



**SEXAGÉSIMO TERCER PERÍODO ORDINARIO DE SESIONES**  
Del 25 al 27 de abril de 2018  
México D.F., México

OEA/Ser.L/XIV.2.63  
CICAD/doc.2388/18  
25 abril 2018  
Original: Español

**ESPAÑA - TENDENCIAS EN LA VENTA DE DROGAS SINTÉTICAS Y NSP A TRAVÉS DE INTERNET: DARKNET, CRIPTOMONEDAS Y USO DE SISTEMAS  
POSTALES**

# Tendencias en la venta de drogas sintéticas y NSP a través de internet:

## Darknet, Criptomonedas y uso de sistemas postales

Roberto Fernández Alonso

Inspector Jefe

Unidad Central de  
Ciberdelincuencia

Policía Nacional, España

**OEA/CICAD**

Ciudad de México 26 de abril de 2018

# Introducción – Impacto de las nuevas tecnologías

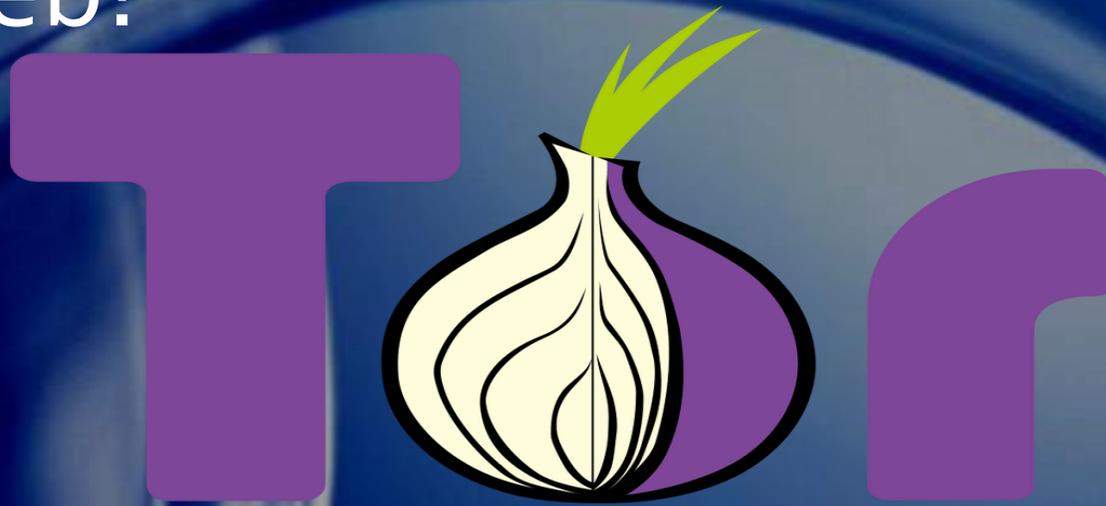
Pasado muy cercano → Delitos tradicionales y delitos tecnológicos (intrusiones y explotación sexual infantil)

Presente → delitos tradicionales apoyados de las nuevas tecnologías y delitos tecnológicos + sofisticados y especializados

Gran impacto de las nuevas tecnologías → anonimización, encriptación (uso de TOR, criptomonedas). Volumen de dispositivos electrónicos

Rápido avance de las nuevas tecnologías y necesidad de actualización

# ¿Cómo navegar por la Darkweb?



The **Onion Router** (enrutamiento de Cebolla). Es un proyecto cuyo objetivo principal es el desarrollo de una **red de comunicaciones distribuida y superpuesta sobre Internet**, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela su **identidad**, es decir, su dirección IP (anonimato a nivel de red) y que, además, mantiene la integridad y el secreto de la información que viaja por ella.

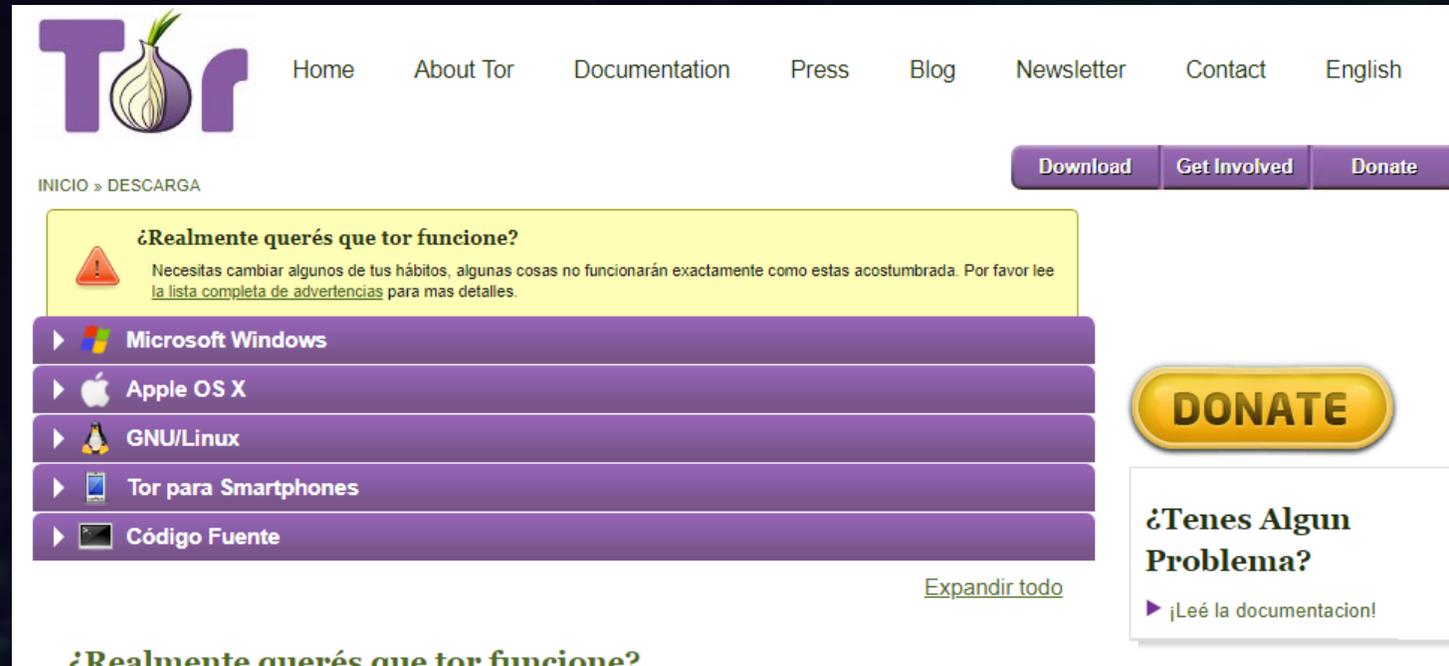
“Wikipedia”



# ¿Cómo navegar por la Darkweb? USO TOR BROWSER

*Tor browser* habitualmente se instala junto con un proxy local HTTP (*Privoxy*) que realiza las conexiones con la red Tor

- Se puede descargar como un *bundle* que lleva todo incluido
- Descarga: <https://www.torproject.org/download/download>



The screenshot shows the Tor Project website. At the top left is the Tor logo (a purple onion). To its right are navigation links: Home, About Tor, Documentation, Press, Blog, Newsletter, Contact, and English. Below these are three buttons: Download, Get Involved, and Donate. A yellow warning box contains the text: "¿Realmente querés que tor funcione? Necesitas cambiar algunos de tus hábitos, algunas cosas no funcionarán exactamente como estas acostumbrada. Por favor lee la lista completa de advertencias para mas detalles." Below this is a list of operating systems with expandable arrows: Microsoft Windows, Apple OS X, GNU/Linux, Tor para Smartphones, and Código Fuente. To the right of this list is a large yellow "DONATE" button. Below the donate button is a box with the text "¿Tenes Algun Problema?" and a link "¡Leé la documentacion!". At the bottom right of the list is a link "Expandir todo". At the bottom left of the page, the text "¿Realmente querés que tor funcione?" is repeated.

# ¿Cómo navegar por la Darkweb? USO TOR BROWSER



The screenshot shows the Tor Project website's 'About Tor' page. The browser's address bar displays the URL <https://www.torproject.org/about/overview.html.en>. The navigation menu includes 'Home', 'About Tor' (highlighted), 'Documentation', 'Press', 'Blog', 'Newsletter', and 'Contact'. On the right, there are buttons for 'Download', 'Volunteer', and 'Donate'. A left sidebar contains a list of links: 'Tor Overview' (highlighted), 'Users of Tor', 'Tor People', 'Jobs', 'Sponsors', 'Financial Reports', 'Projects', and 'Documentation'. The main content area features the heading 'Tor: Overview' and a 'Topics' list with links to 'Overview', 'Why we need Tor', 'The Solution', 'Staying anonymous', and 'The future of Tor'. Below this is an 'Overview' section with a highlighted first sentence: 'The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.'

<https://www.torproject.org/about/overview.html.en>

 Home **About Tor** Documentation Press Blog Newsletter Contact

Download Volunteer Donate

HOME » ABOUT »

- Tor Overview**
- Users of Tor
- Tor People
- Jobs
- Sponsors
- Financial Reports
- Projects
- Documentation

## Tor: Overview

### Topics

- [Overview](#)
- [Why we need Tor](#)
- [The Solution](#)
- [Staying anonymous](#)
- [The future of Tor](#)

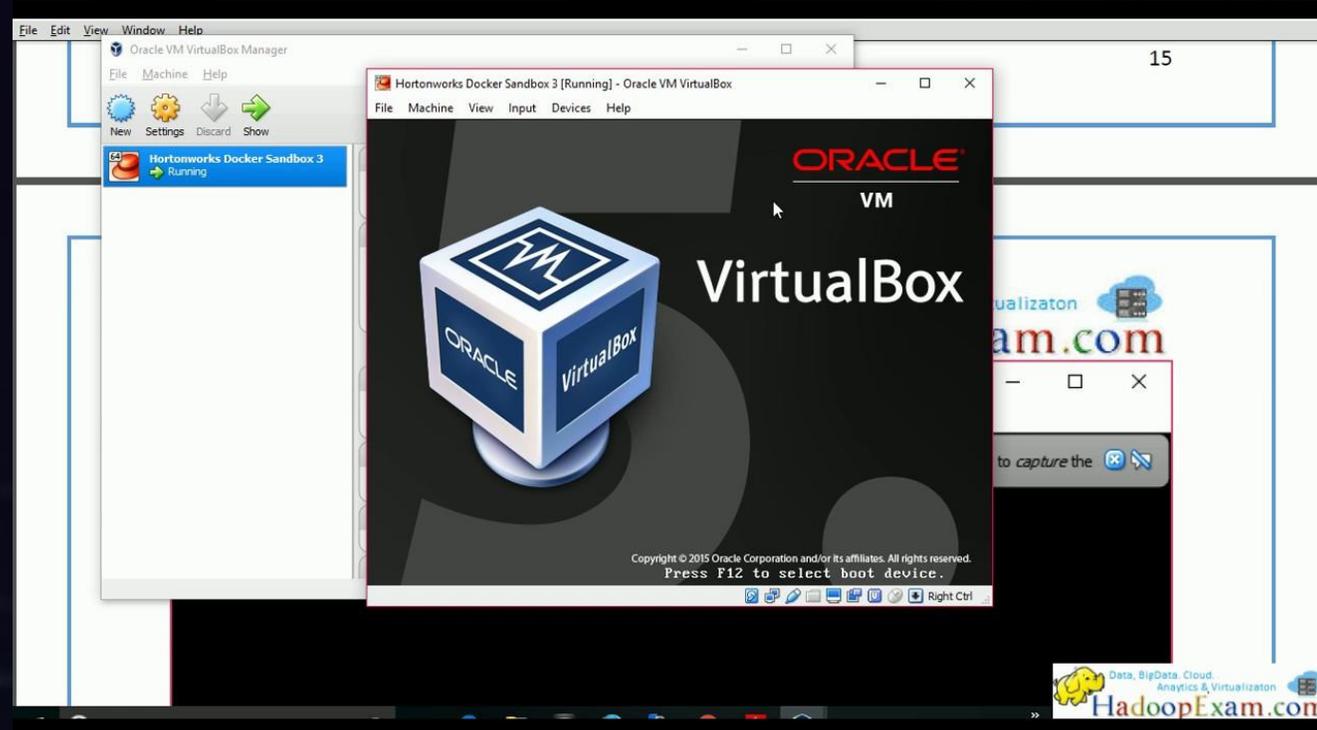
### Overview

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features.

# ¿Cómo navegar por la Darkweb?

## Uso de TOR a través de Sandbox:

- Mecanismo para ejecutar programas con seguridad y de manera separada
- A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros



# Criptomonedas. Su uso en el pago de productos

## Características

- **Descentralizadas y convertibles**
- **Basadas en algoritmo criptográficos**
- **Sistema de claves pública-privada.**
- **Integridad y seguridad del sistema, lo gestiona la comunidad de usuarios**
- **Limitado el número de divisas**

# Criptomonedas. Su uso en el pago de productos

“Las divisas virtuales son un tipo de dinero digital, no regulado, expedido y controlado por sus desarrolladores y usado y aceptado por los miembros de una comunidad virtual específica”

*Banco Central Europeo (2012)*



Costes de Transacción

Tiempo de procesamiento de la transacción

Facilita el comercio internacional

Fuera del control de la autoridades estatales

Anonimato

Favorece el blanqueo de capitales



# Criptomonedas. Su uso en el pago de productos

**MONEDEROS VIRTUALES.-** Permiten al usuario crear y gestionar sus cuentas y hacer transferencias, disponen de medias de seguridad y permiten tener carteras en la "nube"



Bitcoin Core



MultiBit HD



Electrum



mSIGNA



Bitcoin Wallet



breadwallet



Bither



GreenBits



Coinomi



Copay



Airbitz



Mycelium

#	Nombre	Símbol...	Precio (USD)	Ca
1	Bitcoin	BTC	8.118,5	
2	Ethereum	ETH	515,55	
3	Ripple	XRP	0,69290	
4	Bitcoin Cash	BCH	884,82	
5	Litecoin	LTC	138,62	
6	EOS	EOS	8,7731	
7	Cardano	ADA	0,25568	
8	Stellar	XLM	0,34562	
9	NEO	NEO	70,917	
10	IOTA	MIOTA	1,61951	
11	Monero	XMR	226,25	
12	NEM	XEM	0,36437	
13	Dash	DASH	404,02	

# Criptomonedas. Su uso en el pago de productos

**BLOCKCHAIN.** Registro de todas transacciones, carácter público, determina los bitcoins que tiene cada cuenta, se actualiza por la comunidad de usuarios mediante un proceso llamado "minería" (<https://blockchain.info/es>)

## EXCHANGERS:

- Bitstamp, Localbitcoins, Kraken
- Bitfinex, Coinbase, Bitnovo, cex.io



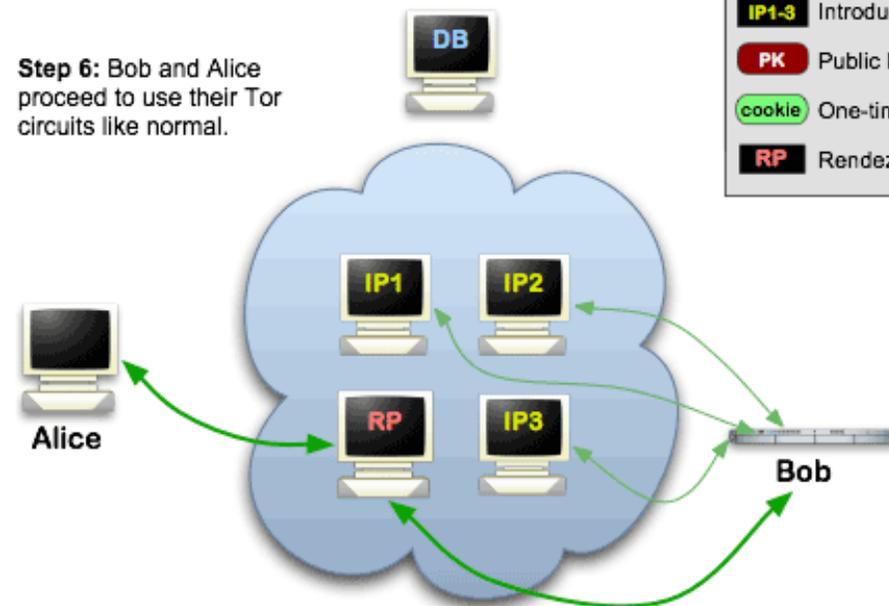
# Darkmarkets - Mercados negros

- La forma de acceder es con el navegador TOR
- No existe conexión directa entre cliente y servicio oculto
- Existen puntos introductorios que generan caminos y enrutan los paquetes mediante un circuito al servicio oculto
- Los "Criptomercados" permiten pago con criptomonedas (Bitcoins, Monero, Litecoin...)
- <https://www.deepdotweb.com/marketplace-directory/listing/>



## Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



# Darkmarkets - Mercados negros

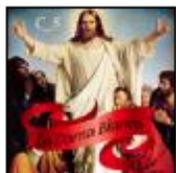
EXISTES DOS TIPOS DE MERCADOS:

- **1. CRIPTOMERCADOS**, donde existen múltiples vendedores ("vendors"). Existe administrador que se lleva parte de comisión de las ventas. Ofrecen servicio de protección frente a pagos. Fideicomiso ("scrow"). FEEDBACK. Respuesta frente a scammers ("scamwatch")
- **2. TIENDAS DE VENDEDORES** ("single-vendor markets"). Único "vendor". Sin comisiones
- ¿QUÉ ES MÁS FIABLE ENTRE LOS COMPRADORES?
- Los criptomercados tienen generalmente secciones en su página web que enumeran reglas tanto para los vendedores como los compradores relacionadas con la transacción y las medidas de seguridad asociadas.



# Darkmarkets - Mercados negros

## chemicals\_spain | User Profile



**chemicals\_spain** ( 3398 ) **Vendor Level 8** **Trust Level 7**

Positive feedback (last 12 months): 99%  
[How is the feedback score calculated?]

Member since: March 26, 2015  
Contracts: 0 in progress, 0 complete

[View Store](#)

[Send Message](#)

[Favorite](#)

[Blacklist](#)

**FE Allowed**

### Seller Feedback Ratings

(last 12 months)

### Buyer Statistics

(since join date)

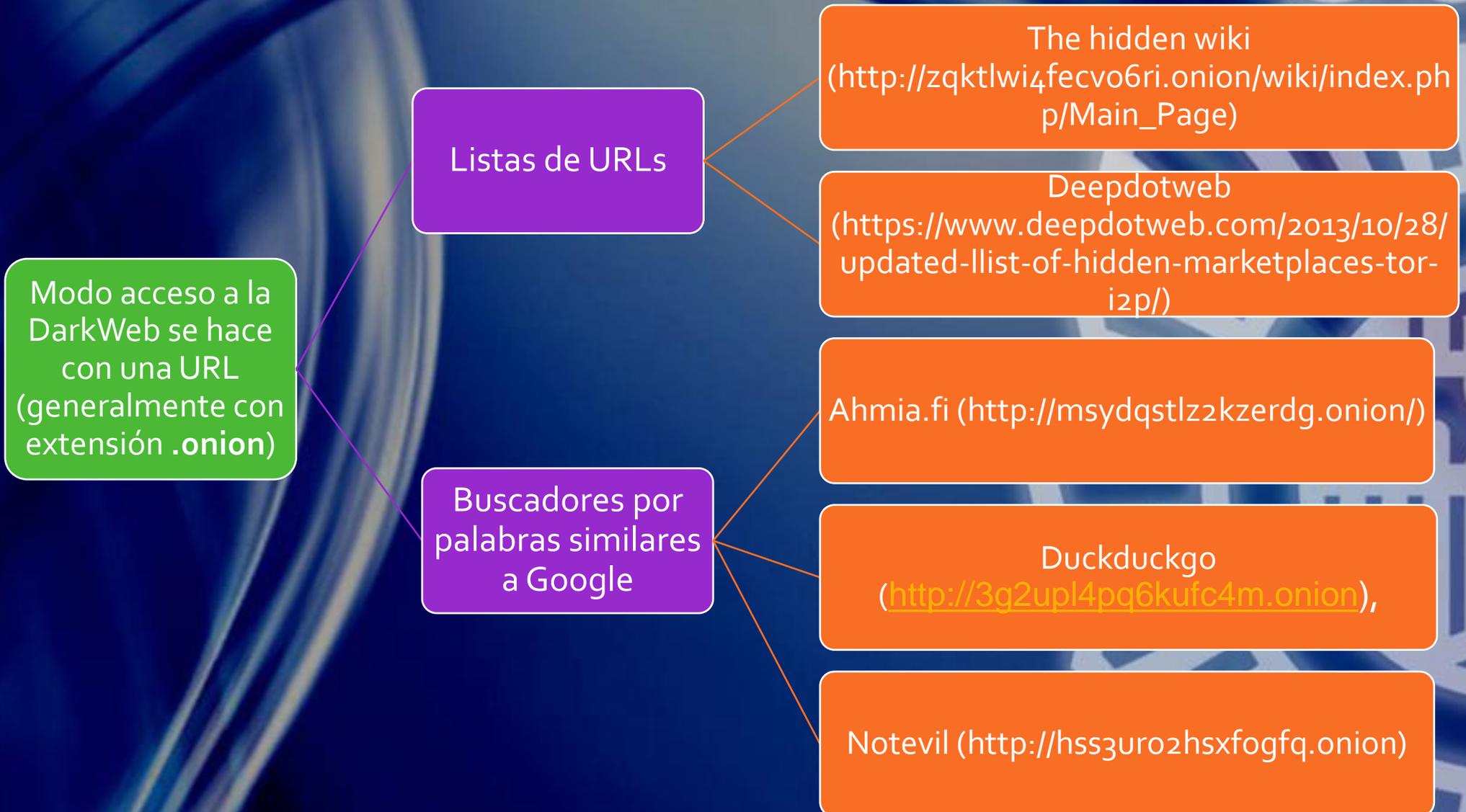
	1 month	6 months	12 months		Since join	
Positive	156	878	900	Total disputes / orders	0 / 2	
Neutral	2	14	7	Total spendings	---	
Negative	0	2	3	Feedback left	2 (100.0% positive)	
				Last online	Feb 14, 2017	
				Stealth	Quality	Value for price
				★★★★★	★★★★★	★★★★★

Detailed seller ratings:

- Fantastic quality, in the mailbox within a few days, and thank you for the friendly price!
- new user. update on arrival
- new user. update on arrival
- New user. Update on arrival
- FE for legendary CS, will update upon arrival



# Darkmarkets - Mercados negros



# Operación Torre – Aspectos destacables

- Incremento de la venta ilegal de medicamentos por Internet
- Desarticulación de la mayor red criminal en España dedicada a la importación, venta y distribución ilegal de medicamentos por Internet. Los medicamentos eran importados desde la India utilizando la Darkweb y criptomonedas (BITCOINS)
- Más de 6000 clientes en España a través de páginas web que operaban con la apariencia de farmacias legales y empresas de distribución postal

# Operación Torre – Investigación

Investigación de carácter multidisciplinar

Investigación  
tecnológica



Investigación  
patrimonial



Investigación  
convencional



O.L.A.



# Operación Torre - Investigación

1. Logística inversa de paquetería → Empresas ficticias
2. Colaboración empresas de paquetería → Listado envíos empresa ficticia (+20k)
3. Identificación del entramado → Técnicas OSINT + Big Data + Investigación Tradicional
4. Localización de diferentes plataformas y páginas web de venta
5. Intervenciones telefónicas + Vigilancia
6. Toma de declaración a compradores → Entrega de muestras
7. Interceptación de paquetería para su escaneo → Rayos X
8. Preparación del dispositivo → EyR + Detenciones + Investigados



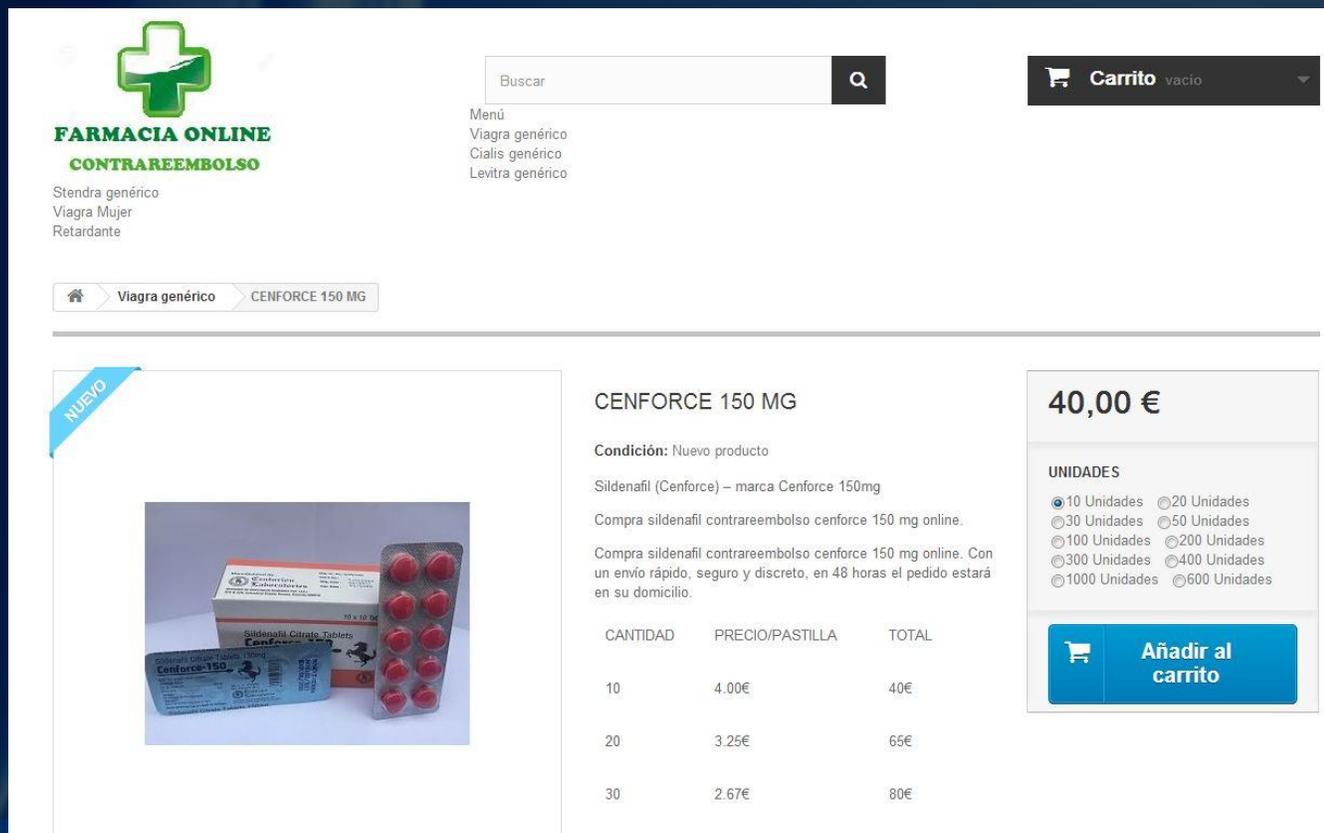
# Identificación del entramado

Análisis de unos 20.000 envíos realizados a toda España por la organización desde marzo hasta diciembre de 2017.



# Identificación del entramado

En el análisis del tráfico de Internet se detectan navegaciones recurrentes a una página web que contenía una tienda online de venta de productos contra la disfunción eréctil.



**FARMACIA ONLINE**  
CONTRAREEMBOLSO

Stendra genérico  
Viagra Mujer  
Retardante

Buscar

Carrito vacío

Menú  
Viagra genérico  
Cialis genérico  
Levitra genérico

Viagra genérico CENFORCE 150 MG

**NUEVO**

**CENFORCE 150 MG**

**40,00 €**

**CONDICIÓN:** Nuevo producto

Sildenafil (Cenforce) – marca Cenforce 150mg

Compra sildenafil contrareembolso cenforce 150 mg online.

Compra sildenafil contrareembolso cenforce 150 mg online. Con un envío rápido, seguro y discreto, en 48 horas el pedido estará en su domicilio.

CANTIDAD	PRECIO/PASTILLA	TOTAL
10	4.00€	40€
20	3.25€	65€
30	2.67€	80€

UNIDADES

10 Unidades  20 Unidades  
 30 Unidades  50 Unidades  
 100 Unidades  200 Unidades  
 300 Unidades  400 Unidades  
 1000 Unidades  600 Unidades

**Añadir al carrito**

# Identificación del entramado

Extracción de contraseñas de administrador de la intervención telefónica mediante *man-in-the-middle* (MitM)  
Autorización judicial para entrada al panel de administrador de la página web utilizando dichas credenciales

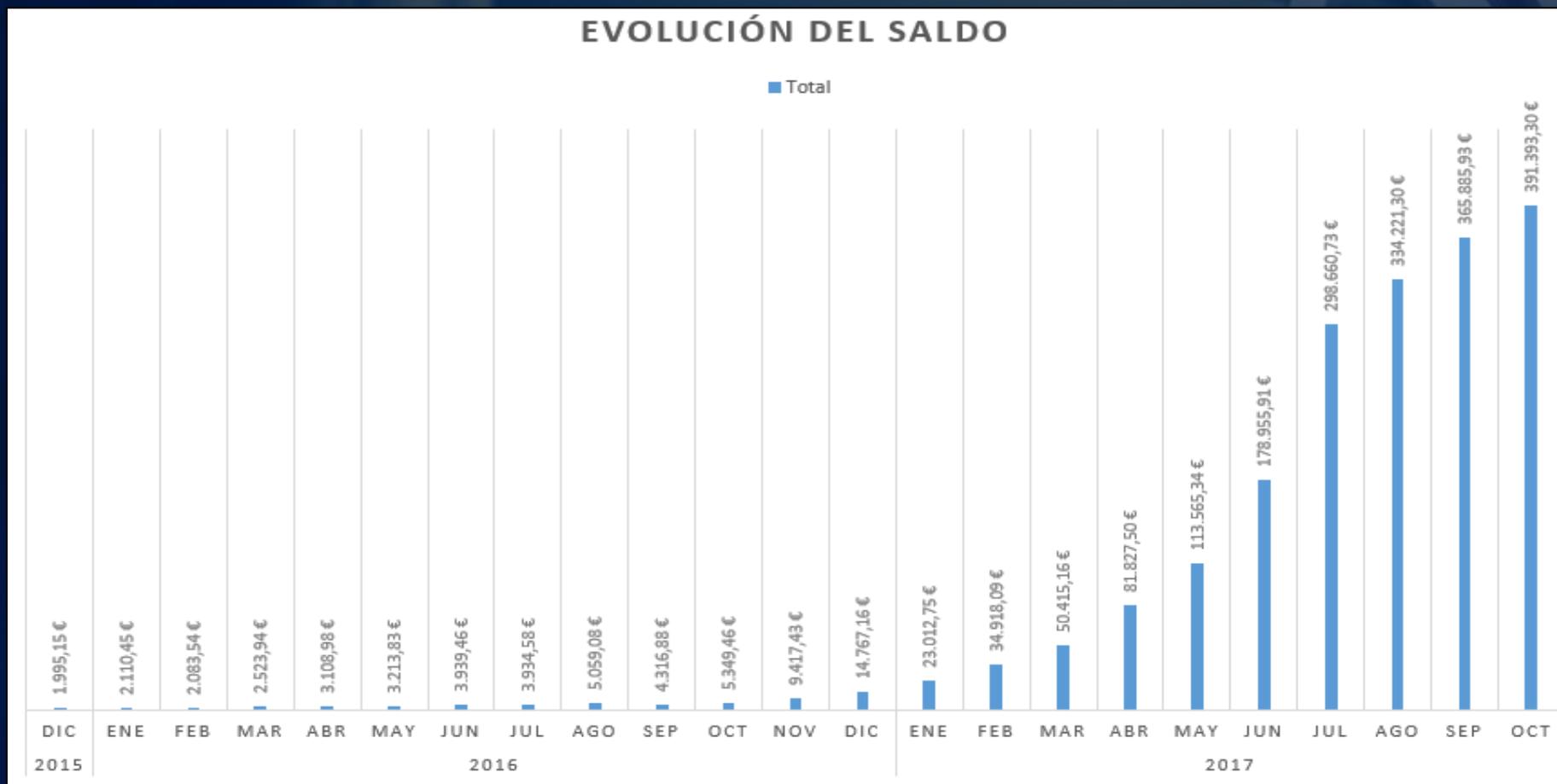
Descarga de BBDD SQL y borrado de rastro dejado por los investigadores

Preparación de servidor web local con el CMS Prestashop, importación BBDD SQL con datos de los pedidos realizados por los clientes (unos 6000)

Identificación de monederos virtuales y uso de TOR

# Identificación del entramado

Beneficios obtenidos por la organización criminal. (Mar 2017 incremento)



# Preparación y ejecución del Operativo



- Más de 100 funcionarios
- 12 EyR en 6 ciudades españolas
- 25 detenidos

# Medicamentos intervenidos



# Medicamentos intervenidos



# Medicamentos intervenidos



# Medicamentos intervenidos



# Medicamentos intervenidos



# Medicamentos intervenidos



# Operación Torre – Resultados

- 25 personas detenidas
- 12 entradas y registros
- Más de 500.000 unidades de medicamentos contra la disfunción eréctil
- 65.000€ en Bitcoins en varios monederos virtuales
- 23.000€ en metálico
- 320.000€ bloqueados en cuentas bancarias
- Documentación y dispositivos electrónicos
- Clausura e intervención de las web

# Operación Torre - Prensa

## Cae una red de venta ilegal de medicamentos por Internet que pagaba con bitcoins a sus proveedores

25 personas han sido detenidas acusadas de integrar una organización de venta ilegal de medicamentos por Internet de España que distribuía unos 60 tipos de fármacos, la mayoría relacionados con la disfunción eréctil y la pérdida de peso, a más de 6.000 clientes.

 politica.elpals.com     

## Cae la mayor red de venta ilegal de medicamentos por internet



 elperiodico.com

## Desarticulada la mayor red de venta ilegal de medicamentos con 25 detenidos



 elmundo.es

## Cae la mayor red de venta ilegal online de medicamentos de disfunción eréctil y tratamiento adelgazante

El grupo usaba criptomonedas para dificultar el rastreo policial y tenía su centro operativo en el Puerto de Santa María (Cádiz) MADRID, 15 Feb.

 europapress.es

## Desarticulada en el Puerto de Santa María la mayor red de venta ilegal de medicamentos por internet de España



 canalsur.es

## Cae la mayor red de venta ilegal online de medicamentos de disfunción eréctil y tratamiento adelgazante



 hoy.es

## La Policía interviene 400.000 pastillas para adelgazar y estimulantes sexuales

La Policía Nacional da por desarticulada la que sería la mayor red hasta ahora de distribución ilegal de medicamentos a través de páginas web con apariencia de farmacias legales dedicadas a la distribución de una amplia gama de fármacos, la mayoría dedicados a la disfunción eréctil y los

 cadenaser.com

## Cae la mayor red de venta ilegal de medicamentos por internet en España con 25 detenidos

La Policía Nacional ha desarticulado la mayor red de venta ilegal de medicamentos a través de internet que funcionaba en España en una operación en la que ha intervenido más de 400.000 unidades de 62 tipos distintos de fármacos y ha detenido a 25 personas, informa

 rtve.es



# Operación Torre – Postdetención

1. Análisis dispositivos intervenidos → Pagos en Bitcoin a través de diferentes exchangers → Localización empresa proveedora
2. Localización del origen de los medicamentos → Técnicas OSINT + BBDD policiales + Análisis conversaciones WhatsApp
3. La investigación sigue abierta

MUCHAS GRACIAS POR SU  
ATENCIÓN

PREGUNTAS



POLICÍA NACIONAL



**UNIDAD CENTRAL DE CIBERDELINCUENCIA  
COMISARÍA GENERAL DE POLICÍA JUDICIAL  
POLICÍA NACIONAL**



*The End*

**Inspector Jefe, Roberto Fernández Alonso**

**[redesabiertas@policia.es](mailto:redesabiertas@policia.es)**

**[rfa@policia.es](mailto:rfa@policia.es)**

**[Tlf. +34 91-582-41.79](tel:+34915824179)**

