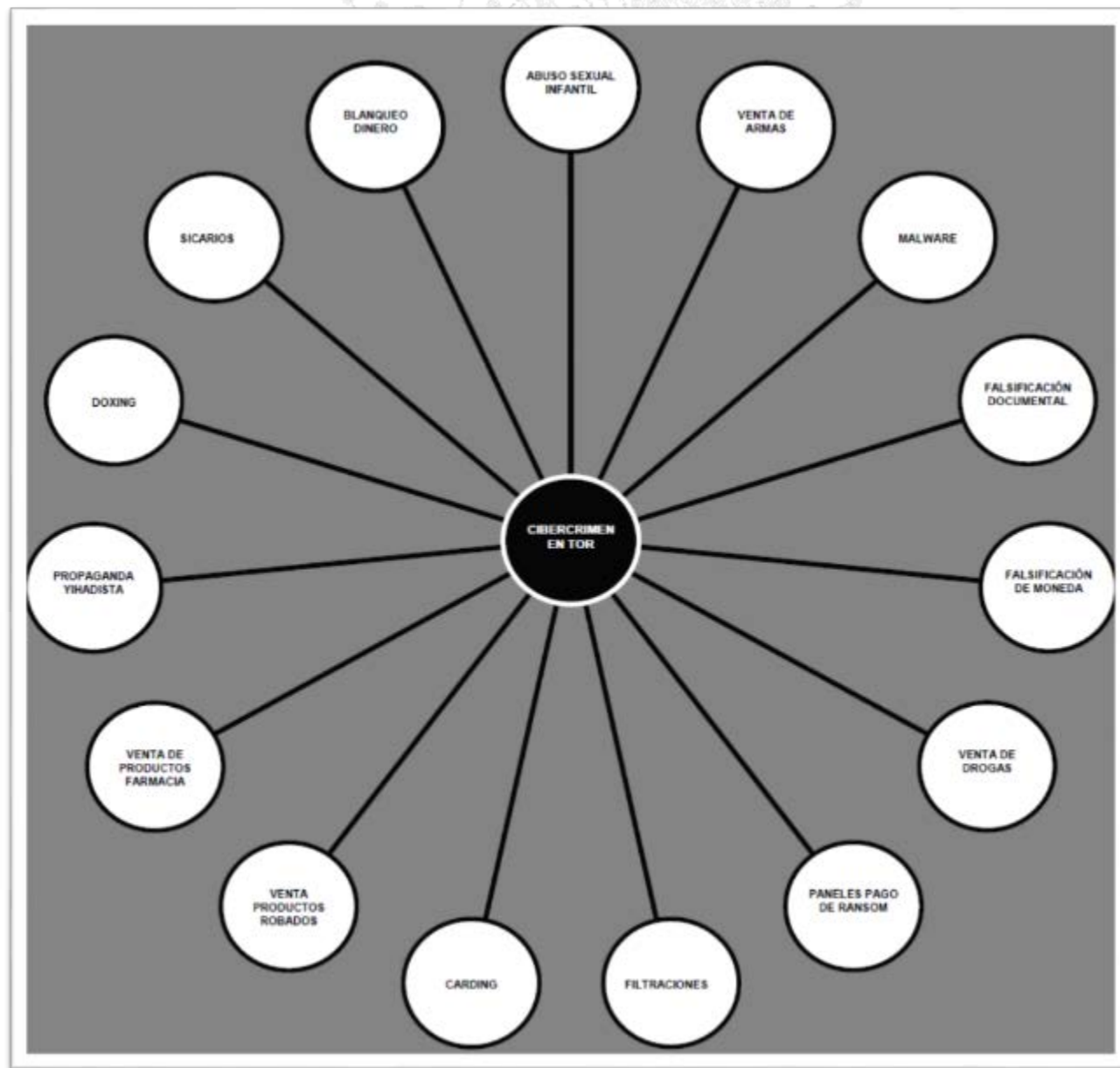
ANONIMATO

CENSURA

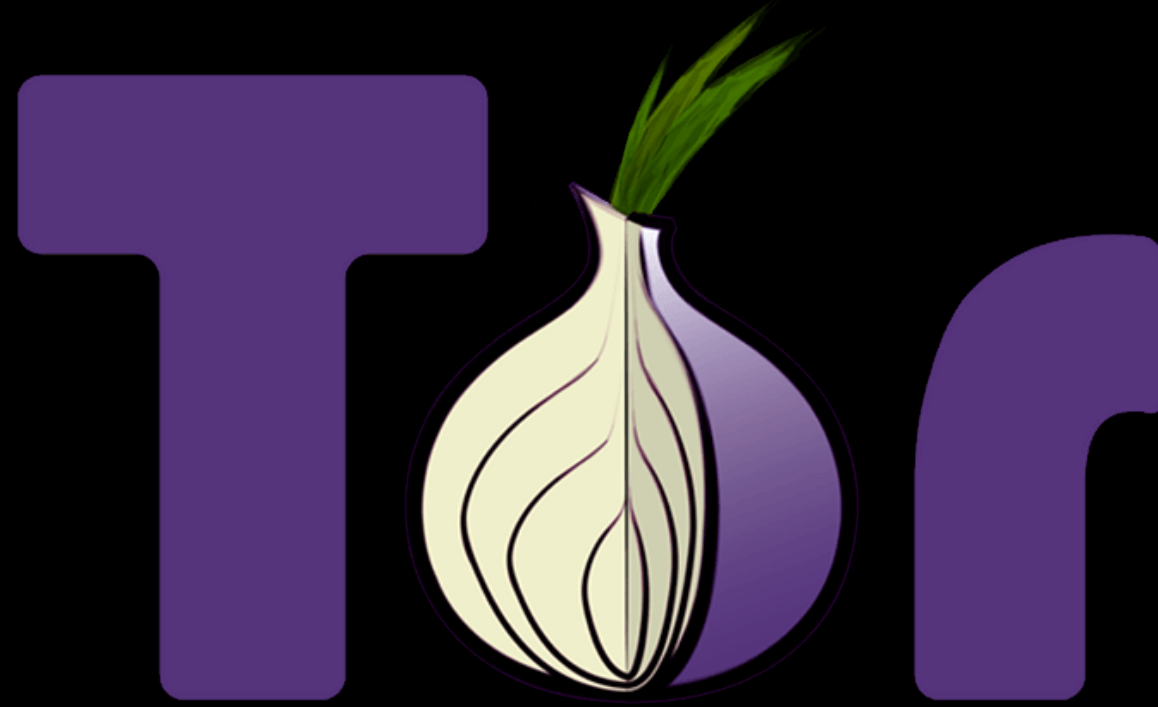
ACTIVIDAD CRIMINAL



Contexto



Contexto



CIBERCRIMEN



Contexto



¿ TELEGRAM? ¿ WHATSAPP?



Contexto

TIMOS

Los cupones de 150 euros de descuento que te han llegado por WhatsApp son una estafa

- Los timadores pueden utilizar tu información para venderla a bases de datos o suscribirte a servicios de pago

11 EN ESPAÑA

50 detenidos en 15 países por distribuir pornografía infantil a través de Whatsapp

El Estado Islámico usa Telegram para distribuir propaganda a través de los canales

El Estado Islamico usa Telegram, concretamente los canales, para distribuir propaganda y enviar mensajes antes incluso que en otras redes como Twitter.

Telegram se mueve contra Daesh: les cierra 78 canales de comunicación



Contexto



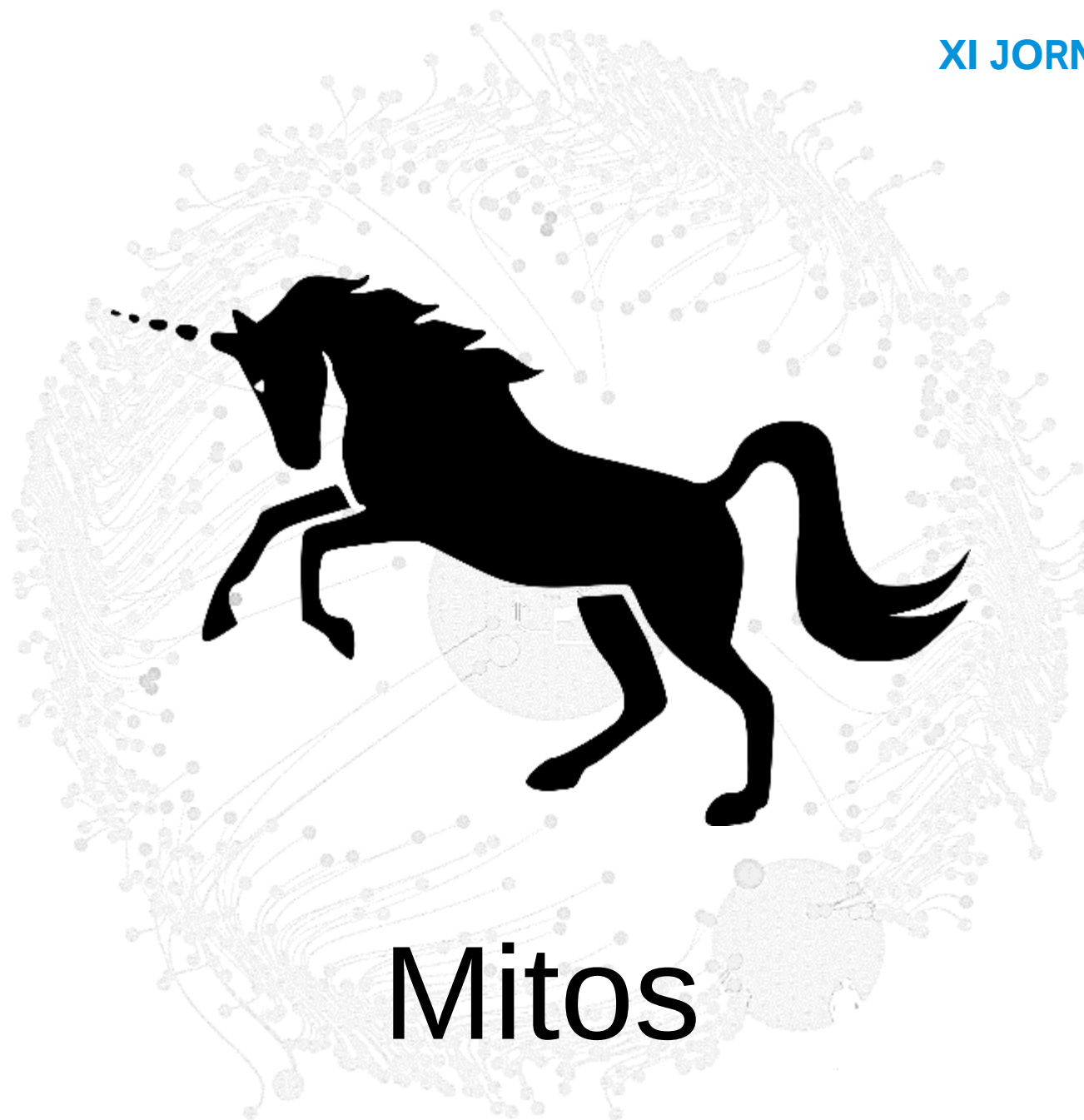
Contexto

NO

CRIMINALIZAR LA TECNOLOGÍA



Contexto



Mitos

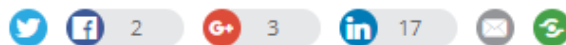
Tor, una puerta al inframundo digital de abusos a menores y otros delitos

02/01/2015 - 21:21

- Un estudio de la Universidad de Portsmouth, recogido por la BBC, revela cómo los sitios más populares de la 'red oscura' son aquellos relacionados con la pornografía infantil.
- Concretamente, el 75% del tráfico analizado refería a estos sitios, por encima de otros recursos cuantitativamente mayores, como webs de venta de drogas.

TOR, LA INTERNET DE LOS MALOS

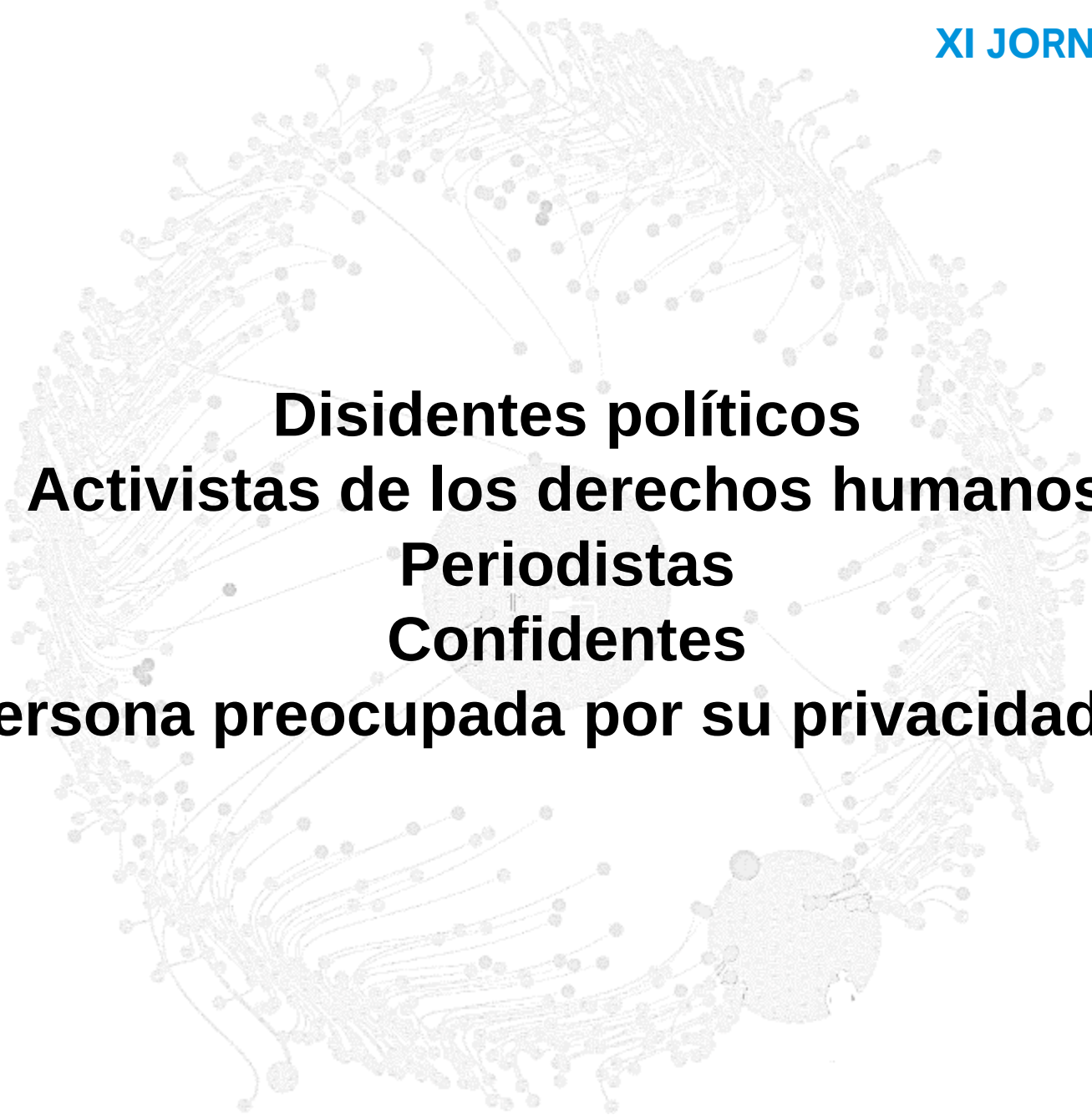
José A del Moral | 11 Abril 2013 | Tendencias | 13 comentarios



English: Tor Logo (Photo credit: Wikipedia)

Presumo de conocer bien todo lo que se cuece en Internet, pero no tuve conocimiento de la existencia de Tor hasta que me la mencionó un político socialista. ¿Por qué él sí sabía de la existencia una herramienta que utilizan muchos delincuentes para no dejar rastro de sus actividades en la Red? Presumo que porque los políticos necesitan actuar a escondidas con relativa frecuencia.

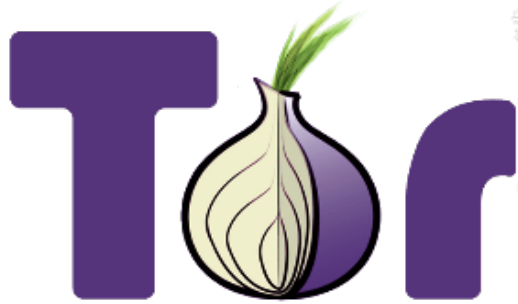




Disidentes políticos
Activistas de los derechos humanos
Periodistas
Confidentes

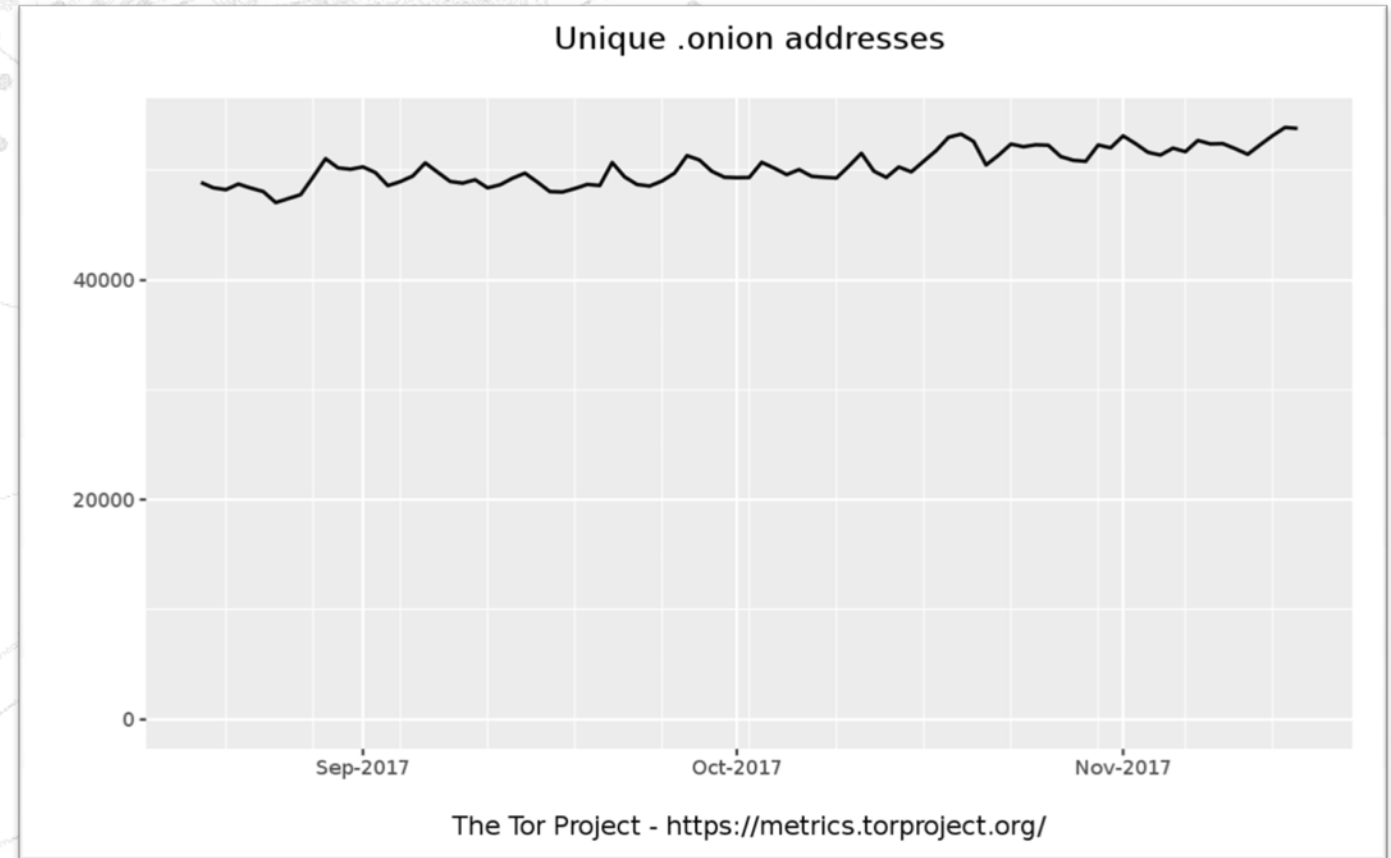
Cualquier persona preocupada por su privacidad y anonimato





**LOS CIBERDELITOS NO SOLO OCURREN
EN REDES ANÓNIMAS**

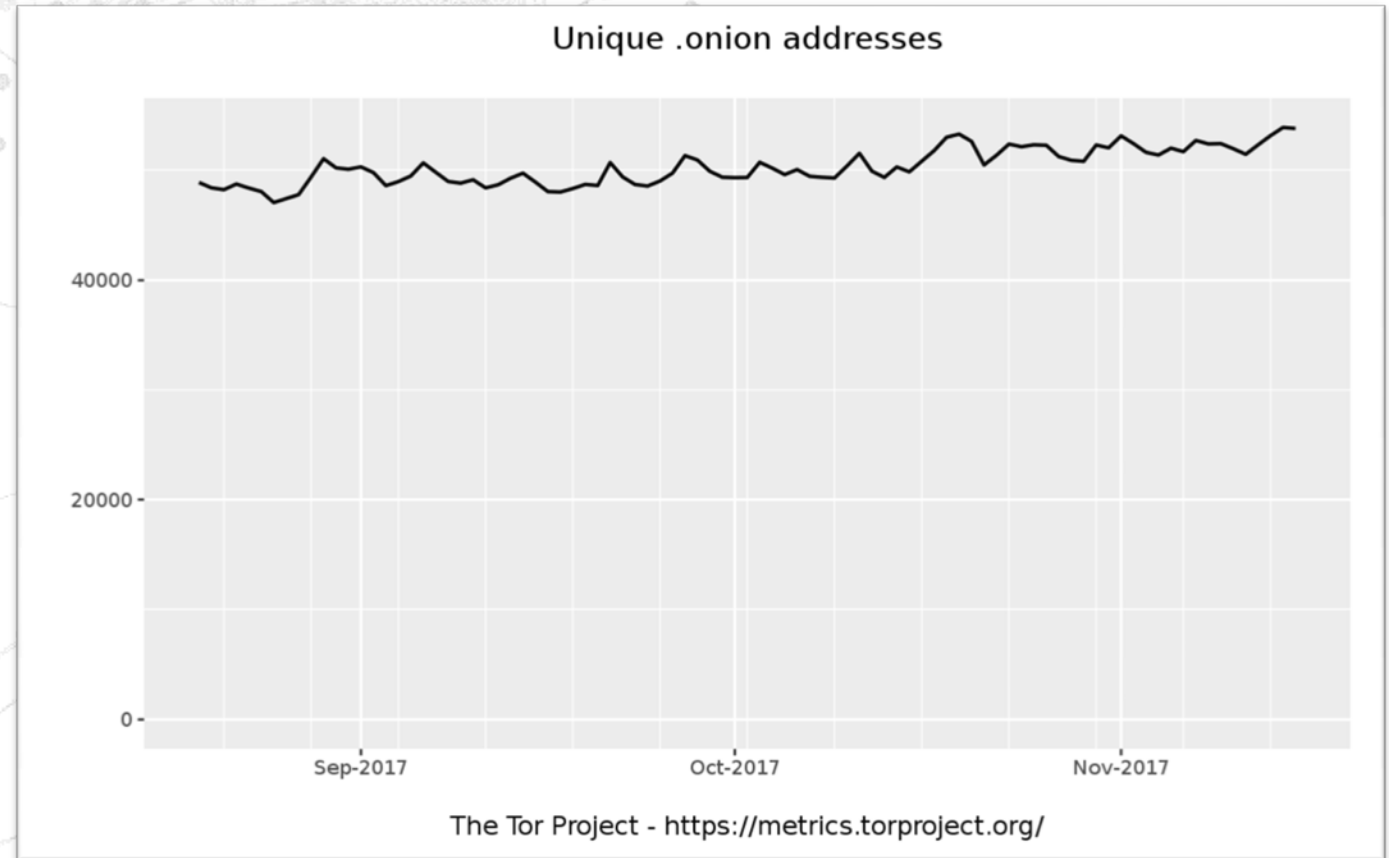




+ 50.000 ONION ÚNICOS

¿SERVICIOS?





+ 50.000 ONION ÚNICOS

¿SERVICIOS?



TCP

HTTP

HTTPS

FTP

TELNET

POP3

SMTP

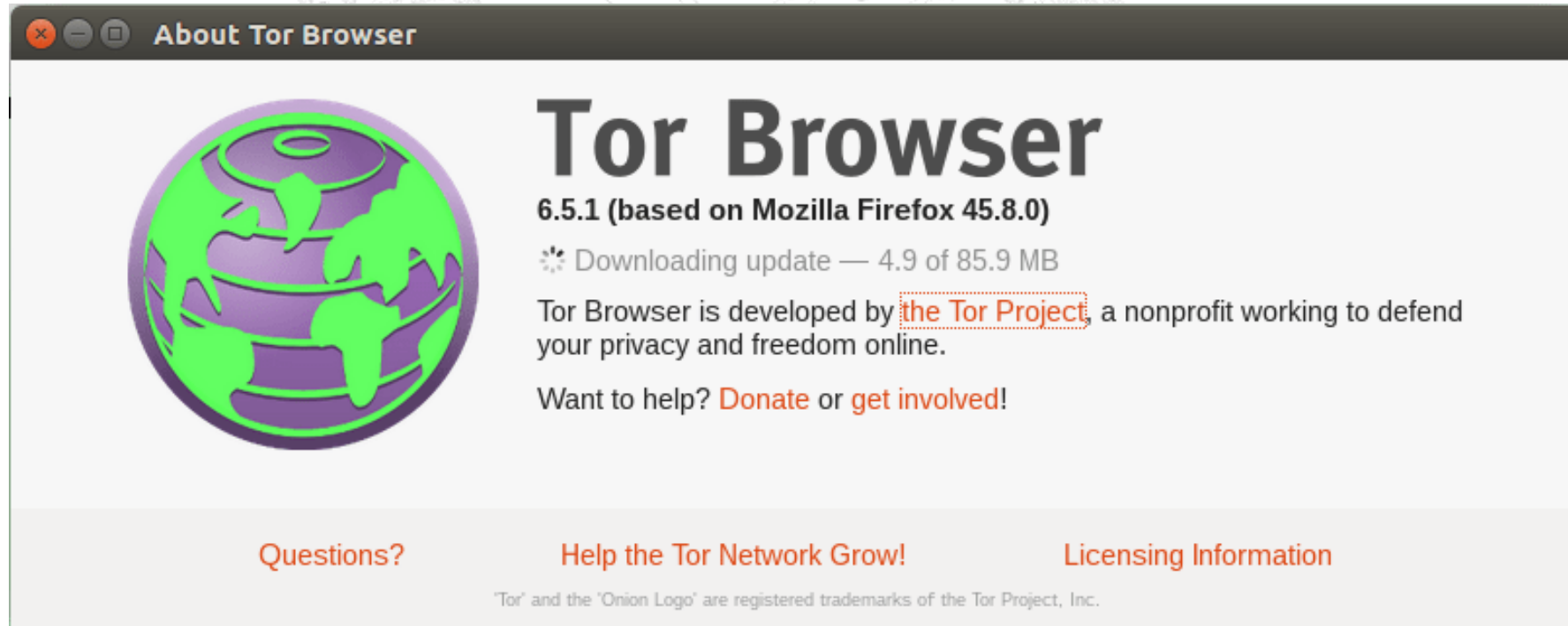
JABBER

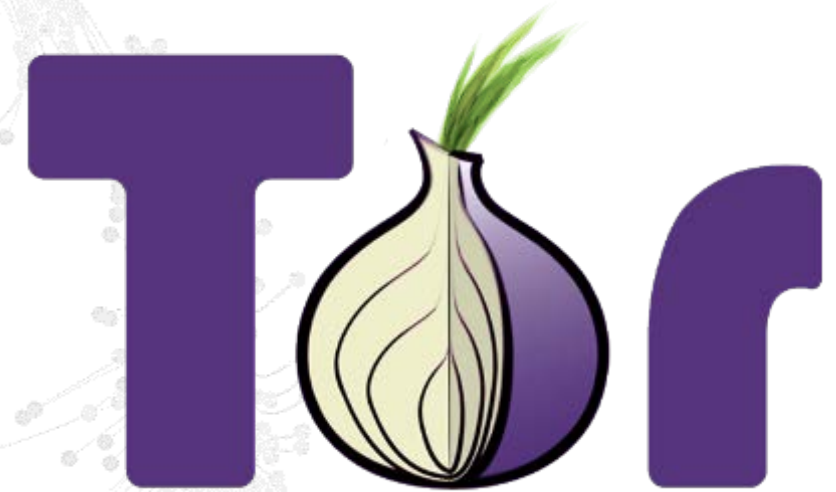
XMMP

IRC

SSH







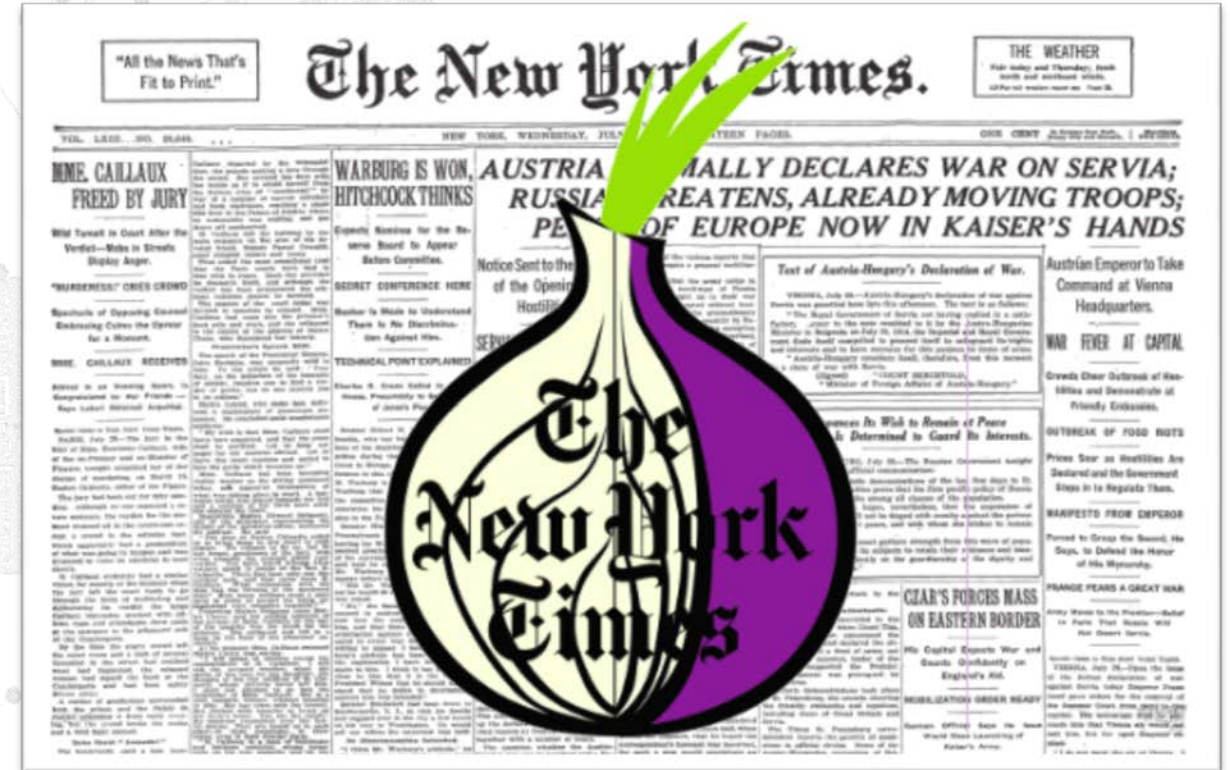
FROP563PLFD45GN.ONION.TO
ASDSAFTZ4286DFG.ONION.CITY
5G47HRUDFFF6574.ONION.LINK

DGRHGJYITOHLTIGUYIFI58396058495867GHTUYJBMCVDGR65HE389OL.ONION

VERSION 3

~~PRIVACIDAD / ANONIMATO~~

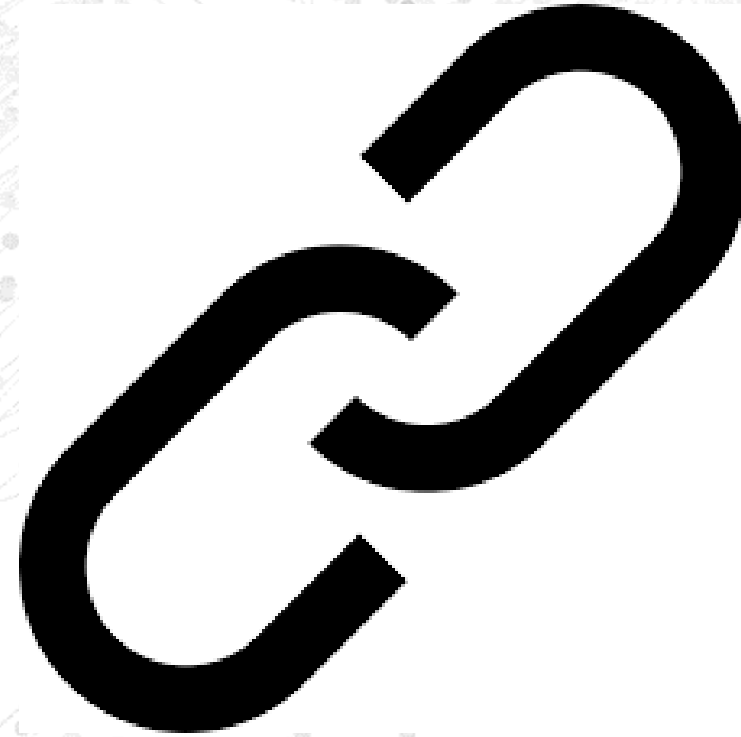




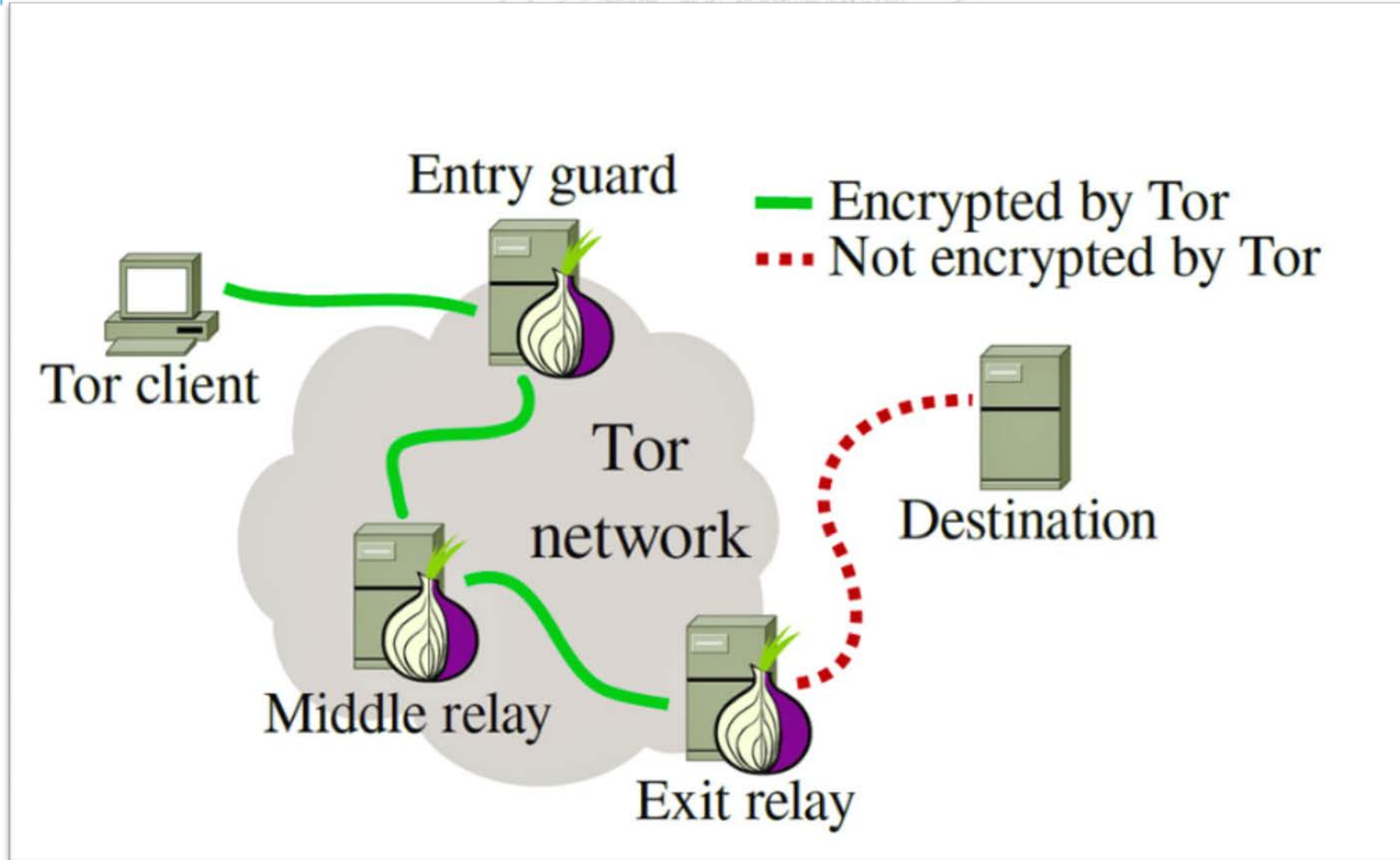
Privacidad Anonimato Seguridad



Mitos



Debilidades



Debilidades

Exploit en Firefox que afecta de lleno a Tor

El exploit fue hecho público en el blog de Tor en el día de ayer con el fin de que sea subsanado lo antes posible por los desarrolladores de Mozilla. En esa publicación se afirmaba que 'estamos ante un exploit de JavaScript y está siendo utilizado en este mismo instante contra el Navegador Tor'. El hecho de que haya sido hecha pública la vulnerabilidad hace que sea aún más peligrosa hasta que Mozilla lance una solución, ya que ahora mismo está al alcance de cualquier posible atacante.



Como muchos exploits, éste se aprovecha de una corrupción de memoria que permite inyectar código malicioso para ser utilizado en ordenadores que funcionan bajo Windows. El exploit es prácticamente **idéntico a uno que utilizó el FBI en 2013** para desanonimizar a usuarios que visitaban una página de pedofilia, el cual se ejecutaba en páginas alojadas por un servicio llamado Freedom Hosting. De hecho, el código es prácticamente el mismo, cambiando sólo algunas pequeñas partes, según afirma **el usuario** que lo ha descubierto.



JavaScript



2013 / 2016

Debilidades



- **Vulnerabilidad TORMOIL (We are Segment)**
- **Expone IP real de los usuarios**
- **Fallo en la forma de gestionar enlaces file:// en Firefox**
- **El SO se conecta de forma directa al recurso sin pasar por Tor**
- **Afecta a Linux y MacOS**
- **Corregido en Tor 7.0.9**

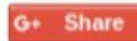
Debilidades

Zerodium Offers \$1 Million for Tor Browser 0-Days That It will Resell to Governments

Wednesday, September 13, 2017 Swati Khandelwal



Tweet



Share



Share

18



Share

323



Share

2.29k



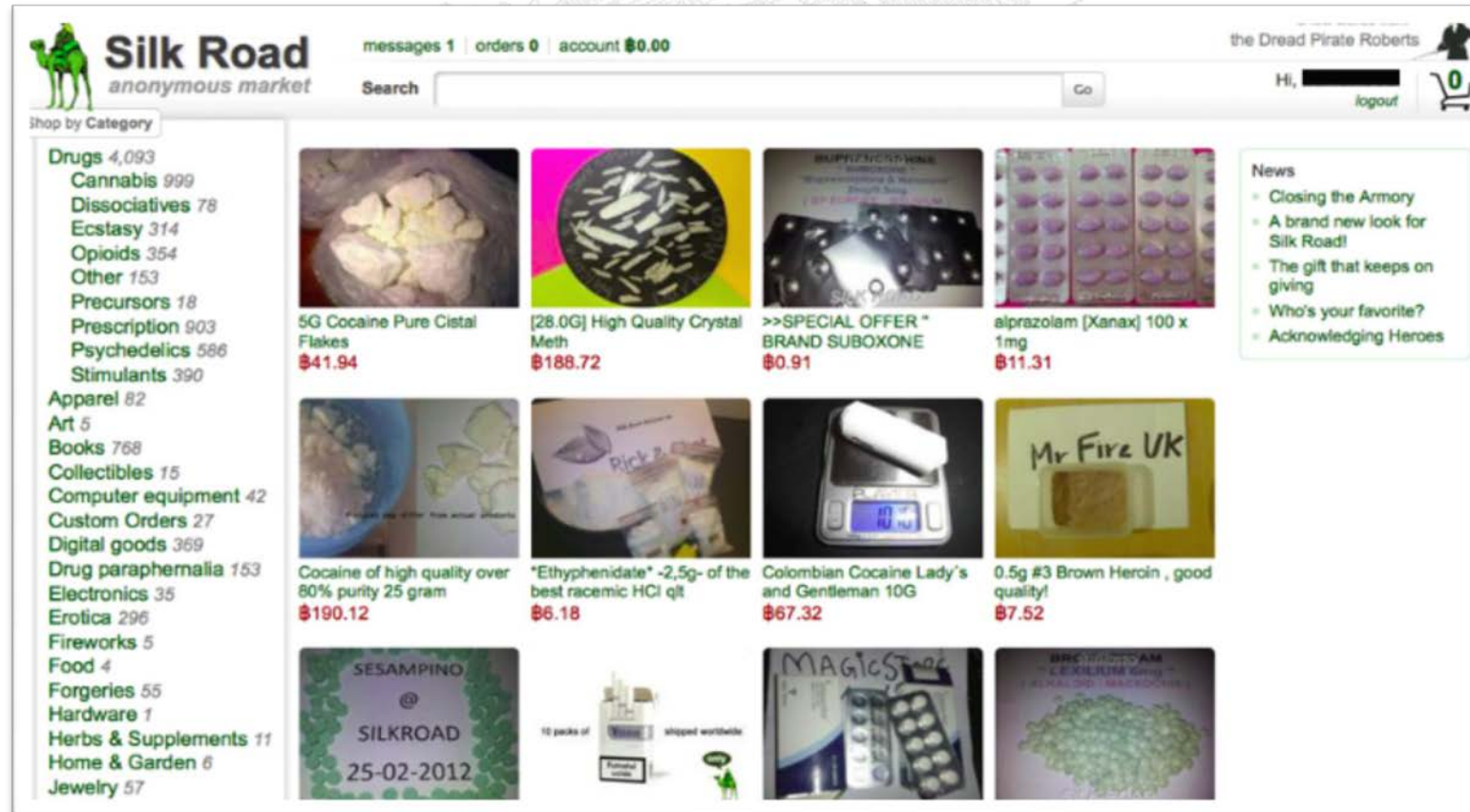
Share



Debilidades



Delitos Imperfectos



EL AUGE Y CAÍDA DE UN IMPERIO DE LA DROGA EN INTERNET

El caso 'Silk Road': la misión policial que acabó con el Temible Pirata Roberts

Delitos
Imperfectos

Europol anuncia el mayor golpe contra la dark web de la historia con el cierre de AlphaBay y Hansa



Miguel Jorge

7/20/17 11:32am • Archivar en: DARK WEB ▾

15.0K

7

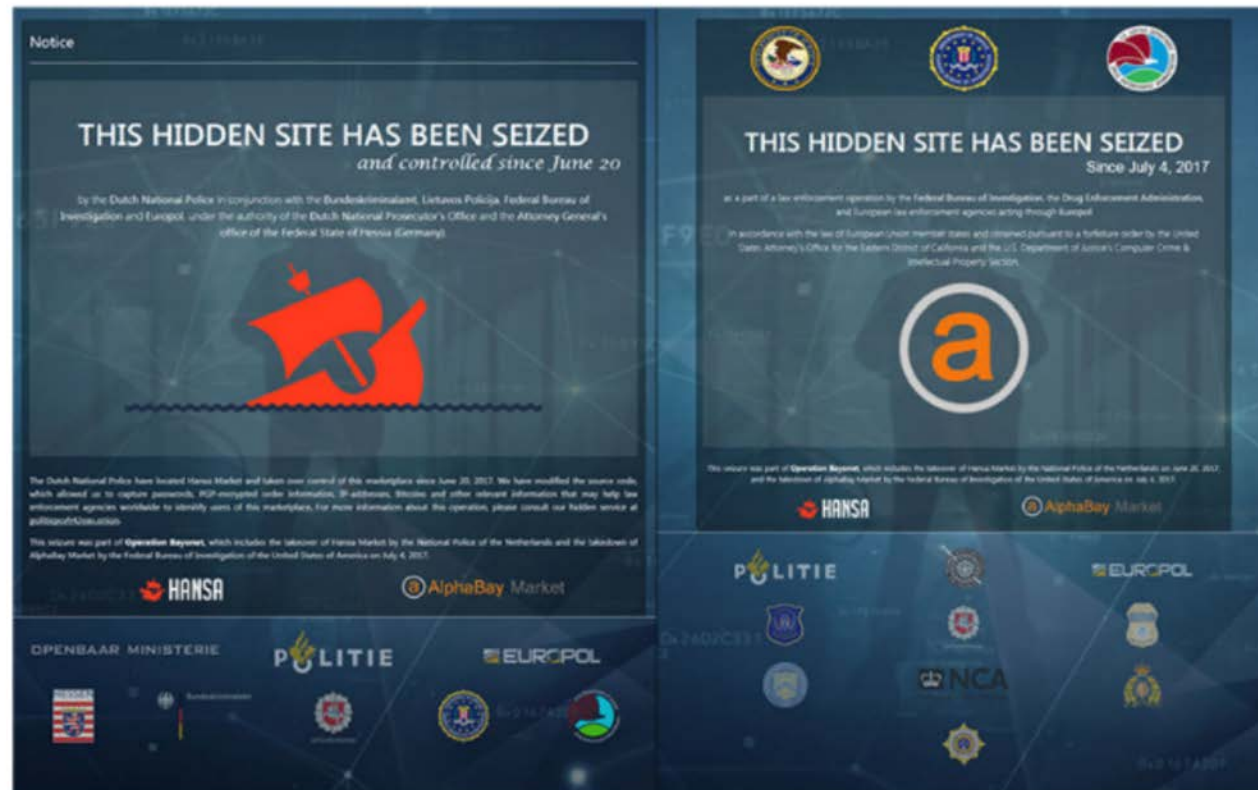


Imagen: Europol

Delitos
Imperfectos

La operación Onymous derriba 414 sitios de la Deep Web

9 noviembre, 2014 • 0 Comentarios



CRIMEN ORGANIZADO Operación Onymous

Macrooperación en Estados Unidos y Europa contra traficantes 'on line' de armas y drogas

Drogas, armas, pasaportes, licencias de conducir, servicios criminales, entre otros.

Firefox Zero-Day Exploit used by FBI to shutdown Child porn on Tor Network hosting; Tor Mail Compromised

Sunday, August 04, 2013 Mohit Kumar

[Tweet](#) [G+ Share](#) [Share](#) 8 [in Share](#) 45 [Share](#) 1,79k [Share](#)



Freedom Hosting
Anonymous Hosting Service with PHP/MySQL

[Register](#) [Login](#) [Contact](#)

[Register](#)
[Login](#)
[Contact](#)
[FTP HowTo](#)
[Privacy](#)

Hosting Features

Here you can get free hosting with PHP and MySQL:
Unlimited Space
Unlimited Bandwidth
Unlimited MySQL Databases
Your own onion domain (xxxxx.onion)
Fast Network with 24/7 Uptime
No javascript or cookies required to login
Upload a zip with your files and extract on server
FTP Access
Daily Backups

What's Allowed

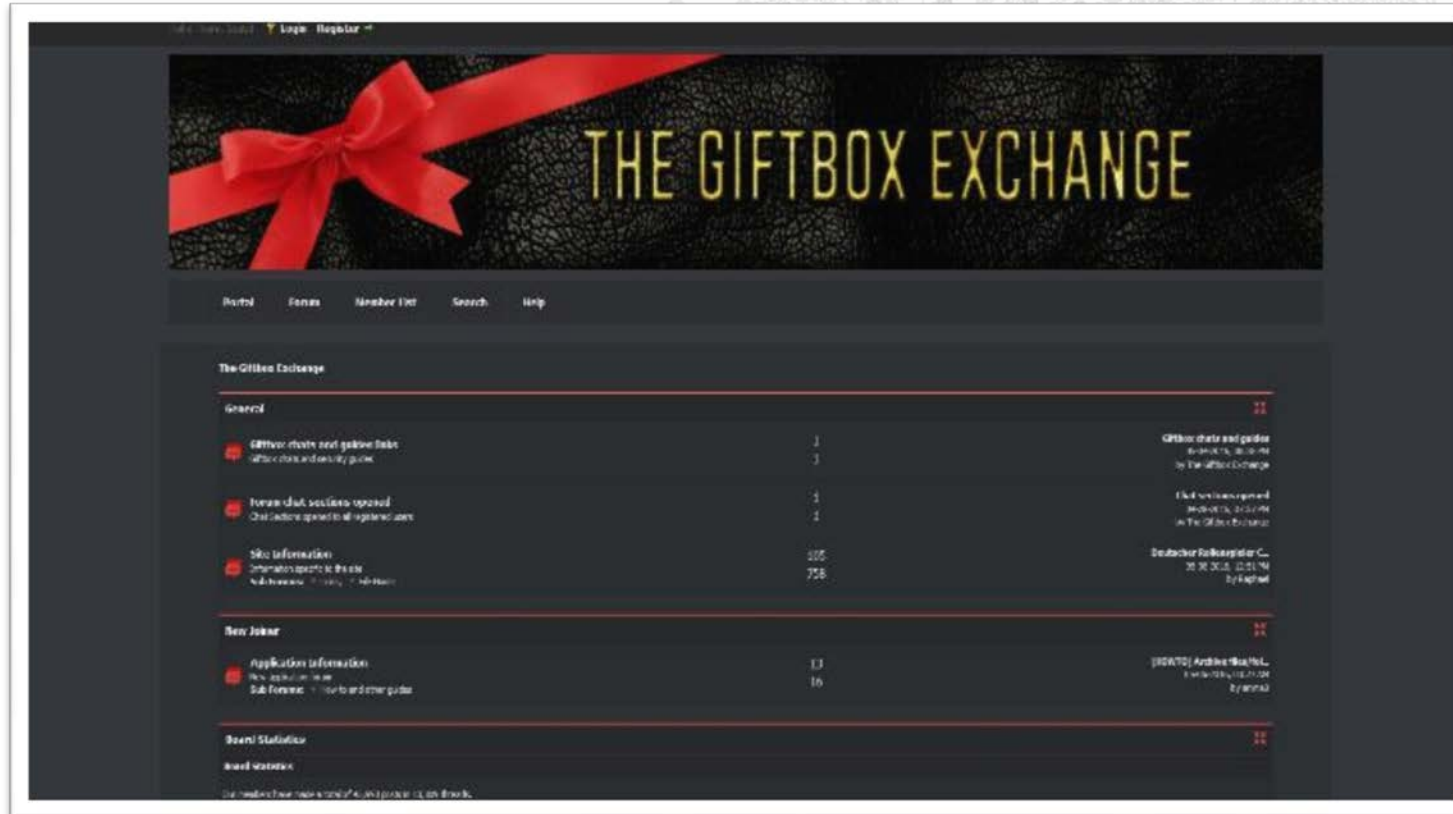
We do not give permission for upload of any illegal files.
If you chose to do so anyway, we are not responsible for your actions.

I've not got a infinite hard drive and the server cpu is limited so please don't upload too much or use resource intensive scripts.

Need Help?



Delitos
Imperfectos

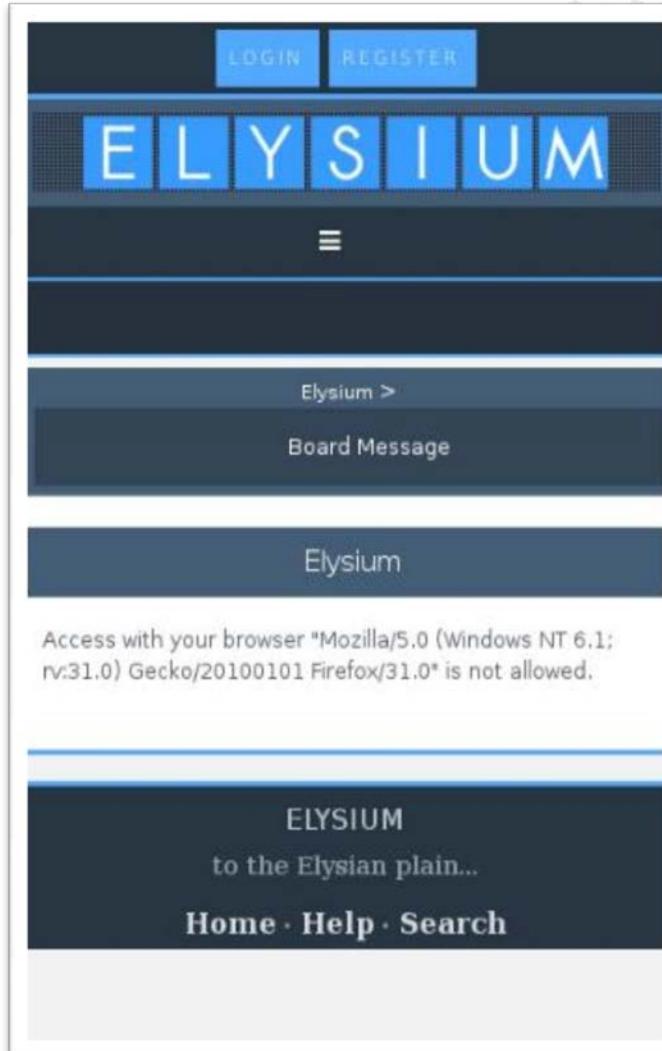


JavaScript

NEWS

Newly Uncovered Tor Browser Exploit Targeted Dark Web Child Porn Site

Delitos
Imperfectos



Cierran un portal de pornografía infantil en Alemania que contaba con 87.000 usuarios

Publicado: 7 jul 2017 00:42 GMT

Solo se podía acceder a la web a través de la llamada red oscura. Se han producido varias detenciones tanto en Alemania como en Austria.



Imagen ilustrativa
imago stock&people / www.globallookpress.com



Delitos
Imperfectos

Sentencian en EU a creador de sitio global de pornografía infantil

El FBI logró la detención del administrador principal de la red en la dark web, 'Playpen', la cual es considerada el sitio más grande en el mundo

Los arrestos iniciaron cuando Chase reveló por equivocación la dirección IP única en internet de Playpen, una ubicación EEUU



Delitos
Imperfectos

'Playpen' by the Numbers

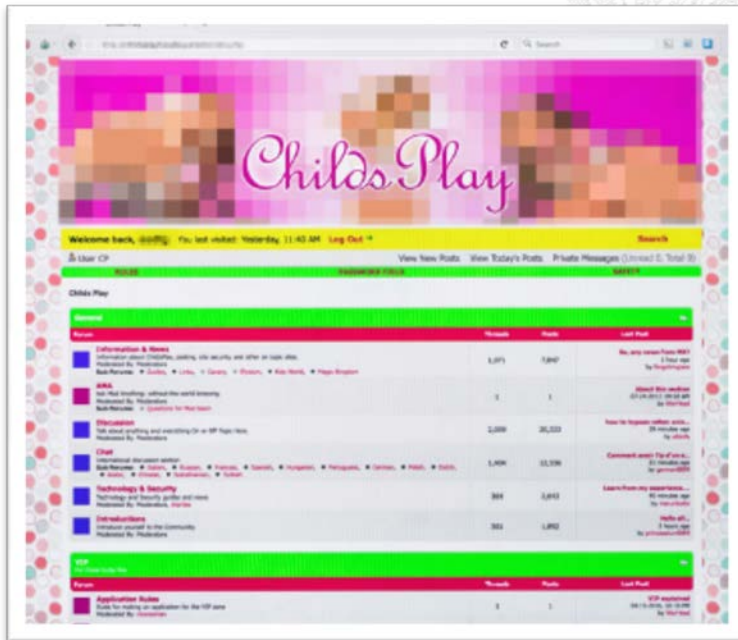
The ongoing investigation of the Playpen child pornography website and its members led to its takedown in 2015 and has produced the following results through continued efforts by law enforcement agencies around the world:



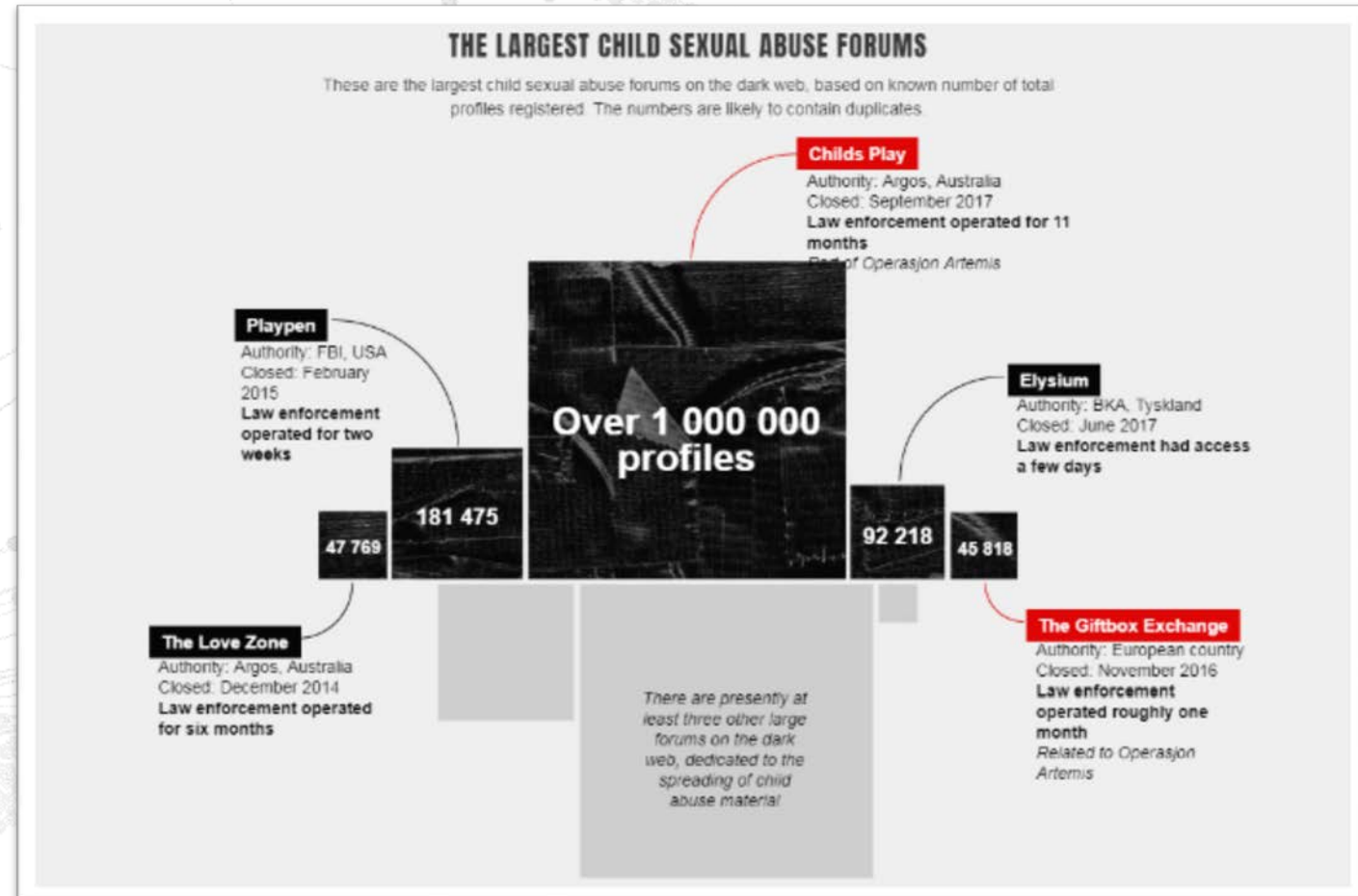
As of May 4, 2017

Operation Artemis: Australian police hijack world's largest paedophile site - and make 1,000 arrests

■ 'Child's Play' site on the dark web had more than 1 million profiles.



Undercover Australian police shared child porn with paedophiles for a YEAR after taking over the world's biggest abuse website to catch offenders



Delitos
Imperfectos



here is how we did it:

1. create a new site or login to an old one
2. login and set sftp password
3. login via sftp and create a symlink to /
4. disable DirectoryIndex in .htaccess
5. enable mod_autoindex in .htaccess
6. disable php engine in .htaccess
7. add text/plain type for .php files in .htaccess
8. have fun browsing files
9. find /home/fhosting
10. look at the content of the index.php file in /home/fhosting/www/
11. find configuration in /home/fhosting/www/_lbs/config.php
12. copy paste database connection details to phpmyadmin login
13. find active users with shell access in /etc/passwd
14. look through the scripts and figure out how password resets work
15. manually trigger a sftp password reset for the user 'user'
16. connect via ssh
17. run 'sudo -i'
18. edit ssh config in /etc/ssh/sshd_config to allow root login
19. run 'passwd' to set root password
20. reconnect via ssh as root
21. enjoy

+ 10.000 ONIONS
800 BASE DE DATOS
DUMPEO CONTENIDO SERVIDOR

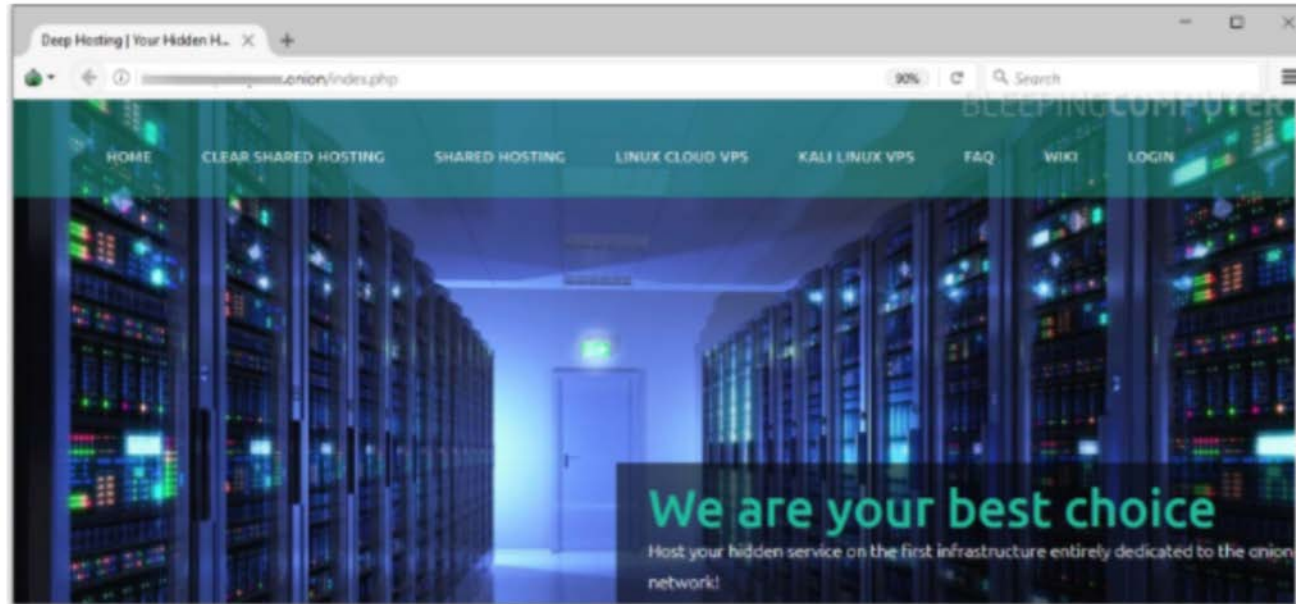


Delitos
Imperfectos

Dark Web Hosting Service Hacked, Some Data Was Stolen

By [Catalin Cimpanu](#)

July 10, 2017 10:45 AM 0



EXCLUSIVE — Deep Hosting — a Dark Web hosting service — admitted yesterday to suffering a major security incident during which "some sites have been exported."

The hack took place on Saturday afternoon and was carried out by a hacker calling himself Dhostpwned, the name he used when he spoke with Bleeping Computer earlier today.

```
23mg64vxd2t6kurv.onion
27mssu6jaqhuk6m.onion
33qvl5je5kif3jq.onion
3kqpypputjn2dhpp.onion
5ehtvruf2ef5h4h.onion
5xwgogyjnfcvrmvj.onion
654krjf5q6iupjot.onion
66xflun3ot54h6re.onion
6ccxadrr4g3qm7d.onion
acteamwneyw3ik2w.onion
alphaor4wguil6wo.onion
anpbcfvqjg2txyw4.onion
aom6u55durkpwaz.onion
assassinuyy7h425.onion
azo3mfttev62hfckw.onion
azvjv2ji2ucukemz.onion
b6kbmmeh5qivsr47.onion
bzip2k3z63s4js3mo.onion
c7wgwx7zlmqntm5.onion
cardobgwrj1zzqf1.onion
cbossftu5bjk5nx6.onion
ccguruetr5jwye5g.onion
cd2bkzjx7vq3gxc.onion
cerberxypcgoxiw5.onion
clonedxpjlq5764s.onion
dc5clejbfoaxcqbq.onion
dhostov5qbwyhwcw.onion
dhwikkgqceifior.onion
dpanely75rdnw7yv.onion
dxke6tzytgqvb6a.onion
e5nocpxm3rccdjeq.onion
e6wdnr4mcrzzefkt.onion
eurx66uednuvulfh.onion
feap5r11vmqi7lka.onion
g3n3bnjwhwokjco7.onion
g6ipitbghd6qutma.onion
gadmai6ebvzji6v6.onion
gbpoundzv2ot73eh.onion
edhvx3nvrnphnd5a.onion
```



1200 direcciones .onion
Varias temáticas delictivas
Una única IP

Fallo Humano



Delitos
Imperfectos

- **Dificultad de encontrar un error en la red TOR**
- **0 Day Tor Browser (TorMoi, Freedom Hosting, GiftBox) aprovechados en operaciones**
- **Tomar el control de un Hidden service (ChildsPlay)**
- **Ingeniería Social para desanonimización de usuarios**
 - **Ganar confianza**
 - **Uso de técnicas para sacar al usuario de Tor (Uso de determinados ficheros o malware)**
- **Servicio Vulnerable (Servidor Web, CMS, Plugin, credenciales débiles, errores de diseño ...)**
- **Fallo Humano para la desanonimización de servicios**
 - **Desconocimiento de los administradores del Hidden Service**
 - **Errores en la configuración**
 - **Servicios en Surface Web y Dark Web**



Delitos
Imperfectos

**Existe siempre una amenaza constante
para la cual no existe un parche
tecnológico efectivo:**

el ERROR HUMANO.

DEMO



LEAK

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

